EL03
Introducing OS/400 V5R2 LDAP Support on the IBM eserver iSeries Server

Lab Student Guide

Presented by:

Thomas Barlen

Consulting IT Specialist

January 2003

Contents

Lab environment conversion table v

Lab 1. Configuring OS/400 Directory Services 1
Task 1: Configuring a suffix using iSeries Navigator 1

Lab 2. Introducing the Directory Management Tool 5
Task 1: Installing IBM SecureWay Directory Management Tools 6
Task 2: Starting and authenticating using DMT 11
Task 3: Changing the Directory Management Tool settings 14
Task 4: Adding organizations and people to LDAP via DMT. 17
Task 5: Viewing object classes using DMT 21

Lab 3. Using LDIF to manage your directory. 25
Task 1: Adding a user entry using the LDIF file from Qshell 26
Task 2: Using the LDAP search commands in Qshell. 27
Task 3: Modifying an LDAP entry using Qshell. 28

Lab 4. Exploiting the HTTP Server for iSeries LDAP support 29
Task 1: Configuring the HTTP Server for LDAP user authentication. 30
Task 2: Configuring the HTTP Server for LDAP configuration support 40

Lab 5. Using an LDAP directory as an address book 57
Task 1: Configuring Outlook mail clients to use LDAP 57

Answers to the lab questions 65

Lab environment conversion table

Table 1 shows the conversion between the variables in the student handouts (*Variable* column) and the value that the student must use in this lab environment (*Lab environment* column).

Table 1. Lab environment conversion table

Value	Variable	Lab environment
User ID	**<UserID>**	LDAPxx
Team Number	**xx**	
Password	**<OS/400_password>**	
iSeries host name	**<ISERIES>**	
Fully qualified host name of the iSeries server	**<Fully_Qual_ISeries_Name>**	
LDAP directory administrator password	**<LDAP_Admin_Password>**	
Directory Service Suffix	**<o=companyXX>**	o=companyXX
Mapped iSeries root IFS directory drive letter	**<drive_letter>**	

Lab 1. Configuring OS/400 Directory Services

The purpose of this lab is to introduce the basic configuration of the OS/400 Directory Services. To publish information to a directory, certain configuration tasks need to be performed first. One of these tasks is to add a directory suffix.

In this lab, you add a directory suffix for your team to the existing directory server configuration. You can find further information on all topics covered in this hands-on lab guide in the redbook Implementation and Practical Use of LDAP on the IBM @server iSeries Server, SG24-6193.

Objectives

Upon completion of this lab, you will be able to:

- Understand Directory Services Properties
- Learn how to add a suffix

Lab environment

This lab environment includes:

- OS/400 V5R2 (5722-SS1)
- iSeries Navigator as part of iSeries Access for Windows (5722-XE1)

Time required

The time required to complete this lab project is 15 minutes.

Task summary

In this lab, you perform the following tasks:

1. View Directory Service Properties
2. Add Team Suffix

Task 1: Configuring a suffix using iSeries Navigator

Only one Directory Service can be configured and started per iSeries server. The instructor has pre-configured the Directory Service for you. But to give you some experience with the configuration, you will re-configure the Directory Service to add your team suffix. Once you complete this task, inform the instructor. Once all teams added their team suffix, the instructor will re-start the Directory service.

The followings steps explain how to add your team suffix:

__ 1. From your desktop, start iSeries Navigator.

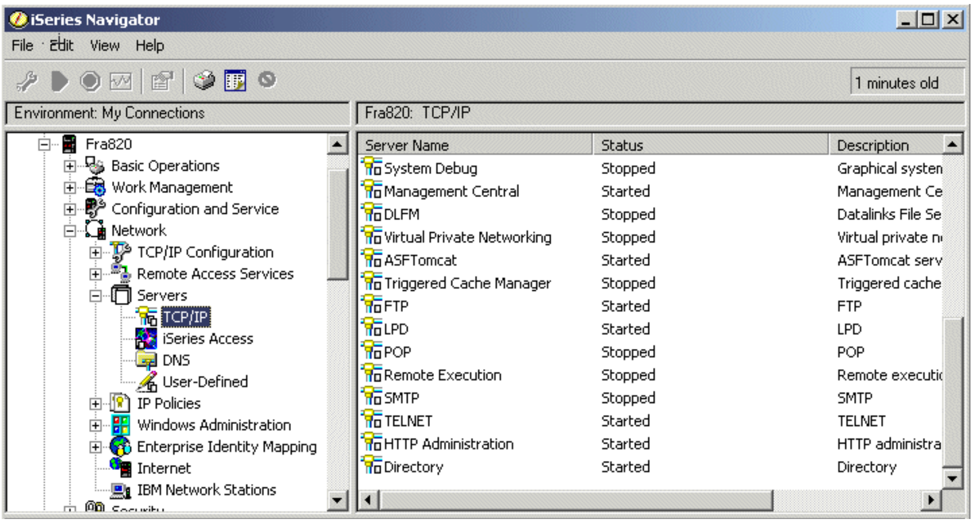
__ 2. Expand **<ISERIES>**.

__ 3. If required, sign on with your OS/400 user ID **<UserID>** and Password **<OS/400_password>**. Your team OS/400 user ID and password can be found on the Lab Sheet provided by the instructor.

__ 4. Expand **Network**.

__ 5. Expand **Servers**.

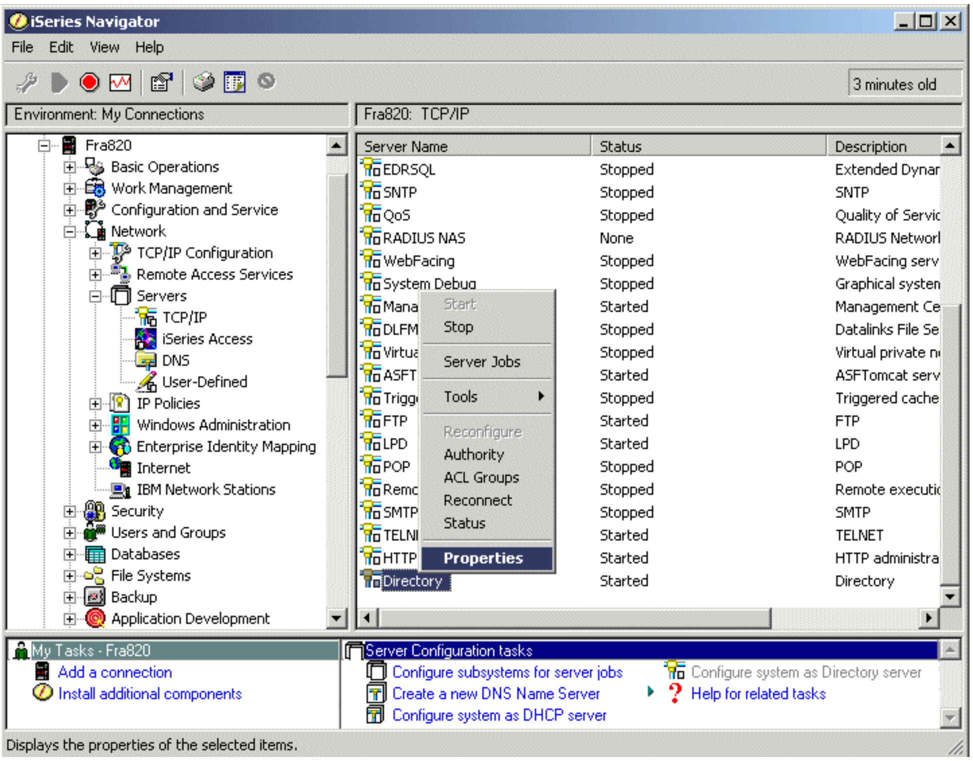
__ 6. Click **TCP/IP**. This shows all the TCP/IP servers that exist on the system as shown in Figure 1.



Server Name	Status	Description
System Debug	Stopped	Graphical systen
Management Central	Started	Management Ce
DLFM	Stopped	Datalinks File Se
Virtual Private Networking	Stopped	Virtual private n
ASFTomcat	Started	ASFTomcat serv
Triggered Cache Manager	Stopped	Triggered cache
FTP	Started	FTP
LPD	Started	LPD
POP	Stopped	POP
Remote Execution	Stopped	Remote executic
SMTP	Stopped	SMTP
TELNET	Started	TELNET
HTTP Administration	Started	HTTP administra
Directory	Started	Directory

Figure 1. All TCP/IP servers

__ 7. Right-click **Directory**, and then select **Properties** from the drop-down menu as shown in Figure 2.



Server Name	Status	Description
EDRSQL	Stopped	Extended Dynar
SNTP	Stopped	SNTP
QoS	Stopped	Quality of Servic
RADIUS NAS	None	RADIUS Networl
WebFacing	Stopped	WebFacing serv
System Debug	Stopped	Graphical systen
Mana	Started	Management Ce
DLFM	Stopped	Datalinks File Se
Virtua	Stopped	Virtual private n
ASFT	Started	ASFTomcat serv
Trigg	Stopped	Triggered cache
FTP	Started	FTP
LPD	Started	LPD
POP	Stopped	POP
Remc	Stopped	Remote executic
SMTP	Stopped	SMTP
TELNI	Started	TELNET
HTTP	Started	HTTP administra
Directory	Started	Directory

Displays the properties of the selected items.

Figure 2. Selecting the directory service properties

__ 8. On the Directory Properties window, select the **Database/Suffixes** tab.

__ 9. Click the Question Mark (**?**) in the top right-hand corner. Use the help to answer the following questions:

Question 1: What is stored in the Database Library?

____

____

____

Question 2: What are suffixes used for?

____

____

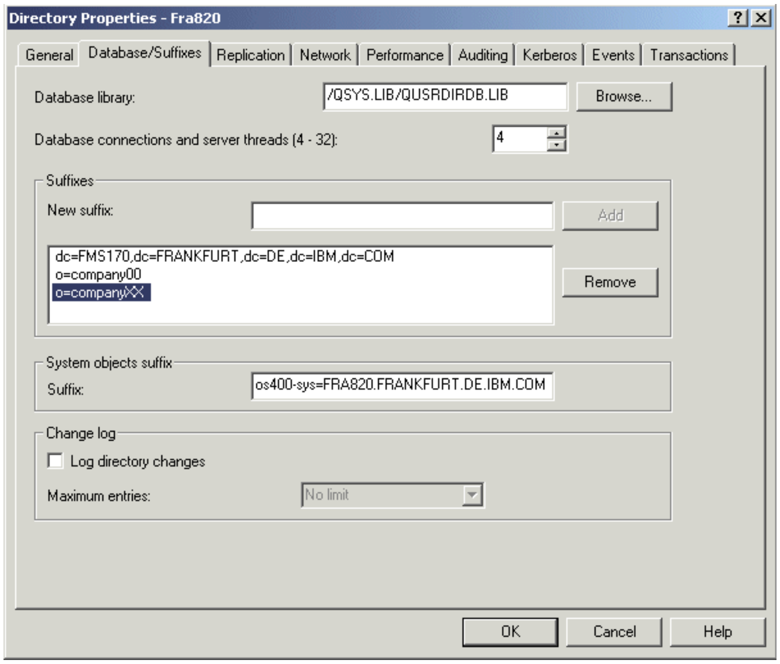
____

Question 3: What are the database connections used for?

____

____

__ 10.In the New Suffix: field, fill in your team's suffix, **<o=companyXX>**. Then click **Add**. Your team suffix can be found on the Lab Sheet provided by the instructor. Once you enter your suffix, your window should look similar to the example in Figure 3.



Directory Properties - Fra820

Database library: /QSYS.LIB/QUSRDIRDB.LIB

Database connections and server threads (4 - 32): 4

Suffixes

New suffix:

dc=FMS170,dc=FRANKFURT,dc=DE,dc=IBM,dc=COM
o=company00
o=companyXX

System objects suffix

Suffix: os400-sys=FRA820.FRANKFURT.DE.IBM.COM

Change log

□ Log directory changes

Maximum entries: No limit

Figure 3. Adding the team suffix

Without a suffix, you cannot create any entry in the directory. In this lab, you added a suffix `o=companyXX`. Adding the suffix does not automatically add the organization *companyXX* to the directory. Rather it allows us to add the organization under the *root* of the directory. You still need to create the organization object in the directory. Beginning with V5R1, the system will add the organization to the directory in case you publish system information and the suffix does not exist.

__ 11. Click **OK** and inform the instructor that you have completed this task.

If you receive a message asking if you want to restart the server, select **Restart the server later**. The instructor will restart Directory Services once all students complete this section.

__ 12. Close iSeries Navigator.

Lab 2. Introducing the Directory Management Tool

The purpose of this lab is to introduce the basic management of directory data using the IBM SecureWay Directory Management Tool (DMT). This tool provides you with a graphical user interface for managing LDAP directory content. The DMT is part of the Windows LDAP client that is included with Directory Services. The client is shipped in the integrated file system directory.

The version of the IBM SecureWay DMT or directory client SDK that is shipped with OS/400 does not include SSL support. You need to obtain the IBM SecureWay Directory Version 3.2.2 for Windows NT from the IBM LDAP Web site (`http://www.ibm.com/software/network/directory`) to use SSL. However, you do not use SSL in this lab.

The IBM SecureWay Directory Management Tool is a graphical tool that allows you to perform the following tasks:

- Search for a directory entry
- Add entries
- Edit entries
- Duplicate entries
- Delete entries
- Create, modify, and delete Access Control Lists (ACLs)
- Edit the Relative Distinguished Name (RDN) of an LDAP entry

Objectives

Upon completion of this lab, you will know how to:

- Install Directory Management Tool
- Start and authenticate with DMT
- Change DMT configuration to automatically start and authenticate with your LDAP server
- Add organizations and people to LDAP using DMT
- View object classes and attributes using DMT

Lab environment

This environment includes:

- OS/400 V5R2 (5722-SS1)
- iSeries Navigator

Time required

The time required to complete this lab project is 50 minutes.

Task summary

In this lab, you perform the following tasks:

1. Install Directory Management Tool.
2. Start and authenticate using DMT.
3. Change DMT configuration.
4. Add organizations and people to LDAP using DMT.
5. View Object classes and attributes using DMT.

Task 1: Installing IBM SecureWay Directory Management Tools

In this first task, you install the IBM SecureWay Directory Management Tools. This tool provides you with a graphical user interface for managing the LDAP directory content.

To install the DMT, onto your PC, follow these steps:

__ 1. From your desktop start iSeries Navigator.

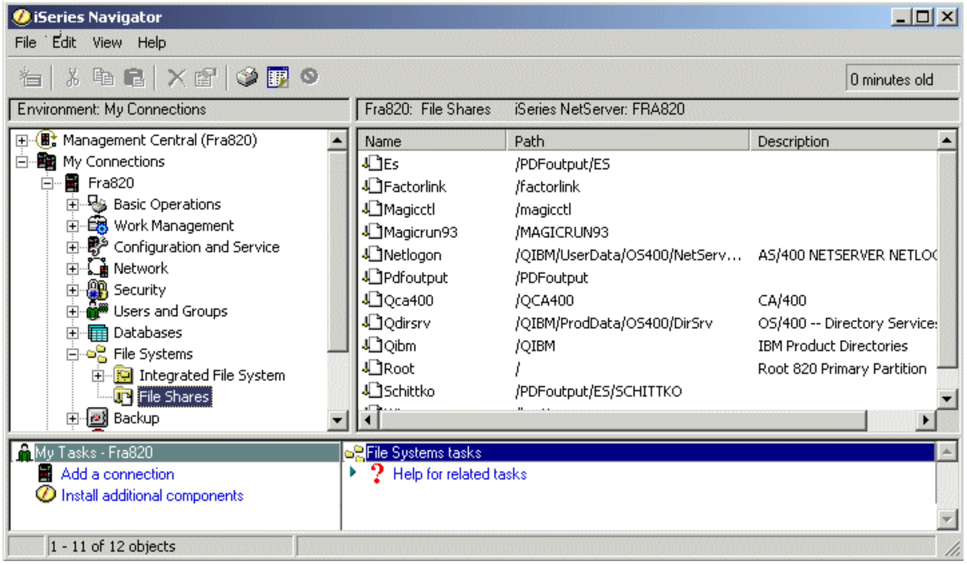
__ 2. Expand the iSeries server **<ISERIES>**.

__ 3. If required, sign on with your OS/400 user ID **<UserID>** and Password **<OS/400_password>**. Your team OS/400 user ID and password can be found on the Lab Sheet provided by the instructor.

__ 4. Expand **File Systems**.

__ 5. Click **File Shares**.

__ 6. In the right panel, double-click **Qdirsrv** as shown in Figure 4.

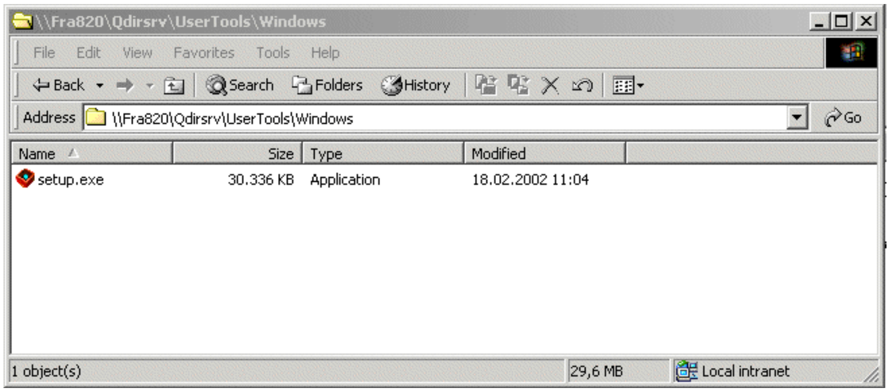


Fra820: File Shares iSeries NetServer: FRA820

Name	Path	Description
Es	/PDFoutput/ES	
Factorlink	/factorlink	
Magicctl	/magicctl	
Magicrun93	/MAGICRUN93	
Netlogon	/QIBM/UserData/OS400/NetServ...	AS/400 NETSERVER NETLO(
Pdfoutput	/PDFoutput	
Qca400	/QCA400	CA/400
Qdirsrv	/QIBM/ProdData/OS400/DirSrv	OS/400 -- Directory Service:
Qibm	/QIBM	IBM Product Directories
Root	/	Root 820 Primary Partition
Schittko	/PDFoutput/ES/SCHITTKO	

Figure 4. Installing DMT: Selecting Qdirsrv

__ 7. From the pop-up window, double-click the **UserTools** folder as shown in Figure 5, and then double-click the **Windows** folder.



\\Fra820\Qdirsrv\UserTools\Windows

Address \\Fra820\Qdirsrv\UserTools\Windows

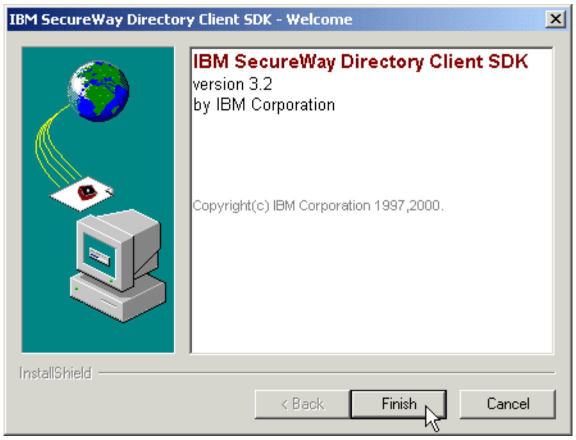
Name	Size	Type	Modified
setup.exe	30.336 KB	Application	18.02.2002 11:04

1 object(s) 29,6 MB Local intranet

Figure 5. Installing DMT: Selecting the Usertools folder

__ 8. Double-click **setup.exe** to start installing the DMT.

__ 9. The only options you have at this point are to click **Finish** or to cancel the installation as shown in Figure 6. Click **Finish**.



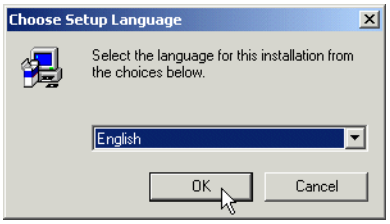
IBM SecureWay Directory Client SDK - Welcome

IBM SecureWay Directory Client SDK
version 3.2
by IBM Corporation

Copyright(c) IBM Corporation 1997,2000.

Figure 6. Installing DMT: IBM SecureWay Directory client - Welcome display

__ 10. On the Choose Setup Language display, select **English** as shown in Figure 7, and then click **OK**.



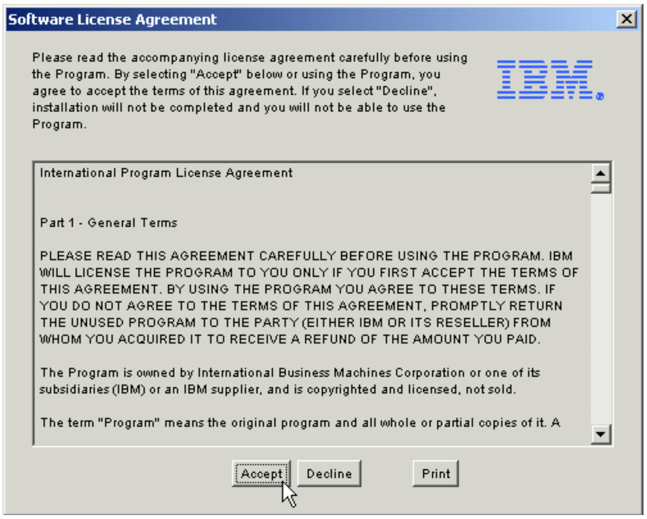
Choose Setup Language

Select the language for this installation from the choices below.

English

Figure 7. Installing DMT: Select the language

__ 11. On the Software Licence Agreement, click **Accept** as shown in Figure 8.



Please read the accompanying license agreement carefully before using the Program. By selecting "Accept" below or using the Program, you agree to accept the terms of this agreement. If you select "Decline", installation will not be completed and you will not be able to use the Program.

International Program License Agreement

Part 1 - General Terms

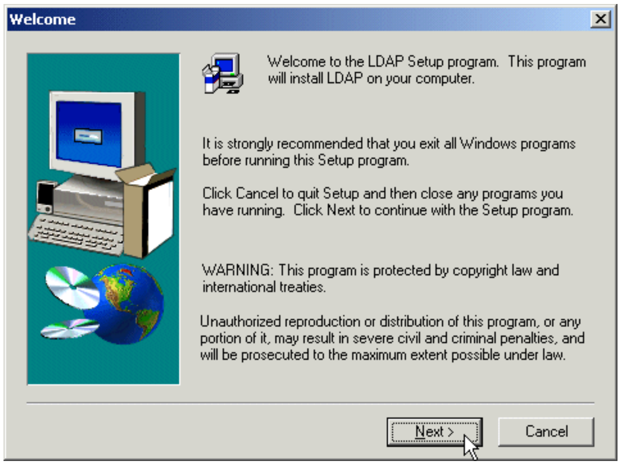
PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE PROGRAM. IBM WILL LICENSE THE PROGRAM TO YOU ONLY IF YOU FIRST ACCEPT THE TERMS OF THIS AGREEMENT. BY USING THE PROGRAM YOU AGREE TO THESE TERMS. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE UNUSED PROGRAM TO THE PARTY (EITHER IBM OR ITS RESELLER) FROM WHOM YOU ACQUIRED IT TO RECEIVE A REFUND OF THE AMOUNT YOU PAID.

The Program is owned by International Business Machines Corporation or one of its subsidiaries (IBM) or an IBM supplier, and is copyrighted and licensed, not sold.

The term "Program" means the original program and all whole or partial copies of it. A

Figure 8. Install DMT: License Agreement

__ 12.Ensure all other programs are closed. Then click **Next** as shown in Figure 9.



Welcome to the LDAP Setup program. This program will install LDAP on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

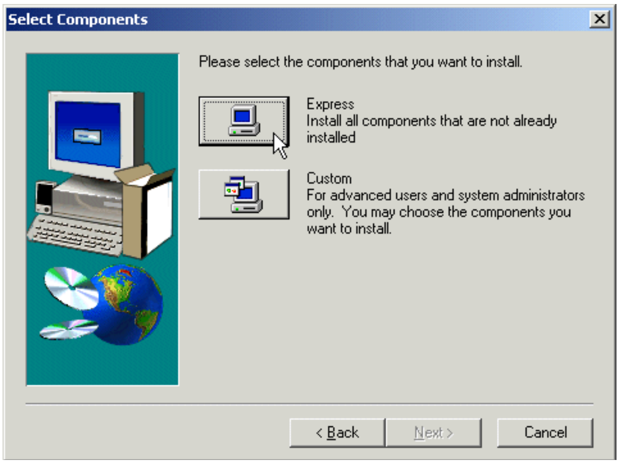
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Figure 9. Installing DMT

__ 13.On the Select Components display, click **Express** as shown in Figure 10.


Select Components

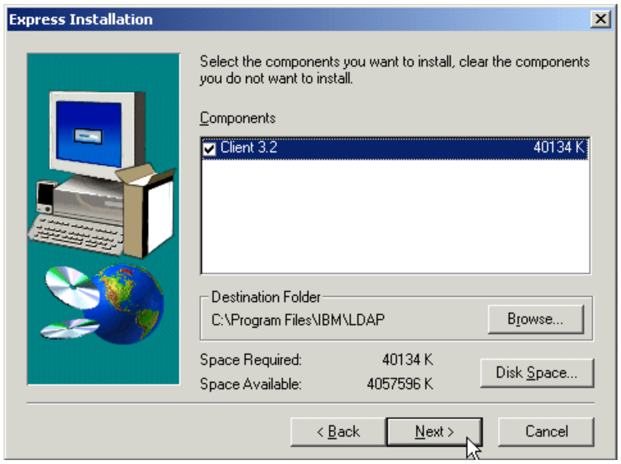
Please select the components that you want to install.

