

VERALAB LDAP Configuration Guide

VeraLab Suite is a client-server application and has two main components: a web-based application and a client software agent.

Web-based application provides access to real-time statistics dashboards, workflow automation functions, reporting, and application administration functions. Once VeraLab server installation is complete you can access a web-based application by opening a browser and navigating to:
`http://yourservername:8080/veralab`



VeraLab Server comes with a built-in Administrator account “admin”. The default password is “password” and we recommend changing it right after the installation.

Client software agent is a client component that does not have any front-end interface. It is designed to monitor client events, such as user log in/out, opening/closing applications, responding to server commands. It also allows you to add an authentication layer if your client computers are not using one yet. If you already have MSAD-integrated environment, where users log into Windows using their Active

Directory credentials, VeraLab client will just register end user log in/out events. However, if you have a lab environment open to public, where you do not have any control over who can access computers in your lab, VeraLab LDAP-enabled client brings a solution by adding a custom authentication layer. The only prerequisite to performing such setup is the connectivity from VeraLab Server to LDAP directory server and setting LDAP configuration properties.

This guide will walk you through the steps required to configure VeraLab with LDAP authentication for both web-based interface and client-side authentication.

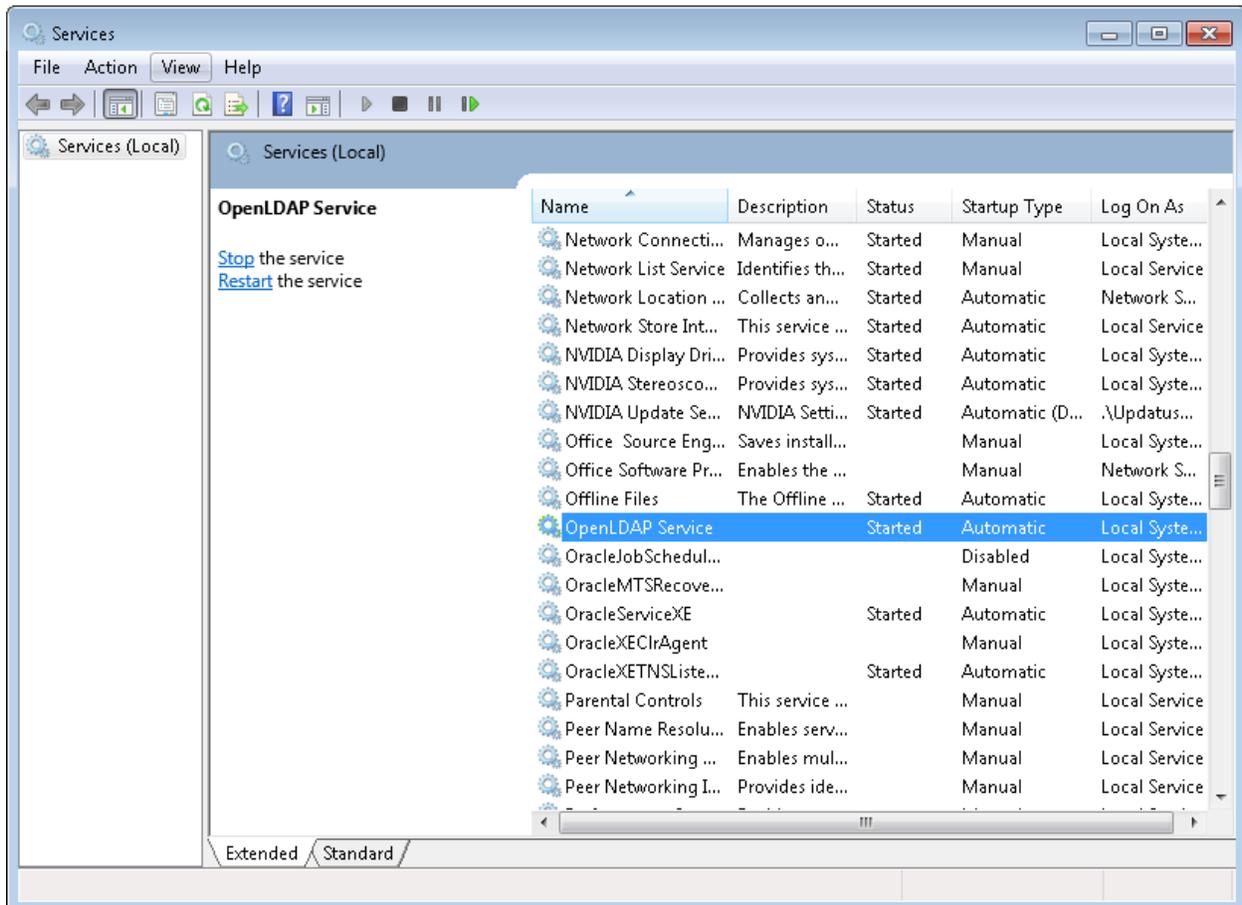
Installing and Configuring OpenLDAP

For Demo purposes we will use Windows-based OpenLDAP software available to download from the Userbooster site: <http://www.userbooster.de/en/download/openldap-for-windows.aspx>

