

# Generic LDAP Integration

In addition to adding users manually as described in chapter [User Management](#), MailStore Server can synchronize its internal user database with the LDAP server of your company.

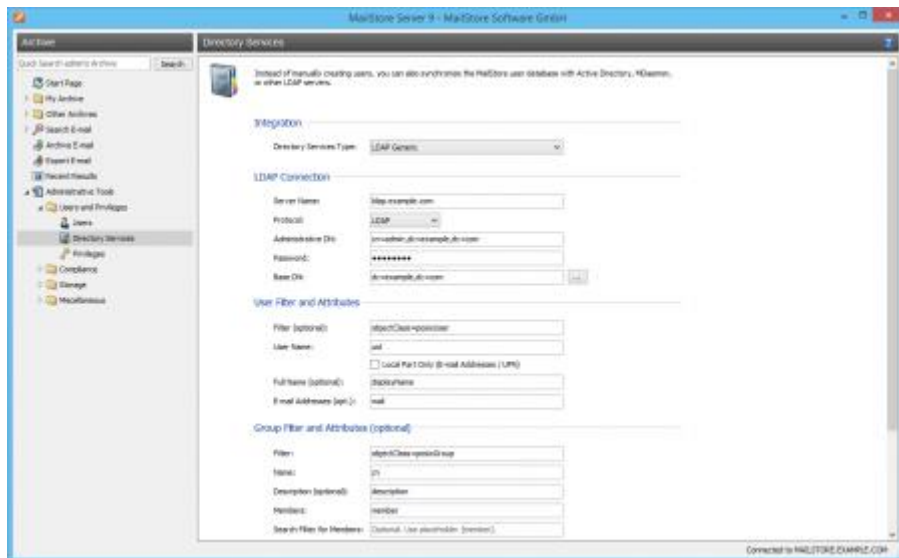
During synchronization user information such as user names and email addresses are read from the LDAP server and recorded in MailStore Server's user database. No changes are made to the LDAP server itself by MailStore Server. The scope of the synchronization can be limited through filters.

## Contents

- [1 Accessing Directory Service Integration](#)
- [2 Connection to the LDAP Directory Service](#)
  - [2.1 LDAP Connection](#)
  - [2.2 User Filter and Attributes](#)
  - [2.3 Group Filter and Attributes](#)
  - [2.4 Options](#)
- [3 Assigning Default Privileges](#)
- [4 Configuration Samples](#)
  - [4.1 Active Directory](#)
  - [4.2 OpenLDAP](#)
- [5 Running Directory Services Synchronization](#)
- [6 Login with LDAP server Credentials](#)
  - [6.1 Procedure for Users Created by Synchronization with LDAP server](#)
  - [6.2 Procedure for Manually Created Users](#)

## Accessing Directory Service Integration

- Log on to MailStore Client as a MailStore Server administrator.
- Click on *Administrative Tools > Users and Privileges* and then on *Directory Services*.
- In the *Integration* section, change the directory service type to *LDAP server*.



## Connection to the LDAP Directory Service

For synchronization MailStore Server requires information on how to connect to the LDAP directory service and how to obtain the required data from it.

### LDAP Connection

Name	Description
Server Name	DNS name or IP address of your LDAP server
Protocol	Configure whether the connection to the LDAP server is to be unencrypted on port 389, LDAP-TLS on port 389, or LDAP-SSL on port 636
Ignore SSL Security Warnings (only when using LDAP-TLS or LDAP-SSL)	Permit connections when a self-signed or non-public certificate is used by the LDAP server
Administrative DN	Distinguished Name (DN) or user name of a user with appropriate privileges on the LDAP server
Password	Password of the user specified in Administrative DN
Base DN	LDAP base DN, if needed

### User Filter and Attributes

---

<b>Name</b>	<b>Description</b>
Filter (optional)	Filter LDAP objects to return only user objects with email addresses
User Name	The LDAP attribute containing the username that you wish MailStore to use
Local Part Only (E-mail Addresses / UPN)	If unchecked, MailStore will use the full username including domain portion, e.g. <i>username@example.com</i> . If checked, MailStore will only use the local part of the User Name specified, e.g. the <i>username</i>
Full Name (optional)	The full name of the user, for display purposes within MailStore
E-mail Addresses (opt.)	The LDAP attribute containing the user's email address. This can contain multiple, comma separated, e-mail addresses

## Group Filter and Attributes

<b>Name</b>	<b>Description</b>
Filter	LDAP filter to return only group objects
Name	The LDAP attribute that contains the common name of a group
Description (optional)	The LDAP attribute that contains a human readable description for each group
Members	The LDAP attribute that contains the common name of group members
Search Filter for Members	LDAP filter to resolve group members when members are not specified as a DN string as part of the group results. MailStore will fill in the {member} variable with values from the <i>Members</i> attribute
Group	The actual group(s) containing users that MailStore Server will synchronize

## Options

<b>Name</b>	<b>Description</b>
Automatically delete users in MailStore Server	If enabled, MailStore will delete users from the local MailStore database when the user is deleted, removed from the filtered group, or falls out of scope based on the above LDAP filter settings

## Assigning Default Privileges

By default, users that have been synchronized to MailStore Server from a directory service have the privilege to log on to MailStore Server as well as read access to their own user archive.

