

Configuring Embedded LDAP Authentication



configure



Configuring Embedded LDAP Authentication

For HP product models:

LaserJet 4345mfp, LaserJet 9040mfp,
LaserJet 9050mfp, LaserJet 9500mfp, and
Digital Sender 9200C

Legal Notice

© Copyright 2005 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice.

Microsoft®, Windows®, and Windows NT®, are U.S. registered trademarks of Microsoft Corporation.

All other products mentioned herein might be trademarks of their respective companies.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

This is an HP copyrighted work that may not be reproduced without the permission of HP.

Configuring Embedded LDAP Authentication
Rev. 5.21

Contents

Overview.....	1
Required tool.....	1
Step 1: Discovering the LDAP server.....	5
Method 1.....	5
Method 2.....	6
Step 2: Setting up LDP.....	7
Step 3: Configure LDAP.....	10
Step 4: Configure the Authentication Manager.....	12
Step 5: Use the MFP control panel.....	13



Overview

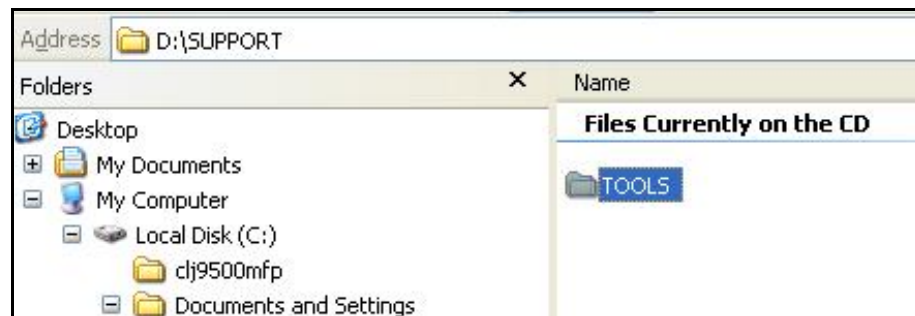
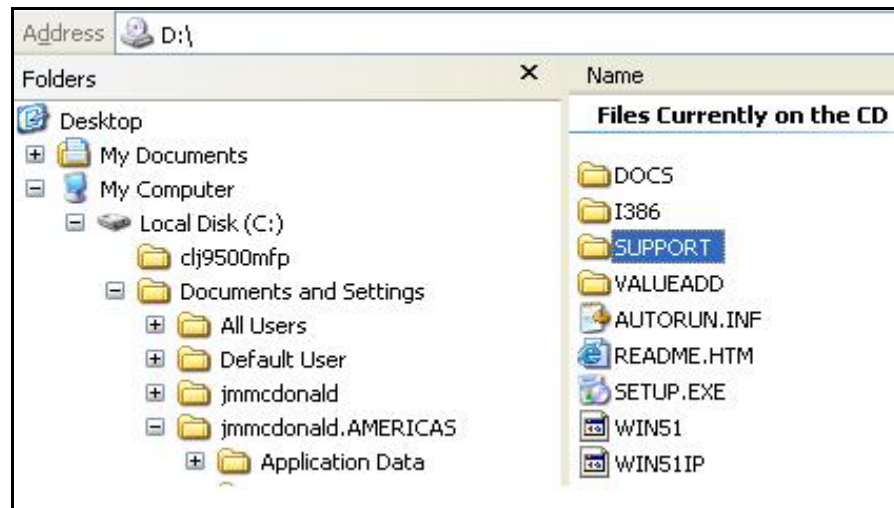
Configuring embedded LDAP authentication is a technical process that involves configuring the MFP to communicate with the LDAP database. This document provides step-by-step instructions on configuring this functionality.