Express
Install all components that are not already installed

Custom
For advanced users and system administrators only. You may choose the components you want to install.

Figure 10. Installing DMT: Selecting the Express installation

__ 14.On the Express Installation window, accept the default values and click **Next** as shown in Figure 11.


Express Installation

Select the components you want to install, clear the components you do not want to install.

Components

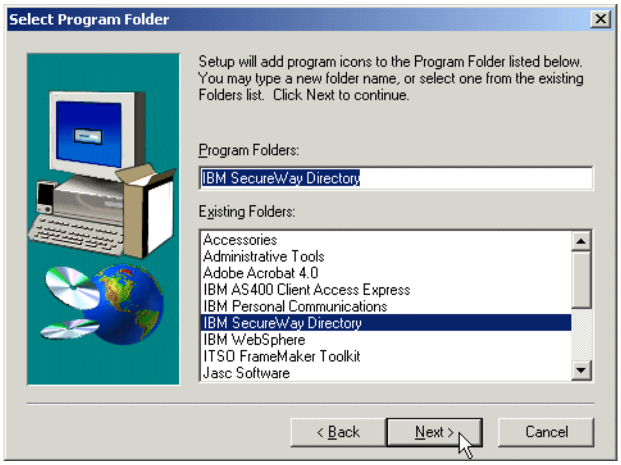
☑ Client 3.2 40134 K

Destination Folder
C:\Program Files\IBM\LDAP

Space Required: 40134 K
Space Available: 4057596 K

Figure 11. Installing DMT: Installation information

__ 15.On the Select Program Folder window, leave the default of **IBM SecureWay Directory**, and then click **Next** as shown in Figure 12.



Select Program Folder

Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing Folders list. Click Next to continue.

Program Folders:

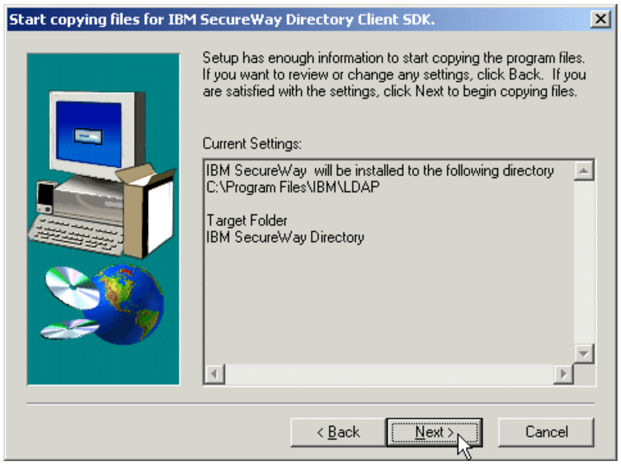
IBM SecureWay Directory

Existing Folders:

Accessories
Administrative Tools
Adobe Acrobat 4.0
IBM AS400 Client Access Express
IBM Personal Communications
IBM SecureWay Directory
IBM WebSphere
ITSO FrameMaker Toolkit
Jasc Software

Figure 12. Installing DMT: Select Program Folder

__ 16.Check the current settings information. It should look like the example in Figure 13. If the information is correct, click **Next** to start copying the files.



Start copying files for IBM SecureWay Directory Client SDK.

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

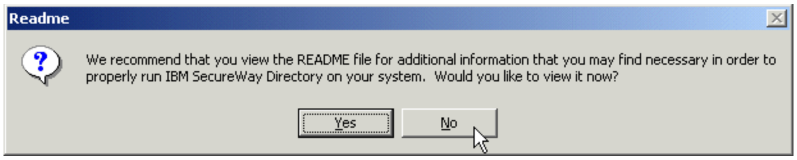
Current Settings:

IBM SecureWay will be installed to the following directory
C:\Program Files\IBM\LDAP

Target Folder
IBM SecureWay Directory

Figure 13. Installing DMT: Start copying files

__ 17.Click **No** to the Readme message shown in Figure 14.



Readme

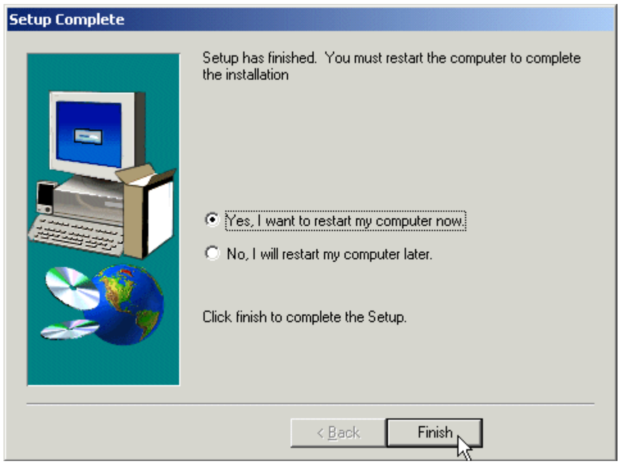
We recommend that you view the README file for additional information that you may find necessary in order to properly run IBM SecureWay Directory on your system. Would you like to view it now?

Figure 14. Installing DMT: Readme Message

A windows folder opens and displays the SecureWay Directory program icons.

__ 18.Close the C:\Documents and Settings\All Users\Start Menu\Programs\IBM SecureWay Directory window.

__ 19.Select **Yes, I want to restart my computer now** as shown in Figure 15. Then click **Finish**.


Setup Complete

Setup has finished. You must restart the computer to complete the installation

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Click finish to complete the Setup.

Figure 15. Installing DMT: Restarting the computer

You have now completed installing the Directory Management Tools. Continue to Task 2.

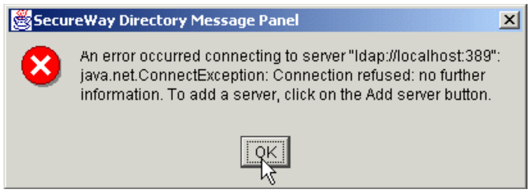
Task 2: Starting and authenticating using DMT

In this task, you start the Directory Management Tools and use the Administrator to authenticate with the LDAP server.

To start DMT, use the following steps:

__ 1. Click **Start-> Programs-> IBM SecureWay Directory-> Directory Management Tool**.

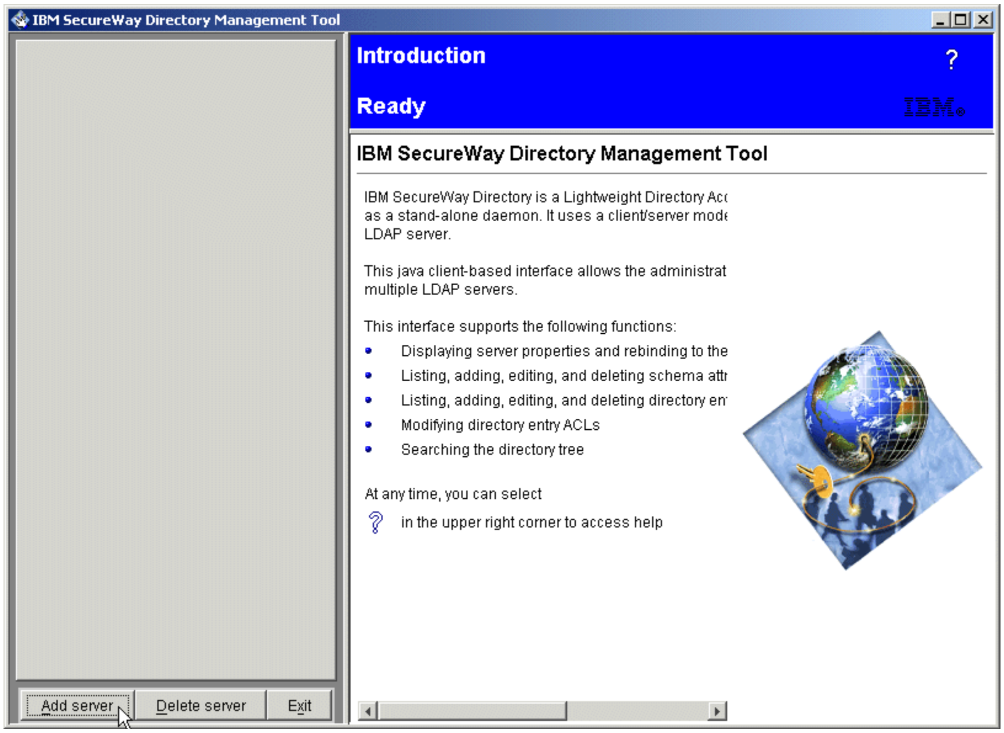
__ 2. An error message appears as shown in Figure 16. You receive this message because you do not have a local LDAP server configured on your PC. You will always receive this message because the localhost must be in the configuration file or DMT will not start. Click **OK**.


SecureWay Directory Message Panel

An error occurred connecting to server "ldap://localhost:389": java.net.ConnectException: Connection refused: no further information. To add a server, click on the Add server button.

Figure 16. SecureWay Directory Message Panel

__ 3. You are now in the Directory Management Tool. You now need to add your LDAP server. Click **Add server** as shown in Figure 17.



IBM SecureWay Directory Management Tool

IBM SecureWay Directory is a Lightweight Directory Acc as a stand-alone daemon. It uses a client/server mode LDAP server.

This java client-based interface allows the administrat multiple LDAP servers.

This interface supports the following functions:

- Displaying server properties and rebinding to the
- Listing, adding, editing, and deleting schema attr
- Listing, adding, editing, and deleting directory en
- Modifying directory entry ACLs
- Searching the directory tree

At any time, you can select

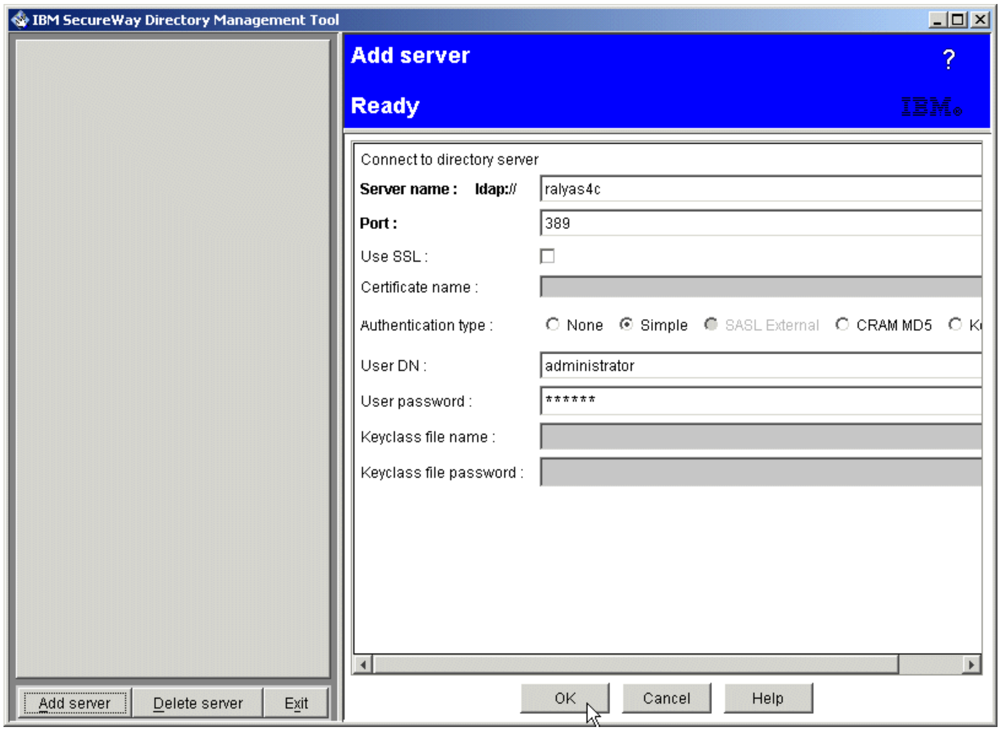
? in the upper right corner to access help

Figure 17. Clicking the Add server button

__ 4. In the Add Server display, fill in the fields as follows:

- **Server name: ldap://**: Enter the name of the iSeries server **<ISERIES>**. In our example, we used *ralyas4c*. Be sure to replace this with the value of the **<ISERIES>** variable.
- **Port:** Leave this default to `389`. This is the default port for LDAP.
- **Use SSL:** Leave this **blank** since we do not use SSL in this lab.
- **Certificate name:** This field is only used in conjunction with SSL. Leave **blank**.
- **Authentication type:** Leave this field as the default of **Simple**. This requires you to enter the administrator for this LDAP server. This is the simplest form of authentication using a DN and a password. In a controlled environment, this might be sufficient. However, when using the Simple authentication type, the user and password information flow in the clear over the network. You have to use SSL to protect the user and password information when connecting to the LDAP server.
- **User DN:** This is the Distinguished Name of the administrator. The administrator was set up when the LDAP server was first configured by your instructor. Enter `administrator`. Note that the DMT internally resolves the name `administrator` to the full DN `cn=administrator`.
- **User password:** The user password is the password of the LDAP administrator. Enter the password of **<LDAP_Admin_Password>**.
- **Key class file name:** Leave this default to **blank**. This field is required when configuring SSL.
- **Key class password:** Leave this default to **blank**. It is only used with SSL.

See Figure 18 for an example of the above settings.



Connect to directory server

Server name : **ldap://** ralyas4c

Port : 389

Use SSL : □

Certificate name :

Authentication type : ○ None ● Simple ○ SASL External ○ CRAM MD5 ○ K

User DN : administrator

User password : ******

Keyclass file name :

Keyclass file password :

Figure 18. Adding Server and authentication

Click **OK** to add the server. The DMT establishes a session to the LDAP server and retrieves the directory schema.

__ 5. Once the server is added, click **Browse tree** as shown in Figure 19.

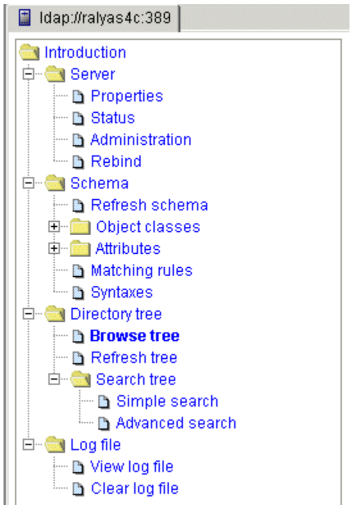
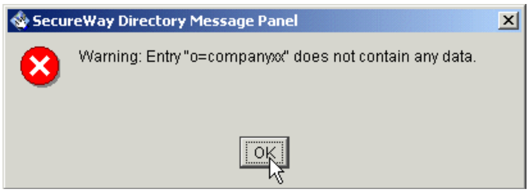


Figure 19. Browse Tree

A number of error messages are received, similar to the one shown in Figure 20. You receive these messages because you and the other teams have not added the suffixes to the directory yet. In Lab 1, you added the suffixes to the server configuration. This enables you to publish data under the suffix, but it does not automatically add the organization specified in the suffix to the directory repository. This is done later in the lab. In V5R1 and later, when publishing system or user information is enabled, the suffixes as specified in the directory properties and the publishing configuration are automatically added to the directory repository.

Click **OK** to all of these messages. In a later task, we show you how to add your suffix and data.



SecureWay Directory Message Panel

Warning: Entry "o=companyxx" does not contain any data.

Figure 20. Error message: Does not contain any data

__ 6. Click **Exit** to close DMT as shown in Figure 21.

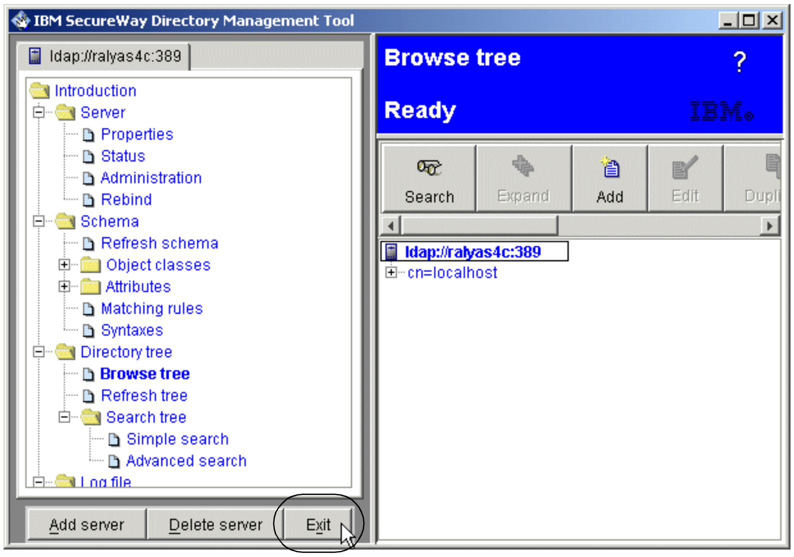


Figure 21. Exiting and closing DMT

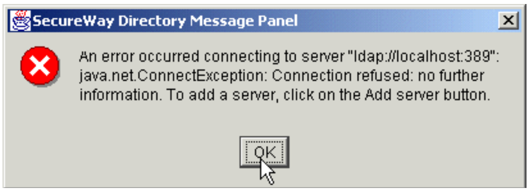
Task 3: Changing the Directory Management Tool settings

In this task, you change the DMT properties to add your server definition permanently. When you exit the DMT, it will not remember the servers you specified on the Add server page as done in Task 2:, “Starting and authenticating using DMT” on page 11. To permanently add the servers so that every time you start the DMT, you bind to the same servers, you need to edit the configuration file *dmt.conf* located in the LDAP client installation sub-directory LDAP/etc/.

To do this, perform the following steps:

__ 1. Click **Start-> Programs-> IBM SecureWay Directory-> Directory Management Tools**.

__ 2. As in step __ 2. on page 11, an error message is displayed as shown in Figure 22. This message is received because you do not have a local LDAP server configured on your PC. You will always receive this message because the localhost must be in the configuration file or DMT will not start. Click **OK**.



An error occurred connecting to server "ldap://localhost:389": java.net.ConnectException: Connection refused: no further information. To add a server, click on the Add server button.

Figure 22. SecureWay Directory Message Panel

__ 3. You are now in the Directory Management Tool. Again you have to add your server because the DMT does not remember the configuration you entered in the previous steps. Exit from DMT.

In the next steps we show you how to add your server permanently to the configuration of DMT:

__ 4. Open Windows Explorer and expand **c:\**.

__ 5. Expand **Program Files-> IBM-> LDAP**.

__ 6. Click **etc**, and then double-click **dmt.conf** as shown in Figure 23.

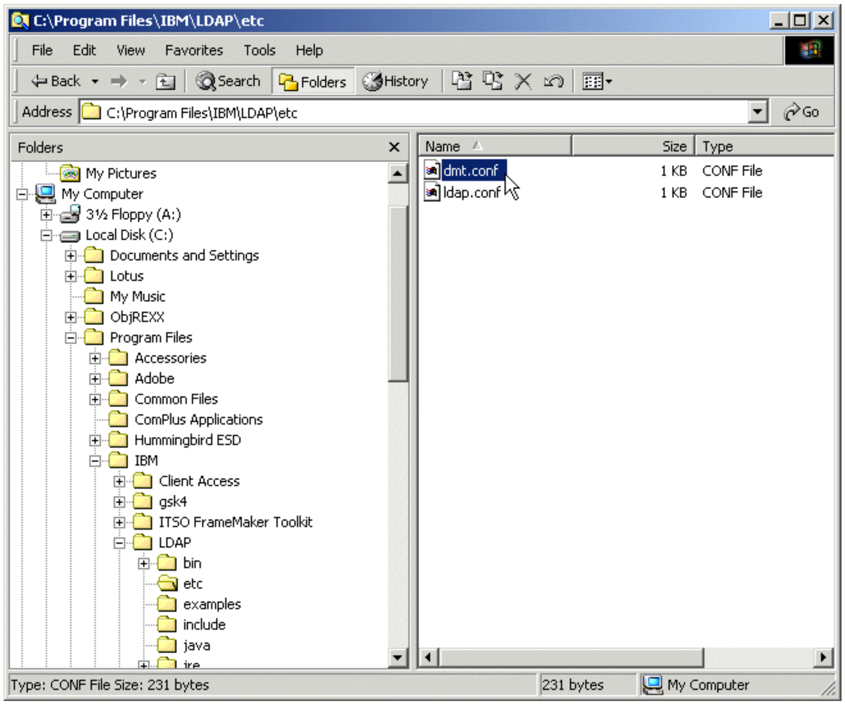
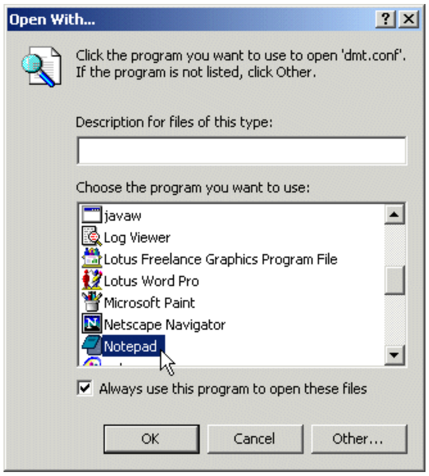


Figure 23. Opening the DMT configuration file

Since the *conf* extension is not known by Windows, the Open with... window opens.

__ 7. On the Open with... window, scroll down, select **Notepad**, and then click **OK** as shown in Figure 24.


Open With...
Description for files of this type:
Choose the program you want to use:
javaw
Log Viewer
Lotus Freelance Graphics Program File
Lotus Word Pro
Microsoft Paint
Netscape Navigator
Notepad
OK
Cancel
Other...

Click the program you want to use to open 'dmt.conf'.
If the program is not listed, click Other.

☑ Always use this program to open these files

Figure 24. Open with Notepad

__ 8. You can now edit the DMT configuration file to add your server. To do this, change the existing configuration so it looks like the following example:

```
#browser=
#toolbar=both
server1.url=ldap://localhost:389
server2.url=ldap://<ISERIES>
server2.security.bindDN=cn=administrator
server2.security.password=<LDAP_Admin_Password>
#server1.security.ssl.keyclass=
#server1.security.ssl.keyclass.password=
#server1.admin.url=http://webserver:80
```

__ 9. Once you make the above changes, save and close the configuration file.

Now when you start DMT, it connects to the non-SSL port 389 of the iSeries server you specified in the configuration **<ISERIES>**. It also binds to the server with a DN of cn=administrator and the administrator password of **<LDAP_Admin_Password>**.

To test that you successfully changed the configuration, complete the following steps:

__ 10. Click **Start-> Programs-> IBM SecureWay Directory-> Directory Management Tools**.

Problem determination

If you start DMT and you receive an error message about not being able to authenticate with your LDAP server (not localhost), try editing the DMT configuration file (dmt.conf) again. Ensure that there are no extra hidden characters or spaces at the end of each line.

Question 1: As in step __ 2. on page 14, an error message is still displayed as shown in Figure 22 on page 15. Why do you still receive this message even after you change the configuration?

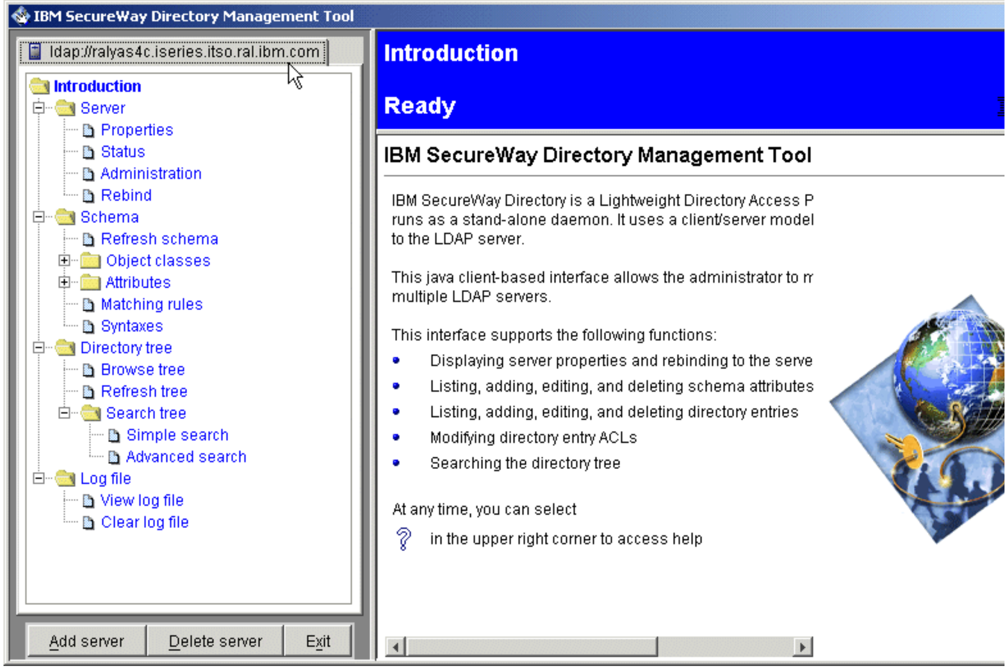
____

____

____

__ 11. Click **OK** to the error message.

You now have an automatic bind and administrator authentication to your LDAP server as shown in Figure 25. Stay in DMT and continue with the next task.



