Author: CE, JTi
Date: 03/2020

Active Directory Integration

EasyOne Connect can use the Active Directory of the customer's organization. This way the User Management system can be centralized within the customer's IT Infrastructure.

1 Prerequisites

The following are prerequisites for making use of the Active Directory Integration:

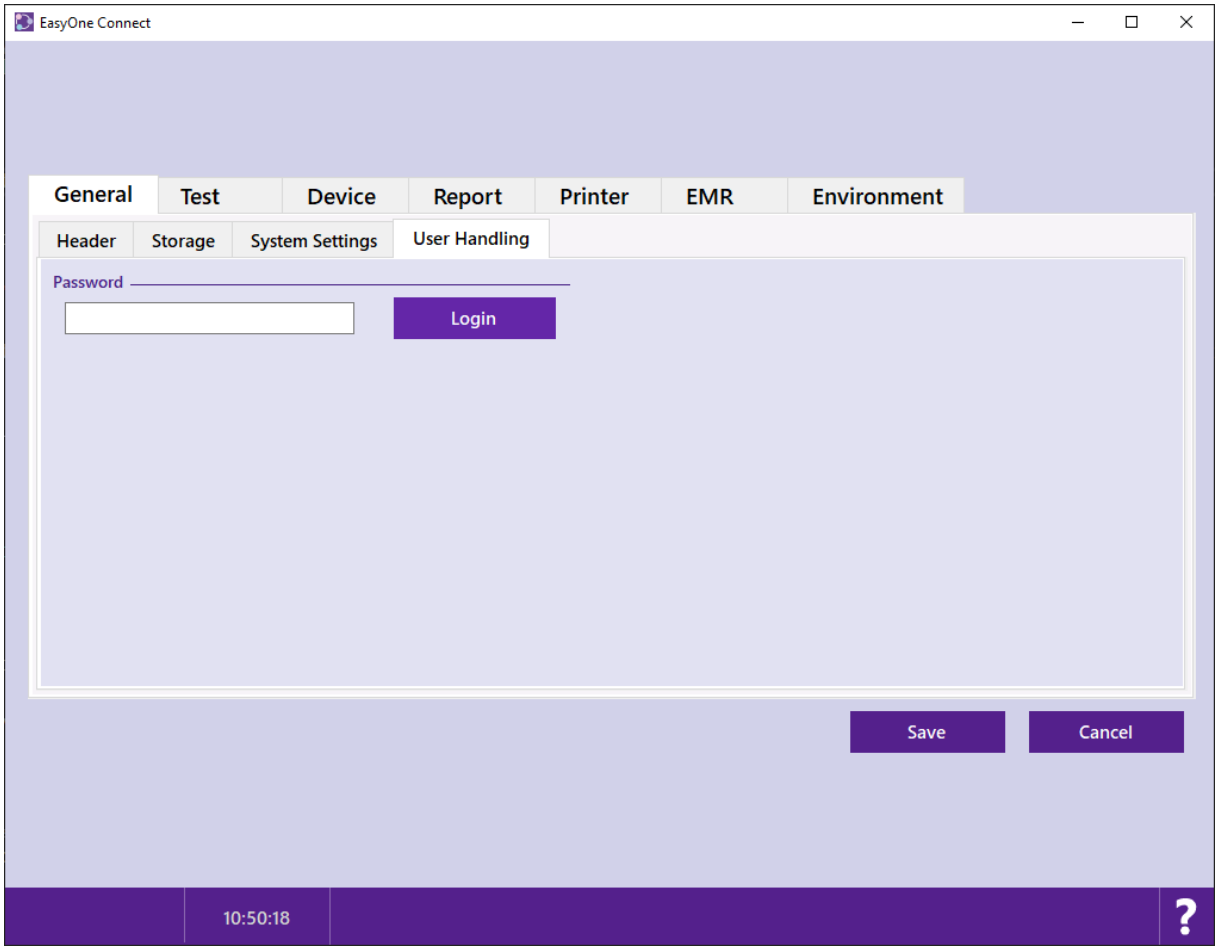
- EasyOne Connect Version 3.7+
- Microsoft Active Directory
- The ability to add/modify security groups in your domain's Active Directory

You will need the IP address or the host name of your LDAP server as well as the ports on which the service is running. Usually this is port 389 and port 636 for SSL. The LDAP Server must be reachable over the LAN/WAN for all clients using the integration.