Follow installation instructions from the vendor web site

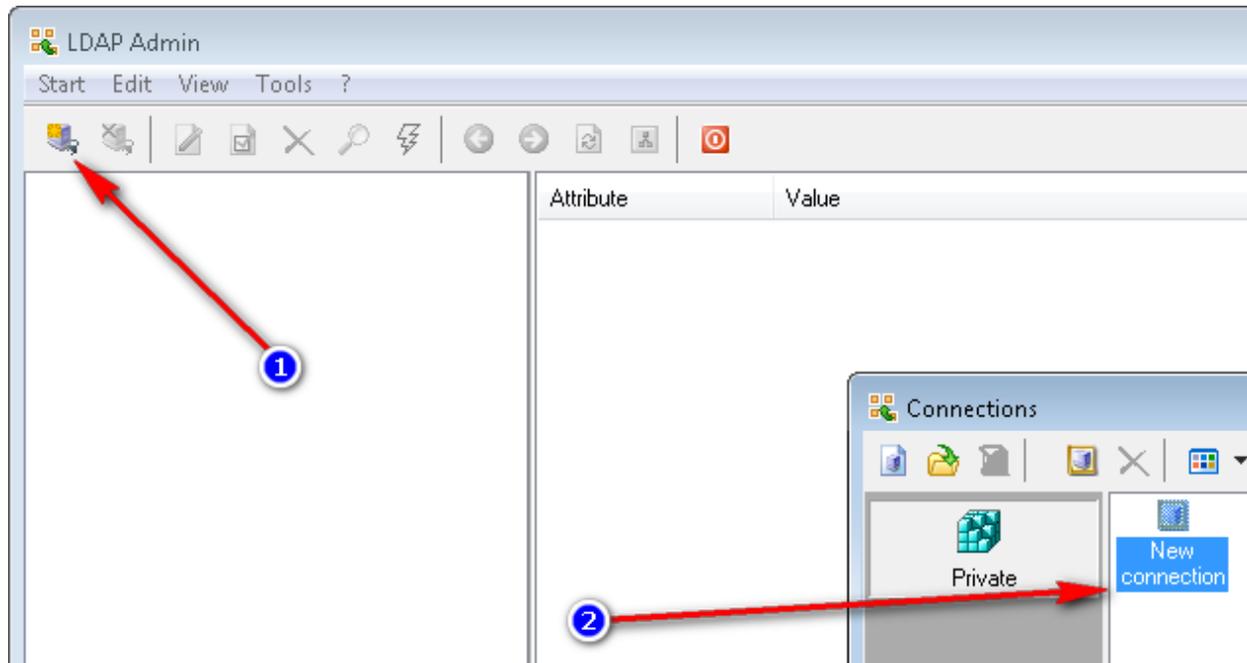
<http://www.userbooster.de/en/support/feature-articles/openldap-for-windows-installation.aspx> or skip this step if you have OpenLDAP directory installed and configured on your site.

You can use all defaults mentioned in the installation guide above. Once installation is complete, you can verify OpenLDAP service is up and running:



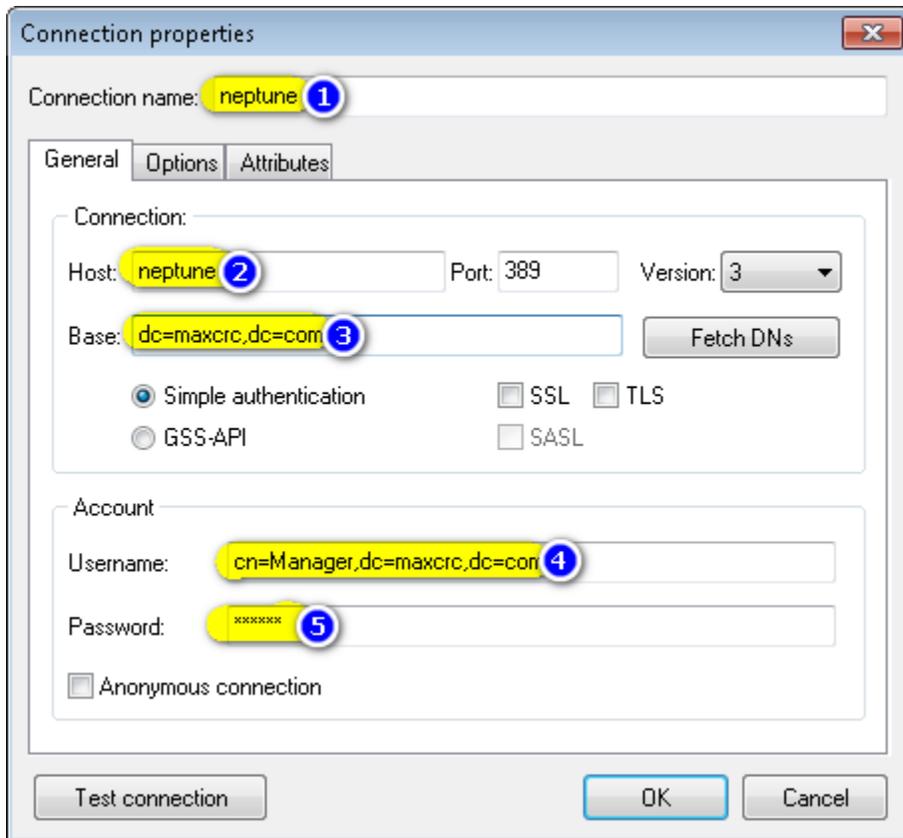
We will use LDAP Admin client tool to add/modify user accounts in OpenLDAP directory. This tool is available for download here: <http://ldapadmin.org/download/ldapadmin.html>

