LapSafe® Active Directory Integration

Introduction

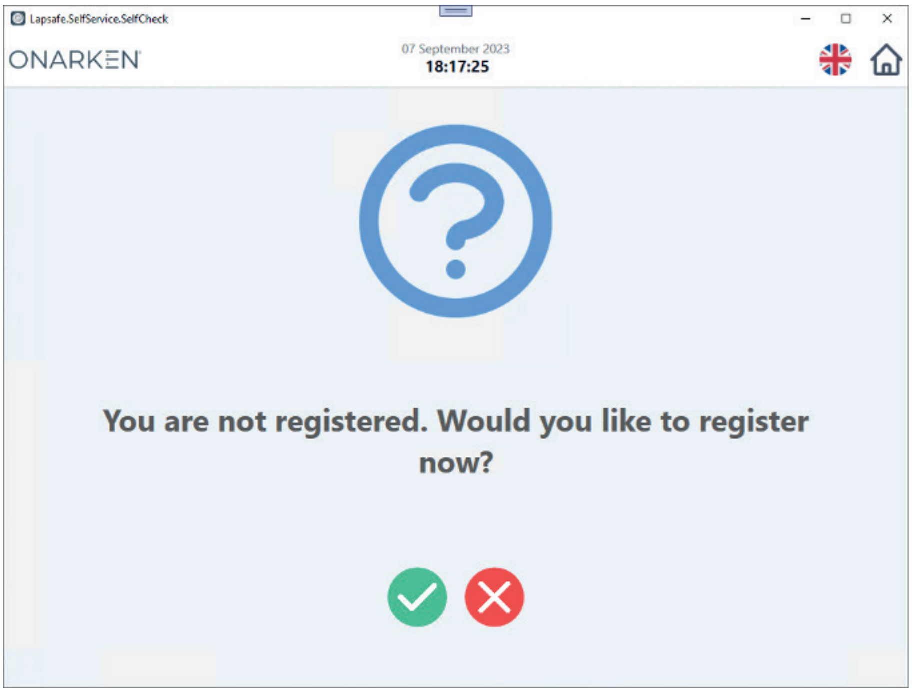
The basic concept of the LapSafe® Active Directory integration is to allow the LapSafe® client application to access the Active Directory database to authenticate the user when the user scans. The integration can either lookup user in the AD database using a specified attribute or request the user to login for self-registration. The LapSafe® installation is an asset loan system, automating the process of asset loan and return by using the LapSafe® client application to control user access and locker selection. The LapSafe® client application connects to the LapSafe® server in the cloud and maintains all the loan records, user permissions and provides user and system management functions.

LapSafe® Active Directory Integration

The LapSafe® Active Directory integration allows the system administrator to specify an Active Directory as a 3rd party user repository. When a user presents an ID at the LapSafe® installation, the LapSafe® client application performs an ID lookup in the Active Directory. This ID can be an attribute in the AD user record (AD Lookup), or it can be associated with the user via self-registration (AD Self-Registration). Note that both authentications require the user having a valid email address.

