

Synchronizing User Accounts with Active Directory

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

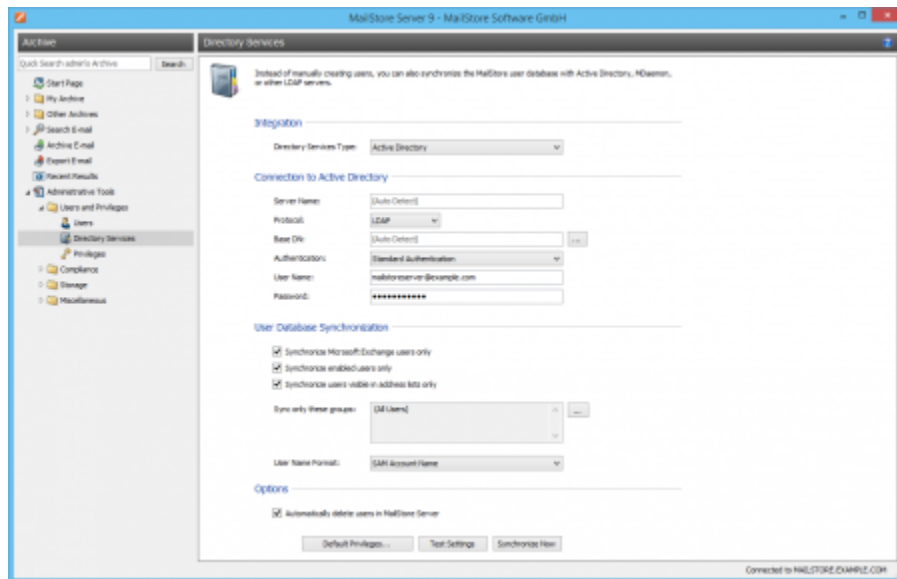
Please note: MailStore Server does not support either subdomains or domain trusts. The MailStore Server service must run as 'Local System account' and the server must be a member of the domain if you want to use 'Integrated Windows authentication'.

Contents

- [1 Accessing Directory Service Integration](#)
- [2 Connection to Active Directory](#)
 - [2.1 User Database Synchronization](#)
 - [2.2 Options](#)
- [3 Assigning Default Privileges](#)
- [4 Running Directory Services Synchronization](#)
- [5 Login with Active Directory Credentials](#)
 - [5.1 Procedure for Users Created by Synchronization with Active Directory](#)
 - [5.2 Procedure for Manually Created Users](#)
- [6 MailStore Client Single Sign-On](#)

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 *Active Directory*.



Connection to Active Directory

For synchronization MailStore Server requires information on how to connect to the Active Directory.

- **Server (optional)**
DNS name or IP address of an Active Directory users domain controller. If the MailStore Server machine is a member of the Active Directory, this setting is detected automatically.
- **Protocol**
The protocol used to communicate with an Active Directory domain controller.
 - *LDAP*
The default protocol when accessing an Active Directory. Though parts of the connection is unencrypted the real payload is encrypted.
 - *LDAPS*
Additionally SSL secured version. Be aware that a properly configured certificate infrastructure is required, in which the MailStore Server computer must classify the domain controller's certificate as trustworthy.
- **Base-DN (optional)**
Base DN of your Active Directory. Often the Base DN can be derived from the Active Directory domain name. For example, if the Active Directory domain name is *company.local* the Base DN usually is *dc=company,dc=local*. The Base DN can also be selected by clicking the button left of the text field if access to an Active Directory domain controller is available. If the MailStore Server machine is a member of the Active Directory, this setting is detected automatically.
- **Authentication**
Define how the MailStore Server service should identify itself to the Active Directory:
 - *Standard Authentication*
If MailStore Server is not installed directly on an Active Directory domain controller, using

standard authentication is required. In this case, fill out the *User Name* and *Password* fields; enter the user name in UPN notation, e.g. *Administrator@company.local*

- **Windows Authentication**

If MailStore Server is installed directly on an Active Directory domain controller, the MailStore Server service already has the necessary privileges to authenticate against Active Directory using Windows authentication.

User Database Synchronization

After configuring the connection settings as described above, you can specify filter criteria for the Active Directory synchronization in this section.