1. Create new connection to OpenLDAP server you just installed. Click on Connect -> New Connection Icon

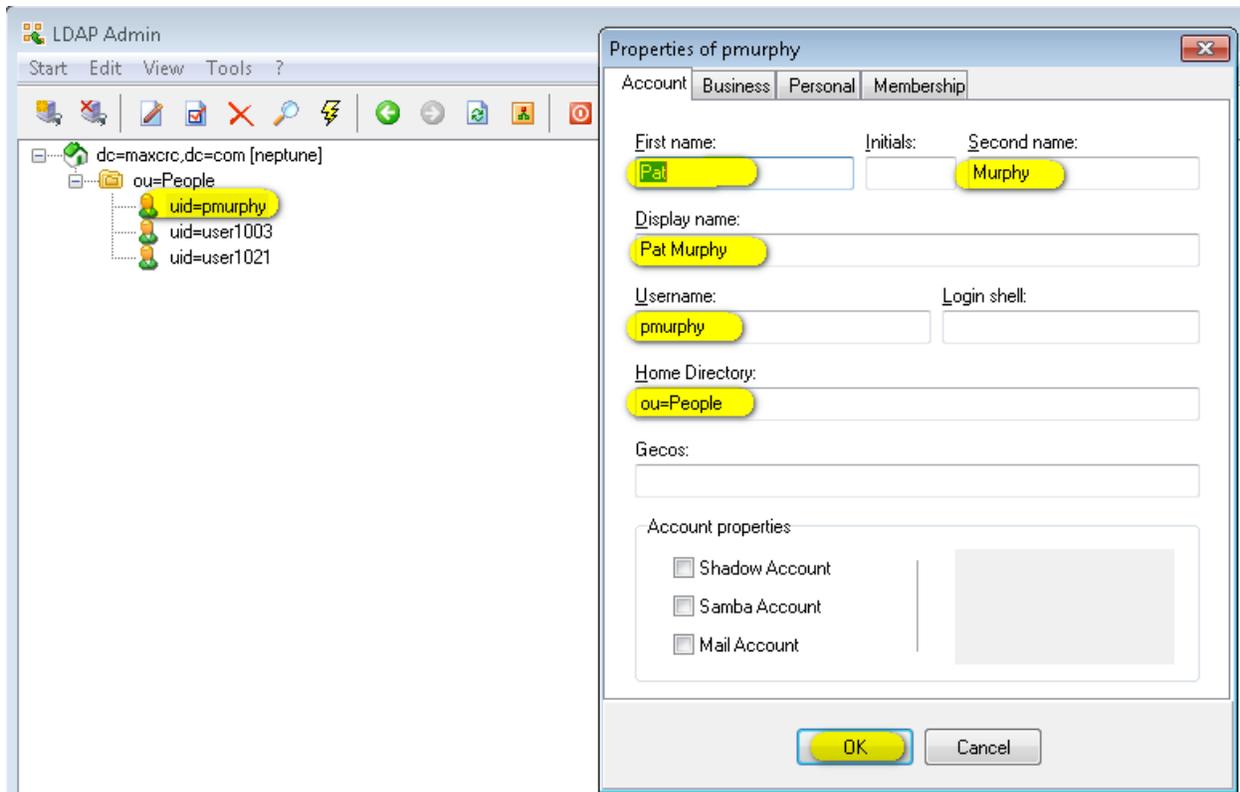


2. Enter your OpenLDAP server connection details, such as connection name, hostname or IP address. Default admin account that comes with Userbooster OpenLDAP is:

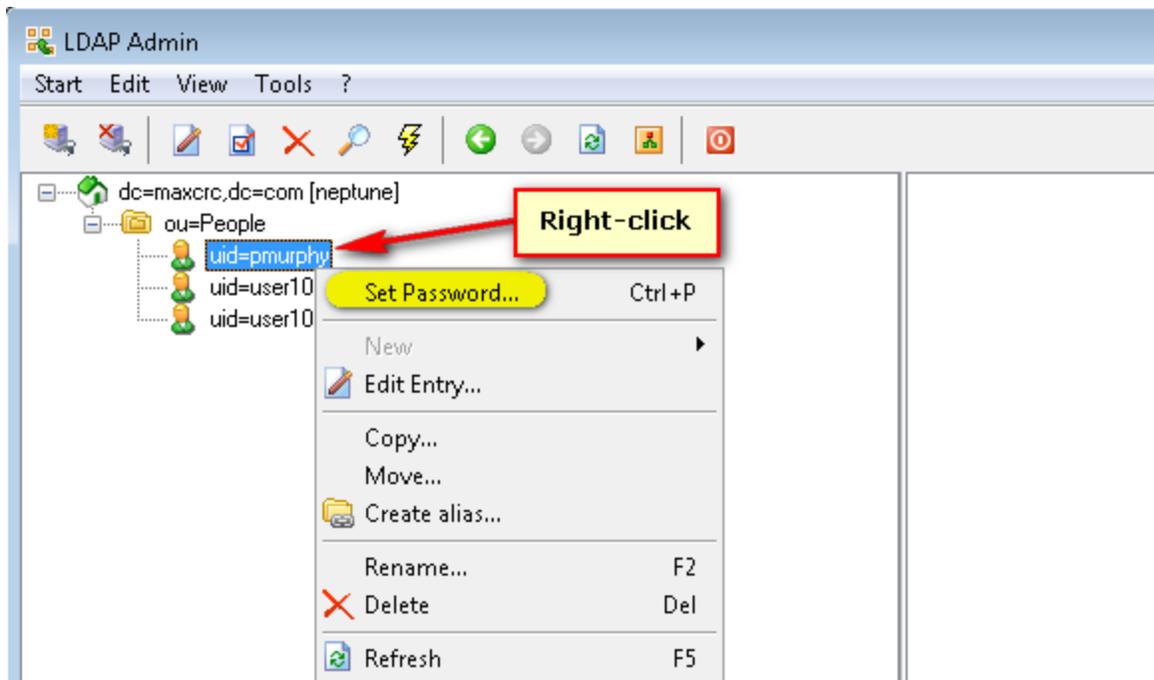
User: `cn=Manager,dc=maxcrc,dc=com`
Password: `secret`



3. Connect to OpenLDAP using newly created connection.
4. OpenLDAP comes with no user accounts (other than built-in Manager). Add few test accounts.



5. Once you add an account, right-click on it and select “Set password” menu option.



Now you are ready to configure VeraLab with OpenLDAP!

Configuring Web-based Application to Use OpenLDAP

1. Login to VeraLab as “admin” user and go to Tools -> Settings. If you have only one LDAP directory and all your user accounts are stored in one single subdirectory, you can re-use “Common LDAP Settings” for client LDAP configuration and for employees web application logins.



2. Click on “Common LDAP Settings” link. Enter LDAP Server URL, path to the directory where user accounts are stored, user unique identifier attribute (usually it can be uid, cn, or sAMAccountName. LDAP Lookup account must have read permissions to search and retrieve account attributes from the user directory container. After testing and verifying connection to LDAP, click on Save button.

Common LDAP Settings

Server URL
Use ldap://ldap_server_host:port format where ldap_server_host is your LDAP server FQDN or IP address

Search Path
Enter user Base DN. Use LDAP Data Interchange Format (LDIF) syntax for the entries, e.g. OU=People,DC=example,DC=edu

User ID Attribute
LDAP attribute that should be used to find the user and is most commonly specified as uid, cn, or sAMAccountName.

LDAP Lookup User DN
e.g. CN=lookupadmin,OU=Service Accounts,DC=example,DC=edu
or lookupadmin@example.edu for MSAD

LDAP Lookup User Password
LDAP Lookup Account will be used to search through LDAP directory accounts when authentication or other operations such as retrieving additional account attributes is required. Lookup Account must have read permissions on LDAP containers you want to search. Leave this field blank if LDAP is setup for anonymous access. When setting up connection to Microsoft Active Directory server user principal name can be used. For all other LDAP servers please use full User DN.

3. To enable LDAP Authentication for Employees, go to Setup -> Users. If you installed VeraLab with the demo data you will see many seeded accounts. If you installed without the demo data, you will see only one "Admin" account record. These are all so called Native accounts at this moment.

Employee Administration

[+ Add Employee](#) [+ Provision LDAP Users](#) [+ Manage Employee Groups](#)

Username	Last Name	First Name	Primary Role	Active	Type	Employee Group	Access to Dashboards	Edit	Delete
Admin	Veralab	Administrator	Administrator	Yes	Native		All counters		
user1003	Smith	John1003	Lab Assistant	No	Native		All counters		
user1021	Smith	John1021	Lab Assistant	No	Native		All counters		
user1025	Smith	John1025	Lab Assistant	No	Native		All counters		
user1028	Smith	John1028	Lab Assistant	Yes	Native		All counters		
user1065	Smith	John1065	Lab Assistant	No	Native		All counters		
user1106	Smith	John1106	Lab Assistant	No	Native		All counters		

- Click on “Provision LDAP Users” link and click on the “LDAP Settings” link.

Provision LDAP Users

[LDAP Settings](#) [Back to Employee Administration](#)

Username First Name Last Name

- You can select “Inherit from Common Settings” option or “Do not inherit...” to override common settings with new values.

Browser address bar: http://127.0.0.1:8080/veralab/LdapSettingsAction.do?current_task_id=1

Page Title: LDAP Settings for Employee provisioning

Welcome Administrator Veralab | Student Portal | Help & Links | Profile | Log Out

Navigation: Setup | Shift Board | Lab Control | Manager Board | Licenses | Reports | Issues | Student Portal | Tools

LDAP Settings for Employee provisioning

Provision LDAP Users

Inherit from Common Settings Do not inherit from Common Settings

Server URL
 Use ldap://ldap_server_host:port format where ldap_server_host is your LDAP server FQDN or IP address

Search Path
 Enter user Base DN. Use LDAP Data Interchange Format (LDIF) syntax for the entries, e.g. OU=People,DC=example,DC=edu

User ID Attribute
 LDAP attribute that should be used to find the user and is most commonly specified as uid, cn, or sAMAccountName.

