

LDAP Authentication with PeopleTools

An Oracle Red Paper
July 2007



Table of Contents

TABLE OF CONTENTS	2
CHAPTER 1 – RED PAPER INTRODUCTION	6
Structure of this Red Paper	6
Related Materials	6
CHAPTER 2 - OVERVIEW OF HOW LDAP AUTHENTICATION WORKS	7
The PeopleSoft Signon Process	7
Signon PeopleCode	8
Business Interlinks	8
Component Interfaces	8
CHAPTER 3 - SETTING UP LDAP AUTHENTICATION ON PEOPLETOOLS 8.1X & 8.2X	10
Step 1 – Set up Directory Authentication	10
Step 2 – Setup Mandatory User Profile Caching	13
Step 3 – Set up Option User Profile Caching	16
Step 4 – Set up Signon PeopleCode	18
Step 5 – Test Test Test!!!	20
Directory Group Import	22
CHAPTER 4 - SETTING UP LDAP AUTHENTICATION ON PEOPLETOOLS 8.4X.....	26
Step 1 – Configure Directory	26
Step 2 - Test Connectivity	29
Step 3 - Caching the Directory Schema	30
Step 4 – Setup Authentication Map	31
Step 5 – Setup User Profile Map	33
Step 6 – Setup Signon PeopleCode page	37
Step 7 – Test Test Test!!!	39
Directory Role Rules for Dynamic Role Assignment	41
APPENDIX A - SETTING UP SSL FOR LDAP AUTHENTICATION	47
Very Brief Introduction to SSL.....	47
Using LDAP with SSL.....	47
Step 1 - Placement of the cert7.db and other required SSL files	48
Step 2 -Configuring Business Interlinks	56
Setting up SSL Token on an iPlanet 5.1 server	61

Setting up SSL Token on an Novell eDirectory server	69
<hr/>	
APPENDIX B – TROUBLESHOOTING TIPS & TOOLS	73
How to use the Business Interlink Tester	73
How to use the LDAPSEARCH tool	76
<hr/>	
APPENDIX C – GSC LDAP SOLUTIONS	83
<hr/>	
APPENDIX D - Q & A	85
<hr/>	
APPENDIX E – DIRECTORY TECHNICAL OVERVIEW.....	88
Definitions	88
DIT and Schema	88
Distribution and Replication	92
Technical Overview Summary	92
<hr/>	
APPENDIX F – ADDENDUM OF UPDATED VERSIONS	93



July 2007

Author: Tom Lenz

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:

Phone: +1.650.506.7000

Fax: +1.650.506.7200

oracle.com

Copyright © 2007, Oracle. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice.

This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Copyright 2004 PeopleSoft, Inc. All rights reserved.

Restricted Rights

The information contained in this document is proprietary and confidential to PeopleSoft, Inc.

Comments on this document can be submitted to redpaper@peoplesoft.com. We encourage you to provide feedback on this Red Paper and will ensure that it is updated based on feedback received. When you send information to PeopleSoft, you grant PeopleSoft a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose without the express written permission of PeopleSoft, Inc.

This document is subject to change without notice, and PeopleSoft does not warrant that the material contained in this document is error-free. If you find any problems with this document, please report them to PeopleSoft in writing.

This material has not been submitted to any formal PeopleSoft test and is published AS IS. It has not been the subject of rigorous review. PeopleSoft assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by PeopleSoft for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

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

PeopleSoft may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

PeopleSoft, PeopleTools, PS/nVision, PeopleCode, PeopleBooks, PeopleTalk, and Vantive are registered trademarks, and Pure Internet Architecture, Intelligent Context Manager, and The Real-Time Enterprise are trademarks of PeopleSoft, Inc. All other company and product names may be trademarks of their respective owners. The information contained herein is subject to change without notice.

Chapter 1 – Red Paper Introduction

This Red Paper is a practical guide for technical users, installers, system administrators, and programmers who implement, maintain, or develop applications for your PeopleSoft system. In this Red Paper, we discuss guidelines on how to diagnose a PeopleSoft Online Transaction environment, including PeopleSoft Internet Architecture and Portal configuration. Configuration of Batch processes is not covered in this document.

Much of the information contained in this document originated within the PeopleSoft Global Support Center and is therefore based on "real-life" problems encountered in the field. Although every conceivable problem that one could encounter with Tuxedo, the PeopleSoft Application Server, or your web server is not addressed in this document, the issues that appear in this document are the problems that prove to be the most common or troublesome.

STRUCTURE OF THIS RED PAPER

This Red Paper provides guidance in properly configuring LDAP for use with PeopleTools. Depending on the needs of your site, this can be a long complex process or one that is relatively straight forward. It is highly recommended that you also review your directory documentation and how it is setup based on your company's needs. You need to become very familiar with how the LDAP directory functions in order to properly setup PeopleSoft authentication to work with it.

Keep in mind that PeopleSoft updates this document as needed so that it reflects the most current feedback we receive from the field. Therefore, the structure, headings, content, and length of this document is likely to vary with each posted version. To see if the document has been updated since you last downloaded it, compare the date of your version to the date of the version posted on Customer Connection.

RELATED MATERIALS

This paper is not a general introduction to environment tuning and we assume that our readers are experienced IT professionals, with a good understanding of PeopleSoft's Internet Architecture. To take full advantage of the information covered in this document, we recommend that you have a basic understanding of system administration, basic Internet architecture, relational database concepts/SQL, and how to use PeopleSoft applications.

This document is not intended to replace the documentation delivered with the PeopleTools 8.14 or 8.42 PeopleBooks. We recommend that before you read this document, you read the PIA and LDAP related information in the PeopleTools PeopleBooks to ensure that you have a well-rounded understanding of our PIA and LDAP technology. Note: Much of the information in this document eventually gets incorporated into subsequent versions of the PeopleBooks. Many of the fundamental concepts related to PIA and LDAP are discussed in PeopleSoft PeopleBooks.

Chapter 2 - Overview of how LDAP authentication works

Before we begin let's get one thing straight; LDAP is a protocol not a Directory. **LDAP** stands for **Lightweight Directory Access Protocol**. A Directory may or may not be LDAP compliant. In order to work with PeopleSoft the directory **MUST** be LDAP V3 compliant. V3 stands for version 3, which is currently the industry standard for this protocol.

So obviously your first question might be "What LDAP Directories does PeopleSoft Certify?"

PeopleSoft currently **only** certifies **Novell's NDS and eDirectory, Sun One's (formerly iPlanet) Directory Server, and Microsoft's Active Directory** at this time. As of PeopleTools 8.46 we started supporting **Oracle's Internet Directory**. **PeopleSoft does not certify ANY and ALL LDAP V3 compliant directories**, although we maintain that the LDAP Business Interlink will work with any LDAP V3 compliant directory therefore support on some may be limited but we will do all we can to help you get authentication working on whatever directory you choose to work with as long as it is V3 compliant.

For all other V3 compliant directories it is up to the customer to figure out the scheme to get it to work with PeopleSoft. If you are using a directory other than the directories mentioned earlier, you might want to contact PeopleSoft consulting as they have worked with several others. Currently Open LDAP has some issues when it comes to connecting over SSL.

Then your second question might be "Who's directory should you use?"

That is entirely up to you! There are many vendors that sell LDAP V3 compliant directories; Novell, iPlanet (Netscape/Sun Alliance), and Microsoft, and several vendors with "me too" entries in the market; Oracle and IBM are the most notable. Also, the major messaging solutions such as Microsoft Exchange and Lotus Notes have LDAP V3 compliant directories built in. The directory market can be divided into 2 distinct segments, (1) the NOS/LAN Administration/Intranet segment, and (2) the B2B/eCommerce/Internet segment.

And your third question is probably "Why should we use a directory?"

Here you might want to jump to **Appendix E** and see the technical overview of a directory and its use, but to summarize a directory is used as a information store, such as a phone book, to hold your company user information to be used in a number of applications, not only with PeopleSoft.

THE PEOPLESOFT SIGNON PROCESS

The following six steps will walk us through the PeopleSoft signon process and explain where the Signon PeopleCode comes into play here.

1. As is the process in ALL PeopleSoft applications, the user signs on with their User ID & Password and the system then validates the ID & password against the PSOPRDEFN table. If ID & Password are valid, then the user is successfully signed on. This will be done no matter what type of authentication process you are going to use. You cannot get around this, as this is the way the application is designed to work.
2. If the initial signon authentication against the PSOPRDEFN table is **unsuccessful**, then the system checks to see if **LDAP Authentication Signon PeopleCode** is enabled. If it is not, then the user is denied access assuming that the user is trying to authenticate with their LDAP user id and password.

3. If the **LDAP Authentication Signon PeopleCode** is enabled, then system invokes LDAP authentication with the directory via the LDAP_SEARCH and LDAP_BIND Business Interlinks.
4. Using these business interlinks the Signon PeopleCode will then validate the User ID & Password against the directory using the values you have setup in the directory authentication setup pages, which will be described in the following chapters.
5. If the Directory does not validate the User ID & password, then the Directory Authentication fails, the PeopleSoft Authentication fails, and the user is denied access. This failure could happen for a number of reasons, as you will see in the following chapters.
6. However, if the directory authentication is successful, then a user profile is created using the USER_PROFILE Component Interface, assuming you have the USER_PROFILESYNCH is enabled as part of your LDAP authentication setup, the PeopleSoft Authentication is validated, and the signon is successful.

NOTE: LDAP AUTHENTICATION WILL NOT WORK FOR USERS THAT REQUIRE A 2-TIER LOGIN. This is because Signon PeopleCode can ONLY be executed in 3-tier. If you have users that require 2-tier-logon access then you will need to create a separate (Developer) account for these users that only give the access they need in 2-tier. There are only a handful of actions that require a 2-tier access. Most development can still be performed on the 3-tier client instead of 2-tier.

SIGNON PEOPLECODE

There are three technologies used during this signon process and they are signon peoplecode, business interlinks, and USER_PROFILE component interface.

Signon PeopleCode is the ability to execute peoplecode during the signon process. Any peoplecode program can be executed at signon time. PeopleSoft delivers LDAP Authentication Signon PeopleCode as of PeopleTools 8.

LDAP Authentication Signon PeopleCode uses the LDAP Business Interlink and the USER_PROFILE Component Interface (UPCI) to verify the USER NAME and PASSWORD and automatically update or create the user profile information in the PeopleSoft database if it does not already exist.

BUSINESS INTERLINKS

Business Interlinks are a Tools technology that expose external systems to peoplecode programs. PeopleSoft 8 delivers several Business Interlinks as well as a Business Interlink SDK so customers/partners can develop their own Interlinks. The LDAP_SEARCH and LDAP_BIND Business Interlinks are called by Signon Peoplecode for LDAP authentication and come delivered, ready to use, with PeopleSoft 8.

The LDAP Business Interlink provides an Application Programming Interface (API) to LDAP with peoplecode. The API is used to access LDAP compliant directories.

COMPONENT INTERFACES

Component Interfaces are another tools technology, which greatly expands the use of peoplecode. Component Interfaces are used to provide an API for accessing a PeopleSoft Component (i.e. collection

of pages) with peoplecode. The **USER_PROFILE Component Interface** provides a peoplecode API for the USER_PROFILE Component. This API can be used in peoplecode programs to manage user profiles. Business Interlinks provide the external access out of PeopleSoft. Component Interfaces provide the internal access into PeopleSoft.

The combination of these three technologies, explained above, provides a flexible way to configure PeopleSoft for integration with your directory server. No set schema is required in the directory. Instead, you are free to customize and extend the Signon PeopleCode to work with any schema implemented in your directory server.

This should have given you a brief overview of how the authentication process works. One thing to mention before we move on is that if you are not already familiar with your directory and its attributes please become familiar before you go on. Taking your Directory Administrator to lunch, to discuss the workings of your directory, would be a good idea because you should have a good working relationship in order to get PeopleSoft LDAP authentication to work...**Now on with the show!**

Chapter 3 - Setting Up LDAP Authentication on PeopleTools 8.1x & 8.2x

This chapter will take you on a step-by-step, page-by-page, walkthrough on how to correctly setup your PeopleSoft application to authenticate against your LDAP compliant directory in PeopleTools 8.1x and 8.2x.

Depending on which directory you choose to use Novell, Microsoft, or Netscape the actual attribute names may be different, but the functionality is the same. Please become very familiar with the directory attributes you will be using in the next few pages and chapters. This will save you a lot of time and headaches.

STEP 1 – SET UP DIRECTORY AUTHENTICATION

The first thing you need to do is to navigate to the PeopleTools > Maintain Security > Setup > Directory Authentication page. The following screen shots are an example of Microsoft's Active Directory however using Sun One or Novell's eDirectory you will use the same setup except for the naming of some of the LDAP attributes or search base.

[Home](#) > [PeopleTools](#) > [Maintain Security](#) > [Setup](#) > **Directory Authentication**

Directory Setup

☒ **Use Directory Authentication**
☒ **Trust Web Authentication**

Directory Connect Information

Server name: PTNTLDAP01

Port: 389

User DN: cn=administrator,cn=users,dc=ptntldap,dc=com


Password: *****

User Search Information

Scope
☒ SUB
☐ ONE
☐ BASE

Search Base: dc=ptntldap,dc=com

Search Attribute: sAMAccountName

 Save

Now we will step through each field on this page and describe what it is used for. All values must be correct and not mistyped or you will not be able to get the signon PeopleCode to talk to your directory correctly.

Use Directory Authentication: Check this box is to enable directory-based authentication into PeopleSoft. (Note: This checkbox also toggles the Enabled checkbox for the LDAP_Authentication row on the Signon PeopleCode page). You MUST check this box to get LDAP authentication to work. At some point you will need to bounce the app server when you are finished with the setup to invoke the signon Peoplecode that is enabled with this checkbox.

Trust Web Authentication: Check this box to enable external web authentication. . (Note: This checkbox also toggles the Enabled checkbox for the WWW_Authentication row on the Signon PeopleCode page). If you are using a third party authentication product like Kerberos or SiteMinder then you will want to use this box and not the Directory Authentication box. Or you can create your own signon PeopleCode. You do not have to check this box if you already checked the Directory Authentication box. But checking both boxes will not hurt either so the choice is yours.

Server name: This is the DNS name (or IP address) of the LDAP directory server (for example, ldap.peoplesoft.com or 192.202.185.90). In PT 8.1x and 8.2x we only allow a place for one server. See **Appendix C** for a solution how to customize this to allow for multiple fail over servers. In PT 8.4x the option is already built in.

Port: This is where you specify the Port number of the LDAP server. The industry standard LDAP port is 389. Port 636 is the industry standard SSL port. You can use any ports available to you if you wish. In Active Directory you may choose to use the Global Catalog port of 3268 or 3269 for SSL as another option.

User DN: The Distinguished Name of directory based account with “Browse” rights to ObjectClass=Person entries and “Read” rights to all needed attributes. **This is one of the first places that we find a mistake.** You may not be using a valid account, or the directory account does not have the rights to read all attributes in the directory. PeopleSoft suggests you use an administrator account but that is not always necessary. The DN is the full path to the user, for example cn=administrator,cn=users,dc=peoplesoft,dc=com which means that this user is located in the container called users under the domain called peoplesoft.com. If you chose to make an anonymous bind to the directory and your directory allows for an anonymous search then you would leave the DN and password fields blank. However as of PeopleTools 8.22 a connect ID is required if attempting to make an anonymous bind. Prior versions did not require this. Be sure to verify if your directory allows an anonymous bind or not.

Password: This is the directory password for User DN. This is important to key in the correct case of the password here and if you use no password then you are making an anonymous bind to the directory. PeopleSoft suggests **not** using anonymous to bind to your directory.

Note: There is a known issue with this page that requires you to re-key the password for the connect DN every time you make a change and save this page. Otherwise your authentication could fail on this minor technicality.

Scope: The scope of the search, which can be one of these values:

Base retrieves information only at the level of your search base. It will not look deeper in you directory for users.

One retrieves information about entries one level below the base.

Sub retrieves information about entries at all levels below the base. The base entry is included in this scope. If no scope is specified, the server performs a base search. PeopleSoft suggests using the sub scope, as it will give you more leverage in your directory tree structure.

Search Base: **This is the second place we have found most errors occurring.** The search base is the container or starting point in the directory that you want to start your search for users. You MUST include the whole DN path for this location for example if all your users are in a container called “Users” and this is located under your root domain of PeopleSoft.com then your search base would look something like this: cn=users,dc=PeopleSoft,dc=com. You can start your search base at the root or your

directory (dc=PeopleSoft,dc=com) however we suggest that you start one container lower in your directory tree and this is for performance purposes. If you start at the root level you may run into issues with unfollowed referrals as noted in a solution about performance and UNIX on **Appendix C** of this red paper.

Search Attribute: **This is the third place we have found confusing information and errors.** The search attribute is the directory attribute of ObjectClass=Person to which the provided User ID should be matched. For example the **uid** (Unique Identifier) **or sAMAccountName** (Active Directory's version of the uid) depending on the directory you are using. This is also the value the user will be typing in at the PeopleSoft logon page. If they were using their email address or employee number to logon to PeopleSoft, then you would need to use the correct directory attribute so the search in the directory will return the right user information like mail or employee number. Again we cannot stress enough that you should become very familiar with the directory attributes you will be using.

Now that you are sure you have entered all the correct data let's move on to step 2.

STEP 2 – SETUP MANDATORY USER PROFILE CACHING

In this step you will need to navigate to the PeopleTools > Maintain Security > Setup > User Profile Caching page.


[Home](#) > [PeopleTools](#) > [Maintain Security](#) > [Setup](#) > [User Profile Caching](#)


Mandatory User Properties

Optional User Properties


☒ **Read Profiles from Directory**
☒ **Cache when SSO token present**

***User ID Attribute:**

***Symbolic Id:** 

***Role Name:** 

ID Type



***ID Type:**  None

***ID Type Attribute:**

Language

☒ **Use Default Language Code** **Language Code:**

LangCD Attribute:

[Mandatory User Properties](#) | [Optional User Properties](#)

Again we will step through each field on this page, as we did on the last page, and describe what it is used for. All values must be correct and not mistyped or you will not be able to get the signon PeopleCode to talk to your directory correctly. Regardless whether or not you will be creating and updating users in PeopleSoft or only using your directory for authentication purposes, all the mandatory fields on this page, marked by an asterisk *, must be completed in order for LDAP authentication to work.

Read Profiles from Directory: This checkbox is used for invoking the USER_PROFILE Component Interface, through Signon PeopleCode, to create or update user Profiles in PeopleSoft. You must have this checked in order to create or update user profiles. This checkbox also toggles the “Enabled” checkbox for the LDAP_PROFILESYNCH found on the Signon PeopleCode page. At some point you will need to bounce the app server, when you are finished with the setup, to invoke the signon PeopleCode that is enabled with this checkbox.

Cache when SSO token present. This is checked when you will be using single signon with LDAP authentication. Meaning if you are setting up LDAP authentication on several different environments and you want the user to be able to logon seamlessly to all the other environments, but only authenticate

against the first environment, then you would check this box in all the other environments. The system authenticates the user's single signon token. This checkbox enables the SSO_Authentication row on the Signon PeopleCode page in PeopleTools Utilities. At some point you will need to bounce the app server when you are finished with the setup to invoke the signon PeopleCode that is enabled with this checkbox. You will also need to setup the PeopleSoft node single signon to get this authentication to work correctly.

User ID Attribute: This is the directory attribute containing the value that will be used as the PeopleSoft OPRID on the PSOPRDEFN table. So once the search attribute, on the last page is found, the signon PeopleCode then binds to this directory attribute. This is also the value that will be updated or created in PeopleSoft if you are using the USER_PROFILE component interface. So if your uid or sAMAccountName, in the directory, were **jsmith** then the OPRID in PeopleSoft would be searching for, or creating would be **JSMITH**.

Note: Although the directory is case insensitive the delivered peoplecode will ALWAYS force UPPER CASE when returning from the directory and searching the PSOPRDEFN table for this user or when creating the user in the PSOPRDEFN table. So you will notice that your users get created in upper case regardless of their case in the directory. See possible solution in **Appendix C** to make changes to this delivered functionality.

Symbolic ID: This must contain the value of the valid symbolic ID for your database. Although Symbolic ID is not used for 3-tier connections it is still a required property field when creating a new User Profile through the USER_PROFILE component interface in PeopleTools 8.1x and 8.2x.

Role Name: This is the default Role you will be assigning to your newly created users. This role cannot have any spaces in it on PT 8.1x and 8.2x. Role membership can be updated automatically by executing Dynamic Role Rules. Therefore since this role will be used by all directory users, or get assigned to the user when they first attempt to logon, this role must have the correct access, Menu, Page, web library, etc. to logon to PeopleSoft. This is where we find a lot of issues also in that if this is the only role assigned to the user and they cannot logon, it may be because this role is too limited in it's access.

ID Type: This is the default ID Type for newly created users. We suggest you first try this with NON (none). Once you have established LDAP authentication and you want to change this to EMP (emplid) you may but bear in mind that when using the value of EMP you must also have the ID Type Attribute value filled with the user's correct employee number.

ID Type Attribute: The name of the LDAP attribute containing valid data for the given ID Type. If using NON then this field is grayed out and no value is required. However, if you are using the EMP ID type then the directory attribute named here must contain the same value on the user profile of the directory as the EMPLID value in the PS_PERSONAL_DATA table in PeopleSoft contains for this user, as there is a cross reference to the employee when the user is created. So if you are using EMP as the ID Type and the ID Type Attribute is employeenumber (which would need to be a valid attribute in your directory) then this value on the employeenumber attribute in the directory would have to match the EMPLID for this user on the PS_PERSONAL_DATA table in order to correctly cross reference and update or create the user profile. See solutions on **Appendix C** for more information regarding this issue.

Use Default Language Code: Check this box if you do not maintain language codes in the directory.

Language Code: Default language code to use if not taken from the directory.

Language Code Attribute: The name of the LDAP attribute containing a valid language code. The value retrieved from the attribute must be a valid PeopleSoft language code.

Reminder: Again you need to be familiar with these attributes you will be using in order to verify all the fields in PeopleSoft are correct or you will run into issues with this setup.

Now let's move to step 3.

STEP 3 – SET UP OPTION USER PROFILE CACHING

In this step you will need to navigate to the PeopleTools > Maintain Security > Setup > User Profile Caching and choose the Optional User Properties page.

[Home](#) > [PeopleTools](#) > [Maintain Security](#) > [Setup](#) > [User Profile Caching](#)

Mandatory User Properties

Optional User Properties

General

☒ User Descr

LDAP Attribute:

cn

☒ Email

LDAP Attribute:

mail

☐ Currency Code

LDAP Attribute:

Permission List

☐ Navigator HomePage

LDAP Attribute:

☐ Process Profile

LDAP Attribute:

☐ Primary

LDAP Attribute:

☐ Row Security

LDAP Attribute:

Workflow Attributes

☐ FormID

LDAP Attribute:

☐ Supervising UserID

LDAP Attribute:

☐ ReassignWork

LDAP Attribute:

Routing Preferences

☐ WorkList User

LDAP Attribute:

☐ Email User

LDAP Attribute:

☐ Forms User

LDAP Attribute:

Save

[Mandatory User Properties](#) | [Optional User Properties](#)

The directory attributes you choose here are optional and will only be used to when creating or updating the user profile using the USER_PROFILE component interface by checking the checkbox called “read profiles from directory” on the previous page.

NOTE: We have only found one issue here and that seems to be with the cn attribute. If you are not using the cn (Common Name) attribute in your directory, or as a value in your search then make sure that before unchecking the user descr checkbox, you change the value to something like uid or sAMAccountName, then uncheck the box and save. For some reason this cn value is hard coded and tends to cause some issues in some customer’s environments when trying to update or create user profiles.

It is your decision to utilize this page or not. There are no mandatory fields on this page therefore you can skip it if you don't need these values updated to or created on a user profile. You are limited, at this time, to the actual fields represented on this page. You may also get errors if you use the same directory attribute for more than one value. See **Appendix C** for solutions on this.

STEP 4 – SET UP SIGNON PEOPLECODE

In this step you will need to navigate to the PeopleTools > Utilities > Use > Signon PeopleCode. The following page holds the signon PeopleCode used with LDAP. LDAP_AUTHENTICATION is used with the authentication against the LDAP directory. LDAP_PROFILESYNCH is used for creating a user for the LDAP user in PSOPRDEFN. It is strongly recommended that you use the “Invoke As” option if you are using LDAP. The “invoke as” user MUST have full access to a Component Interface called USER_PROFILE.

IMPORTANT NOTE: Any change made to the signon PeopleCode page requires a reboot of your application server.

[Home](#) > [PeopleTools](#) > [Utilities](#) > [Use](#) > [Signon PeopleCode](#)

[New Window](#)

Signon PeopleCode

Signon

☐ Invoke as user signing in

☒ Invoke as User ID: Password:

*Sequence	Enabled	*Record	*Field Name	Event Name	Function Name	Exec	Auth Fail
1	<input type="checkbox"/>	FUNCLIB_PWDCTL	PWDCTL	FieldChange	Password_Controls	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	WWW_AUTHENTICATION	<input type="checkbox"/>	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	LDAP_AUTHENTICATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	SSO_AUTHENTICATION	<input type="checkbox"/>	<input type="checkbox"/>
5	<input checked="" type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	LDAP_PROFILESYNCH	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Here we will explain what all the fields, on this page, are used for.