You can configure those default privileges before synchronization, for example, to assign the privilege *Archive E-mail* to all new users. To do this, click on *Default Privileges...*

More information on managing user privileges and their effects is available in the chapter [Users, Folders and Settings](#) which also has details on editing existing privileges.

## Configuration Samples

### Active Directory

It is possible to connect LDAP Generic to Active Directory, allowing for more flexibility and control than MailStore's built-in Active Directory support. For example, LDAP Generic will allow you to accept invalid or self-signed certificates, use custom filters or change which attributes are used by MailStore.

It is assumed that the Active Directory LDAP service is reachable by the MailStore instance on TCP port 389 or 636, including opening ports in the firewall, where applicable.

As most Active Directory configurations are quite similar, it will be possible to copy/paste most of the examples below, making only minor modifications based on your environment.

#### LDAP Connection

Name	Value	Description
Server Name	dc001.example.com	DNS name or IP address of an Active Directory domain controller.
Protocol	LDAP	Do not use transport encryption
	LDAP-TLS	Use TLS as transport encryption
	LDAP-SSL	Use SSL as transport encryption
Ignore SSL Security Warnings	<i>Enabled</i>	Establish a TLS/SSL encrypted connection, even if the certificate validation failed.
	<i>Disabled</i>	Do not establish a TLS/SSL encrypted connection, if the certificate validation failed.

Administrative DN	mailstoreserver@example.com	Active Directory account for MailStore's use
Password	MySecretPassword	Password of the user specified in <i>Administrative DN</i> above
Base DN	Empty	LDAP base DN will be detected automatically in Active Directory environments

### User Filter and Attributes

Name	Value	Description
Filter (optional)	(objectCategory=User)	All users
	(&(objectCategory=User)(mail=*))	All users with Active Directory e-mail addresses
	(&(objectCategory=User)(proxyAddresses=*))	All users with Exchange e-mail addresses
	(&(objectCategory=User)(proxyAddresses=*)(mail=*))	All users with Exchange e-mail addresses who are also listed in the global address book
User Name	userPrincipalName	Use Active Directory user name as MailStore user name
	sAMAccountName	Use pre-Windows 2000 user name as MailStore user name

Local Part Only (E-mail Addresses / UPN)	Enabled	Only use the local part from the Active Directory user name in UPN format
	Disabled	Use the full Active Directory user name in UPN format
Full Name (optional)	displayName	The user's visible name in Active Directory
E-mail Addresses (opt.)	proxyAddresses	Exchange environments
	mail	Non-Exchange environments

### Group Filter and Attributes

Name	Value	Description
Filter	(objectCategory=Group)	All objects of category <i>Group</i> , usually all groups
Name	cn	Use the value of the LDAP attribute <i>CN</i> as group name
Description (optional)	description	Use the value of the LDAP attribute <i>description</i> as group name
Members	member	Use the value LDAP attribute <i>member</i> to determine group members
Search Filter for Members	empty	Group members are returned as Distinguished Names
Group	MailStore Users	Synchronize only users from the <i>MailStore Users</i> group

### OpenLDAP

OpenLDAP is a commonly used LDAP server, configuration will require some knowledge of your LDAP environment.

It is assumed that the LDAP service is reachable by the MailStore instance on TCP port 389 or 636, including opening ports in the firewall, where applicable.

As OpenLDAP is very flexible, configuration options vary from server to server and you may need to make significant modifications to the examples below to fit the schema used in your environment.

## LDAP Connection

Name	Value	Description
Server Name	directory.example.com	DNS name or IP address of the OpenLDAP server.
Protocol	LDAP	Do not use transport encryption
	LDAP-TLS	Use TLS as transport encryption
	LDAP-SSL	Use SSL as transport encryption
Ignore SSL Security Warnings	<i>Enabled</i>	Establish a TLS/SSL encrypted connection, even if the certificate validation failed.
	<i>Disabled</i>	Do not establish a TLS/SSL encrypted connection, if the certificate validation failed.
Administrative DN	cn=admin,dc=example,dc=com	LDAP username that MailStore should use for accessing the OpenLDAP server
Password	MySecretPassword	Password of the user specified in <i>Administrative DN</i> above
Base DN	dc=example,dc=com	The Base-DN of the LDAP directory

## User Filter and Attributes

Name	Value	Description
Filter (optional)	(objectClass=posixAccount)	All objects of

