IBM Tivoli Access Manager for e-business v3.9
Technical Update Workshop

Hands-on Labs

15th April 2002

Oleg Bascurov
Gianluca Gargaro
Jon Harry
Jeff Miller

Table of Contents

1 Introduction

This hands-on lab was written for use in Access Manager v3.9 workshops. It covers some of the major new functions introduced in AM 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
- Access Manager Integration with WebSphere
- Form-based Single Sign-on
- Access Manager Plug-in for Web Servers

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.

1.1 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.

1.2 Addition information resources

If you want additional information while you are going through these labs then please refer to the AM v3.9 Technical Update class notes or the product publications. Copies of the Access Manager publications are available in **D:\Publications** directory.

1.3 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:\>ping -a x.x.x.x
```

Where x.x.x.x is the IP address from the ***ipconfig*** command.

1.4 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*
- *Adobe Acrobat v4.05*

Before starting the Access Manager exercises you will need to have the pre-requisite software installed and configured. This may have been done for you but, if not (or you are following these labs "at home"), then instructions for the following are in Appendix A:

1) IBM HTTP Server 1.3.19
2) GSKit 5
3) DB2 UDB 7.2 plus Fixpack-4

Of course Access Manager also requires a User Registry, so you also need one of the following installed and configured. 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

- 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 Access Manager 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 other lab features.

To install & configure WebSphere 4.02 use the instructions in Appendix B.

1.5 Default Configurations

1.5.1 File Locations

Option	Value
DB2	*C:\SQLLIB*
IBM HTTP Server	*C:\Program Files\IBM HTTP Server*
Access Manager	*C:\Program Files\Tivoli\Policy Director*
WebSphere Application Server	*C:\WebSphere\AppServer*
IBM Java 2 v1.3.0 (included with WAS)	*C:\WebSphere\AppServer\java*
IBM Java 2 JRE v1.3.0 (included with WAS)	*C:\WebSphere\AppServer\java\jre*
Hands-on files	*D:\LabFiles*

1.5.2 IBM Directory Server Configuration Options

Option	Value
Directory Administrator ID	cn=root
Directory Administrator Password	passw0rd
Directory Server Hostname	*<yourhost>.pic.uk.ibm.com*
Suffix	o=ibm,c=gb
Directory Server Port	38900
Installation Directory	*C:\Program Files\IBM\LDAP*

1.5.3 Active Directory Server Configuration Options

Option	Value
Directory Administrator ID	Administrator
Directory Administrator Password	passw0rd
Directory Server Hostname	*<yourhost>.pic.uk.ibm.com*
Suffix	dc=<yourhost>,dc=com
Directory Server Port	389
Installation Directory	(system)

1.5.4 Domino Server Configuration Options

Option	Value
Directory Administrator ID	Notes Admin
Domino Domain	PIC
Directory Administrator Password	passw0rd
Directory Server Hostname	*yourhost.pic.uk.ibm.com*
Directory Server Port	3890
Installation Directory	*C:\Lotus\Domino*

1.6 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:

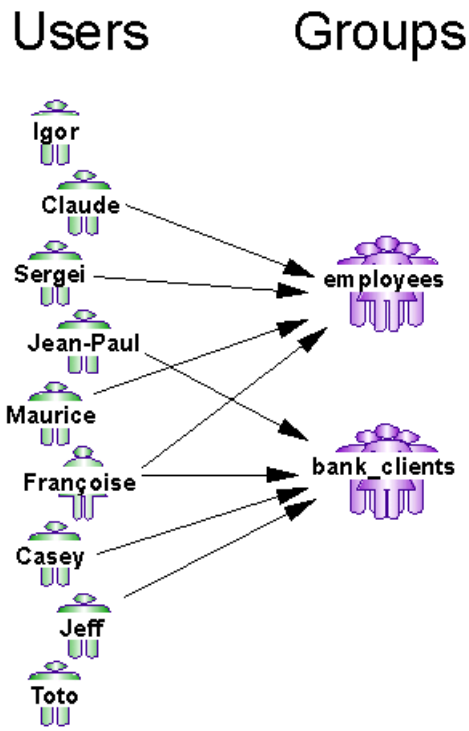
User ID	Password	Purpose
Administrator	*passw0rd*	Machine and directory passw0rd
db2admin	*passw0rd*	Administer DB2
sec_master	*passw0rd*	Access Manager administrator
wasadmin	*passw0rd*	WebSphere administrator
was4jvm	*passw0rd*	Represents the WebSphere JVM in PD

You will also use several ports for HTTP. For reference, here are the lab defaults:

Port	Purpose
80	HTTP Port for WebSEAL
82	TCP Tunnel input port
443	HTTPS Port for WebSEAL
888	HTTP Port for IIS
4444	HTTPS Port for IBM HTTP Server
8000	HTTP Port for Domino HTTP Server
8888	HTTP Port for IBM HTTP Server
9080	Port for WebSphere embedded Web server

1.7 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 any groups.

1.8 Useful utilities

In order to make the most of these labs the following utilities can be used.

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.

TCPTunnel This is a JAVA application that allows TCP traffic to be analysed. It ships in the SOAP jar files that come with WebSphere. A batch file is provided for easy launching of this class.

You may want to create a couple of BAT files yourself that make it easier to CD to the AM directories.

AM.bat This could be a batch file that changes the working directory to the default AM install directory, *C:\Program Files\Tivoli\Policy Director*

AMweb.bat This could be a batch file that changes the working directory to the default WebSEAL install directory, *C:\Program Files\Tivoli\PDWeb*

2 Installing Access Manager

2.1 Setup

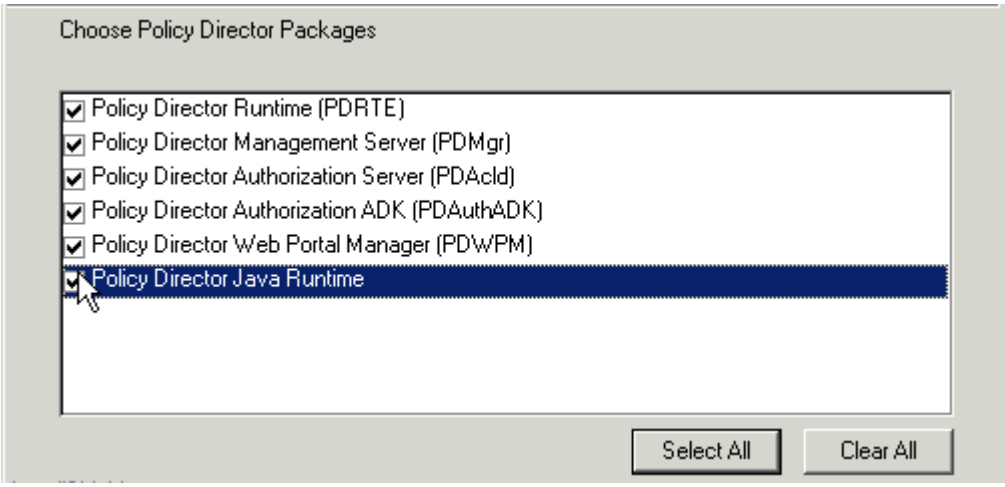
Installation of Web Portal Manager requires that WebSphere Application Server be installed on your machine. This should already be done (per the procedure in 17 Appendix B -- WebSphere Installation). To check WebSphere is installed open a DOS window and enter

```
C:\>echo %WAS_HOME%
C:\WebSphere\AppServer
```

Use Windows Explorer to open the drive where the *Access Manager* code images are located under the *D:\LabFiles\AMImages* directory. This directory has four subdirectories:

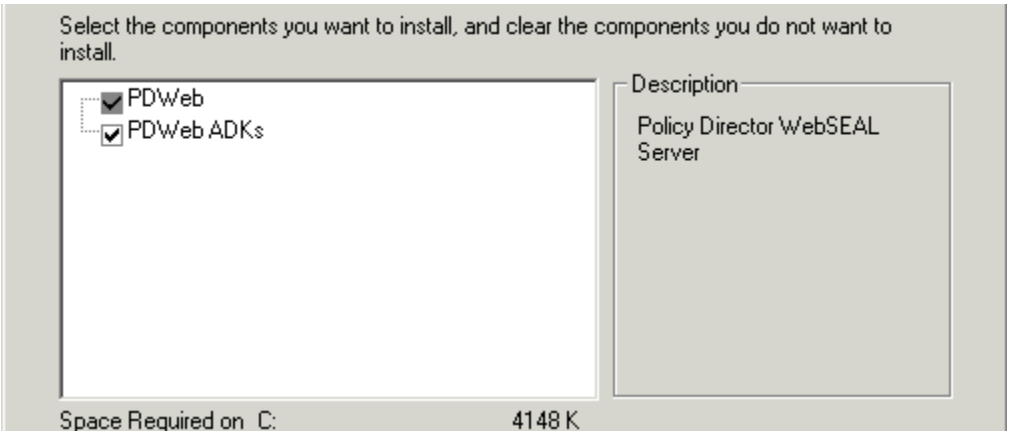
- pd
  - Access Manager setup directory
- pdweb
  - AM WebSEAL setup directory
- pdwas
  - AM for WebSphere Application Server setup directory
- pdwebpi
  - AM Web Plug-in setup directory

Under *pd* launch the *Setup.exe* file by double-clicking on it.



Select all the components and click Next to start the install of the Access Manager files on your machine.

When asked, do not reboot now but navigate to *pdweb* double-click *Setup.exe* to install WebSEAL.



Select all the components for WebSEAL. This will install the Access Manager files on your machine.

The products are now installed but still need to be configured. Reboot your machine.

3 Configure Access Manager with Your User Registry

There are five Access Manager installed packages and each needs to be configured for full AM functionality. All but the first, AMRTE, are the same regardless of the directory server underneath. In this lab, choose the AMRTE section that corresponds to your directory server. Do that part and then skip to section 3.4 Finishing Access Manager Configuration on Your Directory Server that covers configuring the four remaining packages.

3.1 Configuring AMRTE with IBM Directory Server

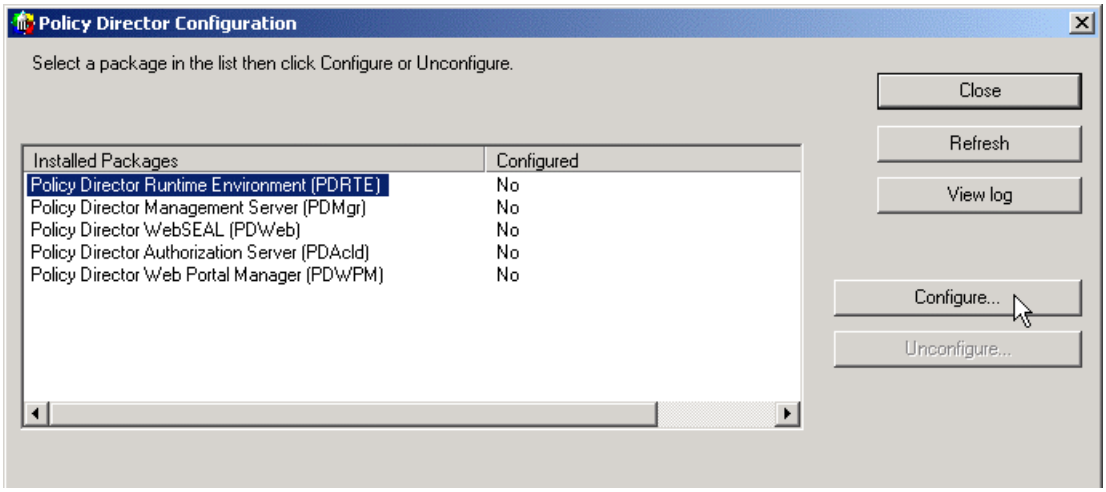
3.1.1 Considerations

IBM Directory Server 3.2.2 should already be installed and configured to listen on port 38900 as per the instructions in section 16.4 Installing IBM SecureWay Directory Server 3.2.2. All the Access Manager components should also be installed in order to start the configuration process.

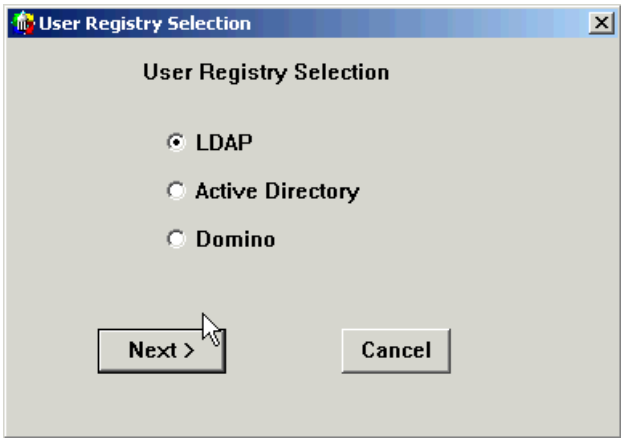
First start your user registry.

3.1.2 Configuration of AMRTE using IBM Directory Server 3.2.2

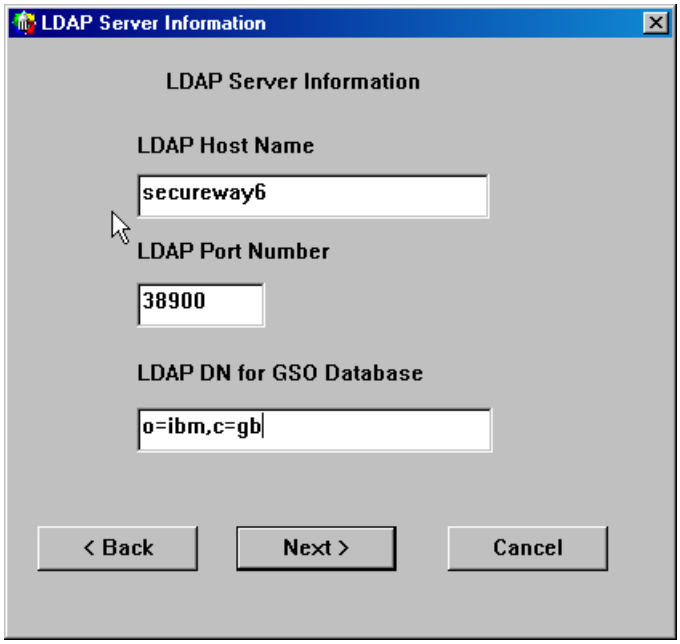
To begin configuration, select START->Programs->Access Manager->Configuration.



This displays the Access Manager Configuration dialog. Select AM Runtime and click Configure....

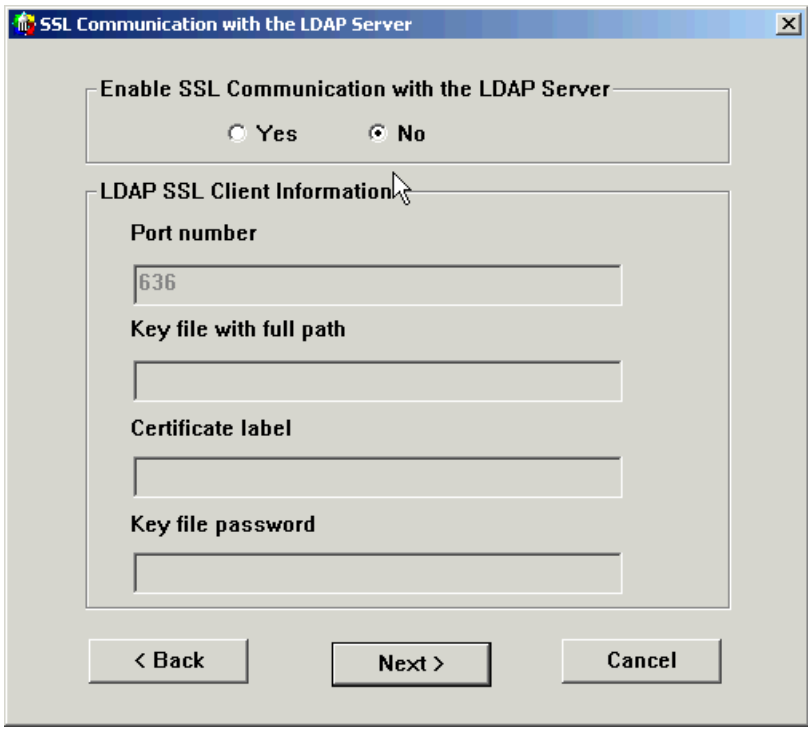


Select LDAP as user registry. Click Next.

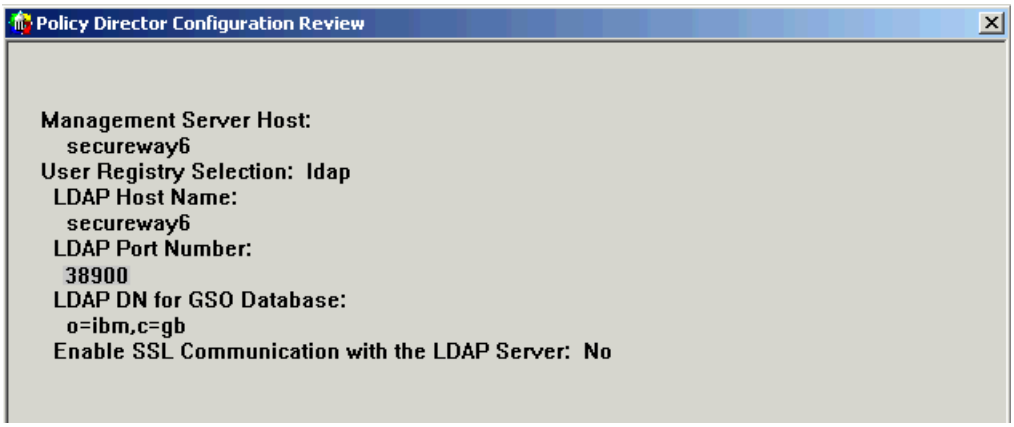


Provide the information as per the table in section 1.5.2 IBM Directory Server Configuration Options. Set the LDAP Host Name to that of your machine. Note that the default port of 389 is changed to 38900. This is because Active Directory also uses 389 by default and it is unable to use another. So to keep all the lab machines consistent, 389 is reserved for Active Directory, 3890 for Domino, and 38900 for IBM LDAP.

Click Next.



These labs don't require SSL for communication between the LDAP client and server, hence disable this feature. Click Next.



At this point the configuration procedure has all the info required to start and will show you what was provided, simply click on Finish to proceed. Now go to section 3.4 Finishing Access Manager Configuration on Your Directory Server to continue.

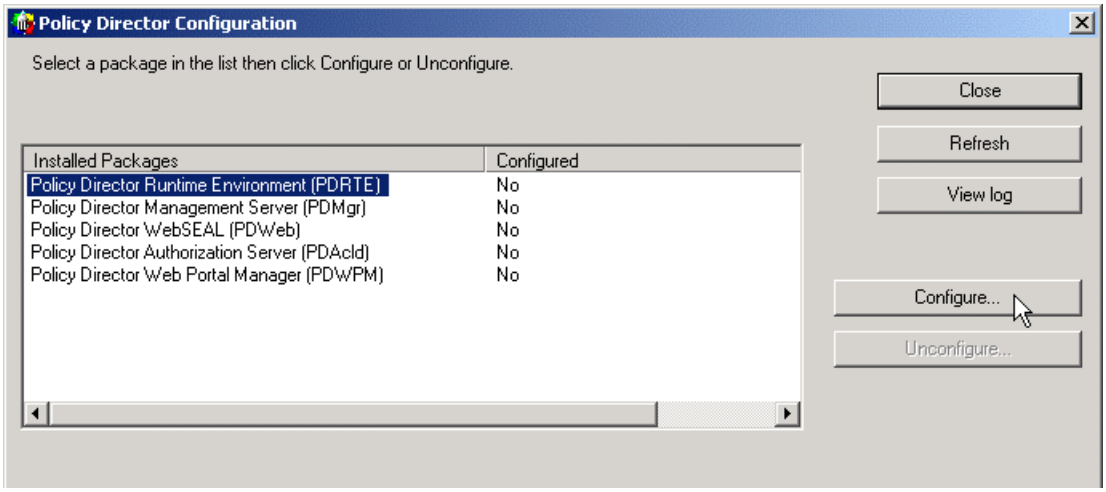
3.2 Configuring AMRTE with Active Directory

3.2.1 Considerations

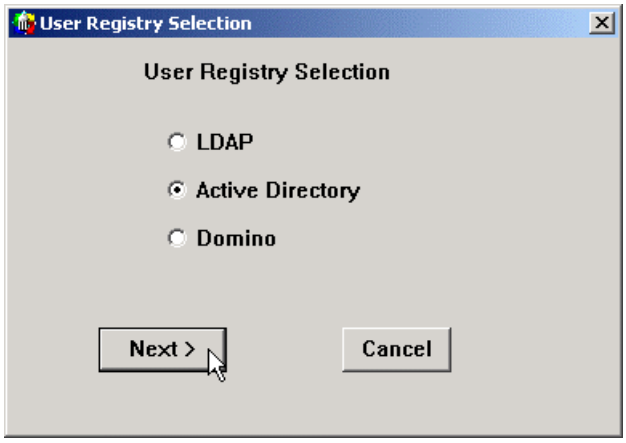
Active Directory should already be installed on your machine with a DNS fully configured. Access Manager should also be installed but not configured. These instructions start with Access Manager configuration and use Active Directory as the LDAP server.

3.2.2 Configuration

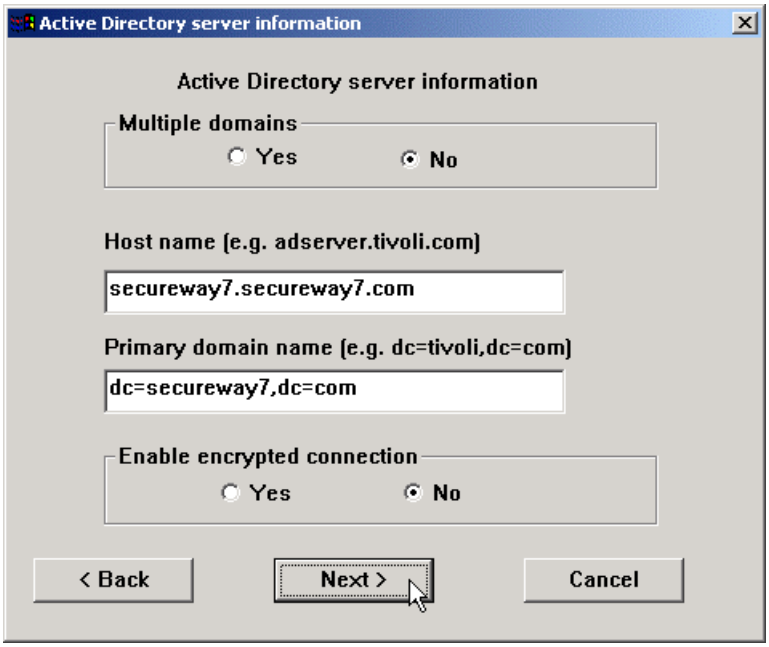
To begin configuration, select START->Programs->Access Manager->Configuration.



This displays the Access Manager Configuration dialog. Each entry must be configured in order, from top to bottom. Select AM Runtime and click Configure....



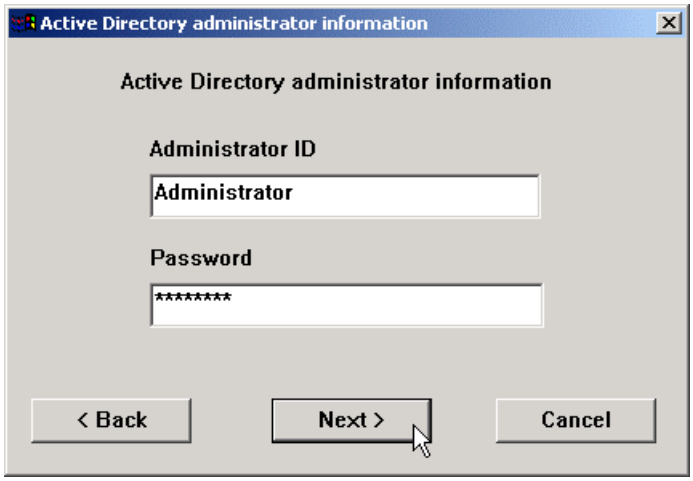
Select Active Directory and click Next.



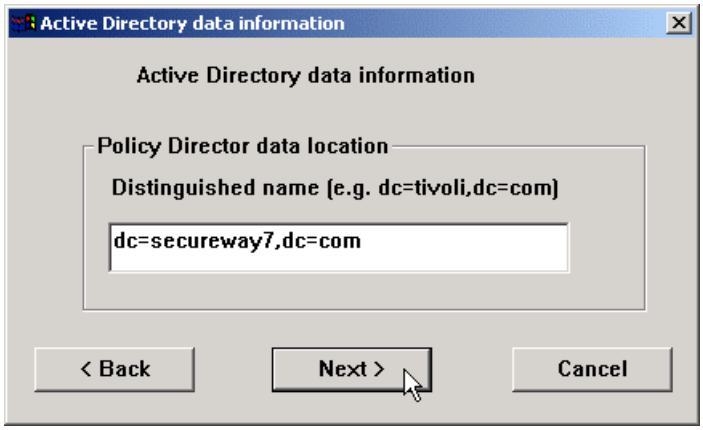
Enter the information for your host and domain names as shown above.

> 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."

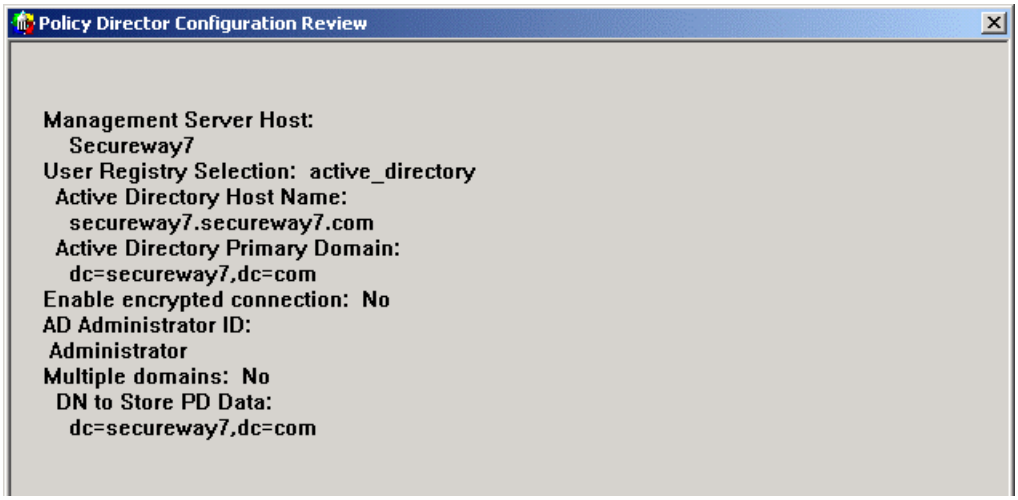
Select No for both Multiple domains and Enable encrypted connection. Click Next.



Enter the Administrator ID and *passw0rd* as the Password and click Next.



Here, *dc* stands for *domain component*. Set the portion shown as secureway7 above to <your hostname>.



Click Finish.

Wait until the configuration finishes. Now go to section 3.4 Finishing Access Manager Configuration on Your Directory Server to continue.

3.3 Configuring AMRTE with Domino

3.3.1 Considerations

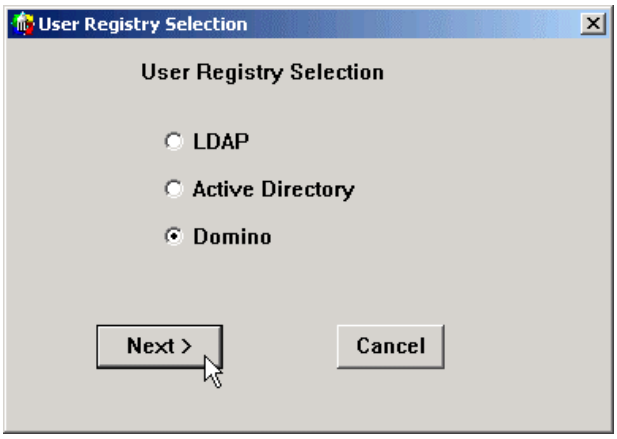
In order to configure Access Manager to use Domino as the directory server, you first need to check that the prerequisites are met. The following components have to be installed, properly configured and **running (Lotus Domino Server)** prior to Access Manager (the whole package) configuration:

- IBM GSKit v5.0.4
- IBM Directory Server 3.2.2 Client
- Lotus Domino Server 5.0.4 or higher
- Lotus Notes 5.0.4 or higher

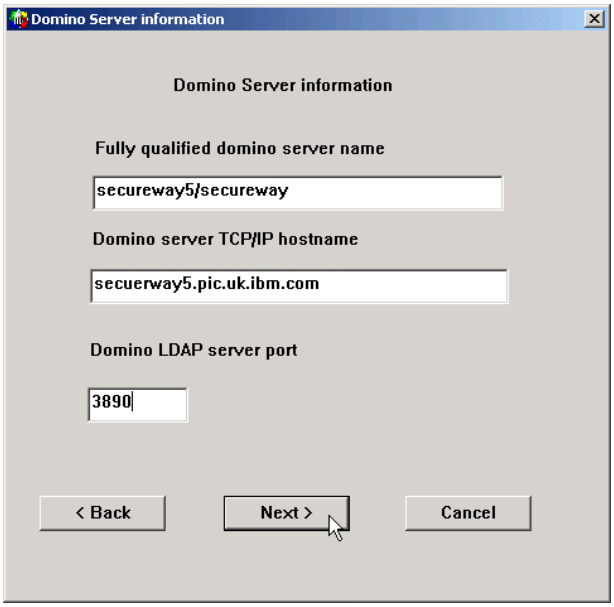
Check the user using the Notes client. This may not be the correct user. You can click cancel on the Notes client login, and change to user PDaemon, whose ID file will be located under the Notes directory in ids\people\PDaemon.id.

3.3.2 Procedure

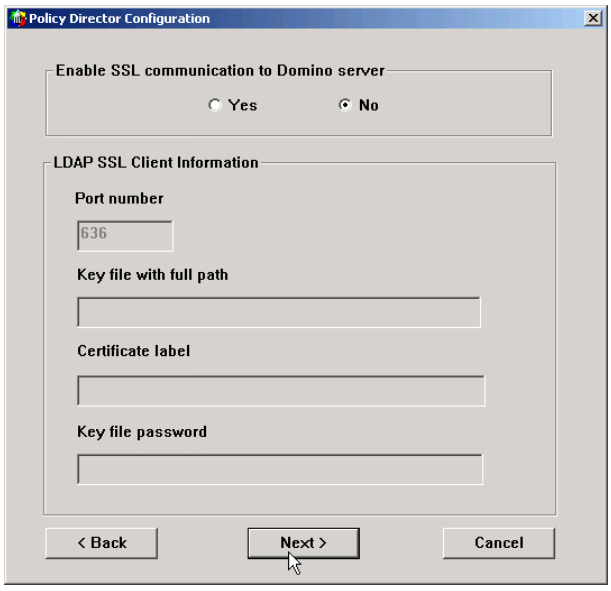
Run Start -> Programs -> Access Manager -> Configuration. Select "Access Manager Runtime Environment" (AMRTE) and click on Configure.



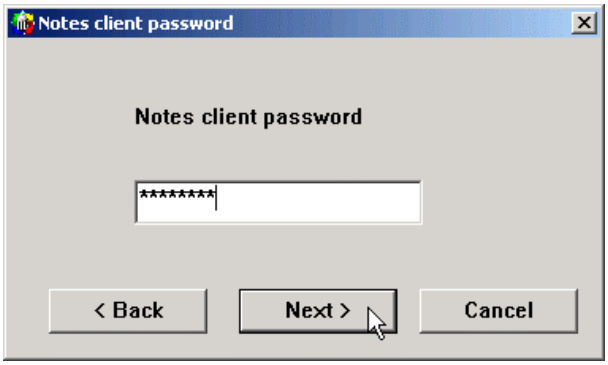
1) Select Domino as the User Registry. Click Next.



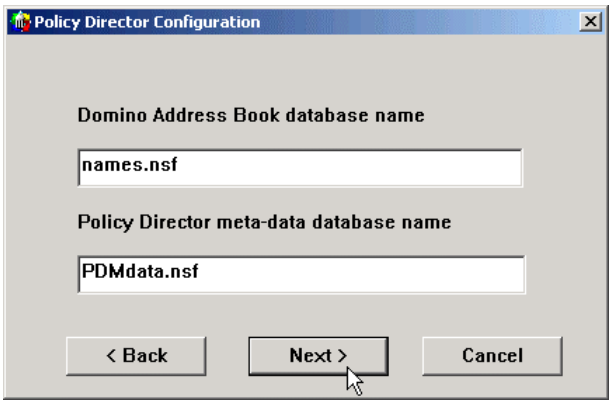
2) Enter the fully qualified Domino server name. This includes the name of the server and the Notes domain.
3) Enter the full DNS name of the Domino server.
4) Enter the port number that the Domino server TCP LDAP interface is listening on. This must match that which was configured on the Domino server, 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.



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.



6) Enter the password of the PD Privileged User. This password will be used by Access Manager 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 AM Privileged user, *passw0rd*. Click Next.

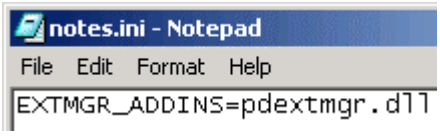


7) Specify the filename of the Domain Address book on the Domino Server. By default this will be *names.nsf* and is pre-filled with that value. This filename is relative to the server Data directory.
8) Specify the filename of the AM metadata database on the Domino Server. By default this is *PDMdata.nsf* and is pre-filled with that value. This filename is relative to the server Data directory and will be used to create the AM metadata database when PDMgr is configured. Click Next.

Confirm by clicking Finish that the information you provided is correct. The configuration of the Access Manager 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.

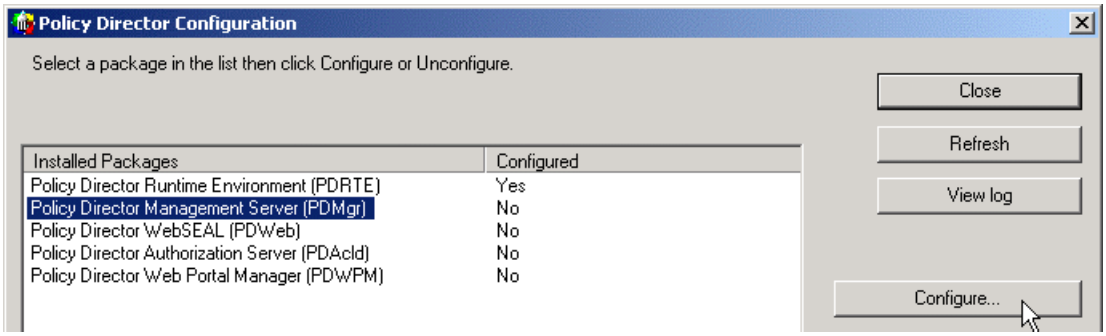
> You may also take a look at the client's *notes.ini* file (by default under x:\Lotus\Notes). It was modified during the AM configuration by adding a line that allows Access Manager to silently log into the Notes client using the password stored in the *domino.conf* file.



Note: Make sure the IBM LDAP client is installed on the Policy Server machine. Continue with AM configuration in the following section.

3.4 Finishing Access Manager Configuration on Your Directory Server

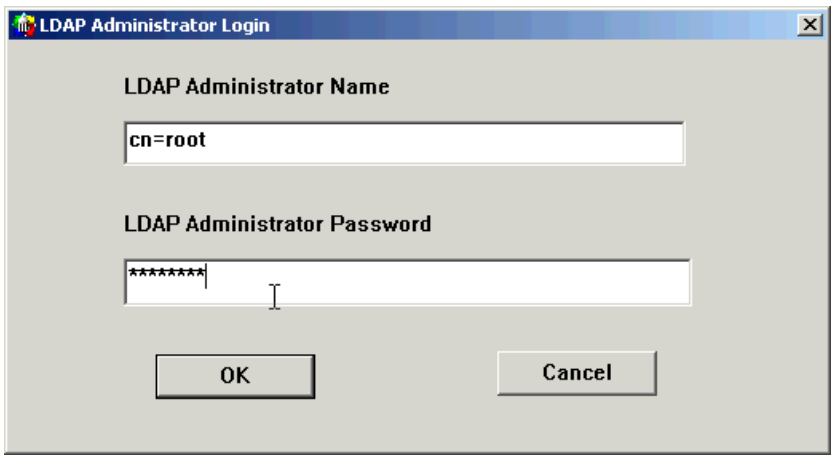
After you've installed AMRTE on your directory server, continue here.



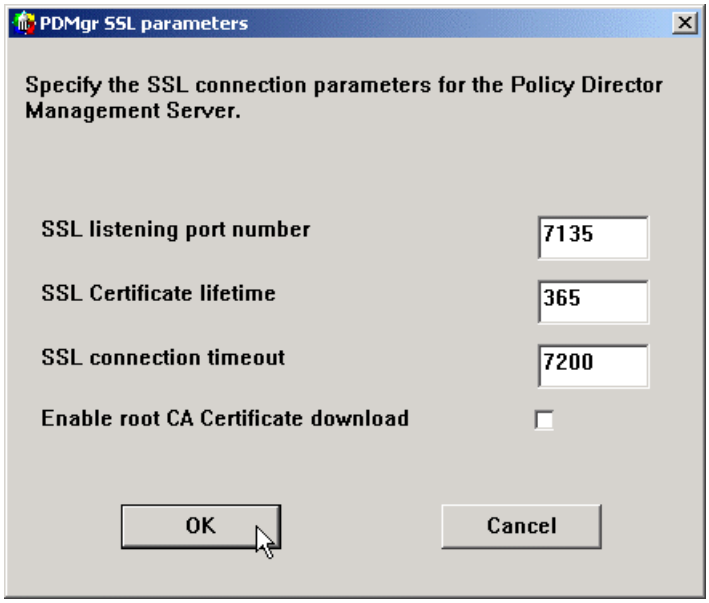
Configure each package in turn.

Enter *passw0rd* as the Administrator Password and click OK.

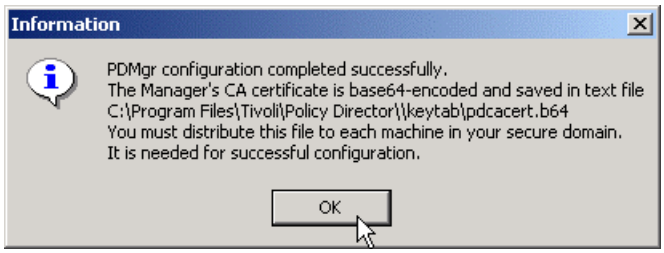
Note: The type of user registry chosen during the configuration of AM Runtime Environment changes slightly the dialogs displayed during configuration of the AM Servers (PDMgr, PDAcl, WebSEA). The dialogs shown in the remainder of this section are for IBM SecureWay LDAP.



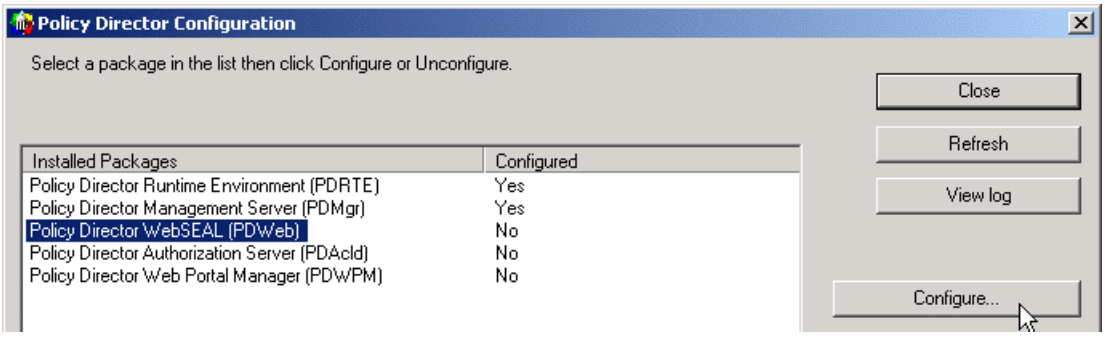
On this dialog enter *cn=root* and *passw0rd* to specify the user name and the password of the directory administrator during both PDMgr and PDAcl configurations.



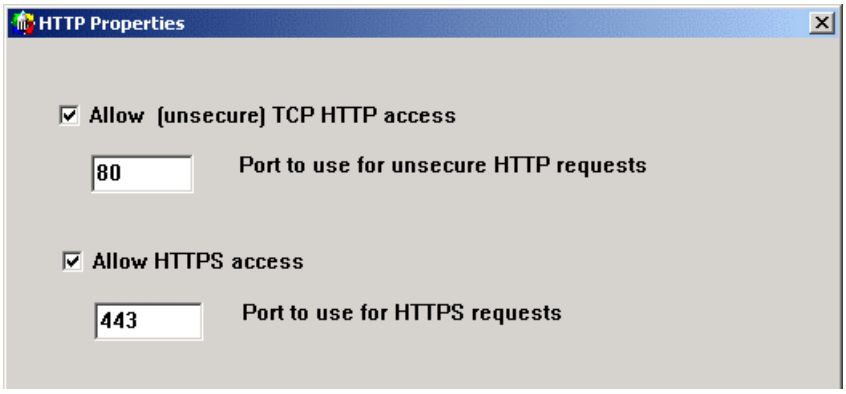
Since you are installing on a single machine, you do not need to enable download of the root CA Certificate – other components can use the file directly from the hard drive. Accept the defaults and click OK. This takes a few minutes to complete. Wait until the configuration finishes.



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.

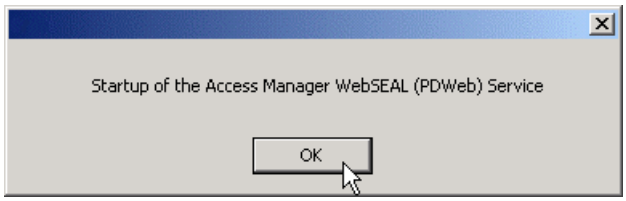


Click Configure....

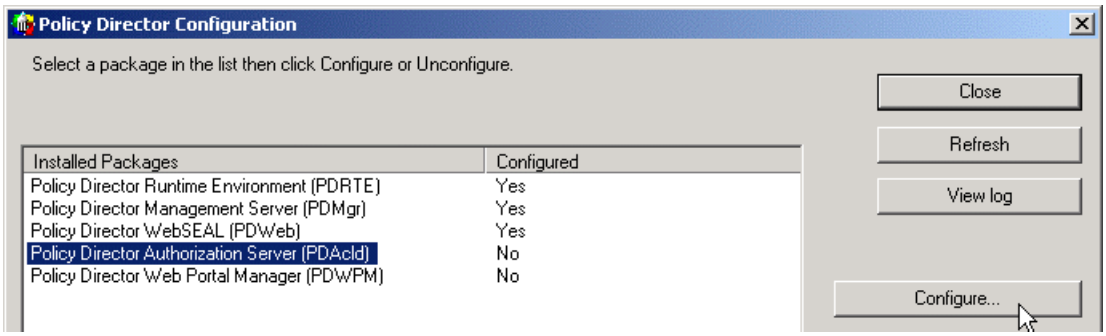


Leave the WebSEAL ports at the standard defaults. (The IBM HTTP Server HTTP ports should be set to 8888 and SSL at 4444 in *C:\IBM HTTP Server\conf\httpd.conf*.) Click OK.

Enter *passw0rd* as the AM Administrator (sec_master) password and click OK. After a moment the configuration will start. Wait until the configuration finishes.



Click OK.



Click Configure to start configuration of PDAcld.

Enter *passw0rd* and click OK. Wait until the configuration finishes.

Access Manager is now fully configured.

NOTE: In AM v3.9 all of the services have been renamed to "Access Manager…" and so appear at the top of the services list like this:

4 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 Multi-platforms and the configuration script only supports the Single Server version of WAS that ships with Access Manager. There is an extra BAT file you must run that will setup simulated commands so that WPM configuration will work with WAS AE.

4.1 Initial Procedure

Make sure WebSphere Admin Server is running (in services). Start the admin console and 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.

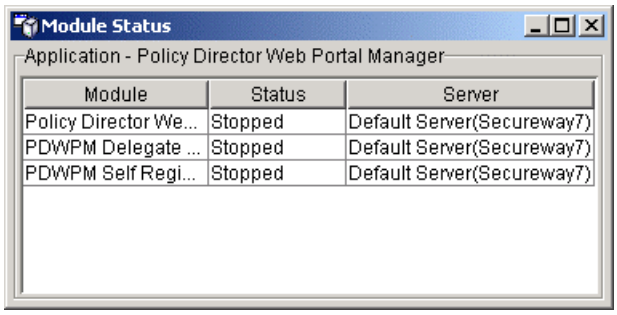
The three BAT files copied are:

- *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

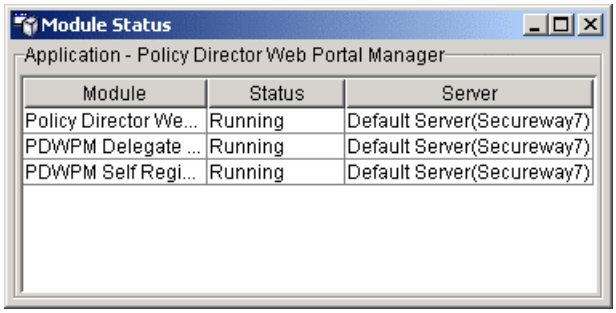
The AM Configuration GUI calls these three BAT files in this order. By copying these, you provide the Configuration GUI what it expects to find with WAS Single Server version.

Now back in the Access Manager Configuration dialog, select AMWPM and click Configure....

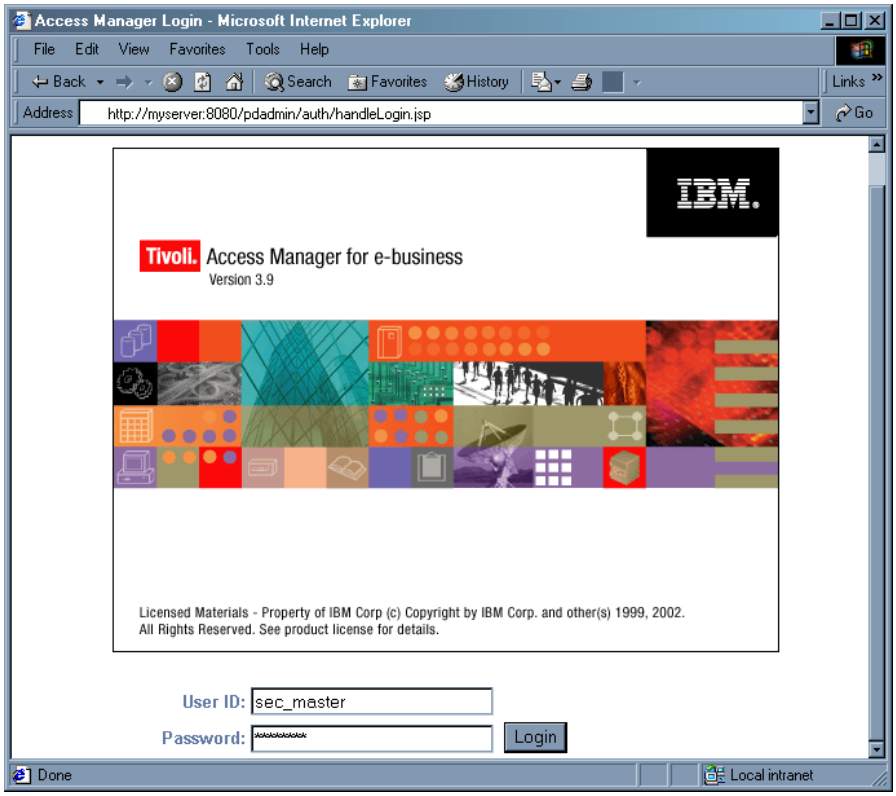
When the configuration completes, in the WebSphere Admin Console expand Enterprise Applications you should see Access Manager Web Portal Manager. Check if is running. Right mouse click on it and select Show Status.



You need to start it if its status is “Stopped”. Close the status dialog and right mouse click on Access Manager Web Portal Manager again, and select Start. Click OK to dismiss the completion dialog. Show status again to verify it is running.



The dialog shows all three Web modules in the application are running. Now it can be tested to make sure the installation succeeded. Enter *http://<your hostname>:9080/pdadmin* in the browser of your choice. You should see the login screen for the Web Portal Manager.



Next go to *http://<your hostname>:8888/pdadmin* to include IBM HTTP Server in the path. You should see the same screen.

4.2 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 PDWPM 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 AMWPM 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.

? 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.

5 Verify the Configuration with PDADMIN and WebSEAL

5.1 Starting PDAdmin

Enter