Invoke as user signing in. This radio button is used for normal PeopleSoft authentication. When using LDAP authentication you will want to use the “Invoke as” radio button as described below. Using this option the user must enter the user id in the correct case as found on the PSOPRDEFN table or the authentication will fail to find the user.

Invoke as. By choosing this option it will make the signon process for the User ID case insensitive. When using LDAP authentication PeopleSoft suggests that you use this option and not the "Invoke as user signing in". There are other reasons for this choice as well. When a PeopleCode program runs, it has to have a context of a user. This is how you indicate to the system the user who is executing the program. This is important because the user ID provided needs to have access to all of the objects that your signon program uses. For instance, when you are using LDAP authentication the signon peoplecode contains a business interlink and a component interface. If the user ID provided does not have the appropriate authority to business interlinks or component interfaces, the program fails to execute the desired function. Whether you use the value of the user signing in or you create a default user ID for all signon attempts depends on your implementation.

With that said what you will want to do is create a permission list called LDAP, on that permission list the ONLY 2 things you need to do is 1) on the general tab make it so the permission list does not time out. 2) On the Component Interface tab add the Component Interface called USER_PROFILE, edit this and give "Full Access" to all options. Save this permission list.

Now, create a role and call it LDAP and assign this LDAP permission list, which you just created, to this role.

Last, Create a user called LDAP; give it a password, and ID type of none, and the LDAP role.

Place this user and password on the Signon PeopleCode page as the "Invoke As" user.

IMPORTANT: You must bounce the app server for this to take affect. Never worry about this user or their password again! Because this user cannot logon to PeopleSoft in any tier, you will not have to worry about its misuse. This user is ONLY used to update LDAP authenticated user profiles.

Sequence. The sequence column shows you the sequence in which your signon programs execute. You can change the sequence by changing the numerical value in the edit box.

Enabled. To enable a program to run at signon, check the Enabled checkbox. If it is not checked, then the system ignores the program at signon. You MUST enable # 3 FUNCLIB_LDAP LDAP_AUTHENTICATION for this to work If you want users to be created or updated when they logon via LDAP then you have to also enable # 5 FUNCLIB_LDAP LDAP_PROFILESYNCH and then bounce the app server.

Record. Specify the record on which you record PeopleCode exits.

Field Name. Add the specific field that contains the PeopleCode.

Event. Add the event that triggers a particular program.

Function Name. Add the name of the function to be called.

Note: Unless you are writing your own Signon PeopleCode or editing the delivered signon PeopleCode, you will not have to make any changes to the record, field, event, or function.

Exec Auth Fail. You MUST have this box checked in order for LDAP authentication to work. This column means "execute if PeopleSoft authentication fails." This means that even if PeopleSoft does not authenticate the user, you still want the program to run. For instance, if you write an LDAP authentication program, you want it to run after PeopleSoft denies access so that your program can authenticate the user instead. Also, you can leave this option unchecked to further secure your system. For instance, if you are not using LDAP authentication, leaving this option unchecked prevents any program or script from running if your PeopleSoft authorization fails, and not user could log on.

STEP 5 – TEST TEST TEST!!!

In order to verify that you have setup everything correctly the best thing to do at this time is test it. There are a couple simple tests you can do to see if your setup was as easy as it seemed.

Test # 1 – PeopleSoft authentication and default role test

Create user Known to PeopleSoft and your LDAP directory. Make the OPRID in Upper Case. Give the user a different password in PeopleSoft than their LDAP directory password. Give the user the default role you are using in your LDAP setup (Mandatory User Properties page). Using the PeopleSoft password first try to logon. This will test the role you have assigned as your default role to see if it has the rights needed to logon to PeopleSoft.

If this test fails then you need to reevaluate the default role and the permission lists assigned to this role. Remember in PeopleTools 8.1x and 8.2x the default role cannot have any spaces in the name.

Test # 2 – LDAP Authentication test

After you have successfully completed test 1 try to logon using the same ID and their LDAP directory password. This will test the signon PeopleCode Authentication process.

If this test fails then there is a problem with one of the following things:

- a) Network connectivity to the directory server
- b) The User DN for the search does not have rights to read all attributes in the directory
- c) The User DN account is locked out
- d) The signon user does not exist in the directory
- e) The signon user account in the directory is locked out
- f) The signon user's password is wrong
- g) The search attribute on the Directory authentication page or the User ID Attribute on the user profile caching page may be incorrect.

Also remember that you needed to bounce the app server after setting up your signon peoplecode page.

If this test is not successful jump ahead to **Appendix B – Troubleshooting**. Here you will find ways of validating all your settings.

Test # 3 – User Profile Creation test

Assuming your first 2 tests worked successfully, and you have invoked the LDAP_PROFILESYNCH signon PeopleCode, delete the OPRID you created from PeopleSoft and try logging in again as that user using their LDAP directory password.

This will test the User Profile Component Interface to see if a user, not known to PeopleSoft, can be created with the default values found on the Mandatory and Optional User Properties pages.

Here are some SQL statements that may help in validating the values in the PeopleSoft tables that are related to your LDAP setup.

```
select * from PSSIGNONPPC - Signon PeopleCode page
select * from PS_DIRECTORYSETUP - Stores Directory Authentication Information
select * from PS_LDAPMAP - Directory Group Import Settings
select * from PS_LDAPATTRIBMAP - Directory Group Import Attributes
```

If you successfully pass all 3 tests, congratulations, you have setup your LDAP authentication with PeopleSoft 8.1x and 8.2x correctly.

DIRECTORY GROUP IMPORT

WARNING!

Before you start setting up Dynamic Role Rules or Directory Group Import please see Solution 200756660 - E-SEC: How to get Dynamic Role Rules to work on PT 8.4x and 8.1x

AND...have a firm understanding of how Application Messaging works, how to ping your local node, setup your Gateway, and have Pub/Sub turned on in your app server.

Now you may proceed.

The Directory Group Import process is the first step required to dynamically assigning PeopleSoft roles, to your users, based on their group memberships in your directory. This means that you can assign PeopleSoft roles to your users, who are in your directory, even before they have ever logged onto PeopleSoft. This is based on the membership to a directory groups the user belongs to.

This part of the setup is NOT essential to getting LDAP authentication to work. It is an optional step that you can use in establishing user role assignments within PeopleSoft by leveraging the group memberships in your directory.

The setup for this process is pretty straightforward. Again, this setup is only needed if you plan on using the dynamic role rule process. This process is not used in PeopleTools 8.4x as directory role assignment is setup differently and will be explained in chapter 4. In this red paper we will not be going over how to dynamically assign roles to your users. We are only discussing this first step of that process. To see more information on Dynamic Role Rules and how that works see PeopleBooks.

The following steps will walk you through the directory group import process.

Step 1 – Set up the Directory Group Import page.

Note: The Map name MUST be named DIRGROUPS or the Import will not work correctly!!!

[Home](#) > [PeopleTools](#) > [Maintain Security](#) > [Setup](#) > **Directory Group Import**

[Settings](#) **Attributes**

Map Name: DIRGROUPS

Directory Connect Information

Server name: PTNTLDAP01
Port: 389
User DN: cn=administrator,cn=users,dc=ptntldap,dc=com
Password: *****


User Search Information

Scope
☒ SUB
☐ ONE
☐ BASE
Search Base: dc=ptntldap,dc=com
Filter: (objectclass=group)

Target

Message: DIRGROUPS

 Save

 Return to Search



 Add

 Update/Display

[Settings](#) | [Attributes](#)

Just as you setup your LDAP authentication pages, the same values need to be used in this setup as far as Server Name, Port, User DN, Password, Search base, and Scope. The filter will be, depending on directory, whatever the objectclass name is for your groups. In this Active Directory example the filter is (objectclass=group) however in iPlanet this would be (objectclass=groupofuniquenames). You will also need to use the delivered message called DIRGROUPS.

Step 2 – Set up the Attribute page

Note: This page should be delivered, depending on the tools release you are on, but may need some modification.

[Home](#) > [PeopleTools](#) > [Maintain Security](#) > [Setup](#) > **Directory Group Import**

Settings Attributes

Map Name: DIRGROUPS

Attribute Map		View All	First	1-2 of 2	Last
Field Name	LDAP Attribute Name				
DESCRLONG	<input type="text" value="description"/>				
GROUPNAME	<input type="text" value="name"/>				

Save Return to Search

Add Update/Display

[Settings](#) | [Attributes](#)

You may find that the GROUPNAME attribute is cn and not name and that is fine too, like it was pointed out earlier this is based on your directory you are using and the valid attributes. Again, the intent of this App Engine process is ONLY to find the name (or cn) of your directory group and it's description. At this point, this has nothing to do with the users assigned to these directory groups.

Step 3 – You must run the Directory Group Import Process to populate the PeopleSoft table

[Home](#) > [PeopleTools](#) > [Maintain Security](#) > [Process](#) > **Directory Group Import**

LDAP Map

Run Control ID: 1

[Report Manager](#)

[Process Monitor](#)

Run

Map Name:

Running this AE process will import the directory group names and their descriptions not the PS_DIRGROUP table within PeopleSoft, so that you can then map the group name to the role you want to dynamically assign your users to.

After running the process check the Process Monitor to make sure it has successfully completed.

See **Appendix C** for any solutions or incidents related to this setup.

To see how to execute Dynamic Role Rules see PeopleBooks.

Here are the PeopleSoft tables used in the directory group import process:

select * from PS_DIRGROUP - Directory Groups found during Directory Group Import process
select * from PSROLEGROUP - Groups in Directory assigned to Roles in PeopleSoft

Chapter 4 - Setting Up LDAP Authentication on PeopleTools 8.4x

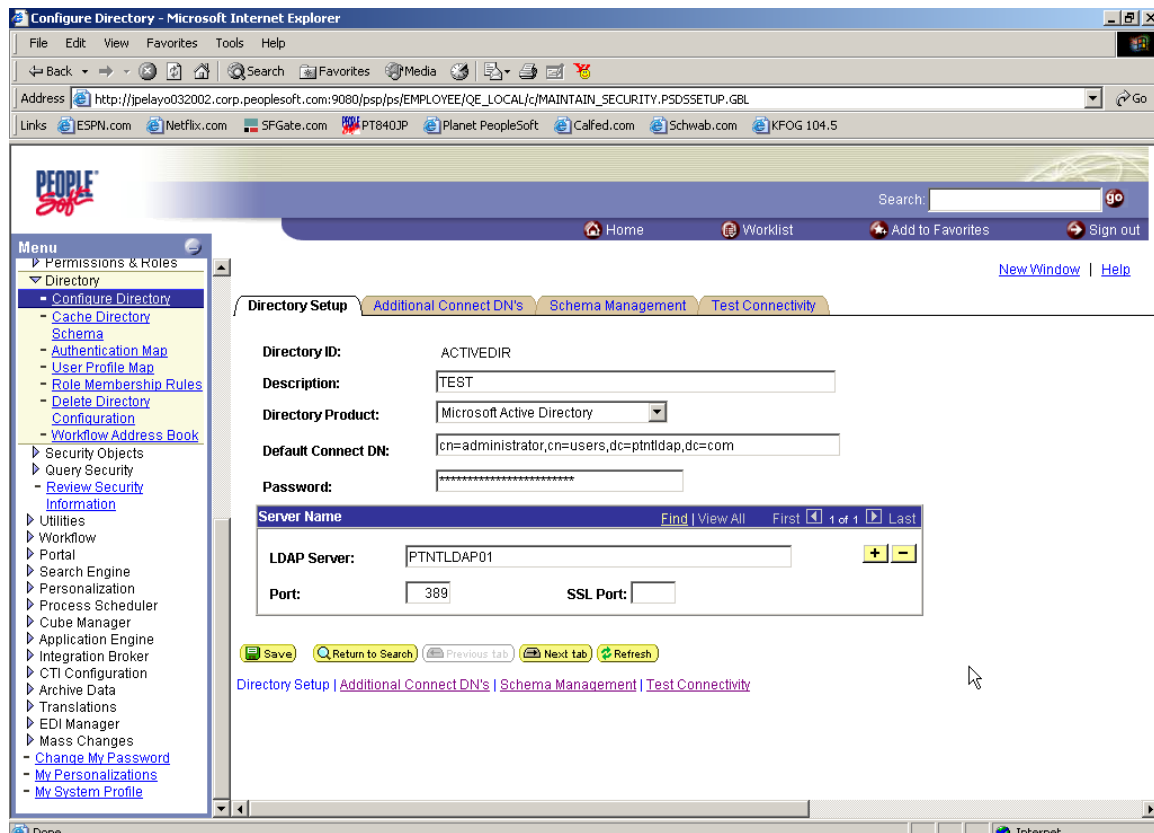
This chapter will take you on a step-by-step, page-by-page, walkthrough on how to correctly setup your PeopleSoft application to authenticate against your LDAP compliant directory in PeopleTools 8.4x.

Depending on which directory you choose to use Novell, Microsoft, Netscape, or Oracle (as of PT 8.46) the actual attribute names may be different, but the functionality is the same. Please become very familiar with the directory attributes you will be using in the next few pages and chapters. This will save you a lot of time and headaches.

STEP 1 – CONFIGURE DIRECTORY

The first thing you need to do is to navigate to the PeopleTools > Security > Directory > Configure Directory page. Configuring the directory is used for caching the directory schema, which is a required process for LDAP authentication in PeopleTools 8.4. The following screen shots are an example of Microsoft's Active Directory however using Sun One or Novell's eDirectory you will use the same setup except for the naming of some of the LDAP attributes.

Although this component has four pages, Directory Setup, Additional DNs, Schema management, and Test Connectivity, to setup LDAP authentication, only the Directory Setup and Test Connectivity pages are important at this point. The Additional DNs page can be used if you want to have other users that can search the directory, that you would want your Authentication map to use instead of the connect DN on the directory setup page. The Schema management page is used for PDI. Information on the other two pages can be found in PeopleBooks.



Now we will step through each field on this page and describe what each is used for. All values must be correct and not mistyped or you will not be able to get the signon PeopleCode to talk to your directory correctly.

Directory ID: Identifies the directory connection that you are creating. The directory ID that you enter can identify a specific LDAP server or a collection of LDAP servers depending on how many servers you add in the Server Name section.

Description: Self explanatory, Enter a description of the directory connection.

Directory Product: Select your directory product from the list of options i.e. Microsoft Active Directory, Novell e-Directory, etc.

Default Connect DN: The Distinguished Name of directory based account with "Browse" rights to ObjectClass=Person entries and "Read" rights to all needed attributes. **This is one of the first places that we find a mistake.** You may not be using a valid account, or the directory account does not have the rights to read all attributes in the directory. PeopleSoft suggests you use an administrator account but that is not always necessary. The DN is the full path to the user, for example cn=administrator,cn=users,dc=peoplesoft,dc=com which means that this user is located in the container called users under the domain called peoplesoft.com. This DN will be chosen by default when creating subsequent maps. The default DN can be overridden on each mapping page by adding addition connect DN's on the following page.

Password: The directory password for User DN. This is important as with no password you are making an anonymous bind to the directory. PeopleSoft suggests not using anonymous to bind to your directory but that is your choice to make. You need a password in order to cache the directory schema, which will be in the next step. The password is stored in encrypted form in the database; not even individuals with administration access to the database can view this password.

Server Name: Add LDAP directory servers to a connection list. You can add multiple servers for failover purposes using the plus button. All servers you add must participate in the same directory service.

LDAP Server: Identify a specific LDAP server. You can use the DNS name or you can use IP address dotted notation. For example, either of the following formats is acceptable: ldap12.yourcompany.com or 192.201.185.90.

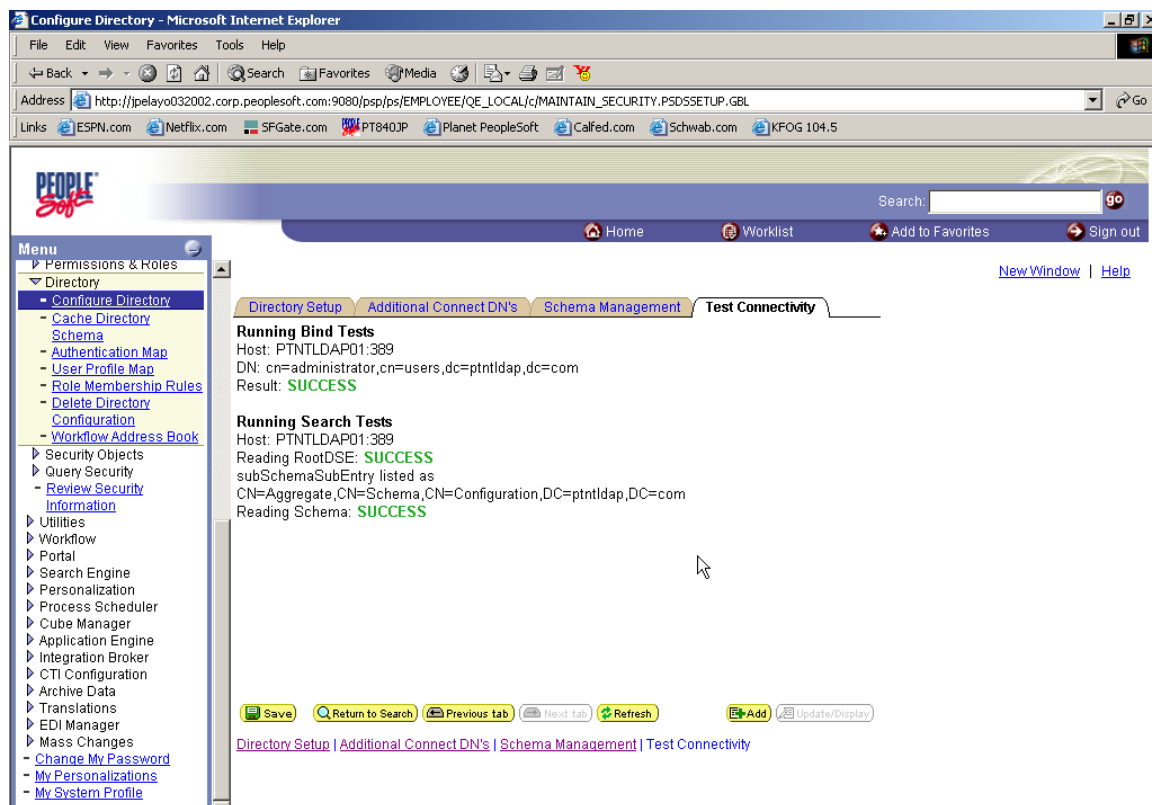
Port: Enter the port number on which the LDAP server is configured to receive search requests. The standard LDAP port is 389. If you do not specify the correct port, PeopleSoft Directory Interface can't exchange data with your LDAP server. In Active Directory you can also choose to use the Global Catalog port of 3268.

SSL Port: If you are implementing Secure Socket Layer (SSL), enter the SSL port on the LDAP server. The standard SSL port is 636. In Active Directory the Global Catalog port for SSL is 3269.

Now, on to step 2.

STEP 2 - TEST CONNECTIVITY

Next we need to verify your settings in Directory Setup page to see if they can pass all the connectivity tests. The page displays the results (**SUCCESS** or **FAIL**) of the connectivity test. If connectivity fails, modify the connect information on the Directory Setup and Additional Connect DN's pages. All tests must return **SUCCESS**. If they do not then either your configuration settings are not correct or the default connect id used does not have full access to your LDAP Directory. If you have the bind and search of the host returning success, but the search of the schema is failing, then that means you are attempting to bind anonymously, and normally anonymous cannot read the schema. Now just because you do have a success result does not mean that your LDAP authentication will work but you are a lot closer than if it fails. What this test does is it verifies that the server and directory are up and running, it makes a bind if you are using a password with the connect DN; otherwise it is making an anonymous bind to the directory. So you may see varied results depending what values you have on your directory setup page.



Things to check if you get a failure on this page.

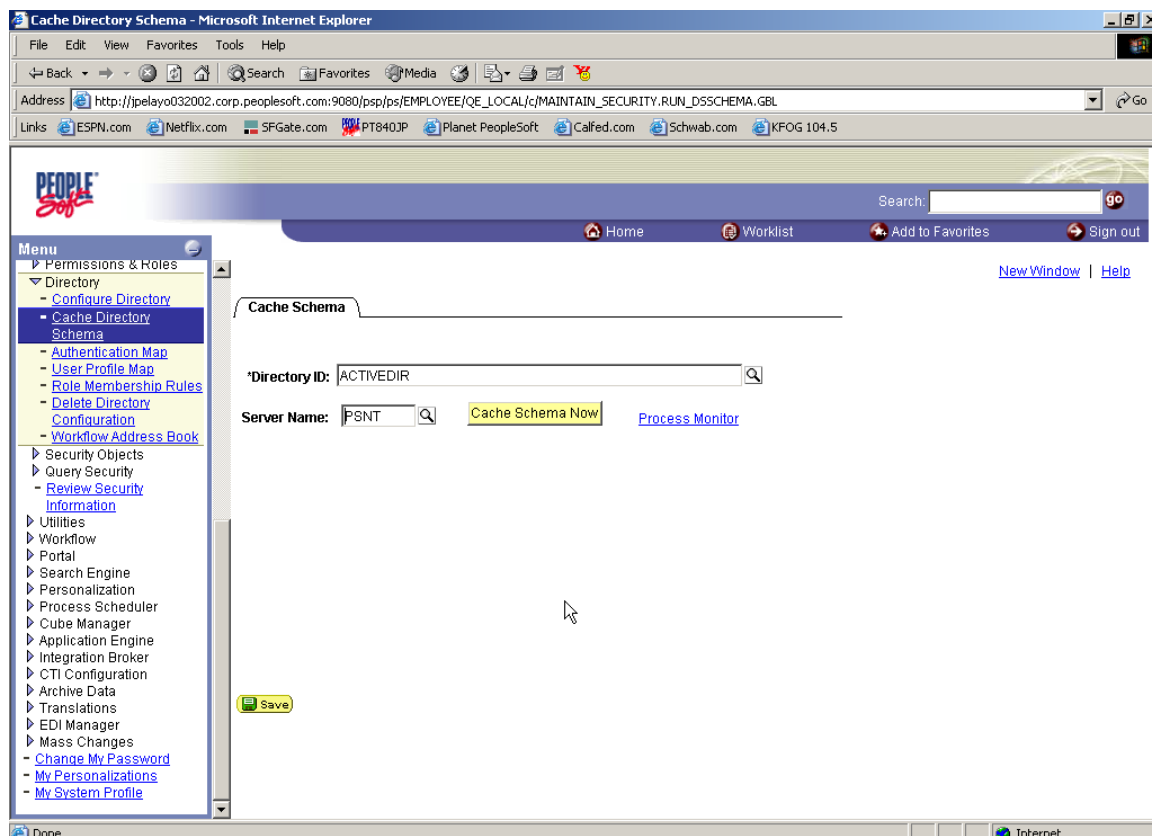
Test the connect DN without a password, this will do an anonymous bind and should return successfully.
Check the port numbers being used that they are valid.
Check the server name, if you are using DNS names you might try using the IP address instead.
Check to make sure the DN being used is correct.

Important Note: As of PT 8.48 there were changes made to the libraries used depending on the App server platform you are on. See GSC SOLUTION ID 201034509 E-LDAP: PT 8.48 Getting business interlink error when configuring LDAP

STEP 3 - CACHING THE DIRECTORY SCHEMA

The next step is to run the Cache Directory Schema. You use the Cache Schema page to specify a directory server and invoke an Application Engine program designed to create a cache in the PeopleSoft database of the directory schema. This enables you to select names of Object Classes and Attribute Types when creating security maps. If you have multiple directory configurations you will need to cache the schema for each configuration. The directory authentication and User Profile maps use these attribute values when mapping your directory.

This step MUST be done before you can setup the Authentication or User Profile maps!!!



When caching the directory schema you will need to choose the directory and the server. This process should only take a few minutes and it needs to be run for every configuration you create.

If you run into any errors while caching the schema then see appropriate solutions in **Appendix C** of this red paper.

The following tables get populated when caching the directory schema:

PSDSATTR
PSDSOCATTR
PSDSOBJCLS
PSDSANCESTOR

STEP 4 – SETUP AUTHENTICATION MAP

This is the information used to bind to the directory and search for the LDAP user that is logging into PeopleSoft.

For all PeopleTools versions prior to 8.45 you can ONLY have ONE active authentication map!!!

As of 8.45 we made it so that you can use multiple active maps for authentication purposes. This will allow you to setup different directories to authenticate against, multiple domains, as well as help in fail over performance.

The first thing is to make sure the map you are using is active.

The **Directory ID** is the configuration that you previously setup in the configure directory. This must be defined in order to properly fill the Connect DN.

Anonymous Bind and **Use Secure Socket Layer** are options you can check at this point if you are using that setup. You can only use one option not both or neither and use the default DN.