Active Directory Self Registration

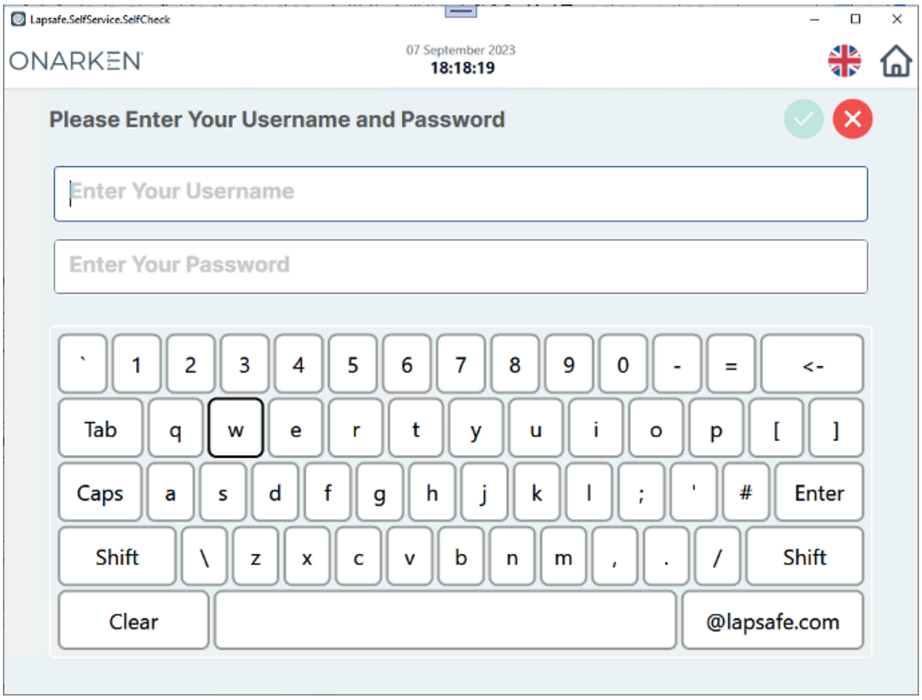
Active Directory Self Registration uses the user's AD credential to validate the user. When the user scans at the terminal the user ID is checked in ONARKEN® first, if the user is not found then the user is invited to self-register.



You are not registered. Would you like to register now?

The self-registration process requests the user to enter his AD user credential and this credential is validated with AD. Once the user is validated the user details are retrieved and