IBM SecureWay Directory Management Tool

IBM SecureWay Directory is a Lightweight Directory Access P
runs as a stand-alone daemon. It uses a client/server model
to the LDAP server.

This java client-based interface allows the administrator to m
multiple LDAP servers.

This interface supports the following functions:

- Displaying server properties and rebinding to the serve
- Listing, adding, editing, and deleting schema attributes
- Listing, adding, editing, and deleting directory entries
- Modifying directory entry ACLs
- Searching the directory tree

At any time, you can select

? in the upper right corner to access help

Figure 25. Automatic bind to LDAP server

Task 4: Adding organizations and people to LDAP via DMT

This task shows you how to add your organization. You already added the suffix to the directory in Lab 1. This is required before you add the organization. You must also add one person to your organization.

To do this, follow these steps:

__ 1. If DMT it is not all ready started, click **Start-> Programs-> IBM SecureWay Directory-> Directory Management Tools**.

__ 2. Click **OK** to the localhost error message.

__ 3. Click **Browse Tree** and **OK** to the error messages relating to no data in o=companyxx.

__ 4. In the right panel, click to select or highlight **ldap://<ISERIES>**.

__ 5. Click **Add** from the toolbar as shown in Figure 26.

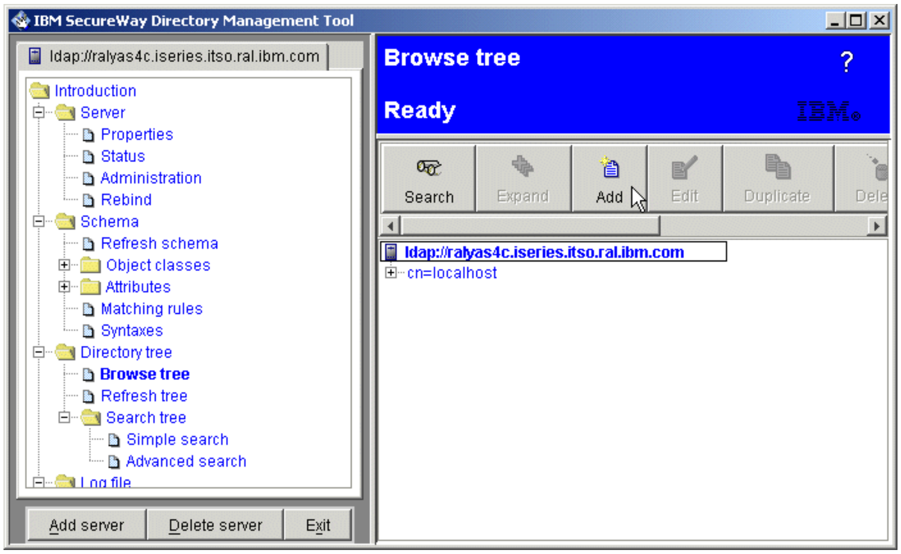
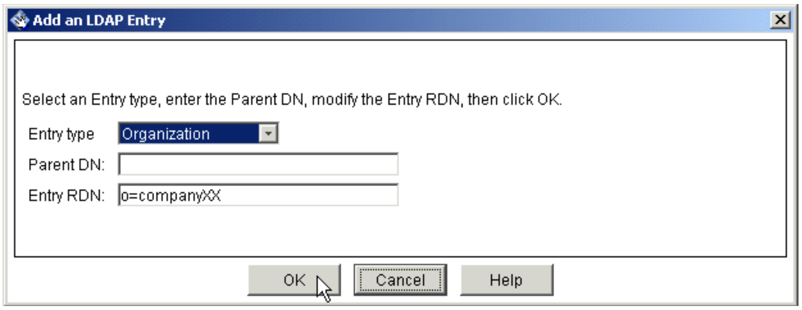


Figure 26. Select LDAP server

__ 6. On the Add an LDAP Entry window, enter the following fields:

- **Entry Type:** Use the drop-down list to select **Organization**
- **Parent DN:** Leave this field **blank**
- **Entry RDN:** Change this field to `o=companyXX` (Remember to replace the XX with your team number.)

See the example in Figure 27.



Select an Entry type, enter the Parent DN, modify the Entry RDN, then click OK.

Entry type: Organization

Parent DN:

Entry RDN: o=companyXX

Figure 27. Adding Organization with DMT

__ 7. Click **OK** to continue.

__ 8. Since the `o` attribute is the only required attribute for the organization (o) object class, no other values are required. Click **Add** to add this entry.

__ 9. You may still see warning messages for other o=companyxx organizations from teams that have not completed this step yet. Click **OK** to this message.

__ 10. You should now see **o=companyxx** in the tree. Click to select or highlight it as shown in Figure 28.

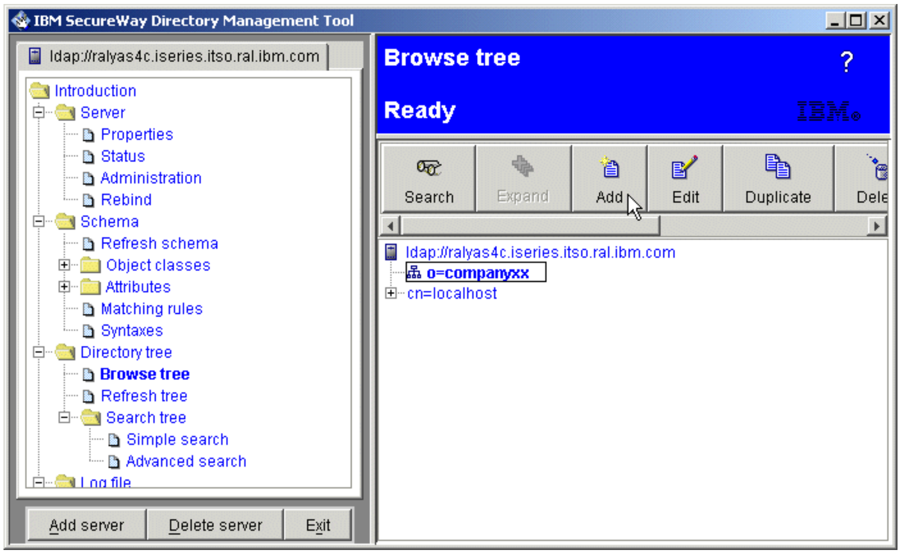


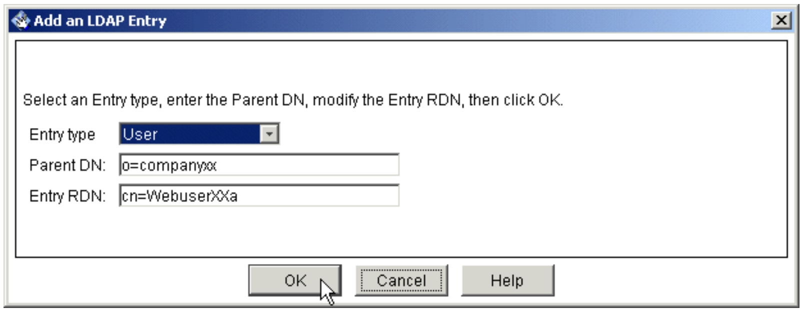
Figure 28. Adding a person with DMT

__ 11.Click **Add** to add a new entry under the selected organization.

__ 12.On the Add LDAP Entry window, fill in the following fields:

- **Entry Type:** Use the drop-down list to select **User**
- **Parent DN:** Leave this field default to `o=companyXX`
- **Entry RDN:** Change this field to `cn=WebuserXXa` (Remember to replace the XX with your team number.)

See the example in Figure 29.


Add an LDAP Entry

Select an Entry type, enter the Parent DN, modify the Entry RDN, then click OK.

Entry type: User

Parent DN: o=companyxx

Entry RDN: cn=WebuserXXa

Figure 29. Entering new user fields

__ 13.Click **OK** to continue.

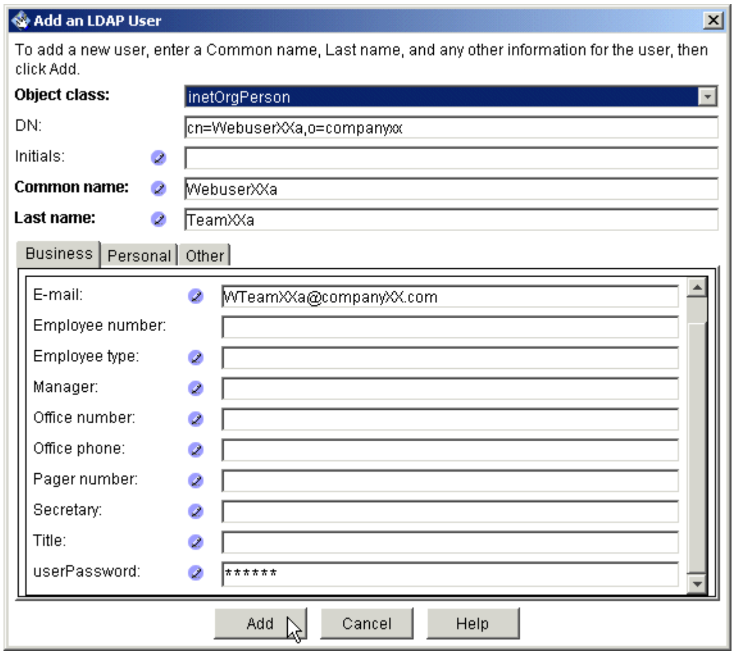
__ 14.Change the fields for the new user to:

- **DN:** Leave as the default of `cn=WebuserXXa,o=companyxx`
- **Initials:** Leave this default to **blank**
- **Common Name:** Leave this as the default of `WebuserXXa`
- **Last Name:** `TeamXXa`

__ 15.Select the **Business** tab and fill in the following fields:

- **E-mail:** `WTeamXXa@companyXX.com`
- **userPassword:** `teamxx`

The example for steps 13 and 14 are shown in Figure 30. (Remember to replace the XX with your team number.)



Add an LDAP User

To add a new user, enter a Common name, Last name, and any other information for the user, then click Add.

Object class: inetOrgPerson

DN: cn=WebuserXXa,o=companyxx

Initials:

Common name: WebuserXXa

Last name: TeamXXa

E-mail: WTeamXXa@companyXX.com

Employee number:

Employee type:

Manager:

Office number:

Office phone:

Pager number:

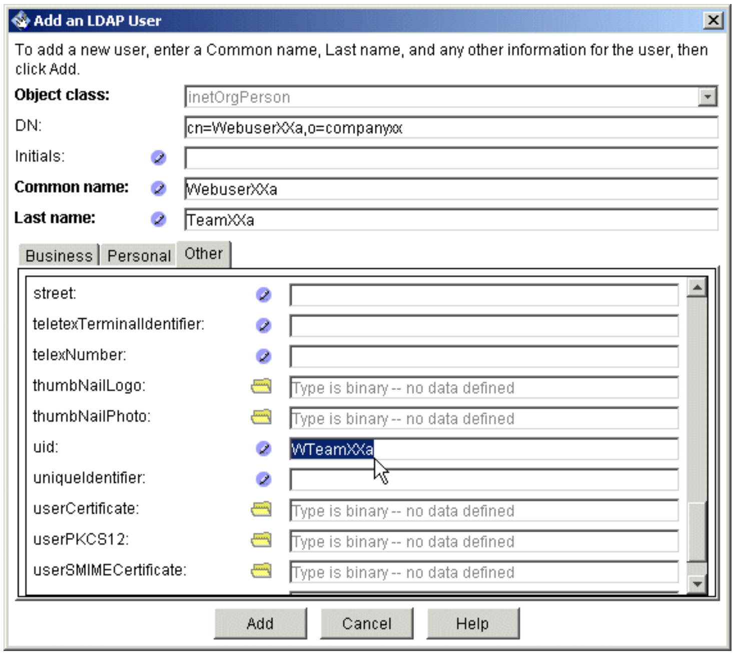
Secretary:

Title:

userPassword: ******

Figure 30. Adding a new user details

__ 16.Click the **Other** tab. Scroll down until you find **uid** and enter a user ID of `WTeamXXa` as shown in Figure 31. (Remember to replace the XX with your team number.)



Add an LDAP User

To add a new user, enter a Common name, Last name, and any other information for the user, then click Add.

Object class: inetOrgPerson

DN: cn=WebuserXXa,o=companyxx

Initials:

Common name: WebuserXXa

Last name: TeamXXa

street:

teletexTerminalIdentifier:

telexNumber:

thumbNailLogo: Type is binary -- no data defined

thumbNailPhoto: Type is binary -- no data defined

uid: WTeamXXa

uniqueIdentifier:

userCertificate: Type is binary -- no data defined

userPKCS12: Type is binary -- no data defined

userSMIMECertificate: Type is binary -- no data defined

Figure 31. Other tab: uid

__ 17.Click **Add** to add your new Person to the LDAP directory.

__ 18.Expand **o=companyXX** to view your new person as shown in Figure 32.

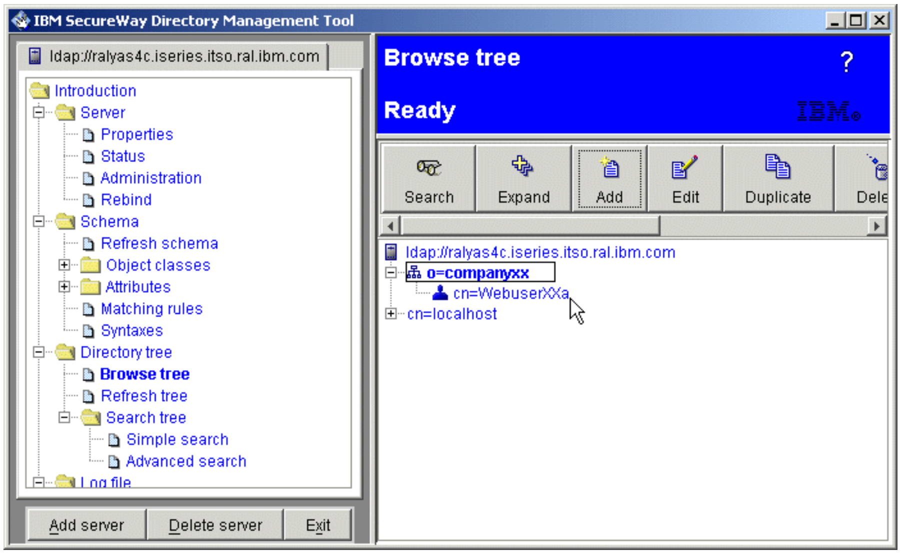


Figure 32. New person in organization

You have now added your team's company organization under the directory's root and added one person entry under your team's organization.

Task 5: Viewing object classes using DMT

In this task, you browse object classes to find required and optional attributes. The steps in this task allow you to browse the directory schema. This is especially useful when you try to add new directory entries and receive error messages about object class violations or syntax errors. Browsing the directory schema allows you to view the object class and attribute definitions. These definitions provide information about whether an attribute is required by an object class or optional. It also tells you the syntax rules for attribute values and much more.

To do this, follow these steps:

__ 1. Open DMT if it is not all ready open. Then expand **Schema** and then **Object classes**.

__ 2. In the navigation pane, click **View object classes** to display all object classes that are defined in the current directory schema as shown in Figure 33.

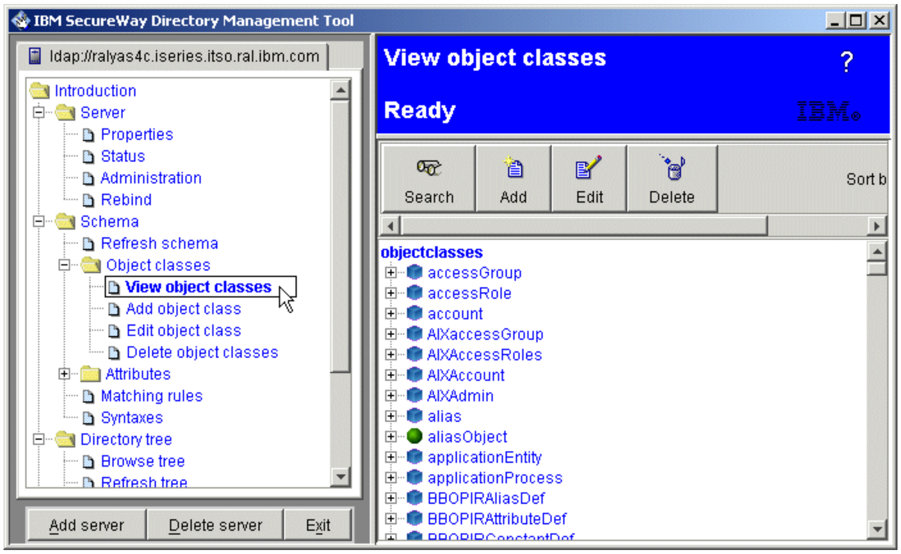
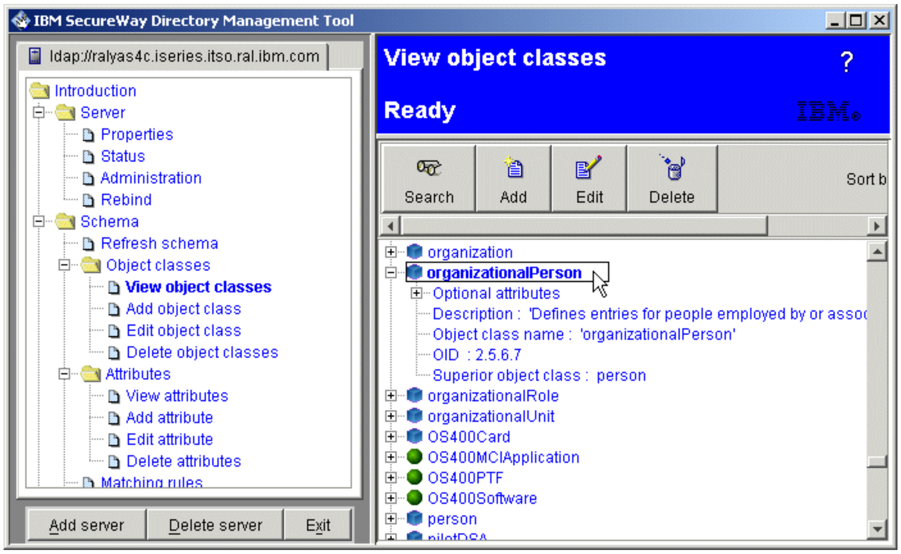


Figure 33. View object classes

__ 3. Scroll down through the list of Object classes to find and expand the **organizationalPerson** class as shown in Figure 34.



Description : 'Defines entries for people employed by or assoc

Object class name : 'organizationalPerson'

OID : 2.5.6.7

Superior object class : person

Figure 34. organizationalPerson Object Class

Question 1: What are three optional attributes of the organizationalPerson object class?

____

____

____

Question 2: What is the Superior object class for organizationalPerson?

____

____

Question 3: What are two required attributes of the Person object class?

____

____

Question 4: What is the Superior object class for Person?

____

Question 5: What is the required attribute of Top object class?

____

Question 6: If you wanted to add a person with an object class of organizationalPerson, what would the required attributes be?

____

____

____

____

__ 4. Exit the DMT.

In this lab, you learned how to add entries to a LDAP directory and browse the directory schema using the Directory Management Tool.

Lab 3. Using LDIF to manage your directory

This lab shows you how to add entries into the LDAP directory using LDAP Data Interchange Format (LDIF) files and Qshell command line utilities.

An LDAP database or repository can be distributed across multiple platforms by using LDIF files. On the iSeries server, iSeries Navigator is used as a GUI interface for exporting or importing LDIF files. LDIF files are stream files and should be transferred in ASCII format especially when using FTP.

The iSeries Directory Services includes five utilities that allow you to perform actions on the LDAP directory server from the Qshell command environment on OS/400. These utilities use the LDAP APIs. You can use these utilities from the Qshell command line or call them from your programs. You may also find them useful as programming examples. When you install the Windows LDAP client that is included with Directory Services, you also install code that is very similar to the source code for the shell utilities.

The utilities are as follows:

- **ldapmodify** and **ldapadd utilities**: Adds and modifies LDAP directory entries.
- **ldapdelete utility**: Removes entries from the LDAP directory.
- **ldapsearch utility**: Searches the LDAP directory for entries.
- **ldapmodrdn utility**: Allows you to change the Relative Distinguished Name (RDN).

This lab covers the ldapadd, ldapmodify, and ldapsearch utilities.

Objectives

Upon completion of this lab, you will be able to:

- Add a new LDAP entry using a LDIF file and the ldapadd utility
- Modify a LDAP entry using a LDIF file and the ldapmodify utility
- Search the LDAP Directory using the ldapsearch utility

Lab environment

This lab environment includes:

- OS/400 V5R2 (5722-SS1)
- iSeries Access for Windows (5722-XE1)
- Windows Notepad

Time required

The time required to complete this lab project is 20 minutes.

Task summary

In this lab, you perform the following tasks:

1. Add a new LDAP entry using a LDIF file and the ldapadd utility.
2. Search the LDAP Directory using the ldapsearch utility.
3. Modify an LDAP entry using a LDIF file and the ldapmodify utility.

Task 1: Adding a user entry using the LDIF file from Qshell

In this task, you add a new person to your LDAP directory using a file for input and the ldapmodify utility. You then modify the entry using the ldapmodify command.

To do this, follow these steps:

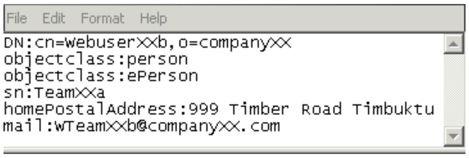
__ 1. From Start menu, select **Programs-> Accessories-> Notepad**.

__ 2. Enter the following information:

(Remember to replace the XX with your team number.)

```
DN:cn=WebuserXXb,o=companyXX
objectclass:person
objectclass:ePerson
sn:TeamXXb
homePostalAddress:999 Timber Road Timbuktu
mail:WTeamXXb@companyXX.com
```

Your entry should look similar to the example in Figure 35.



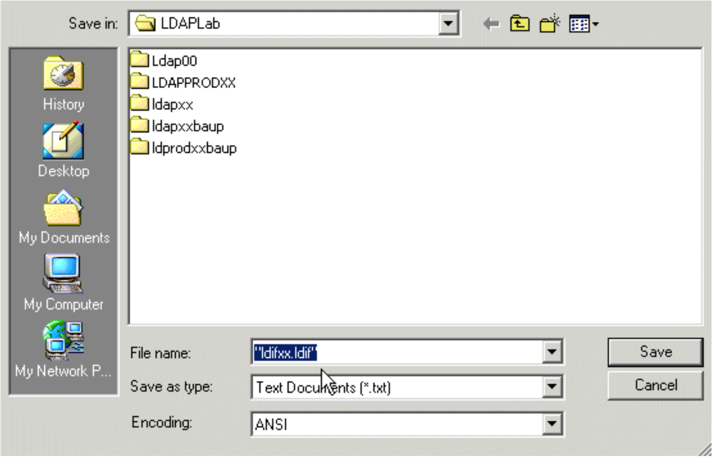
```
DN:cn=WebuserXXb,o=companyXX
objectclass:person
objectclass:ePerson
sn:TeamXXa
homePostalAddress:999 Timber Road Timbuktu
mail:WTeamXXb@companyXX.com
```

Figure 35. Information to be stored in the LDIF file

__ 3. Once you add the information to the file, click **File-> Save As...**.

__ 4. The root directory of the iSeries server is mapped to your PC as drive letter **<drive_letter>**. Open the **LDAPLab** directory on the iSeries server. When prompted for a password while accessing the mapped drive, enter **<OS/400_password>**.

__ 5. Enter the file name of `"ldifxx.ldif"` (make sure you use the quotations (") to surround the file name or the file will be named incorrectly), as shown in Figure 36. Then click **Save** (Remember to replace the XX with your team number.).



Save in: LDAPLab

File name: "ldifxx.ldif"

Save as type: Text Documents (*.txt)

Encoding: ANSI

Figure 36. Saving the LDIF file

__ 6. Start a 5250 session with the iSeries server **<ISERIES>** with your OS/400 user ID **<UserID>** and password **<OS/400_password>**. The 5250 emulation icon is on your desktop.

