Configuring Embedded LDAP Authentication
Configuring Embedded LDAP Authentication

For HP product models:

Configuring Embedded LDAP Authentication
Rev. 5.21
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.

![End User License Agreement](image1.png)

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

![User Information](image2.png)
g. Select **Complete** for the installation type; then click **Next**.

![Select An Installation Type]

- **Typical**
- **Complete**

**Description**
Recommended if you are a server or network administrator.

![Install Now]

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**.
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.

Method 2
The following command can be used to provide a list of DNS servers.

```bash
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.
```
Step 2: Setting up LDP

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

![Run dialog box]

b. From the Ldp menu, select Connection → Connect.

![Ldp window]

c. In the Connect window, input 389 or 3268 as the Port Number; then click OK.

- 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.

![Connect dialog box]

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. The Base DN is normally listed within “defaultNamingContext.”

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. 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.
Hint

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

```
>> Dm:ONE:joshua.mcdonald@hp.com,OU=US,OU=Users,OU=Accounts,DC=america,DC=hp
  cn=joshua.mcdonald,sn=joshua.mcdonald@hp.com,uid=joshua.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.
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
4> contain 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.

```
1> givenName: Joshua;
1> distinguishedName: CN=joshua;
1> instanceType: 4;
1> whenCreated: 4/15/2004 11:0:26
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.

Step 4: Configure the Authentication Manager

a. From the EWS, click the Authentication Manager tab.

b. On the Authentication Manager screen, check the Use internal LDAP radial button.

c. Check all boxes under “Require user authorization for.”

d. Click Apply.
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.

b. Use the touch screen keypad to input the authentication.

  Once input, click OK, and the chosen option appears; for example, the Folder screen appears.