

- All methods are secure and data is never extracted from the customer's system.
- With each login, individual user information is passed to us through attributes.
- All user information is encrypted when passed to us.

## Supported Remote Authentication Methods

Remote authentication provides individual user access through a URL unique to each customer. This is done by connecting to the customer's directory and leveraging their server.

- ✓ Single sign-on experience (LDAP same sign-on).
- ✓ Ability to auto-provision user accounts.
- ✓ Location mapping w/automatic updating.
- ✓ Staff/faculty and student flagging.
- ✓ Content sharing through the use of easy links.
- **Azure AD**
  - Customer must have a Microsoft Azure AD subscription.
  - <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-saas-custom-apps>
- **ADFS**
  - Requires customer to have an ADFS server.
- **CAS**
  - Requires customer to have a CAS server.
- **Clever**
  - Customer must have a Clever subscription.
  - Does not provide rostering.
  - To begin the configuration process; locate the Infobase/Hoonuit app in your Clever account and submit your access request.
- **LDAP**
  - Requires customer to have an LDAP server.
- **Shibboleth**
  - Requires customer to have a Shibboleth server.
  - Set-up fee is waived for members of InCommon.

## Other Authentication Methods

- **OpenID Connect**
- **Individual username / password created through user management or providing .csv upload for import**

Further set-up instructions will be provided once the customer has identified the best possible method of authentication.