LDAP Lookup User DN
 e.g. CN=lookupadmin,OU=Service Accounts,DC=example,DC=edu
 or lookupadmin@example.edu for MSAD

LDAP Lookup User Password

LDAP Lookup Account will be used to search through LDAP directory accounts when authentication or other operations such as retrieving additional account attributes is required. Lookup Account must have read permissions on LDAP containers you want to search. Leave this field blank if LDAP is setup for anonymous access. When setting up connection to Microsoft Active Directory server user principal name can be used. For all other LDAP servers please use full User DN.

- Second option (“Do not inherit from Common Settings”) is needed if you use a different LDAP server or directory container for employee records. If you made any changes, click on Test Connection button, enter any valid account credentials and verify that test connection is successful.

LDAP Settings for Employee provisioning

Provision LDAP Users

Inherit from Common Settings **Modify**

Do not inherit from Common Settings

Server URL
 Use ldap://ldap_server_host:port format where ldap_server_host is your LDAP server FQDN or IP address

Search Path
 Enter user Base DN. Use LDAP Data Interchange Format (LDIF) syntax for the entries, e.g. OU=People,DC=example,DC=edu

User ID Attribute
 LDAP attribute that should be used to find the user and is most commonly specified as uid, cn, or sAMAccountName.

LDAP Lookup User DN
 e.g. CN=lookupadmin,dc=example,dc=com or lookupadmin,dc=example,dc=com

LDAP Lookup User Password

LDAP Lookup Account will be used to search through LDAP directory accounts when authentication or other operations such as retrieving additional account attributes is required. Lookup Account must have read permissions on LDAP containers you want to search. Leave this field blank if LDAP is setup for anonymous access. When setting up connection to Microsoft Active Directory server user principal name can be used. For all other LDAP servers please use full User DN.

Test Connection

Username ②

Password ③

Connection test may take few seconds depending on your network and LDAP server configuration. Please wait for confirmation or error message to come back.

Test ④ **Close**

Message from webpage

⚠ Authentication succeeded!

OK ⑤

Save **Cancel** **Test Connection** ①

7. Click Save and return back to “Provision LDAP Users” screen.

LDAP Settings for Employee provisioning

LDAP settings has been successfully saved

Provision LDAP Users

Inherit from Common Settings **Modify**

Do not inherit from Common Settings

Server URL
 Use ldap://ldap_server_host:port format where ldap_server_host is your LDAP server FQDN or IP address

Search Path
 Enter user Base DN. Use LDAP Data Interchange Format (LDIF) syntax for the entries, e.g. OU=People,DC=example,DC=edu

User ID Attribute
 LDAP attribute that should be used to find the user and is most commonly specified as uid, cn, or sAMAccountName.

8. Enter username or first name or last name in the search criteria and click “Search LDAP” button. If a user record is found you will see it in result set. To provision the user, click “Provision” button.

The screenshot shows a web browser window with the URL `http://127.0.0.1:8080/veralab/EmployeeProvisionAction.do`. The page title is "Provision LDAP Users". The browser's address bar and menu bar are visible. The page header includes the Veralab logo and navigation links: "Welcome Administrator Veralab", "Student Portal", "Help & Links", "Profile", and "Log Out". A secondary navigation bar contains "Setup", "Shift Board", "Lab Control", "Manager Board", "Licenses", "Reports", "Issues", "Student Portal", and "Tools".

The main content area is titled "Provision LDAP Users" and includes links for "LDAP Settings" and "Back to Employee Administration". Below these links are three input fields: "Username" (containing "pmurphy"), "First Name", and "Last Name". A "Search LDAP" button is located to the right of the input fields. A table below the search fields displays the search results:

Username	First Name	Last Name	Provision
pmurphy	Pat	Murphy	Provision

9. A new page will open and you will need to fill out required fields and assign roles and other permissions to the newly created user.

Browser: http://127.0.0.1:8080/veralab/EmployeeAction.do?current_task_id=1&action_command=new_form_command&username=

Page Title: Add New Employee

Navigation: File Edit View Favorites Tools Help

VERALAB

Welcome Administrator Veralab | Student Portal | Help & Links | Profile

Setup | Shift Board | Lab Control | Manager Board | Licenses | Reports | Issues | Student Portal

Add New Employee

Employee type: LDAP

Username: pmurphy Active

First Name: Pat Last Name: Murphy

Email: pmurphy@veralab.edu Phone:

Start Date:

Skillset (max. 255 chars):

Hourly employee, will show in payroll report Pay Rate: 15

Pay Rate Effective: 01-Aug-2014

Roles **Primary Role**

Administrator

Lab Assistant

Supervisor

Manager

Technician

License Administrator

10. New user will appear in the list of Employees and type of account will be "LDAP".

Browser: http://127.0.0.1:8080/veralab/EmployeeAction.do

Page Title: Employee Administration

VERALAB

Welcome Administrator Veralab | Student Portal | Help & Links | Profile | Log Out