The **Connect DN** gets populated automatically when you choose the directory ID from the previous setup. If you wanted to use a different connect DN then you can use the dropdown box which will allow you to choose from the Additional DNs page you may have setup when configuring the directory in step 1. We skipped this page but as mentioned before the Additional DNs page can be used if you want to

have other users that can search the directory, that you would want your Authentication map to use instead of the connect DN on the directory setup page

The **list of servers** is brought over from step 1 also. You can choose to add or subtract any servers for this particular map. Be sure to add the appropriate sequence number for the search order of which server will be first searched.

The **User Search Information** is critical. **Here is where we have also found a lot of errors made.** This is where you will define the Search base, the search scope, and the search attribute used to find the users in the directory.

Search Base: The search base is the container or starting point in the directory that you want to start your search for users. You **MUST** include the whole DN path for this location for example if all your users are in a container called “Users” and this is located under your root domain of PeopleSoft.com then your search base would look something like this: cn=users,dc=PeopleSoft,dc=com. You can start your search base at the root or your directory (dc=PeopleSoft,dc=com) however we suggest that you start one container lower in your directory tree and this is for performance purposes. If you start at the root level you may run into issues with unfollowed referrals as noted in a solution about performance and UNIX on **Appendix C** of this red paper.

Scope: The scope of the search, which can be one of these values:

Base retrieves information only at the level of your search base. It will not look deeper in you directory for users.

One retrieves information about entries one level below the base.

Sub retrieves information about entries at all levels below the base. The base entry is included in this scope. If no scope is specified, the server performs a base search.

Search Attribute: **This is the third place we have found confusing information and errors.** The search attribute is the directory attribute of ObjectClass=Person to which the provided User ID should be matched. For example the **uid** (Unique Identifier) or **sAMAccountName** (Active Directory’s version of the uid) depending on the directory you are using. This is also the value the user will be typing in at the PeopleSoft logon page. If they were using their email address or employee number to logon to PeopleSoft, then you would need to use the correct directory attribute so the search in the directory will return the right user information like mail or emploeenumber. Again we cannot stress enough that you should become very familiar with the directory attributes you will be using.

STEP 5 – SETUP USER PROFILE MAP

This page is used for mapping you directory users to the PSOPRDEFN table.

The screenshot shows the 'User Profile Map' configuration page in a Microsoft Internet Explorer browser. The browser's address bar displays the URL: `http://pelayo032002.corp.peoplesoft.com:9080/ps/ps/EMPLOYEE/QE_LOCAL/c/MAINTAIN_SECURITY.DSUSRPROF2.GBL`. The page title is 'User Profile Map - Microsoft Internet Explorer'. The left sidebar contains a 'Menu' with various options, including 'Permissions & Roles', 'Directory', 'Authentication Map', 'User Profile Map', 'Role Membership Rules', 'Delete Directory Configuration', 'Workflow Address Book', 'Security Objects', 'Query Security', 'Review Security Information', 'Utilities', 'Workflow', 'Portal', 'Search Engine', 'Personalization', 'Process Scheduler', 'Cube Manager', 'Application Engine', 'Integration Broker', 'CTI Configuration', 'Archive Data', 'Translations', 'EDI Manager', 'Mass Changes', 'Change My Password', 'My Personalizations', and 'My System Profile'. The main content area is titled 'Mandatory User Properties' and 'Optional User Properties'. It includes fields for 'User Profile Map' (set to ACTIVEDIRECTORY), 'Authentication Map' (set to ACTIVEDIRECTORY), 'Status' (Active), 'Directory ID' (ACTIVEDIR), 'User ID Attribute' (sAMAccountName), 'ID Type' (None), 'ID Type Attribute' (None), 'Default Role' (Use default Role checked, Role Name: PeopleSoft User, Role Attribute:), 'Language' (Use Default Language Code checked, Language: English, LangCD:), and buttons for 'Save', 'Return to Search', 'Next in List', 'Previous in List', 'Add', and 'Update/Display'.

Again we will step through each field on this page, as we did on the last page, and describe what each field is used for. All values must be correct or you will not be able to get the signon PeopleCode to talk to your directory correctly. Regardless whether or not you will be creating and updating users in PeopleSoft or only using your directory for authentication purposes, all of the mandatory fields on this page must be completed in order for LDAP authentication to work. The User Profile Map works in conjunction with the User Profile Component Interface so all fields need to be correct for the user to be created otherwise you will get errors when the user tries to logon like "All attribute values for id types are required" or "More than one row exists". See **Appendix C** for solutions on this error.

Mandatory User Properties page

Authentication Map: Choose the authentication map, from the dropdown list, that you will be using this profile map with. As stated before you can have multiple authentication maps, therefore you need to have a corresponding profile map with each authentication map. You may **ONLY** have one User Profile Map per authentication Map.

User ID Attribute: This is the directory attribute containing the value that will be used as the PeopleSoft OPRID on the PSOPRDEFN table. So once the search attribute, on the last page is found, the signon PeopleCode then binds to this directory attribute. This is also the value that will be updated or created in PeopleSoft if you are using the USER_PROFILE component interface. So if your uid or

sAMAccountName, in the directory, were **jsmith** then the OPRID in PeopleSoft would be searching for, or creating would be **JSMITH**.

Note: Although the directory is case insensitive the delivered peoplecode will ALWAYS force UPPER CASE when returning from the directory and searching the PSOPRDEFN table for this user or when creating the user in the PSOPRDEFN table. So you will notice that your users get created in upper case regardless of their case in the directory. See possible solution in **Appendix C** to make changes to this delivered functionality.

ID Type: This is the default ID Type for newly created users. We suggest you first try this with NON (none). Once you have established LDAP authentication and you want to change this to EMP (emplid) you may but bear in mind that when using the value of EMP you must also have the ID Type Attribute value filled with the user's correct employee number.

ID Type Attribute: The name of the LDAP attribute containing valid data for the given ID Type. If using NON then this field is grayed out and no value is required. However, if you are using the EMP ID type then the directory attribute named here must contain the same value on the user profile of the directory as the EMPLID value in the PS_PERSONAL_DATA table in PeopleSoft contains for this user, as there is a cross reference to the employee when the user is created. So if you are using EMP as the ID Type and the ID Type Attribute is employee number (which would need to be a valid attribute in your directory) then this value on the employee number attribute in the directory would have to match the EMPLID for this user on the PS_PERSONAL_DATA table in order to correctly cross reference and update or create the user profile. See solutions on **Appendix C** for more information regarding this issue.

Default Role: You have 3 options here. 1) You can choose to assign to your newly created users a default role, that exists in PeopleSoft, that will give only the minimal access you would want EVERY user to have and also allowing the user to logon with only this role. 2) You can choose a directory attribute that will hold the default PeopleSoft role you want to assign to your users, remember with this option you must have an attribute defined in the directory with the PeopleSoft role name value in it for this role to be correctly assigned to the user logging in. 3) You can choose not to assign a default role at all. This is the safest option if you are already dynamically assigning roles to your users, or you are only authenticating users and not creating them through the LDAP_PROFILESYNCH option on the signon peoplecode page.

Note: One thing to keep in mind it that you cannot use both options 1 & 2 and in using the 3rd option, if you have directory groups named the same as your PeopleSoft roles, then your users will get these roles assigned to them "on the fly" as they logon and their static roles will be deleted. See **Appendix C** for solutions regarding Dynamic Role Assignment.

Additional note: If the user is already created in PeopleSoft, then they will not be assigned the default role when they logon through the LDAP_PROFILESYNCH. This is only for users that have not yet been created on the PSOPRDEFN table.

Default Language Code: This is the same as the default role as you can define to use a default value or a directory attribute. Remember you cannot use both.

Now let's look at the optional user properties page.

The screenshot shows the 'Optional User Properties' page. At the top, there are tabs for 'Mandatory User Properties' and 'Optional User Properties'. Below the tabs, it says 'User Profile Map: IPLANET'. The main section is titled 'Optional User Properties' and contains a table with the following columns: '*User Profile Property', 'Use Constant Value', 'Attribute Name', 'Constant Value', and 'Always Update'. There are three rows in the table:

*User Profile Property	Use Constant Value	Attribute Name	Constant Value	Always Update
EmailAddress	<input type="checkbox"/>	mail		<input checked="" type="checkbox"/>
UserDescription	<input type="checkbox"/>	cn		<input checked="" type="checkbox"/>
SymbolicID	<input checked="" type="checkbox"/>		sa	<input type="checkbox"/>

This page is ONLY used if you have enabled the LDAP_PROFILESYNCH option on the signon peoplecode page.

There are several fields of the user profile you can choose to update by using this page. You can also choose to always update these fields, which means that the user will be updated with every successful logon, or by not choosing the always update option, the user will only get these fields populated when the user is initially created through LDAP authentication. If the user already exists in PeopleSoft, then these fields will not be updated unless you choose to use the always update option.

You also have the option to use an LDAP attribute, which holds the value you wish to use for this field in PeopleSoft, or you can use a constant value.

Note: At this time the number of fields you can populate is limited to the following fields shown below. However the UserIDAlias field should not be used, as it WILL NOT work for LDAP authentication. It was designed as an alternative logon for PeopleSoft authentication only.

Also: If you have existing PeopleSoft users that will also be LDAP authenticated users, AND if you have the user profile synch turned on, then your PeopleSoft passwords will not longer work for these users, that is **AS LONG AS YOU ARE UPDATING THEM WITH EVERY LOGON**. Meaning you have to have something on the Optional user properties page checked to always update, like their email address. Otherwise if nothing has been checked to be updated for the users, then the User Profile CI will not make any updates to the user, and their PeopleSoft password will still work. In this case, if the user logs on with their PeopleSoft password, and not their LDAP password, assuming they have the OPRID in the correct case, as defined on PSOPRDEFN, then the password controls will also be invoked to validate the password age for expiration. To get around this you may just want to delete your LDAP user's passwords from PSOPRDEFN or set the ENCRYPTED flag to 0 so that the PeopleSoft logon will fail and thus invoke Signon PeopleCode for LDAP Authentication. This is what the code would do if you were updating a field for the user with every logon.

See solutions on **Appendix C** for more information regarding issues with this page.

Menu

- Directory
 - Configure Directory
 - Cache Directory
 - Schema
 - Authentication Map
 - User Profile Map
 - Role Membership
 - Rules
 - Delete Directory
 - Configuration
 - Workflow Address
 - Book
- Security Objects
- Query Security
- Encryption
- Common Queries
- Mass Change Operator
- Security
- Utilities
- Workflow
- Portal
- Search Engine
- Personalization
- Process Scheduler
- Cube Manager
- Application Engine
- Integration Broker
- REN Server Configuration

Look Up User Profile Property

Search by: User Profile Property begins with

[Look Up](#) [Cancel](#) [Advanced Lookup](#)

Search Results

View All First 1 1-10 of 10 Last

User Profile Property

- [CurrencyCode](#)
- [EmailAddress](#)
- [MultiLanguageEnabled](#)
- [NavigatorHomePermissionList](#)
- [PrimaryPermissionList](#)
- [ProcessProfilePermissionList](#)
- [RowSecurityPermissionList](#)
- [SymbolicID](#)
- [UserDescription](#)
- [UserDAlias](#)

STEP 6 – SETUP SIGNON PEOPLECODE PAGE

The following page holds the signon PeopleCode used with LDAP. LDAP_AUTHENTICATION is used with the authentication against the LDAP directory. LDAP_PROFILESYNCH is used for creating a user for the LDAP user in PSOPRDEFN. It is strongly recommended that you use the “Invoke As” option if you are using LDAP. The “invoke as” user MUST have full access to a Component Interface called USER_PROFILE.

IMPORTANT NOTE: Any change made to the signon PeopleCode page requires a reboot of your application server.

Signon PeopleCode - Microsoft Internet Explorer

Address: http://pelayo032002.corp.peoplesoft.com:9080/psp/ps/EMPLOYEE/QE_LOCAL/c/UTILITIES.SIGNONPPC_PAGE_COM.GBL

Links: ESPN.com, Netflix.com, SFGate.com, PT840JP, Planet PeopleSoft, CalFed.com, Schwab.com, KFOG 104.5

Search: [] go

Home Worklist Add to Favorites Sign out

New Window | Help

Signon PeopleCode

Signon

☐ Invoke as user signing in

☒ Invoke as User ID: QEDMO Password: []

Sequence	Enabled	Record	Field Name	Event Name	Function Name	Exec Auth Fail
1	<input type="checkbox"/>	FUNCLIB_PWDCNTL	PWDCNTL	FieldChange	Password_Controls	<input type="checkbox"/>
2	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	WWW_AUTHENTICATION	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	LDAP_AUTHENTICATION	<input checked="" type="checkbox"/>
4	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	SSO_AUTHENTICATION	<input type="checkbox"/>
5	<input checked="" type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	LDAP_PROFILESYNCH	<input checked="" type="checkbox"/>

Save Refresh

Here we will explain what all the fields on this page are used for.

Invoke as user signing in. This radio button is used for normal PeopleSoft authentication. When using LDAP authentication you will want to use the “Invoke as” radio button as described below. Using this option the user must enter the user id in the correct case as found on the PSOPRDEFN table or the authentication will fail to find the user.

Invoke as. By choosing this option it will make the signon process for the User ID case insensitive. When using LDAP authentication PeopleSoft suggests that you use this option and not the "Invoke as user signing in". There are other reasons for this choice as well. When a PeopleCode program runs, it has to have a context of a user. This is how you indicate to the system the user who is executing the program. This is important because the user ID provided needs to have access to all of the objects that

your signon program uses. For instance, when you are using LDAP authentication the signon peoplecode contains business interlinks and component interfaces. If the user ID provided does not have the appropriate authority to business interlinks or component interfaces, the program fails to execute the desired function. Whether you use the value of the user signing in or you create a default user ID for all signon attempts depends on your implementation.

With that said what you will want to do is create a permission list called LDAP, on that permission list the ONLY 2 things you need to do is 1) on the general tab make it so the permission list does not time out. 2) On the Component Interface tab add the Component Interface called USER_PROFILE, edit this and give "Full Access" to all options. Save this permission list.

Now, create a role and call it LDAP and assign this LDAP permission list, which you just created, to this role.

Last, Create a user called LDAP; give it a password, and ID type of none, and the LDAP role.

Place this user and password on the Signon PeopleCode page as the "Invoke As" user.

IMPORTANT: You must bounce the app server for this to take affect. Never worry about this user or their password again! Because this user cannot logon to PeopleSoft in any tier, you will not have to worry about its misuse. This user is ONLY used to update LDAP authenticated user profiles.

Sequence. The sequence column shows you the sequence in which your signon programs execute. You can change the sequence by changing the numerical value in the edit box.

Enabled. To enable a program to run at signon, check the Enabled checkbox. If it is not checked, then the system ignores the program at signon. You MUST enable # 3 FUNCLIB_LDAP LDAP_AUTHENTICATION for this to work If you want users to be created or updated when they logon via LDAP then you have to also enable # 5 FUNCLIB_LDAP LDAP_PROFILESYNCH and then bounce the app server.

Record. Specify the record on which you record PeopleCode exits.

Field Name. Add the specific field that contains the PeopleCode.

Event. Add the event that triggers a particular program.

Function Name. Add the name of the function to be called.

Note: Unless you are writing your own Signon PeopleCode or editing the delivered signon PeopleCode, you will not have to make any changes to the record, field, event, or function.

Exec Auth Fail. You MUST have this box checked in order for LDAP authentication to work. This column means "Execute this code if initial PeopleSoft authentication fails." This means that even if PeopleSoft does not authenticate the user (SetAuthenticationResult=N), you still want the program to run. For instance, if you write an LDAP authentication program, you want it to run after PeopleSoft denies access so that your program can authenticate the user through your code instead. On the other hand you can leave this option unchecked to further secure your system. For instance, if you are not using LDAP authentication, leaving this option unchecked prevents any program or script from running if your PeopleSoft authorization fails, and not user could log on.

STEP 7 – TEST TEST TEST!!!

In order to verify that you have setup everything correctly the best thing to do at this time is test it. There are a couple simple tests you can do to see if your setup was as easy as it seemed.

Test # 1 – PeopleSoft authentication and default role test

Create user Known to PeopleSoft and your LDAP directory. Make the OPRID in Upper Case. Give the user a different password in PeopleSoft than their LDAP directory password. Give the user the default role you are using in your LDAP setup (Mandatory User Properties page). Using the PeopleSoft password first try to logon. This will test the role you have assigned as your default role to see if it has the rights needed to logon to PeopleSoft.

If this test fails then you need to reevaluate the default role and the permission lists assigned to this role. Remember in PeopleTools 8.1x and 8.2x the default role cannot have any spaces in the name.

Test # 2 – LDAP Authentication test

After you have successfully completed test 1 try to logon using the same ID and their LDAP directory password. This will test the signon PeopleCode Authentication process.

If this test fails then there is a problem with one of the following things:

- a) Network connectivity to the directory server
- b) The User DN for the search does not have rights to read all attributes in the directory
- c) The User DN account is locked out
- d) The signon user does not exist in the directory
- e) The signon user account in the directory is locked out
- f) The signon user's password is wrong
- g) The search attribute on the Directory authentication page or the User ID Attribute on the user profile caching page may be incorrect.

Also remember that you needed to bounce the app server after setting up your signon peoplecode page.

If this test is not successful jump ahead to **Appendix B – Troubleshooting**. Here you will find ways of validating all your settings.

Test # 3 – User Profile Creation test

Assuming your first 2 tests worked successfully, and you have invoked the LDAP_PROFILESYNCH signon PeopleCode, delete the OPRID you created from PeopleSoft and try logging in again as that user using their LDAP directory password.

This will test the User Profile Component Interface to see if a user, not known to PeopleSoft, can be created with the default values found on the Mandatory and Optional User Properties pages.

Here are some SQL statements that may help in validating the values in the PeopleSoft tables that are related to your LDAP setup.

Signon PeopleCode page

```
select * from PSSIGNONPPC
```


Configure Directory

select * from PSDSDIR

Tables that get populated when caching the directory schema

select * from PSDSATTR

select * from PSDSOCATTR

select * from PSDSOBJCLS

select * from PSDSANCESTOR

Authentication Map

select * from PSDSSECMAPMAIN

select * from PSDSSECMAPSRVR

If you successfully pass all 3 tests, congratulations, you have setup your LDAP authentication with PeopleSoft 8.4x correctly.

DIRECTORY ROLE RULES FOR DYNAMIC ROLE ASSIGNMENT

WARNING!

Before you start setting up Dynamic Role Rules please see the following Solutions:

200756660 - E-SEC: How to get Dynamic Role Rules to work on PT 8.4x and 8.1x

200735803 - E-LDAP: E-LDAP: How to get LDAP Dynamic Role Rules to work in 8.4x

AND...have a firm understanding of how Integration Broker works, how to ping your local node, setup your Gateway, and have Pub/Sub turned on in your app server.

Now you may proceed.

This part of the setup is NOT essential to getting LDAP authentication to work. It is an optional step that you can use in establishing user role assignments within PeopleSoft by leveraging the group memberships in your directory.

In PeopleTools 8.4x you have more than one option when it comes to dynamically assigning roles to your directory users. We no longer require the directory group import process as PT 8.1x did. In 8.4x you will see that your role membership rules are located under PeopleTools > Directory > Role Membership Rules.

In this first example (the setup is using Active Directory) we are looking for a group in the directory called "Manager" and then finding the all the members of that group.

The screenshot shows the 'Dynamic Role Assignment' page in PeopleSoft. The page has a left-hand navigation pane with a tree view containing items like 'Information', 'Schedule Resources', 'Self Service', 'Structure', 'Workflow', 'Security Objects', 'Query Security', 'Personalization', 'Process Scheduler', 'Cube Manager', 'Application Engine', 'Integration', 'Multi-Step', 'Audit', and 'Tools'. The main content area is titled 'Dynamic Role Assignment' and contains several sections. The 'Role Policy' section has a 'Role Policy' dropdown set to 'MANAGERS' and a 'Users in the Directory Manager group' text box. The 'Directory ID' is set to 'ACTIVE DIRECTORY'. The 'Directory Search' section has a 'Search Base' of 'dc=ptnldap, dc=com' and a 'Search Scope' of 'Sub'. Below this is a 'Search Filter' table with one row: '1' in the first column, 'cn' in the second, '=' in the third, and 'Manger' in the fourth. There are 'Refresh Search Filter' and 'Clear Search Filter' buttons. The 'Search Filter' text box contains '(cn=Manger)'. Below the search filter is a 'Search Attributes' section with a 'Find' button and a 'First (4) of 1 (2) Last' link. The 'Directory Attribute' is set to 'member'. There are 'Add', 'Update/Display', and 'Refresh' buttons at the bottom. Four red circles with arrows point to specific parts of the interface: 'Create Search base and build Role Rule filter' points to the 'Search Base' field; 'Create Role Policy Choose map' points to the 'Role Policy' dropdown; 'Define Directory Attribute' points to the 'Directory Attribute' field; and 'Assign Rule to Role' points to the 'Assign to Role' link.

Dynamic Role Assignment

PeopleSoft

Role Policy

MANAGERS

Users in the Directory Manager group

Directory ID: ACTIVE DIRECTORY

Directory Search

Search Base: dc=ptnldap, dc=com

Search Scope: Sub

Search Filter

	Attribute	Operation	Value
1	cn	=	Manger

Refresh Search Filter Clear Search Filter

Search Filter: (cn=Manger)

Search Attributes

Find First (4) of 1 (2) Last

Directory Attribute: member

Add Update/Display Refresh

Assign to Role

PeopleSoft Connect

Now let's discuss the steps and fields on this page so that you are clear as to what needs to be entered.

Step 1: Create a role membership rule with whatever name you choose, but make sure that you chose to use an active user profile map, this will then be using the active authentication map to search the directory.

Step 2: The Search Base can be the same value as on your authentication map if your directory groups are all located under that branch in your directory and the same with the search scope.

Step 3: The Build Filter is key here. You need to enter the attribute you are searching for. In the example above the attribute 'cn' is the common name or attribute used to describe the directory group. The Operation is = and the value is the actual directory membership group called 'Manager'.

Step 4: The Directory Attribute is very important in this setup, as we have defined it. This is because the role rule will search the directory and find the group called 'Manager' from step 3, but without the directory attribute it will not find the users. So in this case we are using Active Directory and the LDAP attribute for a group member is 'member'. If you are using iPlanet the Directory Attribute, in the screenshot above will need to be 'UniqueMember'.

Step 5: Next we will assign the role membership rule to a PeopleSoft role. And in this case we have a role in PeopleSoft called 'ALLPAGES'

Dynamic Role Assignment

PeopleSoft

Menu

- PeopleTools
- Security
- User Profiles
- Permissions & Roles
 - Permission Lists
 - Copy Permission Lists
 - Delete Permission Lists
 - Roles
 - Copy Roles
 - Delete Roles
 - Execute Role Rules
- Directory
- Security Objects
- Query Security
- Review Security
- Information
- Mass Change Operator
- Security
- Utilities
- Workflow
- Portal
- Search Engine
- Personalization
- Process Scheduler
- Cube Manager
- Application Engine
- Integration Broker
- MultiChannel Framework
- Archive Data
- Translations
- EDI Manager
- Mass Changes

General | Permission Lists | Members | **Dynamic Members** | Workflow | Role Grant | Links | Role Queries | Audit

Role Name: ALLPAGES
Description: TOM

User ID: [Search] [First] [Previous] [Next] [Last]

Dynamic Members Customize | Find | View All | First | Previous | Next | Last

User ID View Definition View Definition

Rules

- ☐ Query Rule Enabled
- ☒ PeopleCode Rule Enabled
- ☒ Directory Rule Enabled

[Assign Directory Rule](#)

Delete Dynamic Members

Execute on Server:
[Test Rule\(s\)](#)
[Execute Rule\(s\)](#)

PeopleCode Rule

Record: FUNCLIB_LDAP
Field Name: OPRID
Event: FieldFormula
Function: DynRoleMembers

Save Return to Search Next in List Previous in List

Page 27 PeopleSoft. Proprietary and Confidential. Copyright 2003 PeopleSoft, Inc. For Internal Use Only. Do not distribute outside of PeopleSoft.

PeopleSoft. Connect

Step 6: On the role we need to enable the directory role rule by checking the checkbox for Directory Rule Enabled and hitting the hyperlink called Assign Directory Rule.

Step 7: Next we need to assign to this role our newly create role rule. (Note there are several role rules that have previously been created)

Dynamic Role Assignment

PeopleSoft

- Menu
- PeopleTools
- Security
 - User Profiles
 - Permissions & Roles
 - Permission Lists
 - Copy Permission Lists
 - Delete Permission Lists
 - Roles**
 - Copy Roles
 - Delete Roles
 - Execute Role Rules
 - Directory
 - Security Objects
 - Query Security
 - Review Security Information
 - Mass Change Operator Security
 - Utilities
 - Workflow
 - Portal
 - Search Engine
 - Personalization
 - Process Scheduler
 - Cube Manager
 - Application Engine
 - Integration Broker
 - MultiChannel Framework
 - Archive Data
 - Translations
 - EDI Manager
 - Mass Changes

Look Up Rule Name

Search by: **Directory Search Name** begins with

[Look Up](#)
[Cancel](#)
[Advanced Lookup](#)

Search Results

Items: 1-5 of 5

Directory Search Name
MANAGERS
TEST.CCR
TEST.CONFIG
TEST.PT
TOM

Choose from the list of Role Policies you have created

Page 28
PeopleSoft. **Connect**

Step 8: If we take a look at the directory we can see what the group looks like (This is an example of Active Directory)

Group Membership in the Directory

The screenshot shows the 'Active Directory Users and Computers' window. The 'Tree' pane on the left shows the hierarchy: 'Active Directory Users and Computers [ptrtdap.com]' > 'Users'. The 'Main' pane shows the 'GSC Properties' dialog box for the 'GSC' group. The 'Members' tab is selected, showing a list of members: 'jelayo' (ptrtdap.com/Users), 'lrenz' (ptrtdap.com/Users), and 'tom.lenz' (ptrtdap.com/Users). The 'Add...' and 'Remove' buttons are visible at the bottom of the list.