```
C:\> pdadmin
pdadmin>
```

> On Windows you can also start PDADMIN by clicking:
> START->Programs->Access Manager->Administration Command Prompt

5.1.1 Unauthenticated access

While you are still an anonymous user:

- Issue help command, which commands are listed
- Which commands can you execute as an anonymous user
- What happens if you try listing the users and groups

5.1.2 Login as 'sec_master'

```
pdadmin> login
Enter User ID: sec_master
Enter Password: passw0rd
pdadmin>
```

- How do you start and log into PDAdmin all on the same line?

5.2 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.

5.2.1 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

- Does 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

- Does this work? If not, why not?
  (remember that all entries in LDAP require a parent entry)

5.2.2 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

? Does 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

? Does this work? If not, why not?
(remember that all entries in LDAP require a parent entry)

5.2.3 Using Domino

There are some minor differences from the standard way (IBM Directory or MS Active Directory) in operating Access Manager based with Domino.

You should **not** use the Domino Administrator, while Access Manager Services are running. In particular, avoid changing the administrator identity, as Access Manager 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 Access Manager 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 Access Manager (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 Access Manager

First create a Domino Directory user using Domino Administrator or Lotus Notes client. In Access Manager:

```
pdadmin> user import [-gsouser] <user-name> <dn>
pdadmin> user import hugo hugo/secureway
```

The same applies to the creation and import of groups.

5.3 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
```

6 Configure WebSphere with Your User Registry

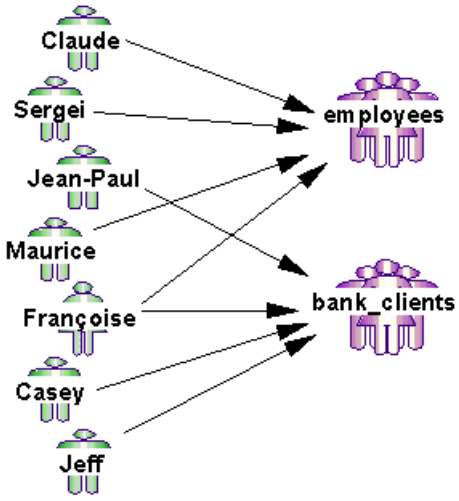
6.1 Objectives

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, your directory's suffix/domain.

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, `PIC` (note no "o=")

From a DOS prompt, run **`D:\LabFiles\create_users-groups.bat <suffix/domain>`**

This will create the Users and Groups to the directory of your choice. It uses Policy Director PDADMIN (in non-interactive mode) to create the users and groups and then deletes them from Policy Director leaving them only in the registry. To verify success use a registry tool to confirm that the users and groups have been created.

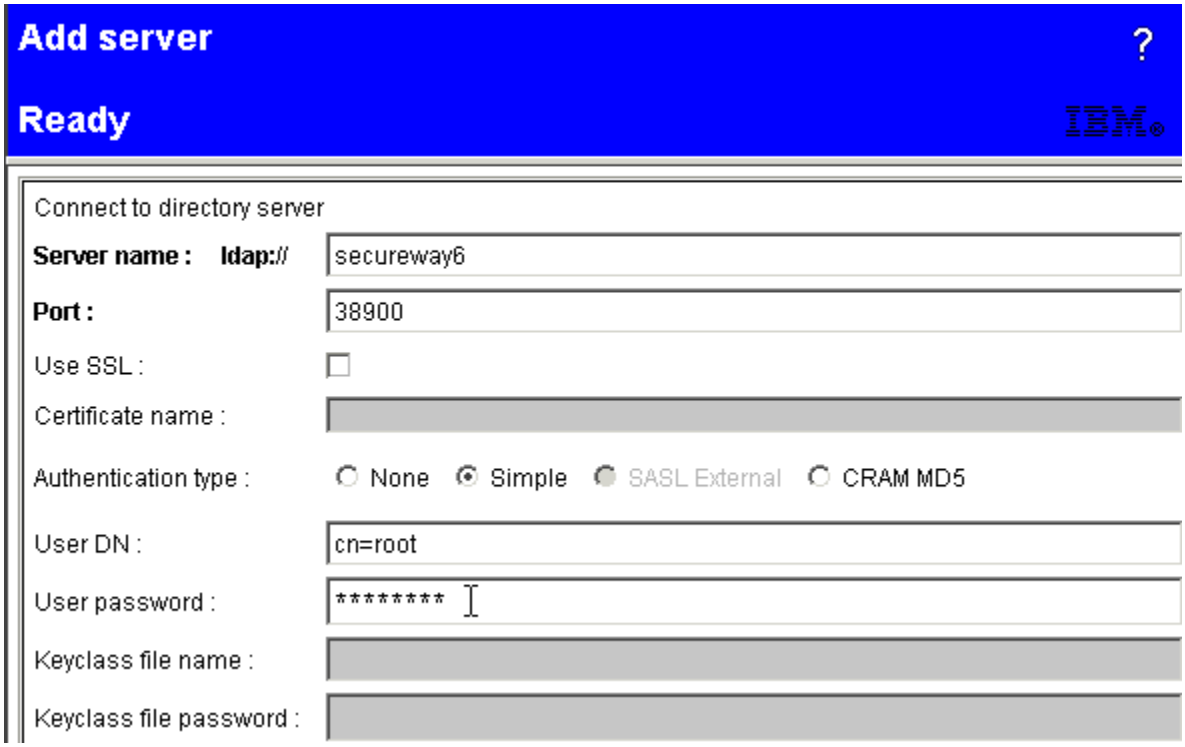
If you have used the batch file go to Section 6.5 to complete the configuration.

6.2 Adding Groups and Users to IBM Directory Server

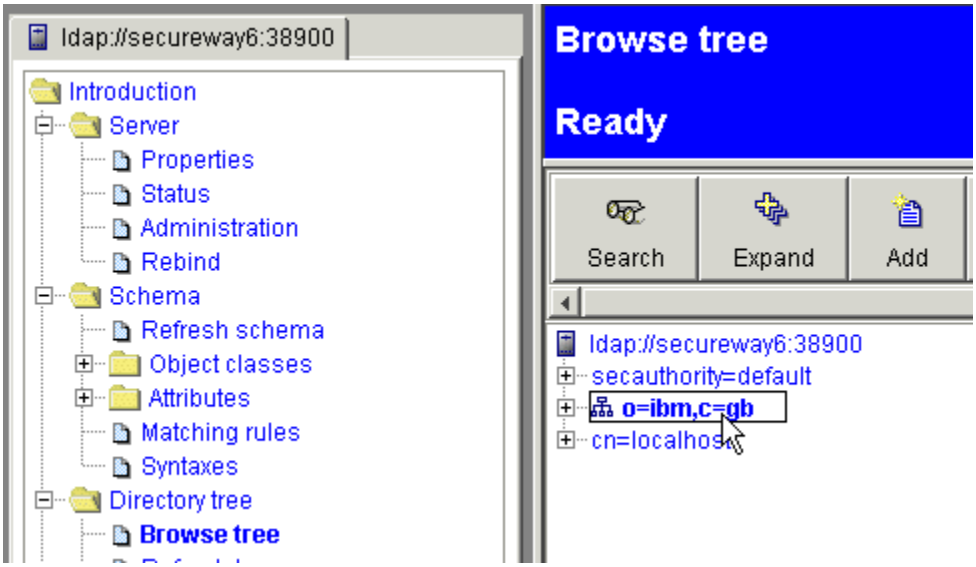
Note: This section provides instructions for manually creating Users and Groups in IBM LDAP. This is not necessary if you have already used the **`D:\LabFiles\Create_users-groups.bat`** command file to create these Users & Groups – go on Section 6.5. (You may wish to confirm that these have been created successfully first)

To do this, start the DMT (Directory Management Tool):

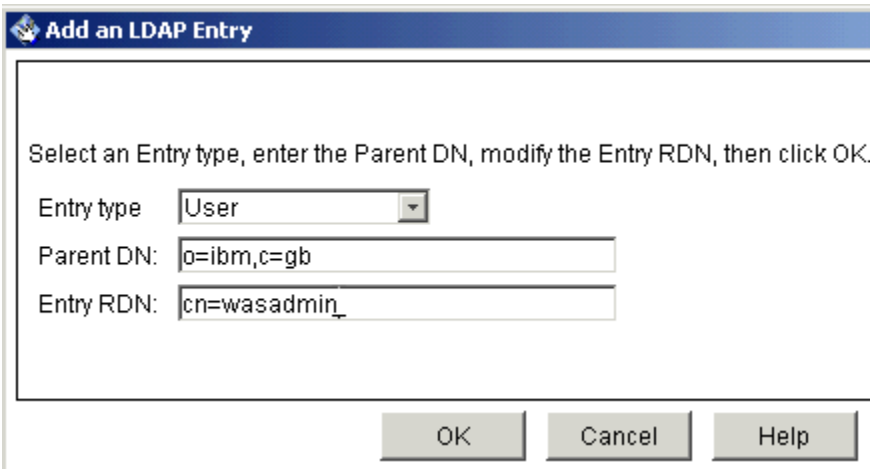
Start->Programs->IBM SecureWay Directory->Directory Management Tool



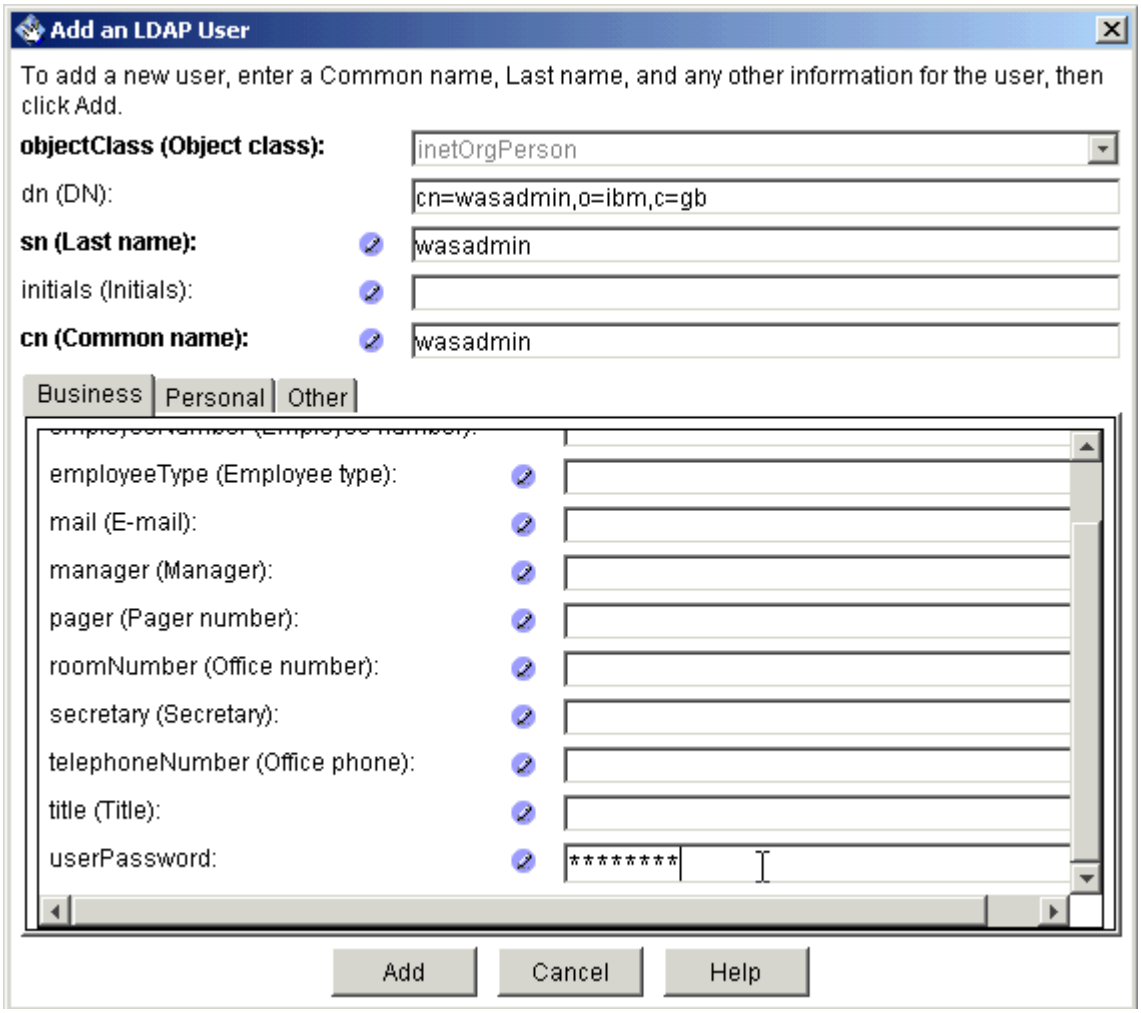
When the DMT is loaded, add your server name and port, and bind as administrator filling in the fields.



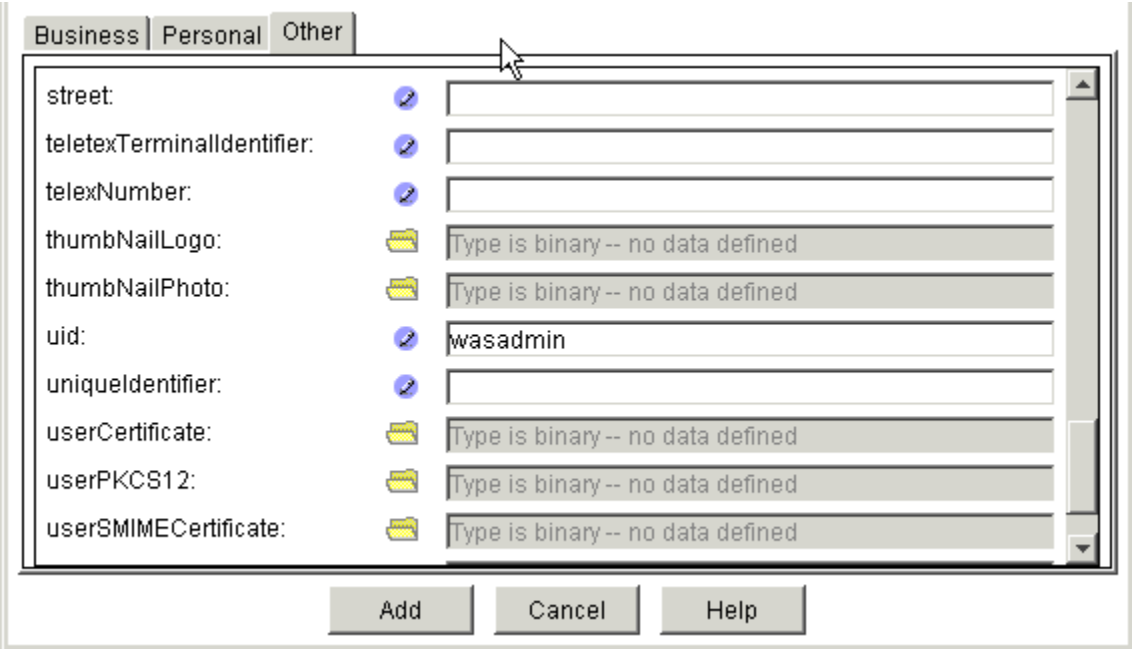
Explore the three entries. Select the suffix o=ibm,c=gb and click on Add to create an LDAP user named *wasadmin* with the password *passw0rd*. This will be the user that is the WebSphere administrator.



Fill in the fields and click OK. The next screen it is opened to provide further information such as the second name and password.

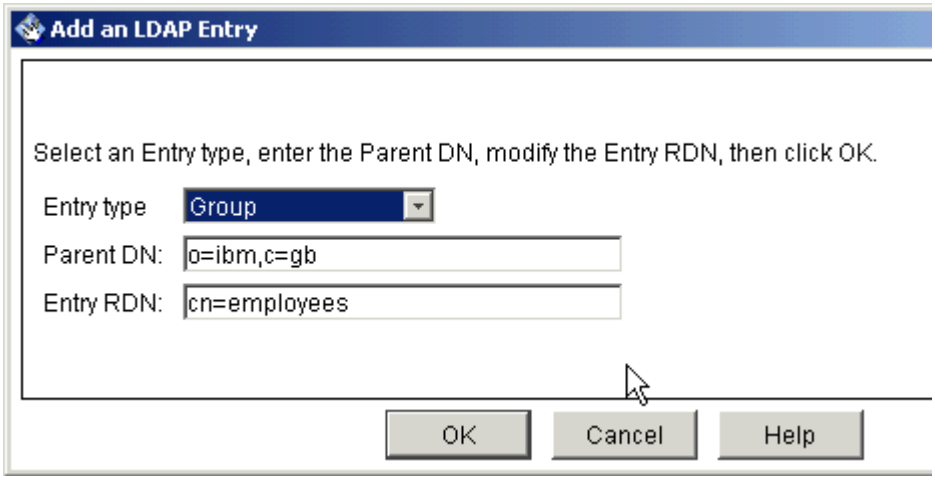


Enter *passw0rd* as the password per the convention throughout these labs. In order to properly use the user with WebSphere you must also set the *uid* attribute with the same name you give for the *cn* attribute. Click on the *Other* tab.

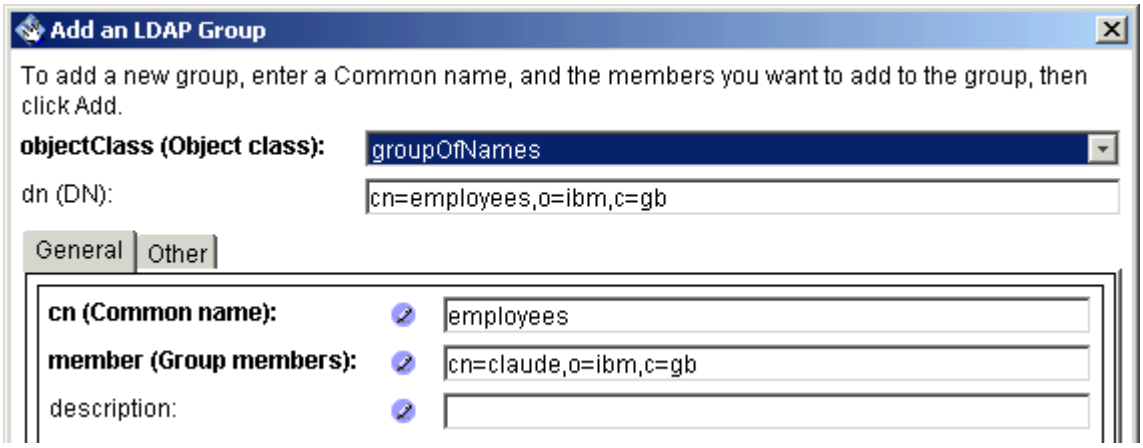


Set the uid: field to *wasadmin*.