Required tool

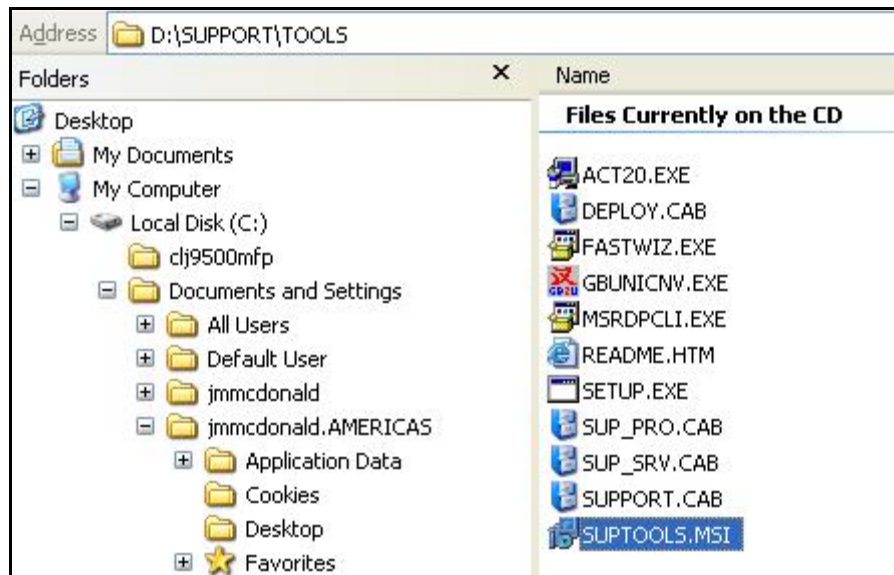
It is necessary to use Microsoft LDP to configure the MFP for embedded LDAP authentication. Microsoft LDP is a support tool that ships with the Windows Support Tools contained on the Windows OS media. It allows you to connect, bind, and query an LDAP database.

Microsoft LDP can be installed and configured by following these instructions:

- a. Browse to the root of the OS media, and open the **Support** folder.
- b. Open the **Tools** folder.



- c. Double click the **SUPTOOLS.MSI** file.



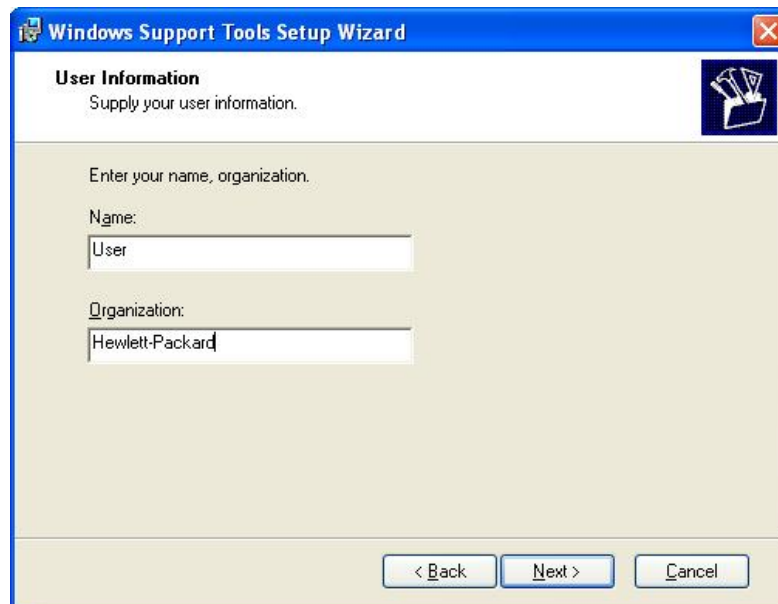
- d. Select **Next** at the Welcome to the Windows Support Tools Setup Wizard.



- e. After reading the licensing agreement, select the **I Agree** radial button and click **Next**.



