

# Configuring Embedded Kerberos Authentication



configure



---

# Configuring Embedded Kerberos Authentication

For HP product model:

LaserJet 9055mfp/9065mfp

---

## Legal Notice

© Copyright 2006 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 authentication using Kerberos 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: Kerberos Authentication.....	10
Step 4: Configure the Authentication Manager.....	13
Step 5: Configure Addressing Settings.....	13
Step 6: Use the MFP control panel.....	15
Troubleshooting.....	16

---

## Overview

Kerberos is a network authentication protocol. It is designed to provide secure authentication for client/server applications by using secret keys delivered with session tickets. This document provides step-by-step instructions for configuring Kerberos.

## 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 the instructions below:

---

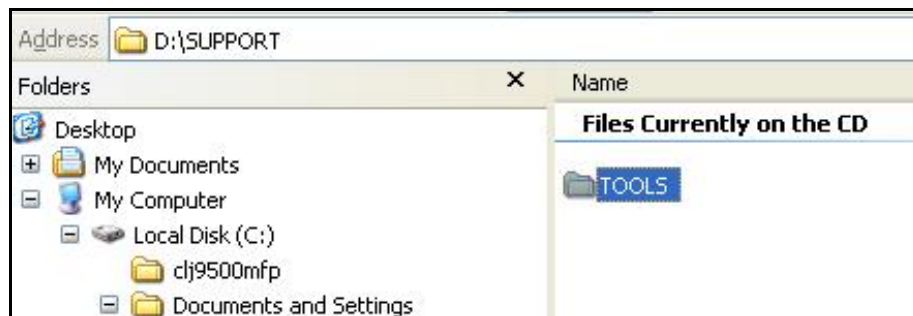
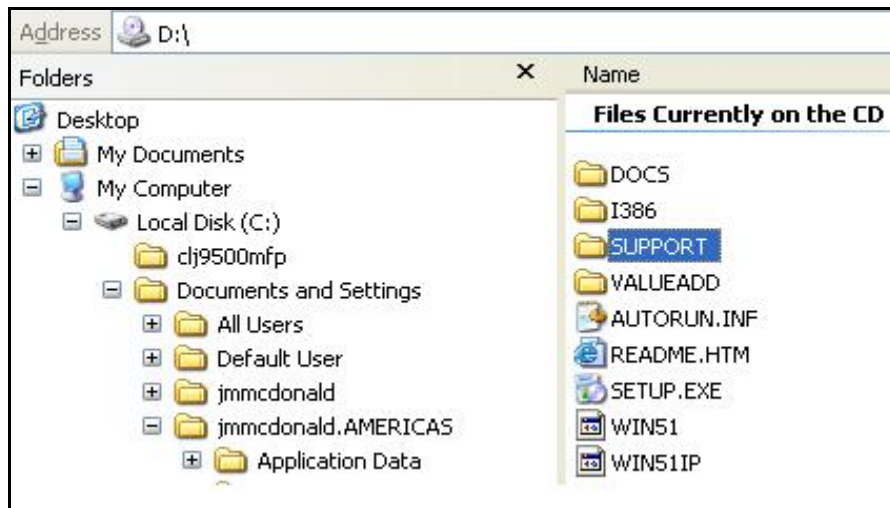
### Note

Another way to obtain the Windows Support tools is to download them from Microsoft at the following address:

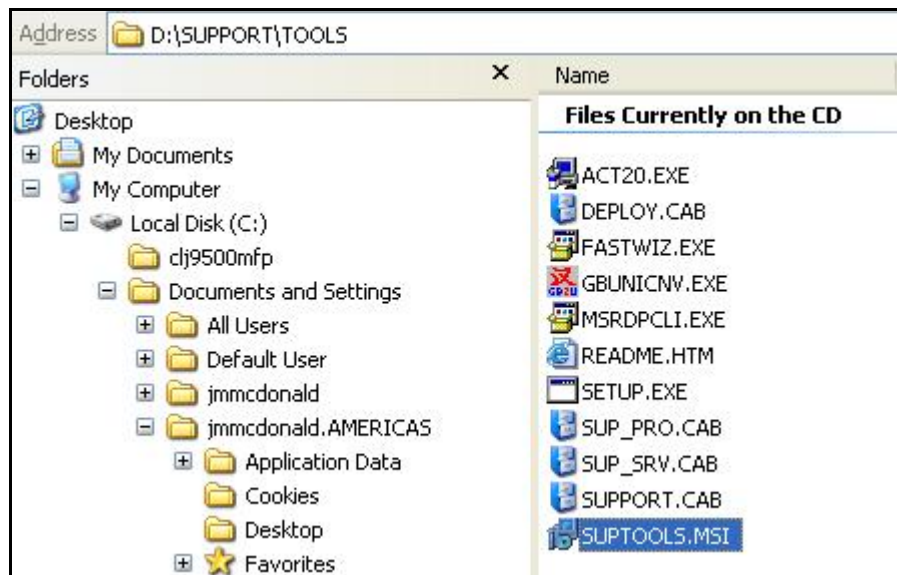
<http://www.microsoft.com/downloads/details.aspx?FamilyId=49AE8576-9BB9-4126-9761-BA8011FABF38&displaylang=en>

---

1. Browse to the root of the OS media, and open the Support folder.
2. Open the Tools folder.



3. Double click the SUPTOOLS.MSI file.



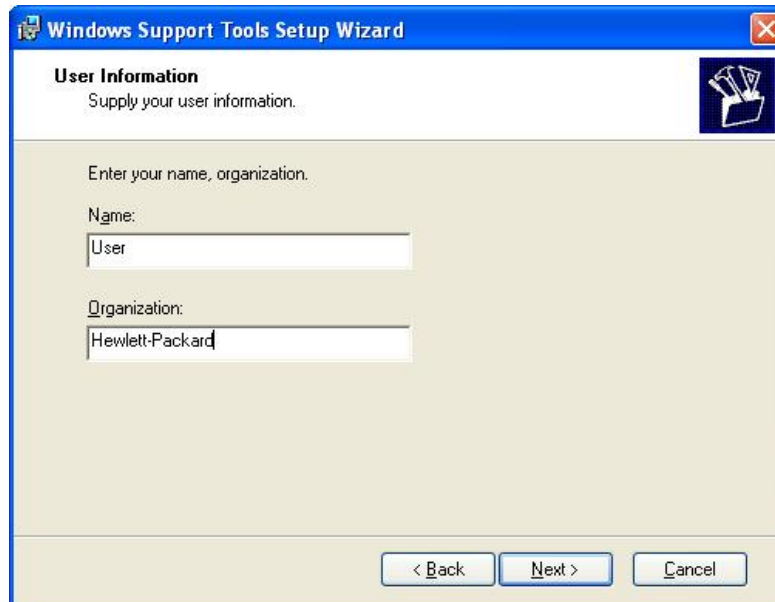
4. Select Next at the Welcome to the Windows Support Tools Setup Wizard.