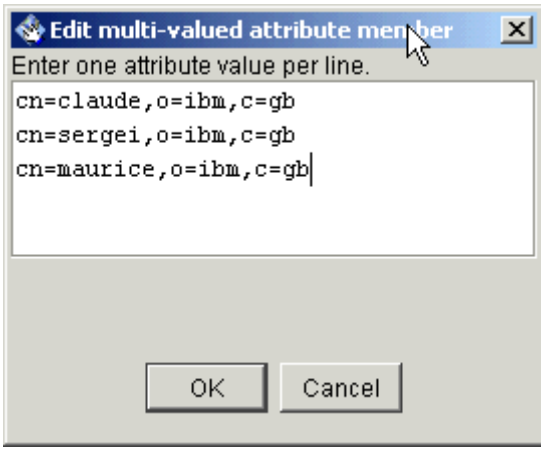
You should repeat all these steps for each user you need to create for the Banker 2001 application. Create a group and add some users on it. Always select the suffix *o=ibm,c=gb* first and then click on Add button. Select *Group* as entry type.



Fill in the fields and click OK. In the next screen provide further information such as the group's member users.



Click on the blue dot and a panel will open allowing you to import multiple users into the group.



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.

6.3 Adding Groups and Users to Active Directory

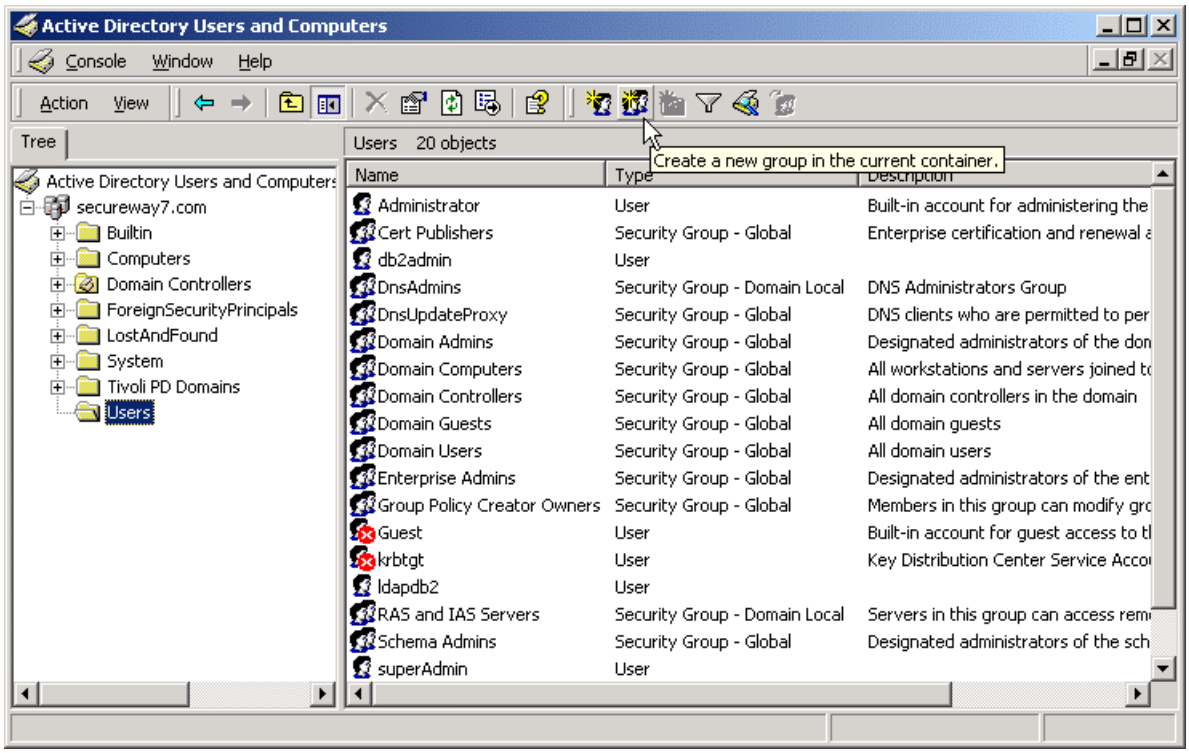
6.3.1 Considerations

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 – go on Section 6.5. (You may wish to confirm that these have been created successfully first)

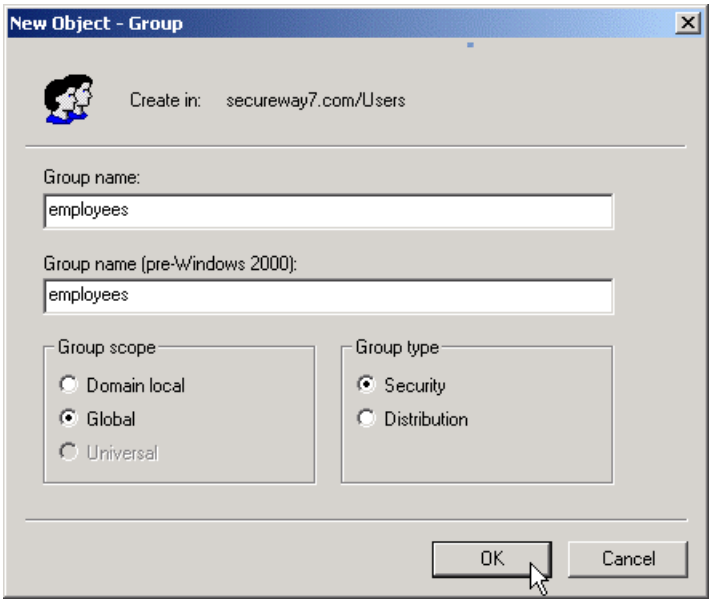
In order to provide authentication and authorization for applications running in WebSphere, users and groups need to be created in Active Directory. You will create the users and group using the Active Director console. Later you will import those users and groups into Access Manager.

6.3.2 Using the Active Directory GUI

Start the Active Directory console by running Start->Programs->Administrative Tools->Active Directory Users and Computers.

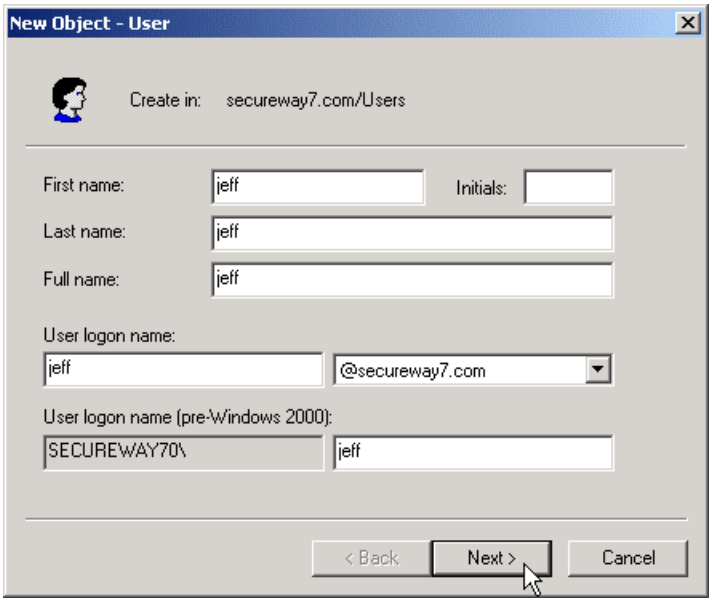


First select the *Users* folder under your hostname. Then click the Create a new group icon.

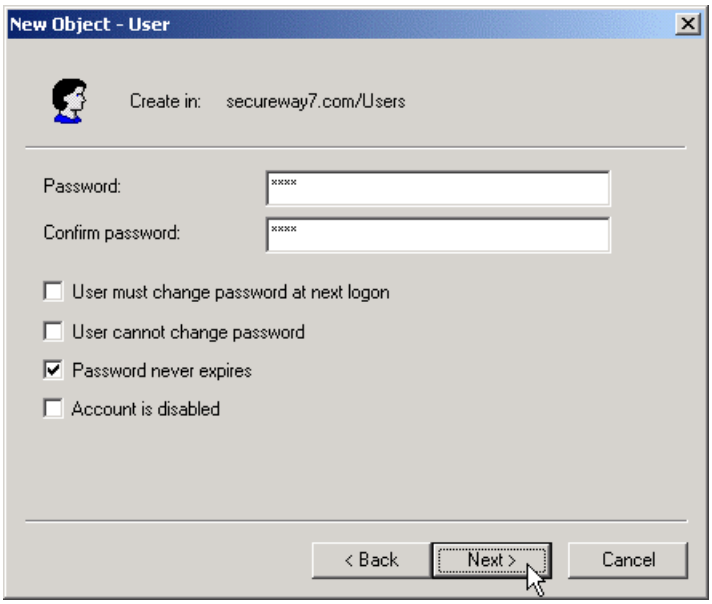


Enter *employees* as the Group name and click OK. Do the same for a group named *bank_clients*. Now you will add users and make some of them members of these groups.

Click the Create a new user icon just next to the Create group icon.



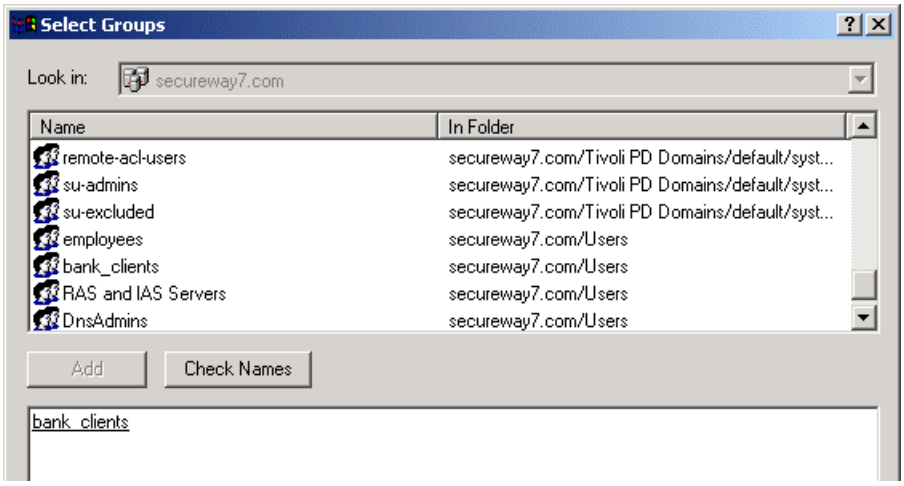
Add a user named *jeff*. Use the same values for First name, Last name, and User logon name. Change the Full name back to a single *jeff*. Click Next.



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 6.1 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.



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.

6.4 Adding Groups and Users to Domino Server

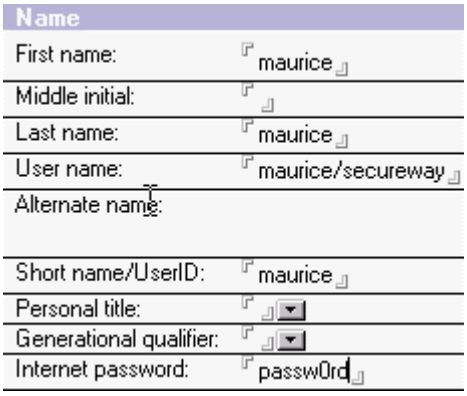
Note: This section provides instructions for manually creating Users and Groups in Domino. This is, obviously, not necessary if you have already used the `D:\LabFiles\Create_users-groups.bat` command file to create these Users & Groups – go on Section 6.5. (You may wish to confirm that these have been created successfully first)

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.

6.4.1 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.



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.

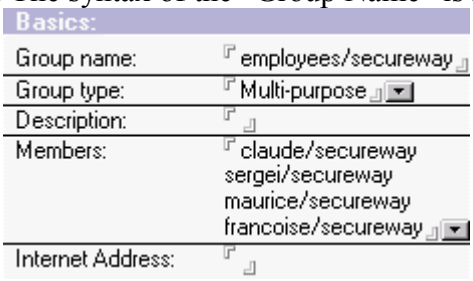
Create all Domino users according to "Banker 2001 Users and Roles" using the Lotus Administration Client. Set all the passwords to *passw0rd*.

Now create a user in Domino named *wasadmin* with the password *passw0rd*. This will be the user that is the WebSphere administrator.

6.4.2 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.



6.4.3 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. Access Manager 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
```

6.5 Configuring WebSphere Security with Your User Registry

6.5.1 Considerations

This lab contains instructions for all the user registries. Where they differ each will be described in turn.

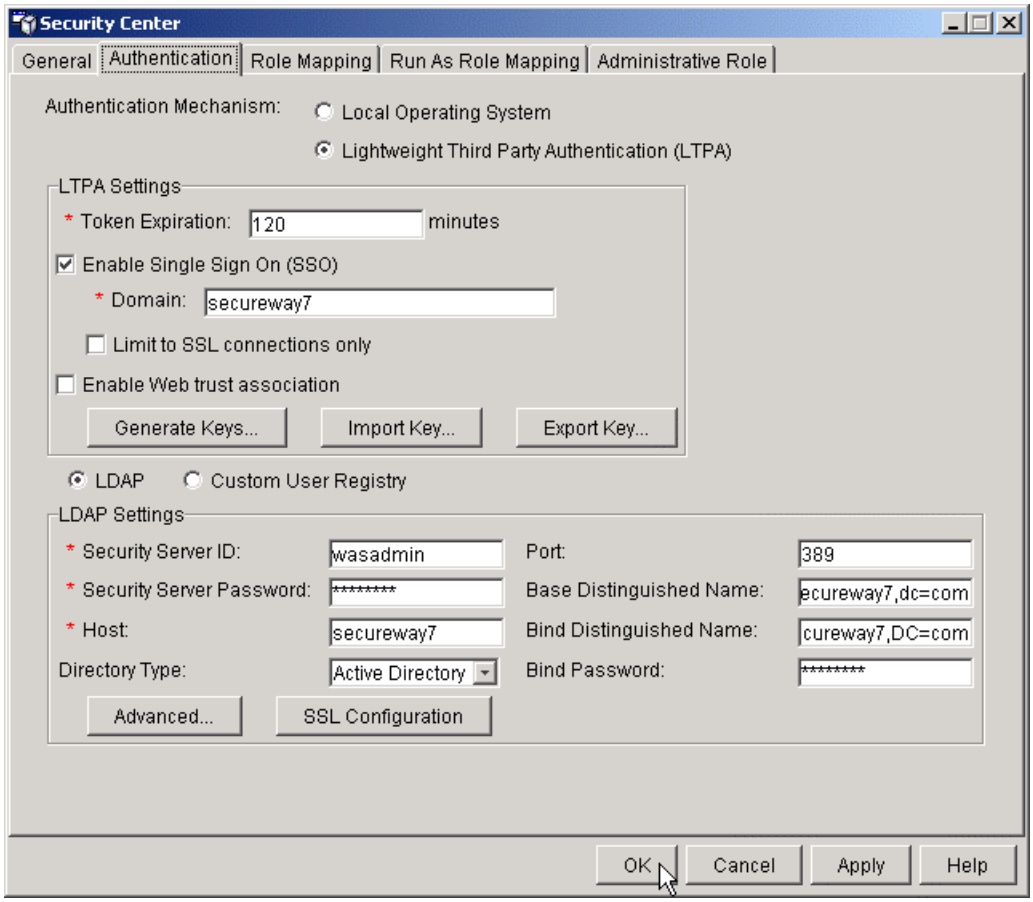
To use each user registry for authentication with WebSphere Application Server, there are some specific steps you must take. By default, none of the directories allows anonymous LDAP queries. To make LDAP queries or browse the directory, an LDAP client must bind to the LDAP server using the distinguished name (DN) of an account that has administrative rights on the directory.

6.5.2 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 is done by the user create batch file if you used it). This user will be the WebSphere administrator account, the user ID you'll use to log into WebSphere after you've enabled WebSphere security.

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.



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 shown as389 above – this is only correct for Active Directory; 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 are using IBM LDAP, you need to make the following change so that WebSphere can recognize groups created by Access Manager. (The create_users-groups.bat file uses AM, so you will need to complete this procedure)

  This change is required because Access Manager creates groups of objectclass *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)(|(objectclass=groupOfNames)(objectclass=groupOfUniqueNames)**(objectclass=accessGroup)**))

   I.e., add *(objectclass=accessGroup)* immediately after '...UniqueNames)'

3) Change 'Group Member ID Map' to

   groupOfNames:member;groupOfUniqueNames:uniqueMember;**accessGroup:member**

   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.

6.6 Mapping Users and Groups to Roles with the WebSphere Admin Console

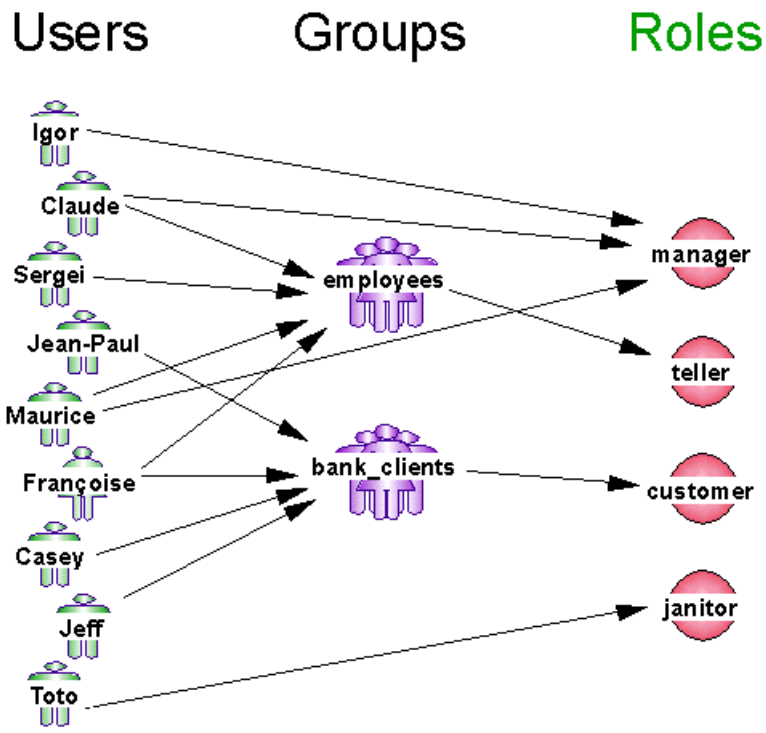
6.6.1 Considerations

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.

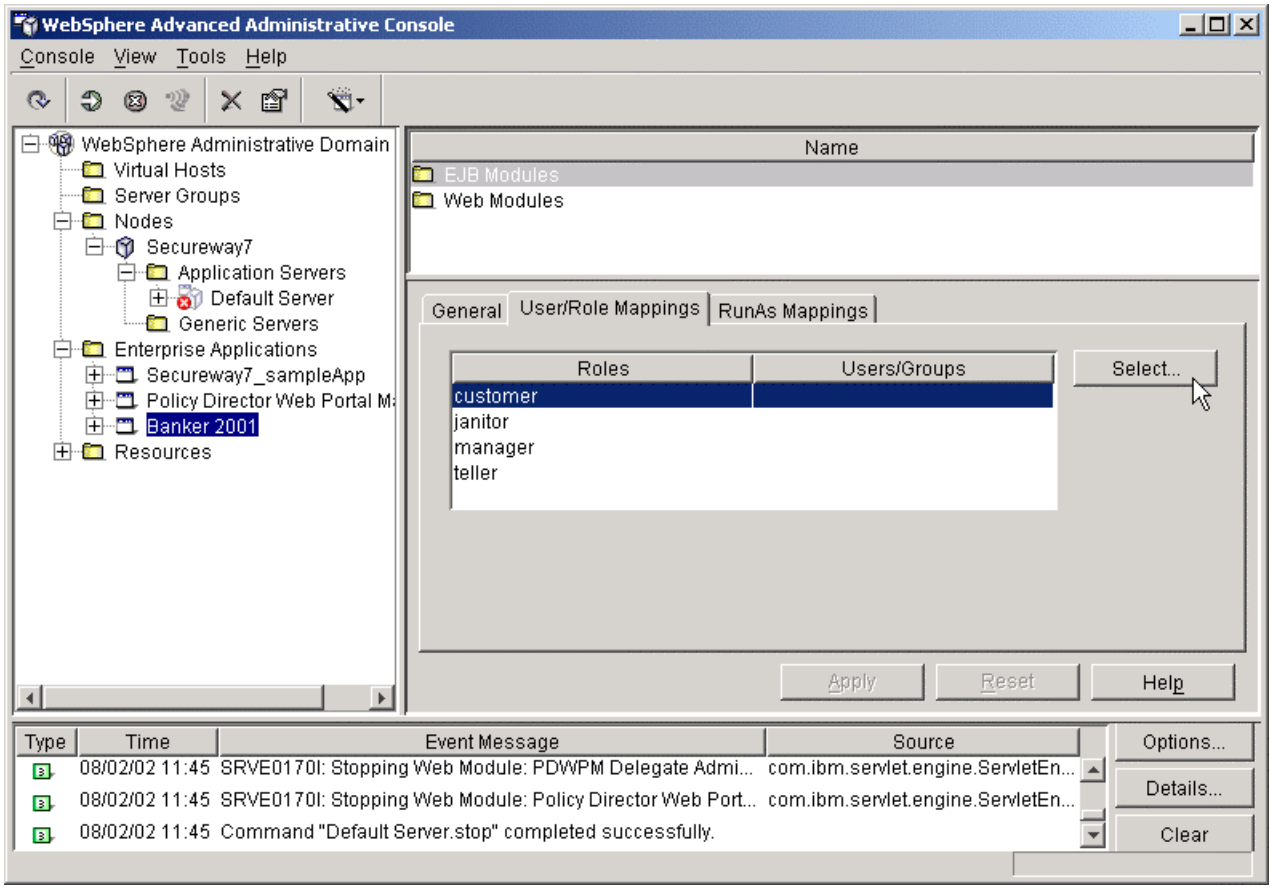
When you install an application into WebSphere you can map users and groups to roles that are defined by the application assembler. You can also do this after the application has been installed. The Banker 2001 application has been pre-installed into WebSphere for you. (See section 17 Appendix B -- WebSphere Installation for reference.) You've defined users above that you will assign to roles already defined in Banker 2001.

6.6.2 Configuring the Banker 2001 Application

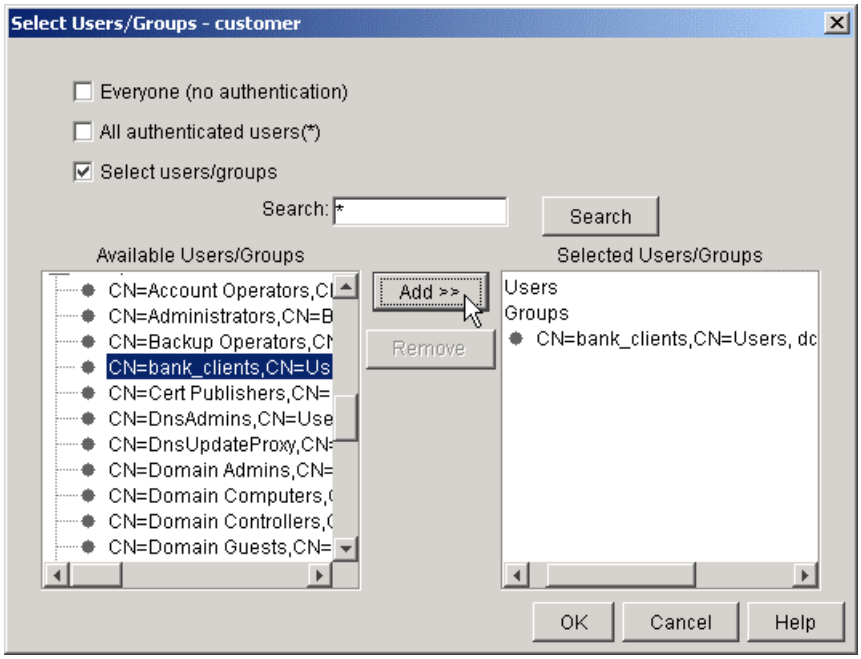
Start the WebSphere Admin Server and Admin Console if they're not already running. Expand WebSphere Administrative Domain, Nodes, your hostname, and Application Servers, and stop the Default Server by selecting it and clicking the Stop icon in the menu bar. (Stopping and restarting the Default Server 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.



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.

> If you can't see any groups listed and you're using IBM LDAP then you need to edit the advanced options for WAS Security to recognize these. See section 6.5.2.

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.

6.7 Testing Banker 2001 Security

6.7.1 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 *http://localhost:9080/Banker2001*. (Case sensitive!)

Why use port 9080? Where is the request received?

The Banker 2001 application welcome screen should display. At the bottom, select the Users and Roles 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. (Note: this is a static GIF file – not a real representation of the configuration!)

6.7.2 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 BA re-authentication (doesn't work with WebSEAL), and
- view the users, roles, and methods for which security has been configured.

6.7.3 Testing Security

In general, security is applied when you actually perform a task. For example, if you are user Igor and try to View Balances, 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 View Request Headers 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.

6.7.4 Importing Banker 2001 Users and Groups into Access Manager

To prepare for labs to come, you need to import users associated with Banker 2001 from your standard user registry into AM. 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 suffix or domain.
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`

And for Domino enter

```
<your domain name>
```

For example, `secureway` (note no "o=")

From a DOS prompt, run **`D:\LabFiles\Import_users-groups.bat <domain/suffix>`**

This will import all the Banker 2001 users and groups to the AM domain. Wow! To verify that your import worked OK, 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.

7 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.

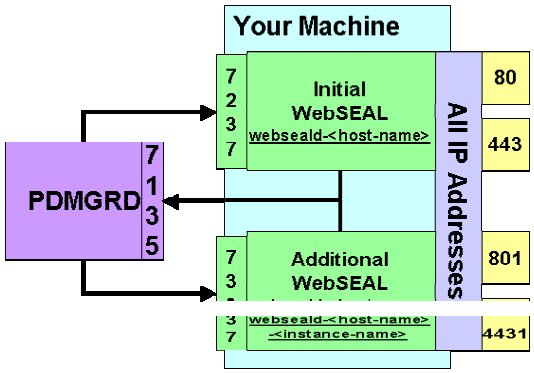
7.1 Configuring a Second WebSEAL Server to Listen on Different Ports Using the Same IP Address as the Initial WebSEAL Server

? 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 Policy 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 /?

Usage:  ivweb_setup   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
    -m pdadmin_pwd      sec_master password
    -i instance instance name
    -M mts_listen_port  mts listen port
    -n interface        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 <instance-name>-webseald-<your-host>* to see, if the new WebSEAL instance has been registered in the AM Domain and see its configuration. The output will look like this:

```
    webseal1-webseald-secureway5
        Description: webseal-webseald/secureway5
        Hostname: secureway5.secureway5.com
        Principal: webseal1-webseald/secureway5
        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 webseal1-webseald-secureway5 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.

? How can you stop the instance? _____

? What is the name of the Windows Service representing the new instance?

_____

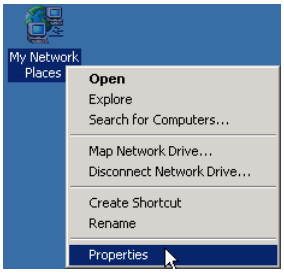
7.2 Configuring a Third WebSEAL Server to Listen on Ports 80 and 443 Using a Different IP Address than the Initial WebSEAL Server

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.

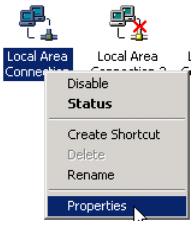
> **This section will only work for computers using static IP addresses - not DHCP.**
>
> **It should also be possible to install the Loopback adapter and configure it to use IP.**

7.2.1 Create a new virtual IP-address

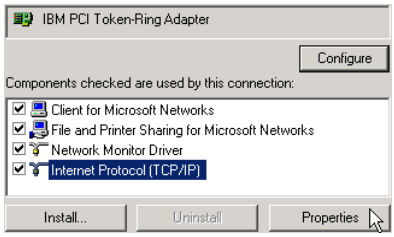
On the Windows Desktop right-mouse click on "My Network Places."



Select Properties.

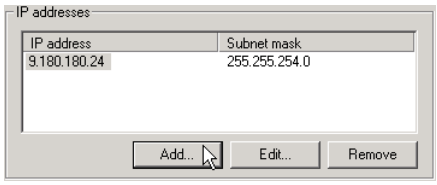


Select the icon representing the Token-Ring Adapter and right-mouse click on it.

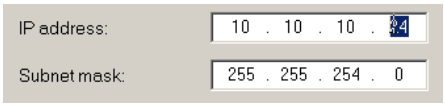


Select TCP/IP Protocol and click on Properties.

Select the "Advanced" button near to the bottom of the window.



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.

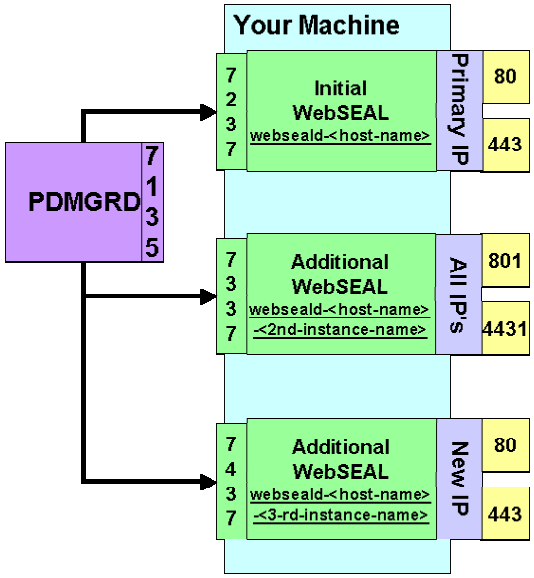
The example shown here uses '24'.

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).

7.2.2 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 IP-addresses (if you would create one more virtual IP-address)?

7.3 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 "Access Manager 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.

```
##############################
# WEBSEAL GENERAL
##############################
[server]
network-interface = 9.180.180.24
```

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.

7.4 Final Question

? Can multiple WebSEAL instances on the same machine belong to different Access Manager Domains?

Hint: are they all not using the same RTE?

8 HTTP 1.1 Support

Among the enhancements to WebSEAL with Access Manager 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.

For 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.

8.1.1 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:

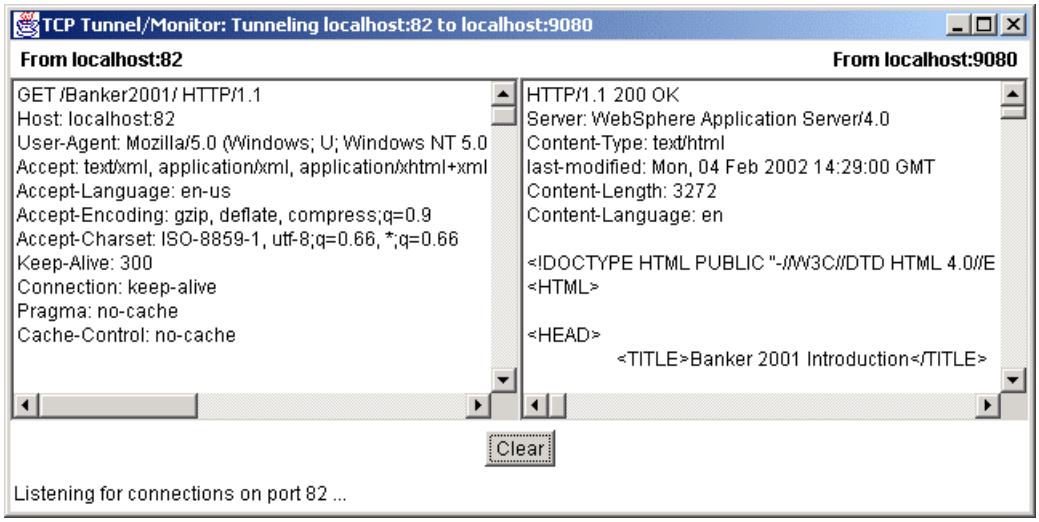
```
C:\TCPTunnel\tunnel 9080
```

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:



8.1.2 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>
```

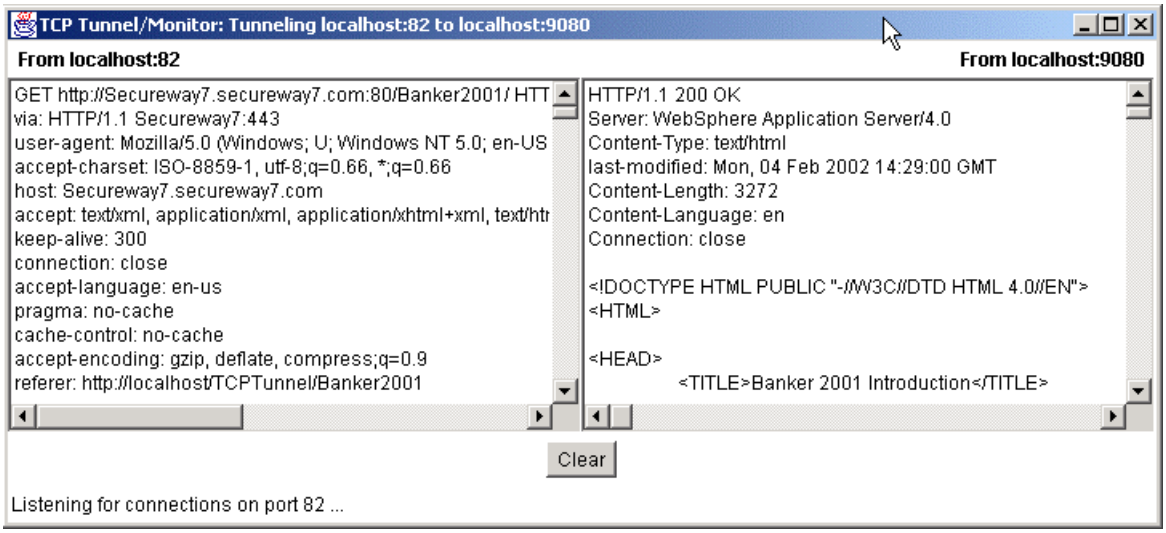
where webseald-**<your host name>** could be **webseald-secureway7** for example.

You have TCP Tunnel forwarding requests to port 9080 already, so the overall flow is

Browser → WebSEAL → TCP Tunnel → WebSphere Embedded Web Server

Now in the browser enter *http://localhost/TCPTunnel/Banker2001/*. 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.



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>.

9 Forced Re-authentication, Constant Session ID and Session Termination

9.1 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.

9.2 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.

9.3 Constant Session ID

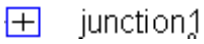
WebSEAL maintains a constant session ID throughout the lifetime of the user credential. This session ID is contained in the EPAC (AM credential), which can be transferred to a junctioned server as the value of the CGI-variable *iv_creds*. *iv_creds* can be parsed with aznAPI. But an easier way to retrieve the session ID on the back-end is to let WebSEAL insert it as the value of the CGI-variable *pd_session_id*.

9.3.1 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 AM WPM.

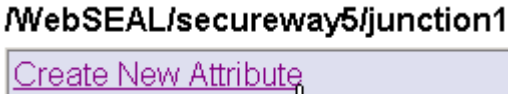
Connect to AM WPM and authenticate as *sec_master*.

Click on *Object Space -> Browse* and navigate to the object representing a junction to WebSphere Application Server (e.g. junction1).

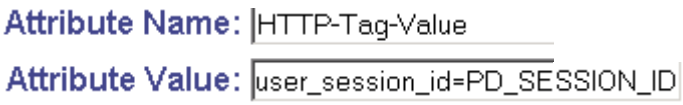


Click on the junction name to see the properties of the junction.

Click on *Extended Attributes.*



Click on *Create New Attribute.*



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.

9.3.2 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 AM session ID.

? What is the name of the variable? _____

It consists of two parts. The first (before the underscore) represents the base64-encoded name of the WebSEAL server. The second part (after the underscore) is the AM session ID. You can see the values just underneath.

The long, unintelligible AM session ID string can be used to terminate a user's session. You'll do that shortly.

9.4 Configure a Constant Session ID on WebSEAL

9.4.1 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.

_____

? Do 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.

9.4.2 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 mark inactive sessions rather than deleting 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.

9.5 Terminating a User Session

9.5.1 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
bjxxPAQAAAAwAAAAEJ6XA3FaMjRmODJ6Z0lrUlNoczA1VGZDU1kyMnlkdC1wZVlmUWczOW5ab29wLWd
BQUFBQQ==
```

Issue the command to terminate the session, using the long session ID (after the underscore) 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.