Page 29
PeopleSoft. **Connect**

Step 9: We will test and execute the role rule and see that the members in our directory group now have been assigned our PeopleSoft role.

Dynamic Role Assignment

PeopleSoft

Home | Worklist | Add to Favorites | Sign out

New Window | Help

Dynamic Role Test Results

Role Name: ALLPAGES [Refresh](#)

Description: TOM

After executing the rules, the listed users will be assigned to the current role.

User ID	Description	Query	PCode	Dir
TLENZ		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
JPDELAYO		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Test your role rule to verify the user's who meet the rule criteria return, and then execute the rule

[Return](#)

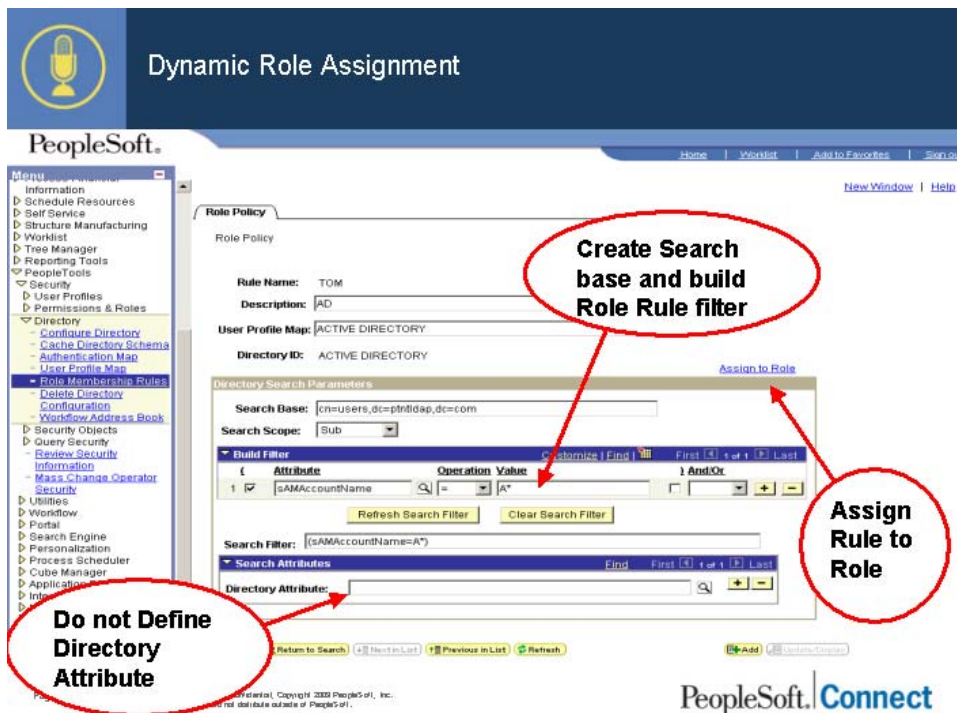
Page 30

PeopleSoft | Proprietary and Confidential. Copyright 2009 PeopleSoft, Inc.
For Internal Use Only. Do not distribute outside of PeopleSoft.

PeopleSoft | **Connect**

In this next example we show you how to use a directory attribute from the user, instead of their group membership to assign the role to the PeopleSoft user. In this case the attribute value must be left blank and only the build filter is created.

The same steps need to be taken here as were required in the previous example.



Step 1: Create a role membership rule with whatever name you choose, but make sure that you chose to use an active user profile map, this will then be using the active authentication map to search the directory.

Step 2: The Search Base can be the same value as on your authentication map if your directory groups are all located under that branch in your directory and the same with the search scope.

Step 3: The Build Filter is key here. You need to enter the attribute you are searching for. In the example above the attribute 'sAMAccountName' is the user identifier in Active Directory or attribute used to describe the directory user. In other directories it might be 'uid'. The Operation is '=' and the value (A*) is the criteria we are using to search the directory. In this case we are looking for all users in the directory that have a sAMAccountName that starts with the letter A.


Step 4: We skip this step as we already have our users attribute. If you were to add an attribute here you would get no returns as there are no other directory attributes assigned to the directory attribute of sAMAccountName.

Step 5: Next we will assign the role membership rule to a PeopleSoft role. And in this case we have a role in PeopleSoft called 'LDAP A Users'


Step 6: On the role we need to enable the directory role rule by checking the checkbox for Directory Rule Enabled and hitting the hyperlink called Assign Directory Rule.

Step 7: Next we need to assign to this role our newly create role rule. (Note there are several role rules that have previously been created)

Step 8: We will test and execute the role rule and see that the members in our directory group now have been assigned our PeopleSoft role.



Dynamic Role Assignment



[Home](#) | [Worklist](#) | [Add to Favorites](#) | [Sign out](#)

[New Window](#) | [Help](#)

Menu

- PeopleTools
- Security
 - User Profiles
 - Permissions & Roles
 - Permission Lists
 - Copy Permission Lists
 - Delete Permission Lists
 - Roles**
 - Copy Roles
 - Delete Roles
 - Execute Role Rules
 - Directory
 - Security Objects
 - Query Security
 - Review Security Information
 - Mass Change Operator Security
 - Utilities
 - Workflow
 - Portal
 - Search Engine
 - Personalization
 - Process Scheduler
 - Cube Manager
 - Application Engine
 - Integration Broker
 - MultiChannel Framework
 - Archive Data
 - Translations
 - EDI Manager
 - Mass Changes

Dynamic Role Test Results

Role Name: LDAP A Users

Description: LDAP A Users

After executing the rules, the listed users will be assigned to the current role.

Refresh

User ID	Description	Query	PCode	Dir
AARONL		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ABELL		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ABISHOFF		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ACONE		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ADMINISTRATOR		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
AGONZALEZ		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
AJAEGAR		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
AJEFFERY		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ALONESTAR		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
AMCCOY		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
AMILLER		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Return

Once again assign the role rule, Test your rule to verify the user's who meet the rule criteria return, and then execute the rule

Page 32

PeopleSoft® Proprietary and Confidential. Copyright © 2009 PeopleSoft®, Inc. For Internal Use Only. Do not distribute outside of PeopleSoft®.

PeopleSoft® | Connect

Here is the PeopleSoft table with your Role rule names:

```
select * from PS_DSSRCHATTR
```

For issues with this setup see **Appendix C** for possible solutions related to the setting up of dynamic role rules.

Appendix A - Setting up SSL for LDAP Authentication

In this document we will discuss how to configure the LDAP Business Interlink to establish Secure Sockets Layer encrypted LDAP connections.

Very Brief Introduction to SSL

If you are unfamiliar with these concepts, please reference Public Key Infrastructure (PKI) and Netscape CertUtil online. Creating the SSL certificates is not a PeopleSoft out-of-the-box feature. It requires development outside of the realm of PeopleSoft, and because of that, PeopleSoft assumes that you have the appropriate level of Internet development expertise to make sure that you are passing the appropriate information to the PeopleSoft system. The support center cannot help with the creation of your certificates that you will be using to setup SSL with LDAP.

Secure Sockets Layer Protocol is a protocol developed by Netscape, which defines an interface for data encryption between network nodes. To establish an SSL encrypted connection the nodes must complete the SSL handshake. Simplified steps of the SSL handshake are given below:

Greatly Simplified SSL Handshake breakdown:

1. Client sends request to connect
2. Server responds to connect request and sends signed certificate
3. Client verifies certificate signer is in its acceptable Certificate Authority (CA) list.
4. Client generates session key to be used for encryption and sends it to the server encrypted with the server's public key (from certificate received in step 2.)
5. Server uses private key to decrypt client generated session key.

As you can see from the steps above, establishing an SSL connection requires two certificates; one containing the public key of the server (Server Certificate/Public Key Certificate) and another to verify the Certificate Authority that issued the Server certificate (Trusted Root Certificate). The server needs to be configured to issue the Server Certificate when a client requests an SSL connection and the client needs to be configured with the Trusted Root Certificate of the Certificate Authority that issued the Server Certificate. The nature of those configurations depends on both the protocol being used and the client and server platforms. Most documentation you'll find is specific to HTTP over SSL (HTTPS) as that's the most prolific use of SSL today. In most cases you can simply replace HTTP with LDAP – SSL is a lower level protocol than the application protocol (i.e. HTTP, LDAP) so it works exactly the same regardless of the app protocol.

Using LDAP with SSL

The first thing to understand is that establishing SSL connections with LDAP (LDAPS) has nothing to do with either web server certificates or certificates used with PeopleSoft App Messaging. Please do not confuse this document with other documents, which address web SSL issues. This document is specific to establishing LDAPS connections using the LDAP Business Interlink. That means a 2 tier SSL connection between the Application Server and your LDAP server.

The LDAP Business Interlink uses a certificate database that resides on the file system of the PeopleSoft Application Server. The certificate database is a file called a cert7.db and needs to reside in the file system of the PeopleSoft application server domain under your PS_Home directory. The cert7.db certificate database needs to contain the Trusted Root certificate of the Certificate Authority that issued the Server Certificate of the LDAP server. Once you have the CA's certificate imported into the cert7.db cert database you are ready to configure the LDAP Business Interlink for SSL.

Note: As of PeopleTools 8.44 and greater, there is a requirement to also have along with the cert7.db a key3.db to get SSL to work correctly.

STEP 1 - PLACEMENT OF THE CERT7.DB AND OTHER REQUIRED SSL FILES

Setting Up the Certificate

To obtain a cert7.db, you must download Netscape Navigator 4.7. (We know this is an older version that may be hard to find but it must be used as using a newer version will only create a cert8.db, which will not work with PeopleSoft at this time.) Once this is downloaded and installed, launch Netscape Navigator, which prompts you to create a user profile. Create a user profile with the name of PeopleSoft. This will create the following directory structure: Netscape\Users\PeopleSoft.

To import the certificate:

1. In the PeopleSoft directory, find cert7.db.
2. With Netscape Navigator open, click the Security button at the top. The Security Information page appears.
3. Select Certificates and Signers. This displays the valid certificates in the database.
4. You can delete all of them. Once they are deleted, click OK, and then close Netscape Navigator.
5. Import the CA's certificate into the cert7.db certificate database.

Once the cert7.db file has been obtained then you will also need to either create a new key3.db file or obtain it from the same location as the cert7.db file. Using the keyutil, which can be found on the Internet, you can create a new key3.db file. **PeopleSoft does not deliver this utility.** The command will be keyutil -N -d. (Note: the period is required to specify the same directory as where the keyutil is being run which should also have the cert7.db file in it)

With these two files created, you will need to place them in the same folder as your app server domain name under PS_Home/appserv/domain/.

This process is the same whether you are running the application server on a NT, Unix, AIX, or Linux machines.

Important Notes:

If you are running the Application Server on a Sun Solaris or HP UNIX server, you may need to download the proper library files attached to GSC solution 200944355 and follow the steps provided to make sure your code will work.

There were changes made to the Netscape libraries that PeopleSoft uses for LDAP authentication in PeopleTools 8.44 and greater that affects how they work on UNIX, specifically HP and Solaris.

As of PeopleTools 8.44, and going forward, there have been several changes to how the LDAP over SSL is setup.

- 1) Both the cert7.db file and the key3.db file are required for the functionality to work. These files must be placed together in the same directory on the Application server. Prior to 8.44 the key3.db file was not required. Now it is.

2) The value of the SSL_DB on the Settings tab in the LDAP_BIND and LDAP_SEARCH Business Interlinks has changed from previous versions.

Previously, the value would be set to cert7.db, which is the delivered default. Now you only need to specify the directory location without the actual file name included. An example would be that the cert7.db and key3.db files are placed in the \$PS_HOME/appserver/DomainName directory. This would mean that you need to set the SSL_DB value to "/". (Note: just type in ./ without the quotes)

In addition to the two previous steps mentioned above, if you are running the Application Server on a Sun Solaris server, you will need to download the Netscapelib.zip file attached to this solution and follow these steps.

1. Detach the attached zip files on this solution, unzip libraries to a temp dir and do an ftp to those unzipped libs to the UNIX OS in "binary mode".
2. Shutdown the Application Server
3. Copy the libraries to \$PS_HOME/bin
4. Reboot the Application Server.
5. Ensure that LDAP_BIND and LDAP_SEARCH contain "/" in the db path.
6. Go to Configure Directory setup then select the Test Connectivity tab to view the connection results. If the SSL is functioning properly you should see Success for the SSL port.

Also see GSC solution 200979296 - E-LDAP: Failed LDAP authentication with SSL causes problems

ISSUE:

Using LDAP SSL, the thread got switch and causing the tux has problem to communicate with it and seems to cause hang. In order to resolve this issue, please include NSPR_NATIVE_THREAD_ONLY=1 as an environment variable. NSPR stand for Netscape Portable Runtime.

WORKAROUND:

Until this is fixed by Sun (Netscape) and then applied to a current tools release we suggest that you use the following workaround provided by Sun:

Add a new path to the Path environment variable by clicking Start->Settings->Control Panel->System->Advanced->Environment Variables->System Variables.

set the environment variable NSPR_NATIVE_THREADS_ONLY to 1
Restart the machine.

REPORT ID:

1183635000 - Will be fixed when Sun fixes their Netscape version.

Important Note from a Customer experience:

We have found out that the 'certutil' tool we were using did not work with Netscape's cert7.db file. The certificates we renewed using certutil were not recognised by Netscape. Also the following customer's example, for some reason, did not work for us as well. This was because we cannot do any https in our production environment. Finally, we simply point Netscape to the .cer files stored in the local machine and we were able to import it in.

The following Customer's Example was created by Rob Ray at Nova Scotia Community College and is being used with his permission and thanks.

PeopleSoft Certificate Store:

Once all of the DCs have their updated certificates you are ready to create the keystore, which PeopleSoft will use. There is lots of information on SSL and certificates online and on the PeopleSoft site. I won't get into it all again here, but will give a little bit on info I found useful before we go into the "how to".

Netscape developed SSL. Other companies have taken it in different directions, but the basis is still the way Netscape created it. PeopleSoft uses Netscape APIs in their LDAP Business Interlinks and thus we have to use Netscape to create our keystore.

We have to use Netscape 4.7x because it creates cert7.db keystores. The newer Netscape programs create the newer cert8.db keystores and PeopleSoft cannot currently use those. You can download the 4.7x version you need from here: <http://browser.netscape.com/ns8/download/archive47x.jsp>

Once you have Netscape installed you are ready to create your keystore

Open Netscape and follow the prompts to create a user profile called "PeopleSoft". It was walk you through this is if it the first time you have used Netscape since the install.

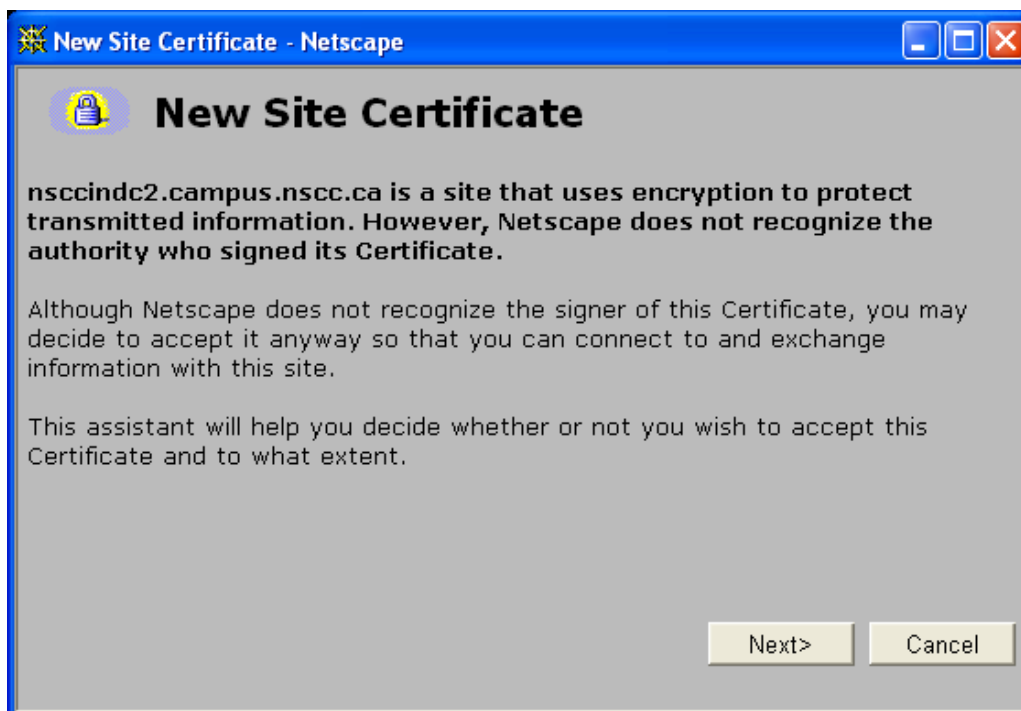
Once you have the profile and are ready to go type in the following:
`https://<Domain Controller Address>:636`

For example:

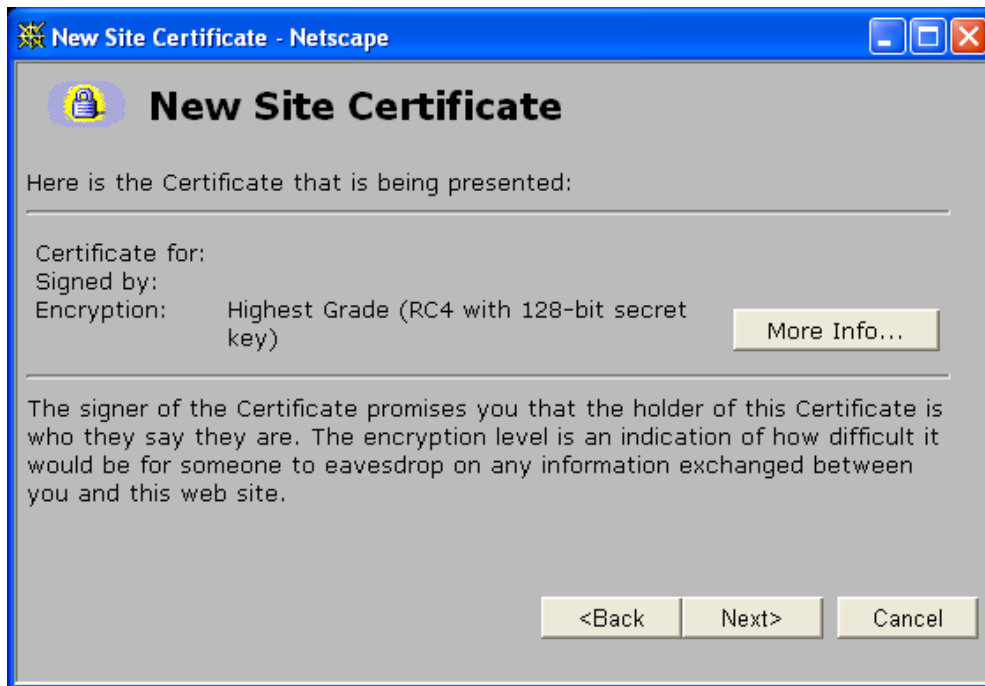
<https://nscindc2.campus.nsc.ca:636>

(This assumes we are still using the standard SSL LDAP port of 636)

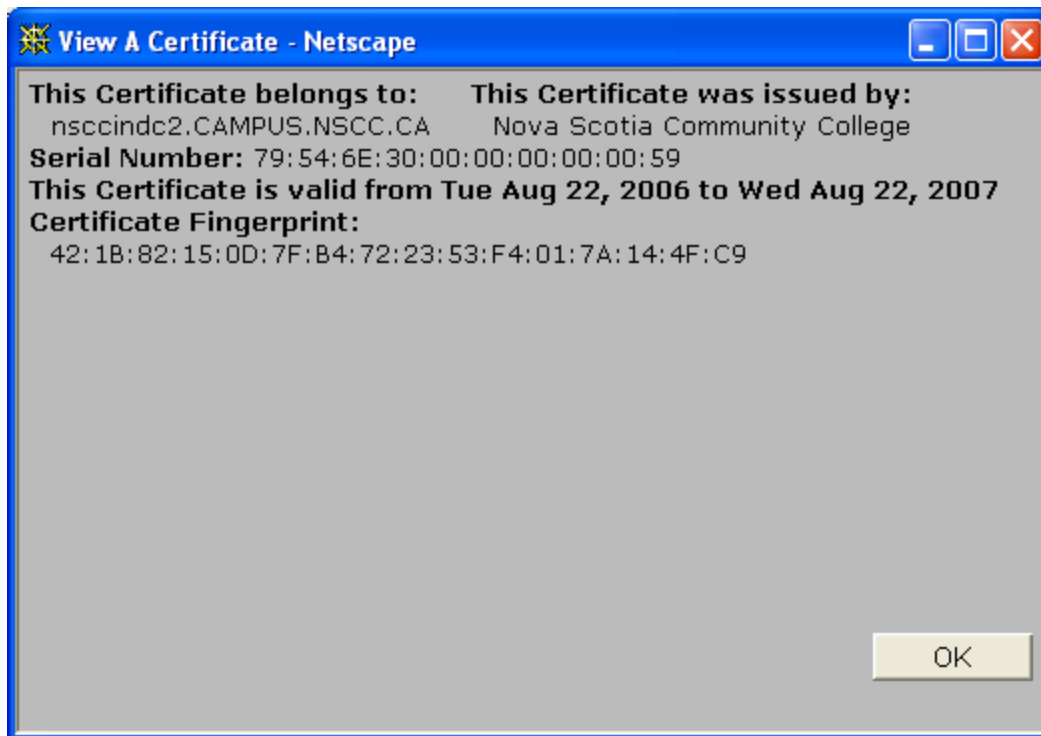
This will bring up the following pop up:



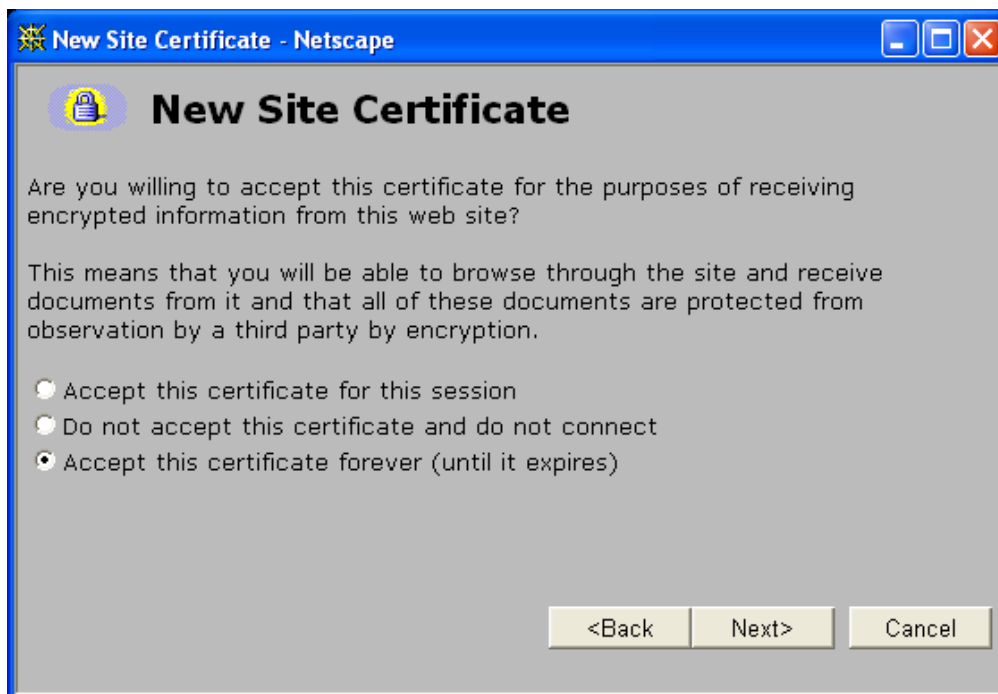
Hit *Next* which gives you:



At this point I would suggest clicking the *More Info* button to verify you have the correct certificate (look at the dates). This is where you will catch the certificate caching issue I mentioned above. When you press that you get:



You can see in the above that we are getting the date range we want (this was in Aug 2006). Press OK to close that window and then press *Next* on the window you started from. That brings you here:

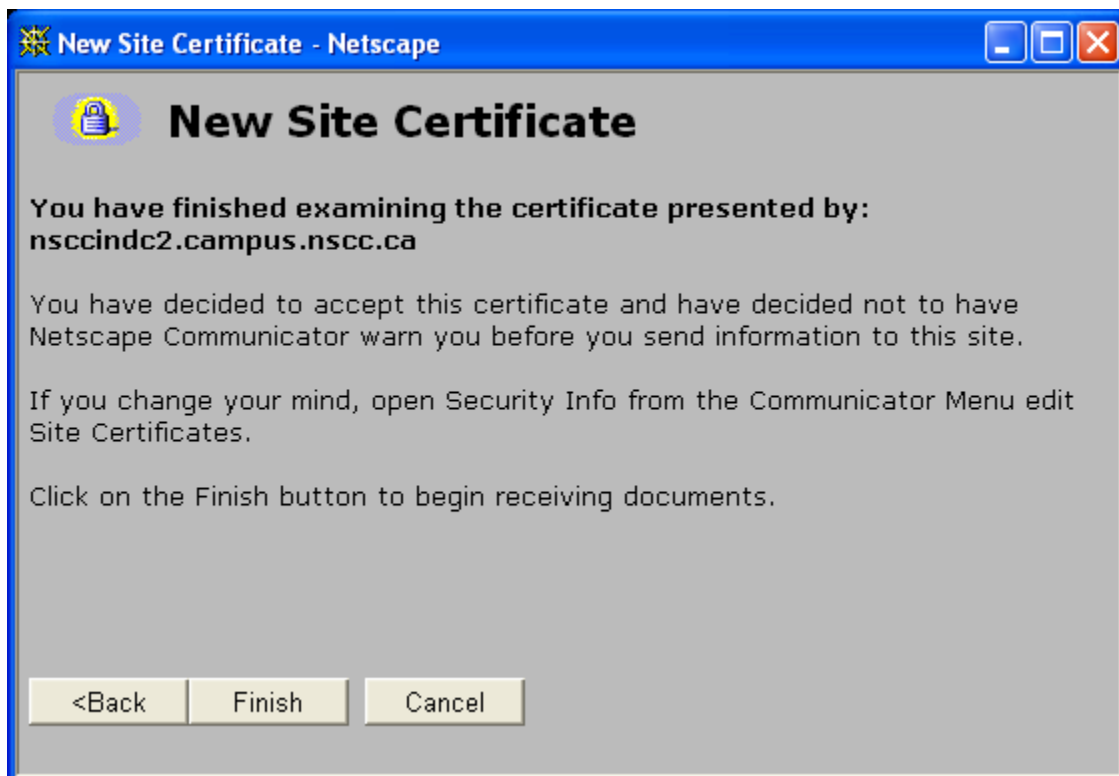


When the window above first comes up it defaults to *Accept this certificate for this session*. You MUST change this to what you see above: *Accept this certificate forever (until it expires)*.