__ 7. Start Qshell by entering `strqsh` on the command line.

__ 8. In Qshell, type the following command on the command line:

```
ldapadd -D cn=administrator -w <LDAP_Admin_Password>
-f /ldaplab/ldifxx.ldif
```

This command string binds with DN cn=administrator (-D) and its password *my5ldap (-w)* to the LDAP server and adds the entry provided in the LDIF input file *(-f) /ldaplab/ldifxx.ldif*.

When you see the $ and no errors, the command has successfully completed and has added the contents of the LDIF file to your LDAP directory.

> **Note**
>
> The commands in Qshell are case sensitive. The above command needs to be entered exactly as shown. Use F12 to exit instead of F3. If you exit with F12, when you start qsh again, you can still use F9 to retrieve your previously entered commands. If you use F3, you cannot retrieve these commands.

Task 2: Using the LDAP search commands in Qshell

In this task, you search the LDAP directory using Qshell and the ldapsearch utility to find the user you added in the previous task.

To do this, perform the following steps:

__ 1. If it is not all ready started, start a 5250 session to the iSeries server **<ISERIES>**.

__ 2. If it is not all ready started, start Qshell by entering `strqsh` on the command line.

__ 3. In Qshell, type the following command:

```
ldapsearch -b o=companyxx cn=webuserxxb
```

Question 1: Why don't you see the homePostalAddess you entered in the LDIF file?

____

____

____

__ 4. Change the Qshell command so access is authorized by the administrator DN and password as follows:

```
ldapsearch -D cn=administrator -w <LDAP_Admin_Password>
 -b o=companyxx cn=webuserxxb
```

This command string binds with DN cn=administrator (-D) and its password *my5ldap (-w)* to the LDAP server and searches within the search base *o=company01 (-b)* for an entry that has a common name *cn=webuser01b*. You should now be able to see the entire entry including the homePostalAddress.

Task 3: Modifying an LDAP entry using Qshell

In this task, you modify an existing LDAP entry using Qshell and the ldapmodify utility. To do this, perform the following steps:

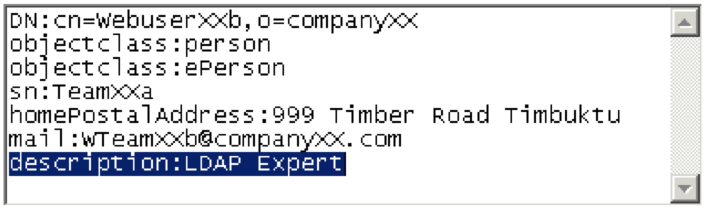
__ 1. From Start menu, select **Programs-> Accessories-> Notepad**.

__ 2. Open the LDIF file you created in __ 5. on page 26. **ldifxx.ldif**.

__ 3. Add a new attribute to the end of the file as follows:

```
description:LDAP Expert
```

See Figure 37.



```
DN:cn=WebuserXXb,o=companyXX
objectclass:person
objectclass:ePerson
sn:TeamXXa
homePostalAddress:999 Timber Road Timbuktu
mail:wTeamXXb@companyXX.com
description:LDAP Expert
```

Figure 37. Adding a new attribute to LDIF file

__ 4. Save the modified LDIF file.

__ 5. If it is not already started, start a 5250 session on the iSeries server **<ISERIES>**.

__ 6. If it is not already started, start Qshell by entering `strqsh` on the command line.

__ 7. In Qshell type the following on the command line:

```
ldapmodify -D cn=administrator -w <LDAP_Admin_Password>
 -f /ldaplab/ldifxx.ldif
```

You have now modified the user entry in the LDAP directory.

__ 8. To check that the entry was changed, use the ldapsearch command as follows:

```
ldapsearch -D cn=administrator -w <LDAP_Admin_Password>
 -b o=companyxx cn=webuserxxb
```

You should now be able to see the entire entry including the new attribute of description.

Lab 4. Exploiting the HTTP Server for iSeries LDAP support

As LDAP directory services are more widely used in various directory-enabled applications, the variety of information that an application stores in a directory increases. The advantage to use an LDAP server is that if data is stored once, it can be accessed by many different applications. An e-mail address stored by a calender application can also be used by a mail application. But not all data should be accessible by everyone. Some people can provide a user ID and a password to get access to the secured data. In this case, we use the LDAP server for authentication.

Assume you operate an HTTP Web server on your iSeries server. To improve performance and availability, you install a second Web server on another iSeries server that is used for backup and load balancing purposes. Since the new Web server serves the same information as the existing one, you want to maintain the server configuration only in a single place. This approach minimizes the administration effort and allows for easy expansion in case you want to add additional servers to the cluster. To achieve this goal, you can exploit the LDAP configuration support included with the HTTP Server for iSeries product.

You also want to offer special information to a group of customers over the Web. To ensure that only these customers have access to the information, the content is protected by the Web server and customers have to authenticate to gain access. That means that each customer is registered and needs a user ID and password to sign on. The operation of multiple Web servers raises another question: How can the company make sure that all Web servers have access to the user authentication data without replicating or copying the information to all Web servers? Well, the answer is pretty easy. You register all customers in the iSeries LDAP directory. Then, you modify the centrally stored Web server configuration to authenticate Internet users via user information stored in the LDAP directory.

This lab teaches you how to configure a HTTP server powered by Apache to access an LDAP server for user authentication and configuration support.

Objectives

Upon completion of this lab, you will be able to:

- Configure a HTTP server (powered by Apache) to use an LDAP server for user authentication.
- Describe how the configuration is performed and what prerequisites are necessary.
- Configure a HTTP server (powered by Apache) to load its server directives from a LDAP directory.

Lab environment

This lab environment includes:

- 5722-SS1 - OS/400 V5R2
- 5722-TC1 - TCP/IP Connectivity Utilities
- 5722-DG1 - HTTP Server for iSeries
- 5722-XE1 - iSeries Access for Windows

Time required

The time required to complete this lab project is 1.5 hours.

Task summary

In this lab, you perform the following task:

- Configure your HTTP server to use an LDAP server for authentication.
- Configure your HTTP server to use an LDAP server for configuration

Task 1: Configuring the HTTP Server for LDAP user authentication

This section guides you through the steps for setting up the IBM HTTP Server (powered by Apache) to perform authentication using user information stored in an LDAP directory. This section also includes the steps for setting up directory protection that only people with a valid user ID and a password have access to. The authentication information is stored in the LDAP server on **<ISERIES>**.

Your instructor has already set up a HTTP server instance LDAPXX (*XX* represents you team number you got from your instructor) for you. You work with this server during the lab. Be sure you select the right server. A directory has been created for which you setup the protection during this lab. The path for the directory you should protect is:

```
/LDAPLAB/LDAPXX/ProtectedInfo
```

In the first part, you create the container and alias for this directory and set up the protection for it.

Complete these steps to create the directory container:

__ 1. Start Internet Explorer and connect to the HTTP Server Administrator window on your iSeries server. Use the URL:

```
http://<ISERIES>:2001/HTTPAdmin
```

__ 2. Sign on with user ID and password:

OS/400 user ID: **<UserID>**
Password: **<OS/400_password>**

Note that the user profile needs to have `*ALLOBJ` and `*SECADMIN` special authorities.

The HTTP Server administration and configuration main window appears. The HTTP server administration and configuration utility requires that the HTTP *Admin instance is up and running. You can use iSeries Navigator (TCP/IP Servers) or the following command to start the *Admin instance:

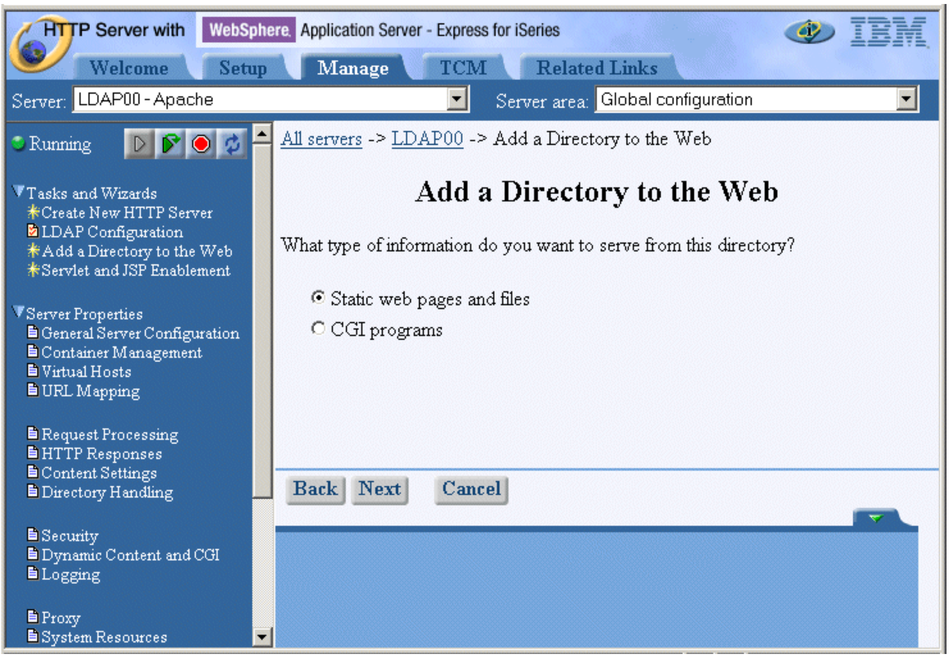
```
STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
```

__ 3. Select the **Manage** tab.

__ 4. Select your HTTP server **LDAPXX - Apache** from the pull-down list of the server field.

__ 5. In the left pane under Tasks and Wizards, click **Add a Directory to the Web**. This option starts the wizard to create the container and alias directives for the new directory you will serve.

__ 6. On the wizard welcome page, click **Next** to continue.



Server: LDAP00 - Apache

Server area: Global configuration

All servers -> LDAP00 -> Add a Directory to the Web

Add a Directory to the Web

What type of information do you want to serve from this directory?

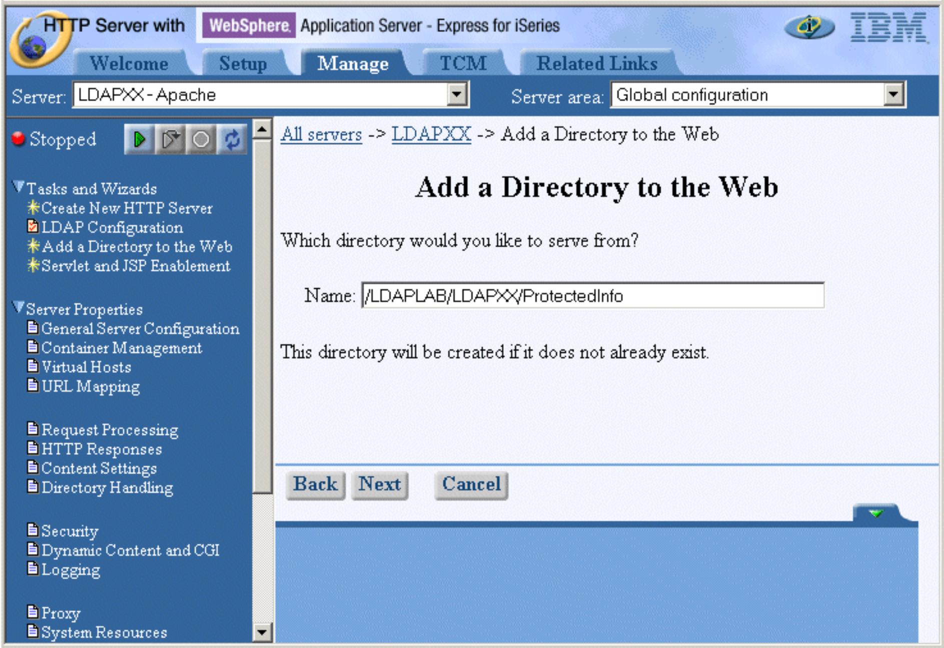
● Static web pages and files

○ CGI programs

Figure 38. Add a Directory to the Web wizard

Select **Static web pages and files.**

__ 7. Click **Next** to continue.



Server: LDAPXX - Apache

Server area: Global configuration

All servers -> LDAPXX -> Add a Directory to the Web

Add a Directory to the Web

Which directory would you like to serve from?

Name: /LDAPLAB/LDAPXX/ProtectedInfo

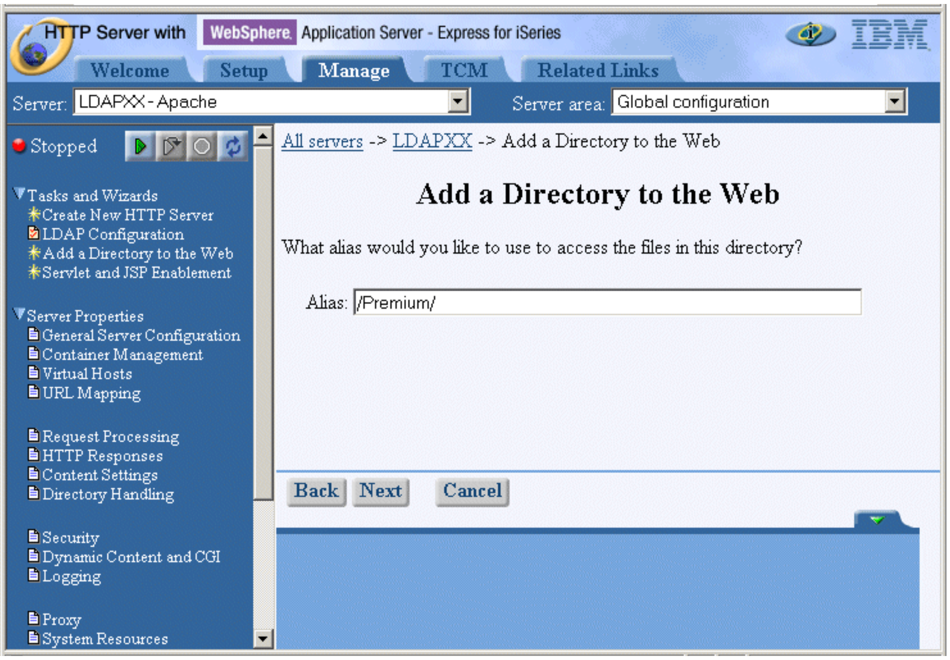
This directory will be created if it does not already exist.

Figure 39. Add a Directory to the Web wizard

Enter the path where the directory you want to protect is defined. Enter the path in the Name field.

Name: `/LDAPLAB/LDAPXX/ProtectedInfo`

__ 8. Click **Next**.



Add a Directory to the Web

What alias would you like to use to access the files in this directory?

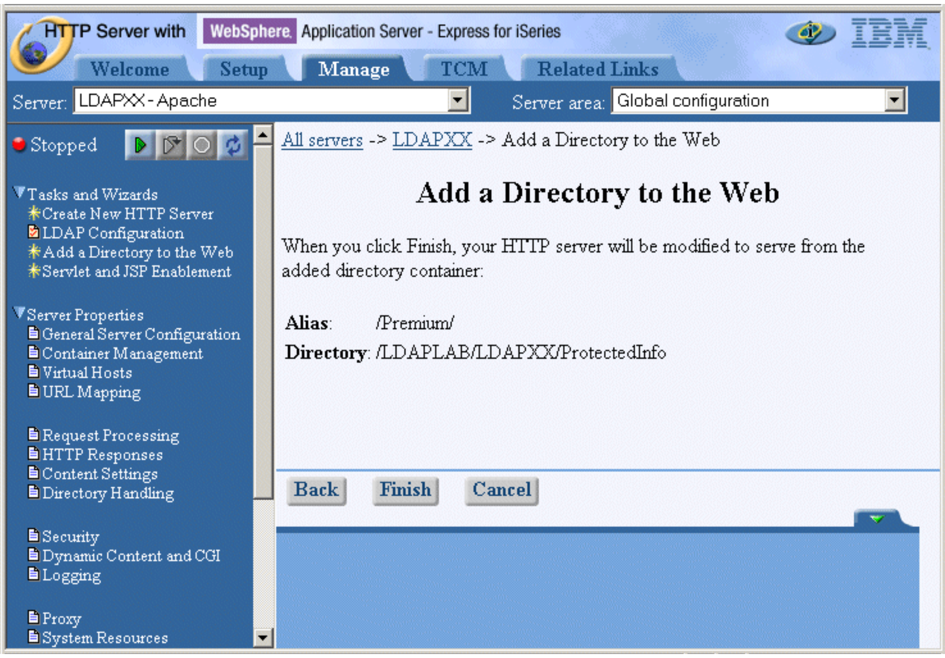
Alias: /Premium/

Figure 40. Add a Directory to the Web wizard

The wizard also requires you to enter an alias name for your directory. Enter your alias name in the Alias field.

Alias: `/Premium/`

__ 9. Click **Next**.



Add a Directory to the Web

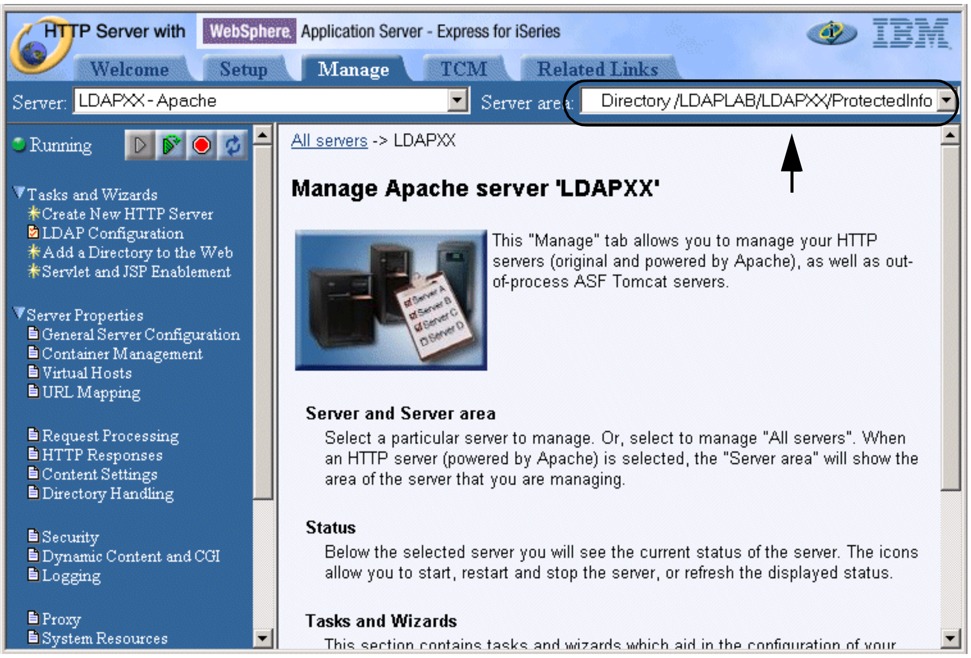
When you click Finish, your HTTP server will be modified to serve from the added directory container:

Alias: /Premium/
Directory: /LDAPLAB/LDAPXX/ProtectedInfo

Figure 41. Add a Directory to the Web wizard - Summary window

__ 10. On the page shown in Figure 41, check to ensure the fields you enter are correct. Click **Finish** to end the wizard and let create your directory.

__ 11. Select **Directory /LDAPLAB/LDAPXX/ProtectedInfo** from the server area list drop-down list. This step changes the current context you are working in.



Server: LDAPXX - Apache

Server area: Directory /LDAPLAB/LDAPXX/ProtectedInfo

All servers -> LDAPXX

Manage Apache server 'LDAPXX'

This "Manage" tab allows you to manage your HTTP servers (original and powered by Apache), as well as out-of-process ASF Tomcat servers.

Server and Server area

Select a particular server to manage. Or, select to manage "All servers". When an HTTP server (powered by Apache) is selected, the "Server area" will show the area of the server that you are managing.

Status

Below the selected server you will see the current status of the server. The icons allow you to start, restart and stop the server, or refresh the displayed status.

Tasks and Wizards

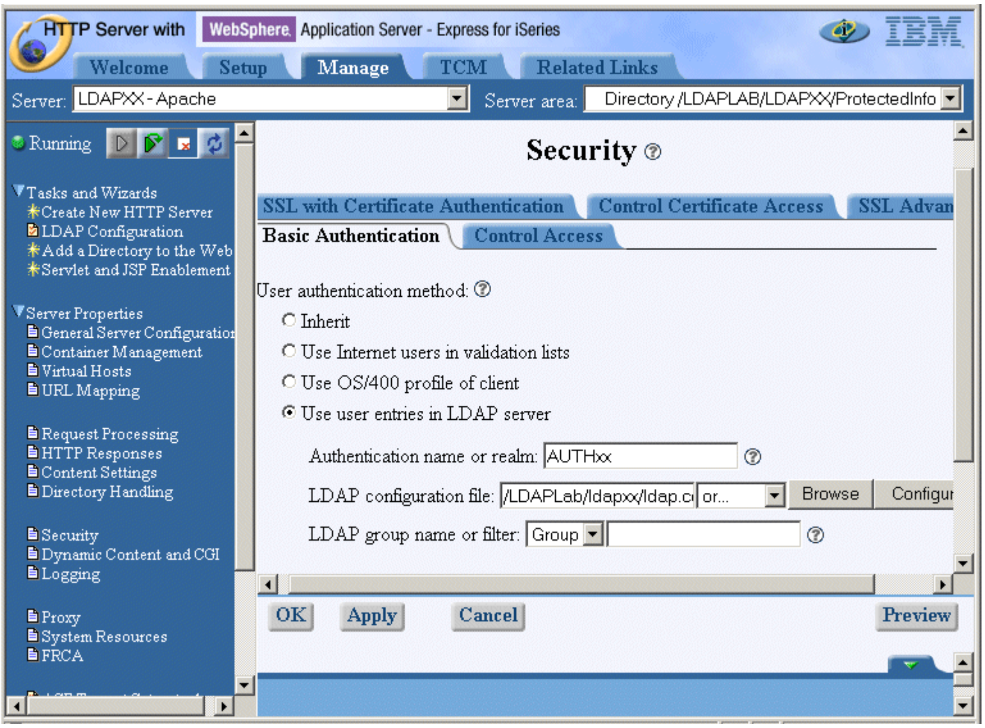
This section contains tasks and wizards which aid in the configuration of your

Figure 42. HTTP server configuration - Manage tab

In the next steps you will protect the new directory so that only authenticated users can view the content.

__ 12. In the Server Properties section, click **Security**. The Security page appears on the right pane of the window.

__ 13. Click the **Basic authentication** tab.



Server: LDAPXX - Apache

Server area: Directory /LDAPLAB/LDAPXX/ProtectedInfo

User authentication method:

○ Inherit

○ Use Internet users in validation lists

○ Use OS/400 profile of client

● Use user entries in LDAP server

Authentication name or realm: AUTHxx

LDAP configuration file: /LDAPLab/ldapxx/ldap.c or...

LDAP group name or filter: Group

Figure 43. Basic Authentication window

On the Basic Authentication window, select the authentication method and enter an authentication name or realm. Enter the fields as follows.

User authentication method: **Use user entries in LDAP server**

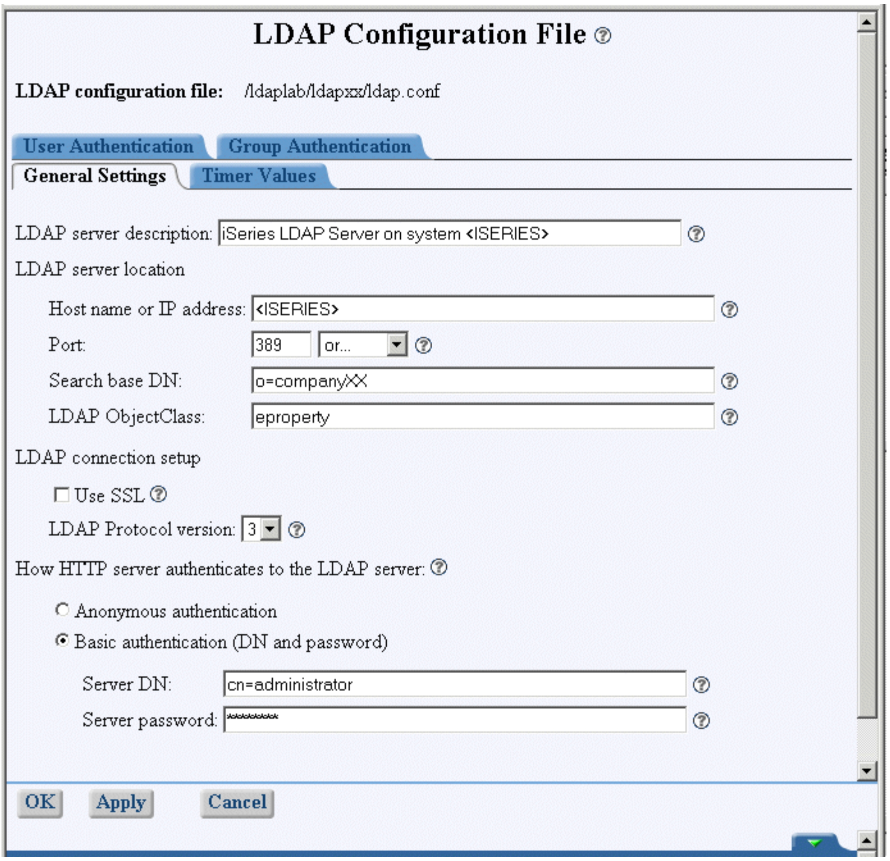
Here you select where the user names and passwords used for basic authentication are maintained. In our case, we use an LDAP server for authentication. There is no default value.