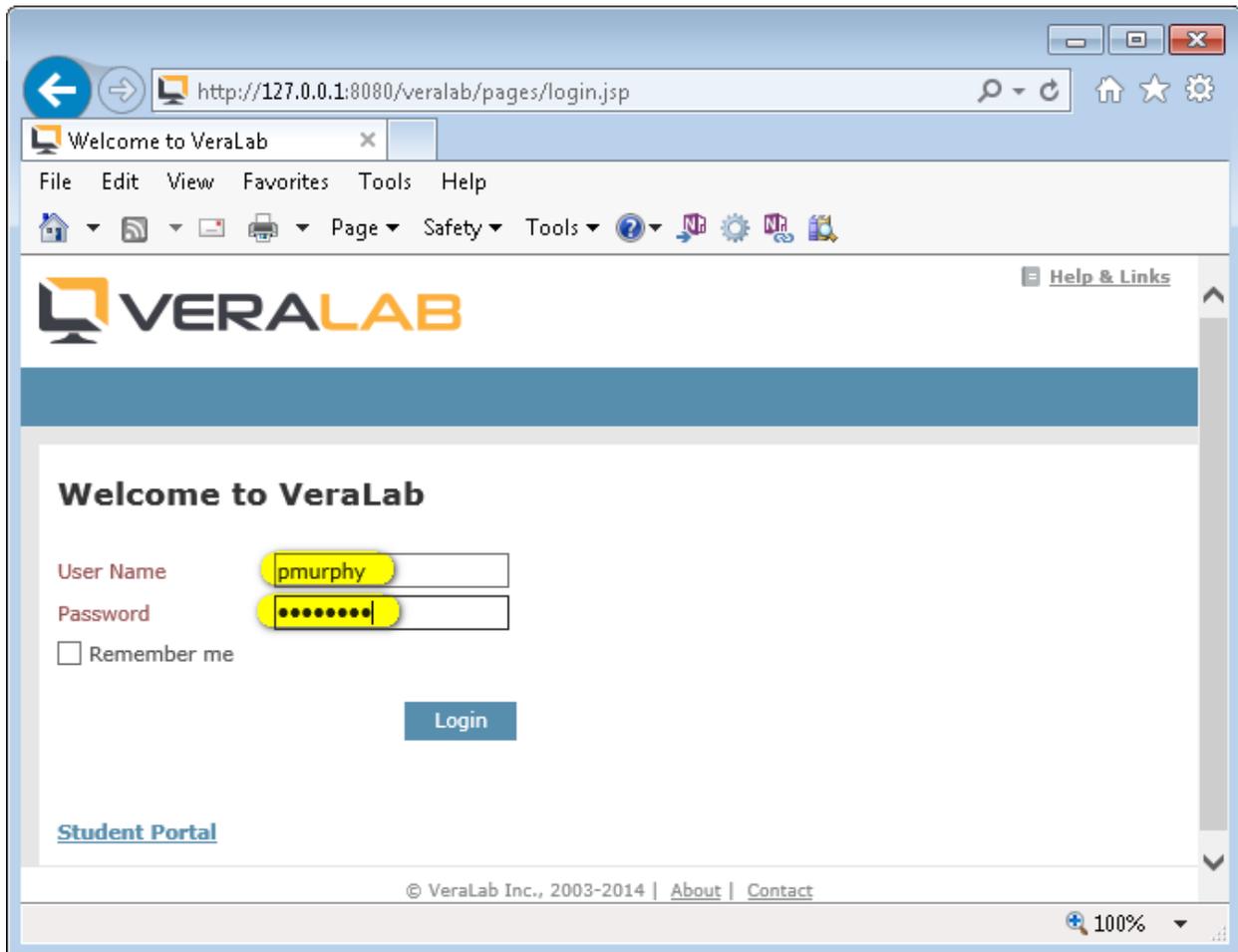
Setup | Shift Board | Lab Control | Manager Board | Licenses | Reports | Issues | Student Portal | Tools

Employee Administration

+ Add Employee | Provision LDAP Users | Manage Employee Groups

Username	Last Name	First Name	Primary Role	Active	Type	Employee Group	Access to Dashboards	Edit	Delete
Admin	Veralab	Administrator	Administrator	Yes	Native		All counters		
pmurphy	Murphy	Pat	Lab Assistant	Yes	LDAP		All counters		
user1003	Smith	John1003	Lab Assistant	No	Native		All counters		

11. Now you can log out and log back in to VeraLab web application using this account and password that was set for that user in OpenLDAP.