9.5.2 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.

10 Switch User

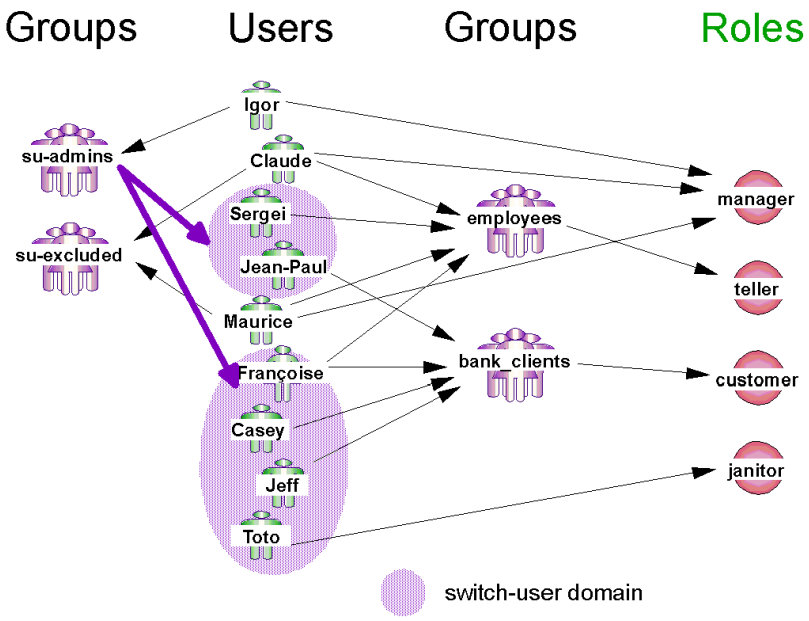
10.1 Objectives

In this lab you will configure, enable and test the new Switch User functionality of WebSEAL 3.9.

10.2 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:



10.3 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?

10.4 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.

10.5 Using the Switch User Function

If you have completed lab 9 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 AM 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://<was-server>: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*

? 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*?

_____

11 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,

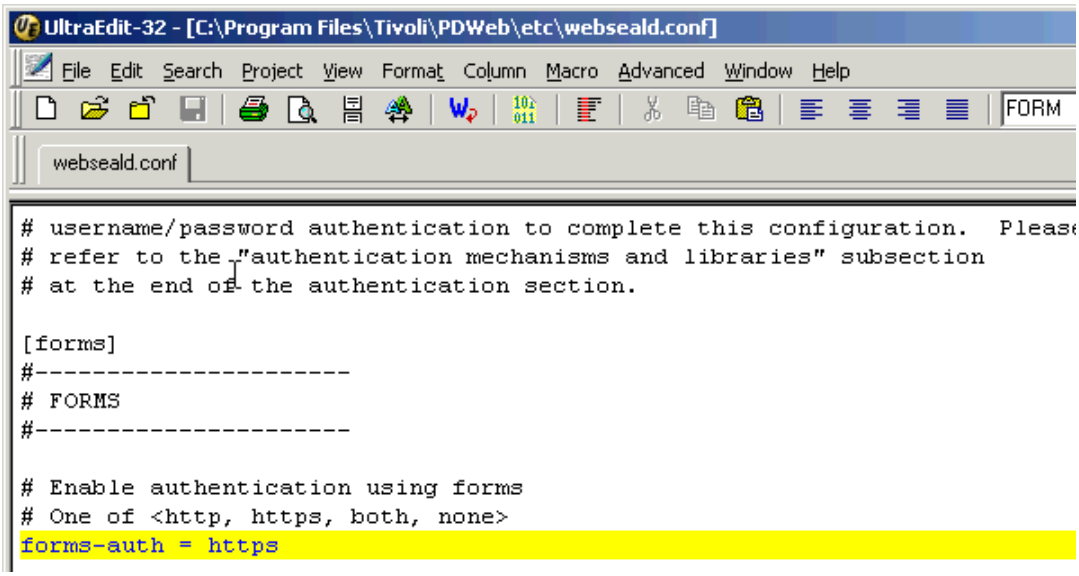
the form data was lost. This could also occur if you were filling out a very long form and your session expired. In WebSEAL 3.9 the form data is now cached so that it is still present when the form is resubmitted. You'll test this in this lab.

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!

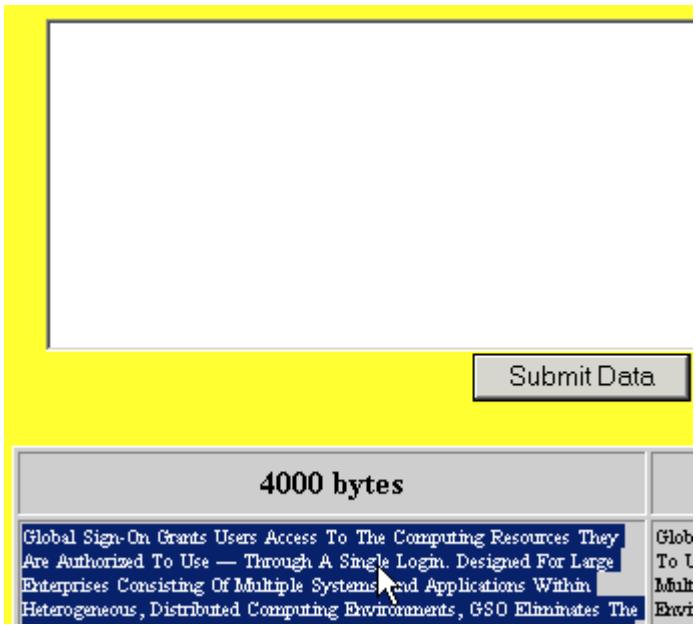
```
# Session timeout for SSL v3 connections (range: 1-86400 secs)
#ssl-v3-timeout = 7200
ssl-v3-timeout = 30
```

Restart WebSEAL to enable the changes.

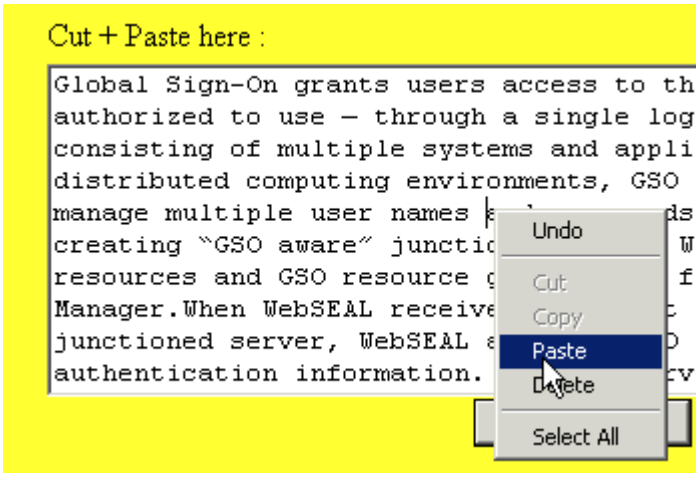
```
http:// yourwebseal/wbsph/Banker2001
```

Connect to the main page of the Banker 2001 application using the junction you just created, and authenticate to Access Manager 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.



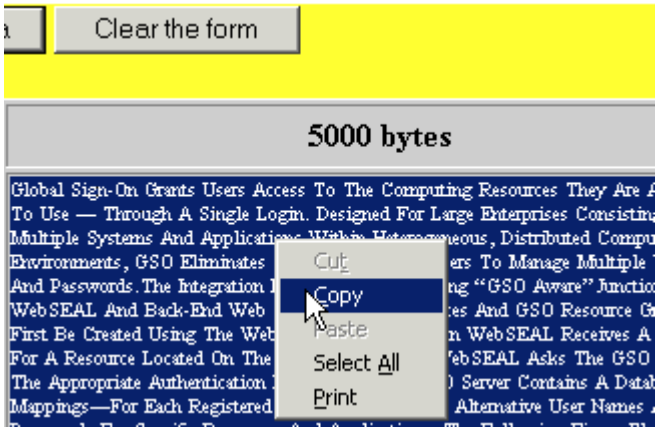
In this sample page select and copy in the clipboard all the text in the 4000-byte column.



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 Access Manager 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.



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?

Access Manager 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.

```
# request-body-max-read = 4096
request-body-max-read = 5096

# When a user is prompted to authenticate before a request
# can be fulfilled, the data from that request is cached
# for processing after the completion 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!

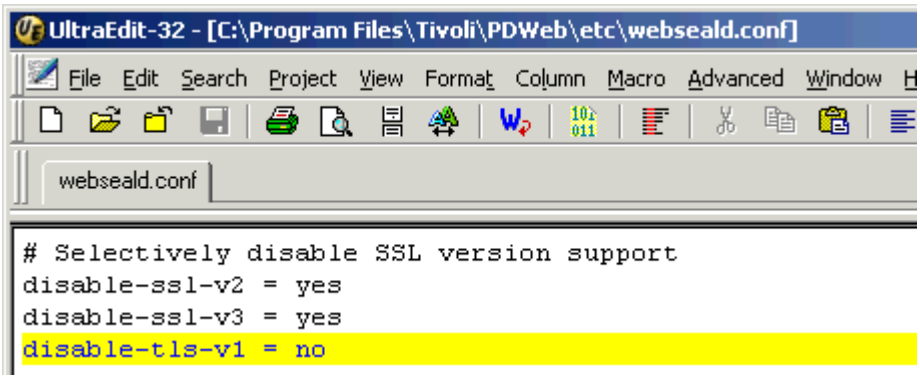
You've completed this lab. Be sure to restore the default values for the parameters you've changed (SSL timeout and Form Based login) in the webseald.conf file to continue with the successive labs.

12 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.



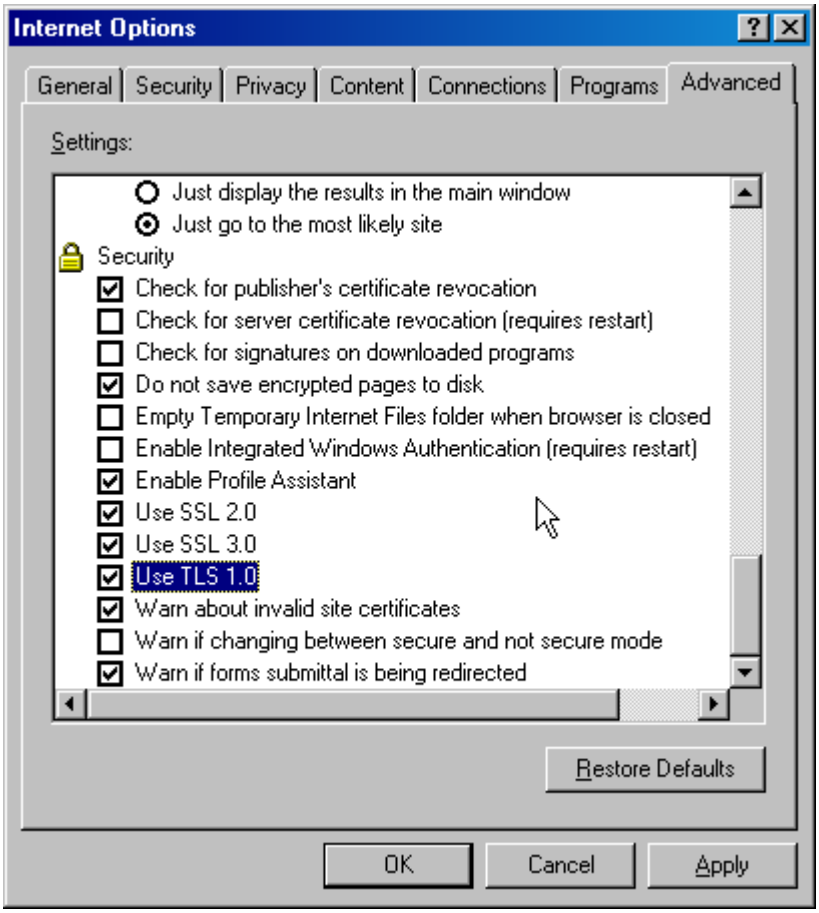
Force WebSEAL to use only TLS by modifying the webseald.conf, disabling SSL.

Restart WebSEAL and try to connect to it with IE5.

? Can you do it? If not, why not?

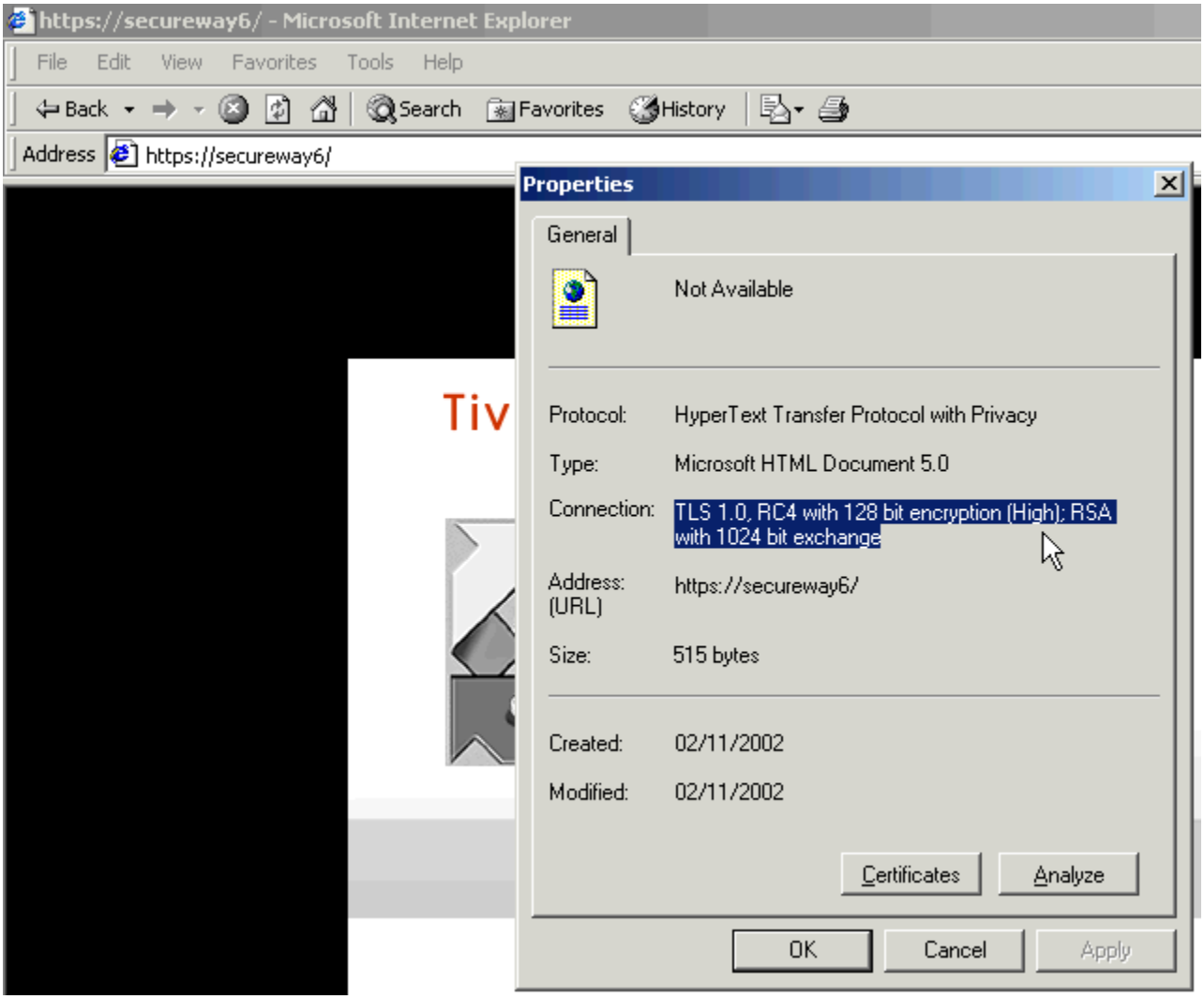
By default IE5 is not configured to use TLS, so this feature must be enabled in the advanced property page of the browser. In IE select

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.

13 Integration of Access Manager and WebSphere Application Server

13.1 Objectives

Using WebSEAL, Tivoli Access Manager can provide authentication for J2EE applications running in WebSphere. Access Manager can also provide programmatic authorization for applications running in WebSphere. Now Access Manager 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, AM for WAS and the Migration Tool.

The overall process will be to

1. Install AMWAS
2. Configure WebSphere Java Runtime for Access Manager
3. Configure AMWAS
4. Perform initial setup for AMWAS
    a. Create action group and action for AMWAS
    b. Migrate the WAS Admin Server application security to AM
5. Test AM and WAS integration
6. Migrate the Banker 2001 application security to AM
7. Test it all

13.2 Instructions

13.2.1 Initial Setup

By now you should have already installed and configured Access Manager and the Authorization Server (PDACLD) and installed the AM Java Runtime component. Not it's time to install Access Manager for WebSphere Application Server (AMWAS).

13.2.2 Perform AMWAS Installation

Navigate to where the AMWAS installation images are and run setup.exe. This launches the InstallShield.

1. Hit OK to accept "English" as the setup language
2. Hit "Next" on the welcome screen
3. Hit "Yes" to agree to the terms and conditions
4. Hit "Next" to confirm the installation directory (C:\Program Files\Tivoli\pdwas)
5. Hit "Next" to confirm installation options

AMWAS is now installed and the InstallShield closes.

13.2.3 Configure AM Java Runtime

In order for AMWAS to function it requires that the WebSphere Java Runtime is configured to communicate with Access Manager. This is what the AM Java Runtime does. Open a command prompt and enter the following commands:

```
C:\>cd %PD_HOME%\sbin
C:\…\sbin>pdjrtecfg -action config -java_home %WAS_HOME%\java\jre
C:\…\sbin>echo off
C:\WebSphere\AppServer\java\jre\PolicyDirector directory does not exist. Creati
ng...
C:\…\sbin>
```

The JAVA AM Runtime is now configured.

> In order for AMWAS configuration and the EAR migration utility to work successfully the java.exe from WebSphere must be used when these java classes are run (since it has the communication with AM). To ensure this is the case, either add c:\websphere\appserver\java\jre\bin to the start of the PATH or specify the path when running java commands (this is what is done in this lab).

13.2.4 Configuration of AMWAS

In AMWAS v3.9, configuration is performed using a java class. On UNIX systems this is front-ended by a script but for windows the class must be run manually. However, a batch file is available to set up the environment.

Check that AM Policy Server and AM Authorization Server are running.

Open a command prompt and type the following:

```
C:\>cd program files\Tivoli\pdwas\sbin
C:\…\pdwas\sbin>pdwascfg
Type the following:
"java –D …
…
C:\…\pdwas\sbin>
```

Rather than typing in the (rather long) string that is presented, type the following; it makes use of environment variables. **This is all one line**:

```
C:\…\pdwas\sbin>%WAS_HOME%\java\jre\bin\java
-Dpdwas.lang.home=%PDWAS_HOME%\nls\java -Dpdwas.home=%PDWAS_HOME%
-Dwas.home=%WAS_HOME% -cp "%CLASSPATH%" PDWAScfg -action config
-remote_acl_user was4jvm -sec_master_pwd <sec_master_pwd> -pdmgrd_host
<hostname> -pdacld_host <hostname>

C:\…\pdwas\sbin>
```

If successful, this command will finish with no messages (as shown above). You can check using PDADMIN that a user called **was4jvm/<*hostname*>** has been created and **was4jvm-<*hostname*>** is listed as a server.

AMWAS is now configured.

> When AMWAS is configured it configures WebSphere to use AM for J2EE application security. YOU MUST now perform the initial migration in the next section. If WebSphere is re-started and AMWAS configuration and initial migration is not complete then it will fail to start. AMWAS configuration can be reversed using the PDWAScfg class with -action unconfig.

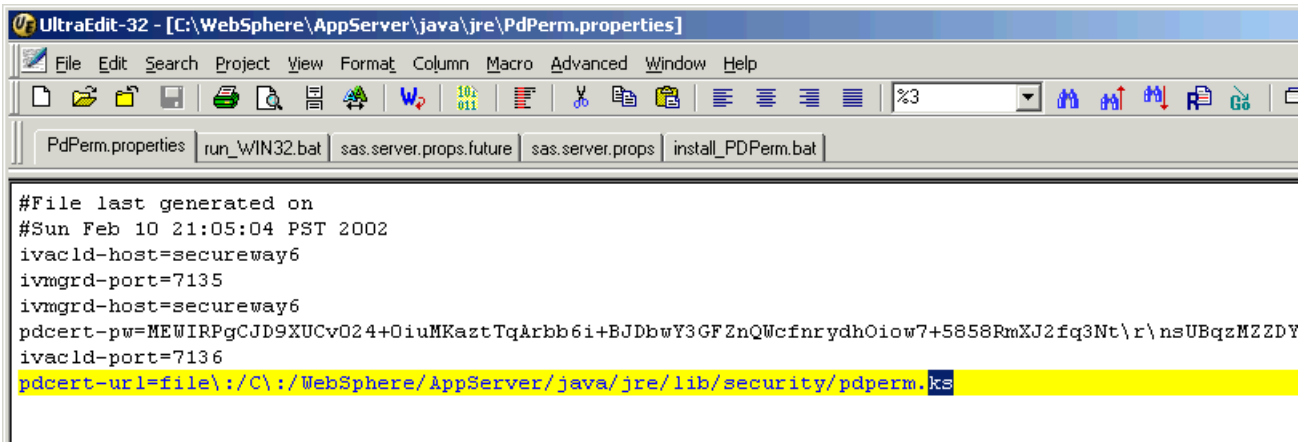
> The PDWAScfg –action unconfig command does not de-register the server from Access Manager. To do this you must use the SvrSSlCfg java class (see AM documentation for details)

In Active Directory, for example, the **was4jvm-<*hostname*>** user has the following DN: CN=was4jvm-<*hostname*>,CN=users,**CN=default,CN=Tivoli Policy Director Domains**,DC=secureway5,DC=com.

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 AM Java API to authenticate to AM.

13.2.5 Initial Migration of Information into Access Manager

In order for AMWAS to protect J2EE applications, Access Manager must have an action defined and be populated with objects to represent the J2EE roles.

Check that AM Policy and Authorization Server are running.

Before the initial migration can be done an action group and action must be added to Access Manager. This is required because the JAVA admin classes for AM do not allow this operation. Action groups and actions can be added using the WPM but it is quicker to use the PDADMIN command line as shown below:

```
C:\>pdadmin
pdadmin> login
Enter User ID: sec_master
Enter Password:
pdadmin> action group create WebAppServer
pdadmin> action create i invoke WebAppServer WebAppServer
pdadmin> action list WebAppServer
i invoke WebAppServer
pdadmin>
```

With this complete, the initial migration can be performed. This involves migrating information about the administration roles from WAS to AM. The utility to perform this operation is a java class. On UNIX a script is provided to front-end this class but on Windows the class must be executed manually. However, there is a batch file to set up the environment.

Open a command prompt and type the following:

```
C:\>cd program files\Tivoli\pdwas\bin
C:\…\pdwas\sbin>migrateEAR
Type the following:
"java -D …
…
C:\…\pdwas\bin>
```

Rather than typing in the (rather long) string that is presented, type the following; it makes use of environment variables. **This is all one line**:

```
C:\…\pdwas\bin>%WAS_HOME%\java\jre\bin\java
-Dpdwas.lang.home=%WAS_HOME%\lib;%PDWAS_HOME%\nls\java -cp "%CLASSPATH%"
com.tivoli.pdwas.migrate.Migrate -j %WAS_HOME%\config\admin.ear -a sec_master
-p <sec_master_pwd> -w wasadmin -d <suffix/domain> -c
FILE:\%WAS_HOME%\java\jre\PDPerm.properties
Logging all activity to file .//pdwas_migrate.log
C:\…\pdwas\bin>
```

Suffix/domain should be:

LDAP	o=ibm,c=gb
Active Directory	cn=Users,dc=<your-host>,dc=com
Domino	<Your Domain> e.g. pic

If successful, this command will finish with no messages (as shown above). You can check using PDADMIN or WPM that object **\WebAppServer\deployedResources\AdminRole\admin** has been created and that ACL **_WebAppServer_deployedResources_AdminRole_admin_ACL** is attached. Also, check that user **wasadmin** has been imported into AM and is a member of the new group **pdwas-admin**

Check that the wasadmin account-valid and password-valid flags are set. User PDADMIN as below:

```
pdadmin> user mod wasadmin password-valid yes
pdadmin> user mod wasadmin acc yes
```

The pdwas-admin group contains WAS administrators. This group must be granted the AdminRole role of the admin application. PDADMIN can be used to update the ACL attached to the object representing the application role (this can also be done in WPM):

```
pdadmin> acl mod _WebAppServer_deployedResources_AdminRole_admin_ACL set group
pdwas-admin T[WebAppServer]i
pdadmin>
```

13.3 Testing AM and WAS Integration

Restart WebSphere. Access Manager 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. Access Manager has 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.

13.4 Migrate the Banker 2001 Application Security to Access Managery

13.4.1 Objectives

Now you will migrate the security management of a real application from WebSphere into Access Manager. Back in section 6.7.4 you imported the Banker 2001 users and groups from your user registry into Access Manager. 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.

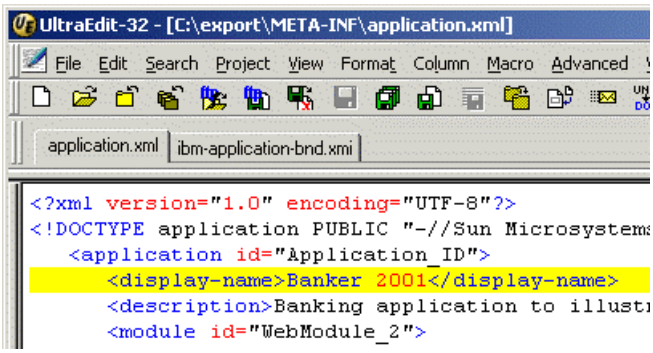
Normally in order to include the user-to-role mappings, you need to export the application back out from WebSphere as an EAR. That one will contain the user-to-role mappings and these should be migrated to AM. However, at the time of this writing the AM Migration application cannot import the roles and associations with users and groups properly.

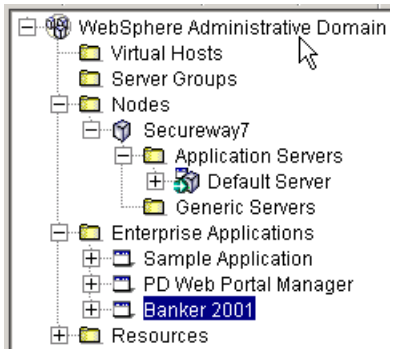
13.4.2 Procedure

The following section, delimited by ###### characters, is left here for reference but should not be performed. The way in which WebSphere formats the proprietary user/group->role mapping in the EAR files when it exports an application is not compatible with AMWAS if there are users or groups specifically defined for the roles.

> ##
> Make sure the Access Manager 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....

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 a problem 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. This does not contain any direct user/group->role mappings.

Open a command prompt and type the following:

```
C:\>cd program files\Tivoli\pdwas\bin
C:\…\pdwas\sbin>migrateEAR
Type the following:
"java -D …
…
C:\…\pdwas\bin>
```

Rather than typing in the (rather long) string that is presented, type the following; it makes use of environment variables. **This is all one line**:

```
C:\…\pdwas\bin>%WAS_HOME%\java\jre\bin\java
-Dpdwas.lang.home=%WAS_HOME%\lib;%PDWAS_HOME%\nls\java -cp "%CLASSPATH%"
com.tivoli.pdwas.migrate.Migrate -j %WAS_HOME%/InstallableApps/Banker2001.ear
-a sec_master -p <sec_master_pwd> -w wasadmin -d <suffix/domain> -c
FILE:\%WAS_HOME%\java\jre\PDPerm.properties
Logging all activity to file .//pdwas_migrate.log
C:\…\pdwas\bin>
```

Suffix/domain should be:

LDAP	o=ibm,c=gb
Active Directory	cn=Users,dc=<your-host>,dc=com
Domino	<Your Domain> e.g. pic

You won't see any messages if the command was successful. Check the activity file mentioned though if you want to see what was done.

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 Access Manager 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.)

13.4.3 Testing Banker 2001 Security with Access Manager

Using the same procedure you used when you first tested users and groups in Banker 2001, test security now that Access Manager is in charge. See section 6.7 Testing Banker 2001 Security for those instructions.

- Now that Access Manager 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 AM and map that user to one of the Banker 2001 roles, will this mapping show up in WebSphere?

14 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 Access Manager user *igor* able to administer Access Manager using WPM as if he were the *sec_master* user. Heady stuff, no?

14.1 Form based SSO to WPM

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 *http://yourhost/websph/pdadmin*, 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*?

15 Installation and Configuration of the Access Manager Web Plug-In for Microsoft Internet Information Server (IIS)

15.1 Objectives

As you know, Access Manager 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 Access Manager Web plug-in with IIS.

Important: When you install IIS you must be disconnected from the network. Otherwise, you-know-what will happen! VIRUSES!

15.2 Prerequisites

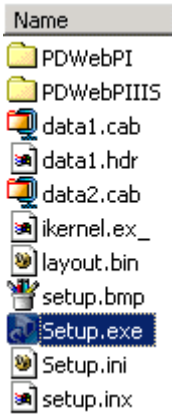
Check the prerequisites for configuring and running Access Manager Web Plug-In for IIS – AM WebPI:

- Access Manager Run Time Environment (AMRTE) and Access Manager Policy 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
    - Restart the Web Server Service

15.3 Installation of Access Manager Web Plug In for IIS

Navigate to the Access Manager WebPI image location at

...D:\Labfiles\AMImages\PDWebPI



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.

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.

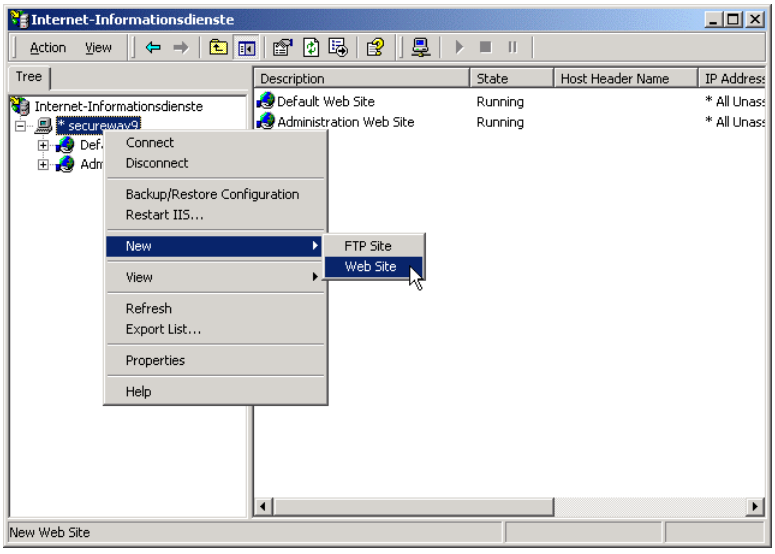
Repeat these installation steps for the next package.

The Access Manager Web Plug In for IIS is now installed.

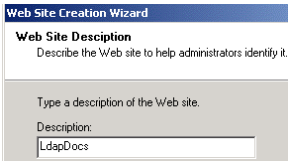
15.4 Configuring a new Virtual Host on IIS

15.4.1 Procedure

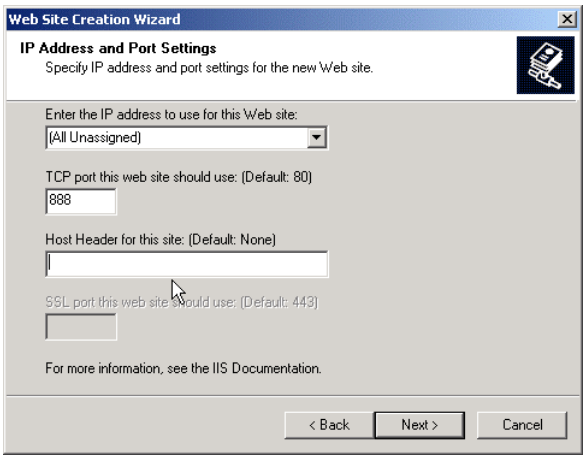
1) Run Start -> Programs -> Administrative Tools -> Internet Services Manager



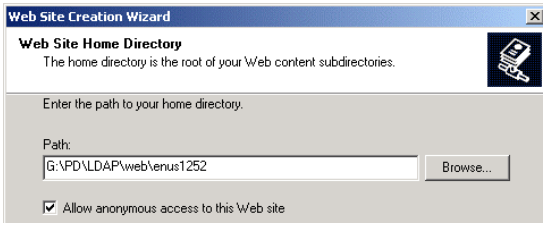
2) Right-click on the server -> New -> Web Site



3) 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.



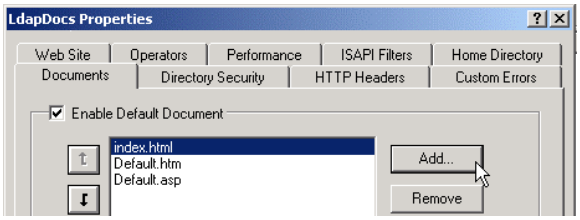
4) Fill in the port. The labs use port 888 (IIS labs default), since the default of 80 is used by WebSEAL. Leave the Host Header field empty.



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.



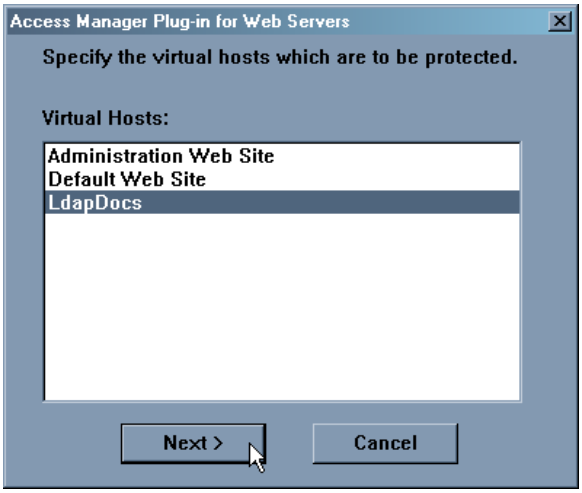
On Internet Services Manager Console right-click on the virtual host LdapDocs, then Properties. Click on the "Documents" tab and the Add… button. Fill in the name of an existing file (e.g. *getting_started.htm*). You've now configured a new virtual host and setup a default Web page for it that points to the IBM LDAP Directory Server documentation.

Now check that it works by pointing your browser to *http://<hostname>:888*.

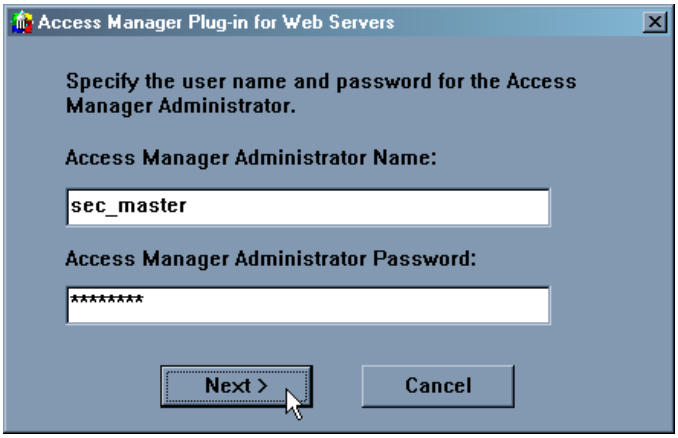
15.5 Configuring the Access Manager Web Plug-In for IIS

1) Use the configuration tool shipped with the Access Manager WPI to configure the plug-in to protect the new virtual host. Launch the graphical configuration tool by selecting

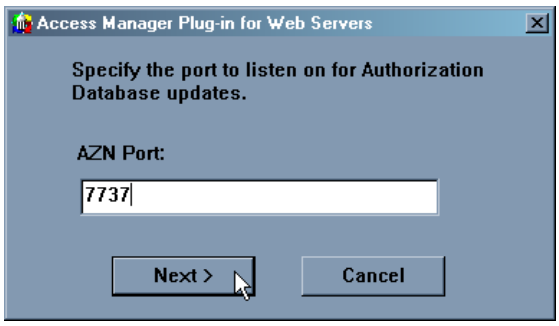
Start -> Programs -> Access Manager Plug-in for Web Servers -> Configuration



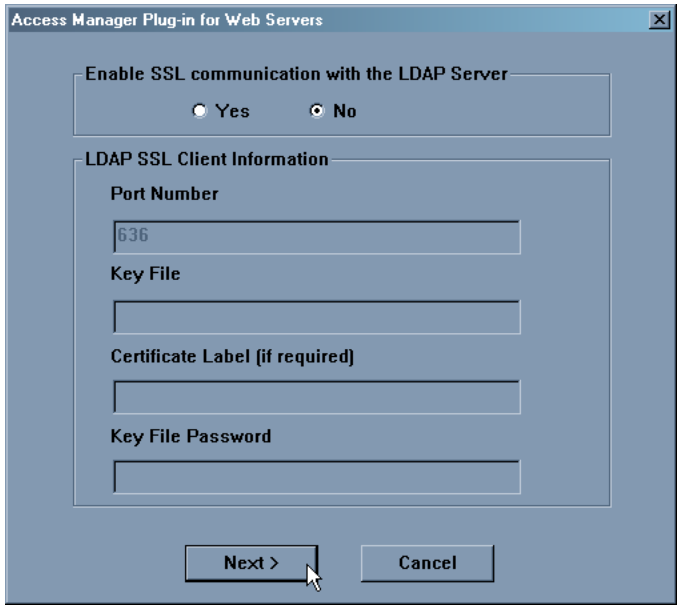
Select the LdapDocs virtual host and click Next



Enter sec_master UserID and password. Click Next.



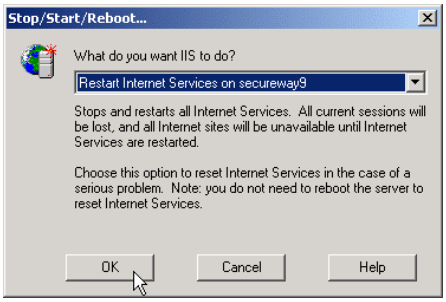
Select a port for the Plug-in Auth Server to use for AM communication . 7737 is OK. Click Next



We could configure SSL communication to LDAP – but we're not going to. Select No and click Next. Configuration begins. When complete you will see the following message telling you that you need to re-start the Web Server to activate the AM plug-in.

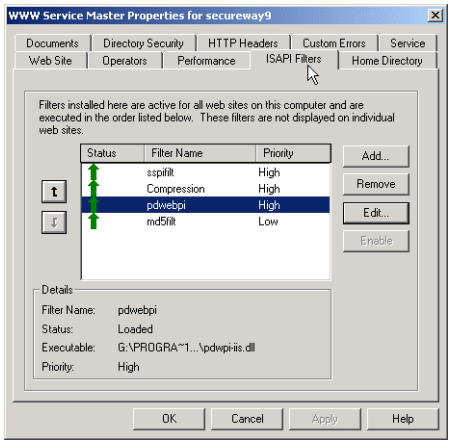
Click OK to exit the configuration.

In order to load the plug-in restart the IIS Web Server by either restarting the "IIS Admin Service" or using the MMC for IIS.



> If you connect to AMWebPI at this point with IE then you will get an unauthorized error. This is because IIS is trying to negotiate a NT Lan Manager login with IE (Integrated Windows Login). In order to bypass this we will set up forms based authentication.
>
> If you want to use AMWebPI and IIS with Basic Auth then you must turn off "Integrated Windows authentication" under IIS Properties->Directory Security->Edit (Authentication Control).

2) Now let's take look at the IIS properties. Right click on your hostname in Internet Information Services and select Properties. Then Click "Edit" next to WWW Service.



Click on to the "ISAPI Filters" tab, which shows installed IIS plug-ins. It should contain "pdwebpi," for **P**olicy **D**irector **W**eb **P**lug **I**n Filter.

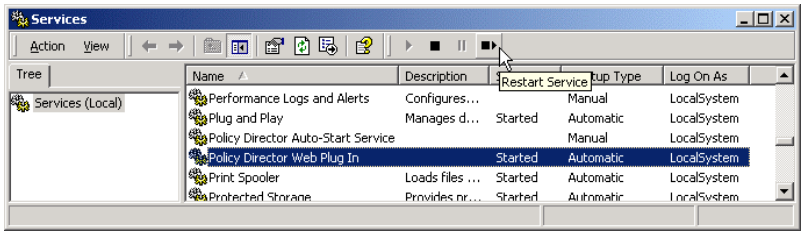
3) Configure forms-based login for Access Manager WebPI. Modify the AMWebPI configuration file. It is located by default at *C:\Program Files\Tivoli\PDWebPI\etc\pdwebpi.conf*.

```
# 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.



5) Restart the AM WebPI Service.

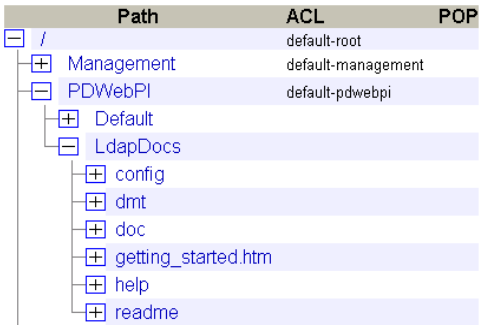
The AM Web Plug-in is now installed and configured.

15.6 Using Access Manager WebPI for IIS

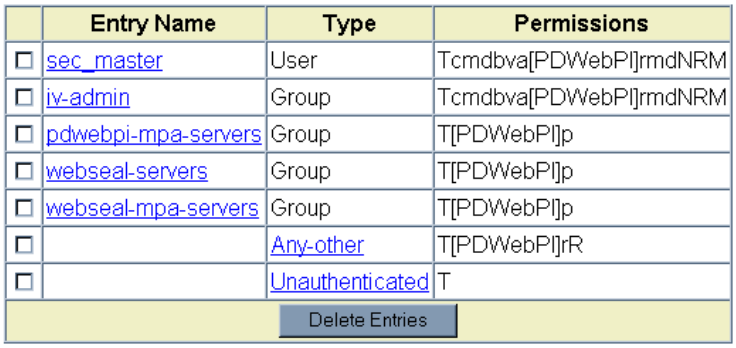
The AMWPI can be managed using the Web Portal Manager. How about protecting resources served by IIS?

15.6.1 Procedure

1) Connect to AM Web Portal Manager or, if you prefer CLI, use pdadmin CLI to perform the following operations. Point the browser to the AM WPM and authenticate as **sec_master**. Navigate to Object Space -> Browse.



2) New object entries have appeared. As AM WebPI works on a virtual host basis, there is no notion of the server that AM WebPI is running on, rather just virtual host names. Take a look at the default-pdwebpi ACL by clicking on it.

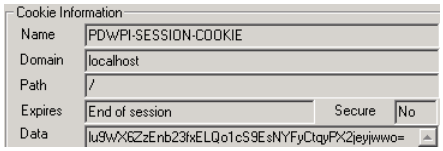


The ACL shows that All Authenticated users are granted the permissions to access the Web resources on the Web server protected by AM WPI and unauthenticated users have no access.

3) The permissions to access IIS resources protected by AM WebPI are put together in a separate Action Group. In order to see it navigate to ACL ->List Action Group -> AMWebPI

	Name	Label	Type
☐	r	Read	HTTP
☐	m	Modify	HTTP
☐	d	Delete	HTTP
☐	N	Create	WebDAV
☐	R	Property Read	WebDAV
☐	M	Property Modify	WebDAV
☐	p	Proxy	Proxy
		Delete	

4) Point the browser to *http://<your hostname>:888*. You are presented with the login page of AM WebPI. Log in providing the user ID and password of any valid user.



If you turn on warnings when receiving cookies on your browser, you will see the cookie from AM 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 AM WebPI in foreground mode rather than as a Service. Consider the order of the actions as follows:

- stop AM WebPI Service
- stop IIS (WWW Service)
- navigate to the AM WebPI "bin" directory and issue

```
c:\Program Files\Tivoli\PDWebPI\bin>pdwebpi -foreground
```

- start IIS (WWW Service)

15.7 Configuring additional virtual hosts

To configure additional virtual hosts re-run the configuration GUI and select the additional hosts. This will added these to your AMWEB PI configuration and will be visible in the objectspace.

At the time of writing an error is displayed when the configuration program attempts to start the AMWebPI service - which is already running. This does not seem to present a problem. The new virtual hosts are immediately protected – no need to restart IIS.

? Can you try this to enable the Default virtual host

15.8 What You Did in this Lab

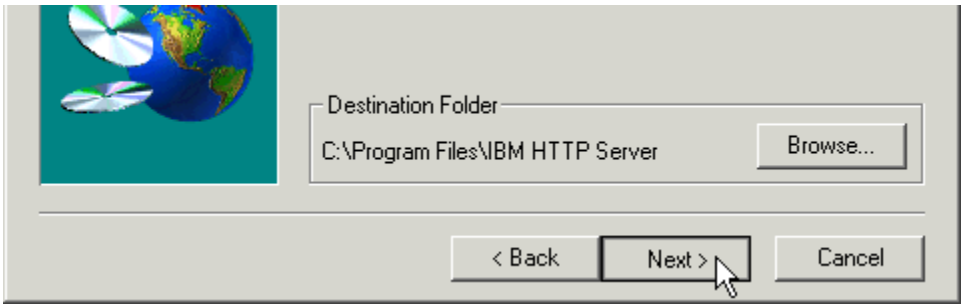
In this lab you installed the Access Manager Web Plug-In into IIS. You created a virtual host. You configured AM WebPI and turned on security for IIS-served resources. Then you re-ran the configuration GUI and added an additional virtual host for AMWebPI protection.

16 Appendix A -- Installation

16.1 Installing IBM HTTP Server 1.3.19

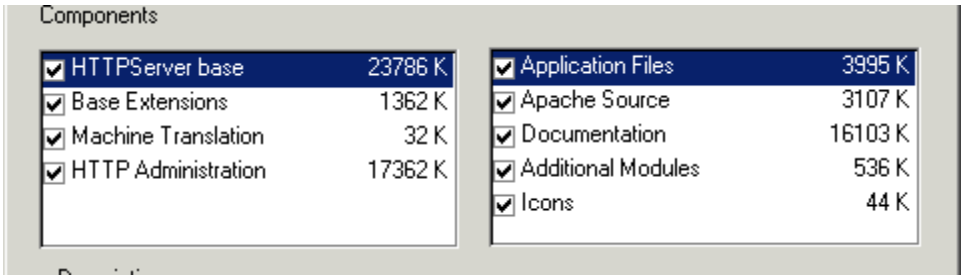
16.1.1 Install IBM HTTP Server 1.3.19

Use Windows Explorer to go to *D:\Lab Setup\HTTP-1-3-19* and launch the *setup.exe.*.

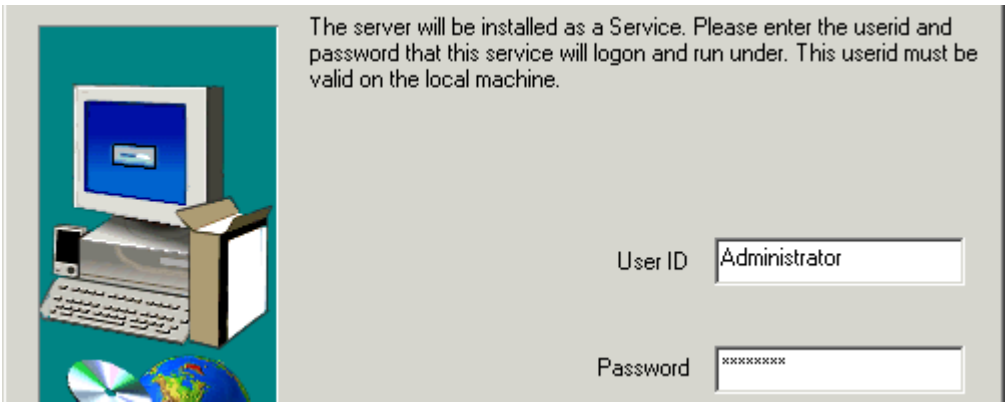


Accept English as the language and the license agreement. As the destination folder select *C:\Program Files\IBM HTTP Server*.

Select *Custom* as the installation type. click Next.



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.

16.1.2 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.

16.2 Installing GSKIT

It is a good idea to install the latest GSKIT, necessary to correctly run AM 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 5.0.4.67.* 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.

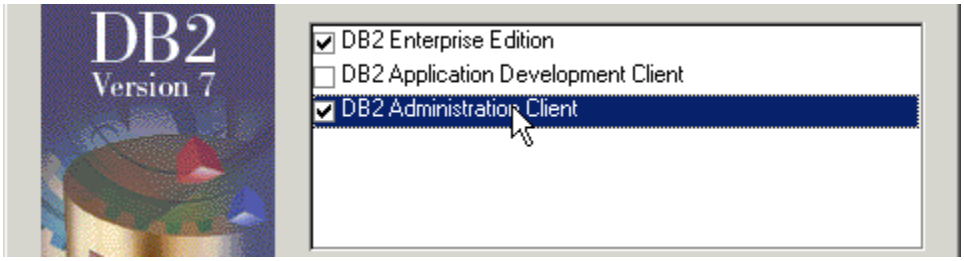
Accept all the default options than click on finish. Should you need to uninstall GSKIT from your machine, use this command:

```
C:\>isuninst -f"C:\Program Files\ibm\gsk5\gsk5BUI.isu"
```

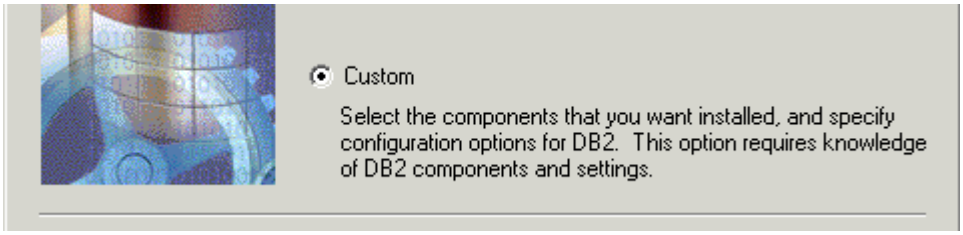
16.3 Installing DB2 7.2

> 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_7.2EE* and launch the *setup.exe.* Then click on Install.

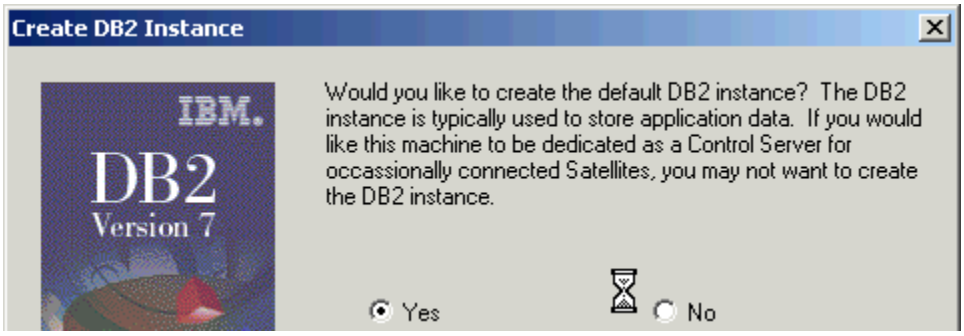


You do not need to install the application development client. Select the other two. Click Next.

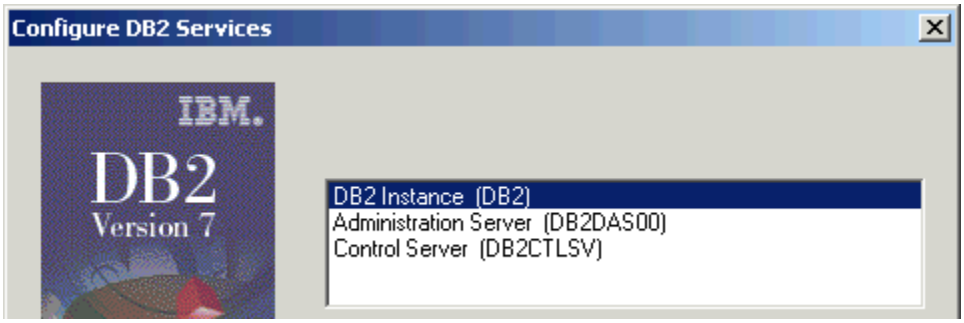


Perform a custom installation to install some administration components that could be helpful to have when working with WebSphere.

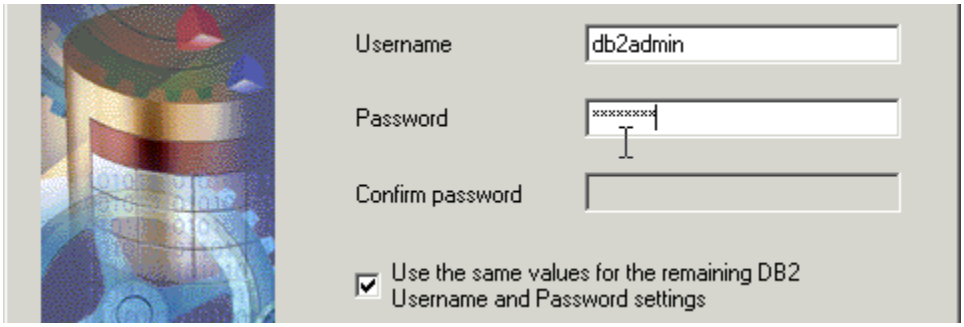
Select the indicated components. The gray'd out components are always installed anyway, so deselect everything else except Administration and Configuration Tools. Click Next.



Choose to create a DB2 instance. Click Next.



Choose to configure the three default services and click Next.



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.

16.3.1 Installing DB2 FixPack4

Use Windows Explorer to open *D:\Lab Setup\db2_7.2EE-fp4* 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.

16.3.2 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.

If running, stop the DB2 processes that use JDBC as shown. Open a DOS prompt and go to *C:\Program Files\SQLLIB\java12*.

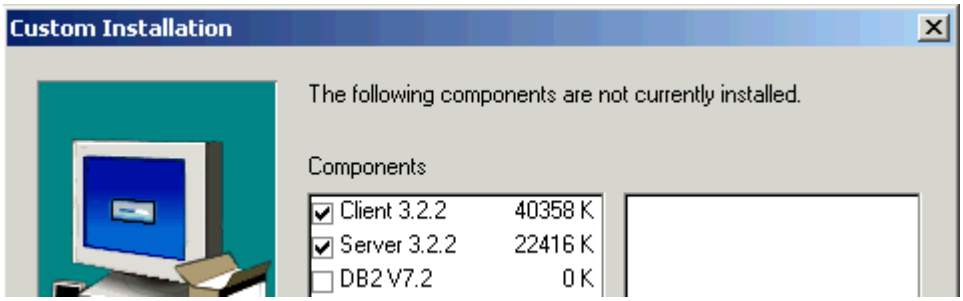
Run *usejdbc2.bat* and be sure that all the files are correctly copied as shown. Your DB2 is now ready to be used by WAS 4.0, and even by IBM Directory Server in case you plan to use this as your user registry for AM 3.9.

16.4 Installing IBM SecureWay Directory Server 3.2.2

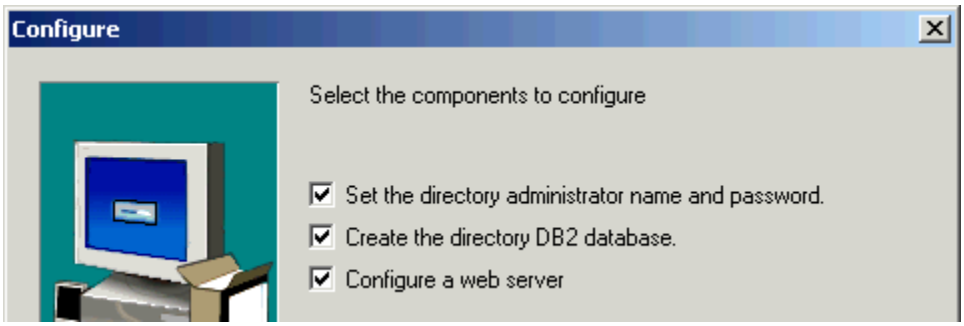
Use Windows Explorer to open the drive where the *D:\Lab Setup\ldap322\ldap32_u* and launch the *setup.exe* .

Accept English as installation language, and accept the licence agreement and the default installation directory.

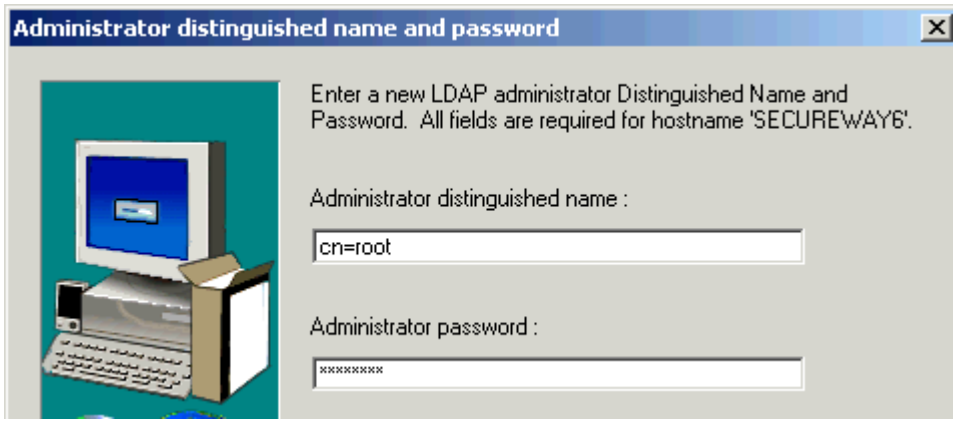
The set-up procedure should find DB2, the GSKIT and the IBM HTTP Server already installed, if all the steps described before have been successfully completed. Select Custom Installation.



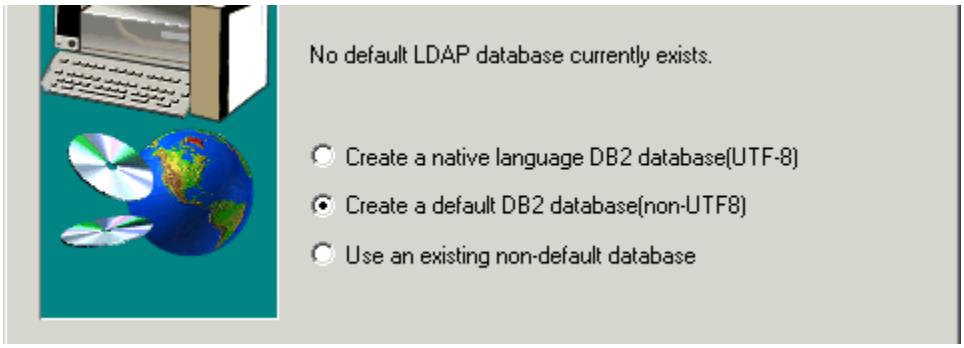
By selecting a custom installation you can verify that only the components not yet installed, such as the LDAP Server and Client, are selected. Click Next.



Accept the creation of a program folder in the Programs menu. When asked, select all three options to configure as shown. Click Next.



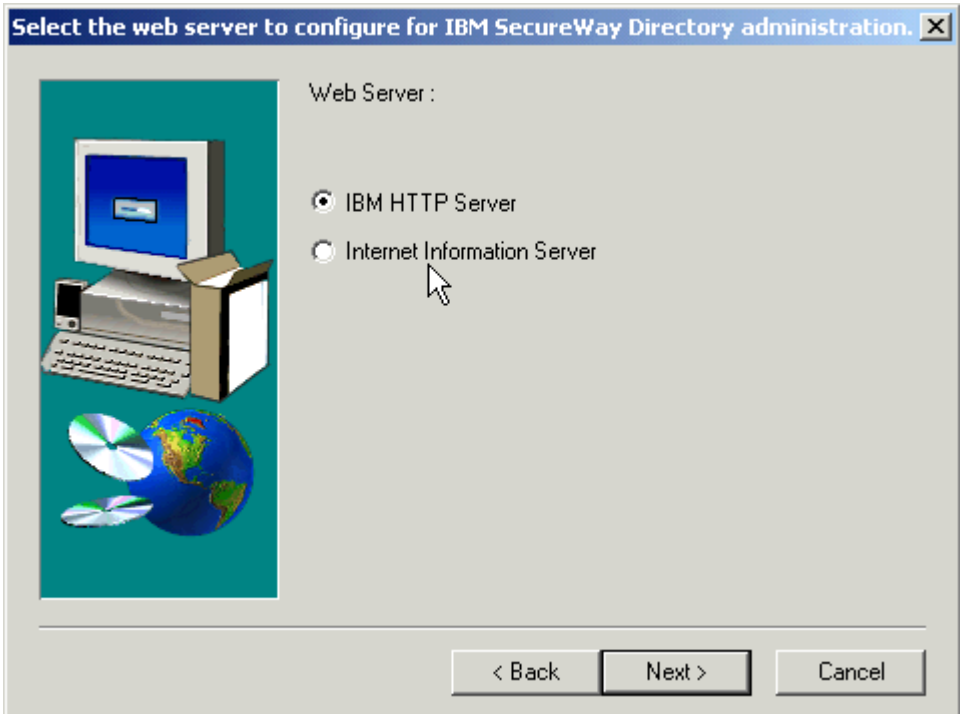
Enter *cn=root* and *passw0rd* for the Administrator DN and password. Click Next.



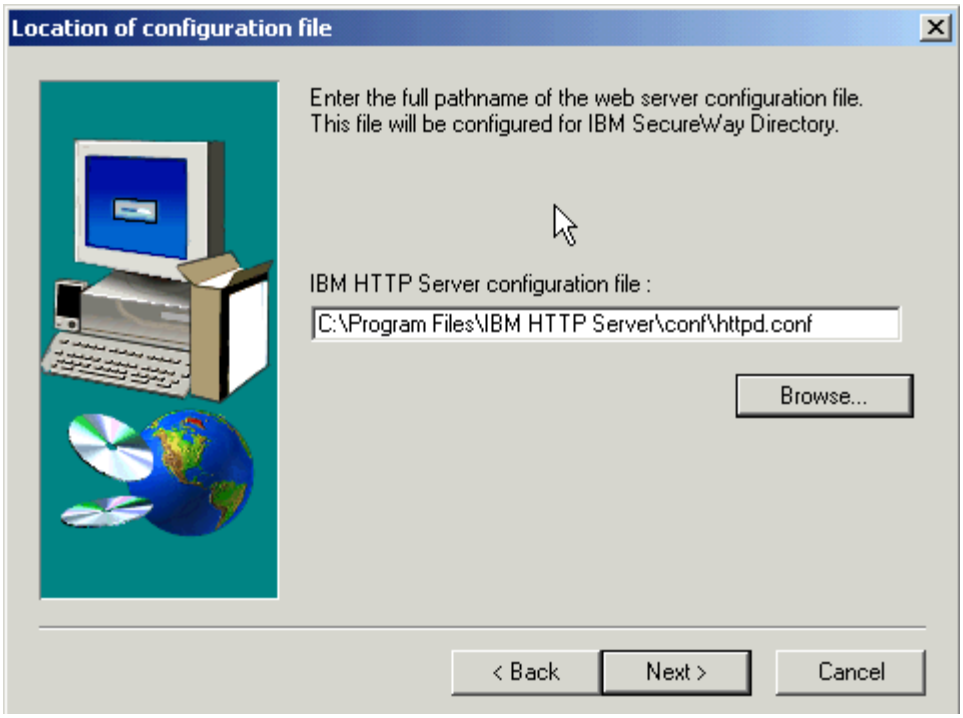
Select the default DB2 database (non-UTF8) and click Next.

? 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.