Authentication name or realm: `AUTHxx`

This name is usually displayed by a Web browser in a pop-up dialog window when challenging for a username and password to access the requested resource. This information can then be used to determine what user name and password to enter.

New in V5R2 is the way LDAP support is configured. Prior to V5R2, LDAP authentication configuration values were entered through the HTTP server administration graphical user interface (GUI), while HTTP server configuration support was defined in LDAP configuration files. In V5R2, all LDAP-related configuration values, whether authentication or configuration support, are defined via LDAP configuration files that are linked into the HTTP server configuration.

Enter the file name `/LDAPLAB/LDAPxx/ldap.conf` for the LDAP configuration file parameter and click **Configure**. This starts a new configuration interface where you defined LDAP settings. By default, if the file does not exist, it will be created.



LDAP Configuration File

LDAP configuration file: /ldaplab/ldapxx/ldap.conf

User Authentication | Group Authentication | General Settings | Timer Values

LDAP server description: iSeries LDAP Server on system <ISERIES>

LDAP server location

Host name or IP address: <ISERIES>

Port: 389 or...

Search base DN: o=companyXX

LDAP ObjectClass: eproperty

LDAP connection setup

☐ Use SSL

LDAP Protocol version: 3

How HTTP server authenticates to the LDAP server:

○ Anonymous authentication

● Basic authentication (DN and password)

Server DN: cn=administrator

Server password: ********

OK | Apply | Cancel

Figure 44. LDAP configuration file - General Settings tab

On the General Settings tab, the parameter specify the host where the LDAP directory resides and the location within the directory tree containing the user information. Enter the information as follows:

LDAP server description: `iSeries LDAP server on system` **`<ISERIES>`**

Host name or IP address: **`<ISERIES>`**

Port: `389` (if SSL is used, you need to specify port 636)

Search base DN: `o=company`**`XX`**

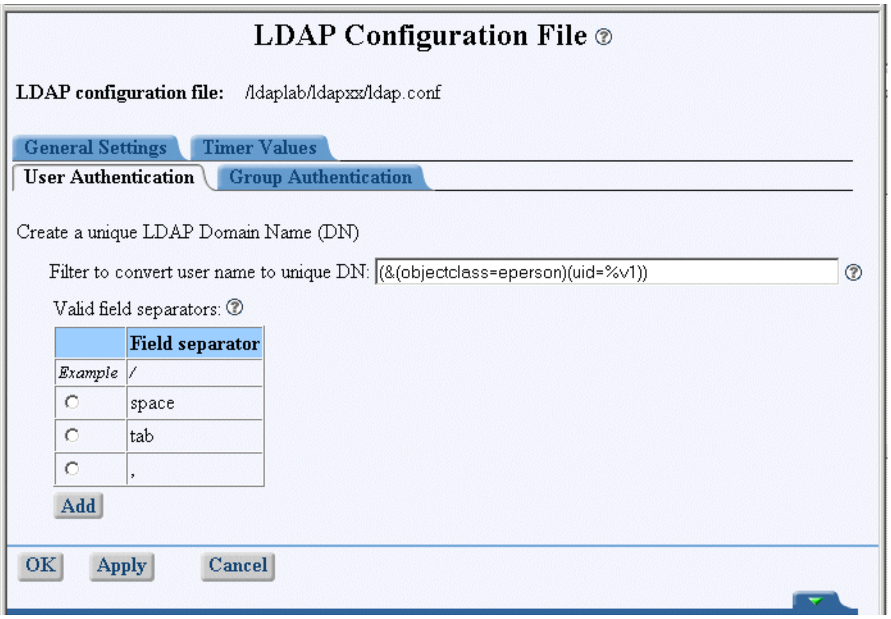
Select **Basic authentication (DN and password)** and enter the following bind information.

Server DN: `cn=administrator`

Server password: **`<LDAP_Admin_Password>`**

The server DN and password are the credentials that are used by the HTTP server to bind to the LDAP server. This DN (user) must have the authority to work with the user entries including the userPassword attribute.

__ 14.Click **Apply** and then the **User Authentication** tab.



LDAP Configuration File

LDAP configuration file: /ldaplab/ldapxx/ldap.conf

Create a unique LDAP Domain Name (DN)

Filter to convert user name to unique DN: (&(objectclass=eperson)(uid=%v1))

Valid field separators:

	Field separator
Example	/
○	space
○	tab
○	,

Figure 45. LDAP configuration file - User Authentication tab

On the User Authentication tab, you can define the search filter for finding LDAP directory entries and the separator character that can be used to separate values in the user name field of the Web browsers user challenge.

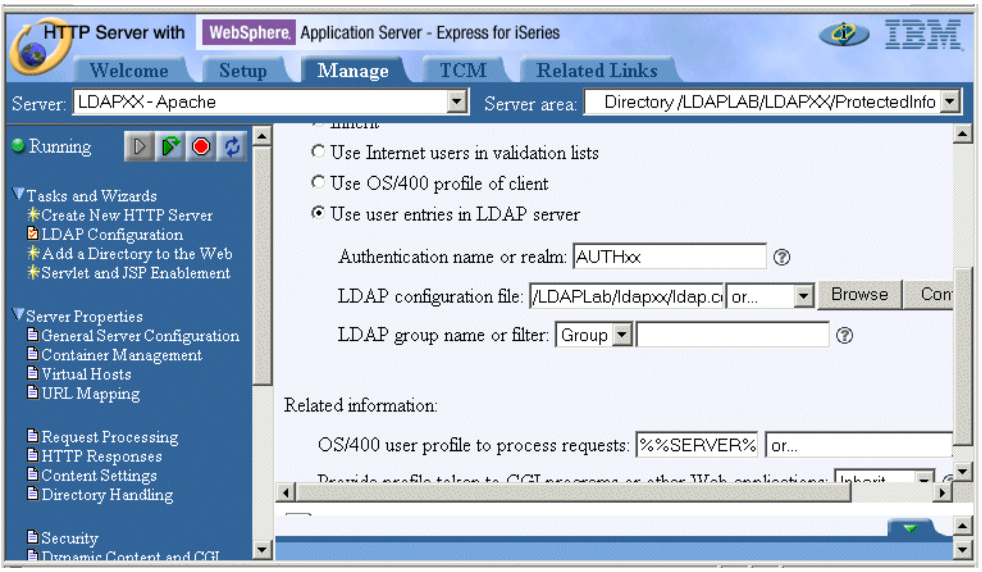
Enter the following filter in the *Filter to convert user name to unique DN* parameter:

```
(&(objectclass=eperson)(uid=%v1))
```

This filter specifies that the HTTP server searches for directory entries of an object class ePerson and where the uid attribute must match the username value entered in the browser’s authentication dialog window. The attribute you want to use for user authentication should uniquely identify a user. That means that you may want to use only the uid or maybe an e-mail address as a unique identifier. Note that there is no space between parameters in the search filter.

__ 15.Click **Apply** and then **OK** to save your settings to the new ldap.conf file. The current window closes and you return to the HTTP server configuration Security page.

__ 16.On the Security page, scroll down until you see the section Related information.



Server: LDAPXX - Apache

Server area: Directory /LDAPLAB/LDAPXX/ProtectedInfo

○ Use Internet users in validation lists

○ Use OS/400 profile of client

● Use user entries in LDAP server

Authentication name or realm: AUTHxx

LDAP configuration file: /LDAPLab/ldapxx/ldap.c or...

LDAP group name or filter: Group

Related information:

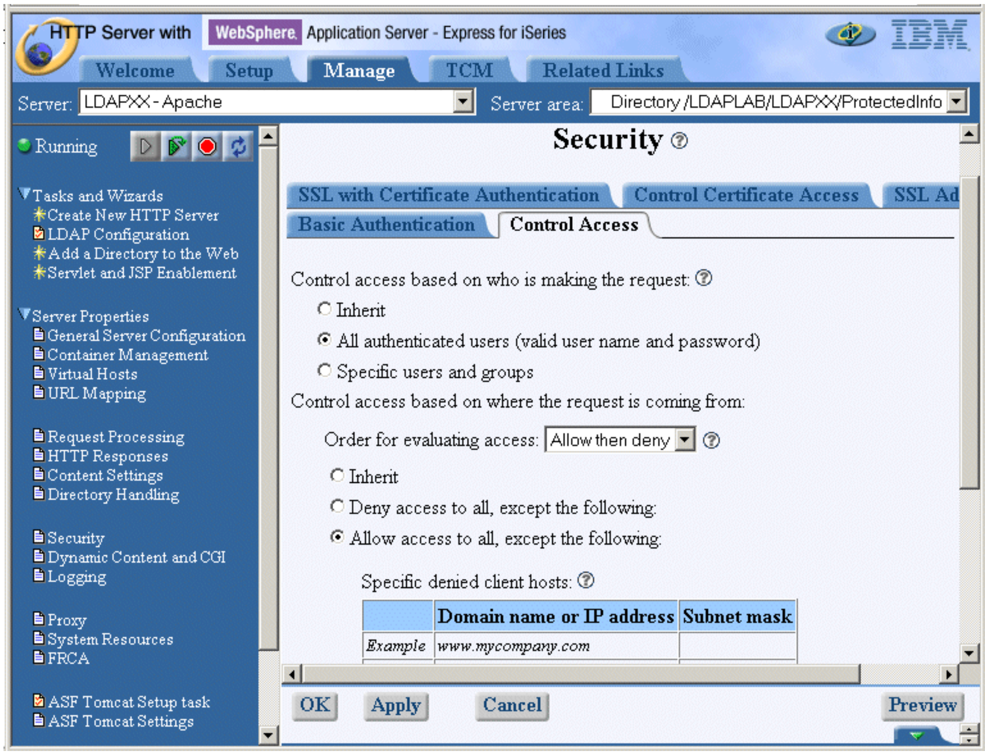
OS/400 user profile to process requests: %%SERVER% or...

Figure 46. Basic Authentication window

For OS/400 u*ser profile to process requests,* click the drop-down list in the adjoining field and select **Default server profile**. This specifies the iSeries system profile to the server. For a protected resource, this option specifies which iSeries system profile the server temporarily swaps to while serving that resource. To start the server, you must have authority to the specified profile. In a production environment, it is recommended to create a separate user profile for accessing the protected resources.

Note that you cannot process server requests under a client user profile when authenticating users with LDAP or validation lists.

__ 17.Click **Apply** to save your changes and then the **Control Access** tab to define the protection level.



Server: LDAPXX - Apache

Server area: Directory /LDAPLAB/LDAPXX/ProtectedInfo

Security

Control access based on who is making the request:

○ Inherit
● All authenticated users (valid user name and password)
○ Specific users and groups

Control access based on where the request is coming from:

Order for evaluating access: Allow then deny

○ Inherit
○ Deny access to all, except the following:
● Allow access to all, except the following:

Specific denied client hosts:

	Domain name or IP address	Subnet mask
Example	*www.mycompany.com*	

Figure 47. Control Access window

You see the Control Access page. Select **All authenticated users (valid user name and password)** for Users and groups who can access this resource on the Control Access window. This option specifies which users and groups are allowed access to server resources. When a request is made, the server checks to see if the requesting host is allowed access to the resource.

In the *Control access based on where the request is coming from* section, select **Allow access to all, except the following** for client hosts allowed access to this resource. This specifies which client hosts are allowed access to server resources.

Scroll down to the bottom to see the remaining parameters. For *Control access policy* select **Control access based on where and from whom the request originates**. Control access policy establishes access policy if both allow and require are used. The parameter can be either 'all' (and) or 'any' (or). This option is only useful if access to a particular area is being restricted by both username/password and client host address.

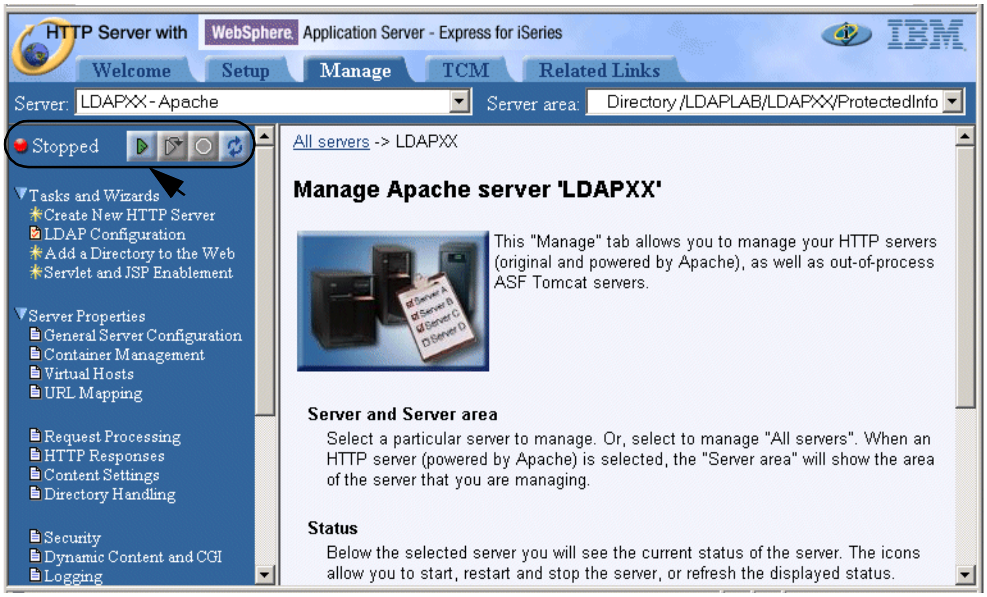
__ 18. Click **Apply** and then **OK** to save your settings.

Now you have configured your LDAPXX HTTP Server to protect the information stored in the /LDAPLAB/LDAPXX/Protectedinfo directory.

If a user now connects to the Web server and enters the alias for the ProtectedInfo directory as previously defined, an authentication challenge is presented to the user. The user has to enter the user ID and password. Then the HTTP server connects to the LDAP server, searches for an entry that contains the entered user ID in the uid attribute and verifies whether the entered password is correct. If the verify is successful, the user gets access to the Protectedinfo directory.

You have to start your HTTP server now.

__ 19.From the Manage tab, click the green arrow to start your server instance. If you do not see the green arrow, the server is already started. In latter case, you need to restart the server.



Server: LDAPXX - Apache

Server area: Directory /LDAPLAB/LDAPXX/ProtectedInfo

All servers -> LDAPXX

Manage Apache server 'LDAPXX'

This "Manage" tab allows you to manage your HTTP servers (original and powered by Apache), as well as out-of-process ASF Tomcat servers.

Server and Server area

Select a particular server to manage. Or, select to manage "All servers". When an HTTP server (powered by Apache) is selected, the "Server area" will show the area of the server that you are managing.

Status

Below the selected server you will see the current status of the server. The icons allow you to start, restart and stop the server, or refresh the displayed status.

Figure 48. Starting the HTTP server window

__ 20.It will successfully start if you configured everything correctly. Use the Refresh button to refresh the window to see if your HTTP server is running. You can now check if your configuration works.

__ 21.Start a new browser window and access your HTTP server home page by entering the following URL:

`http://<ISERIES>:88xx`

Your home page is displayed. Now try to gain access to the protected information.

__ 22.On the home page, click the arrow in front of **Access protected resource (Lab 4)**.

An authentication challenge window is displayed. Sign on with user name and password:

- **User Name**: `WTeamxxa`
- **Password**: `teamxx`

Note that you could access the protected info via your browser with the following URL:

`http://<ISERIES>:88xx/Premium/`

After you sign on, the protected information appears.

__ 23.Close all browser windows.

You have now completed the task.

Task 2: Configuring the HTTP Server for LDAP configuration support

Another fantastic feature of the IBM HTTP Server for iSeries (Original) and (powered by Apache) is the support of retrieving server configuration directives from an LDAP directory. If you operate just one HTTP Web server, you may not use this support. But once you start using at least two Web servers, you can take full advantage of using the LDAP configuration support.

For example, when you use two Web servers for load sharing and backup purposes like our iSeries Shop does, then you need to maintain just a single set of configuration directives. These directives are published into an LDAP directory and both servers retrieve the configuration via include directives during server startup time. Sound good? Well it is good when you follow certain rules:

1. Set up a test server instance. This instance is used to maintain your main server configuration and test configuration changes before deployment. There should be no doubt about this point, because making changes to a production instance without prior testing is asking for trouble.
2. Once the configuration is properly tested, the configuration directives are published into the LDAP server. A second aspect is that you can selectively publish information. That means, if you have a common set of directives that you want to use on three Web servers, you just need to publish those. If required, each of the three servers can still maintain their own directives that only apply to the individual server. The common directives are then included from the LDAP server during server startup. There is virtually no limit to the possibilities you have with this support. For example, you can build logical blocks that hold certain configuration directives. With multiple include directives, you can then link different blocks of configuration directives together. You may want to consider implementing LDAP server replicas for availability reasons.
3. On each server that is designated to include configuration directives from an LDAP server, you create a basic Web server configuration and then add the necessary include directives to load the rest of the configuration from the LDAP server.

This section guides you through the steps for setting up the IBM HTTP Server (powered by Apache) to perform the setup by using configuration information stored in an LDAP directory.

The LDAPXX server instance represents your test server instance. You will create a production HTTP server LDAPPRODXX (*XX* represents your team number you got from your instructor) and do all the configuration that is necessary to use a configuration file on an LDAP server. You will work with this server during the lab. Be sure that you always select your HTTP server during this lab.

Perform the following steps to logon to the HTTP Administration:

__ 1. Start Internet Explorer. Make a connection to the HTTP Server Administrator panel on your iSeries. Use the URL:

```
http://<ISERIES>:2001/HTTPAdmin
```

__ 2. Sign on with user ID and password:

- User ID: **<UserID>**
- Password: **<OS/400_password>**

Note that the user profile needs to have *ALLOBJ and *SECADMIN special authorities.

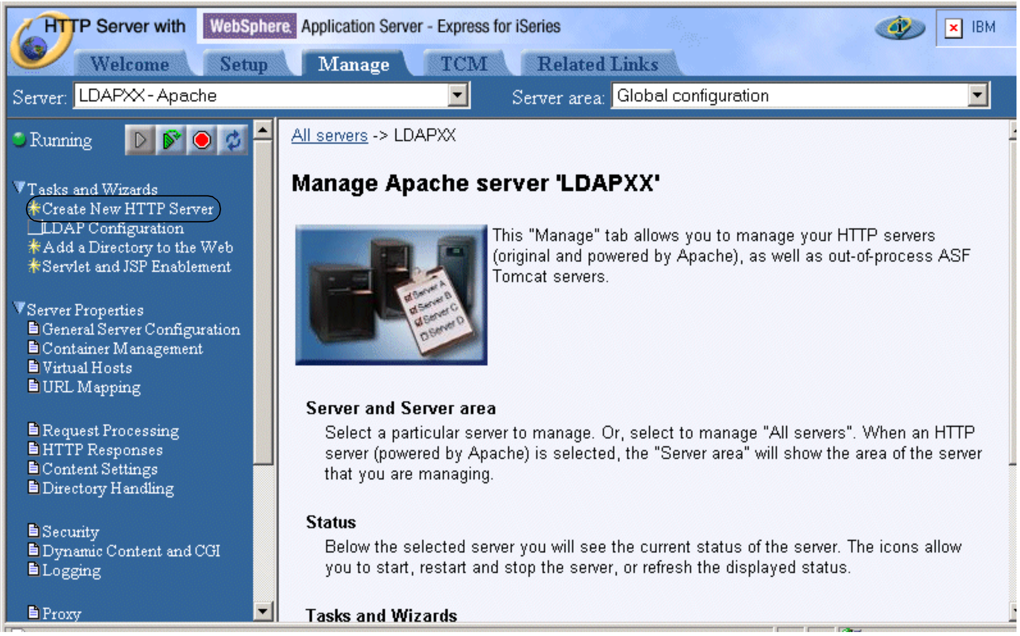
The HTTP Server administration and configuration main window appears.

The HTTP server administration and configuration utility requires the HTTP *Admin instance to be up and running. You can use Operations Navigator (TCP/IP Servers) or the following command to start the *Admin instance:

```
STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
```

__ 3. Select the **Manage** tab.

__ 4. On the Administration page (Figure 49), select **Create new HTTP Server**.



Manage Apache server 'LDAPXX'

This "Manage" tab allows you to manage your HTTP servers (original and powered by Apache), as well as out-of-process ASF Tomcat servers.

Server and Server area

Select a particular server to manage. Or, select to manage "All servers". When an HTTP server (powered by Apache) is selected, the "Server area" will show the area of the server that you are managing.

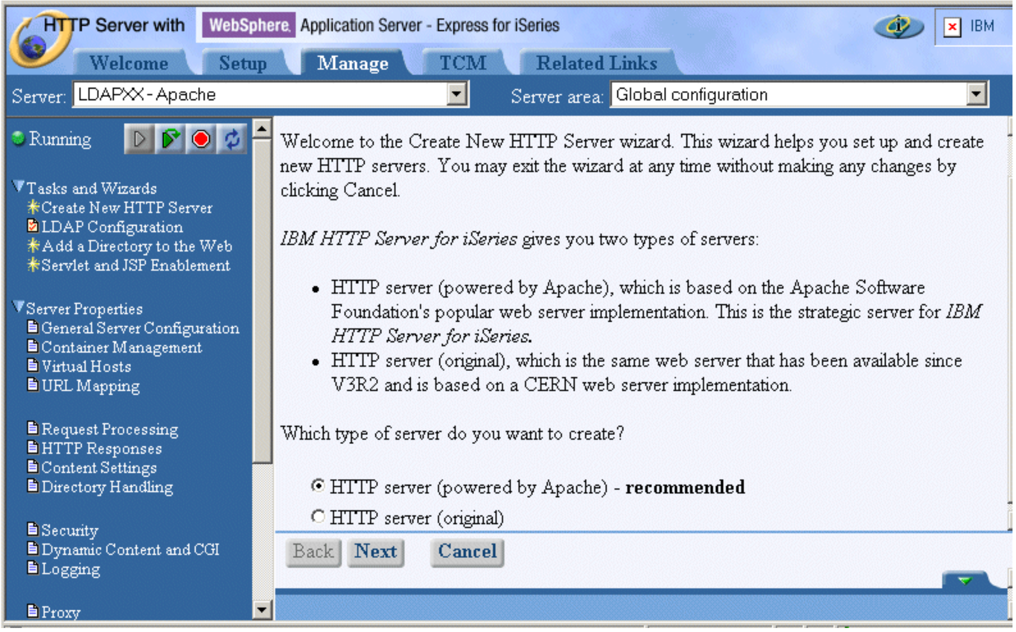
Status

Below the selected server you will see the current status of the server. The icons allow you to start, restart and stop the server, or refresh the displayed status.

Tasks and Wizards

Figure 49. Manage window

__ 5. The HTTP server configuration wizard starts as shown in Figure 50. Select **HTTP server (powered by Apache)**. This is recommended by IBM because further enhancements are only be implemented in the HTTP server (powered by Apache). Click **Next**.



Server: LDAPXX - Apache   Server area: Global configuration

Welcome to the Create New HTTP Server wizard. This wizard helps you set up and create new HTTP servers. You may exit the wizard at any time without making any changes by clicking Cancel.

IBM HTTP Server for iSeries gives you two types of servers:

- HTTP server (powered by Apache), which is based on the Apache Software Foundation's popular web server implementation. This is the strategic server for *IBM HTTP Server for iSeries*.
- HTTP server (original), which is the same web server that has been available since V3R2 and is based on a CERN web server implementation.

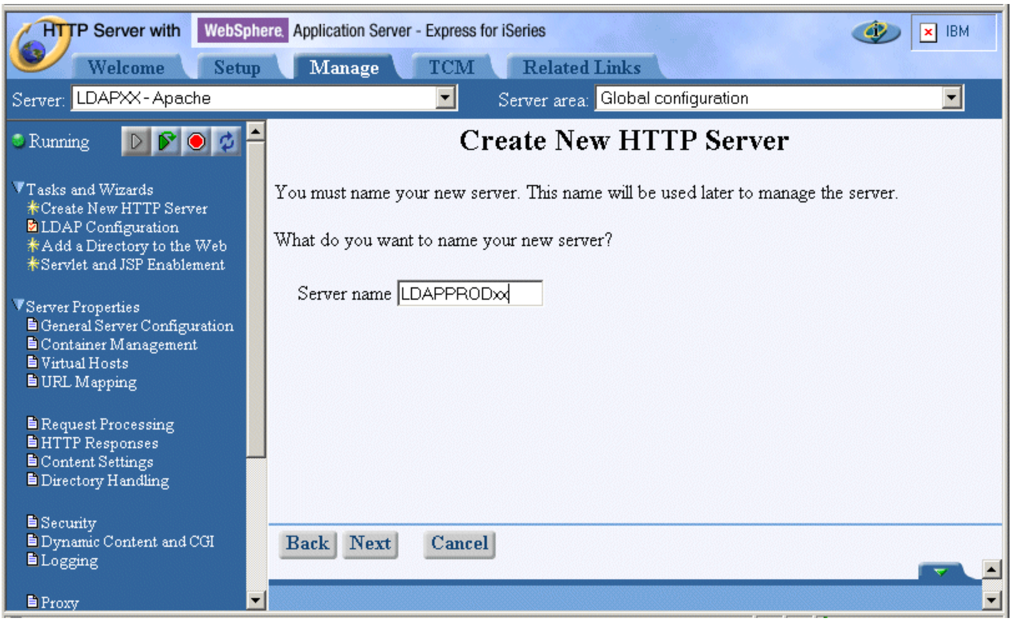
Which type of server do you want to create?