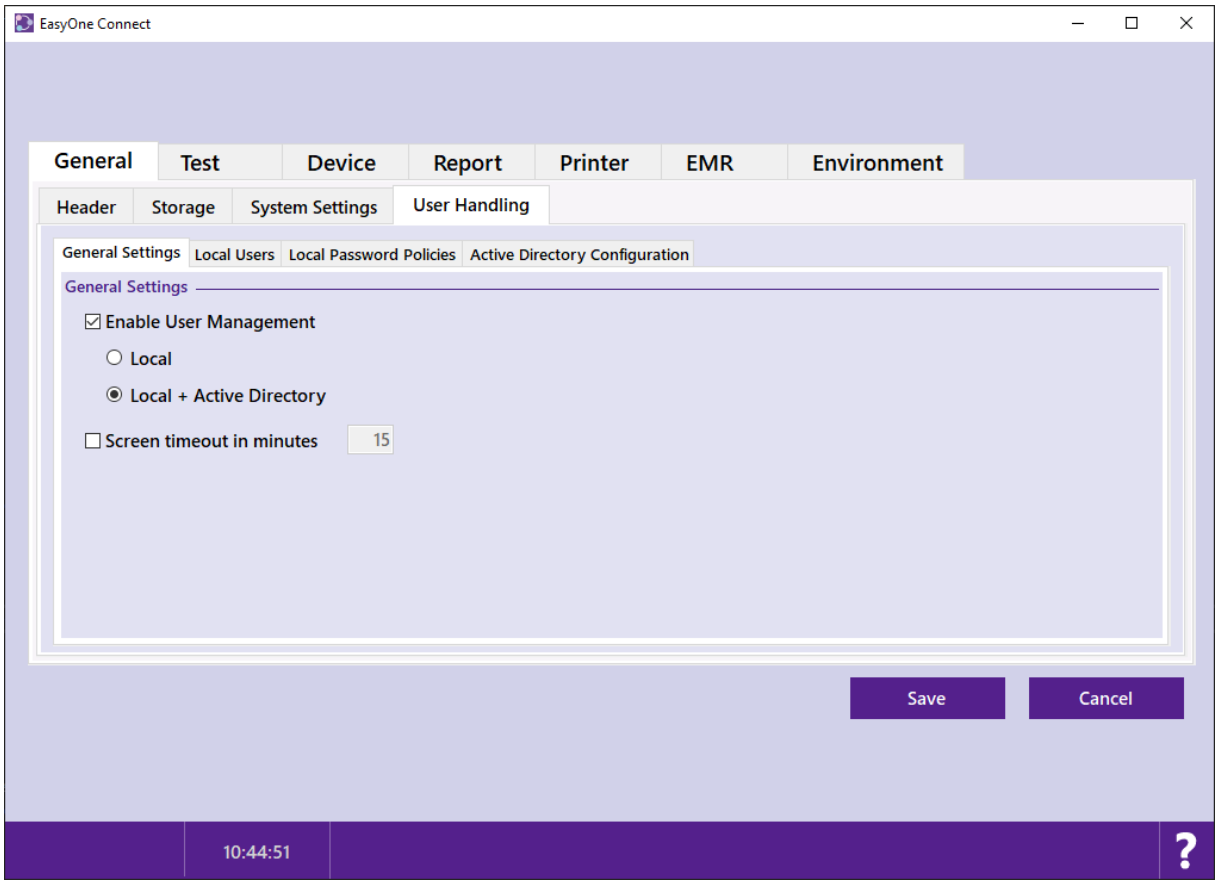
If you plan to run your LDAPS service over SSL/TLS make sure that you have installed a valid Server Certificate on the AD server and enabled it for LDAP(S) as well as enrolled the Trusted Root Certificate to all your clients into the Trusted Root Certificate Authorities. The connection properties are negotiated and will use TLS 1.2 if possible.

2 Setup In EasyOne Connect

In order to setup Active Directory Integration, navigate from the Main Screen to Utilities › Configuration › General › User Handling. You need to enter the admin password from the operator's manual to continue. Note that if you have User Handling already enabled, this password may be different.