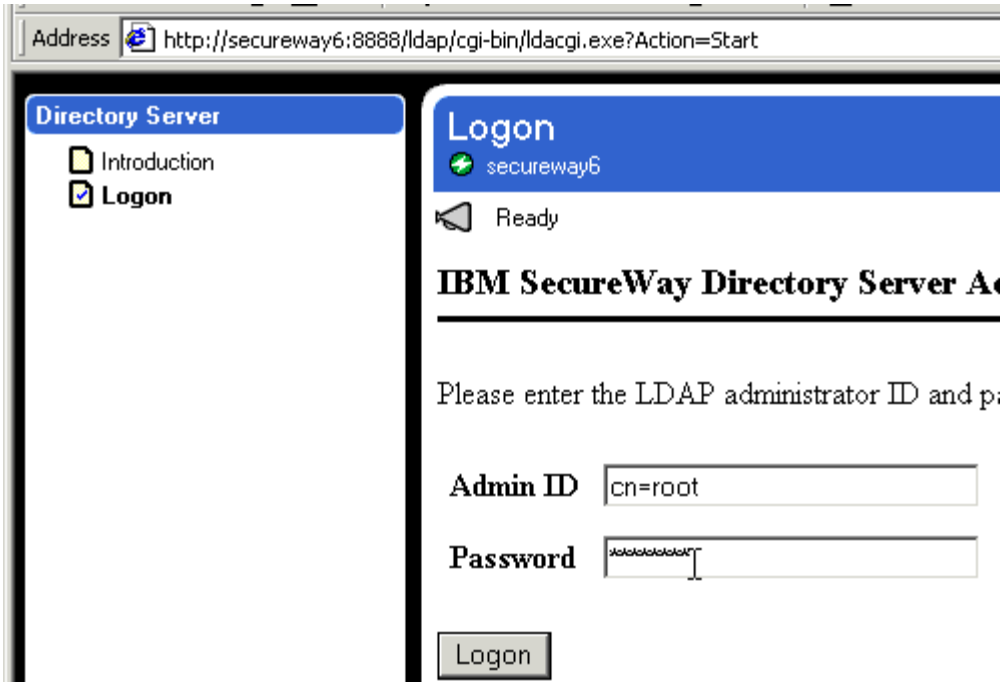


Verify that the IHS configuration file is in the right path. Click Next and proceed with the installation.

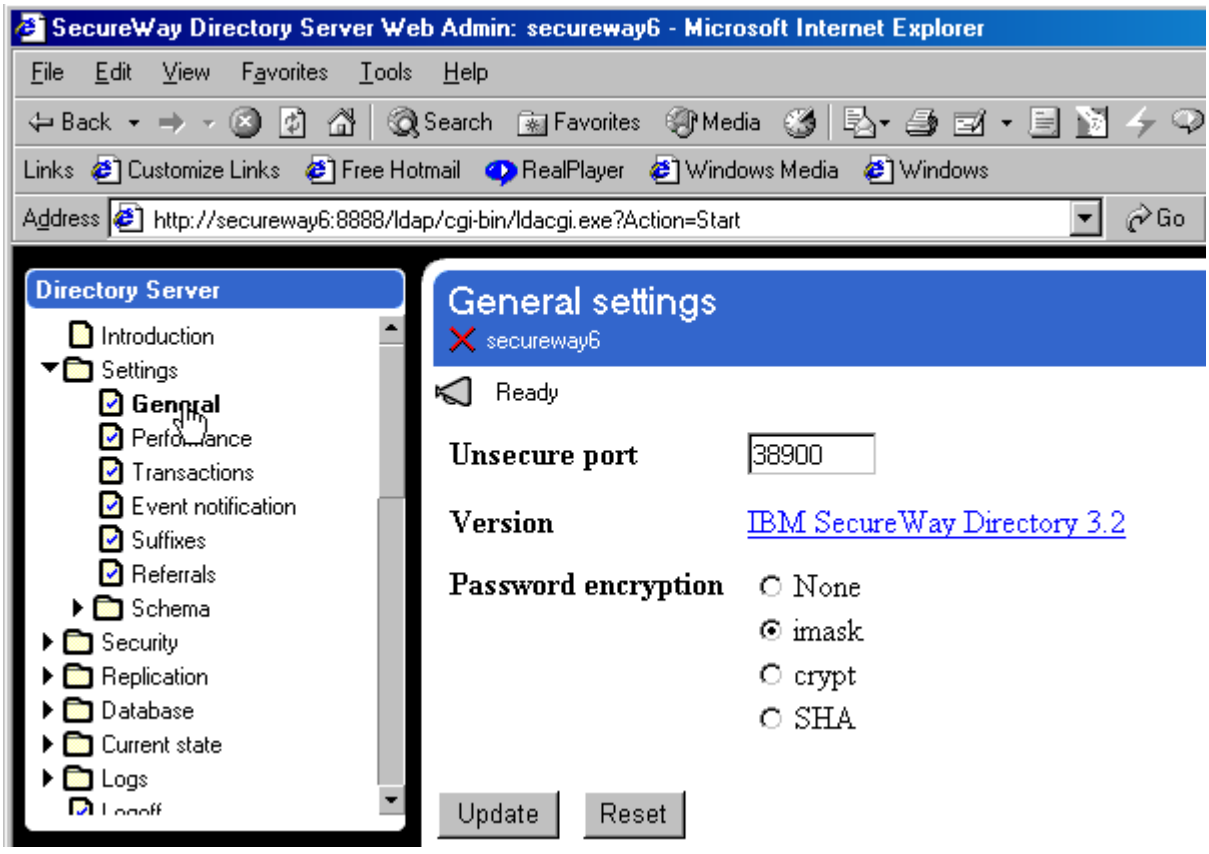
Restart the machine and after rebooting, log in as *Administrator*. You will see that the configuration of the LDAP database takes some time. If the configuration completes successfully you can go on to configure of the directory for Access Manager. If not, run the installation again using Start->Programs->IBM SecureWay Directory->Directory Configuration. Select the same options you selected in this lab. And good luck!

16.4.1 Configuring IBM SecureWay Directory Server 3.2.2 for AM 3.9

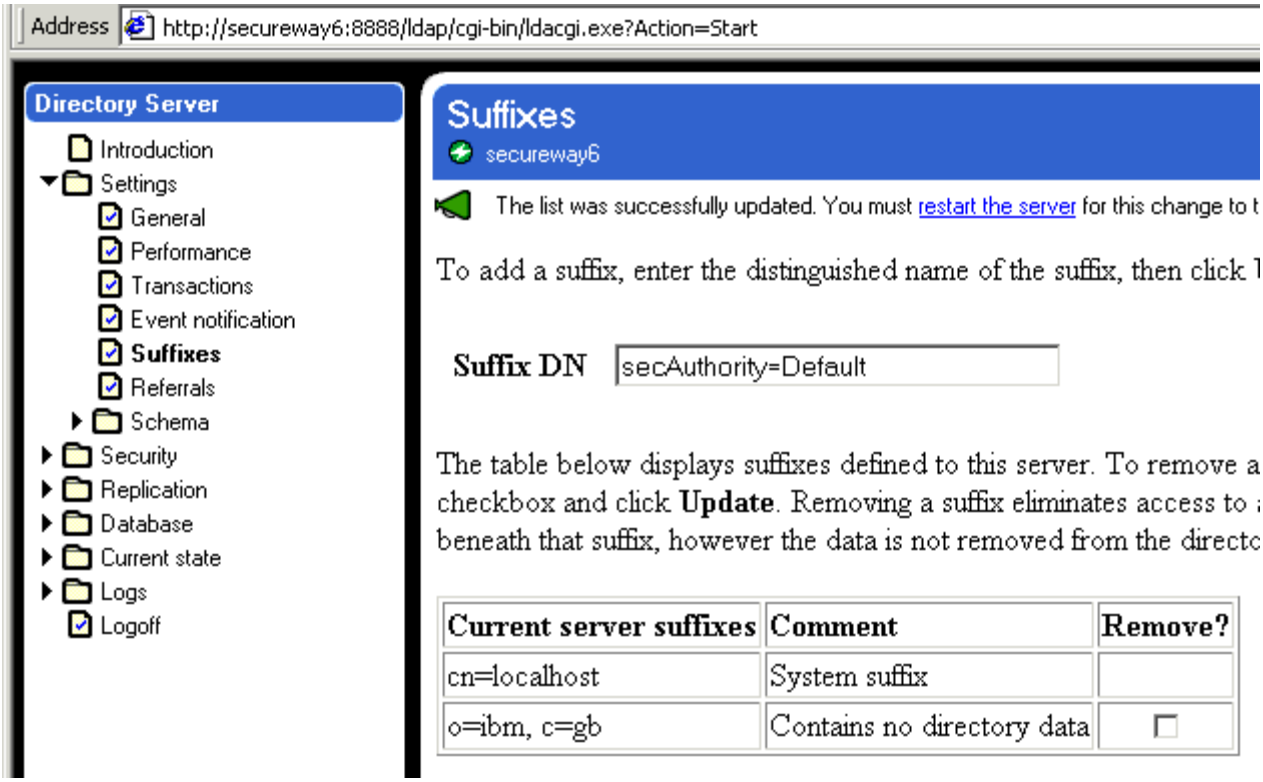
Now it's time to perform some management tasks on the LDAP server. Ensure that IBM HTTP Server and the LDAP Server are running



Point a browser to *http://yourhost:8888/ldap* 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 1.5.2 IBM Directory Server Configuration Options. Click Update. Then on the left click on Suffixes.



Add the Suffix DN *o=ibm,c=gb* (as per conventions for this lab) and the Access Manager suffix, *secAuthority=Default*. Click Add after entering each one.

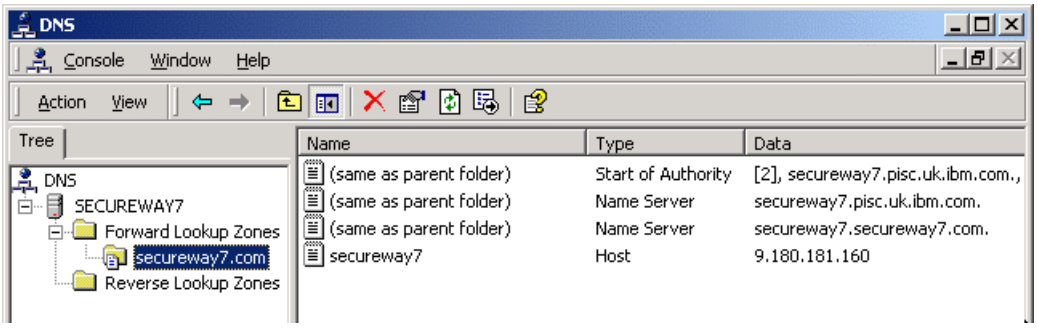
Restart the server by clicking on the restart the server link. The LDAP server is ready to be used by Access Manager 3.9.

16.5 Installing Active Directory

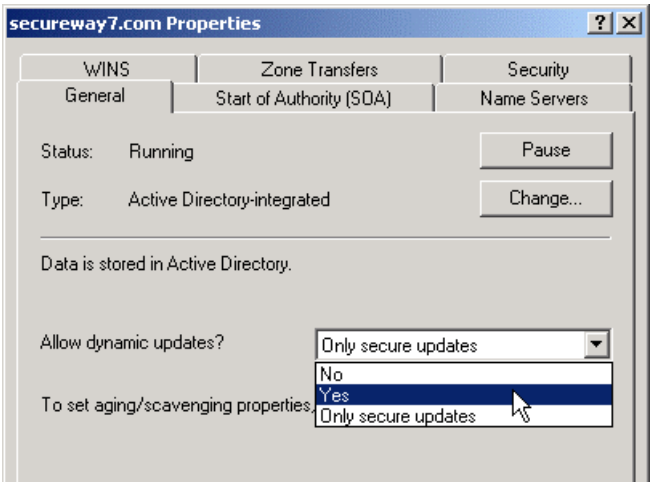
16.5.1 Before You Start Installation

Active Directory can be used as the user registry with Access Manager

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.



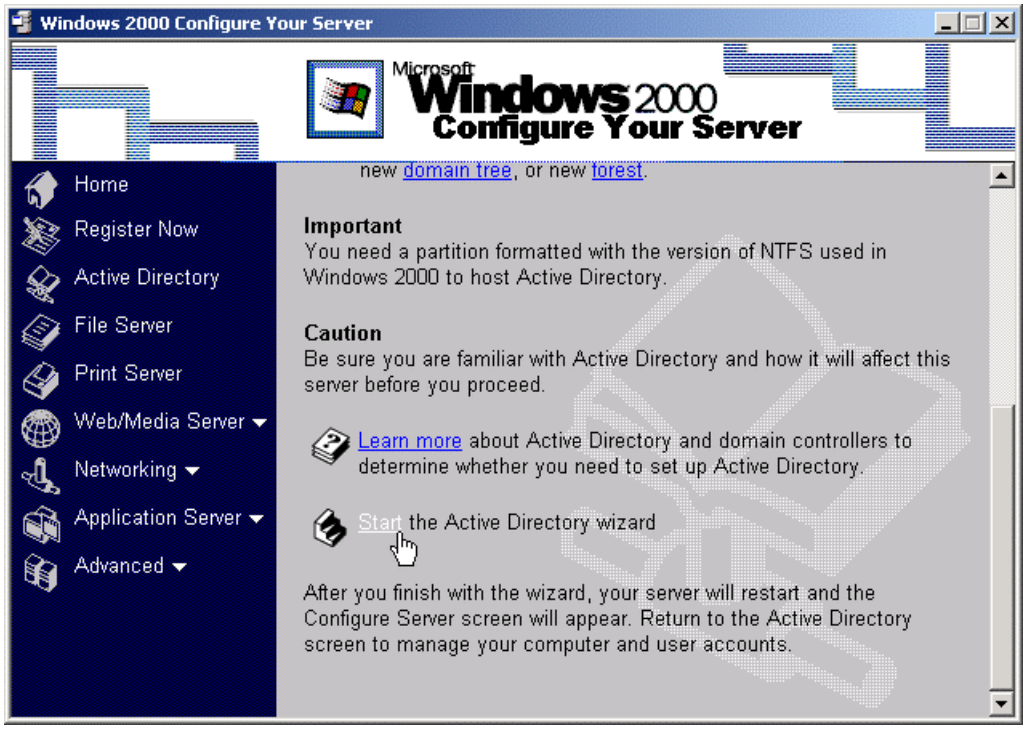
Change Allow dynamic updates to Yes and click OK. Now the Active Directory install wizard should be able to properly configure the DNS.

> 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.

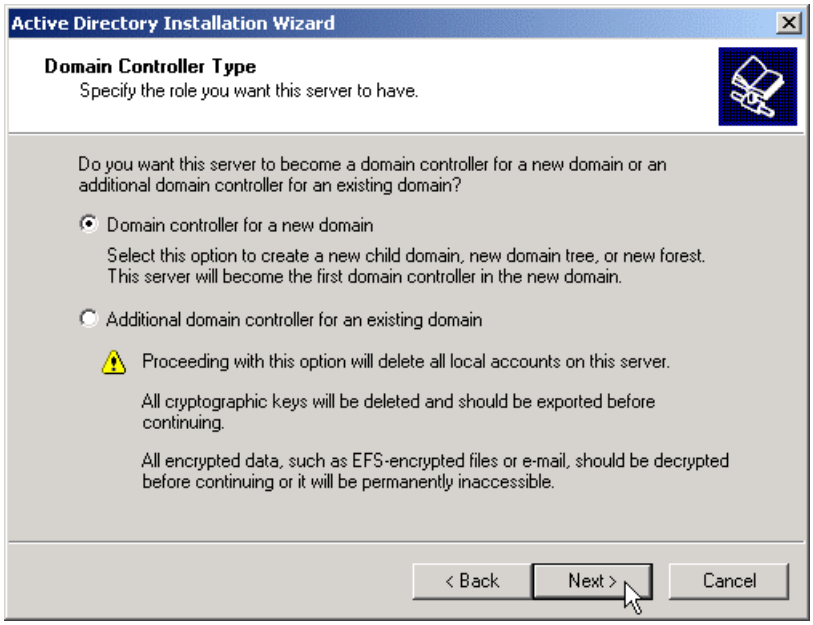
16.5.2 Installation of Active Directory

Now, to begin the Active Directory installation, select

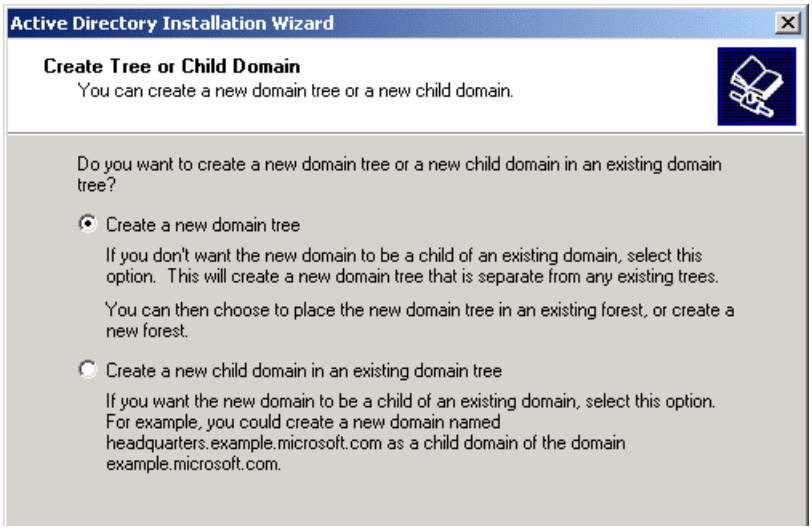
START->Programs->Administrative Tools->Configure Your Server. When the dialog comes up click on Active Directory on the left side.



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.

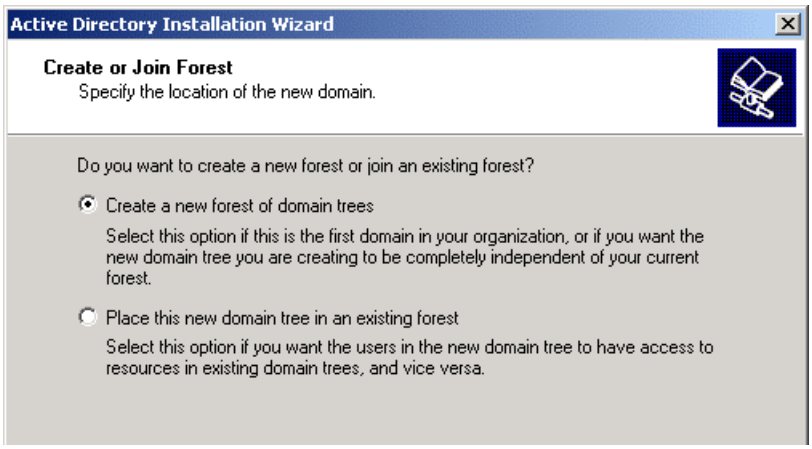


Select Domain controller for a new domain and click Next.



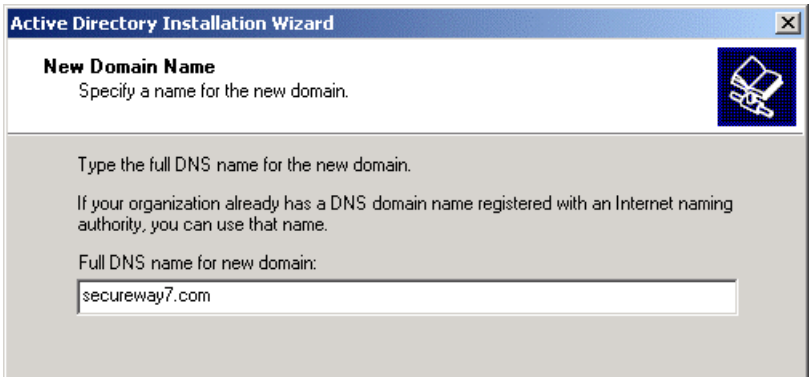
Select Create a new domain tree and click Next.

> 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.



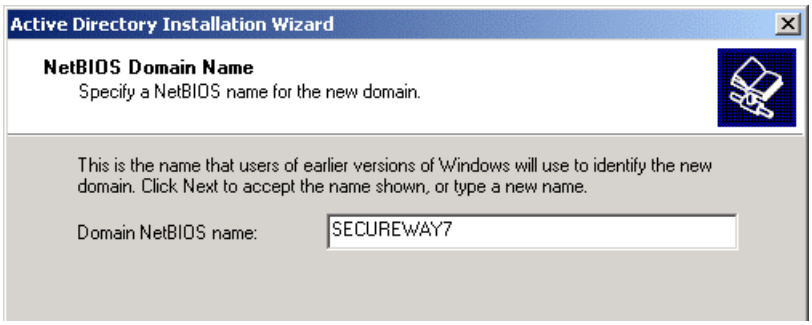
Select Create a new forest of domain trees.

> A forest is one or more domains that share a common schema and global catalog. A forest can contain one or more domain trees.

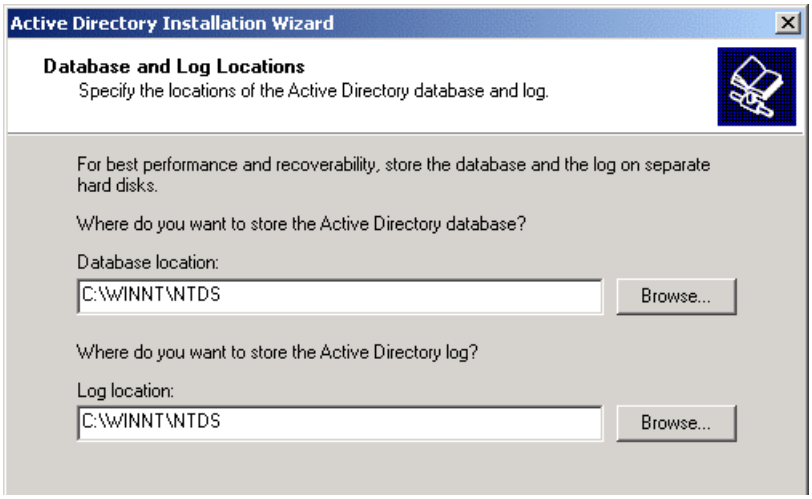


Enter a name, such as <yourhost>.com, for the DNS of the new domain and click Next.

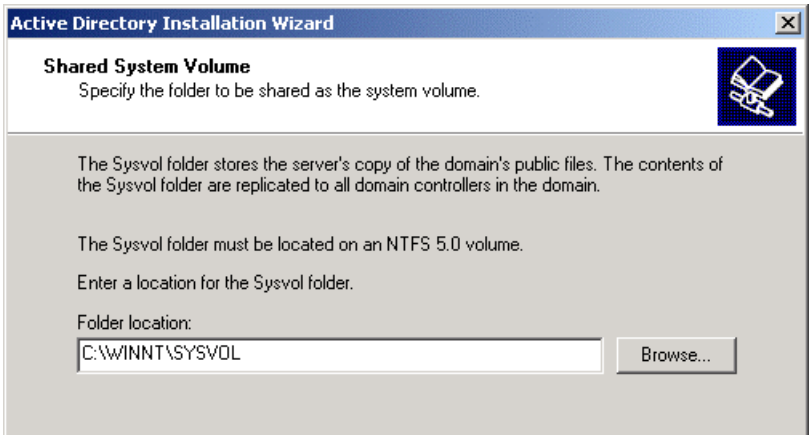
> You might see a message that another NetBIOS name was selected due to name conflicts on the network. Accept this by clicking OK.



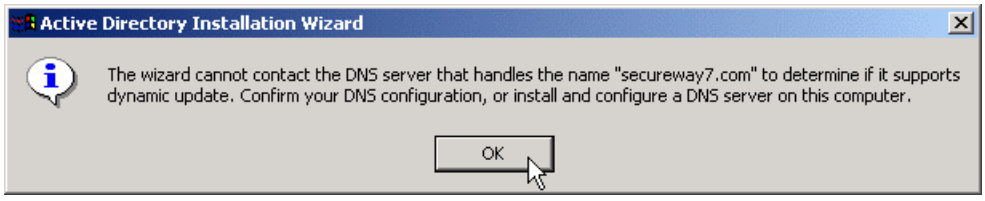
You may see this dialog. Click Next.



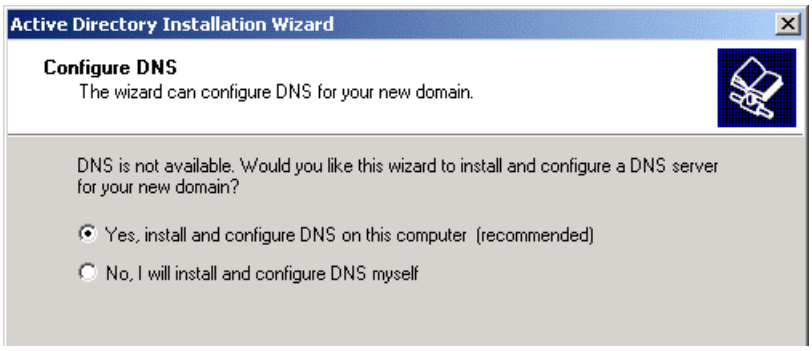
Take the defaults for the database and log locations, and click Next.



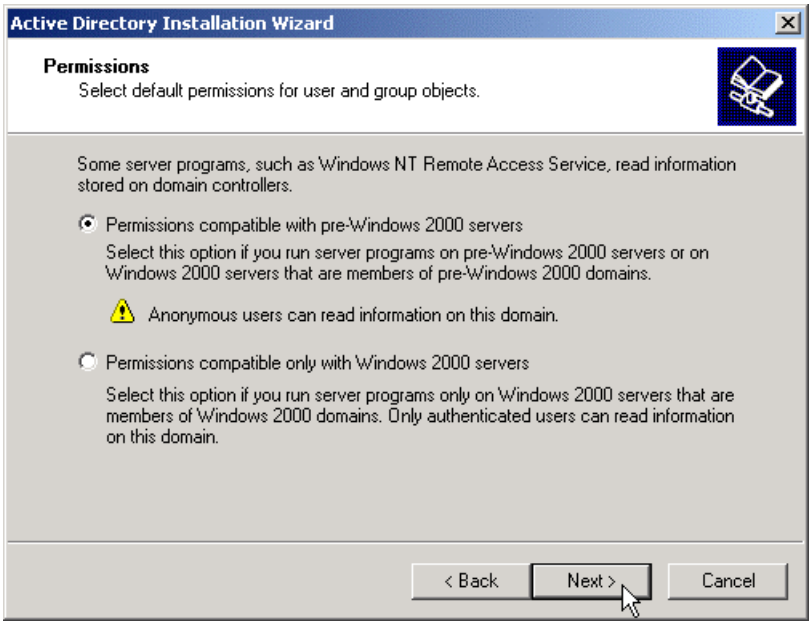
Take the defaults for the Shared System Volume folder location and click Next.



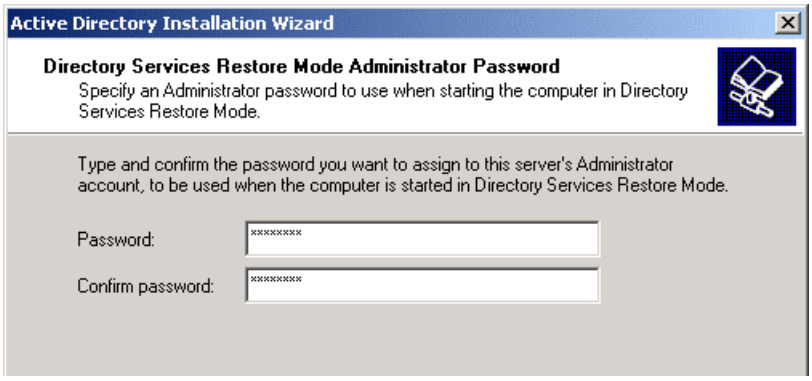
The DNS server is not yet available and configured, so just click OK.



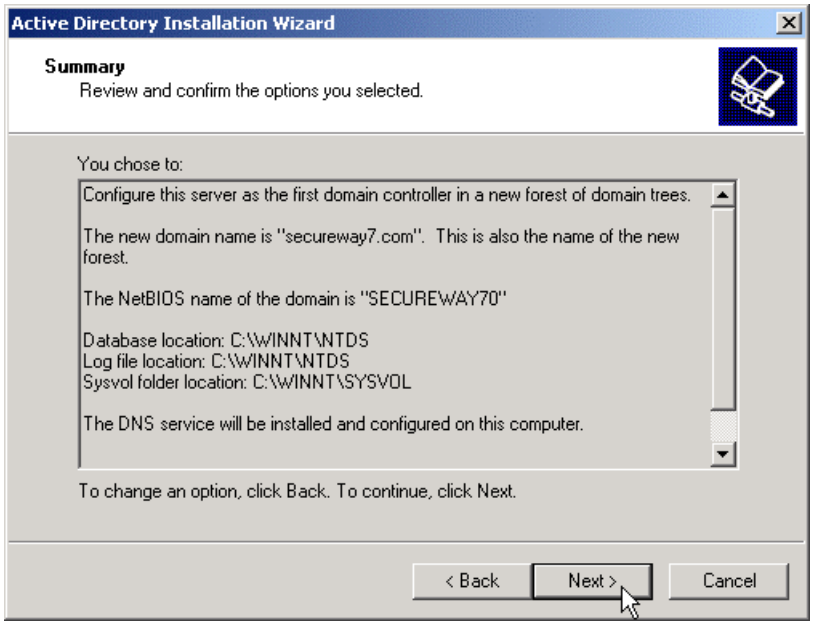
Accept the default to configure the DNS and click Next.



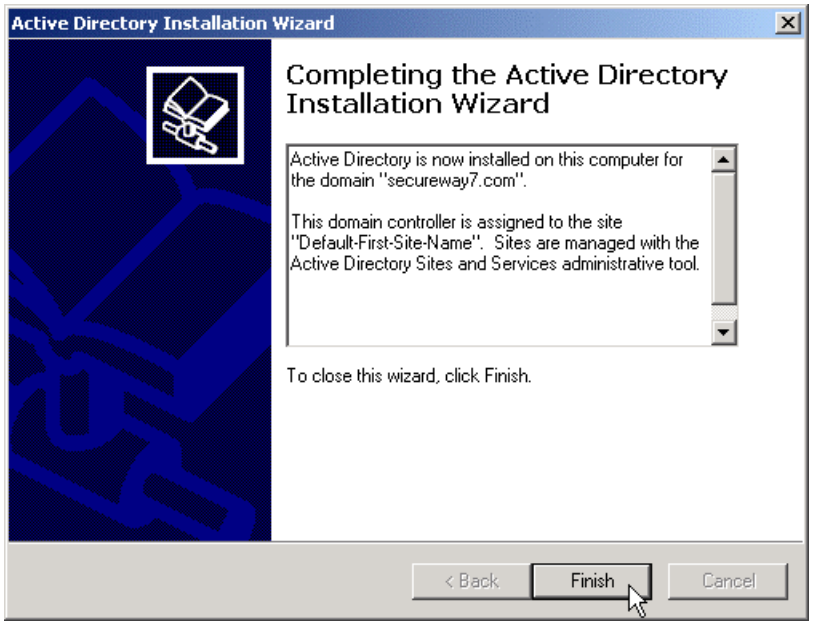
Accept the default permissions and click Next.



Enter "passw0rd" twice and click next.



Review the summary and click Next. Wait while the configuration process runs.



Congratulations! You've installed Active Directory. Click Finish.