5. After reading the licensing agreement, select the I Agree radial button and click Next.



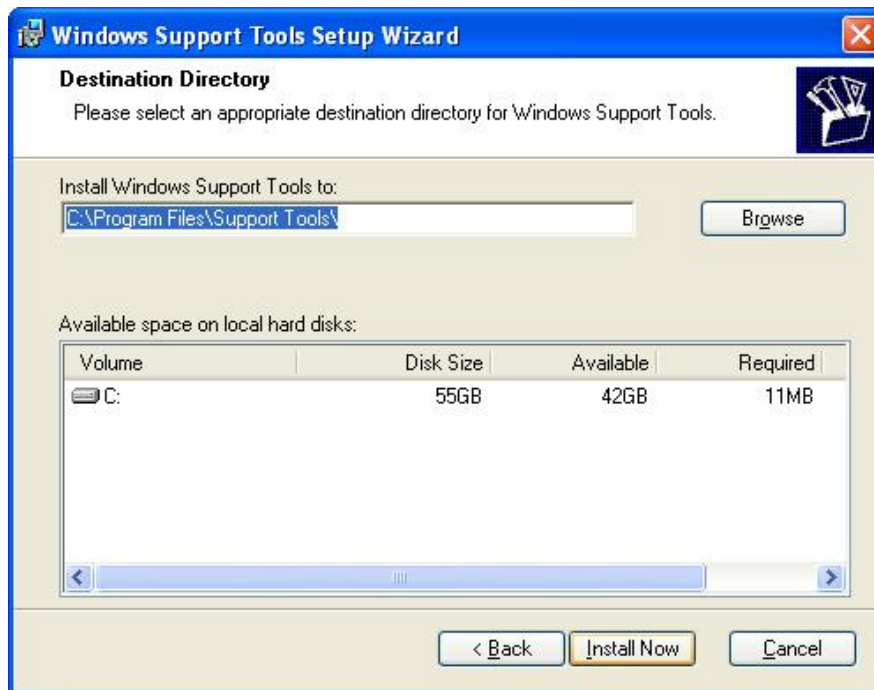
6. Enter your name and organization; then click Next.



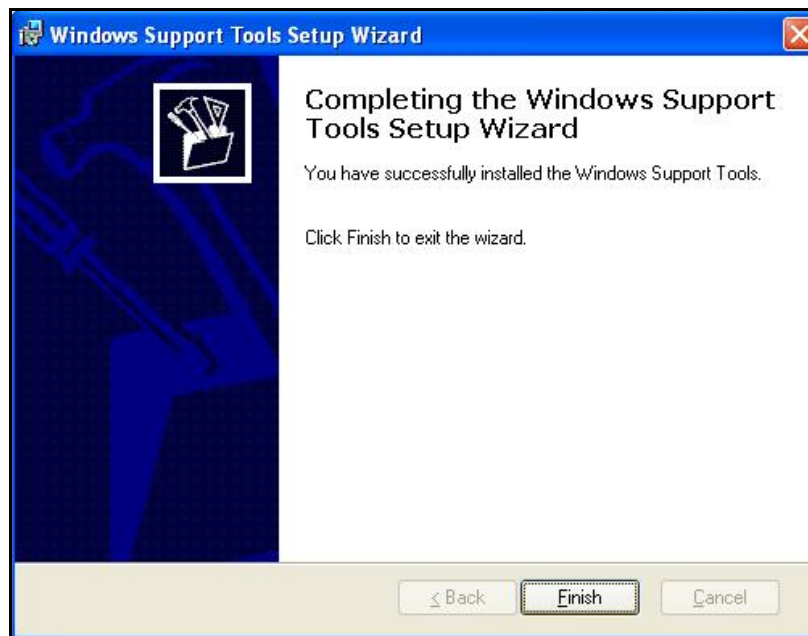
7. Select Complete for the installation type; then click Next.



8. Select Install Now to begin the installation.



9. 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

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



2. To determine which Windows Active Directory logon server you are logged onto, type the following: `echo %logonserver%`. Then press Enter. The server that appears (for example: `\\TMWS3A`) can be used as the LDAP server.

```
C:\WINDOWS\system32\cmd.exe
C:\>echo %logonserver%
\\TMWS3A
C:\>_
```

## Method 2

You must first discover the name of your domain.

1. To determine the name of your domain, input nslookup "server result from echo %logonserver%" discovered in Method 1.
  - The domain is placed behind the "tmws3a" server discovered in Method 1. In this example, technical.marketing.com.

```
C:\WINDOWS\system32\cmd.exe
C:\>nslookup tmws3a
Server: tmws3a.technical.marketing.com
Address: 15.62.64.203
```

2. The following command can then be used to provide a list of DNS servers.
  - nslookup "name of your domain" (i.e. nslookup TECHNICAL.MARKETING.COM). In a Windows Active Directory environment, a DNS server is typically running Active Directory which contains the LDAP database.

