Oliver v5 Authentication FAQ's

(Last reviewed: for V5 Build 8.051)

What is authentication?

Authentication is the process of determining if you have access to a system, this is normally done through the use of a username (or user ID) and password. Username and password are often referred to as credentials.

What is Single Sign On (SSO)?

Often abbreviated to SSO, Single Sign On provides the ability to login just once and get access to various systems without being asked to enter username/password again. For example you could login to a domain or your organisation's portal in the morning, then when you navigate to your v5 library system you would find that you were already automatically logged in.

Is LDAP/LDAPS a form of Single Sign On?

No. If your organisation uses LDAP/LDAPS with your v5 library system, users will still need to enter login details into v5, however these will be the same as their network credentials. The benefit of this is that users do not need to remember numerous logins for different systems. Sometimes this is referred to as "Same Sign On".

What do I need to know to pick an authentication method suitable for my organisation?

You must check with your IT representative what technologies you currently use. For example, you may use one of LDAP, LDAPS, Active Directory (AD), NTLM, Kerberos, SAML, OAuth, or something else. You also need to have a clear idea if you want to be automatically signed into all systems after a single logon, or just share the same credentials.

If we use SSO with v5 do we still need to enter our borrowers into v5?

Yes, borrower records are still required to be stored in v5 as these are linked to borrower information such as loans and reservations. Borrowers can be automatically or manually imported from your student administration system or Active Directory using a CSV import. If you prefer, you can also use the v5 Web API to populate borrowers into your v5 library system.

What methods of authentication are available with v5?

Oliver v5 supports LDAP, LDAPS, NTLM, Kerberos, SAML, OAuth, and authentication via URL. A brief summary of these methods is listed below:

Same Sign On	
LDAP	• Authenticate against Active Directory using LDAP only. • Your users will use their network logins to log into v5.
LDAPS	• Authenticate against Active Directory using Secure LDAP only. • Your users will use their network logins to log into v5.

Single Sign On	
LDAP and NTLM 1.0	• Authenticate against Active Directory using NTLM 1.0 and LDAP combined. • Once your users are signed into your network they will be automatically logged into v5.
Kerberos	• Authenticate against Active Directory using Kerberos. This is preferred method over the LDAP / NTLM method (above) as it is more secure. • Once your users are signed into your network they will be automatically logged into v5.
SAML	• Authentication using an existing identity provider (e.g. a portal). (Requires an existing identity provider that supports SAML v2.0.) • Once users are signed into your organisation’s portal they will be automatically logged into v5.
OAuth	• Authentication using your OAuth authentication provider (e.g. Google, Facebook) • v5 supports OAuth 2.0 • Once users are signed into your OAuth authentication provider (e.g. your portal) they will be automatically logged in to v5.
Login via URL	• Authentication occurs by passing login credentials (either encrypted or not) to v5 embedded in a URL which will allow automatic login. • Users will login by clicking a link from another website / intranet page that they are already logged into.

What are the advantages and disadvantages of each of the available authentication methods?

Each method of authentication has its own requirements and features. The table below outlines which options are available with which methods:

	Same Sign On	Single Sign On (SSO)	Works with Hosting	Works with Safari / iPads	Works outside network	Additional Module Required
LDAP	✓		✓ [1]	✓	✓	
LDAPS	✓		✓ [2]	✓	✓	
Kerberos		✓	✓ [3]			✓
NTLM with LDAP		✓				
SAML [4]		✓	✓	✓	✓	✓
OAuth		✓	✓	✓	✓	✓
URL Login [5]		✓	✓	✓	✓	

1. LDAP authentication with hosting is available. You must allow inbound traffic from our hosted server to your Active Directory server on the LDAP port (default 389) for this to work.

2. LDAPS authentication with hosting is available. You must allow inbound traffic from our hosted server to your Active Directory server on the LDAPS port (default 636) for this to work.

3. Kerberos authentication will work with hosting but will only be Single Sign On within your network. There are some specific configurations needed on your network to enable this including adding the hosted v5 site in as a local URL in your browser settings.

4. SAML requires an existing identity provider that supports SAML v2.0. Some identity providers require your v5 system to be running with HTTPS.

5. Authentication occurs by passing login credentials (either encrypted or not) to v5 embedded in a URL which will allow automatic login. Some assistance may be required to get this working.

Will we need assistance configuring these authentication methods with v5?

For some methods of authentication, Softlink will need to work with your IT staff to complete configuration. This will need to be provided as an additional service.

How do these authentication methods work with eBooks?

Some eBook providers authenticate with v5 using the SIP2 protocol. This allows users to download eBooks using the same credentials as you use in the library system (Same Sign On). If you are using LDAP/LDAPS to authenticate with your v5 library system, you can use your LDAP/LDAPS credentials to login into your eBook provider. The eZRead module allows the borrowing of eBooks via the v5 interface. This means that if your users are logged into v5, they can borrow eBooks without having to sign in again.

Are there any additional requirements?

Depending on your authentication choice, you may require some additional setup:

- Some SAML implementations may require your v5 site to run on SSL.
- Borrower records are still required to be stored in v5 when using a SSO method. Softlink can assist with the import of your borrower records (either automatic or manual).

What SAML Identity providers are supported?

We are continually adding additional Identity providers to our list of supported services as we discover clients using different providers. Below is a list of SAML Identity Provider services we support, there may be additional services which are not shown below.

- Microsoft ADFS
- Microsoft Azure AD.
- Microsoft Office365.
- OpenAM