12. User landing page will be displayed, e.g. for Lab Assistant role it is "Shift Panel" page.

Shift Panel

Welcome Pat Murphy | Student Portal | Help & Links | Profile | Log Out

Shift Start/End | My Payroll | Check-in Dashboard | Waitlist | Class Registrations | Inventory

Shift Panel

Current Time Is : 02-Aug-2014 10:03 PM

Start Shift | End Shift

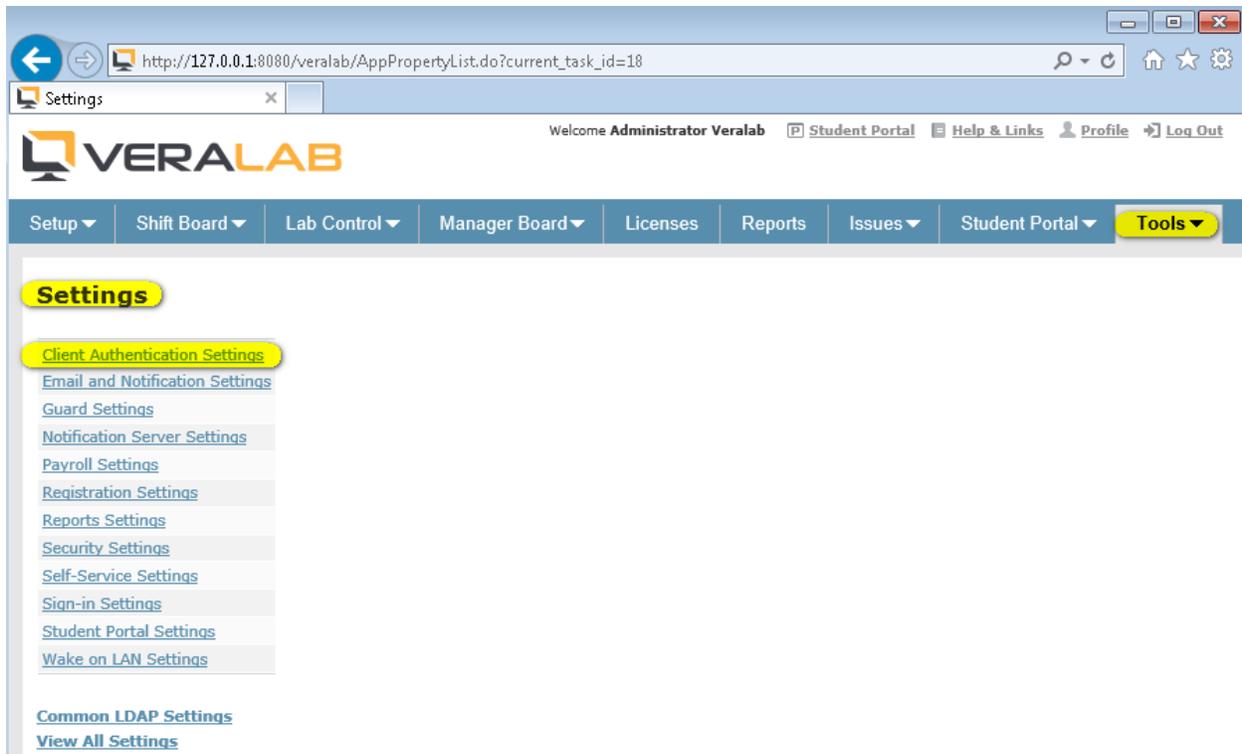
Excel

Current Pay Period Shifts for pmurphy:

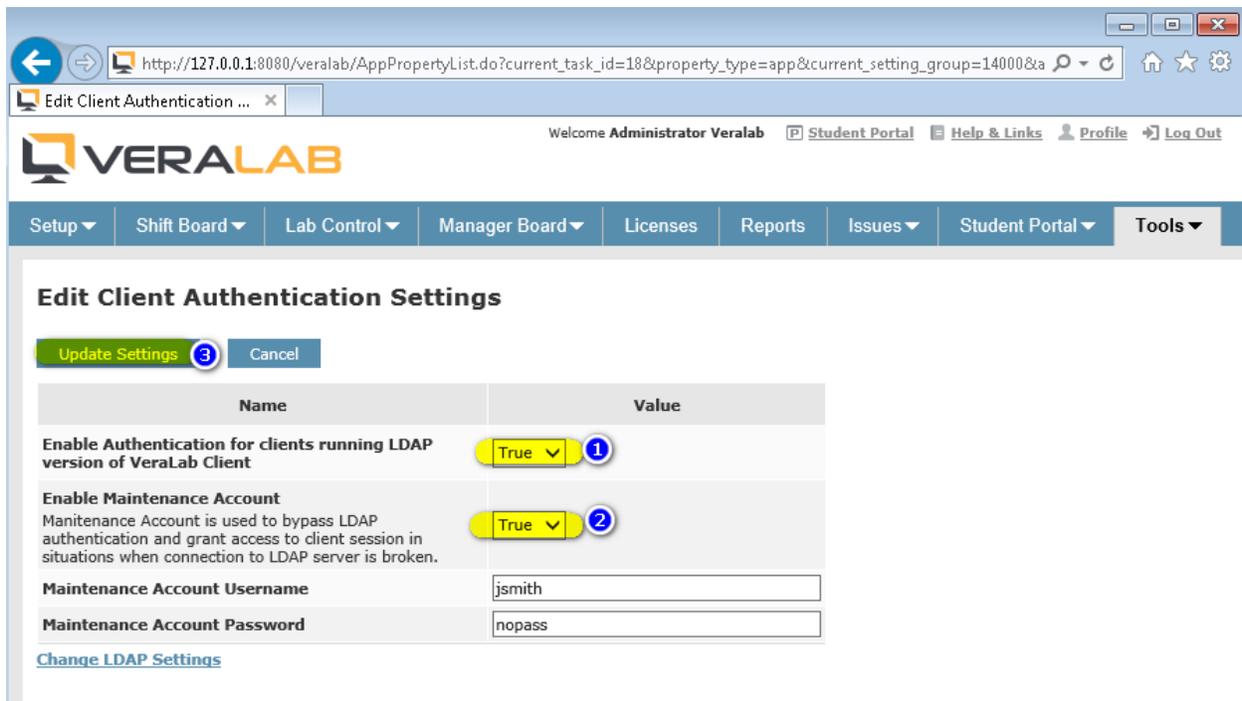
Shift Started	Shift Ended	Total Time	Sign On IP Address
02-Aug-2014 10:03 PM			127.0.0.1
Total		0:00	