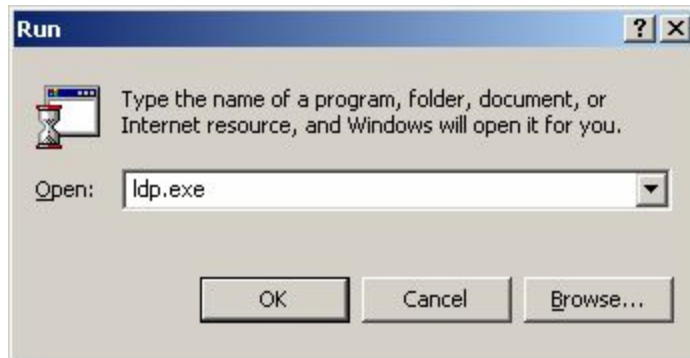
```
C:\WINDOWS\system32\cmd.exe
C:\>nslookup technical.marketing.com
Server: tmws3a.technical.marketing.com
Address: 15.62.64.203

Name: technical.marketing.com
Address: 15.62.64.203
```

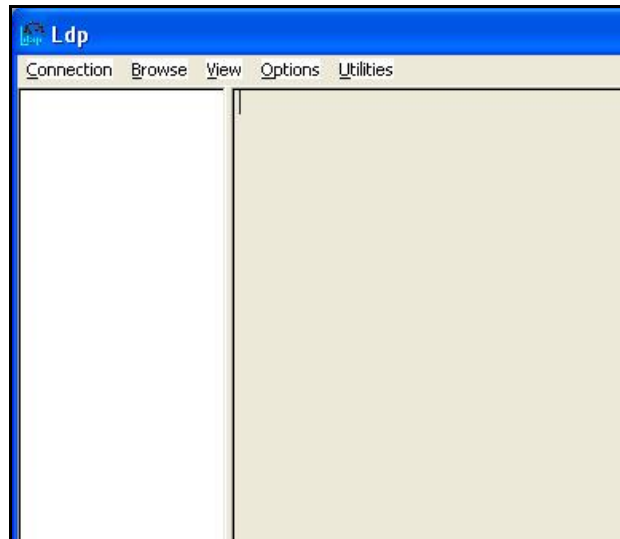
---

## Step 2: Setting up LDP

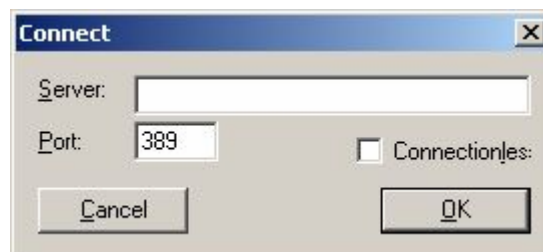
1. Open LDP by clicking on Start ® Run, and typing ldp.exe; then press Enter or click OK.



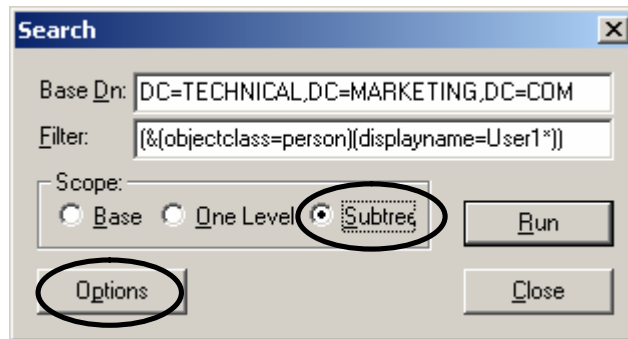
2. From the Ldp menu, select Connection ® Connect.



