Recast

LDAP

Last Modified on 2026-09-24

Overview screen

Here you can configure a few basic options for the identity source.

Name – The name of the identity source. In the case of Active Directory, we recommend you use the same value as the NetBIOS name of the Active Directory.
Type – The type of identity source.
Hidden – When an identity source is hidden it will not appear on the login screen.

> Note that the **Name** and **Type** cannot be changed once the identity source is created.

Settings screen

Schema – There are three options available: Active Directory, eDirectory and JumpCloud. The schema cannot be changed once the identity source is created.
Server discovery method (available only for Active Directory)

- *Manual* – Manually configure LDAP servers and priorities.
- *DNS* – Auto detect LDAP servers based on DNS records for the specified FQDN of the Active Directory domain.
- *DC Locator* – Auto detect LDAP servers using the Microsoft DC Locator process, take into account Active Directory sites and use the LDAP servers that are geographically closer to the Application Workspace servers.

Domain name – (available only for Active Directory) – the FQDN of the Active Directory domain; For example: ad.liquit.com
Secure connectivity – (available only for Active Directory) – If enabled, only secure LDAP connectivity will be used to connect to the Active Directory domain.
Username – The username to log into the identity source.
Password – The password to log into the identity source.
Photos – Determines how the user images are retrieved:

- *None* – No user photos are retrieved or shown in the Application Workspace.
- *Query* – The user photos are actively retrieved upon requesting. Note that this can have performance impact on large LDAP directories.
- *Cache* – The user photos are stored in the cache of Application Workspace.

Modifications – Determines which modification can be made to the LDAP directory:

- *None* – No modifications are allowed.
- *Only Passwords* – Only the passwords of the users can be modified.
- *All* – All user attributes can be modified.

ID Attributes – Determines which attribute will be used to synchronize to the Application Workspace. This option cannot be changed once the identity source is created. The following options are available:

- *objectGUID* – The guid corresponding to the user is used to synchronize (available only for Active Directory).
- *sAMAccountnam* – The SAM-Account-Name attribute is used to synchronize (available only for Active Directory).
- *guid* – The guid attribute is used to synchronize (available only for eDirectory).
- *CN* – The CN attribute is used to synchronize (available only for eDirectory).
- *uid* – The uid is used to synchronize (available only for JumpCloud).

Use delta synchronization* – Use delta synchronization to synchronize changes since last synchronization operation instead of performing a full synchronization at every refresh. (available only for Active Directory)

Recast

*Use delta synchronization
For Active Directory delta synchronization you need to apply additional rights. Grant the LDAP user "Replicating Directory Changes" rights on the AD domain object as explained in the Microsoft documentation.

Servers screen

The **Server** screen is displayed only if **Server discovery method** is set to *Manual* in the **Settings** screen of this identity source.

Define the LDAP server that can be contacted for retrieving data.

Address – The DNS name or IP address of the LDAP server.
Secure – If enabled, the connection is secure. (this is LDAPS (TLS), the LDAP extension "StartTLS" is not supported)
Port – The port of the LDAP server. Ports 389 and 636 are standard. Port 389 is suitable for environments where encryption is not a requirement while port 636 is specifically designated for secure LDAP communication using SSL/TLS encryption.
Priority – Servers will be accessed in a particular order based on their assigned priority. Round robin will be used for servers with the same priority.
Page size – The number of results that will be retrieved per chunk.
Connection timeout – The number of seconds before an LDAP connection times out.
Search timeout – The number of seconds an LDAP server can spend on a search.

Authentication screen

Configure the methods available to authenticate. The following options are available:

Form authentication – Allow the user to login via the Application Workspace login page (http/https).
Basic authentication – Enable basic login for the identity source.
Federated – For example: AD FS
NTLM – Not available for Azure AD.

Contexts screen

Define the context in which the users and groups need to be fetched. When no context is specified, all users and groups known to the LDAP server(s) will be synchronized.

The following options are available:

Context – Defines the container in which the users/groups will be synchronized.
Scope – The location in the LDAP tree where the LDAP DSA looks for matched entities.

- *Base* – Only the users or groups that are contained within the specified container are used.
- *Subtree* – All users or groups that are contained within the specified container or in sub containers are used.

Users – If enabled, the users will be synchronized within this container.
Groups – If enabled, the users will be synchronized within this container.

Contacts screen

Enable contacts – If enabled, contacts from this identity source will be used.
Require Email – If enabled, all objects without an email address will be hidden.

Group – Only show members of a certain group.

Show attributes section

Choose which attributes to be synchronized to Application Workspace.

Authenticator screen

Assign an authenticator to the identity source.

Authenticator – You can select one of the existing authenticators defined in Application Workspace.
Prefix – Insert a string to add before the username to form the base distinguished name (DN).
Suffix – Insert a string to add after the username to form the base distinguished name (DN).

Further reading

Contact automatic synchronization