16.6 Installing Domino Server

16.6.1 Domino Server Configuration Options

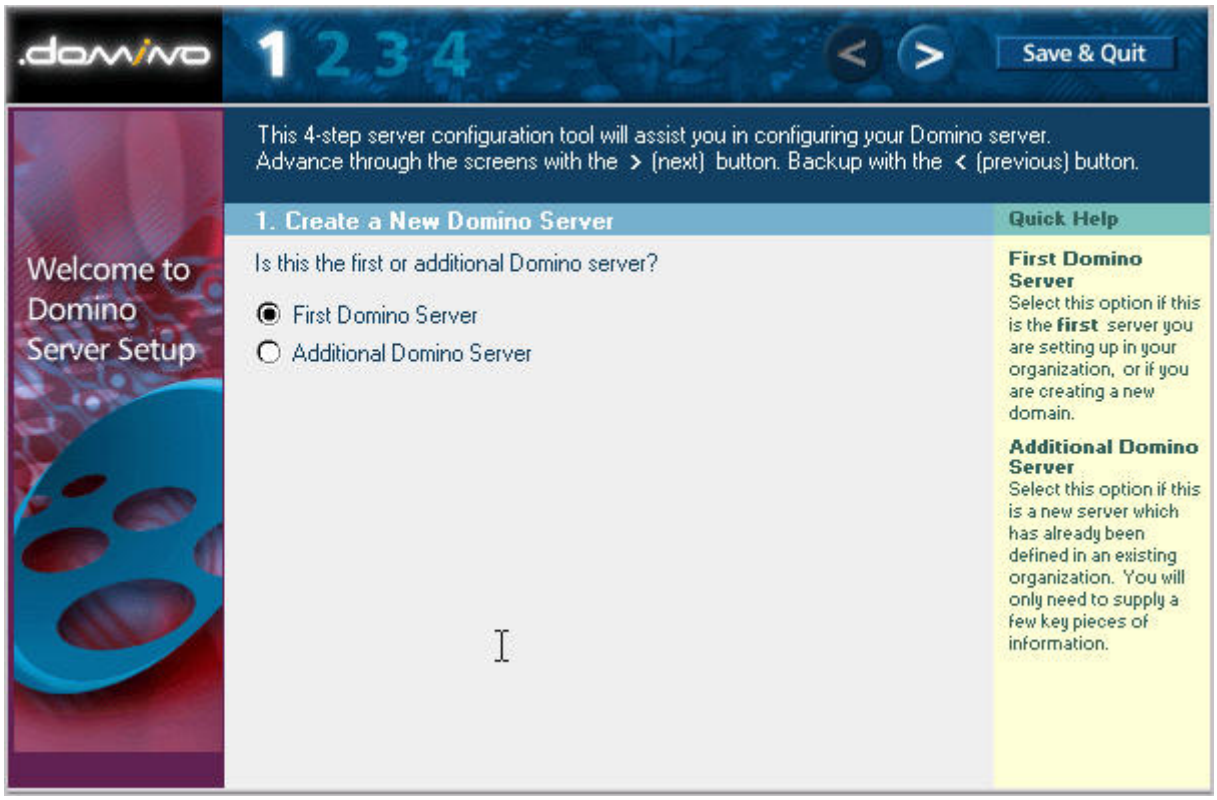
Install the Domino Server 5.0.4 (or higher) on Windows 2000 Server using the defaults. It installs the package into *C:\Lotus\Domino* and creates a menu in the "Start-Menu:"

Start -> Programs -> Lotus Applications -> Domino

> In order to configure Domino Server and run it with Access Manager 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)

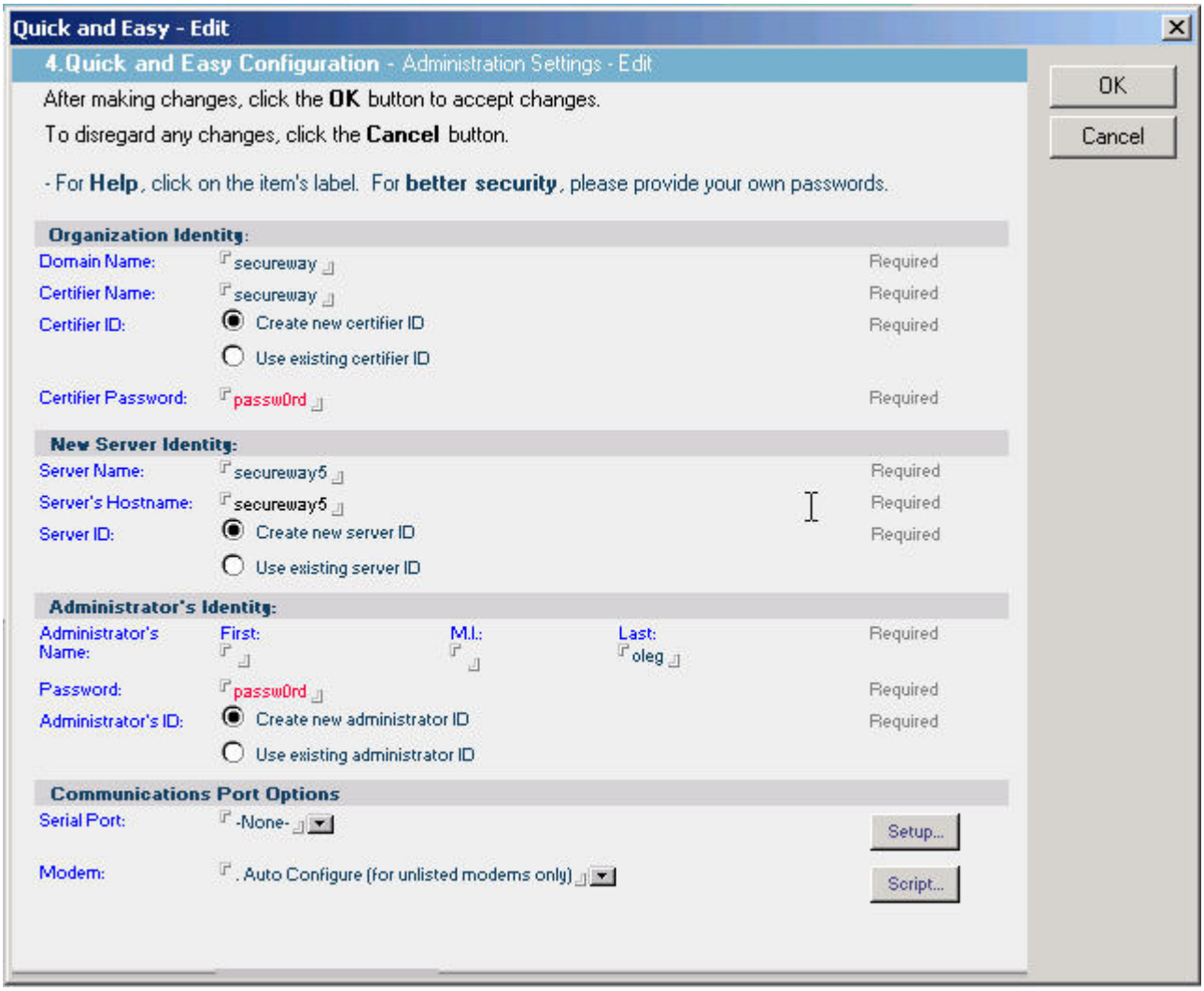
16.6.2 Basic Configuration of Domino Server

Run Start -> Programs -> Lotus Applications -> Domino -> Lotus Domino Server.



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.



Enter *passw0rd* twice, and fill in other required parameters and note them for the future use.

Domain Name: _____

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.

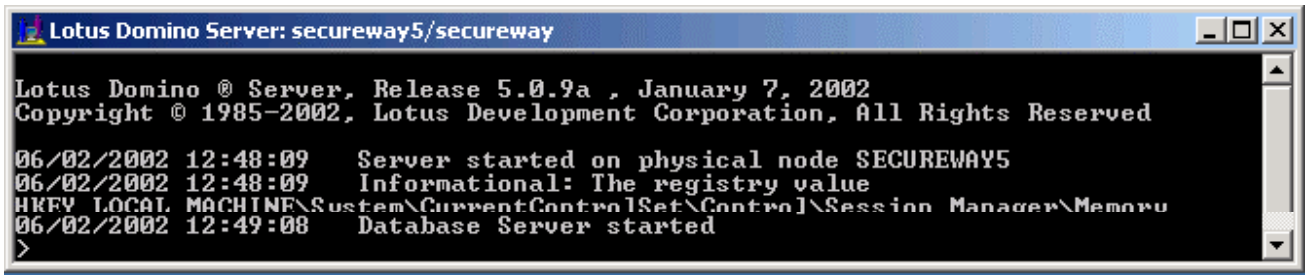
Click OK. Then click Finish.

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

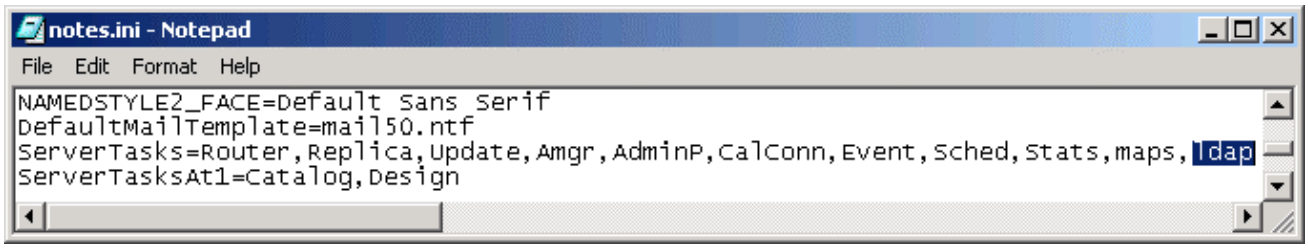
A healthy Domino Server provides console output like this:



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.*



16.6.3 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

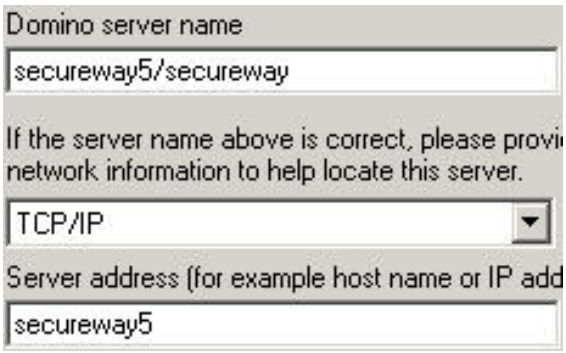
Start -> Program Files -> Lotus Applications -> Lotus Domino Administrator

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:
<Server name>/<Domain name>

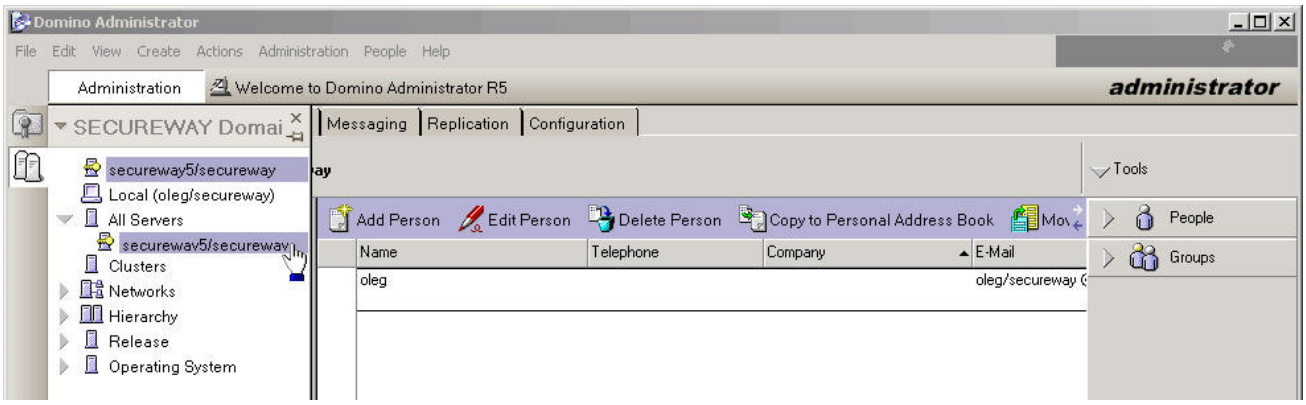
Use a name as identification. User name:
<Administrator's name>



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.

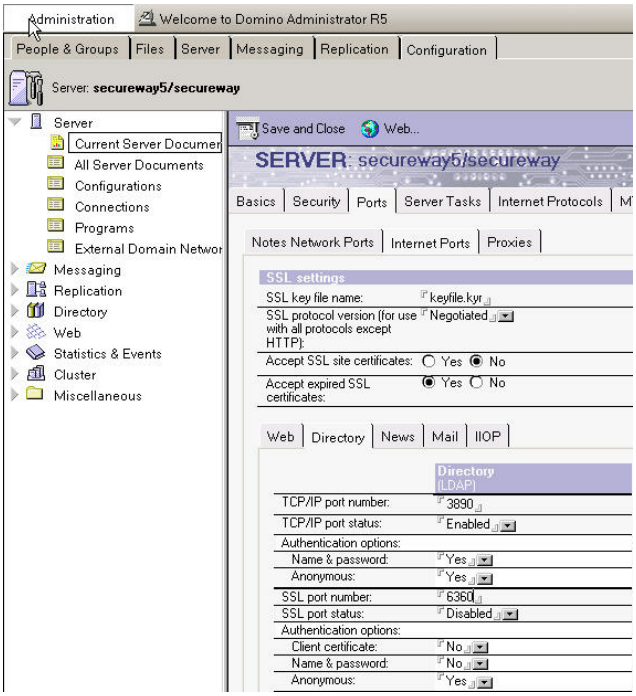
After the connection to a Domino server is set up, the client connects to the Domino server and retrieves the ID file of the administrator. You will be prompted for the password to logon as the administrator (user ID that was filled in in the previous step, e.g. "oleg").

16.6.4 Configuring Lotus Domino Server to Run with Access Manager



16.6.4.1 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.

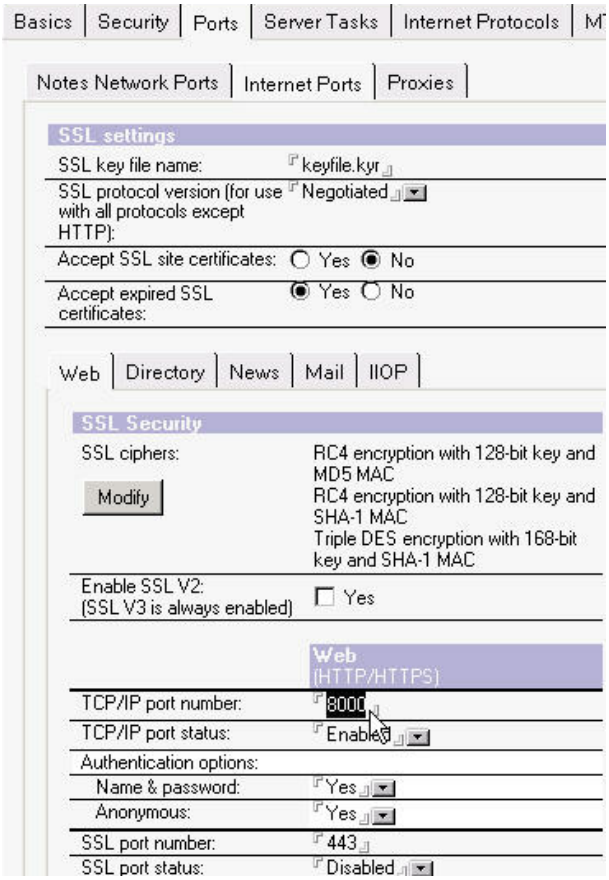


Change the TCP/IP port number to 3890, the port you will use for Domino throughout the labs. Apply the change by restarting the Domino LDAP task using the Domino Server Console:

```
> tell ldap quit
> load ldap
```

16.6.4.2 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.



Set the TCP/IP port number to 8000 and restart the HTTP task using the Domino Server Console:

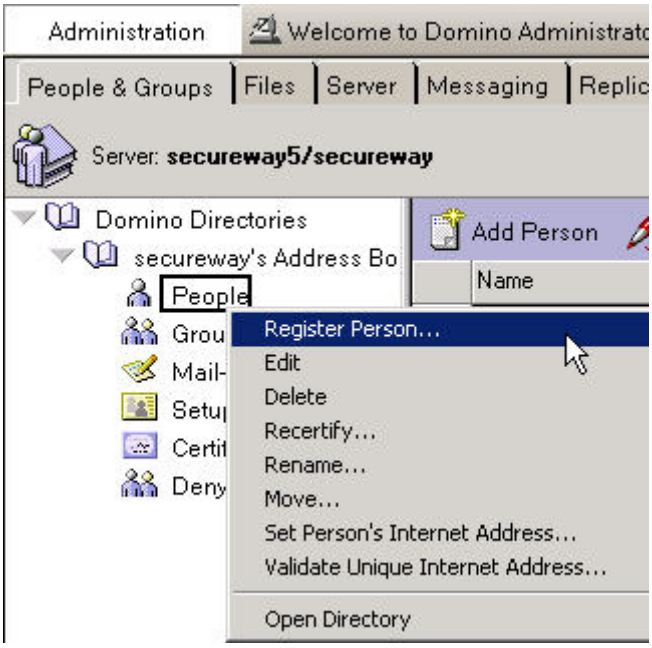
```
> tell http quit
> load http
```

16.6.4.3 Configure the AM Privileged User in Domino

In order to give Access Manager 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 AM *Privileged User*, must be configured before Access Manager configuration is started.

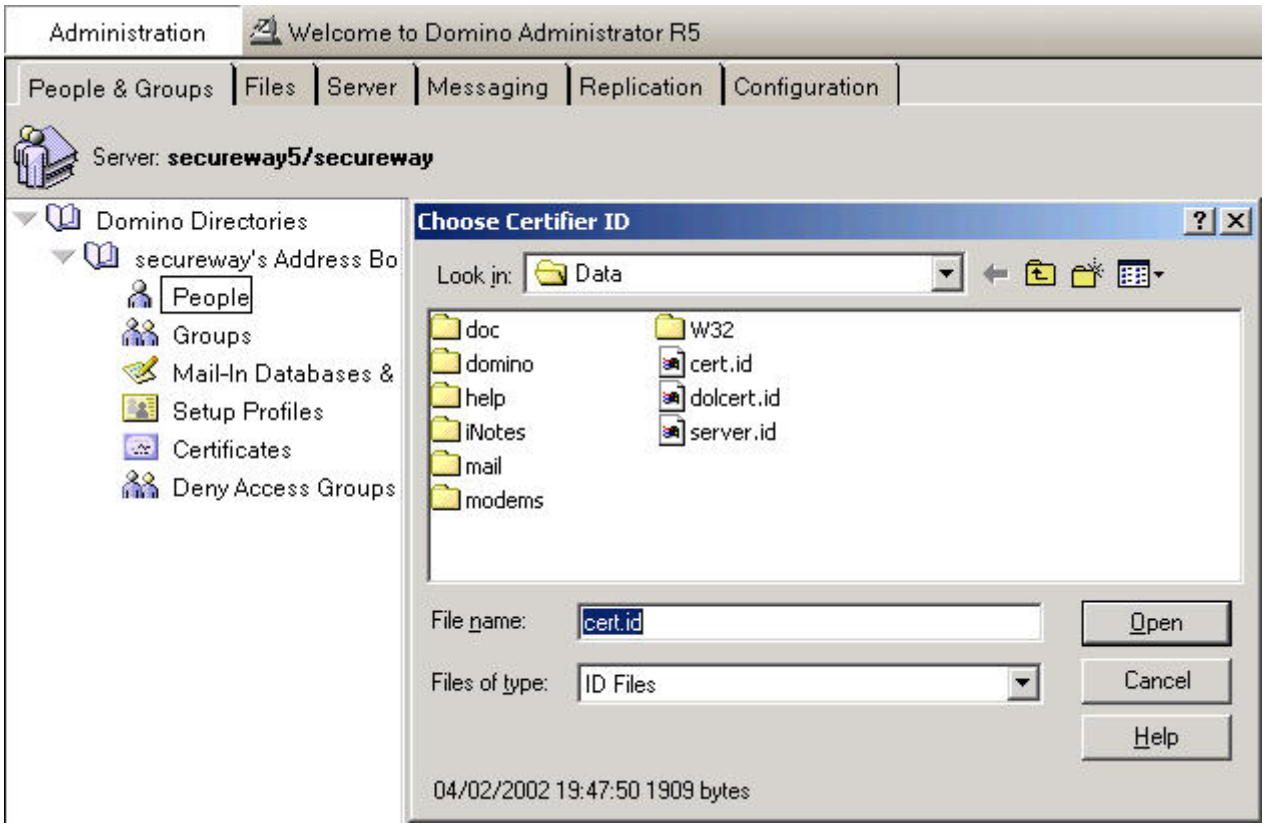
The AM Privileged User identity is used during configuration. All Access Manager servers also use this identity in order to access the Domino environment – this is different from an LDAP environment where each server has its own identity to access the registry.

To create the AM Privileged User, use Lotus Domino Administrator (GUI).

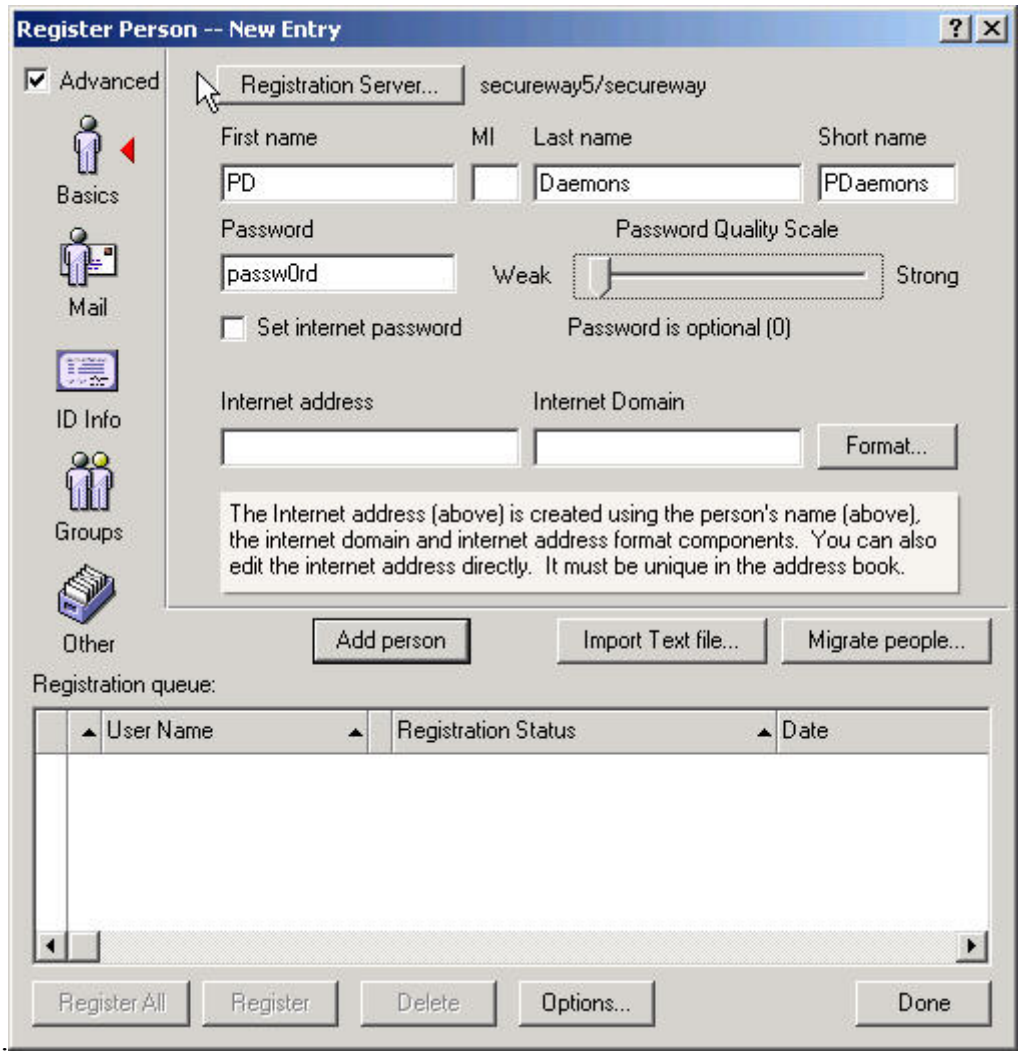


Navigate to the Domino server, go to the "People & Groups" tab and right click on the People object in the domain's Address Book (there also may be the personal Address Book, we don't want use that). Select "Register Person…."

You may be asked for the ID file of the certifier (essentially the Certification Authority in Domino).

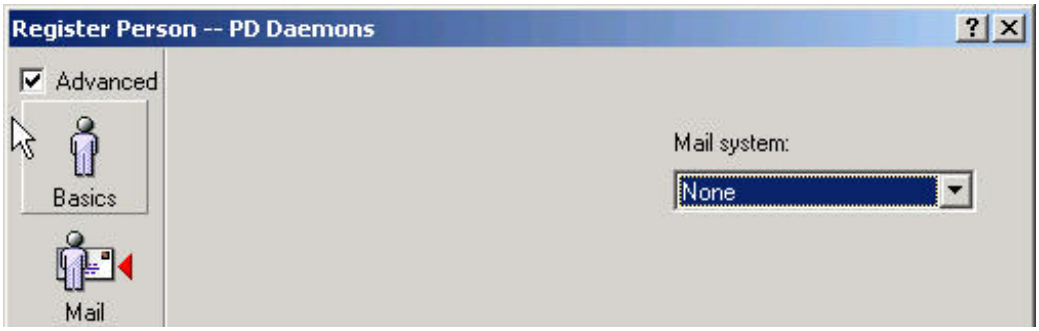


Find the ID file in *C:\Lotus\Domino\Data*. The password for this ID file corresponds to Certifier Password provided for the Organisation Identity (4th step while configuring Domino Server – see earlier screenshot). Click Open.

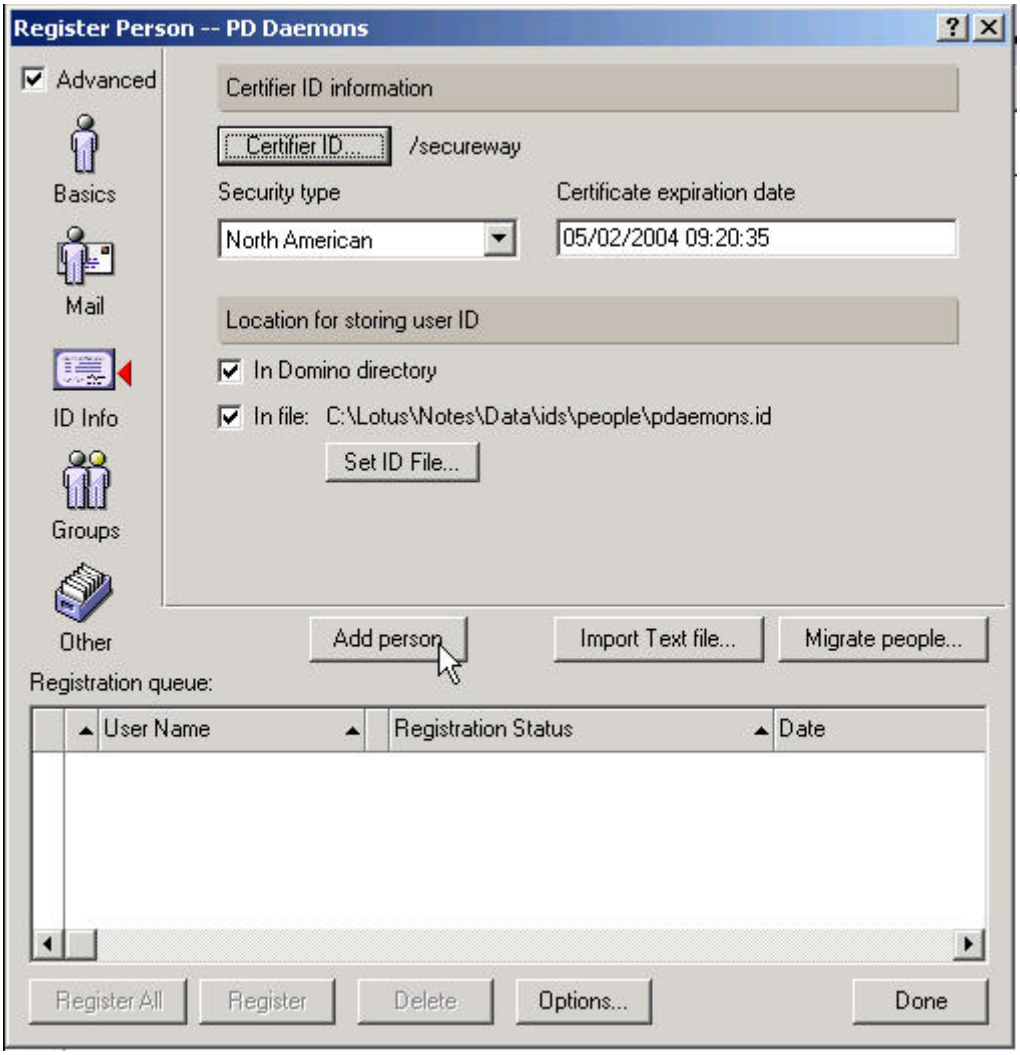


Fill in the basic information about the new user as shown. The name of the AM Privileged User is not restricted – it can be anything that is valid in Domino. In this example, PDaemons is the identity of Access Manager in Domino.

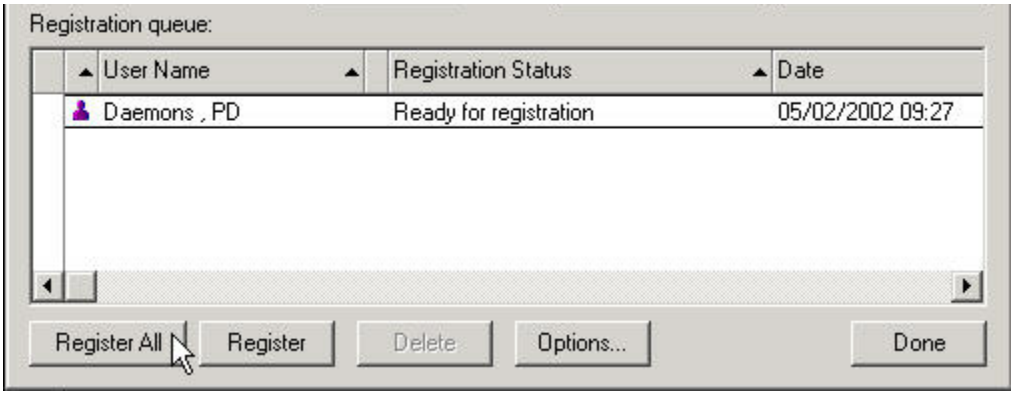
To disable Mail for that user, click on the Mail button.



Select None in the Mail system drop-down. Then click the ID Info button.

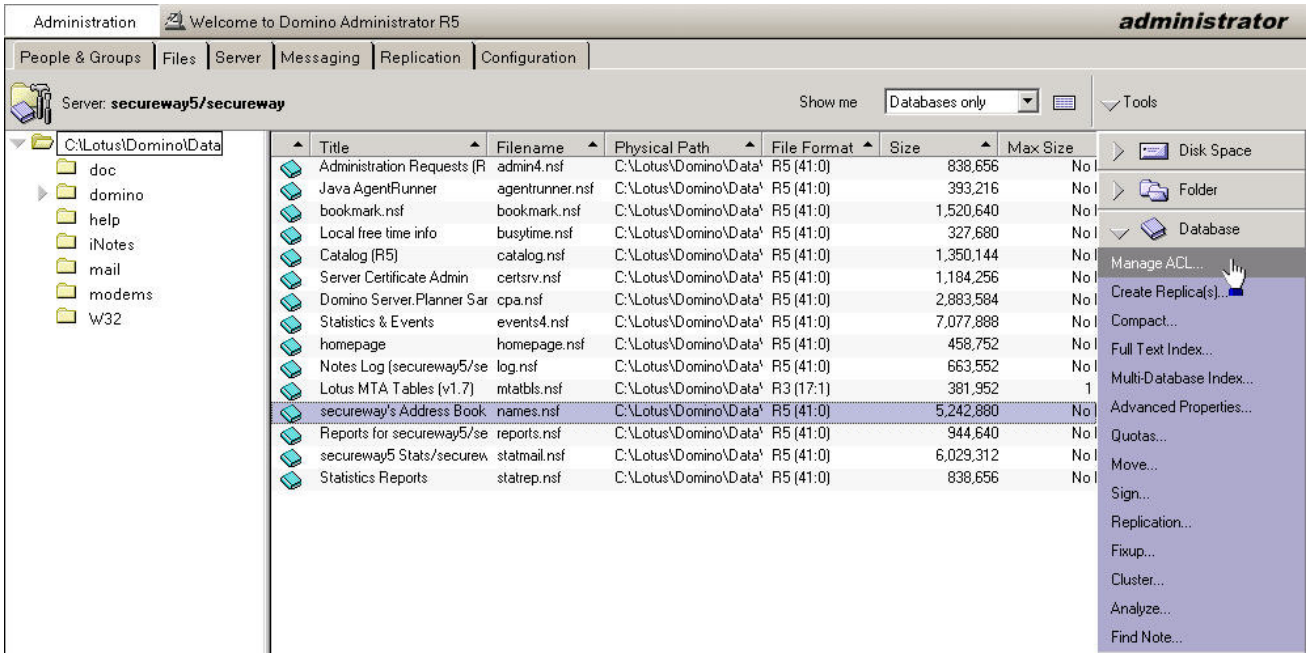


Select the option to save the ID file to disk and put the registration into the queue. Click the "Add person" button.

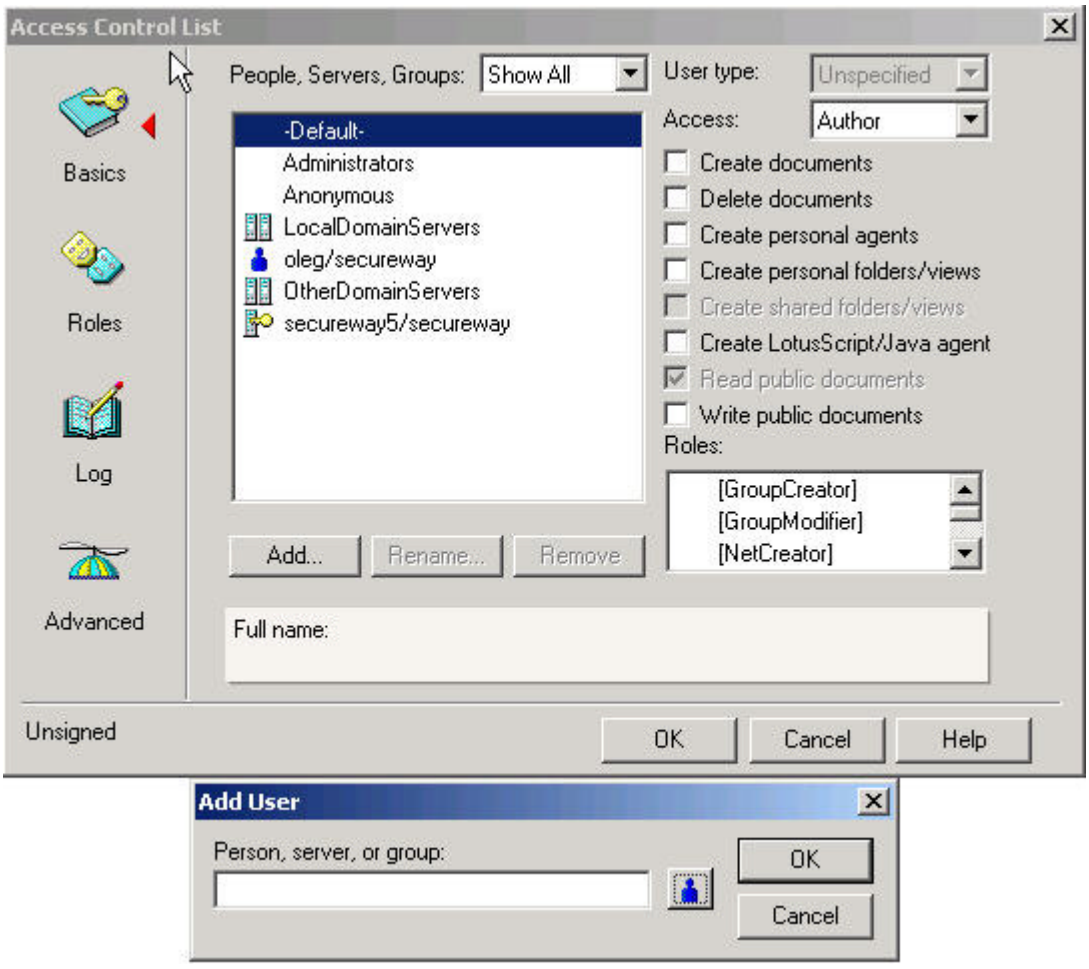


Next register the user by pushing the "Register All" button.