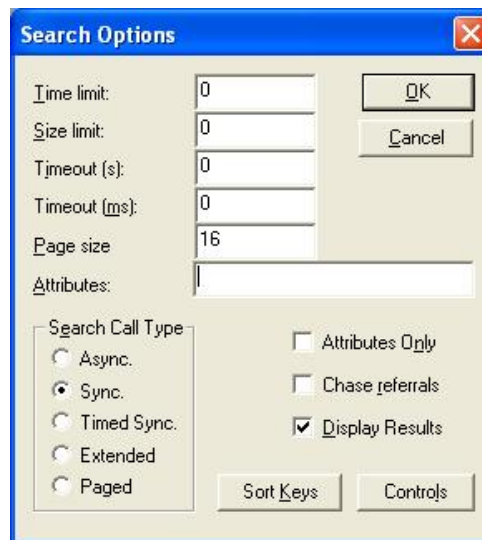
3. In the Connect window, input the IP address or hostname of the LDAP server in the Server box; then input 389 or 3268 as the Port number. Click OK.
  - Port 389 is the standard LDAP port. However, it may be necessary to use port 3268 when communicating with a Windows Global Catalog Active Directory Server.



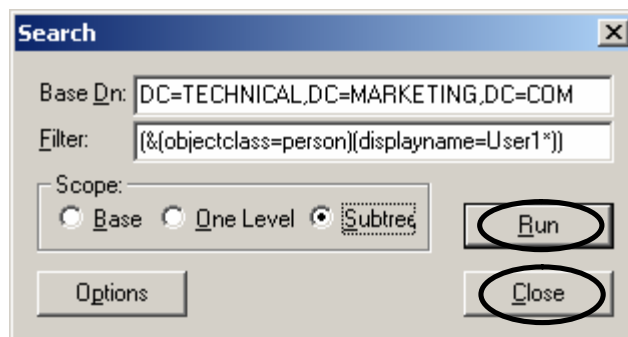




- In the Search Options window, remove all entries in Attributes; then click OK.



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



- 
9. On the LDP screen, locate the user DN from the returned results. Copy it for use in the Embedded Web Server (EWS).
    - The Search Prefix begins after the individual user CN.

```
>> Dn: CN=User1,CN=Users,DC=TECHNICAL,DC=MARKETING,DC=COM
4> objectClass: top; person; organizationalPerson; user;
1> cn: User1;
1> sn: User1;
1> description: Standard User;
1> physicalDeliveryOfficeName: Boise;
1> givenName: User1;
1> distinguishedName: CN=User1,CN=Users,DC=TECHNICAL,DC=MARKETING,DC=COM;
1> instanceType: 0x4 = ( IT_WRITE );
1> whenCreated: 11/16/2005 11:41:10 Mountain Standard Time Mountain Daylight Time;
1> whenChanged: 11/16/2005 11:41:39 Mountain Standard Time Mountain Daylight Time;
1> displayName: User1;
```

---

#### 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. The example below is User1.

```
>> Dn: CN=User1,CN=Users,DC=TECHNICAL,DC=MARKETING,DC=COM
4> objectClass: top; person; organizationalPerson; user;
1> cn: User1;
1> sn: User1;
1> description: Standard User;
```

---

## Step 3: Kerberos Authentication

---

#### Note

Embedded Kerberos Authentication uses session tickets in the authentication process. The session tickets are time stamped by both the Kerberos Domain Controller (KDC) and the MFP. It is essential that the stamped times are within five minutes of each other. This can be accomplished by setting identical time on both the KDC and MFP.

1. Open the EWS in a web browser.
2. Select the Settings tab, and then Kerberos Authentication.
3. Under the Accessing the Kerberos Authentication Server section,
  - a. Enter the Kerberos Default Realm (Domain).
    - w The Kerberos Default Realm (Domain) is case-sensitive and needs to be input using capital letters. Example: TECHNICAL.MARKETING.COM

- 
- b. Enter the Kerberos Realm for the Kerberos Server Hostname. DNS finds the first available Kerberos Domain Controller.
    - w As an alternative, this can be a hostname or an IP address.
  - c. The Kerberos Server Port should be auto filled as 88.

Accessing the Kerberos Authentication Server

Enter information about the Kerberos Realm (Domain).

Kerberos Default Realm (Domain):	TECHNICAL.MARKETING.COM
Kerberos Server Hostname:	TECHNICAL.MARKETING.COM
Kerberos Server Port:	88

4. Under the Accessing the LDAP Server section,
  - a. Select Kerberos from the LDAP Server Bind Method drop-down box.
  - b. Choose the radial button of the Credential method desired.
    - w If choosing Use Public Credentials, enter a username and password.