sent to ONARKEN® and an ONARKEN® user is created. The ID used is then associated with the ONARKEN® user. If AD failed to validate the credential, then access to the lockers is denied.

Below is the self-registration screen.



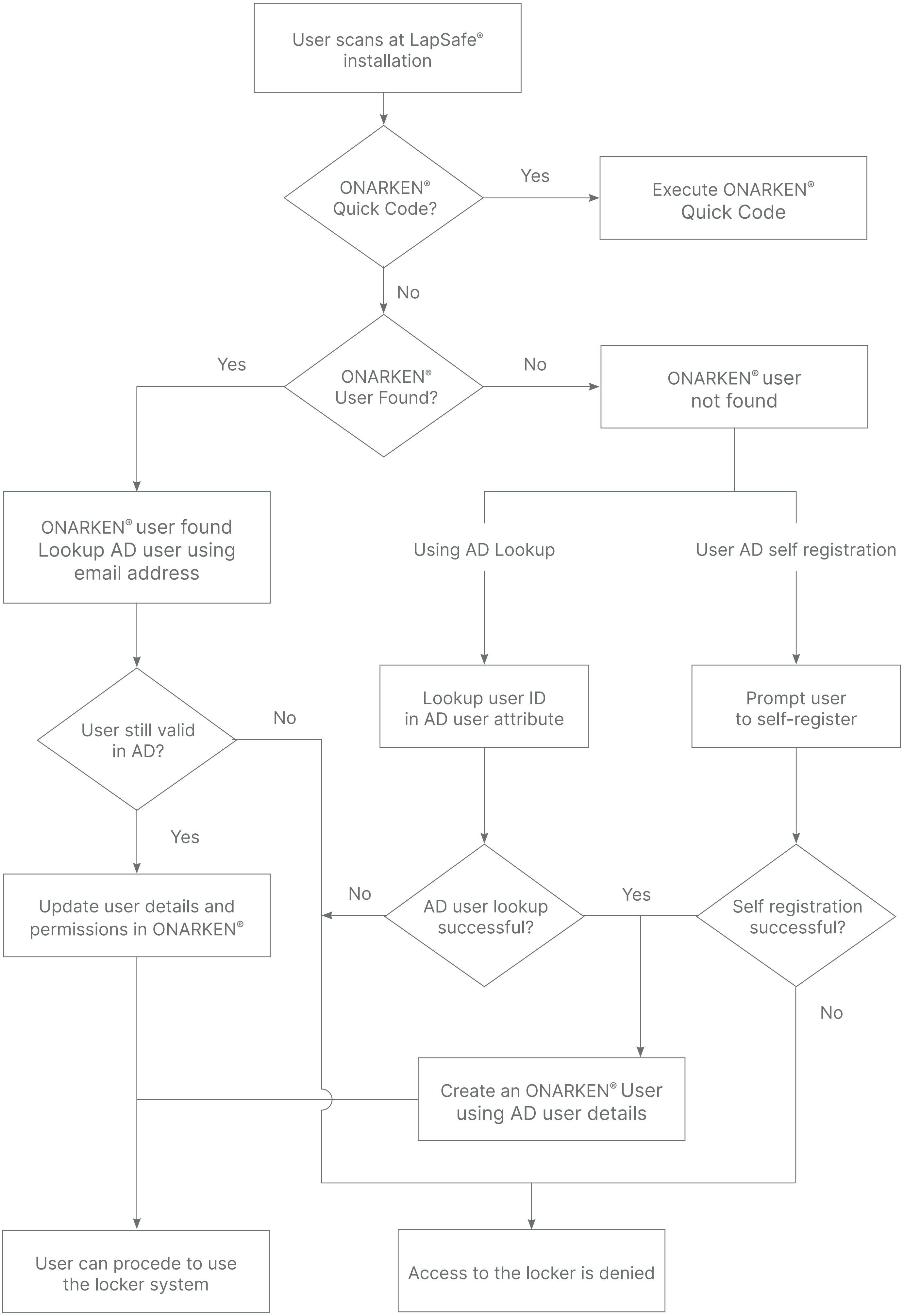
Lapsafe.SelfService.SelfCheck
ONARKEN
07 September 2023
18:18:19
Please Enter Your Username and Password
Enter Your Username
Enter Your Password
` 1 2 3 4 5 6 7 8 9 0 - = <-
Tab q w e r t y u i o p [ ]
Caps a s d f g h j k l ; ' # Enter
Shift \ z x c v b n m , . / Shift
Clear
@lapsafe.com