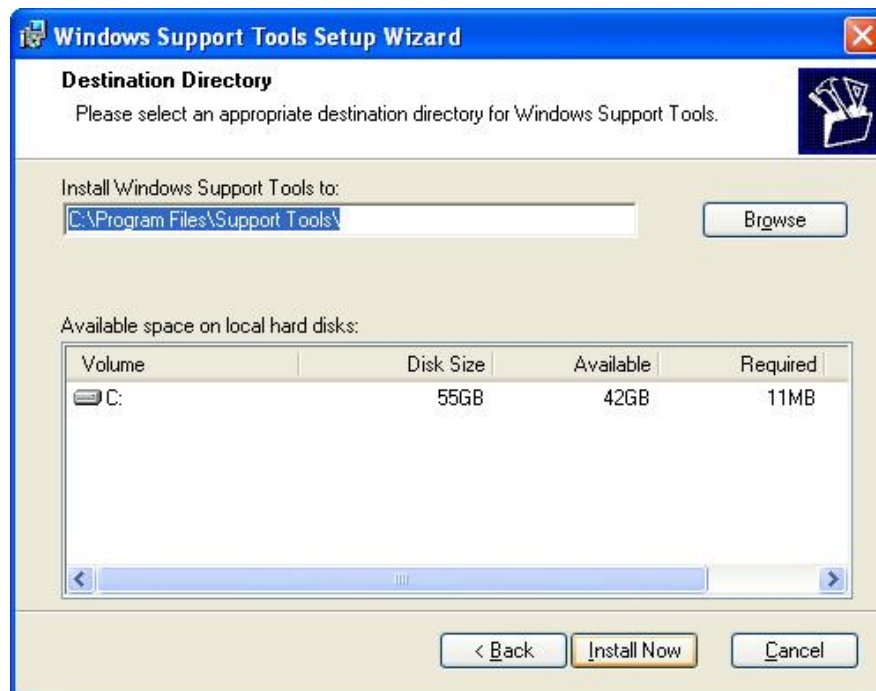
- f. Enter your name and organization; then click **Next**.



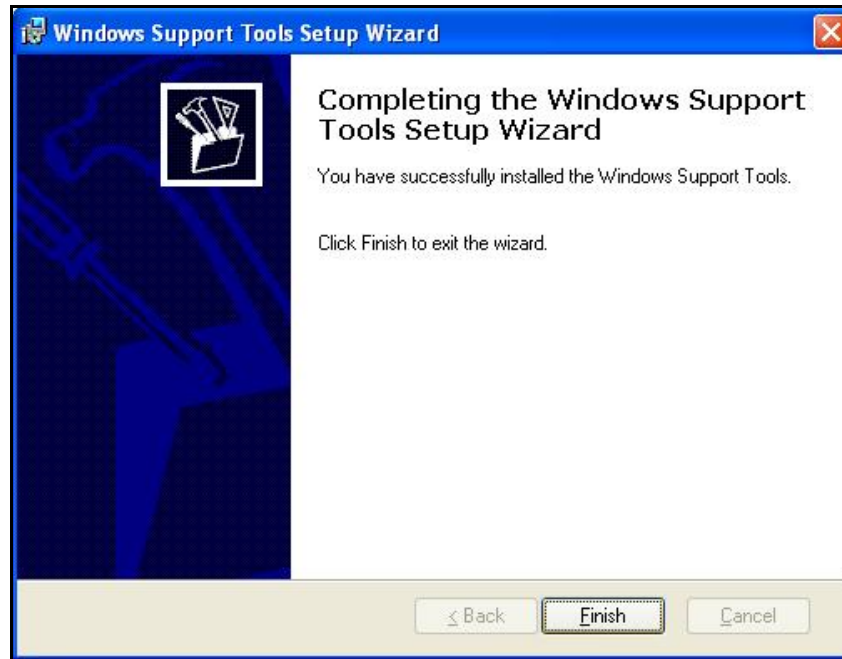
- g. Select **Complete** for the installation type; then click **Next**.



- h. Select **Install Now** to begin the installation.



- i. Click **Finish** to complete the installation.