- **Synchronize Microsoft Exchange users only**

Only user accounts with email addresses configured in Active Directory will be taken into account by the synchronization. Clear this checkbox only if all Active Directory users should be created as MailStore Server users as well.

- **Synchronize enabled users only**

Only user accounts enabled in Active Directory will be taken into account by the synchronization. Deactivating this option may be useful if certain Exchange mailboxes should be archived whose Active Directory user accounts are deactivated by default.

- **Synchronize users visible in address lists only**

Only Active Directory user accounts will be taken into account by the synchronization whose Exchange mailboxes are not hidden from Exchange address lists.

- **Sync only these groups**

Choose one or several Active Directory security groups if you only want their members to be created as MailStore Server users. That way it's possible to exclude certain Active Directory accounts from being synchronized to MailStore Server, e.g. system accounts.

Options

- **Automatically delete users in MailStore Server**

Here you can choose whether users whose accounts have been deleted in the Active Directory will also be deleted in MailStore Server's user database by the synchronization. If the archive folder of such a user already contains archived emails, only the user entry but not its archive folder will be deleted in MailStore Server. Additionally, only MailStore Server users that have their authentication method set to *Directory Services* will be deleted.

Assigning Default Privileges

By default, users that have been synchronized to MailStore Server from an Active Directory 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

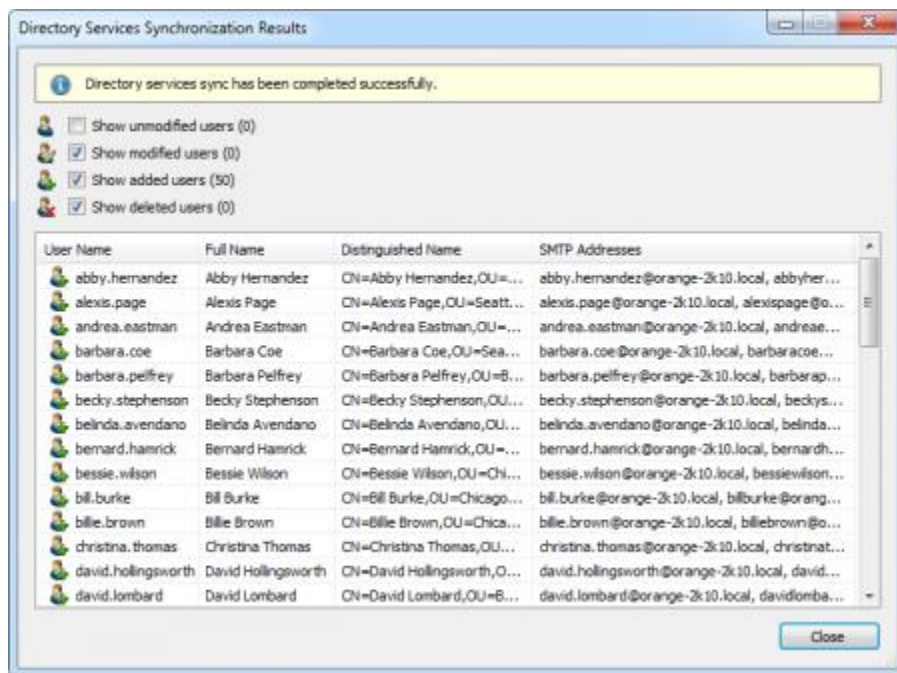
Archive E-mail to all new users. To do this, click on *Default Privileges...*

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.

Running Directory Services Synchronization

Click on *Test Settings* to check synchronization configuration and the results returned by the Active Directory 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 Active Directory 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 Active Directory is available, you can configure MailStore Server to allow users to log on to MailStore Server using their Active Directory credentials.

Procedure for Users Created by Synchronization with Active Directory

If you have created MailStore Server users by Active Directory 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 Active Directory username and Active Directory 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 Active Directory credentials, please proceed as follows after you have configured the Active Directory integration as described above.

- Verify that the names of the MailStore Server users match those of the corresponding Active Directory 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 Active Directory username and Active Directory password.

MailStore Client Single Sign-On

For information on using the single sign-on functionality in Active Directory environments, please refer to the article [MailStore Client Deployment](#).