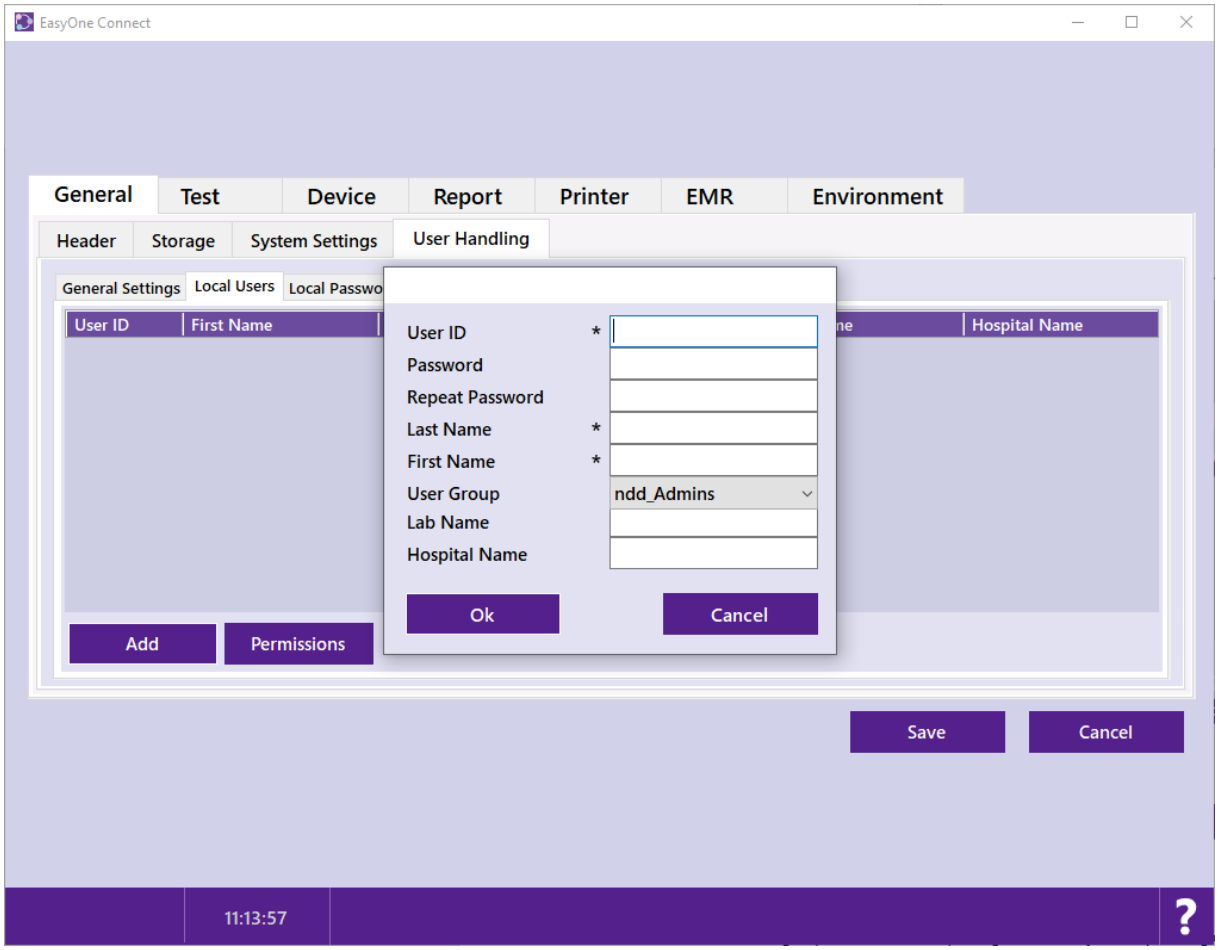


Activate the Enable User Management checkbox and select Local + Active Directory.



2.1 Setting up a Local EOC Admin Account

A local EOC Admin account is needed as an alternative when the LDAP-Service is out of reach or the configuration needs to be changed. To create a new user switch to the “Local Users” tab and click on the “Add” button. A dialog pops up where the local EOC admin account name and password can be entered. It is important to select the ndd_Admins user group.



3 Active Directory Security Groups

The group names in EasyOne Connect are matched one-to-one with the security groups of the Active Directory.

There are two ways to grant access rights to users:

1) The (two) groups from EOC need to be added to the organization's Active Directory and assigned to those users which require access to the EasyOne Connect service.
2) The groups on EOC need to be renamed so they match the names of the security groups on the Active Directory with the corresponding users.