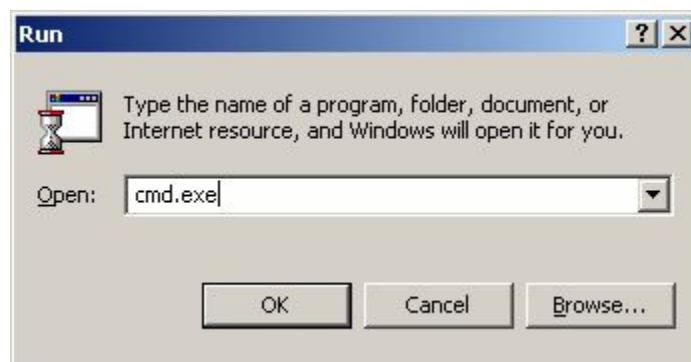


Step 1: Discovering the LDAP server

There are two key methods to discover an available LDAP server on the network.

Method 1

- a. Open a command window by clicking on **Start** ® **Run** and typing **cmd.exe** in the dialog box. Then press **Enter** or click **OK**.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\jmmcdonald.AMERICAS>
```

- b. To determine which Windows Active Directory logon server you are logged onto, type the following: **echo %logonserver%**. This server can be used as the LDAP server.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\jmmcdonald.AMERICAS>echo %logonserver%
\\IDBGCAM03
C:\Documents and Settings\jmmcdonald.AMERICAS>_
```

Method 2

The following command can be used to provide a list of DNS servers.

- n **nslookup “name of your domain” (i.e. nslookup AMERICAS.HPQCORP.NET)**. In a Windows Active Directory environment, a DNS server is typically running Active Directory which contains the LDAP database.

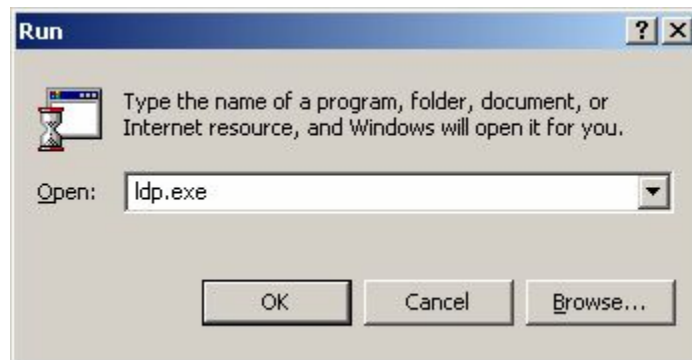
```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\jmmcdonald.AMERICAS>nslookup AMERICAS.HPQCORP.NET
DNS request timed out.
    timeout was 2 seconds.
*** Can't find server name for address 16.88.97.243: Timed out
Server: cagcam01.americas.hpqcorp.net
Address: 16.92.3.243

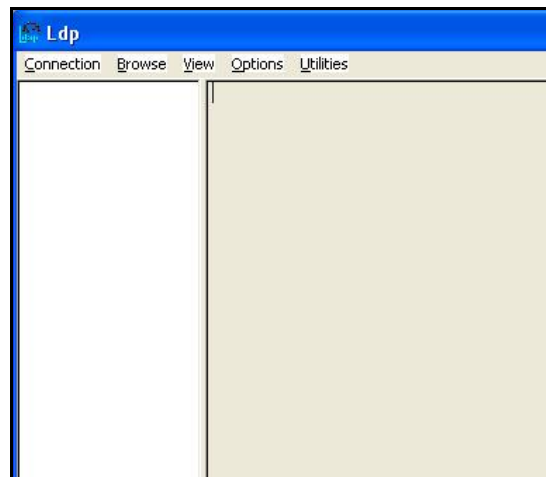
Name:    AMERICAS.HPQCORP.NET
```

Step 2: Setting up LDP

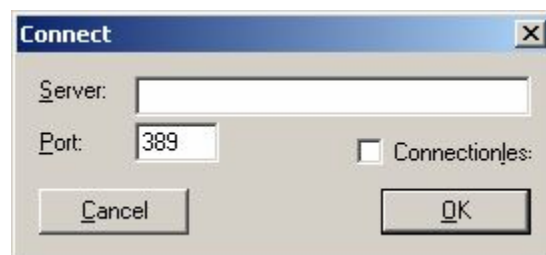
- a. Open LDP by clicking on **Start** ® **Run**, and typing **ldp.exe**; then press **Enter** or click **OK**.