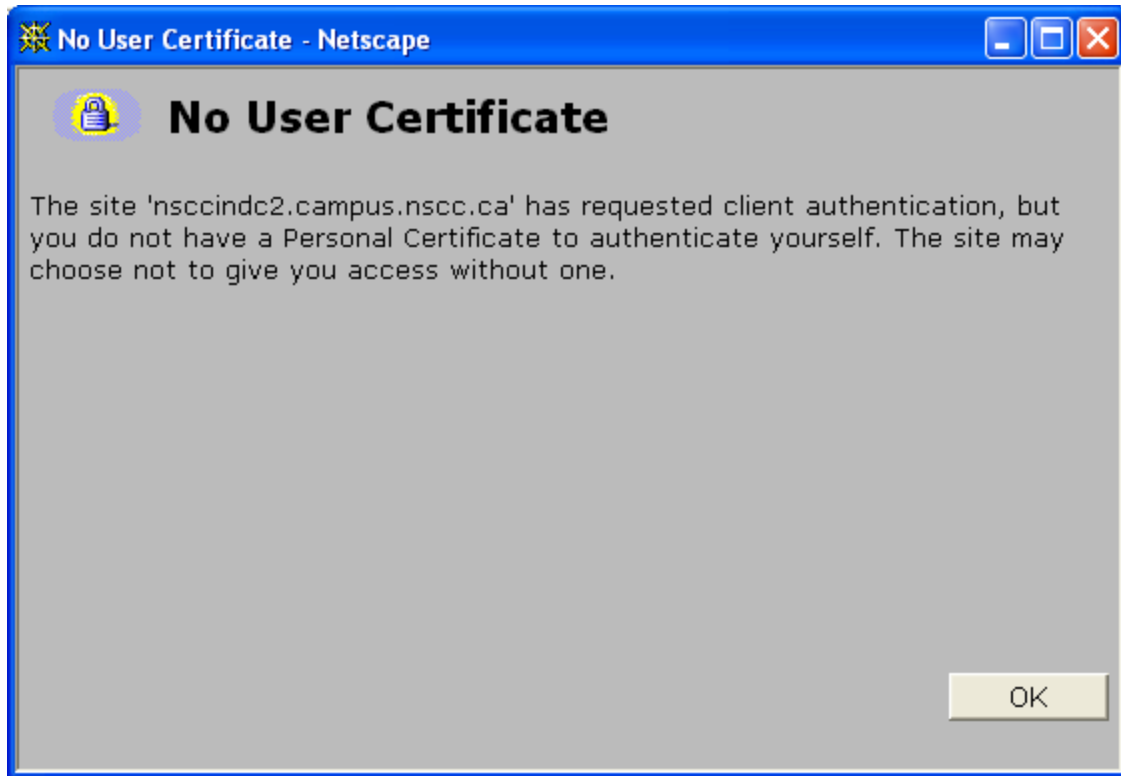
Then press *Next*:



Press *Next* again:

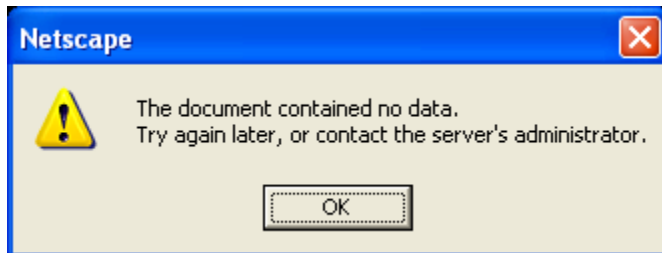


Press *Finish* (this is where things differ from the PeopleSoft document):



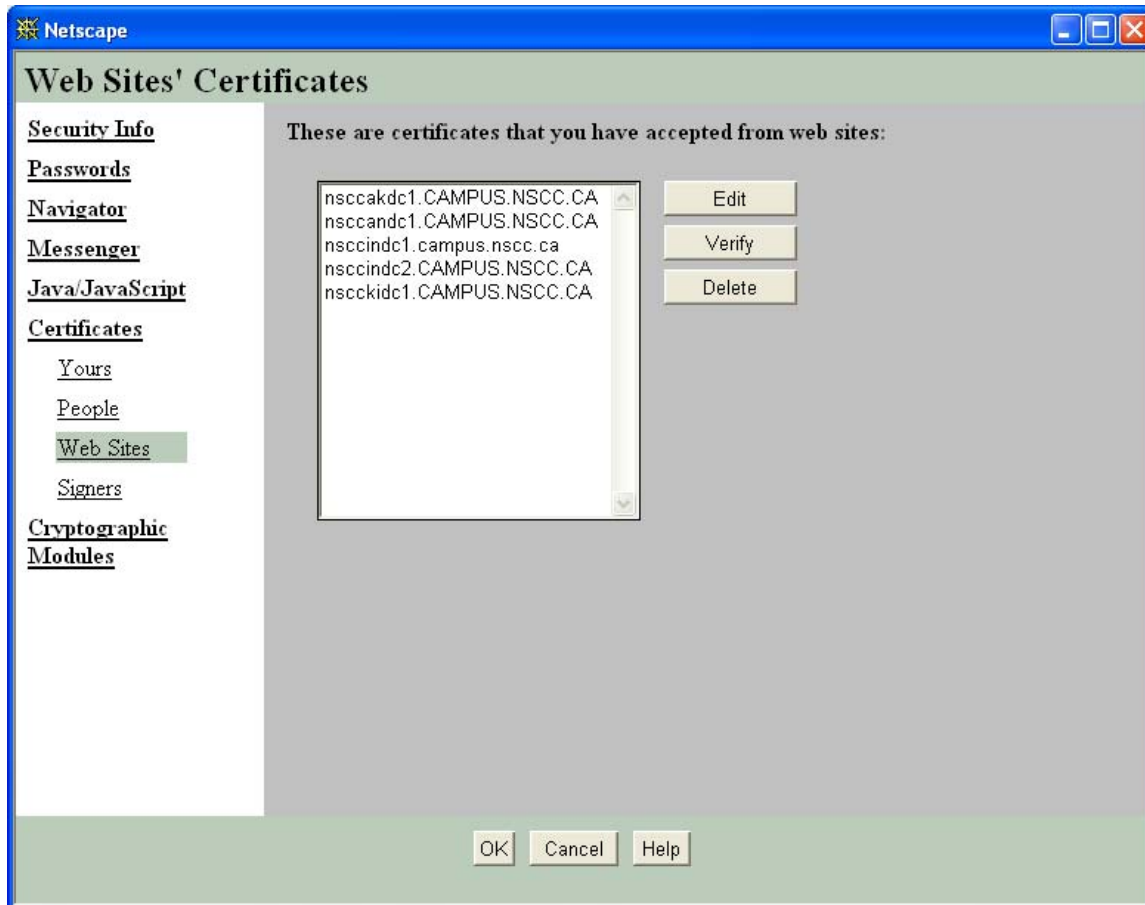
At this point we tried using a personal certificate. DON'T DO THIS!!! It gets rid of the errors below, but the keystore will NOT work with PeopleSoft.

Press OK:



Press OK and the error pop-up goes away.

You can then press the Security icon, which will give you access to the certificates. Navigate as seen in the screenshot below:



You can see we have added the cert for nscckindc2.

You must close this window and close Netscape at this point. Netscape does not save the cert7db file until you close it so if you ship this step your keystore will not have the data you tried to add.

Once you close Netscape navigate to the following directory (assuming you installed in the default location): c:\program files\netscape\users\peoplesoft\

You should see the 2 files we need in their which are named cert7.db and key3.db. Copy these 2 files and place them into the following locations (subject to changes since this document was created of course).

In the SA/HRMS system you need to put the 2 files into 3 places (4 very soon so I will include it).

```
nscckprdsaapp02 PS_HOME/appserv/SAPRD/cert
nscckprdsaapp02 PS_HOME/appserv/SELF_SERV/cert
```

```
nscckprdsaapp01 PS_HOME/appserv/SAPRD/cert
nscckprdsaapp01 PS_HOME/appserv/SELF_SERV/cert (this one will be set up soon)
```

When the files are used by PeopleSoft a 3rd file will appear in that directory called secmod.db. The appears a few hours after the system is up and being used and I do not know what the trigger is to create

it or what the file is for. This year I deleted (backed it up of course) it when I moved the cert7.db and key3.db files into the directory and let it recreate. I do not know if I needed to do this, but it worked fine so I would suggest doing that next summer.

In the finance system you need to put the files into a different location and the secmod.db file is not created. The files go here:

nscapp01 PS_HOME/appserv/FDMPRD

As we are going to be doing a finance upgrade this winter this will likely change to match the SA/HRMS system.

Each app server needs to be bounced and the cache cleared after the new keystores are in place. Once that is done you should be able to log in successfully. You can also use the test connection utility that is part of PeopleSoft delivered directory interface, which will allow you to verify all of your DCs. Signing in just tests the one you hit when you log in.

Once that is working you should bounce your application messaging services and clear the cache if it was not done above with the app server bounces.

Everything should now be working correctly!

STEP 2 -CONFIGURING BUSINESS INTERLINKS

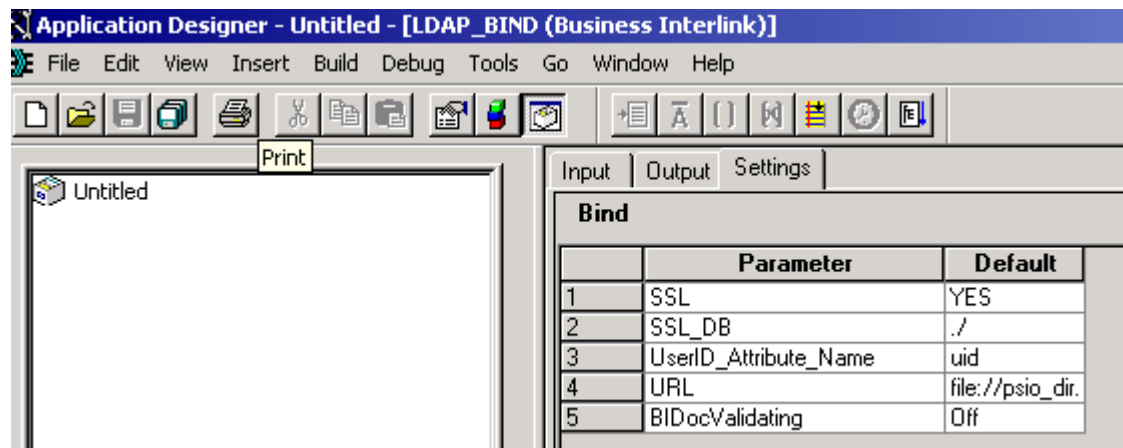
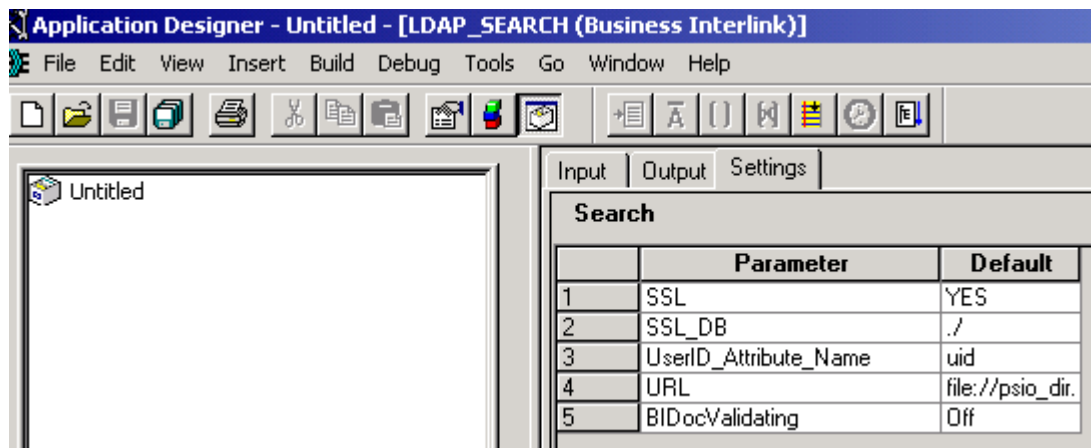
For PeopleSoft to understand where to find the cert7.db file you need to specify in the Business Interlinks for LDAP. These settings are found on the Settings tab of LDAP_Bind and LDAP_Search. The SSL_DB is name of the directory that was created above not the name of the file or the complete path of the location of the file. When the system is attempting to find the file it adds in the PS_Home/appserv/domain name along with the value entered below and cert7.db, which is hardcoded into the PeopleSoft code (C++).

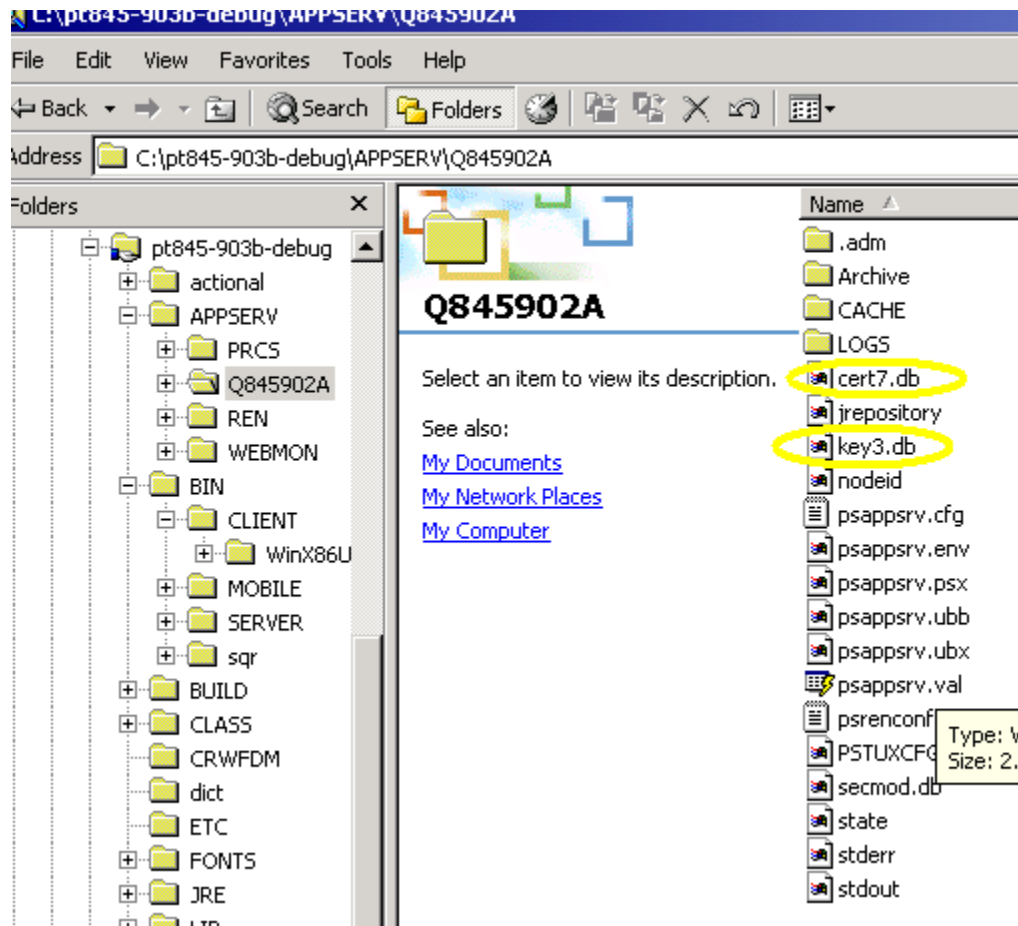
Check list for setup of LDAP over SSL

1) Launch App Designer. Open LDAP_BIND and LDAP_SEARCH BI's settings tab and setup the cert7.db/key3.db location in SSL DB.

2) Using CertUtil, create a new cert7.db, insert the root CA's certificate into it. Copy that new created cert7.db and key3.db under your PS_HOME/appserv/domain_name directory. In the screen shot below of the app server location the domain name is Q845902A as an example of where to place the cert7.db and key3.db.

NOTE! The **certutil tool** is a very complicated piece of software. It's a command line tool which a lot of users dislike as they are used to GUI tools. Basically said the Netscape option is easier to use from what most customers have reported. Certutil will work and do what is needed, but it may take some work to find the right combination of values and version.





3) Setup Sign-on PeopleCode.

Signon PeopleCode

Signon

☐ Invoke as user signing in

☒ Invoke as User ID: Password:

Signon PeopleCode Customize | Find | View All | First 1-6 of 5 Last

Sequence	Enabled	Record	Field Name	Event Name	Function Name	Exec Auth Fail
1	<input checked="" type="checkbox"/>	FUNCLIB_PWDCTL	PWDCNTL	FieldChange	Password_Controls	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	WWW_AUTHENTICATION	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	LDAP_AUTHENTICATION	<input checked="" type="checkbox"/>
4	<input type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	SSO_AUTHENTICATION	<input type="checkbox"/>
5	<input checked="" type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	LDAP_PROFILESYNCH	<input checked="" type="checkbox"/>

4) Configure Directory Setup by adding in your SSL port (Default is 636)

The screenshot shows the PeopleSoft Directory Setup configuration page. The left sidebar contains a menu with options like 'Configure Directory', 'Cache Directory Schema', 'Authentication Map', 'User Profile Map', 'Role Membership Rules', 'Delete Directory Configuration', 'Workflow Address Book', 'Security Objects', 'Query Security', 'Encryption', 'Common Queries', 'Mass Change Operator Security', 'Utilities', 'Workflow', 'Portal', 'Search Engine', 'Personalization', and 'Process Scheduler'. The main content area has tabs for 'Directory Setup', 'Additional Connect DN's', 'Schema Management', and 'Test Connectivity'. The 'Directory Setup' tab is active, showing fields for 'Directory ID' (JJAMES111302), 'Description' (JJAMES111302), 'Directory Product' (Sun One Directory Server), 'Default Connect DN' (cn="Directory Manager"), and 'Password'. Below these is a table for 'LDAP Server' with columns 'Server Name', 'Find', 'View All', 'First', '1 of 1', and 'Last'. The table contains one row for 'JJAMES111302' with 'Port' 389 and 'SSL Port' 636. At the bottom are buttons for 'Save', 'Return to Search', 'Previous tab', 'Next tab', and 'Refresh'.

4a) Click on the Test Connectivity tab to verify that the system is finding the SSL cert7.db file

The screenshot shows the 'Test Connectivity' tab in the PeopleSoft Directory Setup configuration page. The left sidebar is the same as in the previous screenshot. The main content area shows the results of the tests. Under 'Running Bind Tests', it shows 'Host: JJAMES111302:389', 'DN: cn="Directory Manager"', and 'Result: SUCCESS'. Under 'Running Search Tests', it shows 'Host: JJAMES111302:389', 'Reading RootDSE: SUCCESS', 'subSchemaSubEntry: cn=schema', 'Reading Schema: SUCCESS', 'Host: JJAMES111302:636', 'Reading RootDSE: SUCCESS', 'subSchemaSubEntry: cn=schema', and 'Reading Schema: SUCCESS'.

5) Setup Authentication Map by ensuring that the “Use Secure Socket Layer” is checked.

The screenshot shows the 'Authentication' configuration page for the 'JJAMES111302_AM' system. The left sidebar contains a menu with options like 'Directory', 'Authentication Map', 'User Profile Map', 'Role Membership', 'Rules', 'Delete Directory', 'Configuration', 'Workflow Address', 'Book', 'Security Objects', 'Query Security', 'Encryption', 'Common Queries', 'Mass Change Operator', 'Security', 'Utilities', 'Workflow', 'Portal', 'Search Engine', 'Personalization', 'Process Scheduler', 'Cube Manager', 'Application Engine', 'Integration Broker', 'REN Server Configuration', 'MultiChannel Framework', 'Archive Data', 'Data Archive Manager', 'Translations', 'EDI Manager', and 'Mass Changes'. The main content area is titled 'Authentication' and includes a 'Map Name' field set to 'JJAMES111302_AM' and a 'Status' dropdown set to 'Active'. Below this is the 'Directory Information' section, which includes a 'Directory ID' field set to 'JJAMES111302', a checkbox for 'Anonymous Bind' (unchecked), and a checked checkbox for 'Use Secure Socket Layer'. The 'Connect DN' field is set to 'cn="Directory Manager"'. A 'List of Servers' table shows one server with 'SeqNum' 10 and 'LDAP Server' 'JJAMES111302'. The 'User Search Information' section includes a 'Search Base' field set to 'ou=People, dc=corp, dc=peoplesoft, dc=com', a 'Search Scope' dropdown set to 'Sub', a 'Search Attribute' field set to 'uid', and a 'Search Filter' field set to '(uid=%SignonUserId)'. At the bottom are buttons for 'Save', 'Return to Search', 'Add', and 'Update/Display'.

6) Setup User profile Map.

The screenshot shows the 'User Profile Map' configuration page for the 'JJAMES111302_UP' system. The left sidebar contains a menu with options like 'Directory', 'Authentication Map', 'User Profile Map', 'Role Membership', 'Rules', 'Delete Directory', 'Configuration', 'Workflow Address', 'Book', 'Security Objects', 'Query Security', 'Encryption', 'Common Queries', 'Mass Change Operator', 'Security', 'Utilities', 'Workflow', 'Portal', 'Search Engine', 'Personalization', 'Process Scheduler', 'Cube Manager', 'Application Engine', 'Integration Broker', 'REN Server Configuration', 'MultiChannel Framework', 'Archive Data', 'Data Archive Manager', 'Translations', 'EDI Manager', and 'Mass Changes'. The main content area is titled 'User Profile Map' and includes a 'User Profile Map' field set to 'JJAMES111302_UP'. Below this is the 'Mandatory User Properties' section, which includes an 'Authentication Map' field set to 'JJAMES111302_AM', a 'Status' dropdown set to 'Active', a 'Directory ID' field set to 'JJAMES111302', and a 'User ID Attribute' field set to 'uid'. The 'ID Type' section includes an 'ID Type' dropdown set to 'None' and an 'ID Type Attribute' field set to 'None'. The 'Default Role' section includes a checked checkbox for 'Use default Role', a 'Role Name' field set to 'PeopleSoft User', and a 'Role Attribute' field. The 'Language' section includes a checked checkbox for 'Use Default Language Code', a 'Language' dropdown set to 'English', a 'LangCD' field, and a 'Language Code' field. At the bottom are buttons for 'New Window' and 'Custom'.

7) Save this page - Logout of the system - bounce App Server and Web Server - login as an LDAP user.