● HTTP server (powered by Apache) - **recommended**

○ HTTP server (original)

Figure 50. HTTP configuration

__ 6. On the Create HTTP Server page (Figure 51) appears. If you instead see the Security Information window, click **Continue**.



Server: LDAPXX - Apache   Server area: Global configuration

Create New HTTP Server

You must name your new server. This name will be used later to manage the server.

What do you want to name your new server?

Server name LDAPPRODxx

Figure 51. Create HTTP server page

On the Create HTTP Server page, enter your HTTP server name in the Server name field (Remember to replace the XX with your team number.).

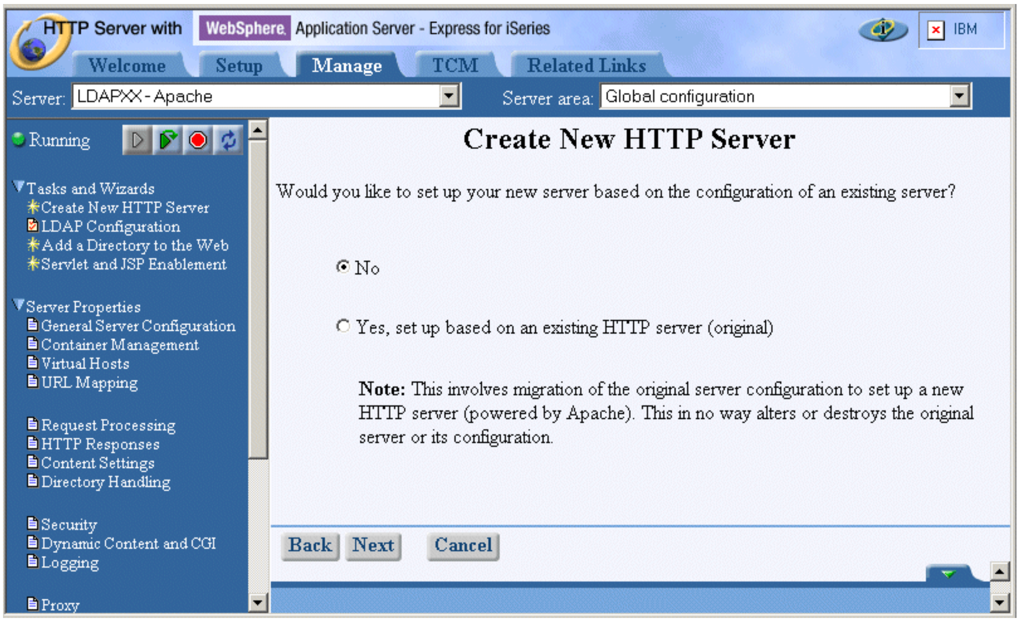
Server name: LDAPPRODXX

Click **Next** to continue.

__ 7. On the next page (Figure 52), select **No** so that you can build your own server configuration. The new server is not based on an existing HTTP server configuration. Only the default values and directives are included in the configuration file.

Select Yes only if you want to build your configuration on an existing HTTP server configuration. The new server is based on an existing HTTP Server (original). This involves a migration of the HTTP Server (original) configuration to an HTTP Server (powered by Apache) configuration. This in no way alters or destroys the existing server or its configuration.

Click **Next**.



Create New HTTP Server

Would you like to set up your new server based on the configuration of an existing server?

● No

○ Yes, set up based on an existing HTTP server (original)

Note: This involves migration of the original server configuration to set up a new HTTP server (powered by Apache). This in no way alters or destroys the original server or its configuration.

Figure 52. HTTP server-based selection page

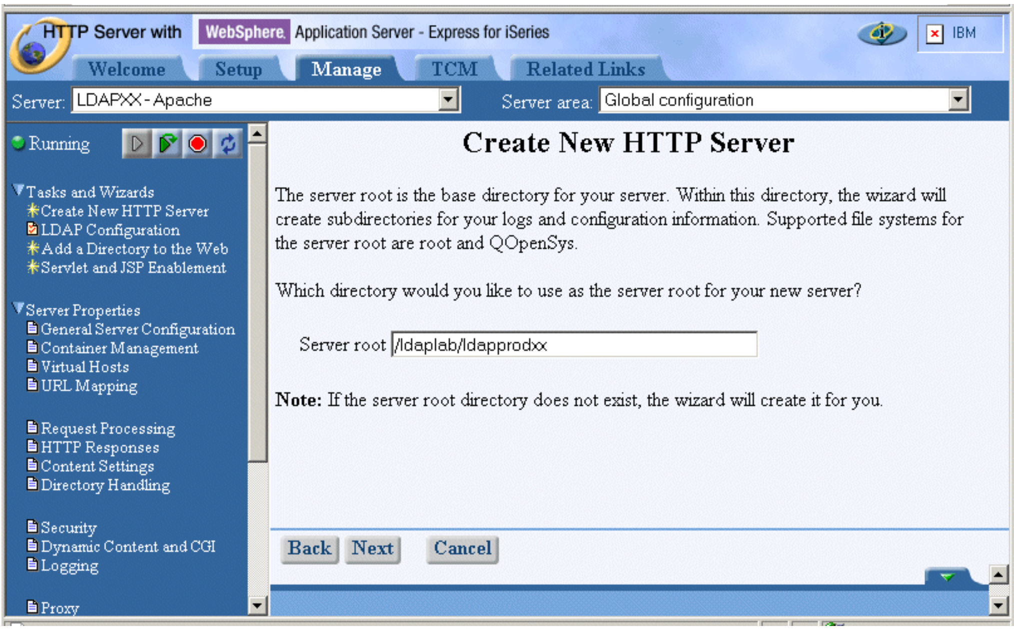
__ 8. On the create HTTP Server page (Figure 53) in the field Server root, enter:

Server root: `/LDAPLAB/LDAPPRODXX`

The server root is the base directory for your HTTP server. Within this directory, the wizard create subdirectories for your logs, and configuration information.

Note: If the server root does not exist, the wizard creates it for you.

Click **Next**.



Create New HTTP Server

The server root is the base directory for your server. Within this directory, the wizard will create subdirectories for your logs and configuration information. Supported file systems for the server root are root and QOpenSys.

Which directory would you like to use as the server root for your new server?

Server root /ldaplab/ldapprodxx

Note: If the server root directory does not exist, the wizard will create it for you.

Figure 53. Server root window

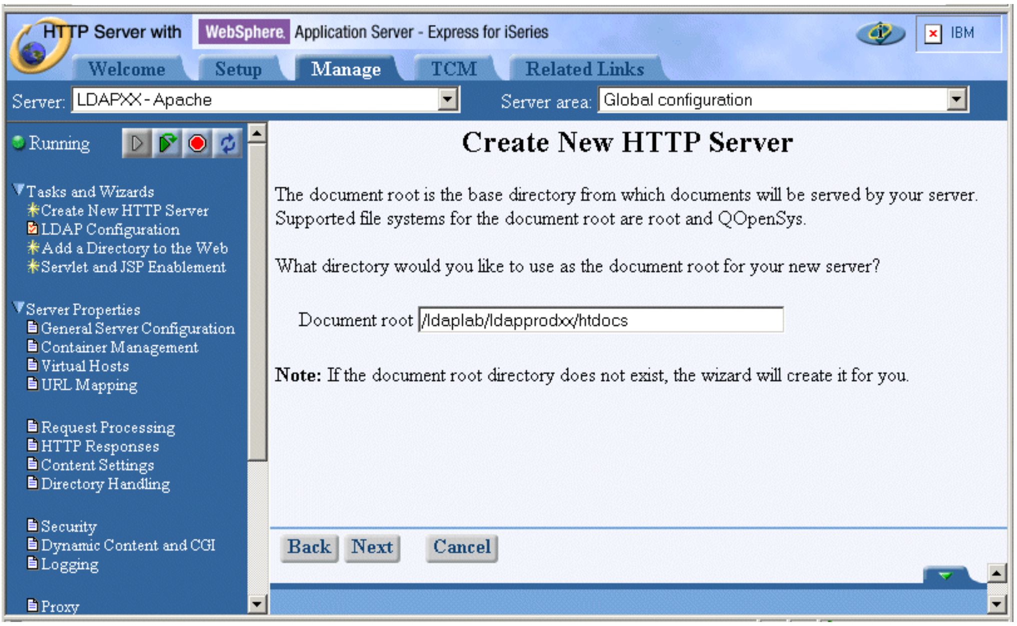
__ 9. On the create HTTP Server window (Figure 54), in the field Document root, enter:

Document root: `/LDAPLAB/LDAPPRODXX/htdocs`

The document root is the directory from which your Web documents are served by your HTTP server.

Note: If the server root does not exist, the wizard creates it for you.

Click **Next**.



Create New HTTP Server

The document root is the base directory from which documents will be served by your server. Supported file systems for the document root are root and QOpenSys.

What directory would you like to use as the document root for your new server?

Document root /ldaplab/ldapprodxx/htdocs

Note: If the document root directory does not exist, the wizard will create it for you.

Figure 54. Document root window

__ 10. On the next page (Figure 55) window, select the IP address and TCP/IP port on which your server listen to client requests. In the IP address field, you can specify to which IP addressees on your system your server listens. In the Port field you specify which port the HTTP server listens on.

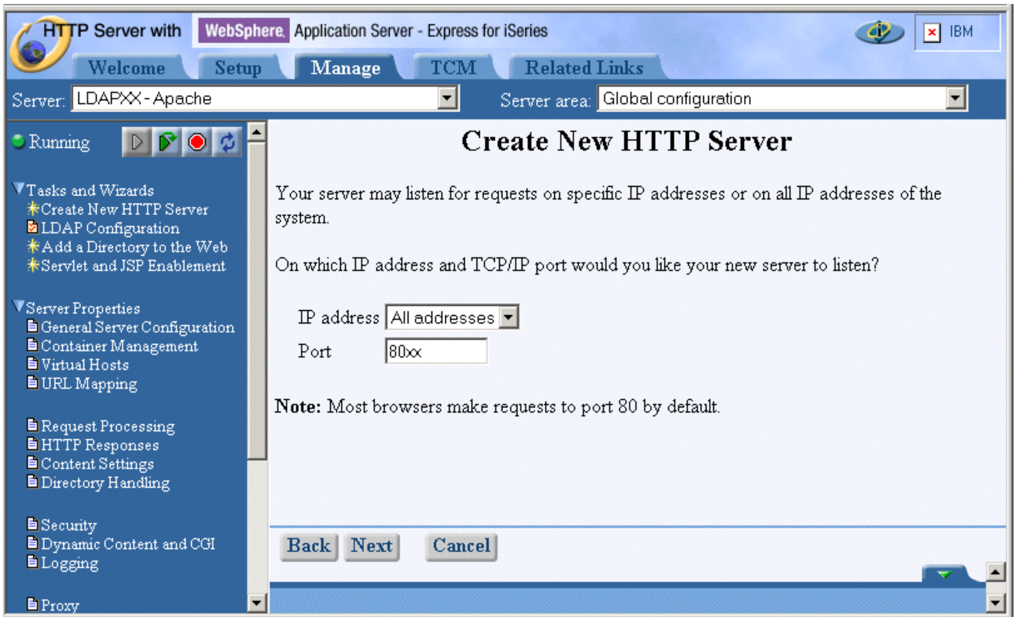
Most browsers make HTTP requests on ports 80 and 443 by default. Typically, the default configuration option is for servers to listen on all IP addresses on port 80. Multiple servers cannot listen on the same port and IP numbers. Multiple servers may listen on the same IP address, but require a unique port, or they may listen on the same port, but require a unique IP address. If you want each server to listen on port 80, then you should configure each server to listen on a specific unique IP address.

If you add another Web server product, such as Lotus Domino (with the HTTP task enabled) on the same iSeries, it cannot listen on the same IP address and the same port as the HTTP Server.

Enter the following information in the fields:

- IP Address: **All addresses**
- Port: `80XX` (Remember to replace the XX with your team number.)

Click **Next** to continue.



Server: LDAPXX - Apache

Server area: Global configuration

Create New HTTP Server

Your server may listen for requests on specific IP addresses or on all IP addresses of the system.

On which IP address and TCP/IP port would you like your new server to listen?

IP address: All addresses

Port: 80xx

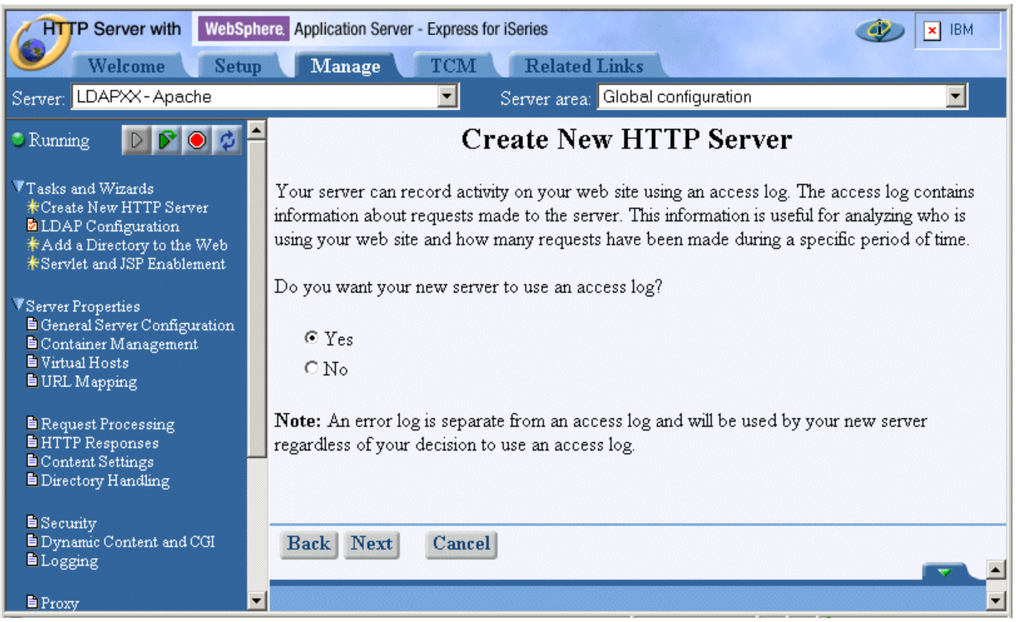
Note: Most browsers make requests to port 80 by default.

Figure 55. IP address and port window

__ 11. The HTTP server can keep a log of activity on your site. The combined activity log contains information on access requests and both the Referrer and UserAgent headers from incoming requests.

As shown in Figure 56, select **Combined log files** to get the log files created. You can view this log files in your HTTP server directory, and it can be very helpful for problem determination.

Click **Next**.



Server: LDAPXX - Apache

Server area: Global configuration

Create New HTTP Server

Your server can record activity on your web site using an access log. The access log contains information about requests made to the server. This information is useful for analyzing who is using your web site and how many requests have been made during a specific period of time.

Do you want your new server to use an access log?

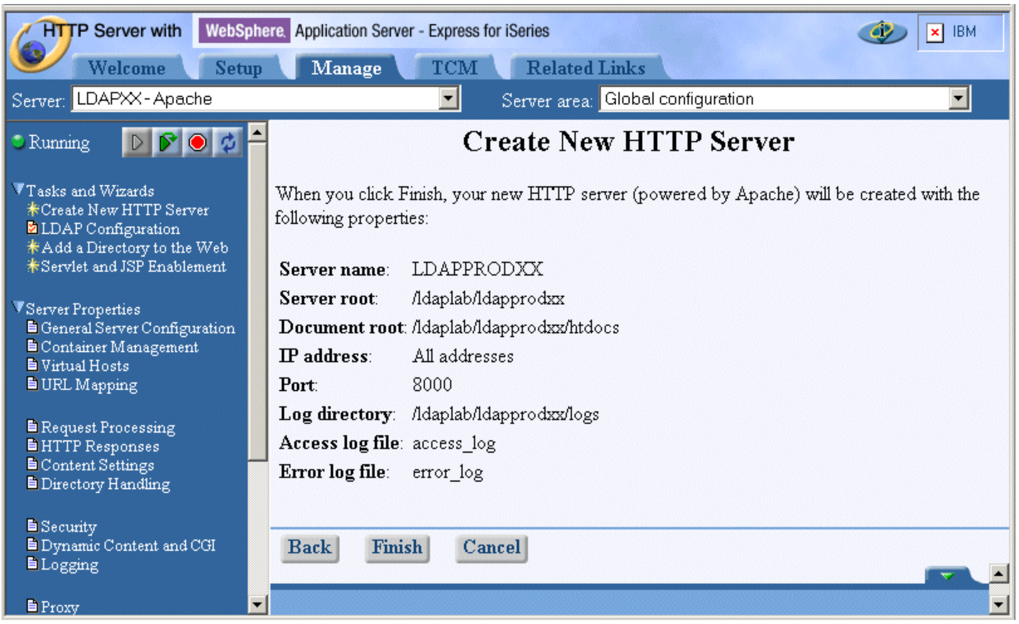
● Yes

○ No

Note: An error log is separate from an access log and will be used by your new server regardless of your decision to use an access log.

Figure 56. Log file window

__ 12.You see the configuration summary as shown in Figure 57. Here you get the overview for your HTTP server configuration you performed. Verify that the data you entered is correct. Click **Finish**.



Server: LDAPXX - Apache

Server area: Global configuration

Create New HTTP Server

When you click Finish, your new HTTP server (powered by Apache) will be created with the following properties:

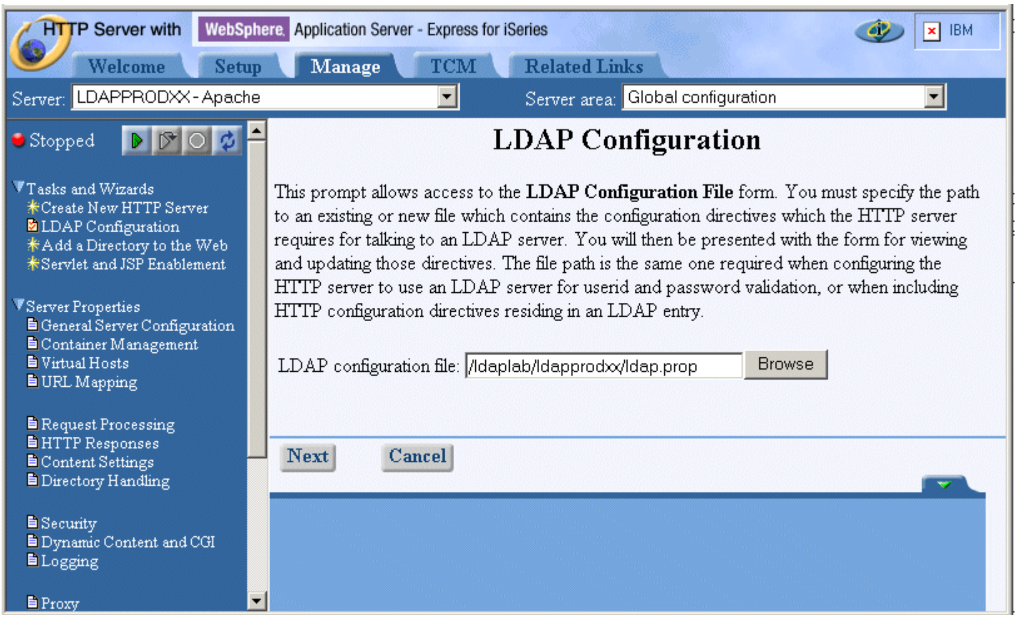
Server name:	LDAPPRODXX
Server root:	/ldaplab/ldapprodxx
Document root:	/ldaplab/ldapprodxx/htdocs
IP address:	All addresses
Port:	8000
Log directory:	/ldaplab/ldapprodxx/logs
Access log file:	access_log
Error log file:	error_log

Figure 57. HTTP server overview window

__ 13.This creates your HTTP server LDAPPRODXX. You are on the Create HTTP Server window. Click **Manage newly creates server** to continue.

In the following steps you will set up the new server instance to access the LDAP server in order to load the HTTP server directives.

__ 14.Make sure that you manage your newly created HTTP server instance and the Global configuration server area is selected before continuing. Click **LDAP Configuration** from the navigation pane.



Server: LDAPPRODXX - Apache

Server area: Global configuration

LDAP Configuration

This prompt allows access to the **LDAP Configuration File** form. You must specify the path to an existing or new file which contains the configuration directives which the HTTP server requires for talking to an LDAP server. You will then be presented with the form for viewing and updating those directives. The file path is the same one required when configuring the HTTP server to use an LDAP server for userid and password validation, or when including HTTP configuration directives residing in an LDAP entry.

LDAP configuration file: /ldaplab/ldapprodxx/ldap.prop

Figure 58. LDAP Configuration window

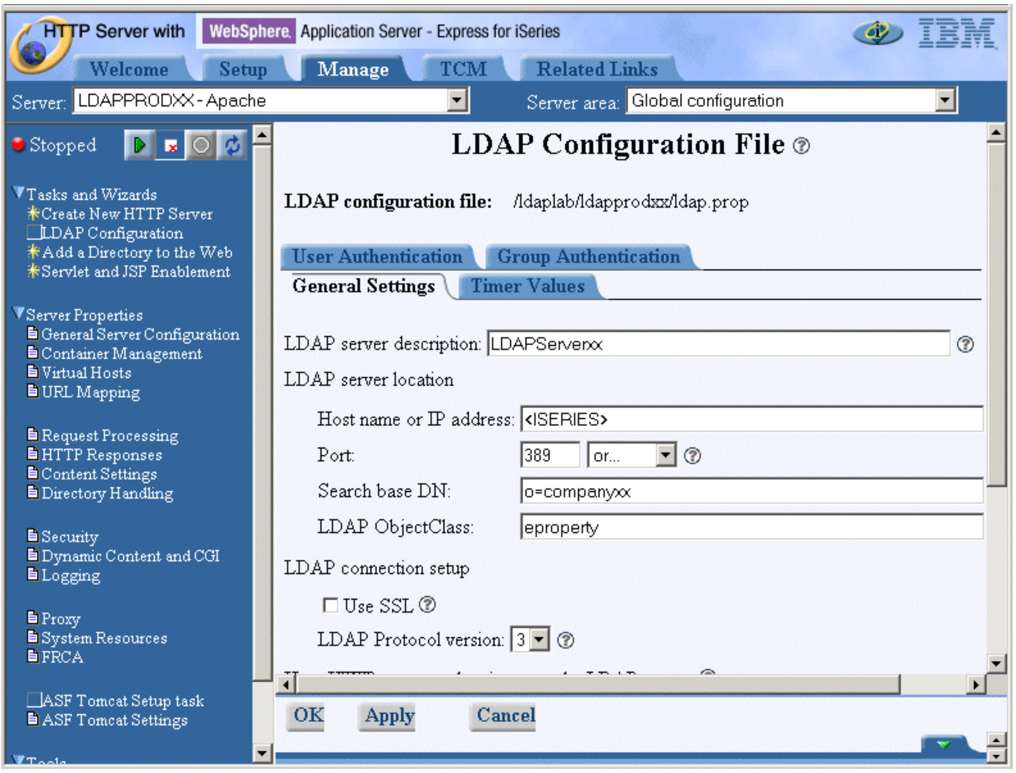
You can select an existing configuration file or create a new one. In either case, you need to specify the path and file name for the LDAP configuration file (this file is also know as the LDAP properties file).

Enter the following information:

LDAP configuration file: `/ldaplab/ldapprodxx/ldap.prop`

Replace the xx in the path with your team number.

__ 15.Click **Next** to continue. The LDAP Configuration File window appears.



Server: LDAPPRODXX - Apache

Server area: Global configuration

LDAP Configuration File

LDAP configuration file: /ldaplab/ldapprodxx/ldap.prop

LDAP server description: LDAPServerxx

LDAP server location

Host name or IP address: <ISERIES>

Port: 389 or...

Search base DN: o=companyxx

LDAP ObjectClass: eproperty

LDAP connection setup

□ Use SSL

LDAP Protocol version: 3

Figure 59. LDAP Configuration File window

On the General Settings tab of the LDAP Configuration File window, you can specify how to access and where to search in the LDAP directory server. Enter the following values:

LDAP server description: `LDAPServer`**`xx`**
Host name or IP address: **<ISERIES>**
Port: `389`
Search base DN: `o=company`**`xx`**

Scroll down to the section How HTTP server authenticates to the LDAP server.

Select **Basic authentication (DN and password)**.