- b. From the Ldp menu, select **Connection** ® **Connect**.



- c. In the Connect window, input **389** or **3268** as the Port Number; then click **OK**.
 - w Port 389 is the standard LDAP port. However, it may be necessary to use port 3268 when communicating with a Windows Global Catalog Active Directory Server.



- d. From the LDP menu, select **Connection** ® **Bind**.

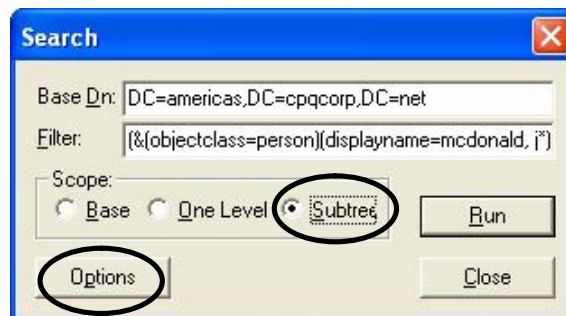
- e. In the Bind window, input username, password, and domain name; then click **OK**.



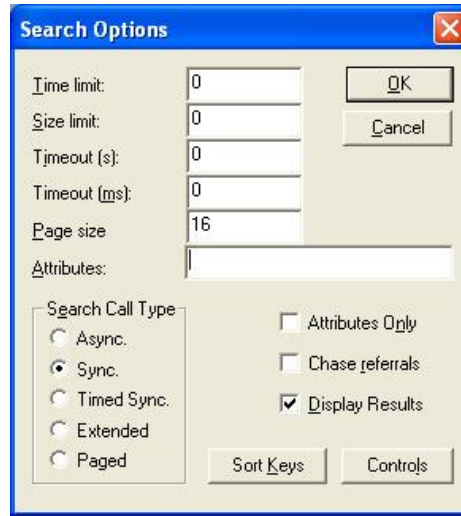
- f. On the LDP screen, find and copy the Base DN.
 w The Base DN is normally listed within “defaultNamingContext.”

```
ld = ldap_open("16.88.97.11", 389);
Established connection to 16.88.97.11.
Retrieving base DSA information...
Result <0>: (null)
Matched DNs:
Getting 1 entries:
>> Dn:
    1> currentTime: 6/28/2005 15:51:42 Mountain Standard Time Mountain Daylig
    1> subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=
    1> dsServiceName: CN=NTDS Settings,CN=IDBGCAM03,CN=Servers,CN=S
    3> namingContexts: CN=Configuration,DC=cpqcorp,DC=net; CN=Schema,C
    1> defaultNamingContext: DC=americas,DC=cpqcorp,DC=net
    1> schemaNamingContext: CN=Schema,CN=Configuration,DC=cpqcorp,DC
    1> configurationNamingContext: CN=Configuration,DC=cpqcorp,DC=net;
    1> rootDomainNamingContext: DC=cpqcorp,DC=net;
```

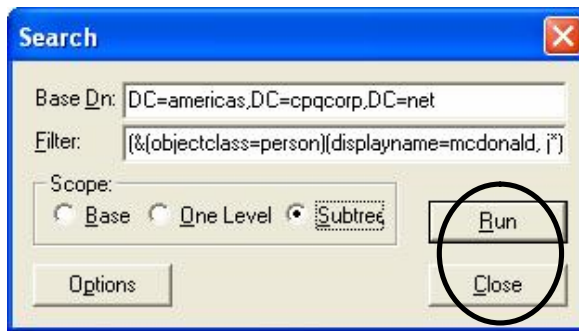
- g. From the LDP menu, select **Browse ® Search**.
- h. In the Search window, paste the Base DN into the Base Dn box. Input the LDP Filter into the Filter box.
- w Use (&(objectclass=person)(displayname="customer last name, first name letter"*)) as the LDP Filter. For example, (&(objectclass=person)(displayname=mcdonald,j*))
- w Select **Subtree** for the Scope.
- w Click **Options**.



- w In the Search Options window, remove all entries in Attributes; then click **OK**.