The AD self-registration method does not require user ID to be stored in Active Directory and hence reduces the overhead of keeping the user ID in sync with the user. This also has the advantage that the User can use any from of ID as it is simply associated with the ONARKEN® user. Once the self-registration is completed the user's email address is used to uniquely identify the user.

Active Directory User Lookup

Active Directory Lookup uses an attribute in the user record to store the user ID. When the user scans at the terminal, a search is performed in the Active Directory on the specified attribute for the ID. If the ID is found, the user details are retrieved and sent to the ONARKEN® server to create/update the user. If the ID is not found, access to the lockers is denied.
This method relies on the user ID being stored in Active Directory and the ID must match with the ID used by the user. If the ID of the user was changed the ID in AD must also change to match the user's ID.

For both AD Lookup and AD Self-registration, if the user is valid then the user details are retrieved, namely the user's display name, user's email address and the department that the user belongs to. All these user details are sent to ONARKEN® and an ONARKEN® user is created. The initial user permission is setup using the department setting of the user, where the department name is mapped to one of the user roles in the LapSafe® server. However, the user permissions can be further refined after the user has been created to allow for extra functionality provided by the LapSafe® system.

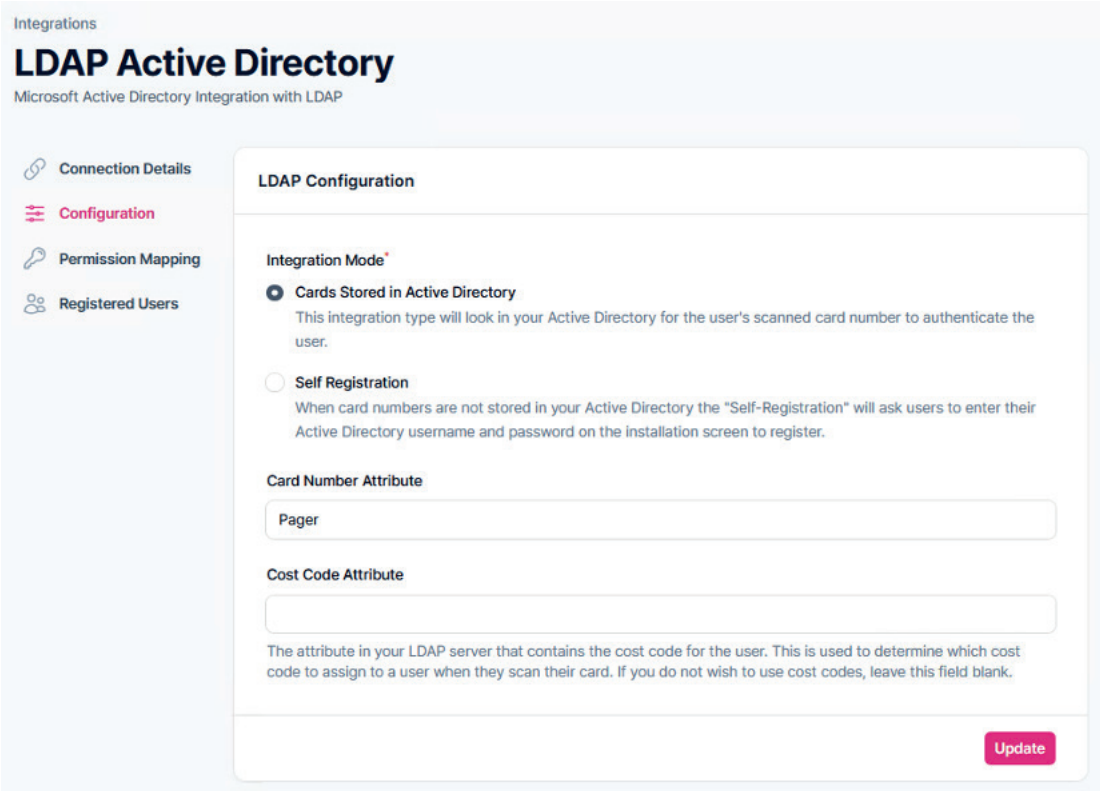

User scans at LapSafe® installation
ONARKEN® Quick Code?
Yes
Execute ONARKEN® Quick Code
No
ONARKEN® User Found?
Yes
No
ONARKEN® user not found
ONARKEN® user found Lookup AD user using email address
Using AD Lookup
User AD self registration
User still valid in AD?
No
Lookup user ID in AD user attribute
Prompt user to self-register
Yes
Update user details and permissions in ONARKEN®
No
AD user lookup successful?
Yes
Self registration successful?
No
Create an ONARKEN® User using AD user details
User can procede to use the locker system
Access to the locker is denied

It is worth noting that a user lookup is always performed at AD even if the user is already known in ONARKEN®. This means Active Directory maintains control of the user and if the user is removed or blocked at Active Directory the corresponding ONARKEN® user is automatically blocked and denied access.

LapSafe® Active Directory Integration Configuration

The series of pictures below depict the configuration options available under the LDAP Active Directory integration.

The configuration screen allows you to specify which integration method to use, and in the case of User Lookup, which attribute is used for the user ID.



LDAP Active Directory

Microsoft Active Directory Integration with LDAP

LDAP Configuration

Integration Mode*

● Cards Stored in Active Directory

This integration type will look in your Active Directory for the user's scanned card number to authenticate the user.

○ Self Registration

When card numbers are not stored in your Active Directory the "Self-Registration" will ask users to enter their Active Directory username and password on the installation screen to register.

