# LDAP/Active Directory Setup

Updated Jul 13, 2021

As of July 12, 2021, this "Learn Veracross" site has been deprecated. It will remain live at least through October 1, 2021, but will no longer be updated. All knowledge content has moved to the new Veracross Community. Please update your bookmarks.

Here is the new version of this article in the Veracross Community.

## Overview

Veracross can authenticate with Microsoft's Active Directory server to achieve Single Sign On. Single Sign On allows end users to use their primary network (Active Directory) account to log into Veracross, thus eliminating yet another password. Typically, Active Directory (AD) is for staff, faculty, and student accounts only. Parent accounts often are handled exclusively within Veracross since they typically won't have school network accounts.

The process works as follows:

1. The user attempts to log into Veracross.
2. If the login credentials are successfully authenticated by Veracross (the local security database), the user proceeds as normal.
3. If the login credentials fail, an attempt is made to authenticate against the client's Active Directory server.
4. If the credentials successfully authenticate against the AD server, Veracross' local security database is updated to reflect the new credentials. The most likely cause for this is a user changing a password in Active Directory.

This Veracross integration with Active Directory is really merely a password-synchronization mechanism, since the user's credentials are stored in two places (AD and Veracross). The reason we do not exclusively rely on a client's AD server is that it would create a hard dependency on the client's infrastructure, which if unavailable would prevent access to Veracross.

NOTE: LDAP synchronization does not work at all Veracross login screens**LDAP sync cannot occur at the Admission Portal, Enrollment Portal or Program Registration Portal login pages.** LDAP password synchronization works at the most common places staff or faculty would need to log in:

- https://portals.veracross.com/{school_name}

- https://axiom.veracross.com/{school_name}
- https://family.veracross.com/{school_name}
- … and any of the other major apps such as scheduler, event registration, etc.

### Preparing for Veracross Integration with your Active Directory Server

1. Test that Veracross can connect with your Active Directory server using this tool: **https://accounts.veracross.com/*school_name*/ldap** .Replace *school_name* with your school's short name (same as used in Axiom URLs).
2. Supply us with the Active Directory server information:
    - Fully qualified domain name of the server or IP address (which must resolve to an IP address from outside your network)
    - LDAP server type (Active Directory, Novell, other)
    - School Domain
    - A valid username and password which can be used for testing the connection
3. Make sure port 389 (LDAP) and 636 (LDAPS) are allowed for inbound traffic on your firewall from the following IP addresses:
    - US IP (.com): 54.164.105.59
    - EU IP (.eu): 35.159.44.22
4. Ensure that the Veracross usernames for all relevant users match the corresponding AD account names.
5. Confirm with your Account Manager that Veracross user accounts have been migrated for AD integration.
6. When internal AD integration is verified to be working in step 5, let your Account Manager know so he/she can confirm external (web) AD integration.

### A Note about Client Portal

After Active Directory/LDAP integration has been enabled, Veracross will need to rename any pre-existing Client Portal user account usernames to match the new Active Directory/LDAP usernames. This should be done before further use of the Client Portal.