- w Back in the Search window, click **Run**; then click **Close**.



- i. On the LDP screen, locate the user DN from the returned results. Copy it for use in the Embedded Web Server (EWS).

- w The Search Prefix begins after the individual user CN.

```

1> canonicalName: americas.cpqcorp.net/Accounts/Users/US/jmcdonald@hp.com;
>> Dn: CN=joseph.mcdonald@hp.com,OU=US,OU=Users,OU=Accounts,DC=americas,DC=cpqcorp,DC=net
4> objectClass: top, person, organizationalPerson, user;
1> cn: joseph.mcdonald@hp.com;
1> distinguishedName: CN=joseph.mcdonald@hp.com,OU=US,OU=Users,OU=Accounts,DC=americas,DC=
1> name: joseph.mcdonald@hp.com;
1> canonicalName: americas.cpqcorp.net/Accounts/Users/US/joseph.mcdonald@hp.com;
>> Dn: CN=joshua.mcdonald@hp.com,OU=US,OU=Users,OU=Accounts,DC=americas,DC=cpqcorp,DC=net
4> objectClass: top, person, organizationalPerson, user;
1> cn: joshua.mcdonald@hp.com;
1> distinguishedName: CN=joshua.mcdonald@hp.com,OU=US,OU=Users,OU=Accounts,DC=americas,DC=
1> name: joshua.mcdonald@hp.com;
1> canonicalName: americas.cpqcorp.net/Accounts/Users/US/joshua.mcdonald@hp.com;
>> Dn: CN=julie.mcdonald@hp.com,OU=US,OU=Users,OU=Accounts,DC=americas,DC=cpqcorp,DC=net

```

Hint

Notice how the username is set up on the LDAP screen. The username format is defined within the device user DN. This can be viewed in the LDAP trace. The format is often in email address format, but can be defined in many different combinations.

```
>> Dn: CN=joshua.mcdonald@hp.com,OU=US,OU=Users,OU=Accounts,DC=americas,DC=com;
4> objectClass: top, person; organizationalPerson; user;
1> cn: joshua.mcdonald@hp.com;
1> sn: McDonald;
```

Step 3: Configure LDAP

- a. Open the EWS in a web browser.
- b. Select the **Settings** tab, and then **LDAP Authentication**.
- c. On the LDAP Authentication screen, paste the copied Search Prefix into the Bind and search Root box.
- d. Input **cn** into the Bind Prefix box.
- e. Input **389** or **3268** in the Port box.
- f. Input the LDAP server IP address or server name into the LDAP Server box.

Hint

Using the command `echo %logonserver%` earlier, IDBGCAM03 was the server name discovered.

- g. Leave the LDAP Server Bind Method at **Simple** unless configuring SSL.

The screenshot shows the 'LDAP Authentication' configuration page. The 'LDAP Server Bind Method' is set to 'Simple'. The 'LDAP Server' is 'IDBGCAM03' and the 'Port' is '389'. The 'Bind Prefix' is 'cn'. The 'Bind and search Root' is 'OU=US,OU=Users,OU=Accounts,DC=americas,DC=com'. Below this, there are three sections for matching LDAP attributes: 'Match the name entered with the LDAP attribute of' (cn), 'Retrieve the device user's email address using attribute of' (mail), and 'Retrieve the device user's name using the attribute of' (displayName). A 'Test' button is at the bottom left, and 'Apply' and 'Cancel' buttons are at the bottom right.

- h. Input **cn** into the “Match the name entered with the LDAP attribute of” field.
- i. Find the device user email address in the LDP trace. Copy the attribute defining the email address.

```

1> lockoutTime: 0;
1> objectCategory: CN=Person,CN=Schema,C
5> dSCorePropagationData: 5/6/2005 1:23:14 M
tain Standard Time Mountain Daylight Time; 7/14/16
1> lastLogonTimestamp: 6/27/2005 9:40:52 Mc
1> textEncodedORAddress: c=US;a= ;p=COMP.
1> mail:joshua.mcdonald@hp.com;