---

		type <i>posixAccount</i> , usually all users
	<code>(&amp;(objectClass=posixAccount) (mail=*))</code>	All users with configured email address
User Name	uid	Use the value of LDAP attribute <i>UID</i> as MailStore user name
	cn	Use the value of LDAP attribute <i>CN</i> as MailStore user name
Local Part Only (E-mail Addresses / UPN)	<i>Enabled</i>	Only use the local part from a user name in UPN format
	<i>Disabled</i>	Use the full user name in UPN format
Full Name (optional)	displayName	Use the value of LDAP attribute <i>displayName</i> as MailStore user name
E-mail Addresses (opt.)	mail	Use the values of LDAP attribute <i>mail</i> for the email addresses of MailStore users

---

---

## Group Filter and Attributes

Name	Value	Description
Filter	(objectClass=posixGroup)	All objects of category <i>posixGroup</i> , usually all groups
Name	cn	Use the value of the LDAP attribute <i>CN</i> as group name
Description (optional)	description	Use the value of the LDAP attribute <i>description</i> as group name
Members	members	Use the value LDAP attribute <i>members</i> to determine group members
Search Filter for Members	<i>empty</i>	Group members are returned as Distinguished

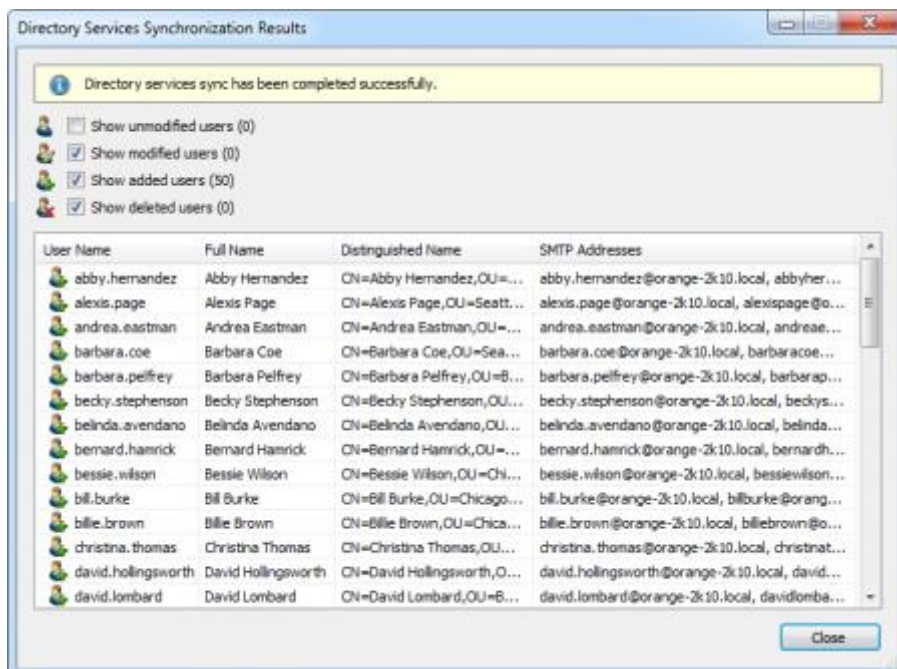
		Names
	<code>(   (&amp; (objectClass=posixAccount) (uid={member})) (&amp; (objectClass=p osixGroup) (cn={member}))) )</code>	members in <i>memberU</i> <i>id</i> are only given as plain user or group names
Group	MailStore Users	Synchron ize only users from the <i>MailStore</i> <i>Users</i> group

---

## Running Directory Services Synchronization

Click on *Test Settings* to check synchronization configuration and the results returned by the directory service without any changes to the MailStore Server user database being actually committed.

To finally run the synchronization, click on *Synchronize now*. The results are shown with any changes committed to the MailStore Server user database.



## Login with LDAP server Credentials

By default, each user created in MailStore Server has a local password. The MailStore Server administrator can specify this password during creation of a new user account. The respective user can later change this password in MailStore Client's *Quick Access* section if he or she has ample privileges.

Alternatively, if an LDAP server is available, you can configure MailStore Server to allow users to log on to MailStore Server using their LDAP server credentials.

### Procedure for Users Created by Synchronization with LDAP server

If you have created MailStore Server users by LDAP server synchronization as described in the previous section, no further action is required. In this case, MailStore Server has already configured all necessary settings automatically for you. Users can log on to MailStore Server via *Standard Authentication* by using their LDAP server username and LDAP server password.

### Procedure for Manually Created Users

If you have created MailStore Server users manually and want them to be able to log on using their LDAP server credentials, please proceed as follows after you have configured the LDAP server integration as described above.

- Verify that the names of the MailStore Server users match those of the corresponding LDAP server users.
- In the *General Information* section of the user properties select *Directory Services for Authentication*.



Users can now log on to MailStore Server via *Standard Authentication* by using their LDAP server username and LDAP server password.