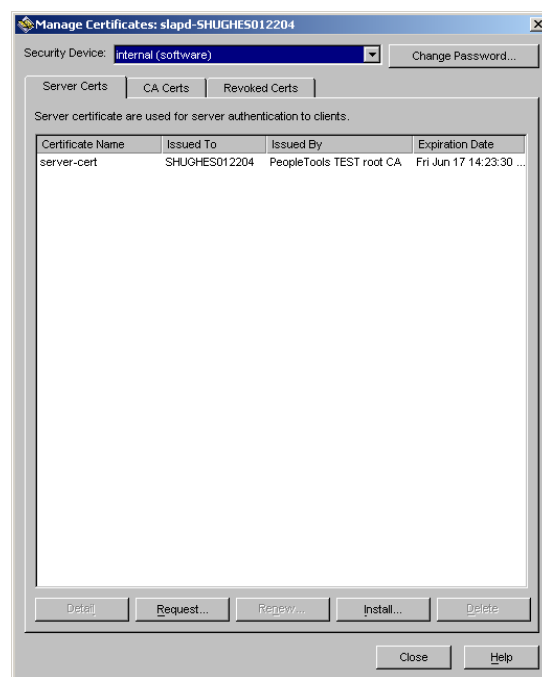
SETTING UP SSL TOKEN ON AN IPLANET 5.1 SERVER

Establishing a connection to the LDAP server using SSL requires that you obtain and install both a server certificate and a CA certificate from a certified Authority. In this example we are using Microsoft Certificate server.

Step 1- Request a Certificate on the iPlanet server

This is done by opening up iPlanet Directory Server console and selecting the manage certificates from the tasks tab.

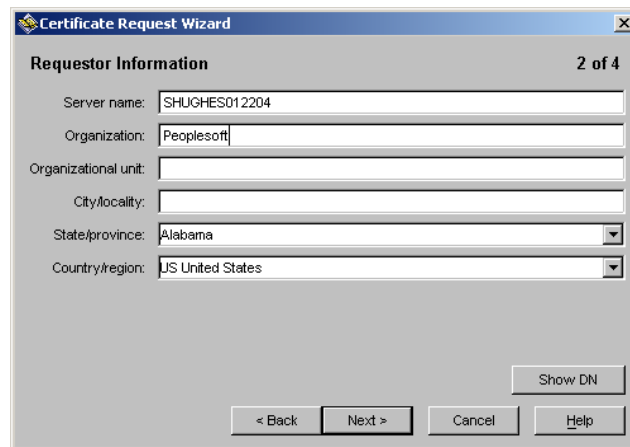
A. Once the Manage Certificates page (illustrated below) opens select Request.



B. Select next

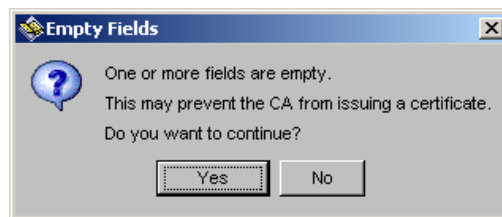


C. Enter your computer name and Organization but you can leave the rest as the default.



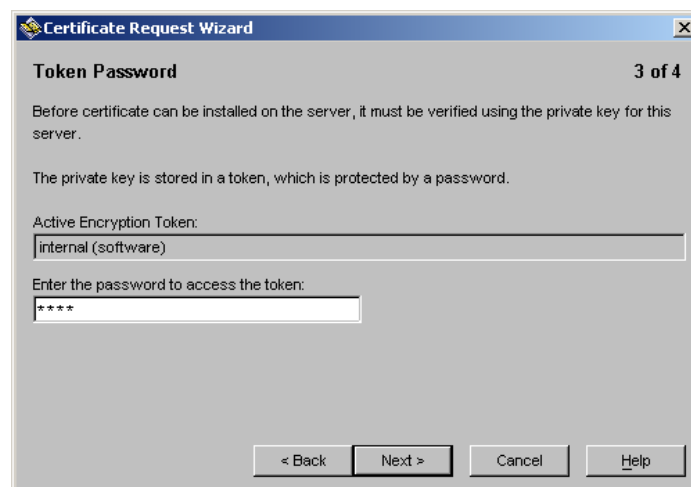
The screenshot shows the 'Certificate Request Wizard' window, step 2 of 4, titled 'Requestor Information'. It contains several input fields: 'Server name' with the value 'SHUGHES012204', 'Organization' with 'Peoplesoft', 'Organizational unit' (empty), 'City/locality' (empty), 'State/province' with a dropdown menu showing 'Alabama', and 'Country/region' with a dropdown menu showing 'US United States'. At the bottom right is a 'Show DN' button. At the bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

D. Error that appears if not all the values are selected. Just click YES.



The screenshot shows an 'Empty Fields' error dialog box. It features a question mark icon and the text: 'One or more fields are empty. This may prevent the CA from issuing a certificate. Do you want to continue?'. At the bottom are two buttons: 'Yes' and 'No'.

E. Select a basic password that will not allow people to break into your token.



The screenshot shows the 'Certificate Request Wizard' window, step 3 of 4, titled 'Token Password'. It contains the following text: 'Before certificate can be installed on the server, it must be verified using the private key for this server.' and 'The private key is stored in a token, which is protected by a password.' Below this is a dropdown menu for 'Active Encryption Token' showing 'internal (software)'. Then, it says 'Enter the password to access the token:' followed by a password input field with four asterisks '****'. At the bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

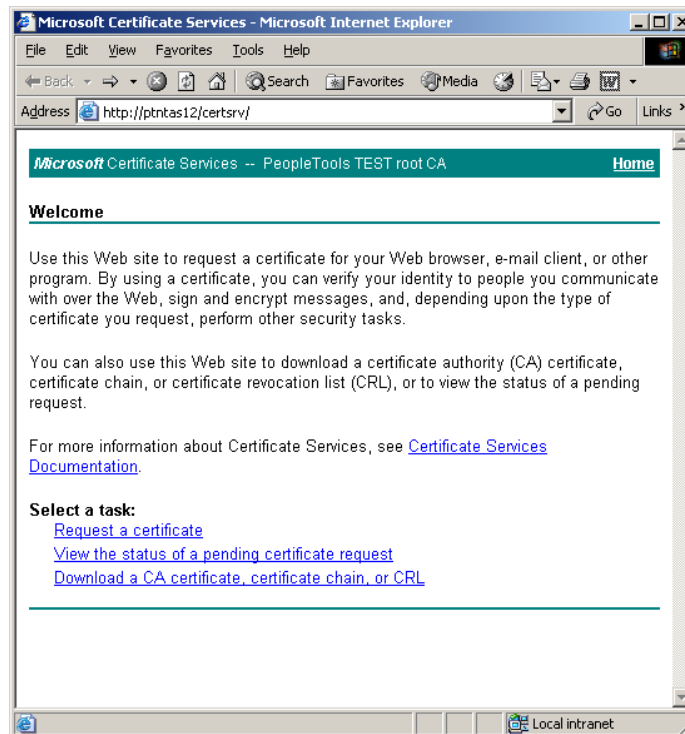
F. Select Save to file



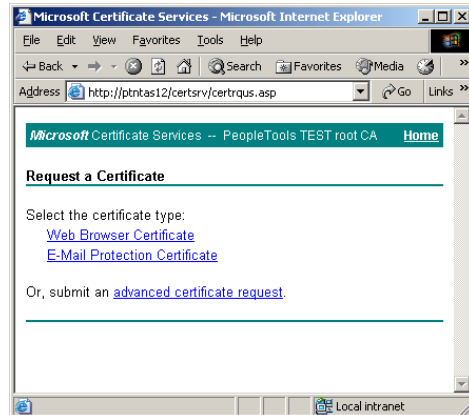
Step 2 - Post iPlanet request to Certificate Server

- You will either need to email your CA or obtain it through a web site. For our case we will use a web site.

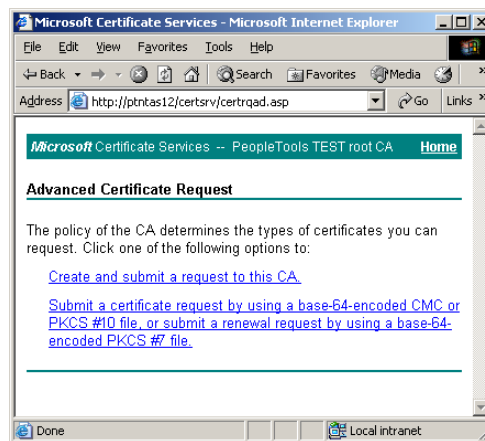
A. Select Request a Certificate.



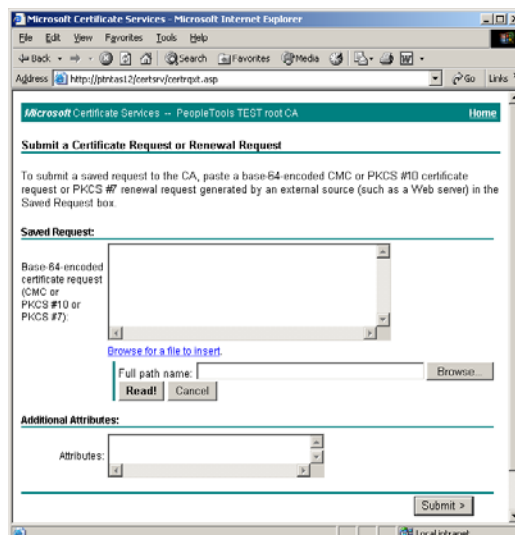
B. Select advanced certificate request



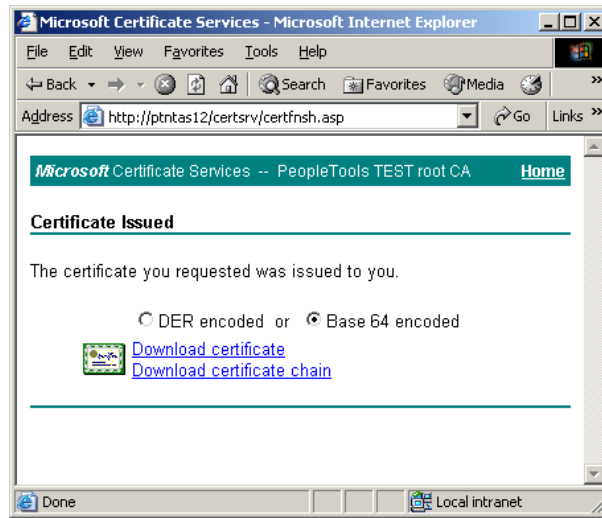
C. Select [Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.](#)



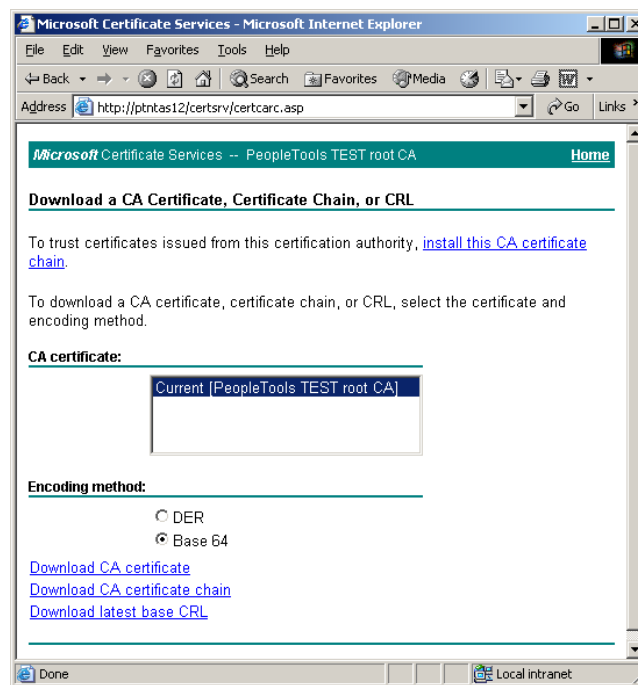
D. Open the request file you created in iPlanet through the Browse for a file. Browse to the file and then click the read button. For final submission you will need to click on the submit button on the bottom. This process will create a certnew.cer file



E. Ensure you select Base 64 encoded and then download the certificate to a known location. (file name will be certnew.cer)



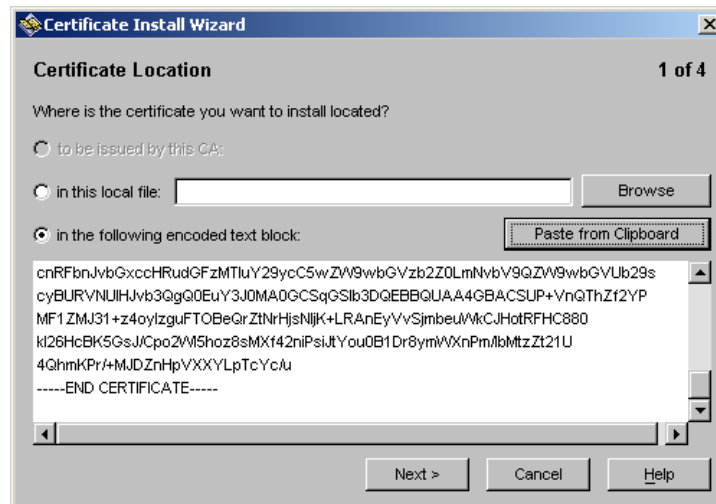
F. You will also need to download the CA Certificate, which can be found on the root page the Certificate web site. Change the Encoding method to Base 64 and select Download CA certificate. Save this file as CA Cert.cer.



Step 3 - Install certificate and CA certificate on iPlanet Server

- Connect back into iPlanet Directory Server console and open the Manage Certificate page.

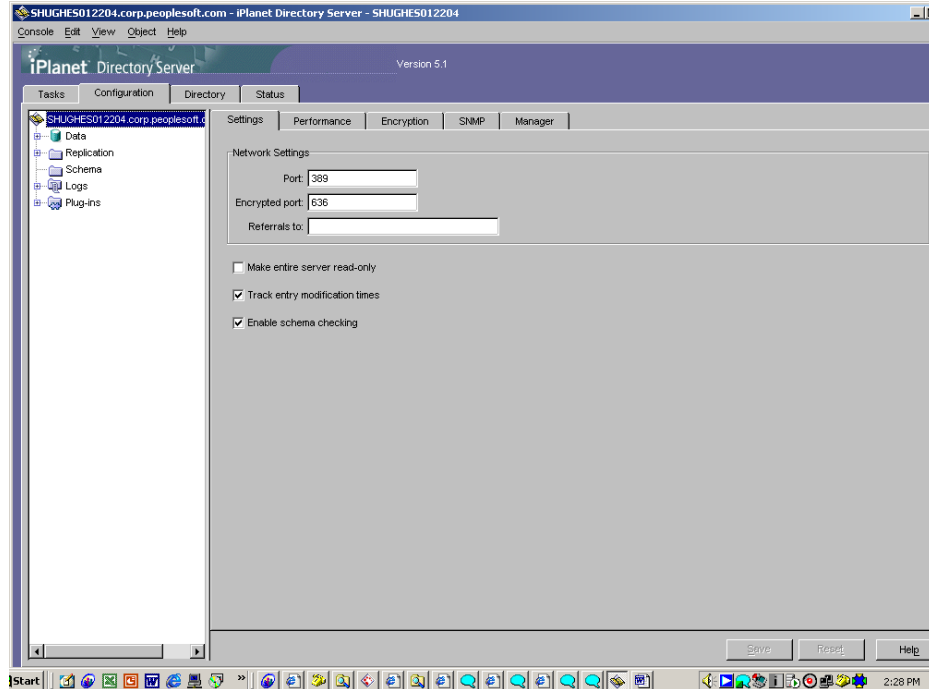
A. On the Server Certs Tab select the install button. The following window will appear. At this point you will need to open the certnew.cer file with notepad and copy the contents. On the Certificate Install Wizard page click on Paste from Clipboard. Click next through the rest of the pages until you are prompted for a password, which will be the password you choose earlier to create the certificate.



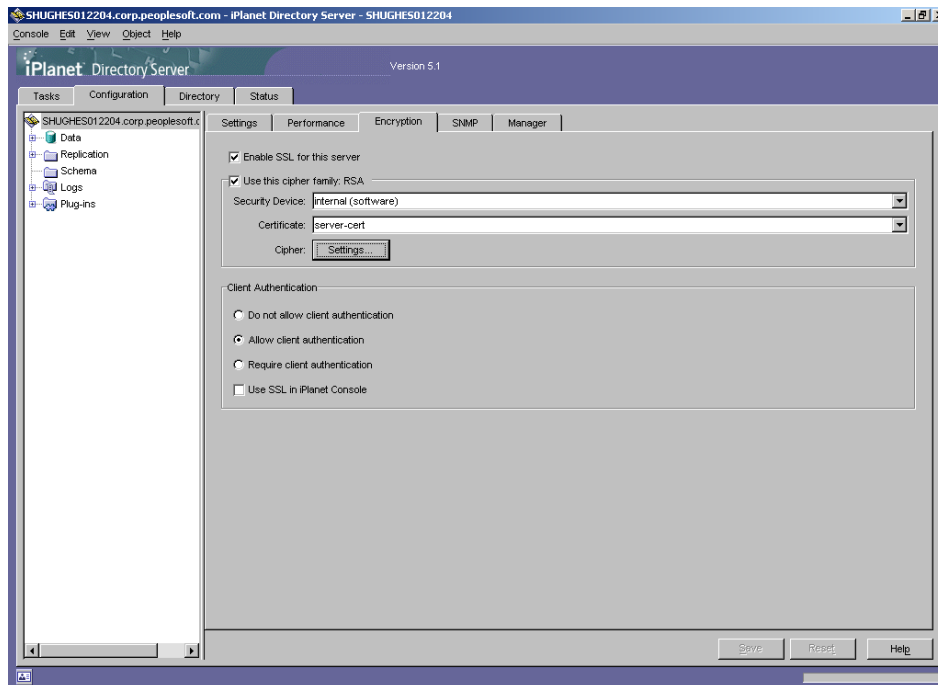
B. On the CA Certs tab, do exactly as in A but instead of opening the certnew.cer, open the CA Cert.cer file.

Step 4 - Configure the iPlanet Directory Server to accept SSL connections

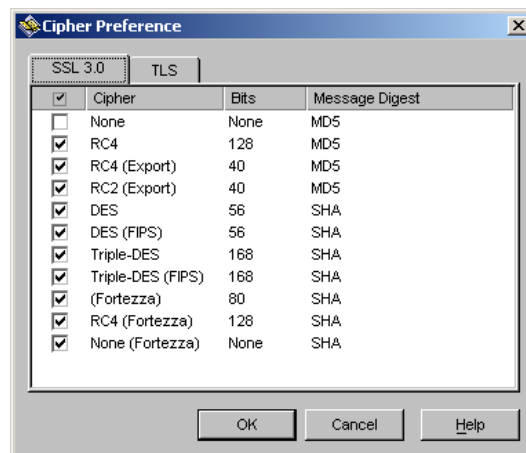
A. Within the console you need to select the Configuration tab then highlight the server from the list. On the settings tab you will need to establish the port to be used for encryption. The default is 636. If you change this value you will need to note the address so that you can change it in PeopleSoft.



B. Next we move to the Encryption tab where we will set up the cipher family and the client authentication. Check the Enable SSL for this server box along with the Use this cipher family: RSA box. From the certificate drop down select the server-cert, which is the server certificate installed earlier.



C. To select the cipher level that you want to allow to connect either check or uncheck the levels you want.



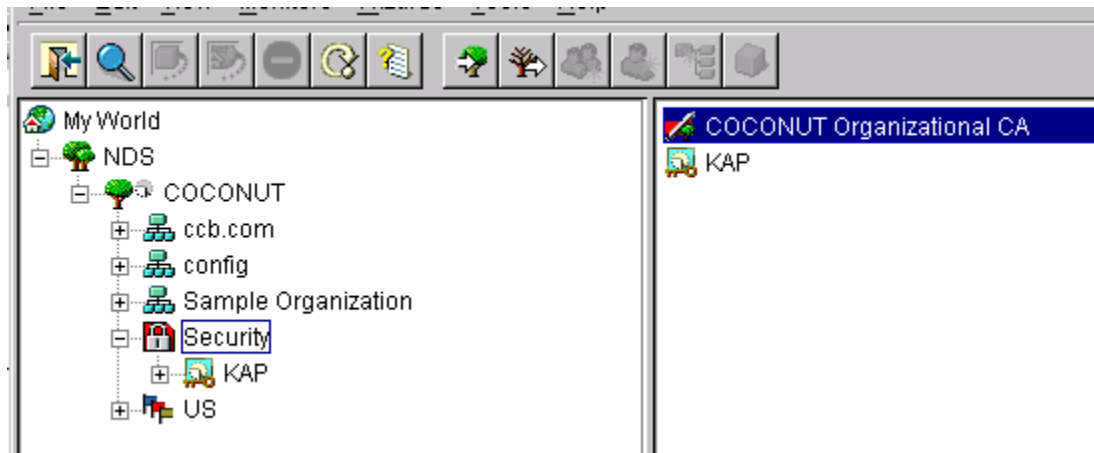
D. Once all these changes have been done you will need to restart the iPlanet server service for them to take affect.

SETTING UP SSL TOKEN ON AN NOVELL EDIRECTORY SERVER

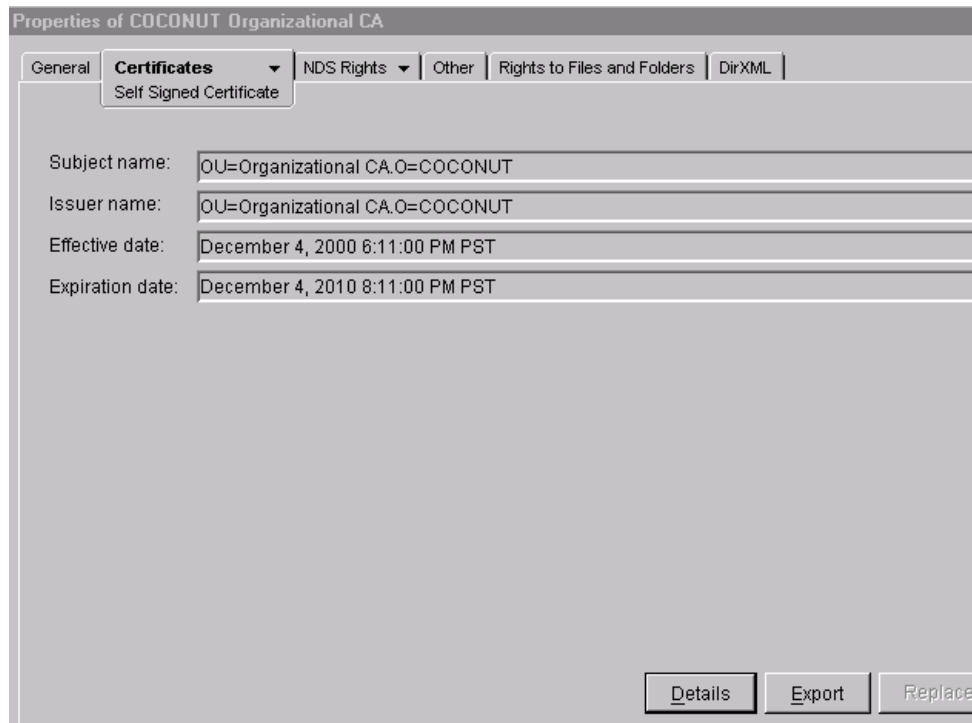
This section details how to configure NDS eDirectory V8.5 for LDAPS using the Organizational CA built into NDS's PKI services. This process will be different based on the directory you are using.