Enter the following values:

Server DN: `cn=administrator`
Server password: **<LDAP_Admin_Password>**

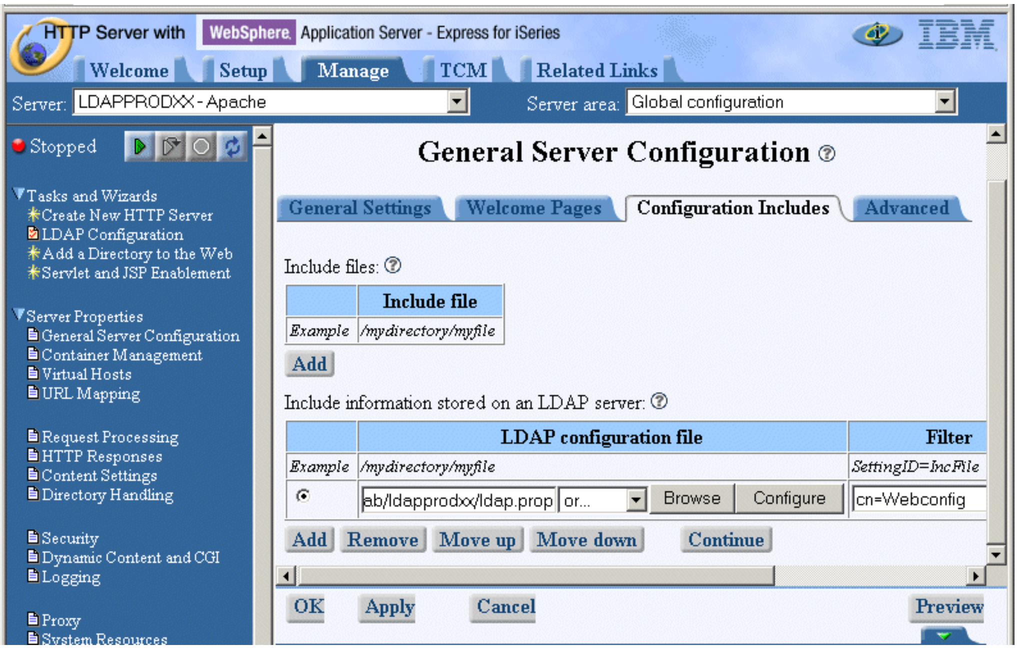
__ 16.Click **Apply** to save your settings and then **OK** to exit the current window.

After the LDAP configuration has been completed, you will configure your instance to include configuration directives from the LDAP server.

__ 17.From the navigation pane, click **General Server Configuration**.

__ 18.On the General Server Configuration window, click the **Configuration Includes** tab.

__ 19.In the Include information stored in an LDAP server, click **Add**.



Server: LDAPPRODXX - Apache

Server area: Global configuration

General Server Configuration

Include files:

	Include file
Example	*/mydirectory/myfile*

Include information stored on an LDAP server:

	LDAP configuration file		Filter
Example	*/mydirectory/myfile*		*SettingID=IncFile*
●	ab/ldapprodxx/ldap.prop	or...	cn=Webconfig

Figure 60. Configuration Includes window

In this section, you have to specify how to access the LDAP server and where to find the information (directives) to be included by entering the following values:

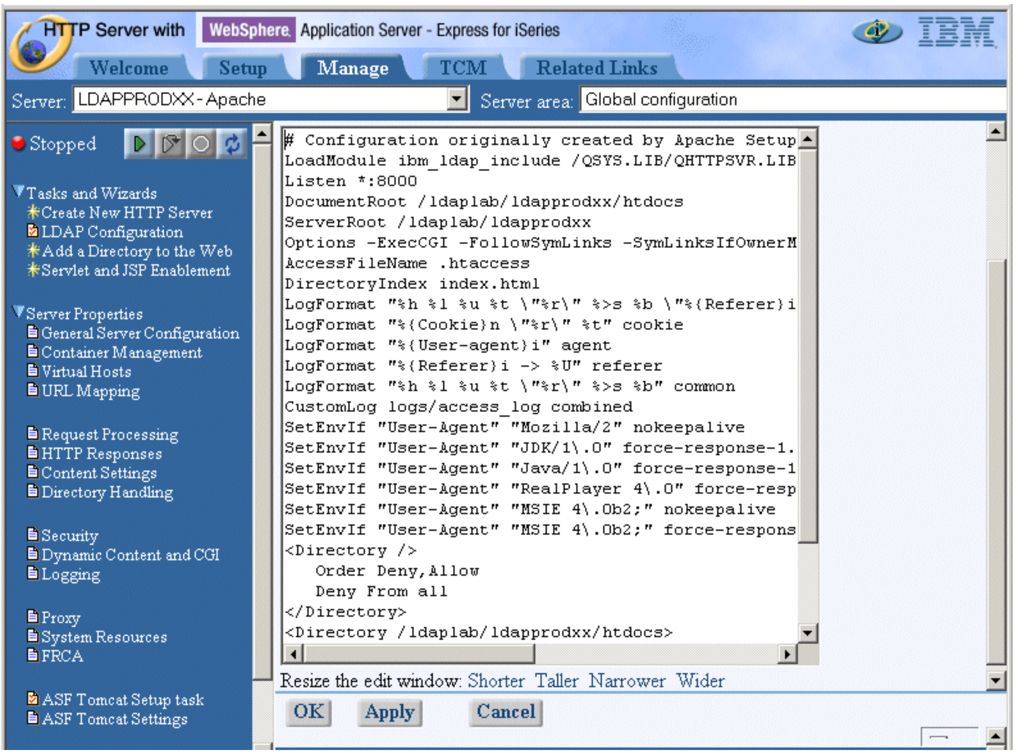
LDAP configuration file	`/ldaplab/ldapprod`**`xx`**`/ldap.prop`
Filter	`cn=Webconfig`
Attribute	`binProperty`

Remember to replace the xx with your team number.

__ 20.Click **Continue** and the **OK** to save your configuration.

All the necessary configuration to include HTTP configuration directives from a LDAP directory is complete. However, there are still some default directives in the ldapprodxx instance that need to be removed. At the end, only the necessary directives to load the configuration from the LDAP directory will remain.

__ 21.From the navigation pane, click **Edit Configuration File**.


HTTP Server with WebSphere Application Server - Express for iSeries
IBM
Welcome
Setup
Manage
TCM
Related Links

Server: LDAPPRODXX - Apache
Server area: Global configuration

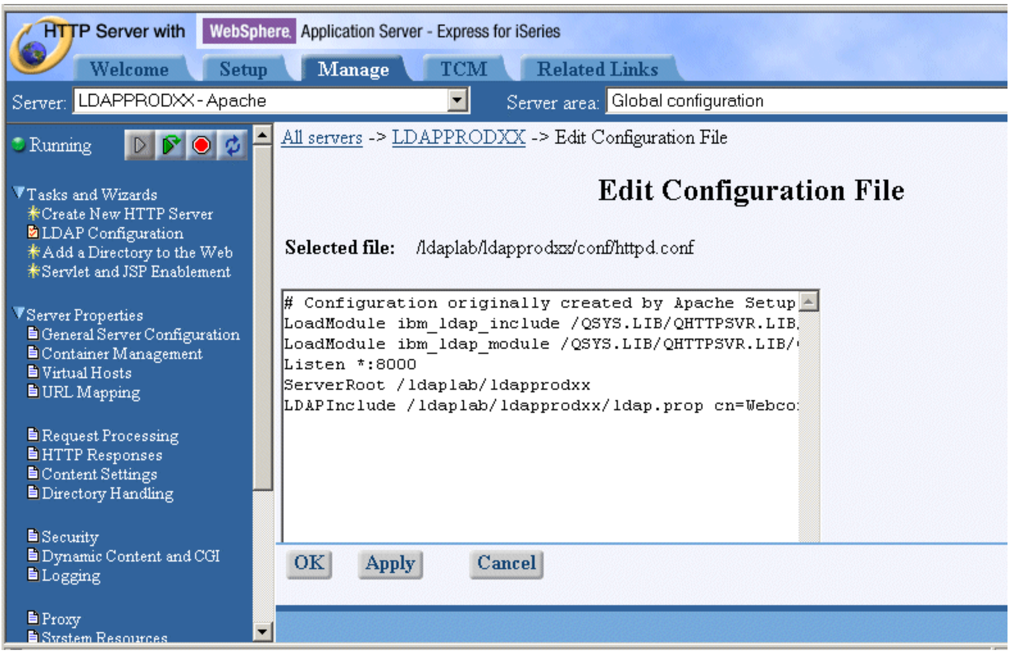
```
# Configuration originally created by Apache Setup
LoadModule ibm_ldap_include /QSYS.LIB/QHTTPSVR.LIB
Listen *:8000
DocumentRoot /ldaplab/ldapprodxx/htdocs
ServerRoot /ldaplab/ldapprodxx
Options -ExecCGI -FollowSymLinks -SymLinksIfOwnerM
AccessFileName .htaccess
DirectoryIndex index.html
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i
LogFormat "%{Cookie}n \"%r\" %t" cookie
LogFormat "%{User-agent}i" agent
LogFormat "%{Referer}i -> %U" referer
LogFormat "%h %l %u %t \"%r\" %>s %b" common
CustomLog logs/access_log combined
SetEnvIf "User-Agent" "Mozilla/2" nokeepalive
SetEnvIf "User-Agent" "JDK/1\.0" force-response-1.
SetEnvIf "User-Agent" "Java/1\.0" force-response-1
SetEnvIf "User-Agent" "RealPlayer 4\.0" force-resp
SetEnvIf "User-Agent" "MSIE 4\.0b2;" nokeepalive
SetEnvIf "User-Agent" "MSIE 4\.0b2;" force-respons
<Directory />
   Order Deny,Allow
   Deny From all
</Directory>
<Directory /ldaplab/ldapprodxx/htdocs>
```

Figure 61. Edit Configuration File window

The window shows all configuration directives that are currently configured. The only exception is the LoadModule directive for the ibm_ldap_module. This directive was used in the test instance to enable the directives for LDAP user authentication. As the LoadModule statements have to be at the beginning of the configuration file, they cannot be included via an include file. Therefore, this directive has been added manually. You need to delete all directives except the ones in the following list:

```
#Configuration originally created by Apache Setup Wizard Fri Jan 17
LoadModule ibm_ldap_include /QSYS.LIB/QHTTPSVR.LIB/QZSRVLDAP.SRVPGM
LoadModule ibm_ldap_module /QSYS.LIB/QHTTPSVR.LIB/QZSRVLDAP.SRVPGM
Listen *:8000
ServerRoot /ldaplab/ldapprodxx
LDAPInclude /ldaplab/ldapprodxx/ldap.prop cn=Webconfig binProperty
```

The configuration window should be similar to the one shown in Figure 62.



Server: LDAPPRODXX - Apache

Server area: Global configuration

Edit Configuration File

Selected file: /ldaplab/ldapprodxx/conf/httpd.conf

```
# Configuration originally created by Apache Setup
LoadModule ibm_ldap_include /QSYS.LIB/QHTTPSVR.LIB.
LoadModule ibm_ldap_module /QSYS.LIB/QHTTPSVR.LIB/
Listen *:8000
ServerRoot /ldaplab/ldapprodxx
LDAPInclude /ldaplab/ldapprodxx/ldap.prop cn=Webco
```

Figure 62. Edit Configuration Window - cleaned up directives

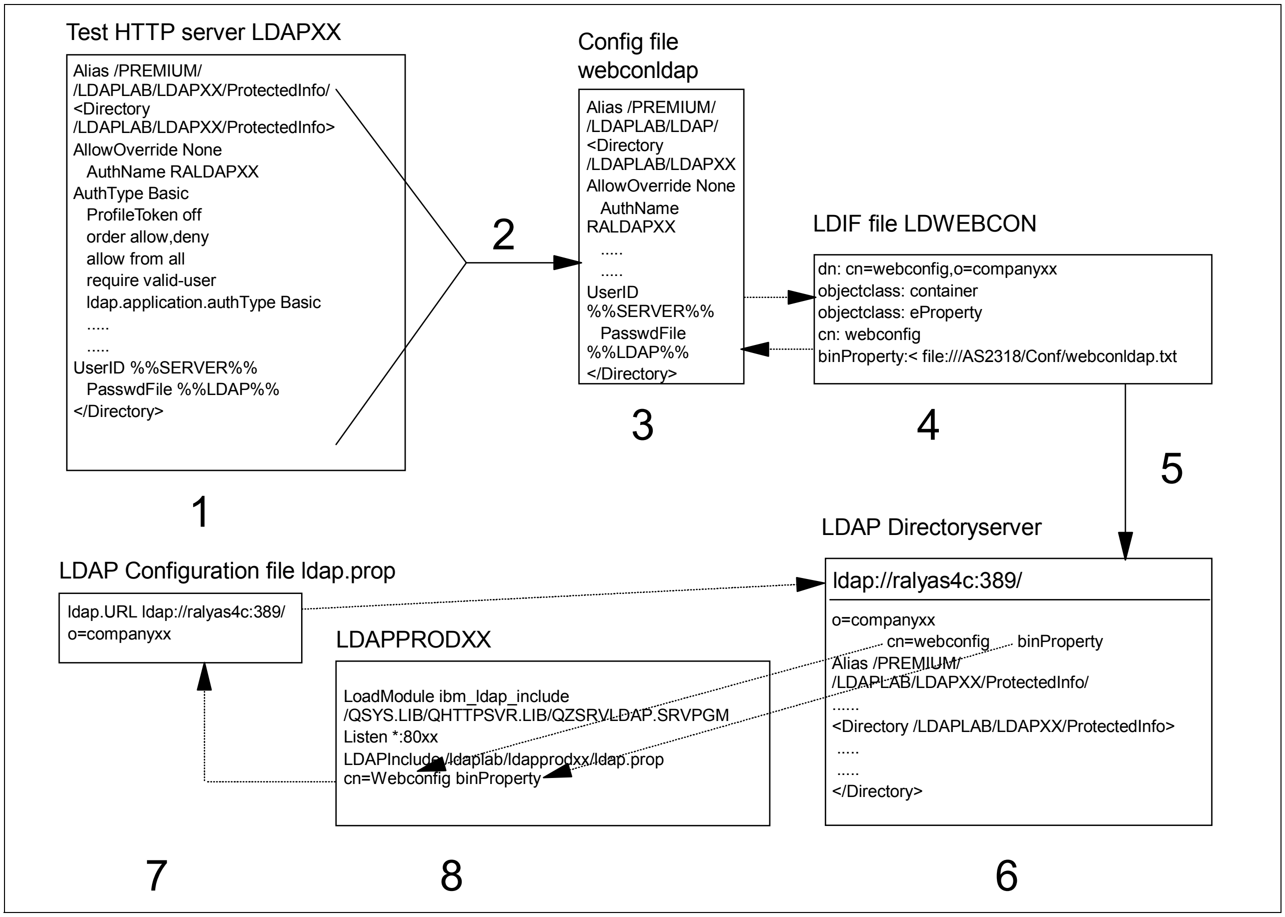
__ 22.Click **Apply** and then **OK** to save your configuration.

Do not start the instance at this time as you did not publish your directives to the LDAP server yet.

Click **OK** to finish the HTTP server configuration.

At this step in the lab, the Web server configuration of your test instance LDAPXX can be exported into a file. This text file will later be published to the LDAP directory. The text file is named WEBCONLDAP.TXT.

You will take the configuration directives from your test HTTP server LDAPXX and copy the common configuration statements into the configuration file WEBCONLDAP.TXT. This file is then published to the LDAP server. The publishing is done via the LDIF file LDWEBCON.TXT that is stored in your HTTP server directory /LDAPLAB/LDAPPRODXX on the iSeries server. An overview of this flow is shown on Figure 63.



```
Alias /PREMIUM/
/LDAPLAB/LDAPXX/ProtectedInfo/
<Directory
/LDAPLAB/LDAPXX/ProtectedInfo>
AllowOverride None
  AuthName RALDAPXX
AuthType Basic
  ProfileToken off
  order allow,deny
  allow from all
  require valid-user
  ldap.application.authType Basic
  .....
  .....
UserID %%SERVER%%
  PasswdFile %%LDAP%%
</Directory>
```

```
Alias /PREMIUM/
/LDAPLAB/LDAP/
<Directory
/LDAPLAB/LDAPXX
AllowOverride None
  AuthName
RALDAPXX
  .....
  .....
UserID
%%SERVER%%
  PasswdFile
%%LDAP%%
</Directory>
```

```
dn: cn=webconfig,o=companyxx
objectclass: container
objectclass: eProperty
cn: webconfig
binProperty:< file:///AS2318/Conf/webconldap.txt
```

```
ldap://ralyas4c:389/

o=companyxx
        cn=webconfig    binProperty
Alias /PREMIUM/
/LDAPLAB/LDAPXX/ProtectedInfo/
......
<Directory /LDAPLAB/LDAPXX/ProtectedInfo>
 .....
 .....
</Directory>
```

```
ldap.URL ldap://ralyas4c:389/
o=companyxx
```

```
LoadModule ibm_ldap_include
/QSYS.LIB/QHTTPSVR.LIB/QZSRVLDAP.SRVPGM
Listen *:80xx
LDAPInclude /ldaplab/ldapprodxx/ldap.prop
cn=Webconfig binProperty
```

Figure 63. Configuration files overview

The flow is further explained here:

1. This is your test HTTP server environment where you configured and tested all the HTTP server configuration directives and applications (user authentication).
2. This step represents the export of the configuration directives from your test instance LDAPXX.
3. In step 3, the exported configuration is copied into a configuration file WEBCONLDAP.TXT in the /LDAPLAB/LDAPPRODXX directory. This file contains all directives that will be published to the LDAP server and then loaded by the LDAP server LDAPPRODXX.
4. The LDIF file LDWEBCON.TXT that is used to create or update the binProperty attribute of the cn=webconfig object on the LDAP server in the directory context o=companyxx.
5. The HTTP server configuration data is published to the LDAP directory using the ldapmodify utility.
6. On the LDAP server, the HTTP configuration is stored in DN: cn=webconfig,o=companyxx attribute binProperty.
7. The LDAP configuration file is used during the HTTP server start. The information in it is used to contact the LDAP server and retrieve the configuration directives from the binProperty attribute of entry cn=webconfig.

8. This is the production environment HTTP server LDAPPRODXX. This server has only the Load Module directive and LDAPInclude directive configured to get the HTTP server started. During startup, the HTTP server uses the information from the LDAP configuration file to connect to the LDAP server and loads the remaining directives from the LDAP directory.

In the following steps, you copy the configuration directives from your test HTTP server into a text file WEBCONLDAP.TXT and save it to your HTTP server directory /LDAPLAB/LDAPPRODXX.

__ 1. From the server list on the Manage tab, select your HTTP server **LDAPXX** (you configured it in the previous lab).

__ 2. On the navigation pane click **Edit Configuration File** to display the configuration from your test HTTP server LDAPXX.

__ 3. Click one directive in the editor window and press Ctrl-A to select all directives in the editor window.

__ 4. Press Ctrl-C to copy the directives into the clipboard.

__ 5. Click **OK** to close the HTTP configuration editor window.

__ 6. From the Windows desktop, click **Start-> Programs-> Accessories-> Notepad** to start Notepad.

__ 7. Within Notepad press Ctrl-V to paste the directives from the clipboard into the Notepad editor window.

Edit the file as shown below.

Remove the Listen, the ServerRoot, and the LoadModule ibm_ldap_module statements from the configuration listed as they have to be adjusted for the production instance.

__ 8. Save the file in your HTTP server directory /LDAPLAB/LDAPPRODXX on the iSeries server with file name WEBCONLDAP.TXT. by clicking **File-> Save as**.

- Save in: `/LDAPLAB/LDAPPRODXX`
- File name: `WEBCONLDAP.TXT`

An example of how the file should look is shown here:

```
  # Configuration originally created by Apache Setup Wizard Fri Jan 17 14:24:31 UTC
2003
DocumentRoot /ldaplab/ldapxx/htdocs
Options -ExecCGI -FollowSymLinks -SymLinksIfOwnerMatch -Includes -IncludesNoExec
-Indexes -MultiViews
AccessFileName .htaccess
DirectoryIndex index.html
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%{Cookie}n \"%r\" %t" cookie
LogFormat "%{User-agent}i" agent
LogFormat "%{Referer}i -> %U" referer
LogFormat "%h %l %u %t \"%r\" %>s %b" common
CustomLog logs/access_log combined
SetEnvIf "User-Agent" "Mozilla/2" nokeepalive
SetEnvIf "User-Agent" "JDK/1\.0" force-response-1.0
SetEnvIf "User-Agent" "Java/1\.0" force-response-1.0
SetEnvIf "User-Agent" "RealPlayer 4\.0" force-response-1.0
SetEnvIf "User-Agent" "MSIE 4\.0b2;" nokeepalive
SetEnvIf "User-Agent" "MSIE 4\.0b2;" force-response-1.0
<Directory />
   Order Deny,Allow
   Deny From all
</Directory>
<Directory /LDAPLAB/LDAPXX/ProtectedInfo>
   Order Allow,Deny
   Allow From all
   Require valid-user
   PasswdFile %%LDAP%%
   UserID %%SERVER%%
   AuthType Basic
   AuthName AUTHxx
   Satisfy All
   LDAPConfigFile /LDAPLab/ldapxx/ldap.conf
</Directory>
<Directory /ldaplab/ldapxx/htdocs>
   Order Allow,Deny
   Allow From all
</Directory>
Alias /Premium/ /LDAPLAB/LDAPXX/ProtectedInfo/
```

__ 9. Exit Notepad.

__ 10. In the next step you create the LDIF file to publish the HTTP configuration directives from file WEBCONLDAP.TXT to the LDAP server. Click **Start-> Programs-> Accessories-> Notepad**.

Enter the following statements in the Notepad editor window:

```
dn: cn=webconfig,o=companyxx
objectclass: container
objectclass: eProperty
cn: webconfig
binProperty:< file:///LDAPLAB/LDAPPRODXX/webconldap.txt
```

dn is the path to the object where the HTTP server configuration on the LDAP server is stored.

The entry *webconfig* has a class *container* and *eProperty*. The attribute that holds the data is *binProperty*.

This LDIF file is used to create or update the *webconfig* object on the LDAP server and store the content of the *webconldap.txt* file into the binProperty attribute.

__ 11. Save the file in your HTTP server directory /LDAPLAB/LDAPPRODXX with file name LDWEBCON.TXT by clicking **File->Save as** and specifying the following values:

- **Save in**: `/LDAPLAB/LDAPPRODXX`
- **File name**: `LDWEBCON.TXT`

You use now the Qshell environment to publish the configuration directives to the LDAP server.

__ 12. Start a 5250 session and sign on with your **<UserID>** and **<OS/400_password>**.

__ 13. Enter `QSH` on your 5250 window in the command line. The QSH Command Entry screen appears.

__ 14. Enter the following command:

```
 ldapmodify -D "cn=administrator" -w "<LDAP_Admin_Password>"
 -f "/LDAPLAB/LDAPPRODXX/LDWEBCON.TXT" -a
```

The ldapmodify utility creates the object webconfig and uploads the HTTP configuration. This utility is used for the first time if the webconfig object does not exist.

-D is used to bind to the LDAP directory. In our example, it is the administrator DN to access the LDAP server.

-w is the password for the DN to access the LDAP server.

-f reads the entry modification information from an ldif file instead of from standard input.

"/LDAPLAB/LDAPPRODXX/LDWEBCON.TXT" is the path to the LDIF file used.

-a is only used by ldapmodify. It indicates that the utility add entries. Using this parameter is the same as using ldapadd.

-r is used if you update the existing object. Replace existing values by default.

If you make changes in your HTTP configuration file WEBCONLDAP.TXT on the iSeries server and you have to update the LDAP server with the new data, you have to use the `ldapmodify` command with the following format.

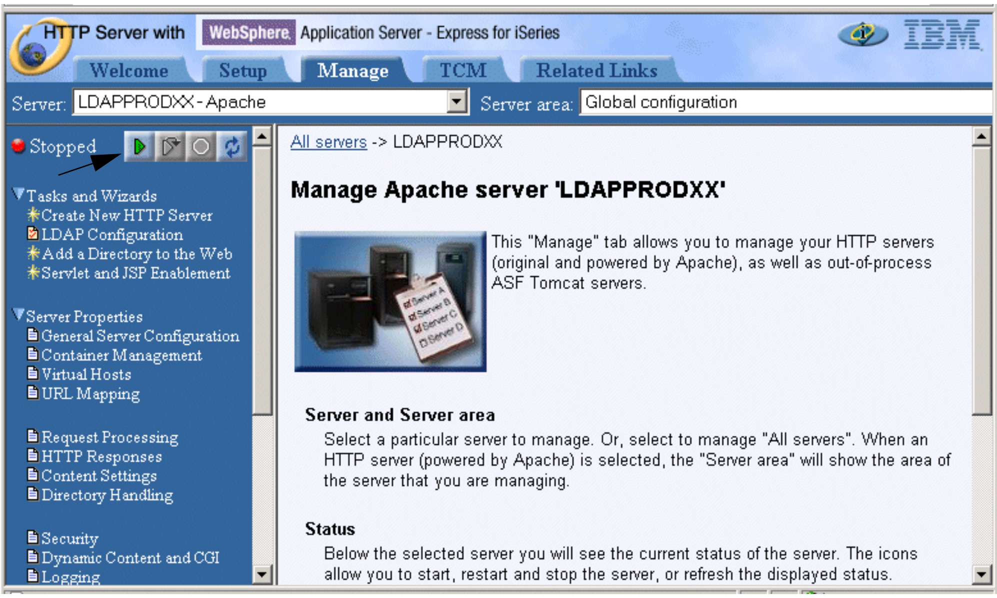
```
ldapmodify -D "cn=administrator" -w "<LDAP_Admin_Password>" -f
"/LDAPLAB/LDAPPRODXX/LDWEBCON.TXT" -r
```

The difference with the previous command used is the -r for replace.