---

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.

- 
- c. Input the LDAP server in the LDAP Server field.

---

Hint

Using the command “nslookup technical.marketing.com” earlier, 15.62.64.203 was the server IP address discovered.

- 
- d. Input 389 in the Port field.

Accessing the LDAP Server

Enter the method and credentials used to access the LDAP server. The user will not be fully authenticated until the LDAP protocol retrieves the user's e-mail address.

LDAP Server Bind Method: Kerberos

**Credentials**

Use Device User's Credentials

Use Public Credentials:

Username:	Administrator
Password:	*****
LDAP Server:	15.62.64.203
Port:	389

5. Under the Searching the LDAP Database section,
  - a. Paste the Search Prefix into the Search Root field.
  - b. Input sAMAccountName into the “Match the name entered with the LDAP attribute of” field.

```

1> logonCount: 2;
1> sAMAccountName: User1;
1> sAMAccountType: 805306368;
1> userPrincipalName: User1@TECHNICAL.MARKETING.COM;
1> objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=TECHNICAL,DC=MARKETING,DC=COM;
1> mail: user1@marketing.com;

```

- c. Find the device user email address in the LDP trace. Copy the attribute defining the email address.
  - w Paste the attribute into the “Retrieve the device user’s email address using attribute of” field.

```

1> logonCount: 2;
1> sAMAccountName: User1;
1> sAMAccountType: 805306368;
1> userPrincipalName: User1@TECHNICAL.MARKETING.COM;
1> objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=TECHNICAL,DC=MARKETING,DC=COM;
1> mail: User1@marketing.com;

```

- d. Find the device user “name using the attribute of” in the LDP trace. Copy the attribute defining the name.

```

>> Dn: CN=User1,CN=Users,DC=TECHNICAL,DC=MARKETING,DC=COM
4> objectClass: top; person; organizationalPerson; user;
1> cn: User1;
1> sn: User1;
1> description: Standard User;
1> physicalDeliveryOfficeName: Boise;
1> givenName: User1;
1> distinguishedName: CN=User1,CN=Users,DC=TECHNICAL,DC=MARKETING,DC=COM;
1> instanceType: 0x4 = ( IT_WRITE );
1> whenCreated: 11/16/2005 11:41:10 Mountain Standard Time Mountain;
1> whenChanged: 11/16/2005 11:41:39 Mountain Standard Time Mountain;
1> displayName: User1;
1> uSNCreated: 14019;
1> uSNChanged: 14026;

```

- e. Paste the attribute into the “and name using the attribute of” field.
- f. Click Apply.

## Step 4: Configure the Authentication Manager

1. Click Authentication Manager on the left-side menu.
2. On the Authentication Manager screen, select Kerberos Authentication from the Authentication method drop-down list.
3. Click Apply.

## Step 5: Configure Addressing Settings

1. Click the Digital Sending tab.
2. Select Addressing from the right-side menu.
3. Select the "Allow device to directly access an LDAP Address Book" check box (screenshot on next page).
4. Under the Accessing to LDAP Server section,
  - a. Select Kerberos from the LDAP Server Bind Method drop-down list.
    - w The LDAP Server Bind Methods on the Addressing Settings and Kerberos Authentication screens must match for Kerberos authentication to work properly.
  - b. Under Credentials, select the Use Public Credentials radial dial.
    - w Input the Username and Password.

- w Input the Kerberos Default Realm (Domain).  
Example: TECHNICAL.MARKETING.COM
- w Input the Kerberos Server Hostname. Example: 15.62.64.203
- w Input the Kerberos Server Port. Example: 88.
- c. Input the LDAP Server. Example: 15.98.10.51
- d. Input the Port number. Example: 389

### Addressing Settings

Allow Device to directly access an LDAP Address Book

Accessing the LDAP Server

LDAP Server Bind Method:

**Credentials**

Use Device User's Credentials

Use Public Credentials:

Username:

Password:

Kerberos Default Realm (Domain):

Kerberos Server Hostname:

Kerberos Server Port:

LDAP Server:

Port:

5. Under the Searching the Database section,
  - a. Input the Search Prefix into the Search Root field.
  - b. Select an option from the "Device user information retrieval method" drop-down list. The list contains three options. The appropriate choice depends on the customer network environment.
    - w Select Exchange 5.5 Defaults when exchange 5.5 servers are used in LDAP addressing.
    - w Select Active Directory Defaults for Windows 2000 or later network environments.
    - w Select Custom for specialized network environments.
6. Click Apply.

