Eval25 and LDAP

Overview

Students and faculty must log into the Eval25 system to complete evaluations or to view evaluation results and reports. To make the login experience more convenient, Eval25 provides "single sign-on," where one user password is shared among many systems and services, allowing users to log in just one time from one place—such as your school's portal—to access Eval25 and other online services.

Eval25 employs an open, vendor-neutral, industry-standard protocol for single sign-on called "Lightweight Directory Access Protocol," or LDAP. LDAP has a number of uses, but for Eval25 purposes, it is limited to user authentication. The system validates the username and password provided by each user against your school's LDAP directory to ensure that the user is authorized to access the system. It does not, however, check membership in user groups, roles, and so on.

> **Note**
>
> Because the usernames and passwords being validated are managed by your institution, CollegeNET will not be able to assist with user login support (find username, send password reminder, unlock account, and so on).

In This Article:

- Overview
- Implementation Requirements and Considerations
  - CollegeNET LDAP Requirements
  - Specific LDAP Questions for Schools

Implementation Requirements and Considerations

CollegeNET LDAP Requirements

- **Your school's server must interoperate with OpenLDAP**. Active Directory typically allows interoperation after some adjustments have been made on the OpenLDAP side, which CollegeNET has already done to ensure successful LDAP integration for all customers.

- **All remote LDAP servers must support connection via implicit SSL**. CollegeNET's proxy connects to your LDAP servers using SS without issuing a command to start SSL. We do not support explicit SSL connections.

- **All LDAP queries must use suffixes which are unique and easily distinguishable from those of all other clients.**

Domain Name Example	Acceptable Suffix Example	Non-Acceptable Suffix Example

---

collegenetu.edu	dc=cnetu, dc=edu or o=collegenetu	ou=Administrators,ou=TopologyManagement, o=NetscapeRoot

Regarding the non-acceptable suffix example above, it could be made acceptable if changed to:

cn=cnetu CIS EVAL Proxy,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot

Specific LDAP Questions for Schools

To implement LDAP authentication, you must provide CollegeNET answers to the following questions. In addition, you must be able to provide one or more test users we can contact and work with during development.

- What is the root entry of your LDAP directory?
  - **Example**: *uid=username,ou=people,dc=cnetu,dc=edu*
- Are all user accounts under the same node (like an organizational unit in the directory), or are they under different nodes?
- What attribute is used for the DN (distinguished name) of the user entries? (for example, uid)
  - **Example**: *ou=people,dc=cnetu,dc=edu*
- What encryption do you use in your entries?
  - **Example**: *SSHA*
- Can you provide us with a test user or a few test users for development?
- Do you have a password policy that locks out users after a certain number of failed login attempts? If so, how many login attempts can be made before lock out?
- Do you have an account support page (find username, password reset, etc.) that we need to link to if authentication fails
  - **Example**: *https://usersupport.collegenetu.edu*