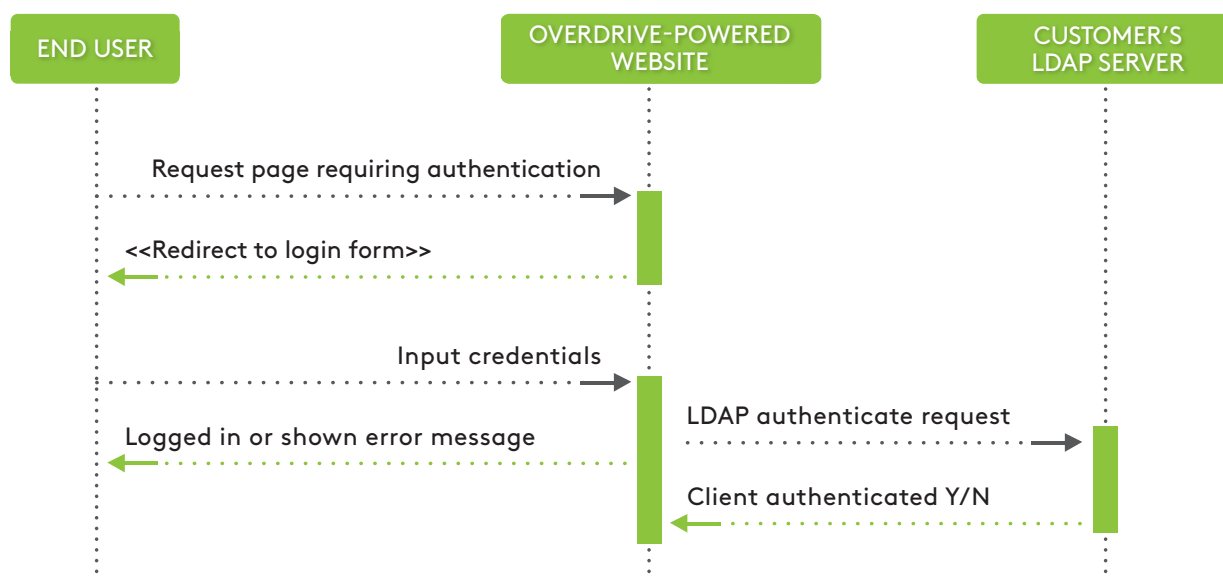# LDAP Authentication Overview

## WHAT IS LDAP?

LDAP (Lightweight Directory Access Protocol) is an Internet protocol that email and other programs use to retrieve information from a server. It is used to look up encryption certificates, points to printers and other services on a network, and provide one password for a user that is shared between many services. LDAP is appropriate for any kind of directory-like information.

## HOW DOES LDAP AUTHENTICATION WORK?

To check out or place a hold on a title, a user will be prompted to sign in to the OverDrive-powered website. OverDrive then connects to the LDAP server either directly or indirectly to verify permitted access to materials. Based on the response, the user can either proceed or they are notified that there is a problem with their account and denied access. Alternatively, the user could be redirected to a website to authenticate and then redirected back to the OverDrive-powered website with a signature to identify and authorize them.

## HOW CAN OVERDRIVE IMPLEMENT LDAP AUTHENTICATION?

The below steps detail LDAP implementation for your OverDrive service.



## DATA PROTECTION

For solutions where OverDrive servers attempt to authenticate users by calling a webservice, the http communication will be made via SSL (https). For direct LDAP integration, "LDAPS" ("Secure LDAP," commonly known as "LDAP over SSL") protocol will be used. Upon request, OverDrive can implement the newer LDAPv3 Transport Layer Security (TLS).

ebooks | audiobooks | streaming video | magazines