## Step 6: Use the MFP control panel

1. At the MFP, touch the print mode button once to display the “Send/Store setting menu” screen. Touch the Network icon, and the screen displays a request for authentication (shown below).
  - The control panel screens for Kerberos Authentication and NTLM Authentication are identical.

### 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.

2. Use the touch screen keypad to input the authentication.
  - Once input, touch OK. The message “Authentication in progress. Please wait” displays. When the authentication completes, the Send to Network Folder screen appears.
  - If authentication fails, the message “Authentication Failed. Try Again” displays. If this occurs, re-input your credentials.

---

# Troubleshooting

The following section covers three troubleshooting issues: Reverse DNS, Time Synchronization, and Kerberos Realm Syntax.

## Reverse DNS must be configured

Kerberos authentication uses reverse DNS in the authentication process. Reverse DNS helps prevent “Man In The Middle” attacks, and adds an added level of security to the Kerberos process. Kerberos authentication fails and will not operate in a network environment that does not have reverse DNS enabled.

You can verify that reverse DNS is operational using the Nslookup command. Nslookup (Name Server Look Up) is a standard tool available in most Windows, Unix, and Linux environments. You can perform this operation in Windows with the following steps:

Start > Run > cmd > Nslookup “IP Address of the Kerberos Domain Controller”

An example of a proper forward and reverse DNS lookup:

```
C:\>nslookup server1.technical.marketing.com
```

```
Server: server1.technical.marketing.com
```

```
Address: 10.0.0.1
```

```
Name: server1.technical.marketing.com
```

```
Address: 10.0.0.1
```

An example of an in-correct forward and reverse DNS lookup:

```
C:\>nslookup server1.technical.marketing.com
```

```
Server: server1.technical.marketing.com
```

```
Address: 10.0.0.1
```

```
Name: server1.technical.futuremarketing.com
```

```
Address: 10.0.0.1
```

## Time Synchronization

Embedded Kerberos Authentication uses session tickets in the authentication process. The session tickets are time stamped by both the Kerberos Domain Controller (KDC) and the MFP.

It is essential that this time synchronization remain within five minutes of each other. This can be accomplished by setting identical time on both the KDC and the MFP.

## Kerberos Realm Syntax

When specifying the Kerberos Realm, it is essential that the entry is capitalized. This entry must be entered into three separate sections of the EWS: Kerberos Authentication, Addressing Settings, and Network Settings.

### Kerberos Authentication

---

Accessing the Kerberos Authentication Server

Enter information about the Kerberos Realm (Domain).

Kerberos Default Realm (Domain): TECHNICAL.MARKETING.COM

Kerberos Server Hostname: SERVER1

Kerberos Server Port: 88

### Addressing Settings

Allow Device to directly access an LDAP Address Book

---

Accessing the LDAP Server

LDAP Server Bind Method: Kerberos

**Credentials**

Use Device User's Credentials

Use Public Credentials:

Username: User1

Password: ●●●●●●

Kerberos Default Realm (Domain): TECHNICAL.MARKETING.COM

Kerberos Server Hostname: SERVER1

Kerberos Server Port: 88

LDAP Server: SERVER1

Port: 389

### Network Settings

TCP/IP | IPX/SPX | AppleTalk

IP Configuration Method: Manual

**Note: A change in IP Address will res**

Host Name: MFP1

IP Address: 10.0.0.2

Subnet Mask: 255.255.248.0

Default Gateway: 10.0.0.3

Domain Name: TECHNICAL.MARKETING.COM