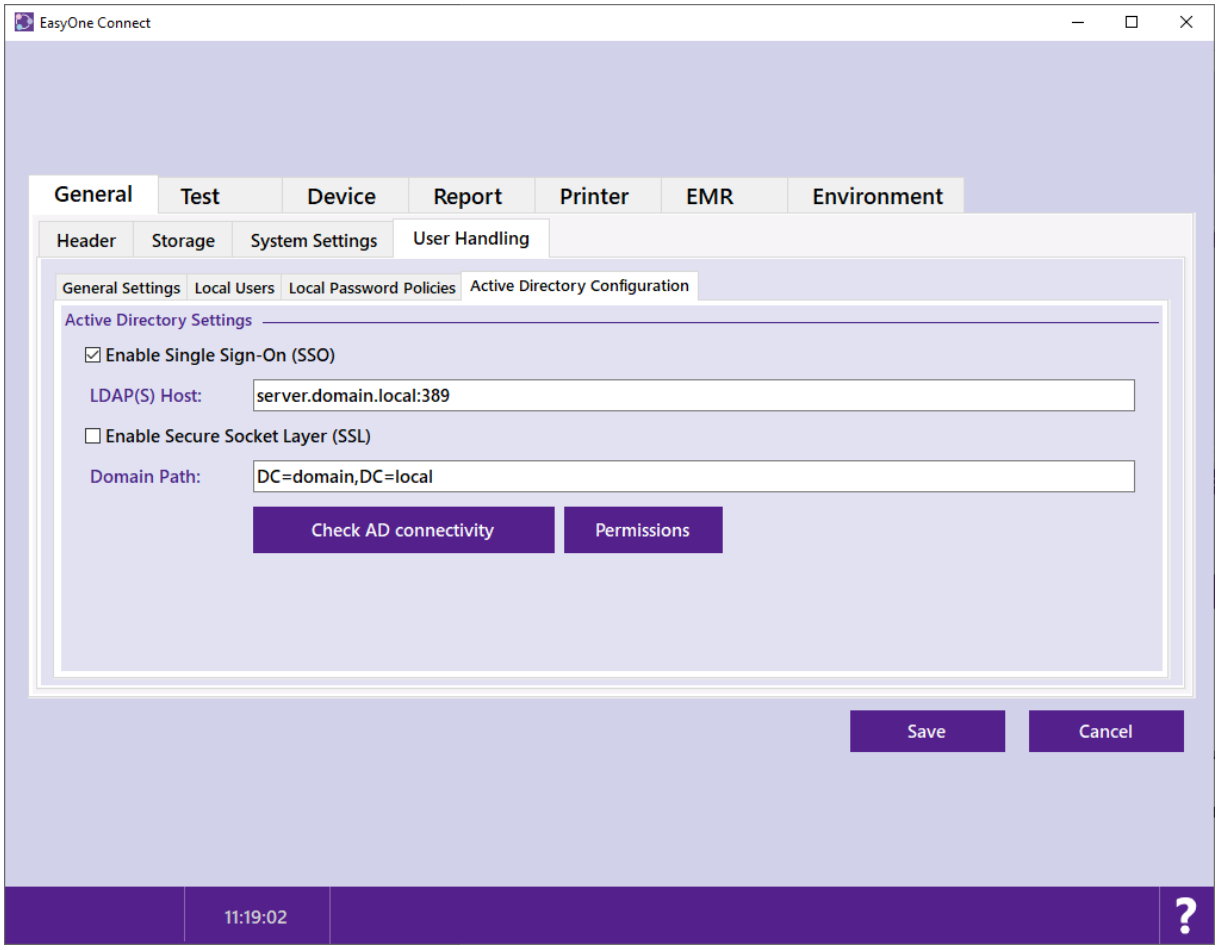
The user group names, and their privileges can be adjusted by clicking on Permissions on either the Local Users tab or on the Active Directory Configuration tab. The default privileges are recommended.

Note: EOC assigns the user to the group they belong to with the highest privileges. For example, if a user belongs to 2 groups, the group with higher privileges (user group level) will be used.

Note: The connection to the LDAP server will be authenticated by the current user's credentials. The required permissions are read-only.

4 Active Directory Configuration

The Active Directory Integration can be configured by switching to the "Active Directory Configuration" tab.