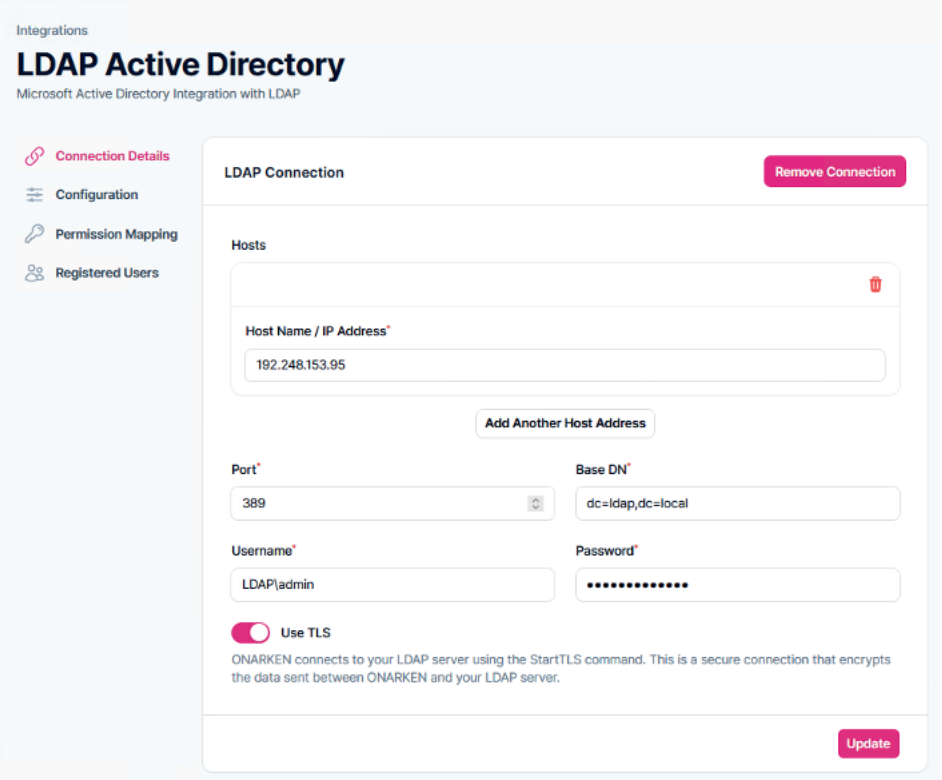
Card Number Attribute

Pager

Cost Code Attribute

The attribute in your LDAP server that contains the cost code for the user. This is used to determine which cost code to assign to a user when they scan their card. If you do not wish to use cost codes, leave this field blank.

The Connection Details screen allows you to specify the connection details to the Active Directory. Note that TLS is recommended when connecting to the Active Directory.