Step 1 - Export the Self-Signed Trusted Root Certificate from the Certificate Authority

- A. Start Console1 and drive to the Organizational CA object in the Security container



- B. Bring up the Properties dialog, go to the Certificates tab, and choose Self Signed Certificate from the tab menu



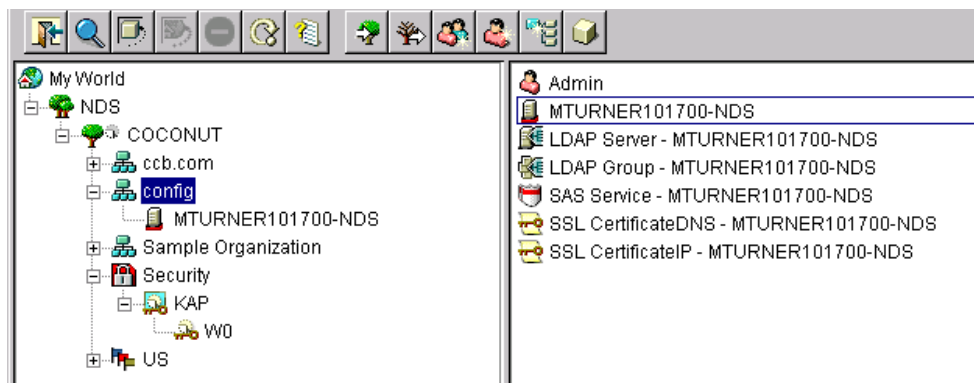
C. Click the Export button



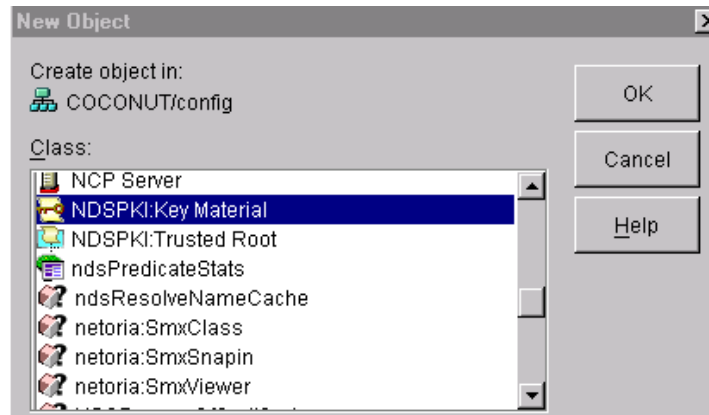
D. Choose File in binary DER format, pick a file name and location and click Export

Step 2 - Create a Server Certificate to be used by LDAP

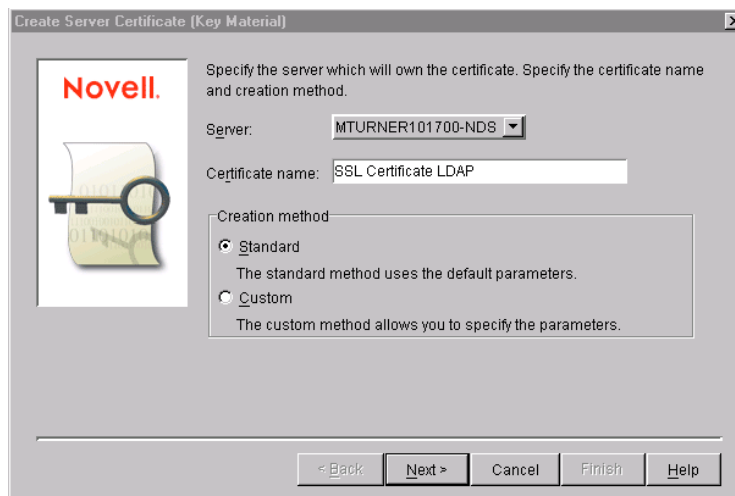
A. In Console1 drive to the container that holds the Server Object for the LDAP Server (this will be the config context if you installed using my instructions).



B. Right click on the container entry (i.e. Config) and choose NewObject. Scroll down and find NDSPKI: Key Material in the list and click OK. (Novell refers to certificates as Key Material objects).



C. In the ensuing dialog make sure the server name is the name of the directory server running the LDAP service, give the new certificate a meaningful name like “Public Key Server Cert to be used by LDAP” (ok maybe that’s a little long), choose the Standard creation method and click Next.

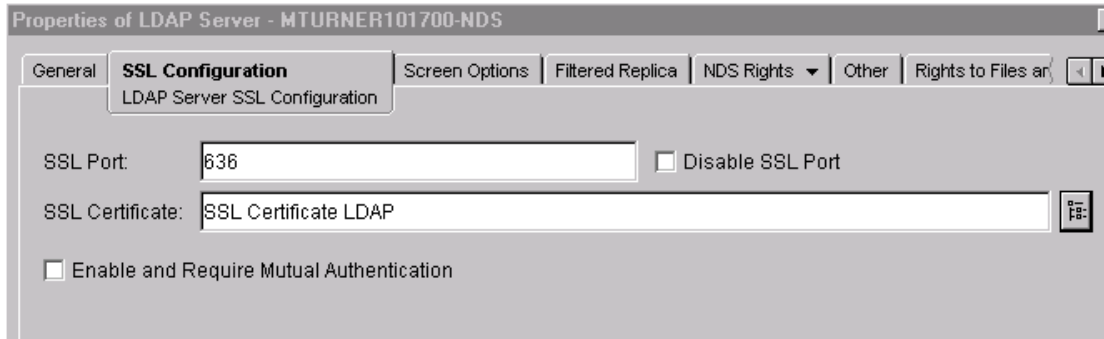


D. Review the information in the next dialog and click Finish if everything looks ok. You now have a certificate that contains the public key for the server running the LDAP service stored in your directory as an object



E. Next we tell the LDAP service what port to use for SSL connections and to issue that certificate when a client requests a connection on that port. Find the object representing your

LDAP Server; it will be in the same container you just created the cert in and will be named "LDAP Server - <hostname>-NDS. Bring up the properties dialog on the LDAP Server object and get yourself to the SSL Configuration tab.



F. Enter the port number you want to use for LDAPS and in the SSL Certificate field click the browse button and pick the cert you just created. Do not check "Enable and Require Mutual Authentication" unless you know what you're doing.

You're now ready to do LDAPS with NDS.

Microsoft has software similar to Novell's Certificate Service that can be used to generate certificates for use with LDAP. Please refer to Microsoft's documentation for info on using their certificate software and likewise for iPlanet.

Note: In real world scenarios you will get certificates from a bonafied Certificate Authority such as Entrust.Net or Verisign.

Note: As for utilizing Active Directory, first off, you will need to be running certificate services for your Active Directory domain. Once that is up and running, you need to grab the CA cert for your domain and then import it into the cert7.db file. Then just configure the Business Interlinks as defined in the documentation above and that was pretty much it.

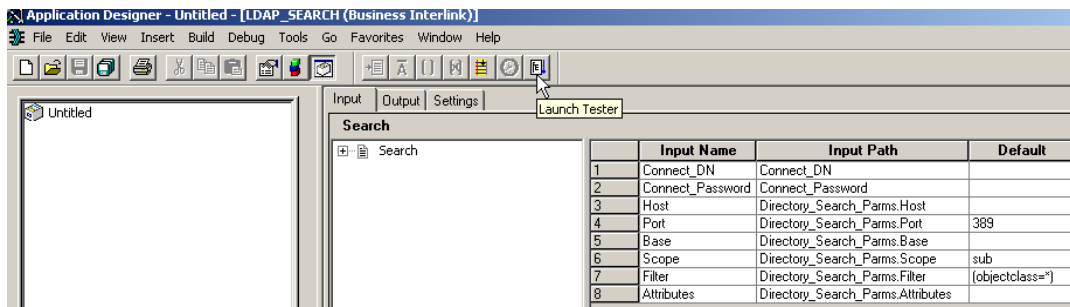
Appendix B – Troubleshooting Tips & Tools

In this section we will go through a few tools to test your LDAP connectivity within PeopleSoft and outside of PeopleSoft to validate the information you are using to search your directory.

HOW TO USE THE BUSINESS INTERLINK TESTER

This will work in PeopleTools 8.1x, 8.2x, and 8.4x

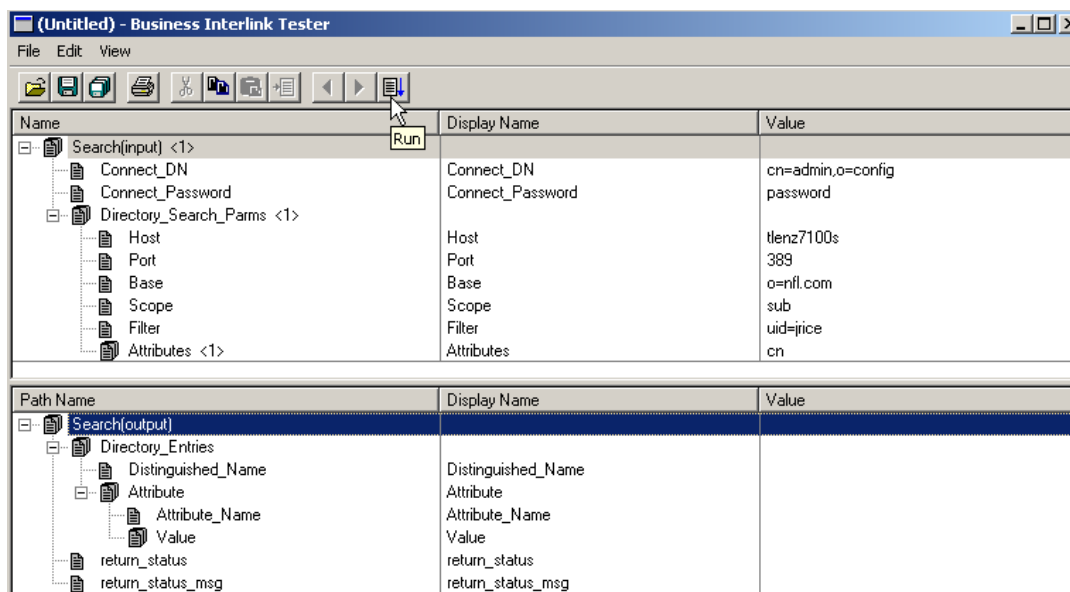
Go into Application Designer and open the Business Interlink called LDAP_SEARCH



Fill in the Default settings with your settings found on the Directory Authentication page. You can do this either before you launch the tester or after. You may want to do a “save as” and call this LDAP_SEARCH_TEST that way you will have your settings saved and not have to re-key your settings every time you want to test this.

After you have entered your setting correctly hit the Launch tester icon on the tool bar and this is what you will see. Make sure you expand the trees to see all the values.

Remember that every directory has different attributes, therefore you need to make sure the values you test with are valid values, and that your user DN has rights to read those attributes.



Now press the Run icon on the tool bar, and the tester will do the search, again expand all the trees to see the returned values.

(Untitled) - Business Interlink Tester		
File Edit View		
Name	Display Name	Value
[-] Search(input) <1>		
[-] Connect_DN	Connect_DN	cn=admin,o=config
[-] Connect_Password	Connect_Password	password
[-] Directory_Search_Parms <1>		
[-] Host	Host	tlenz7100s
[-] Port	Port	389
[-] Base	Base	o=nfl.com
[-] Scope	Scope	sub
[-] Filter	Filter	uid=jrice
[-] Attributes <1>	Attributes	cn
Path Name	Display Name	Value
[-] Search(output) <1>		
[-] Directory_Entries <1>		
[-] Distinguished_Name	Distinguished_Name	cn=Jerry Rice,ou=Oakland Raiders,ou=Tea...
[-] Attribute <1>	Attribute	
[-] Attribute_Name	Attribute_Name	cn
[-] Value <1>	Value	Jerry Rice
[-] return_status	return_status	0
[-] return_status_msg	return_status_msg	Success

If you have a bad filter or invalid attribute or the attribute you will get a different error:

(Untitled) - Business Interlink Tester		
File Edit View		
Name	Display Name	Value
[-] Search(input) <1>		
[-] Connect_DN	Connect_DN	cn=admin,o=config
[-] Connect_Password	Connect_Password	password
[-] Directory_Search_Parms <1>		
[-] Host	Host	tlenz7100s
[-] Port	Port	389
[-] Base	Base	o=nfl.com
[-] Scope	Scope	sub
[-] Filter	Filter	uid = jrice
[-] Attributes <1>	Attributes	cn
Path Name	Display Name	Value
[-] Search(output) <1>		
[-] Directory_Entries <1>		
[-] Distinguished_Name	Distinguished_Name	
[-] Attribute	Attribute	
[-] return_status	return_status	87
[-] return_status_msg	return_status_msg	Bad search filter

If the password or User DN is incorrect you will get this error:

(Untitled) - Business Interlink Tester		
Name	Display Name	Value
Search(input) <1>		
Connect_DN	Connect_DN	cn=admin,o=config
Connect_Password	Connect_Password	tom
Directory_Search_Parms <1>		
Host	Host	tlenz7100s
Port	Port	389
Base	Base	o=nfl.com
Scope	Scope	sub
Filter	Filter	uid=jrice
Attributes <1>	Attributes	cn
Path Name	Display Name	Value
Search(output) <1>		
Directory_Entries <1>		
Distinguished_Name	Distinguished_Name	
Attribute	Attribute	
Attribute_Name	Attribute_Name	
Value	Value	
return_status	return_status	49
return_status_msg	return_status_msg	Invalid credentials

If you are looking for a group then the search will look like this:

Application Designer - Untitled - [LDAP_SEARCH_TEST (Business Interlink)]

File Edit View Insert Build Debug Tools Go Favorites Window Help

File Edit View Insert Build Debug Tools Go Favorites Window Help

Search

Search

	Input Name	Input Path	Default
1	Connect_DN	Connect_DN	cn=admin,o=config
2	Connect_Password	Connect_Password	*****
3	Host	Directory_Search_Parms.Host	tlenz7100s
4	Port	Directory_Search_Parms.Port	389
5	Base	Directory_Search_Parms.Base	o=nfl.com
6	Scope	Directory_Search_Parms.Scope	sub
7	Filter	Directory_Search_Parms.Filter	(objectclass=group)
8	Attributes	Directory_Search_Parms.Attributes	member

And your results will look like this:

(Untitled) - Business Interlink Tester		
Name	Display Name	Value
Search(input) <1>		
Connect_DN	Connect_DN	cn=admin,o=config
Connect_Password	Connect_Password	password
Directory_Search_Parms <1>		
Host	Host	tlenz7100s
Port	Port	389
Base	Base	o=nfl.com
Scope	Scope	sub
Filter	Filter	(objectclass=group)
Attributes <1>	Attributes	member
Path Name	Display Name	Value
Search(output) <1>		
Directory_Entries <1>		
Distinguished_Name	Distinguished_Name	cn=Coaches,ou=Teams,o=NFL.com
Attribute <1>	Attribute	
Attribute_Name	Attribute_Name	member
Value <1>	Value	cn=Mike Shanahan,ou=Denver Broncos,ou...
return_status	return_status	0
return_status_msg	return_status_msg	Success

HOW TO USE THE LDAPSEARCH TOOL

This is not a PeopleSoft delivered tool but an industry standard and can be found at various sites on the internet or attached to the PeopleSoft GSC **SOLUTION ID 200762991**.

1. You need the ldapsearch tools. These need to be installed in your Winnt, System32 directory.

See Attached LDAPTOOLS zip file in **SOLUTION ID 200762991** that contain the search tool executables.

2. Now you need to know how to use these tools.

From the command prompt you will type in: C:\> ldapsearch

This will give you the parameters you will need to know to search your directory and will show you that you have the search tools installed correctly.

```
MS Command Prompt
C:\>ldapsearch
usage: ldapsearch -b basedn [options] filter [attributes...]
       ldapsearch -b basedn [options] -f file [attributes...]
where:
  basedn      base dn for search
              <if the environment variable LDAP_BASEDN is set,
              then the -b flag is not required>
  filter      RFC-2254 compliant LDAP search filter
  file        file containing a sequence of LDAP search filters to use
  attributes  whitespace-separated list of attributes to retrieve
              <if no attribute list is given, all are retrieved>
options:
  -n          show what would be done but don't actually do it
  -v          run in verbose mode <diagnostics to standard output>
  -h host     LDAP server name or IP address
  -p port     LDAP server TCP port number
  -U n        LDAP protocol version number <2 or 3; default is 3>
  -Z          make an SSL-encrypted connection
  -P pathname path to SSL certificate database
  -N pathname name of certificate to use for SSL client authentication
  -K pathname path to key database to use for SSL client authentication
  -m pathname path to security module database
  -W          SSL key password
  -Q [token] certificate name] PKCS 11
  -X pathname FORTEZZA compromised key list <CKL>
  -I pin      card password file
  -D binddn   bind dn
  -w passwd   bind passwd <for simple authentication>
  -E          ask server to expose <report> bind identity
  -R          do not automatically follow referrals
  -O hop lim  maximum number of referral hops to traverse
  -M          manage references <treat them as regular entries>
  -0          ignore LDAP library version mismatches
  -i charset  character set for command line input <default is locale>
  -k dir      conversion routine directory <default is .>
  -y proxydn  DN used for proxy authorization
  -H          display usage information
  -t          write values to files in temp directory.
  -U          produce file URLs in conjunction with -t
  -e          minimize base-64 encoding of values
  -u          include User Friendly entry names in the output
  -o          print entries using old format <default is LDIF>
  -l          don't fold <wrap> long lines <default is to fold>
  -1          omit leading "version: 1" line in LDIF output
  -A          retrieve attribute names only <no values>
  -B          print non-ASCII values when old format <-o> is used
  -x          performing sorting on server
  -F sep      print 'sep' instead of '=' between attribute names and values
  -S attr     sort the results by attribute 'attr'
  -s scope    one of base, one, or sub <search scope>
  -a deref    one of never, always, search, or find <alias dereferencing>
  -l time lim time limit <in seconds> for search
  -z size lim size limit <in entries> for search
  -G before:after:index:count ; before:after:value where 'before' and
              'after' are the number of entries surrounding 'index.'
              'count' is the content count, 'value' is the search value.
```

3. Here is an example of a directory search using eDirectory from Novel:

C:\>ldapsearch -h host name -p "port" -b "search base" -D "Distinguish name" -w "password" (search filter) attribute

searching for uid = JPelayo:

```

C:\>ldapsearch -h JPELAY0061900 -b "o=gsc.com" -D "cn=admin,o=config" -w admin (
uid=JPelayo)
version: 1
dn: cn=John Pelayo,ou=AppDev,o=GSC.com
uid: JPelayo
Language: ENGLISH
sn: JPelayo
securityEquals: cn=Managers,o=GSC.com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: ndsLoginProperties
objectClass: top
networkAddress:: OSMEC9iD3P4=
networkAddress:: OSMECX8AAAE=
loginTime: 20010816143557Z
groupMembership: cn=Managers,o=GSC.com
cn: John Pelayo

```

Notice the list of attributes for this user. In this case the uid is what the signon PeopleCode would be looking for.

Here is an example of a search for all directory groups under the search base of gsc.com:

```

C:\>ldapsearch -h JPELAY0061900 -b "o=gsc.com" -D "cn=admin,o=config" -w admin (
objectclass=groupofnames) member
version: 1
dn: cn=Managers,o=GSC.com
member: cn=John Pelayo,ou=AppDev,o=GSC.com
member: cn=Tom Lenz,ou=AppDev,o=GSC.com

dn: cn=Supervisors,o=GSC.com
member: cn=Erin Knapp,ou=Reporting Tools,o=GSC.com

dn: cn=TEST,o=GSC.com

```

Notice that the search found 3 groups, Managers, Supervisors, and test, and also shows the members of those groups.

Here are some Microsoft Active Directory examples:

Search for a sAMAccountName:

sAMAccountName = JLENZ

```
ldapsearch -h ptntldap01 -p 389 -b "cn=users,dc=ptntldap,dc=com" -D "cn=administrator,cn=users,dc=ptntldap,dc=com" -w "password" samaccountname=JLENZ
```

Or you can do samaccountname=* and get all users to return

```
M:\>ldapsearch -h ptntldap01 -p 389 -b "cn=users,dc=ptntldap,dc=com" -D "cn=administrator,cn=users,dc=ptntldap,dc=com" -w "password" samaccountname=JLENZ
version: 1
dn: CN=Julie Lenz,CN=Users,DC=ptntldap,DC=com
memberOf: CN=TEST,CN=Users,DC=ptntldap,DC=com
accountExpires: 9223372036854775807
badPasswordTime: 126769464906024368
badPwdCount: 0
codePage: 0
cn: Julie Lenz
countryCode: 0
displayName: Julie Lenz
givenName: Julie
instanceType: 4
lastLogoff: 0
lastLogon: 126769464960903280
logonCount: 0
distinguishedName: CN=Julie Lenz,CN=Users,DC=ptntldap,DC=com
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=ptntldap,DC=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
objectGUID:: aUPT62MmLUGLzGES/PAt4Q==
objectSid:: AQUAAAAAAAAUAAAA+jxPessfsqKmxTHUMwkAAA==
primaryGroupID: 513
pwdLastSet: 126769470839856800
name: Julie Lenz
sAMAccountName: jlennz
sAMAccountType: 805306368
sn: Lenz
userAccountControl: 512
userPrincipalName: jlennz@ptntldap.com
uSNCchanged: 302468
uSNCreated: 278950
whenChanged: 20020919221123.0Z
whenCreated: 20020805151712.0Z
M:\>
```


Searching for a group

ldapsearch -h ptntldap01 -p 389 -b "cn=users,dc=ptntldap,dc=com" -D "cn=administrator,cn=users,dc=ptntldap,dc=com" -w "password" (objectclass=group) cn

```
M:\>ldapsearch -h ptntldap01 -p 389 -b "cn=users,dc=ptntldap,dc=com" -D "cn=administrator,cn=users,dc=ptntldap,dc=com" -w "password" (objectclass=group) cn
version: 1
dn: CN=nisgroup,CN=Users,DC=ptntldap,DC=com
cn: nisgroup

dn: CN=Informix-Admin,CN=Users,DC=ptntldap,DC=com
cn: Informix-Admin

dn: CN=GSC,CN=Users,DC=ptntldap,DC=com
cn: GSC

dn: CN=Domain Computers,CN=Users,DC=ptntldap,DC=com
cn: Domain Computers

dn: CN=Domain Controllers,CN=Users,DC=ptntldap,DC=com
cn: Domain Controllers

dn: CN=Schema Admins,CN=Users,DC=ptntldap,DC=com
cn: Schema Admins

dn: CN=Enterprise Admins,CN=Users,DC=ptntldap,DC=com
cn: Enterprise Admins

dn: CN=Cert Publishers,CN=Users,DC=ptntldap,DC=com
cn: Cert Publishers

dn: CN=Domain Admins,CN=Users,DC=ptntldap,DC=com
cn: Domain Admins

dn: CN=Domain Users,CN=Users,DC=ptntldap,DC=com
cn: Domain Users

dn: CN=Domain Guests,CN=Users,DC=ptntldap,DC=com
cn: Domain Guests
```

LDAP SEARCH with a DN that has limited rights

If the connect DN has limited rights to view only certain directory objects, this could impact your ability to logon correctly if other attributes are required from the user profile creation or authentication process.

```
C:\>ldapsearch -htlenz7100s -h=nfl.com -Dcn=tlenz,o=config -wpassword uid=jrice
version: 1
dn: cn=Jerry Rice,ou=Oakland Raiders,ou=Teams,o=NFL.com
mail: jrice@raiders.com
uid: jrice
givenName: Jerry
sn: Rice
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: ndsLoginProperties
objectClass: top
networkAddress:: 05MEBtiD3ME=
groupMembership: cn=Players,ou=Teams,o=NFL.com
```

LDAP SEARCH with a DN that has **FULL** rights to read **ALL** attributes in the directory that have values.

```
C:\>ldapsearch -htlenz7100s -h=nfl.com -Dcn=tlenz,o=config -wpassword uid=jrice
version: 1
dn: cn=Jerry Rice,ou=Oakland Raiders,ou=Teams,o=NFL.com
mail: jrice@raiders.com
uid: jrice
givenName: Jerry
fullName: Jerry Rice
language: ENGLISH
title: 6602
telephoneNumber: ALLPAMLS
sn: Rice
securityEquals: cn=Players,ou=Teams,o=NFL.com
ou: ALLPAMLS
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: ndsloginProperties
objectClass: top
networkAddress:: OSMEBTiD3ME=
loginTime: 20020410214419Z
l: ALLPAMLS
groupMembership: cn=Players,ou=Teams,o=NFL.com
facsimileTelephoneNumber: ALLPAMLS
description: ALLPAMLS
cn: Jerry Rice
```

You can see the difference in the number of attributes the limited user could see as compared to the user with full rights.

To do a search to see the directory schema run the following command:

```
ldapsearch -h ptntldap01 -p 389 -D "cn=admin,dc=ptntldap,dc=com" -w "password" -s
base -b "CN=Aggregate,CN=Schema,CN=Configuration,DC=ptntldap,DC=com" "objectclass=*
```

NOTE: This will validate that your user DN can read the schema of your directory. You will need to make corrections in the syntax above for YOUR user DN and the location of your schema.

If you leave out any variable like the search base, the DN, or the host you will get the main page back. If you use the wrong password or do not have rights to read the directory you will get invalid credentials. If you just get a blank line with the C:\ prompt back to whatever you are looking for is not there.

Ldapsearch for SSL

You need to add a -Z -P "put the full path of your cert7.db"

Here is an example:

```
ldapsearch -h ptntldap02 -p 636 -Z -P c:\certificate\cert7.db -D "cn=admin,o=ccb.com" -w"password" -b
"o=ccb.com" "objectclass=*
```

Searching for unfollowed referrals

You will want to add a -v -R to your ldapsearch string and this will show you if your search is waiting on a referral. This should be done if you are searching from the root of your directory, or if you are

experiencing any performance issues during the logon process. So your ldapsearch would look something like this:

```
ldapsearch -v -R -h ptntldap01 -p 389 -b "cn=users,dc=ptntldap,dc=com" -D  
"cn=administrator,cn=users,dc=ptntldap,dc=com" -w "password" samaccountname=JLENZ
```

Appendix C – GSC LDAP Solutions

This is not a complete list and this document will be updated periodically with corrected information.