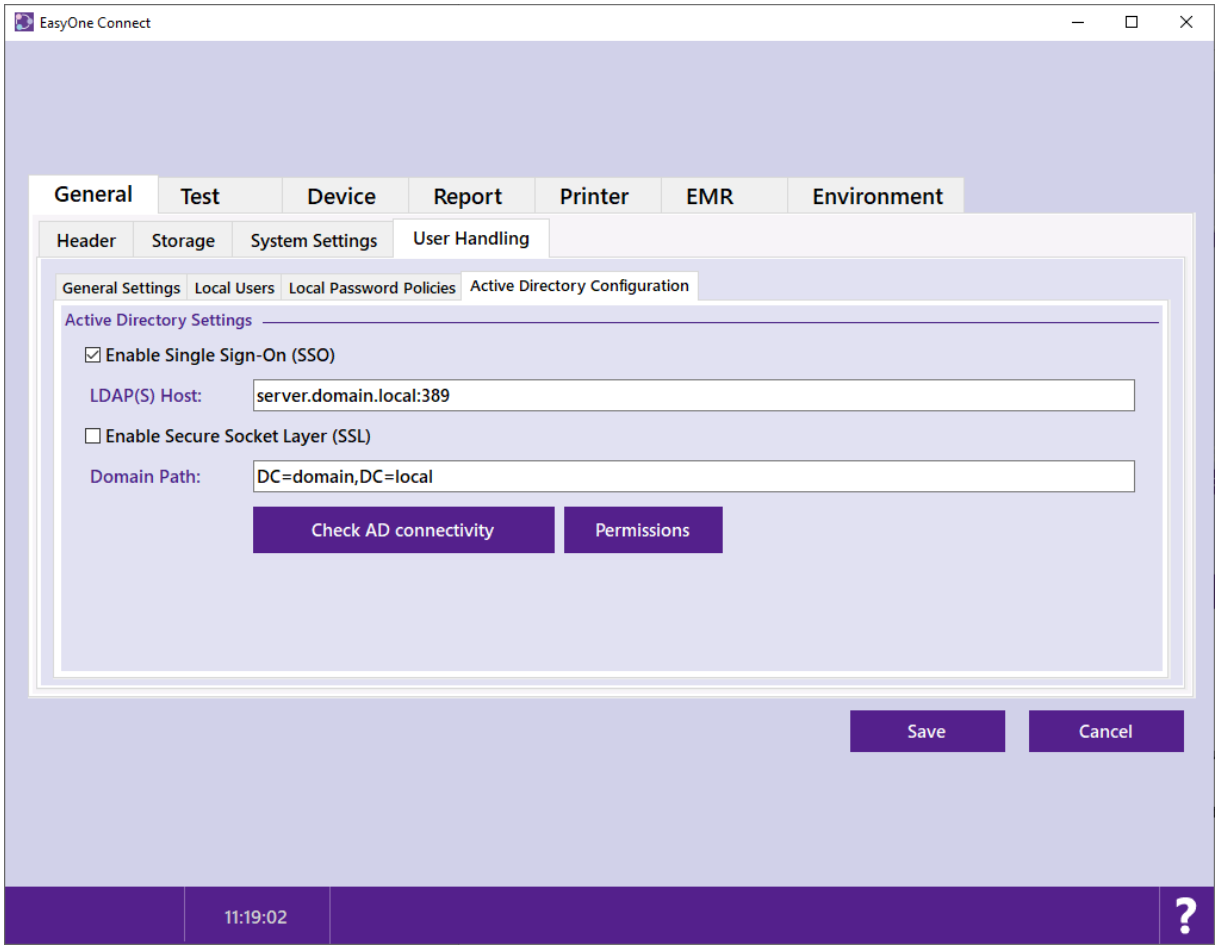
Single Sign-On (SSO) can be enabled. This will use the credentials from the currently logged in Windows user to authenticate against the Active Directory system during application startup. If the Single Sign-On attempt fails, a logon screen will appear instead. This feature is not available for EasyOne Pro and EasyOne Pro LAB due to the fact that the default user accounts on these devices cannot be part of an existing Active Directory.

LDAP(S) Host: The URL of the LDAP-service needs to be specified. The standard port for non-SSL connections is 389 as shown in the example. But this can vary from system to system. If "Enable Secure Socket Layer" is activated, the default SSL-port for LDAP-service is 636, but that can vary from system to system.

Domain Path: The domain path consists of subdomain(s) (optional), domain, and top-level domain from left to right. It is entered as a list of comma-separated Domain Components (DC).

4.1 Check Active Directory Connection

You can test your Active Directory configuration by pressing the “Check AD connectivity” button.



If you are logged in as a local user, you should - at least temporarily - activate “Single Sign-On (SSO)”. This way the client can connect to the LDAP-Service using your Windows Credentials. Otherwise you would need to be already logged in through LDAP-Service.

Note: If you click on save, you will be prompted to log in. Use your local admin account in this case. Or use your windows account, if you have already configured the Active Directory (AD) settings on EOC correctly and provided that the user is existing in the AD and already assign to the correct Security Group with privileges on EOC