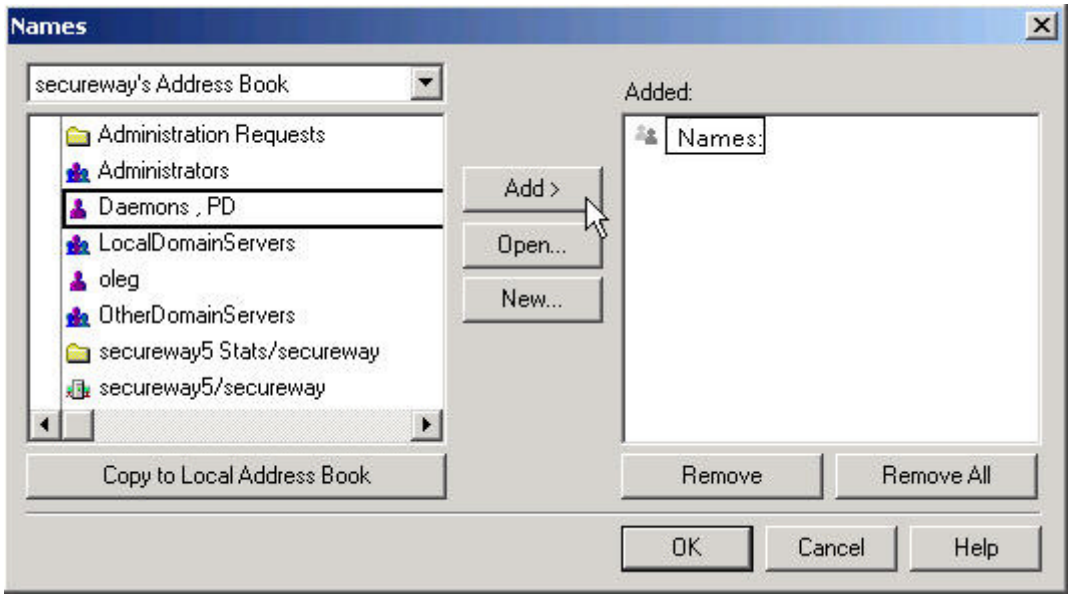
The AM Privileged User requires Manager access (including delete) to the domain NAB. To grant this user the permissions, navigate to the "Files" tab. (You were previously in the "People & Groups" tab.)



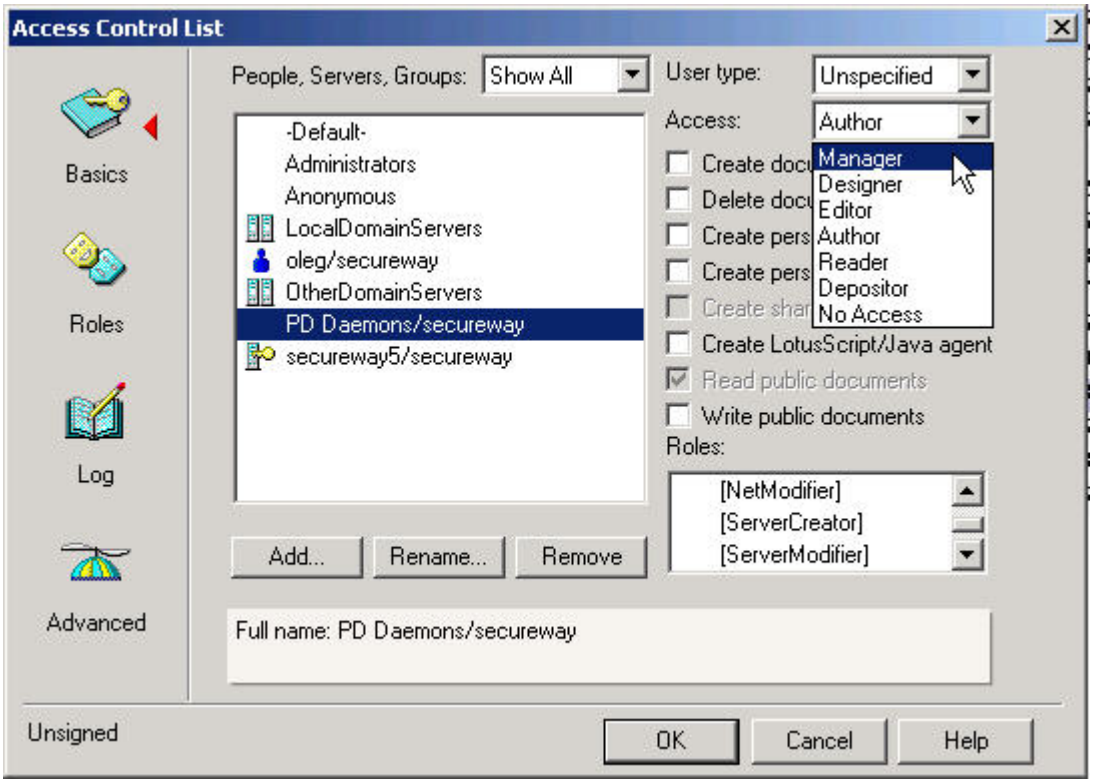
Highlight your domain's Address Book, and select “Manage ACLs” from Tools. In the next dialog click “Add” under the list of People, Servers, and Groups.



Then select the AM Privileged User from the **Domain** Address Book by clicking the small Person button.



Click on the "Add" button, then OK on the Names dialog, and then OK again on the small Add User dialog.



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 AM.

17 Appendix B -- WebSphere Installation

17.1 Prerequisites and Preparations

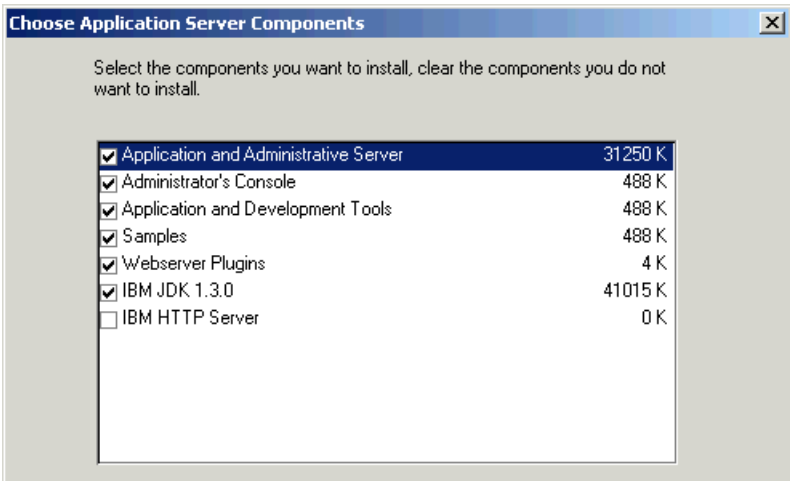
In order to successfully install WebSphere 4.02, verify that you already have the prerequisite software installed and configured. (In these labs we need latest GSKIT, currently 5.0.56 and DB2 7.2 FP4.) In case you have not updated the DB2 drivers to JDBC 2.0, do so following the instructions provided in section 16.3.2 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

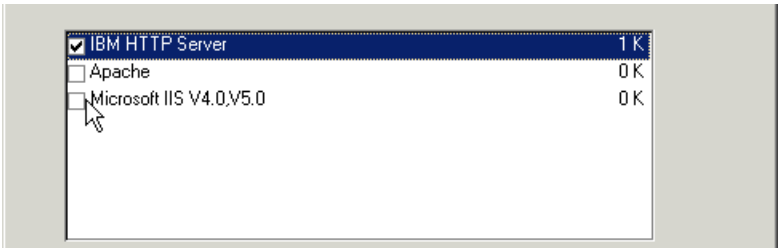
Start->Programs->IBM HTTP Server->Stop HTTP Server

17.2 Procedure

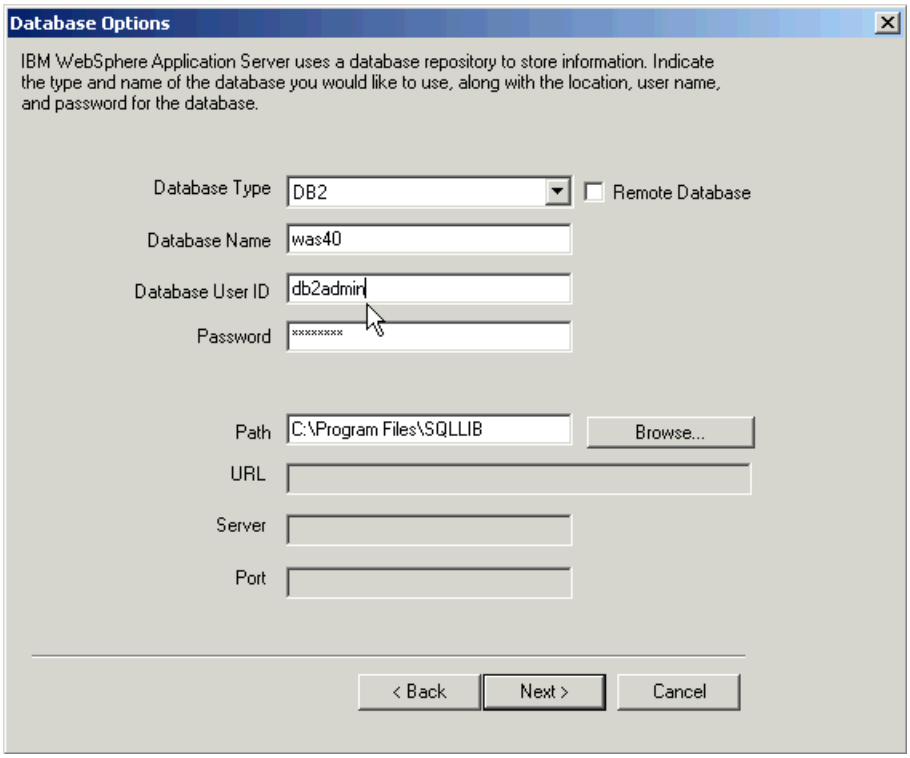
Use Windows Explorer to *D:\Lab Setup\WAS402WIN* and launch *setup.exe.* Accept English as installation language and continue until you are asked to choose the installation option. Select a *Custom Installation.* Click Next.



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.



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**.

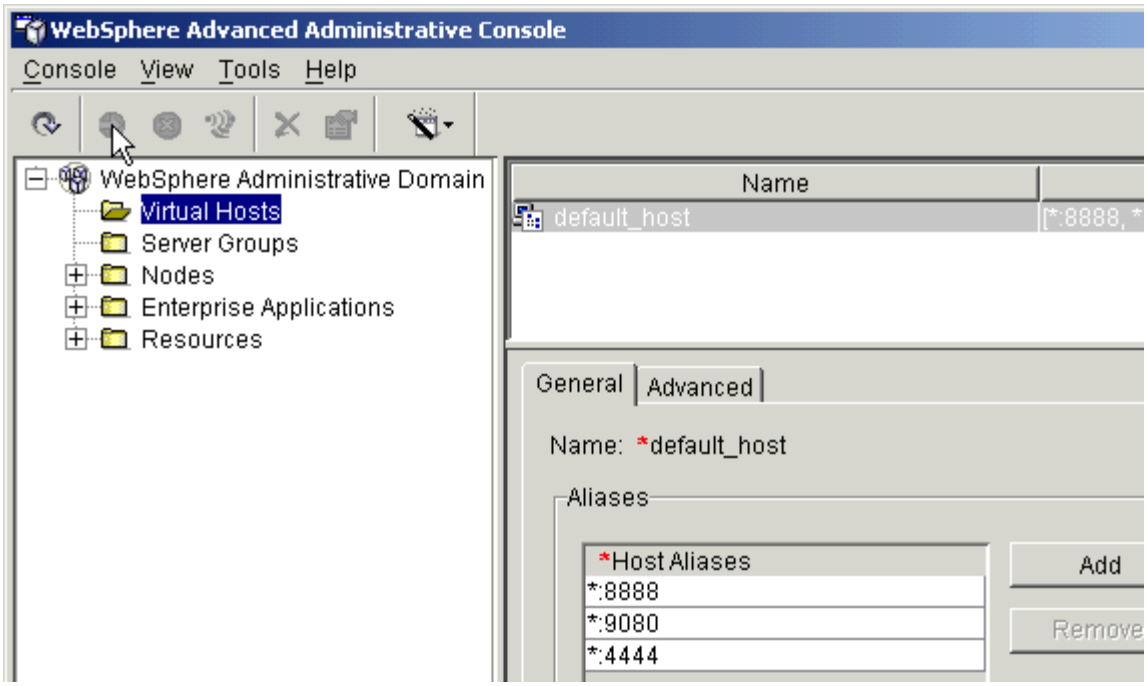
17.3 Configuring and Testing Your WebSphere Installation

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

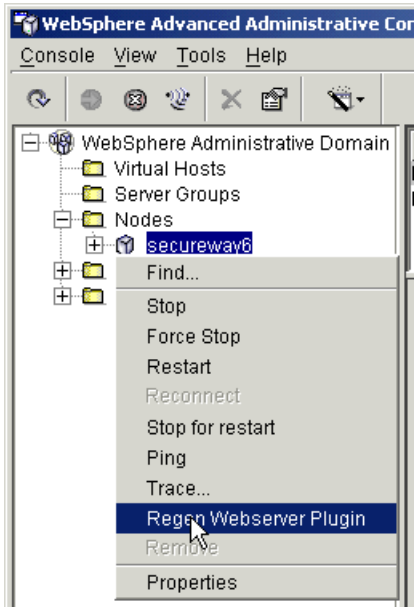
Depending on the power of your machine, the console can take some seconds before it appears, so be careful not to launch multiple consoles. Just be patient for a few moments!

On the Admin Console select expand WebSphere Administrative Domain. Click on Virtual Hosts.



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.

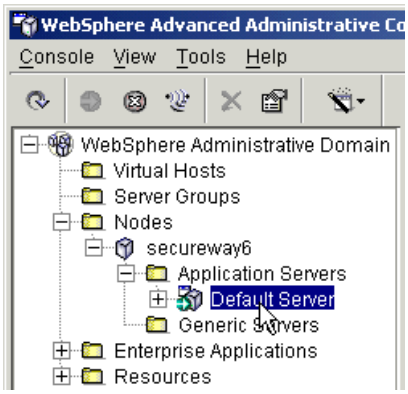
After this change you need to regenerate the Web server Plug-In.



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 *http://yourhost:8888/webapp/examples*. You should see a page with all the examples. If so, you have successfully installed WebSphere. Congratulations.

18 Appendix C -- Manual Installation of AM Web Portal Manager

18.1 Manually Installing AM 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 AM WPM manually, here are the instructions.

18.1.1 Considerations

This section describes how to install AMWPM into WAS manually using the WAS Admin Console application. You will still need to run the Configure... command in the Access Manager Configuration dialog because that adds the necessary stanzas to *httpd.conf*.

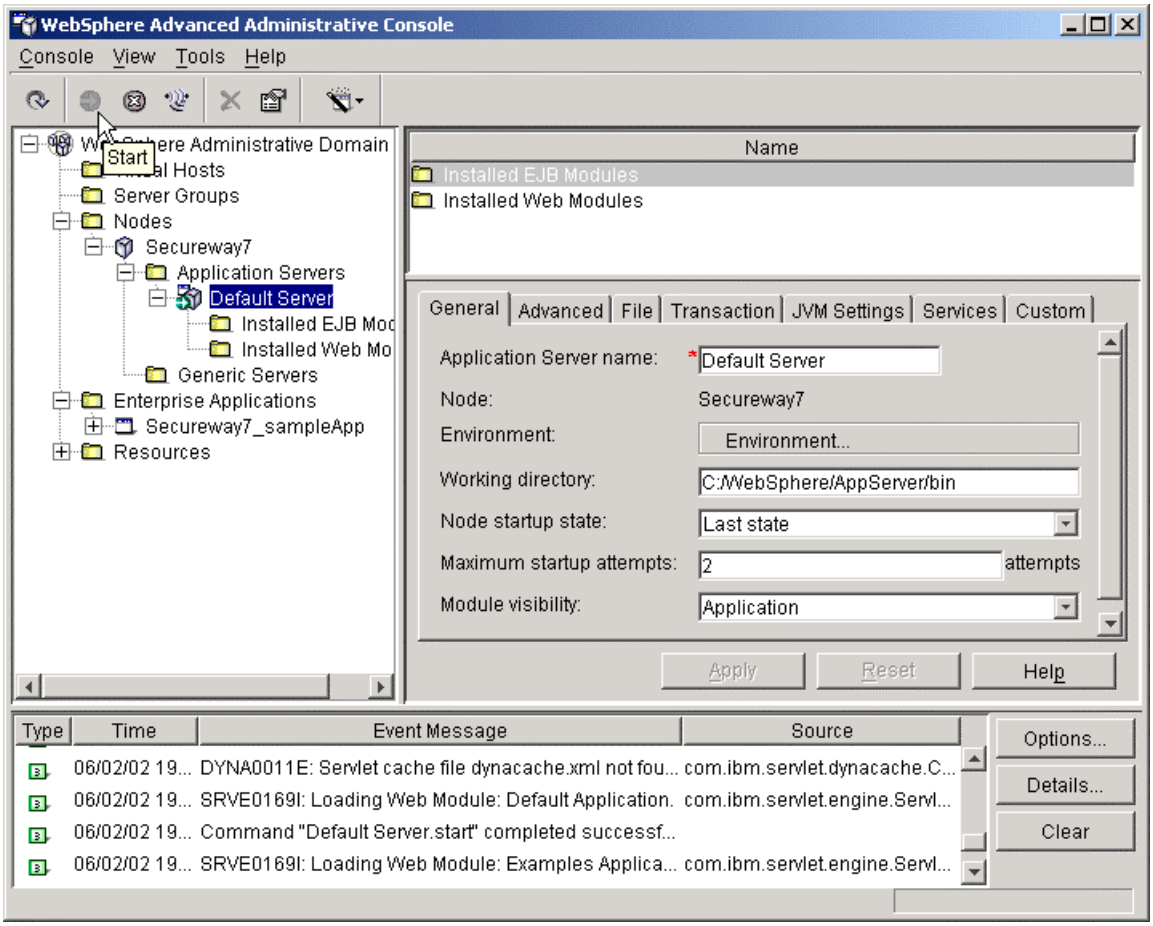
18.1.2 Procedure

Select Access Manager 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.

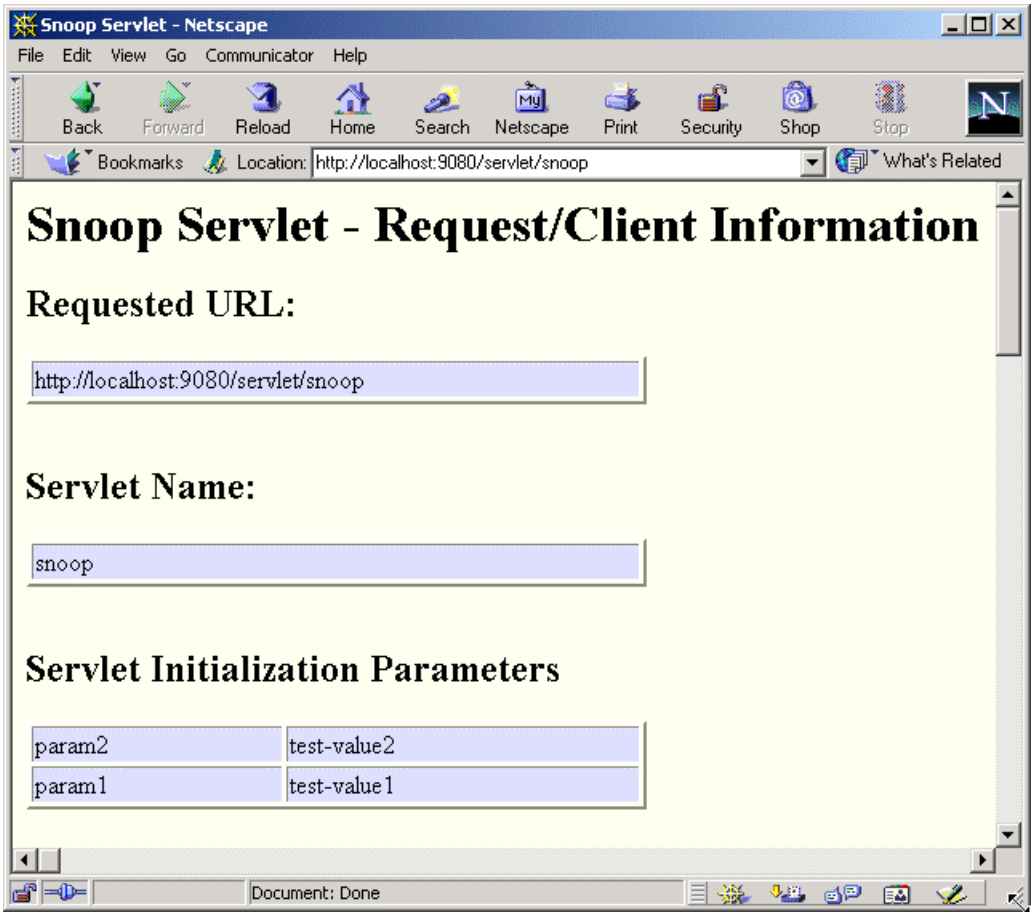
Start the WAS Admin Server by running Start->Programs->IBM WebSphere->Application Server V4.0 AE->Start Admin Server. (Note that you can also start the Admin Server from the Services window by running IBM WS AdminServer 4.0.) A DOS window will open and display messages as the Admin Server starts.

Next, start the WAS Admin Console by running Start->Programs->IBM WebSphere->Application Server V4.0 AE->Administrator's Console.

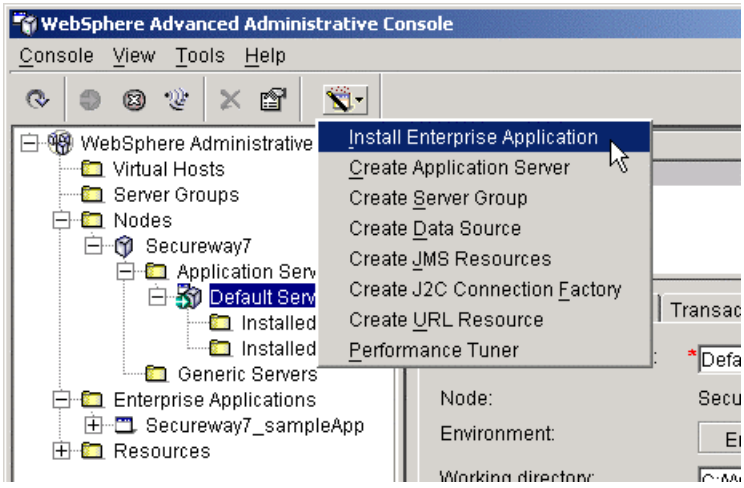


Expand WebSphere Administrative Domain, Nodes, <your host name>, and Application Servers. If there is a red X next to the Default Server instead of a green arrow, select the Default Server and click the green Start button as shown above. Click OK on the dialog that confirms starting the Default Server.

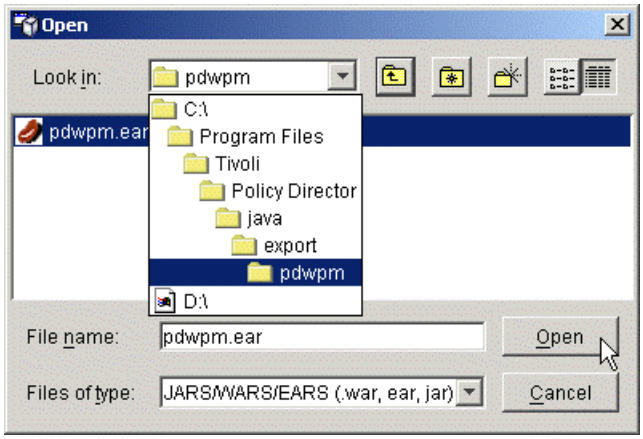
Test that WAS is running properly by opening Netscape (Netscape must be setup to not use a proxy for local addresses, etc.) or preferably IE and entering *http://localhost:9080/servlet/snoop*. You should see the output of the Snoop Servlet.



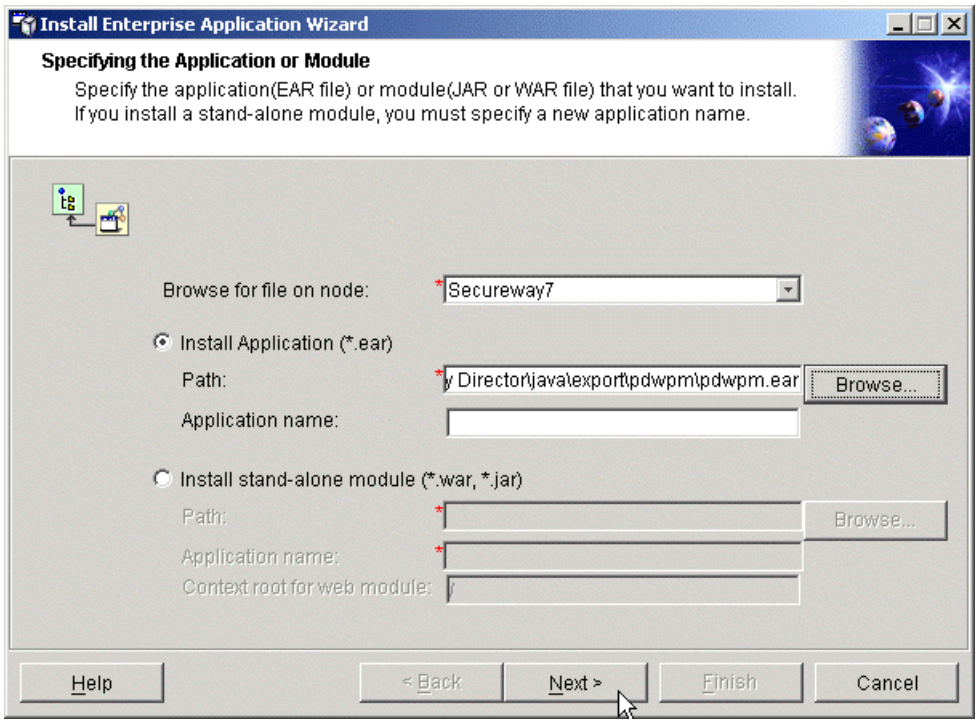
The port is 9080 because it is the port for WebSphere's own embedded Web server. Using the embedded Web server allows you to bypass the added complexity of a standalone Web server. Now to install Web Portal Manager....



Click on the toolbar button on the right and select Install Enterprise Application. Next click Browse for the Install Application (*.ear) Path:.



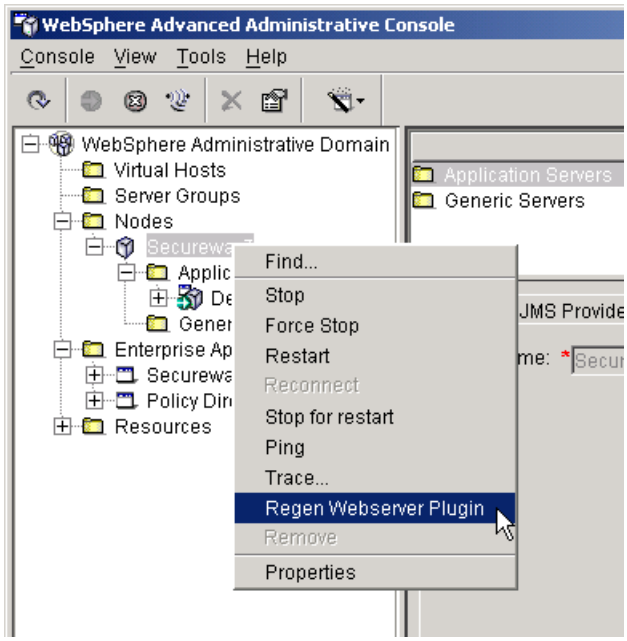
Navigate as shown, select *pdwpm.ear*, and click Open.



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 **Mapping Resource References to References** 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 **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.

19 Appendix D Banker 2001 Installation

19.1 Loading the Banker 2001 Application into Websphere

19.1.1 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.

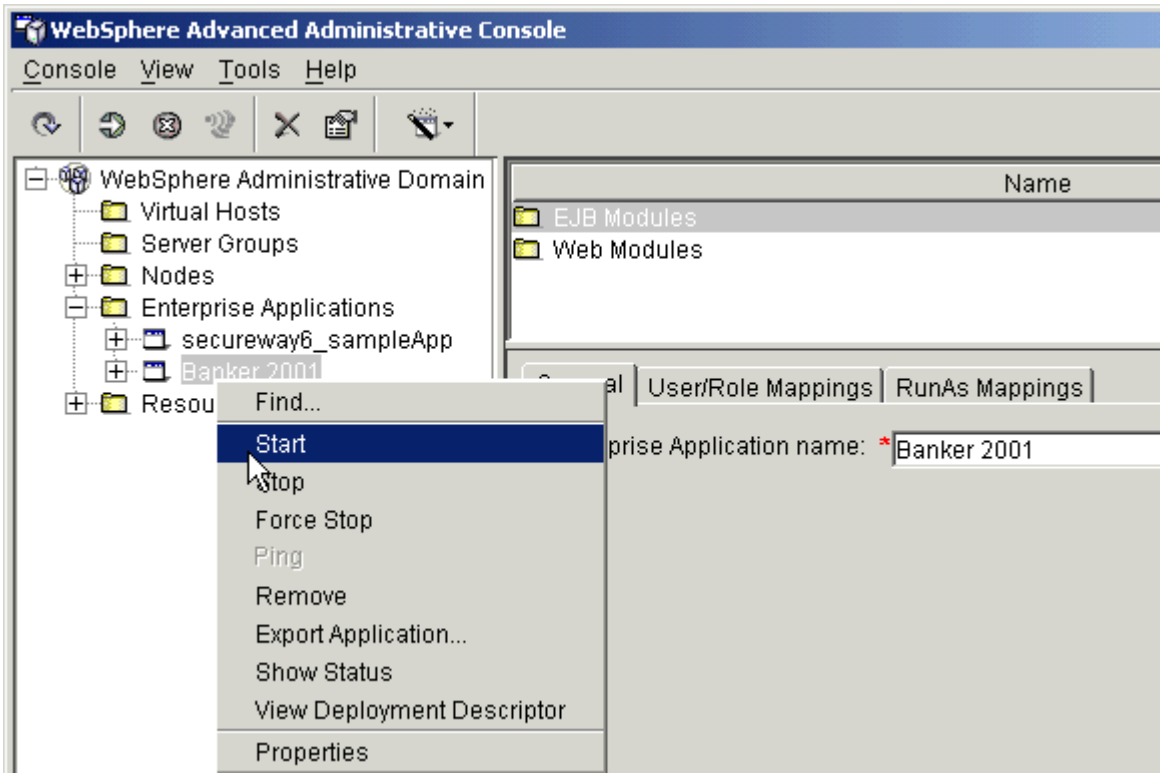
Remember to restart the IBM HTTP Server service.

19.1.2 Starting and Testing the Application

To start the application open the WAS Admin Console as follows:

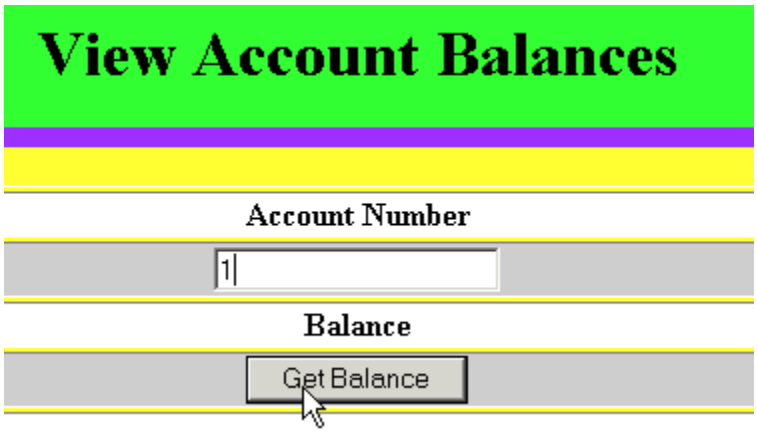
Start>Programs->IBM WebSphere->Application Server V4.0 AE->Administrator's Console

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 *http://yourhost:8888/Banker2001* and click on the View Balances link.



? Be a little bit curious and get the balance for account number 1. Can the account 1 owner buy a round for everyone?