LDAP Active Directory

Microsoft Active Directory Integration with LDAP

LDAP Connection

Hosts

Host Name / IP Address*: 192.248.153.95

Port*: 389

Base DN*: dc=ldap,dc=local

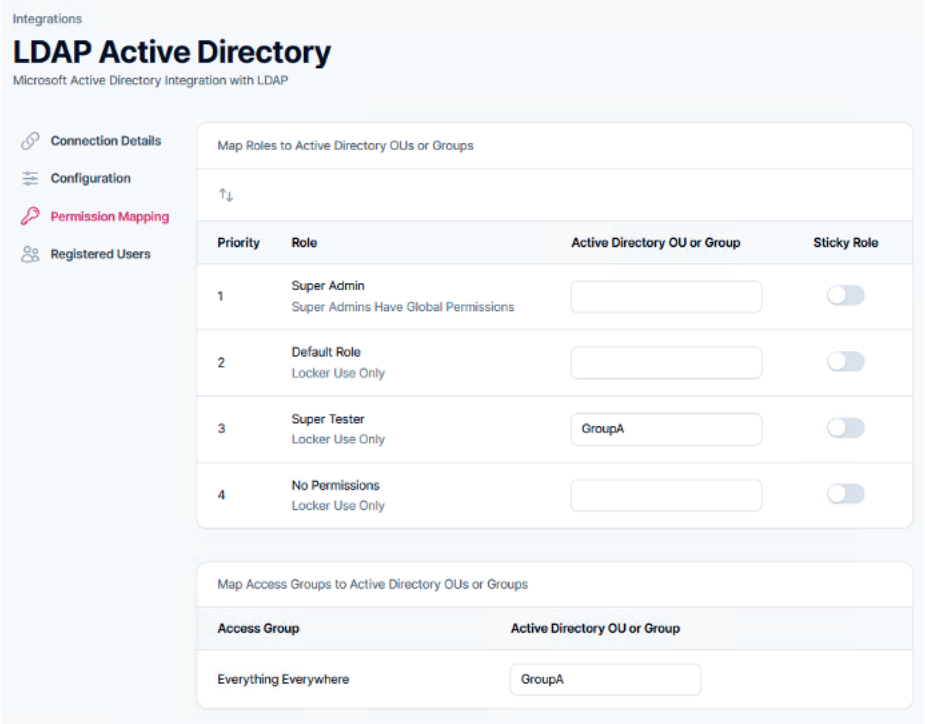
Username*: LDAP\admin

Password*: ••••••••••••••

Use TLS: on

ONARKEN connects to your LDAP server using the StartTLS command. This is a secure connection that encrypts the data sent between ONARKEN and your LDAP server.

The Permissions Mapping screen allows you to specify the user role and access group according to the user groups or OUs the AD user belong to.



LDAP Active Directory

Microsoft Active Directory Integration with LDAP

Map Roles to Active Directory OUs or Groups

Priority	Role	Active Directory OU or Group	Sticky Role
1	Super Admin Super Admins Have Global Permissions		○
2	Default Role Locker Use Only		○
3	Super Tester Locker Use Only	GroupA	○
4	No Permissions Locker Use Only		○

Map Access Groups to Active Directory OUs or Groups

Access Group	Active Directory OU or Group
Everything Everywhere	GroupA

Under The Hood

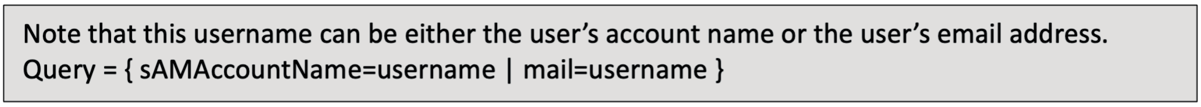
The Active Directory Integration connects to the Active Directory database and query for the user. Depending on the integration method different user credentials are needed.

AD User Lookup

In AD user lookup, only the AD admin's username and password are used. The integration connects to AD using the admin username and password, a query is then constructed using the specified attribute for the user ID. If the user ID is found, then the user attributes are retrieved to check the validity of the user. If the user is valid then an ONARKEN® user is created. If the ONARKEN® user already exists, then the user permissions are updated according to the user's attributes.

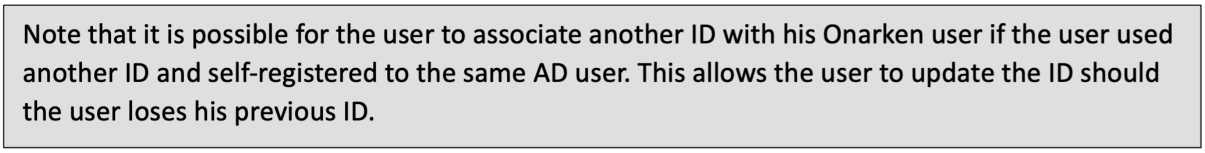
AD User Self-Registration

In AD user self-registration, the AD administrator and the user's username and password are used. The integration connects to AD using the admin's username and password, a query is then constructed using the user's username.



Note that this username can be either the user's account name or the user's email address.
Query = { sAMAccountName=username | mail=username }

Once the user is found and validated, the username and password of the user is used to validate the user with AD. After the user is validated with AD an ONARKEN® user is then created and the ID used is associated with the ONARKEN® user. If the ONARKEN® user already exists, then the user's permissions are updated according to the user's attributes.



Note that it is possible for the user to associate another ID with his Onarken user if the user used another ID and self-registered to the same AD user. This allows the user to update the ID should the user loses his previous ID.

In both integration methods the following list of AD attributes are retrieved from the user:

AD attribute	Description
sAMAccountName	The user’s AD account name
mail	Email address of the user
memberOf	The OUs or groups the user is a member of, used to map to user role and access group.
cn	‘Common name’ for the user, used as the user’s display name.
accountExpires	The user’s account expires date/time.
userAccountControl	Used to check user account, the following conditions are checked. - User account locked - User account diabled - User password expired
logonHours	The permitted logon hours of the user