You have performed the complete HTTP configuration to use the LDAP server as a source for many HTTP servers. Changes can be made in a single place for many HTTP servers. When the HTTP server is started, the new configuration is loaded from the LDAP server.

__ 15.Start your HTTP server now. On the Manage tab select your new server instance LDAPPRODxx from the server list.

__ 16.Click the green arrow to start your server.



Server: LDAPPRODXX - Apache   Server area: Global configuration

All servers -> LDAPPRODXX

Manage Apache server 'LDAPPRODXX'

This "Manage" tab allows you to manage your HTTP servers (original and powered by Apache), as well as out-of-process ASF Tomcat servers.

Server and Server area

Select a particular server to manage. Or, select to manage "All servers". When an HTTP server (powered by Apache) is selected, the "Server area" will show the area of the server that you are managing.

Status

Below the selected server you will see the current status of the server. The icons allow you to start, restart and stop the server, or refresh the displayed status.

Figure 64. Manage tab

Your HTTP server starts successfully if you configured everything correctly. Use the **Refresh** button (two arrows in a circle) to refresh the window to see if your HTTP server is running. You can now check if your configuration works. Start a browser and continue.

__ 17.From a browser, use the following URL to access your HTTP server home page:

```
http://<iSeries_Server>:80xx
```

Your home page is displayed.

__ 18. Now try to access the protected information. On the home page click the arrow in front of Access protected resource (Lab 4).

An authentication challenge window is displayed. Sign on with user ID and password:

- **User ID**: `WTeamxxa`
- **Password**: `teamxx`

After you sign on, the protected information is displayed.

__ 19. Close all browser windows.

You have now completed Task 2.

Lab 5. Using an LDAP directory as an address book

The purpose of this lab is to search for users e-mail addresses in the LDAP Directory, while in a mail client.

Everybody knows the hassle of keeping individual address books for different mail clients or other applications. For example, some users might use Outlook as their mail client, while others might use Netscape Messenger or Lotus Notes. Maintaining address books for each software product requires some effort and many companies cannot afford this luxury. One solution is to maintain a single company-wide or cross-company directory that contains information about all employees, contractors, customers, and so forth. Then, whatever mail client is used to send an e-mail to one of these recipients, the recipient’s e-mail address can be easily retrieved from the central directory. An LDAP directory is the right choice, since most of the currently available mail clients support LDAP search capabilities.

In this lab, you use Outlook Express as the mail client, but the same theory could apply to any mail client. In fact, the IBM Redbook *Implementation and Practical Use of LDAP on the IBM @server iSeries Server*, SG24-6193, contains the configuration steps to set up Netscape Messenger and Lotus Notes to lookup e-mail addresses from an LDAP directory.

Objectives

Upon completion of this lab, you will be able to:

- Learn how add an account to a mail client to access one or more LDAP Directories
- Learn how to search one or more LDAP Directories for e-mail addresses

Lab environment

This environment includes:

- OS/400 V5R2 (5722-SS1)
- Outlook Express

Time required

The time required to complete this lab project is 15 minutes.

Task summary

In this lab, you perform the following tasks:

1. Add an account to access the LDAP Directory.
2. Search the LDAP Directory from Outlook to find e-mail addresses.

Task 1: Configuring Outlook mail clients to use LDAP

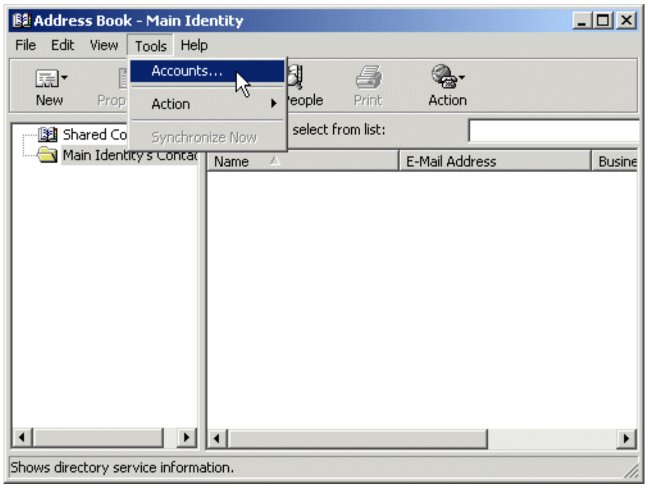
In this task, we configure the Outlook mail client to use your LDAP Directory to look-up e-mail addresses of people you created in this directory. To do this perform the following steps:

__ 1. From the desktop, click the **envelop** icon to open Outlook.

Figure 65. Open Outlook icon

__ 2. From the Outlook Express client, click **Addresses**.

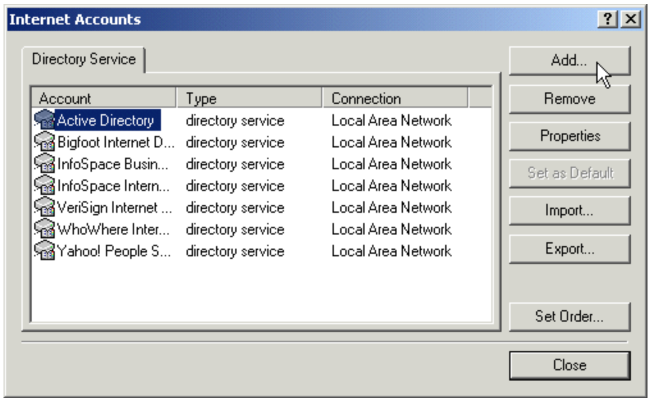
__ 3. From Outlook Express Address Book, click **Tools** and from the drop-down menu select **Accounts...** as shown in Figure 66.



Shows directory service information.

Figure 66. Creating a new account

__ 4. From Internet Accounts click **Add** as shown in Figure 67.



Account	Type	Connection
Active Directory	directory service	Local Area Network
Bigfoot Internet D...	directory service	Local Area Network
InfoSpace Busin...	directory service	Local Area Network
InfoSpace Intern...	directory service	Local Area Network
VeriSign Internet ...	directory service	Local Area Network
WhoWhere Inter...	directory service	Local Area Network
Yahoo! People S...	directory service	Local Area Network

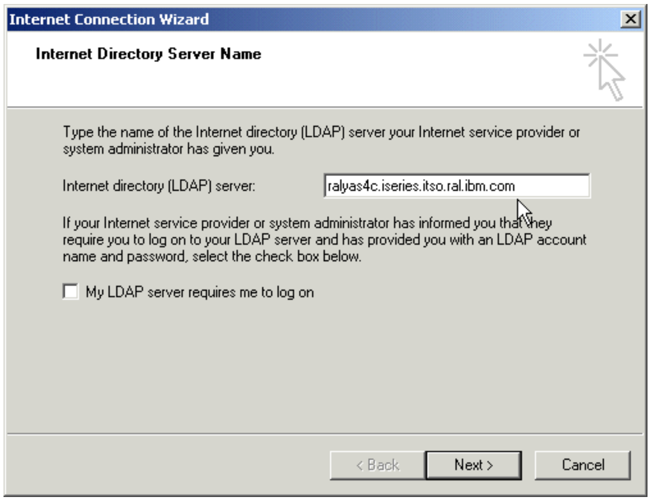
Figure 67. Adding a new directory service

__ 5. In the Internet (LDAP) Directory field, enter the fully qualified name of your LDAP server, **<Fully_Qual_ISeries_Name>**. As shown in Figure 68, the value used in our example is:

```
RALYAS4C.ISERIES.ITSO.RAL.IBM.COM
```

Make sure you use your own fully qualified LDAP server name.

We did not need to select the My LDAP server requires me to log on option because we do not require users to authenticate with this LDAP server.



Internet Directory Server Name

Type the name of the Internet directory (LDAP) server your Internet service provider or system administrator has given you.

Internet directory (LDAP) server: ralyas4c.iseries.itso.ral.ibm.com

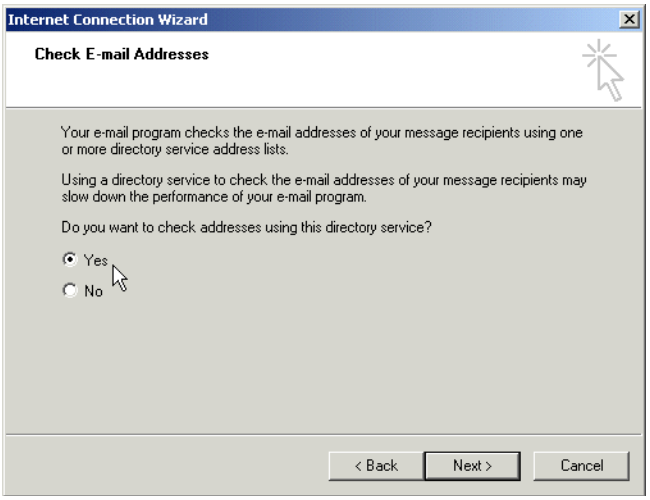
If your Internet service provider or system administrator has informed you that they require you to log on to your LDAP server and has provided you with an LDAP account name and password, select the check box below.

□ My LDAP server requires me to log on

Figure 68. Internet Directory (LDAP) Server

__ 6. Click **Next** to continue.

__ 7. On the Check E-mail Addresses window, select **Yes** because we do want to check this directory service for e-mail addresses as shown in Figure 10-11.



Check E-mail Addresses

Your e-mail program checks the e-mail addresses of your message recipients using one or more directory service address lists.

Using a directory service to check the e-mail addresses of your message recipients may slow down the performance of your e-mail program.

Do you want to check addresses using this directory service?

● Yes

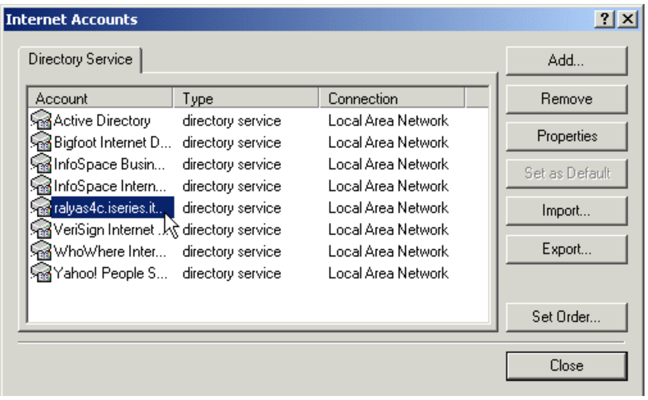
○ No

Figure 69. Checking e-mail addresses in this directory

__ 8. Click **Next** to continue.

__ 9. On the Congratulations window, click **Finish**.

You now see the new account in the directory service list as shown in Figure 70.

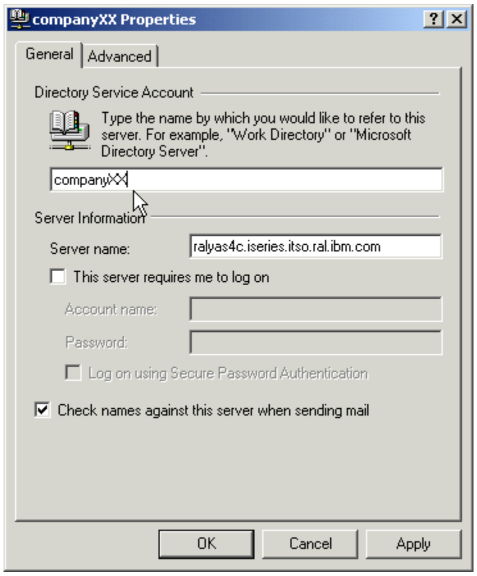


Account	Type	Connection
Active Directory	directory service	Local Area Network
Bigfoot Internet D...	directory service	Local Area Network
InfoSpace Busin...	directory service	Local Area Network
InfoSpace Intern...	directory service	Local Area Network
ralyas4c.iseries.it...	directory service	Local Area Network
VeriSign Internet ...	directory service	Local Area Network
WhoWhere Inter...	directory service	Local Area Network
Yahoo! People S...	directory service	Local Area Network

Figure 70. New directory service account

__ 10.Select your new Directory Service account and click **Properties**.

__ 11.In the first field, you can change the name of the Directory Service to the name of your organization `companyXX` (Remember to replace the XX with your team number.). See Figure 71.



Directory Service Account

Type the name by which you would like to refer to this server. For example, "Work Directory" or "Microsoft Directory Server".

companyXX

Server Information

Server name: ralyas4c.iseries.itso.ral.ibm.com

☐ This server requires me to log on

Account name:

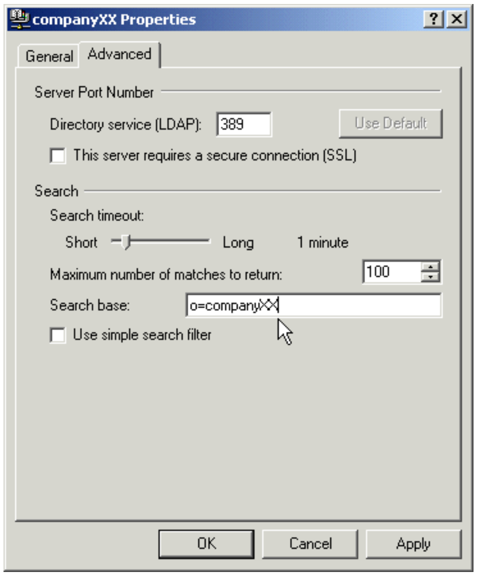
Password:

☐ Log on using Secure Password Authentication

☑ Check names against this server when sending mail

Figure 71. Changing the properties of the Outlook account

__ 12.Click the **Advanced** tab, and then change the Search base: field to the base DN of your LDAP directory. In our example, this is `o=companyXX` as shown in Figure 72. (Remember to replace the XX with your team number.)



Server Port Number

Directory service (LDAP): 389

□ This server requires a secure connection (SSL)

Search

Search timeout:

Short — Long 1 minute

Maximum number of matches to return: 100

Search base: o=companyXX

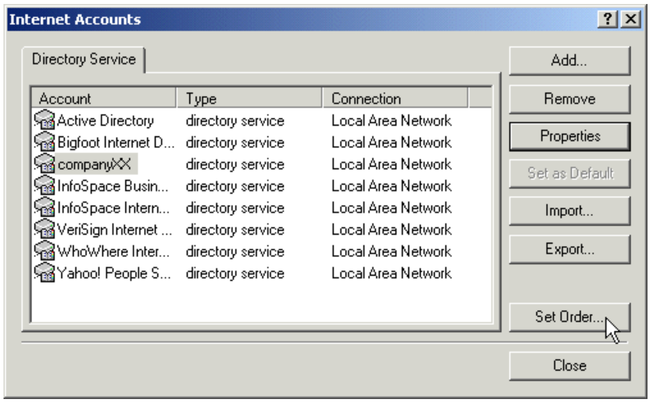
□ Use simple search filter

Figure 72. Changing Search base

Note: If you are using a Domino LDAP directory, the Search base is not required, but strongly recommended.

__ 13.Click **OK** to save and close.

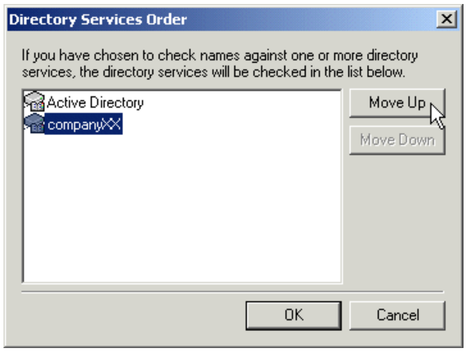
__ 14.You can set the order in which Directory Services are searched by clicking the **Set Order...** button on the Internet Accounts window, as shown in Figure 73.



Account	Type	Connection
Active Directory	directory service	Local Area Network
Bigfoot Internet D...	directory service	Local Area Network
companyXX	directory service	Local Area Network
InfoSpace Busin...	directory service	Local Area Network
InfoSpace Intern...	directory service	Local Area Network
VeriSign Internet ...	directory service	Local Area Network
WhoWhere Inter...	directory service	Local Area Network
Yahoo! People S...	directory service	Local Area Network

Figure 73. Setting the LDAP directory search order

__ 15.Select the directory you want to move. Then use the Move Up or Move Down buttons. In our example, we want to move the **companyXX** to the top by selected move up as shown in Figure 74.



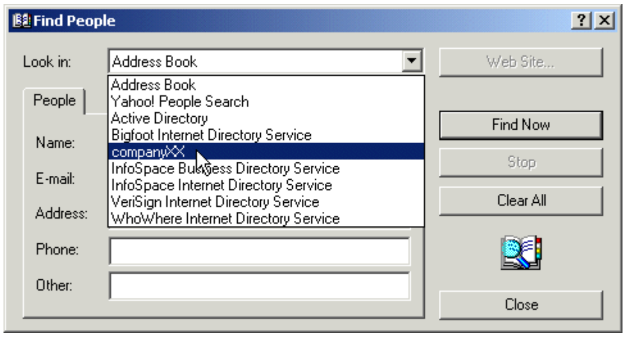
If you have chosen to check names against one or more directory services, the directory services will be checked in the list below.

Figure 74. Moving the directory up to search first

__ 16.Click **OK** to continue.

__ 17.Click **Close** to close the Internet Accounts window. From your Address Book, select **Find People**.

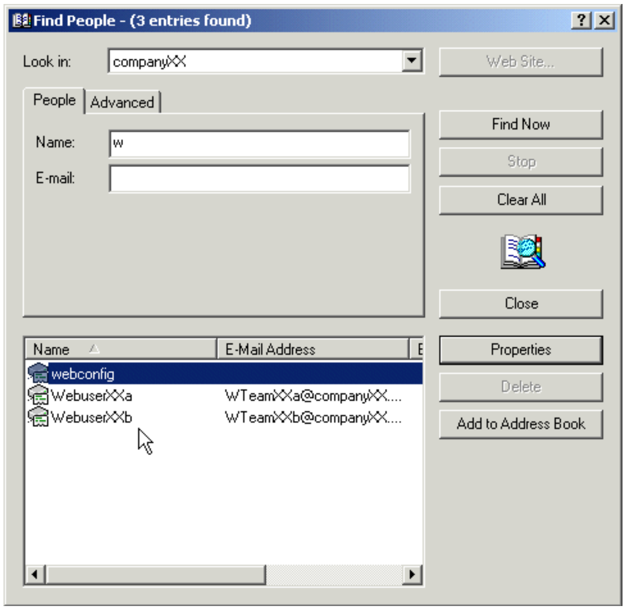
__ 18.Click the drop-down in the Look in: field and select the LDAP directory you want to search. In our example, we selected **companyXX** as shown in Figure 75. (Remember to replace the XX with your team number.)



Find People
Look in:
Address Book
Address Book
Yahoo! People Search
Active Directory
Bigfoot Internet Directory Service
companyXX
InfoSpace Business Directory Service
InfoSpace Internet Directory Service
VeriSign Internet Directory Service
WhoWhere Internet Directory Service
People
Name:
E-mail:
Address:
Phone:
Other:
Web Site...
Find Now
Stop
Clear All
Close

Figure 75. Selecting the directory to search for an e-mail address

__ 19.In the Name: field, enter at least one character of the recipients first or last name. Then click **Find Now**. In our example, we entered `w` as the search criteria and it returned three names from the companyXX LDAP directory, as shown in Figure 76.


Find People - (3 entries found)

Look in: companyXX

Name: w

E-mail:

Name	E-Mail Address
webconfig	
WebuserXXa	WTeamXXa@companyXX....
WebuserXXb	WTeamXXb@companyXX....

Figure 76. Search result

You could now select one or more entries to add to your address book. Note that the webconfig entry represents the entry containing the HTTP server configuration from the previous lab. In a typical implementation, you would store special purpose entries, such as the configuration of a Web server under a different subcontext in the directory tree as described in Implementation and Practical Use of LDAP on the IBM @server iSeries Server, SG24-6193.

To check an e-mail address in an LDAP directory while writing an Outlook Express e-mail, follow these steps:

__ 20.Close the Address Book.

__ 21.Click **New Mail** from the Outlook toolbar.

__ 22.Click the **Address Book** icon before typing the users e-mail address, as shown in Figure 77.

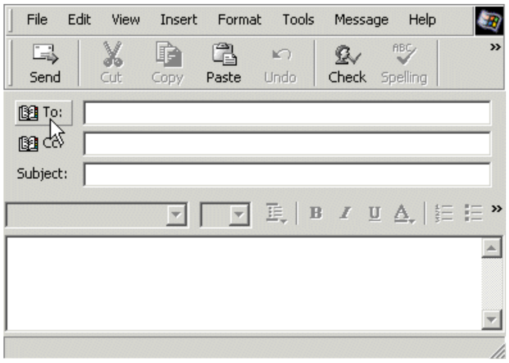


Figure 77. Address Book icon

__ 23.On the Select Recipients window, click **Find**...

__ 24.On the Find People window, select the LDAP directory of **companyXX**. Type at least one character, which in our case could be `w`. Then click **Find Now**.

__ 25.Once it has found the user(s) based on your search criteria, you can select the name required. Then click **To, Cc**, or **Bcc**.

> **Restriction**
>
> Check Name will only check for names in your local address book. It will only go on to list names in the first LDAP directory if there are no names in your local address book that meet your search criteria. Using the above method ensures you get all recipients from the selected LDAP directory that meet your search criteria.

__ 26.Close all windows.

Congratulations! You have finished all labs and should now be able to implement and use LDAP directory services on your iSeries server. Remember, you can find the introductions and detailed instructions to all topics covered in this hands-on lab guide in *I*mplementation and Practical Use of LDAP on the IBM @server iSeries Server, SG24-6193.

Answers to the lab questions

This section contains the answers to the questions asked in the various lab tasks.

Lab 1. Configuring OS/400 Directory Services

This section provides the answers to questions presented in Lab 1.

Task 1, "Configuring a suffix using iSeries Navigator" on page 1

Question 1, "What is stored in the Database Library?" on page 3

The database library contains the journal files and other objects for the directory.

Question 2, "What are suffixes used for?" on page 3

The suffix is a representation for a root entry in a directory. A suffix specifies the Distinguished Name (DN) for the root of a directory name. In our example, this is o=companyXX, but could be ou=rochester,o=ibm,c=us.

A server for multiple departments may have multiple suffixes. Requests to the server must specify a DN with a suffix that matches one of the server's suffix strings.

Question 3, "What are the database connections used for?" on page 3

Database connections specifies the number of connections that the directory server can create to the underlying database. This effects the number of requests that the directory server can simultaneously perform.

Lab 2. Introducing the Directory Management Tool

This section provides the answers to questions presented in Lab 2.

Task 3, "Changing the Directory Management Tool settings" on page 14

Question 1, "As in step __ 2. on page 14, an error message is still displayed as shown in Figure 22 on page 15. Why do you still receive this message even after you change the configuration?" on page 17

This message is received because we do not have a local LDAP configured. You will always receive this message because the localhost must be in the configuration file or DMT will not start.

Task 5, "Viewing object classes using DMT" on page 21

Question 1, "What are three optional attributes of the organizationalPerson object class?" on page 22

street
registeredAddress
title
destinationIndicator
facsimileTelephoneNumber

internationalISDNNumber
l
ou
physicalDeliveryOfficeName
postalAddress
postalCode
postOfficeBox
preferredDeliveryMethod
st
telexNumber
teletexTerminalIdentifier
x121Address

Question 2, “What is the Superior object class for organizationalPerson?” on page 23

person

Question 3, “What are two required attributes of the Person object class?” on page 23

- common name (cn)
- surname (sn)

Question 4, “What is the Superior object class for Person?” on page 23

top

Question 5, “What is the required attribute of Top object class?” on page 23

objectclass

Question 6, “If you wanted to add a person with an object class of organizationalPerson, what would the required attributes be?” on page 23

- object class
- common name
- surname

Lab 3. Using LDIF to manage your directory

This section provides the answers to questions presented in Lab 3.

Task 2, “Using the LDAP search commands in Qshell” on page 27

Question 1, “Why don’t you see the homePostalAddess you entered in the LDIF file?” on page 27

The attributes in SecureWay have, by default, three security classes:

- Normal
- Sensitive
- Critical

homePostalAddress is *sensitive*, and therefore, by default, is not listed by anyone other than the administrator. However, access may be given to others by the administrator.