```

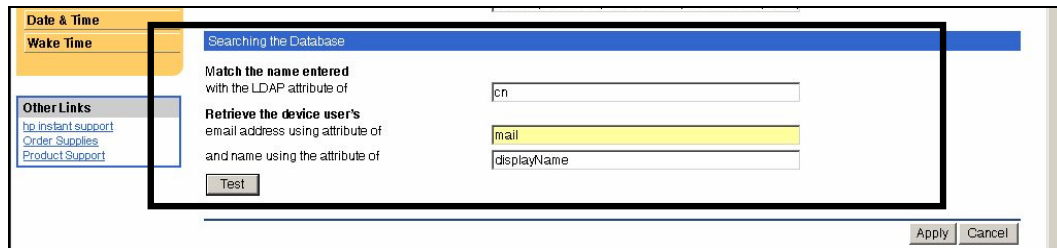
- w Paste the attribute into the “Retrieve the device user’s email address using attribute of” box.
- j. Find the device user display name in the LDP trace. Copy the attribute defining the display name.
- w This is usually set as displayName.

```

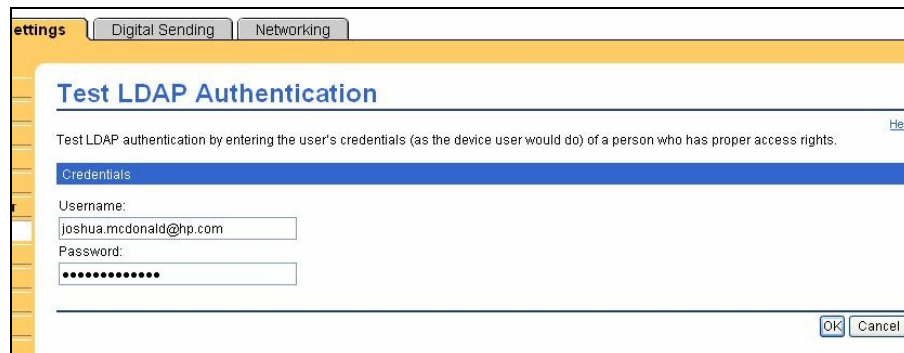
1> givenName: Joshua;
1> distinguishedName: CN=joshua.r
1> instanceType: 4;
1> whenCreated: 4/15/2004 11:0:26 I
1> whenChanged: 6/27/2005 9:40:52
1> displayName: McDonald, Joshua

```

- w Paste the attribute into the “Retrieve the device and name using the attribute of” box.
- k. Click **Test**.



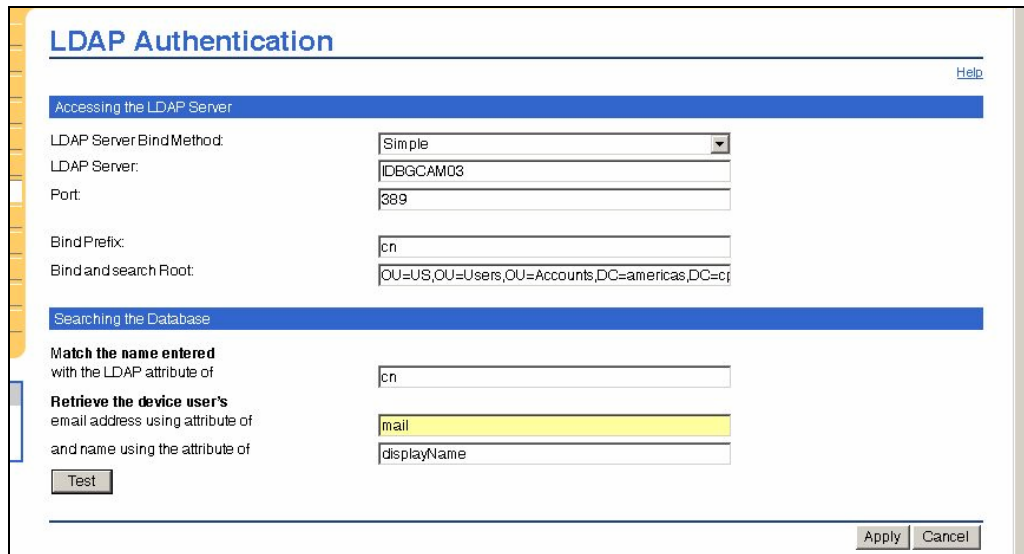
- l. The Test LDAP Authentication screen appears. Input your username and password; then click **OK**.



