LDAP Interface

Last Modified on 09/06/2022 11:37 am ACST

> This article is part of the systems administration guide. You will require administration access to view the pages mentioned in this article.

CareRight allows authenticating user logins against an Active Directory or LDAP server. This integration is be provided through the implementation of Lightweight Directory Access Protocol (LDAP) v3 client support in CareRight. LDAP v3 is supported by Active Directory.

CareRight supports the following functionality via LDAP only:

- Authenticate that the user name provided during a CareRight login attempt exists on the LDAP server.
- Authenticate that the password provided during a CareRight login attempt is accepted by the LDAP server for the supplied user name.

LDAP authentication is only supported in the CareRight web based application only. A user account must be created in CareRight with a username that is compliant with the LDAP server configuration.

CareRight restricts usernames to:

- Maximum of 255 characters
- Minimum of 1 character
- Cannot begin with an underscore (_)
- Usernames must be unique regardless of case (e.g. Cannot have both usernames of Bob and bob)

Configuration in CareRight

LDAP Configuration is available by navigating to: **Administration** > **Users and Groups** > **LDAP**

LDAP Server Configuration

Setting	Description	Example
LDAP Enabled	true to enable LDAP authentication	true
LDAP Host	The hostname or IP address of the LDAP server	ldap.example.com
LDAP Port	The TCP port number of the LDAP server	389 (no encryption) 636 (encrypted)
LDAP Encryption	SSL (Simple TLS) - The connection to the LDAP server will be encrypted TLS (Start TLS) - The connection to the LDAP server will negotiate encryption after connecting No Encryption - The connection to the LDAP server will not be encrypted	SSL (Simple TLS)

N.B.

- Encryption option "none" should not be used unless other security precautions are implemented by the client to

prevent network sniffing of usernames and passwords

Direct Bind

This section should be used if all CareRight users are in the same tree or organisational unit in LDAP. For example, all users have a DN matching "uid=username,dc=example,dc=com" where only "username" changes.

Setting	Description	Example
LDAP Bind DN	Contains the pattern of all users' DNs. The string "{login}" will be replaced by the username at time of login.	uid={login},dc=example,dc=com OrganisationName\{login}

Search then Bind

This section should be used if CareRight users might be across multiple trees within LDAP - for example, if users position includes an organisational unit. A search is performed for the user before authenticating them.

For example, if one user is "uid=alice,ou=doctors,dc=example,dc=com" and another user is "uid=bob,ou=staff,dc=example,dc=com" then this section should be used.

Setting	Description	Example
LDAP Admin Bind DN	Optional - DN of an LDAP user or service account which has permission to search for other users. If your LDAP server supports searching without authentication, leave this blank.	cn=admin,dc=example,dc=com
LDAP Admin Bind Password	Optional - Password for the Admin Bind DN if required	
LDAP Search Base	Location in the LDAP tree from which all users wlil be found below.	dc=example,dc=com
LDAP Search Filter	An LDAP search filter which finds the LDAP account for each CareRight user. The string "{login}" will be replaced by the username at time of login	uid={login} (&(sAMAccountName={login}) (accountClass=CareRightUser))

User Account Options

Each user account will have the option of defining the authentication method to user on login. The available options will be CareRight, LDAP & Default. The option of default will be the preset option. This option only appears if you have LDAP = TRUE set in Global Settings.

Authentication Process

During the login process CareRight will check the user account for the authentication method. If the method is set to CareRight then the existing authentication process will be followed. If the method is set to LDAP then the LDAP process, described next, will be followed. If the option is default then if the user is a Staff Member the setting of “default

authentication type to use for Staff Member logins" will be used to determine the method. If the user is not a Staff Member then the authentication method of CareRight will be used.

LDAP Authentication Process

When authenticating the user against the LDAP server one of the following results will occur.

- LDAP Technical Issue: This might occur if the LDAP server is unreachable or fails to negotiate the correct connection method. The user will be displayed a message that a technical error has occurred processing their login, and that they should notify the system administrator.
- LDAP Bind Failure: This will occur if the LDAP server rejects the attempt to authenticate (bind) the user. This may happen because :
    - The password is wrong.
    - The username doesn't exist.
    - The account has been disabled or locked.
    - The username and password is correct, but the user is required to change their password due to policy or configuration settings on the LDAP server.
- In all these cases the user will receive a message providing a summary of the possible errors and to contact the system administrator if they are unable to login after checking the possibilities.
- LDAP Bind Success: This occurs if the user name and password are correct and no other server policy conditions exist blocking the authentication attempt. The user is issued a session and continues as per existing CareRight behaviour.

User Account Creation

During the process of creating a user account the option will exist to select the authentication method. This is set pre-set to "default". The option to set the password will still exist, but blank values will be accepted.

Forgotten Password Option

The "Forgot your password?" option will not be functional for account configured to authenticate to LDAP servers. The user will be advised that the reset instructions have been sent, as per normal, but the contents of the email will advise the user to contact the system administrator as their account is centrally managed.

Changing a user's authentication method

If a user was configured to use LDAP authentication and this is then changed to CareRight method then the user will require a password to log in. This can be manually set for each user by an appropriately authorised user. Or if the user has an email address they can use the "Forgot your password?" option to send a password reset email to gain access to their account.

Please contact Clintel if you require further information on LDAP.