Solution ID - Solution Summary

699537 E-LDAP: Authentication Troubleshooting guide for PT 8.1x
701179 E-LDAP: No rows exist for the specified keys USER_PROFILE (91,50)
703564 E-LDAP: Directory Group Import Map DIRGROUPS is not delivered in PT 8.1x
705055 E-LDAP: How to enable SSL with LDAP on PeopleTools 8.x
705616 E-LDAP: Error at log in says More than one row exists (91,51)
705907 E-LDAP: Configuration and Setup issues that are beyond the GSC support
713290 E-LDAP: Can PeopleSoft password controls be used with LDAP authentication?
715498 E-LDAP: How to setup LDAP Directory Group Import in PeopleTools 8.1x
716723 E-LDAP: PT 8.1x cannot logon to application in client 3-tier mode with LDAP
720353 E-LDAP: User profiles are created in UPPER CASE on the PSOPRDEFN table
720608 E-LDAP: Portal Guest Home Page Pagelet doesn't login properly using LDAP
200723906 E-LDAP: What is caching directory schema in PeopleTools 8.4? Is it required?
200725223 E-LDAP: How to setup LDAP authentication with PeopleTools 8.4
200725514 E-LDAP: Directory Dynamic Role Rules AE process is not completing successfully
200725515 E-LDAP: UserLDAPAlias on the optional user properties page is not being written to the User Profile
200727181 E-LDAP: LDAP Authentication fails on PT 8.41
200727401 E-LDAP: If password is greater than 8 characters the bind will fail
200729501 E-LDAP: Dynamic Members based on LDAP role rule displays User ID = Common
200729697 E-LDAP: What is encryption used for in the LDAP_BIND Business Interlink?
200729872 E-LDAP: PT 8.18 LDAP authentication fails when app server on UNIX
200730300 E-LDAP: SSO between Portal on PT 8.4x and Content Provider on PT 8.1x
200731865 E-LDAP: Users not able to logon via 3-tier client on PT 8.4x
200734446 E-LDAP: Connections are not getting disconnected from Directory
200734995 E-LDAP: Can't run Crystal Reports when logging in through 3 tier and LDAP Server
200735608 E-LDAP: LDAP Authentication does not work in 2-tier
200735803 E-LDAP: How to get Dynamic Role Rule to work in 8.4x
200735878 E-LDAP: Does LDAP authentication work with multiple Domains?
200739189 E-LDAP: How to setup ID Type as EMP for employee self service
200751493 E-LDAP: Authentication is taking over 30 seconds to logon via LDAP
200759911 E-LDAP: DSNAMEAT field is too small in PSDSOCATTR and PSDSATTR tables
200765684 E-LDAP: Authentication Map search shows the ID, not the Description
200767905 E-LDAP: Can the ExceltoCI application will work authenticate with LDAP?
200769833 E-LDAP: PT 8.4x LDAP role assignment removes workflow route controls from users
200772333 E-LDAP: Cache Directory Schema Error ABENDED at step LDAPSCHEMA.MAIN. Step02
200775317 E-LDAP: Authentication with App servers on UNIX fails when searching referrals
200775681 E-LDAP: What is the "Invoke As "user on signon PeopleCode page used for?
200776124 E-LDAP: Cannot logon 3 tier with LDAP user as ENCRYPTED field gets set to 0
200944355 E-LDAP: Changes to the Configuration of LDAP over SSL for PeopleTools 8.44
200948000 E-LDAP: User Profile is Being Updated On Every Logon
200949763 E-LDAP: Email Address on User Profile Map is not getting updated when using LDAP
200950508 E-LDAP: Language Code on User Profile not updated with anything other than ENG
200955970 E-LDAP: Cannot run client tools when SignonUserId id different from OPRID
200972108 E-LDAP: Performance downgraded after PeopleTools only upgrade to PT8.21
200978849 E-LDAP: LDAP_PROFILESYNCH is not working with SSO_AUTHENTICATION in PT 8.45
200979296 E-LDAP: LDAPS performance issues with App Server on Windows
200988478 E-LDAP: Dynamic Role Rules: Execute Role does not work over SSL
200992755 E-LDAP: Can signon code point to a member of a group instead of the uid?

201004601 E-LDAP: Error Setting App Server context to user
201007089 E-LDAP: LDAP business interlinks connect at 40 bit encryption not 128 bit
201014834 E-LDAP: Cannot get App Engine to work over SSL with LDAP
201015785 E-LDAP: Need certification for cert8.db for LDAP SSL Setup
201015922 E-LDAP: LDAPS libraries are not able to interpret V2 certificate template
201016262 E-LDAP/PDI: Receiving "Bad parameter to an ldap routine" when using PDI
201021919 E-LDAP: LDAP issues with search on disabled Active Directory IDs
201033025 E-LDAP: How to setup SSO between tools 8.4x and Oracle Internet Directory (OID)
201034509 E-LDAP: PT 8.48 Getting business interlink error when configuring LDAP
201042240 E-LDAP: PT 8.48 How to setup SSL for LDAP with Oracle Wallet Manager

Appendix D - Q & A

Questions and answers will be added as they come in, this is not a complete list by any means.

Question:

My LDAP implementation allows the user to signon both Using PeopleSoft UserID and password and Network Logon id and password why is this?

Answer:

The reason this is happening is because when you created a user in PeopleSoft you gave the user a PeopleSoft password. Any time this password is used, LDAP authentication will not be used. Depending on the PeopleTools version you are on this is an easy fix to stop this from happening. This is working by design in PeopleTools releases on 8.1x and 8.2x only if you do not have the user profile caching turned on, otherwise a random password will be created on the PSOPRDEFN table for the user with every successful logon. If you are on PT 8.43 or greater and you have the LDAP_PROFILESYNCH enabled on your signon PeopleCode page, AND you must be updating a field on the optional user's properties page, then you will see that if a user uses their LDAP password, assuming that it is a different password from what is on PSOPRDEFN, then the ENCRYPTED field will be updated to 0. If you do not have the LDAP_PROFILESYNCH enabled on your signon PeopleCode page, then the users will not be updated and they can use both passwords. In that case you need to either delete the user's password, make it something that the user does not know, or change the ENCRYPTED field on PSOPRDEFN for that user to 0 through SQL.

Question:

Why does the Business email address in PT 8.4x not get updated each time when I have chosen on the User Profile map, Optional user properties page, to always update?

Answer:

This is because the PT 8.4x LDAP code will ONLY update and create an email address of "OTH" other, it does not update any other email address. This is part of the FUNCLIB_LDAP record peoplecode.

Question:

Why does failover not work? We have three LDAP Servers where authentication can be done and it carries the same info. Currently we have all three servers listed on the same authentication map but when one server goes down the other servers are not being used to failover. How is this corrected?

Answer:

From what we have seen, instead of having one active map with 3 servers, try having 3 active authentication maps and identical User profile maps, with 1 server each and test that? The reason being is that the request to the server will not attempt another server on the same map until the first one times out. The maps should also be in alpha/numeric order, as you want them to be selected based on the order found for active maps on the PSDSSECMAPMAIN table.

Question:

We need to be able to use LDAP authentication and have it search for either Emplid or StudentID in our e-directory. In the directory setup, you enter a search attribute to control how PS matches to the LDAP value. Is it possible to have it search for either attribute A or attribute B?

Answer:

Not without a customization. The way it works now in the code is to use the attribute you specify in the authentication map, then to get the value identified on the user profile map to pass back to PeopleSoft. The code is found in the record called FUNCLIB_LDAP.LDAPAUTH.FieldDefault

Question:

Does PeopleSoft support client machines to use Oracle OID for TNS lookup?

Answer:

PeopleSoft supports OID (Oracle's Internet Directory) server for LDAP authentication and the ability to use Single Signon via the web, but what you are asking is a database level question. LDAP does not work in 2-tier at the TNS names level for database connectivity. This would be standard Oracle DB connectivity in this case.

Question:

Using LDAP with a password of 42 characters. This caused authentication errors when trying to connect to PeopleSoft via LDAP. While our directory supports passwords up to 512 characters, it appears that there is a limit in PeopleSoft. Why is this?

Answer:

The delivered LDAP authentication uses the PeopleSoft logon restrictions as the system will first try to logon to PeopleSoft, and then with a failure will invoke the signon PeopleCode to use LDAP authentication. The PeopleSoft password restriction is up to 32 characters. Although we are LDAP compliant, unless you are using an External SSO solution, and only passing the OPRID to PeopleSoft, you will have to conform to the PeopleSoft logon process, which restricts a user's password length to 32 characters.

Question:

If the OPRIDs on the PSOPRDEFN table are in lower or mixed case what needs to be done to get these users to authenticate? Why do they always get created in UPPER CASE?

Answer:

As delivered in the LDAP authentication PeopleCode PeopleSoft converts all User IDs to uppercase. For an organization supporting mixed case User IDs a minor modification needs to be made to PeopleCode. When you use LDAP authentication the directory doesn't care about the case of the User ID, but PeopleSoft does. You MUST be using the "Invoke as" option on the signon PeopleCode page too. If you are using "Invoke as user signing in" then your user base will have to enter the user id, on the logon screen, as it appears on the PSOPRDEFN table (exact case) or they will not logon. By using the "invoke as" option with a default user, this allows the user to logon on the logon screen without case sensitivity, except for the password of course.

If you support mixed case User IDs you can modify this PeopleCode. PeopleSoft suggests that customers using LDAP should UPPER CASE all OPRIDs in PSOPRDEFN if they don't want to customize the code.

To modify the PeopleCode you need to remove ALL instances of the word "upper" from the PeopleCode in the record FUNCLIB_LDAP in the LDAPAUTH.FieldDefault and OPRID.FieldFormula. This is also a customization, and if you are using the User Profile Component Interface then the users will be created in the PSOPRDEFN table in the exact case as they are in the directory. Make sure that you track this change as every tools upgrade and patch will put it back to the delivered method.

IMPORTANT NOTE:

What making this code change will do is authenticate your LDAP users to PeopleSoft based on the case sensitivity of their ID in the LDAP directory. For example, if I have a user called Mickey Mouse with an ID of MMouse in my directory, when that user logs onto PeopleSoft, regardless if they enter MMOUSE, mmouse, Mmouse, mMOUSE, or MMouse on the logon screen, as long as the LDAP password is correct the code will pass to PSOPRDEFN the OPRID of MMouse (as it appears in the directory) So in order for your user to logon to PeopleSoft an OPRID in PSOPRDEFN must either be there in that exact case, or if you are using the User Profile caching (option # 5 on the signon PeopleCode page) then the user will get created as MMouse. So you will want to verify that your user base in your LDAP directory is the same case as your user base in PeopleSoft's PSOPRDEFN table.

Question:

We want to change the User DN password in our LDAP server per our 90-day password controls. How can we effectively do this and update our PeopleSoft environments without disclosing the new password?

Answer:

If you want the Connect DN password to change in your directory every 90 days or so, in order to keep PeopleSoft in synch with this user's password change, and not disclose the new DN password to your other environments, for security purposes, you will need to do the following:

1) Change the password in LDAP for the user DN

2) Logon to a PeopleSoft environment and navigate to PeopleTools > Security > Directory > Configure Directory page.

Here you will enter the new password for the Connect DN user.

3) In your SQL too you will want to look up the now encrypted value for this password by running the following SQL statement:

```
SELECT DSCNCTDN, DSCNCTPWD FROM PSDSDIR
```

This will return the user DN and the encrypted password.

4) Now you will send out the following SQL statement to your other databases to update their PSDSDIR tables, without knowing the DN password.

```
UPDATE PSDSDIR SET DSCNCTPWD = 'the encrypted value from your last statement' WHERE  
DSCNCTDN = 'the value for this field from the last statement'
```


Appendix E – Directory Technical Overview

This section is provided as an overview and reference for those who may need more information on directory technology in general. If you are already familiar with directories and LDAP please refer to the sections on PeopleSoft/Directory Integration.

DEFINITIONS

Directory – Distributed hierarchical database

LDAP – Lightweight Directory Access Protocol

RootDSE – Directory entry retrieved by searching with search base equal to the empty string and scope equal to base

Schema – Contents of the subSchemaSubEntry entry as specified in the RootDSE

Directory Information Tree (DIT) – Hierarchically structured entries, which make up the Directory database.

Distinguished Name – A string, which uniquely identifies an entry in the directory.

Entry – A list of attribute/value pairs identified by a single Distinguished Name (DN).

Attribute – Attributes hold the data for the Entry. Any single Attribute may hold more than one value unless otherwise specified.

Syntax – The data type of an Attribute.

LDAP Server – A single machine running an LDAP Server process. There can be many LDAP Servers to one Directory.

DIT AND SCHEMA

Directories are comprised of two major components; the Directory Information Tree (DIT) and the Schema. The DIT is comprised of all the entries in the Directory. Each Entry in the DIT is specified by its Distinguished Name and is made up of Attribute/Value pairs. To clarify, let's look at an example DIT and a few of its Entries.



The above image depicts a partial DIT made up of four entries, the ccb.com organization entry, the Applied Science organizationalUnit entry, and two user entries, KSchnabel and MLewis. Now let's look at this entries in more depth. The ccb.com organization entry can also be represented as follows:

dn: o=ccb.com

o: ccb.com

objectClass: top

objectClass: organization

This representation clearly shows the Distinguished Name of the entry in the first line, dn: o=ccb.com. The next four lines display the Attribute/Value pairs that exist for the o=ccb.com entry. The first Attribute,

o, has only a single value, ccb.com. The second attribute shown, objectClass, has two values and thus is repeated two times in the display.

The same representation of the Applied Science entry appears as follows:

```
dn: ou=applied science,o=ccb.com
```

```
ou: Applied Science
```

```
objectClass: top
```

```
objectClass: organizationalUnit
```

```
description: Applied Science
```

As with the former example, the DN of the entry appears in the first line. Notice that o=ccb.com appears in the DN for Applied Science. This indicates the hierarchical nature of the DIT; Applied Science is “contained by” ccb.com. The next few lines are very similar to those for the ccb.com entry, each show and Attributes and their Value or Values that make up the entry.

The user entries are similar to the previous examples:

```
dn: cn=KSchnabel,ou=Applied Science,o=ccb.com
```

```
mail: KSchnabel@ccb.com
```

```
uid: KSchnabel
```

```
givenName: Katherine
```

```
fullName: Katherine Schnabel
```

```
sn: Schnabel
```

```
ou: Applied Science
```

```
objectClass: top
```

```
objectClass: person
```

```
objectClass: organizationalPerson
```

```
objectClass: inetOrgPerson
```

```
cn: KSchnabel
```

```
dn: cn=MLewis,ou=Applied Science,o=ccb.com
```

```
mail: MLewis@ccb.com
```

```
uid: MLewis
```

```
givenName: Margaret
```

```
fullName: Margaret Lewis
```

```
title: Professor-Applied Sciences
```

```
telephoneNumber: 215/789-0778
```

```
sn: Lewis
```

```
ou: Applied Science
```

```
objectClass: top
```

```
objectClass: person
```

```
objectClass: organizationalPerson
```

```
objectClass: inetOrgPerson
```

```
cn: MLewis
```

In both cases the first line of the entry is the DN and in both cases the DN indicates the “location” of the entry in the DIT. By glancing at the DN we can instantly see that the entries for both KSchnabel and MLewis are in the Applied Science organizationalUnit, which is in the ccb.com organization. We also see that there are a greater number of Attributes that have Values for these entries than for the former examples.

The Schema is the set of rules that define (among other things) which attributes can and must be defined for the entries that make up the DIT. Referring back to the example entries provided above you’ll notice that each entry contains several values for the objectClass attribute. The objectClass is a special attribute and must be provided, along with the DN, for any new entry being created in the DIT. Each objectClass is defined in the Schema using an encoded representation defined in RFC 2252. The encoded representations are stored in the objectClasses attribute of the subschemaSubentry entry. Here’s an example definition of the person objectClass taken from Novell NDS eDirectory.

objectClasses: (2.5.6.6 NAME 'person' DESC 'Standard ObjectClass' SUP 'top' STRUCTURAL MUST (cn \$ sn) MAY (description \$ seeAlso \$ telephoneNumber \$ fullName \$ givenName \$ initials \$ uid \$ userPassword) X-NDS_NAMING ('cn' 'uid') X-NDS_CONTAINMENT ('organization' 'organizationalUnit' 'domain') X-NDS_NOT_CONTAINER '1' X-NDS_NONREMOVABLE '1')

The definition begins with the Object Identifier (OID), 2.5.6.6, for the objectClass. The OID is followed by a user-friendly name, person, and next is a description. The string that follows the SUP identifier lists the objectClasses that are parents to this objectClass (more on that later). The MUST and MAY identifiers precede the list of mandatory and optional attributes for this objectClass, respectively. In this case you'll see that to create a new person entry, values for both the cn and sn attributes must be provided, and values for attributes following MAY be able to be provided. The remaining identifiers, those beginning with X, indicate implementation specific extensions to LDAP. (The extensibility of LDAP is beyond the scope of this doc; please refer to the LDAP RFC's for more info). Some of you may have noticed that there are more attributes displayed for Mlewis than there are attributes listed for the person objectClass. Specifically, Mlewis has a value for the mail attribute but mail is not listed as either a mandatory or optional attribute in the objectClass definition. So where does the mail attribute come from? This brings us to the topic of objectClass inheritance. objectClass inheritance provides an explanation for the SUP identifier mentioned above as well as the multiple values for the objectClass attribute on each of the example entries. Each objectClass defined in the schema has the ability to inherit attributes from any other objectClasses. When an entry is created with any objectClass, all other objectClasses in the inheritance tree are included for that entry. To see this, let's look again at the dn: cn=Mlewis,ou=Applied Science,o=ccb.com entry.

```
dn: cn=Mlewis,ou=Applied Science,o=ccb.com
mail: Mlewis@ccb.com
uid: Mlewis
givenName: Margaret
fullName: Margaret Lewis
title: Professor-Applied Sciences
telephoneNumber: 215/789-0778
sn: Lewis
ou: Applied Science
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
cn: Mlewis
```

Notice that the entry contains four values for the objectClass attribute. To see all the mandatory and optional attributes for this entry you have to look at the objectClass definitions for each objectClass listed. We do this starting from the bottom of the inheritance tree, objectClass inetOrgPerson.

objectClasses: (2.16.840.1.113730.3.2.2 NAME 'inetOrgPerson' DESC 'Standard ObjectClass' **SUP organizationalPerson** STRUCTURAL MAY (groupMembership \$ homeDirectory \$ loginAllowedTimeMap \$ loginDisabled \$ loginExpirationTime \$ loginGraceLimit \$ loginGraceRemaining \$ loginIntruderAddress \$ loginIntruderAttempts \$ loginIntruderResetTime \$ loginMaximumSimultaneous \$ loginScript \$ loginTime \$ networkAddressRestriction \$ networkAddress \$ passwordAllowChange \$ passwordExpirationInterval \$ passwordExpirationTime \$ passwordMinimumLength \$ passwordRequired \$ passwordUniqueRequired \$ printJobConfiguration \$ Profile \$ securityEquals \$ accountBalance \$ minimumAccountBalance \$ messageServer \$ Language \$ UID \$ lockedByIntruder \$ lastLoginTime \$ typeCreatorMap \$ printerControl \$ Timezone \$ userCertificate;binary) X-NDS_NOT_CONTAINER '1' X-NDS_NONREMOVABLE '1')

The SUP identifier indicates that inetOrgPerson inherits from organizationalPerson.

objectClasses: (2.5.6.7 NAME 'organizationalPerson' DESC 'Standard ObjectClass' **SUP person** STRUCTURAL MAY (facsimileTelephoneNumber \$ l \$ ou \$ physicalDeliveryOfficeName \$ postalAddress \$ postalCode \$ postOfficeBox \$ st \$ street \$ title \$ uid \$ mail \$ employeeNumber \$ destinationIndicator \$ internationaliSDNNumber \$ preferredDeliveryMethod \$ registeredAddress \$ teletexTerminalIdentifier \$ telexNumber \$ x121Address \$ businessCategory \$ roomNumber \$ x500UniquelIdentifier) X-NDS_NAMING ('cn' 'ou' 'uid') X-NDS_CONTAINMENT ('organization' 'organizationalUnit' 'domain') X-NDS_NOT_CONTAINER '1' X-NDS_NONREMOVABLE '1')

We can now see that organizationalPerson inherits from person and we already know that person inherits from top.

objectClasses: (2.5.6.0 NAME 'top' DESC 'Standard ObjectClass' STRUCTURAL MUST objectClass MAY (equivalentToMe \$ Obituary \$ Reference \$ revision \$ GUID) X-NDS_NONREMOVABLE '1')

There is no superior to top so we have reached the top of the inheritance tree. By looking at all four objectClass definitions, we can construct a full list of mandatory and optional attributes for the cn=MLewis,ou=Applied Science,o=ccb.com entry.

Attributes are also defined by the schema and their encode representation looks very much that of objectClasses. I'll provide mail as an example for the reader to dissect.

attributetypes: (0.9.2342.19200300.100.1.3 NAME 'mail' DESC 'Standard Attribute' SYNTAX '1.3.6.1.4.1.1466.115.121.1.15')

Now that we have a little understanding of what the DIT and the Schema are we can look at how we can learn the schema for a particular implementation. The schema is actually contained in a special entry of the DIT known as the subschemaSubentry, which is of objectClass subschema. To learn the location of the subschemaSubentry you can look at another special entry known as the rootDSE. The rootDSE holds pertinent information about a particular instance of a directory and must be provided if the directory is to be LDAP V3 compliant. Here's an example rootDSE from an instance of iPlanet Directory Server 4.1:

```
dn:
objectclass: top
namingcontexts: o=config
namingcontexts: o=NetscapeRoot
namingcontexts: o=ccb.com
subschemasubentry: cn=schema
supportedcontrol: 2.16.840.1.113730.3.4.2
supportedcontrol: 2.16.840.1.113730.3.4.3
supportedcontrol: 2.16.840.1.113730.3.4.4
supportedcontrol: 2.16.840.1.113730.3.4.5
supportedcontrol: 1.2.840.113556.1.4.473
supportedcontrol: 2.16.840.1.113730.3.4.9
supportedcontrol: 2.16.840.1.113730.3.4.12
supportedsaslmmechanisms: EXTERNAL
supportedldapversion: 2
supportedldapversion: 3
```

And here's one from an instance of Novell NDS eDirectory:

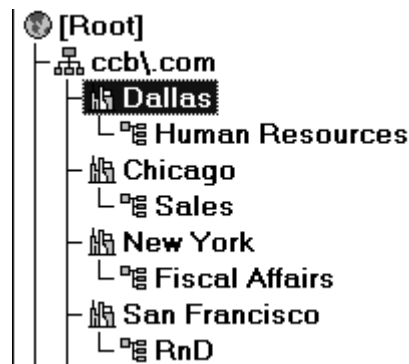
```
dn:
supportedLDAPVersion: 2
supportedLDAPVersion: 3
supportedControl: 1.2.840.113556.1.4.473
supportedControl: 2.16.840.1.113730.3.4.9
```

subschemaSubentry: cn=schema
namingContexts:

Notice that in both examples the DN is blank, the rootDSE has no DN. Both servers provide the supportedLDAPVersion, supportedControl, and subschemaSubentry attributes in the rootDSE.

DISTRIBUTION AND REPLICATION

The directory database itself can be both distributed and replicated. In other words, there can be more than one server participating in a given directory, and each server can hold all or just some of the database. To illustrate let's again look at an example directory.



In this case, our example organization, CCB, has four different departments (organizationalUnits) in four different cities spread across the U.S and the directory administrators have designed the DIT to reflect the company's physical topology. To support the distributed nature of the company, CCB maintains data-center facilities in each of the four cities and each facility houses three servers participating in the directory, yielding a total of twelve servers in the tree. Given this scenario, the directory administrators could partition the DIT at each of the locality entries and store each part of the DIT on the servers in the corresponding data-center. In other words, the servers in Dallas would store only the Dallas entry and those entries beneath it. Within the Dallas locality the Dallas partition would then be replicated across all three servers. The distributed nature of the directory can be hidden from user processes. When a user in one locality performs an operation on an entry in another locality the directory server can refer the request to a server holding the appropriate partition. Distribution, replication, and referrals cause directories to be highly available.

TECHNICAL OVERVIEW SUMMARY

Directories are comprised of two main components, the DIT and the Schema. The DIT is the complete collection of entries in the directory and the Schema is the set of rules that define the possible content of the entries. The entries that make up the DIT are of one or more objectClasses and are comprised of attributes that hold a value or values. There are two special entries, the rootDSE and the subschemaSubentry. The location of the subschemaSubentry can be found on the rootDSE. Both the DIT and the Schema are hierarchical in structure. And finally, directories can be broken into pieces and those pieces replicated across servers establishing a many-to-one relationship between servers and directories, respectively.

Appendix F – Addendum of updated versions

Here is a list of revisions that have been added to this red paper and changes that have been made.

6/07 – Page 10 - Updated that PT 8.22 requires a connect ID if attempting to make an anonymous bind. Prior versions did not require this.

5/07 – Added SOLUTION ID 201034509 E-LDAP: PT 8.48 Getting a business interlink error when configuring LDAP to page 23 LDAP test connectivity

5/07 – Updated GSC solutions on Appendix C

5/07 – Added customer comments on top of Appendix A.

5/07 – Removed page numbers from TOC sub chapters. Only have page numbers on Chapter headings and Appendixes.

1/07 – Added Customer experience in Appendix A