Hint

Remember how the username was set up on the LDP screen. The username is defined within the device user DN value in the LDP trace and is not in standard Windows domain account format. The format is often your entire email address, including the @xx.xx.

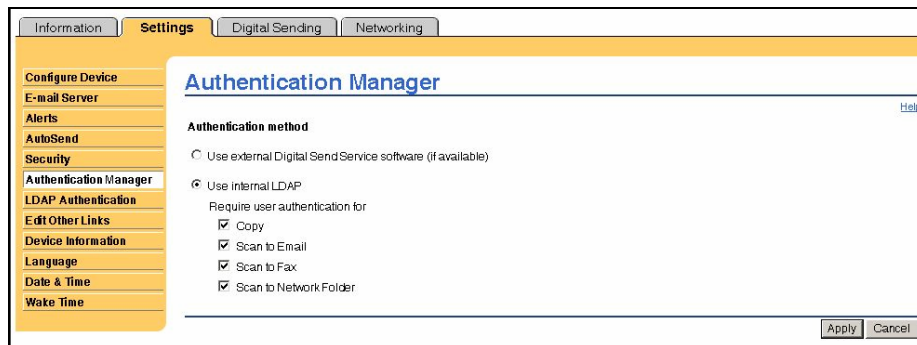
- m. The LDAP Authentication screen appears. Click **Apply**.



The screenshot shows the 'LDAP Authentication' configuration window. It is divided into two main sections: 'Accessing the LDAP Server' and 'Searching the Database'. In the 'Accessing the LDAP Server' section, the following fields are visible: 'LDAP Server Bind Method' (Simple), 'LDAP Server' (IDBGCAM03), 'Port' (389), 'Bind Prefix' (cn), and 'Bind and search Root' (OU=US,OU=Users,OU=Accounts,DC=americas,DC=c). The 'Searching the Database' section includes three fields: 'Match the name entered with the LDAP attribute of' (cn), 'Retrieve the device user's email address using attribute of' (mail), and 'and name using the attribute of' (displayName). A 'Test' button is located below these fields. At the bottom right, there are 'Apply' and 'Cancel' buttons.

Step 4: Configure the Authentication Manager

- From the EWS, click the **Authentication Manager** tab.
- On the Authentication Manager screen, check the **Use internal LDAP** radial button.
- Check all boxes under “Require user authorization for.”
- Click **Apply**.



The screenshot shows the 'Authentication Manager' configuration window. The left sidebar contains a list of settings categories: 'Configure Device', 'E-mail Server', 'Alerts', 'AutoSend', 'Security', 'Authentication Manager', 'LDAP Authentication', 'Edit Other Links', 'Device Information', 'Language', 'Date & Time', and 'Wake Time'. The 'Authentication Manager' section is active, showing the 'Authentication method' options: 'Use external Digital Send Service software (if available)' (unselected) and 'Use internal LDAP' (selected). Under 'Require user authorization for', the following options are checked: 'Copy', 'Scan to Email', 'Scan to Fax', and 'Scan to Network Folder'. At the bottom right, there are 'Apply' and 'Cancel' buttons.

Step 5: Use the MFP control panel

- a. At the MFP, touch any option on the main screen. The screen displays a request for authentication.

Hint

Remember the username is defined within the device user DN value in the LDP trace and is often your entire email address, including the @xx.xx.



The image shows a dialog box titled "Authentication Required". It contains two input fields: "User Name:" and "Password:". Below the input fields are two buttons: "OK" and "Cancel".

- b. Use the touch screen keypad to input the authentication.
 - w Once input, click **OK**, and the chosen option appears; for example, the Folder screen appears.