Configuring VeraLab Client for LDAP Authentication

1. Enable Windows Automatic logon on Windows clients if not enabled already. You can reference Microsoft article for Windows 7 OS: http://answers.microsoft.com/en-us/windows/forum/windows_7-security/how-to-turn-on-automatic-logon-in-windows-7/99d4fe75-3f22-499b-85fc-c7a2c4f728af
2. Enable LDAP Authentication for client stations by logging into Web Application and going to Tools->Settings-> Client Authentication Settings.



3. Enable client authentication and click on “Update Settings” button.



Note: Maintenance account is used to bypass LDAP authentication when connection to LDAP server is broken or you need to open client screen without LDAP credentials, e.g. for some quick maintenance task.

- To use Common LDAP settings or to make LDAP settings changes, return back to the same screen and click on “Change LDAP Settings” link.

The screenshot shows a web browser window with the URL `http://127.0.0.1:8080/veralab/AppPropertyList.do?current_task_id=18&property_type=app¤t_s`. The browser tab is titled "Edit Client Authentication ...". The page header includes the Veralab logo and the text "Welcome Administrator Veralab" and "Student F". A navigation menu contains links for "Setup", "Shift Board", "Lab Control", "Manager Board", "Licenses", "Reports", and "Iss".

Edit Client Authentication Settings

Update Settings Cancel

Name	Value
Enable Authentication for clients running LDAP version of Veralab Client	True ▾
Enable Maintenance Account Maintenance Account is used to bypass LDAP authentication and grant access to client session in situations when connection to LDAP server is broken.	True ▾
Maintenance Account Username	jsmith
Maintenance Account Password	nopass

Change LDAP Settings

- Select desired option and click Save button.

LDAP Settings for Client Workstations Authentication

Inherit from Common Settings

Do not inherit from Common Settings

Server URL
 Use ldap://ldap_server_host:port format where ldap_server_host is your LDAP server FQDN or IP address

Search Path
 Enter user Base DN. Use LDAP Data Interchange Format (LDIF) syntax for the entries, e.g. OU=People,DC=example,DC=edu

User ID Attribute
 LDAP attribute that should be used to find the user and is most commonly specified as uid, cn, or sAMAccountName.

LDAP Lookup User DN
 e.g. CN=lookupadmin,OU=Service Accounts,DC=example,DC=edu
 or lookupadmin@example.edu for MSAD

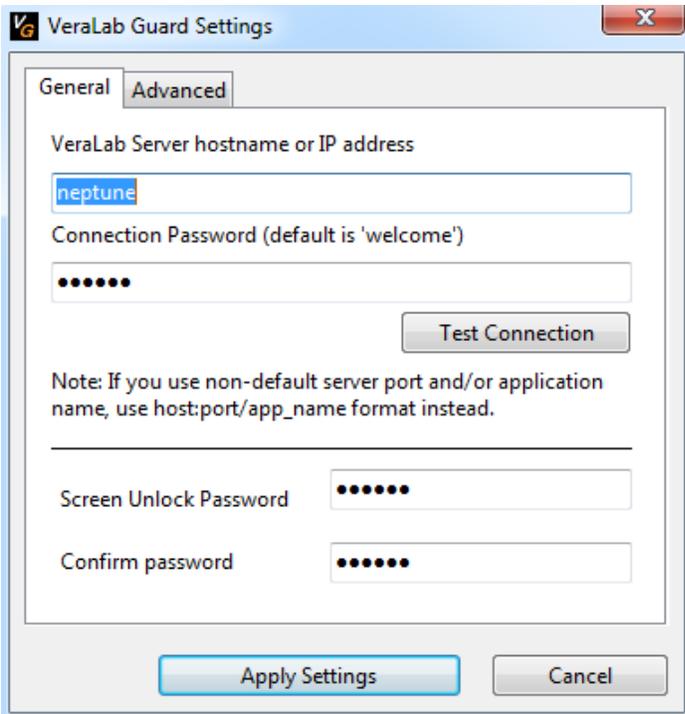
LDAP Lookup User Password

LDAP Lookup Account will be used to search through LDAP directory accounts when authentication or other operations such as retrieving additional account attributes is required. Lookup Account must have read permissions on LDAP containers you want to search. Leave this field blank if LDAP is setup for anonymous access. When setting up connection to Microsoft Active Directory server user principal name can be used. For all other LDAP servers please use full User DN.

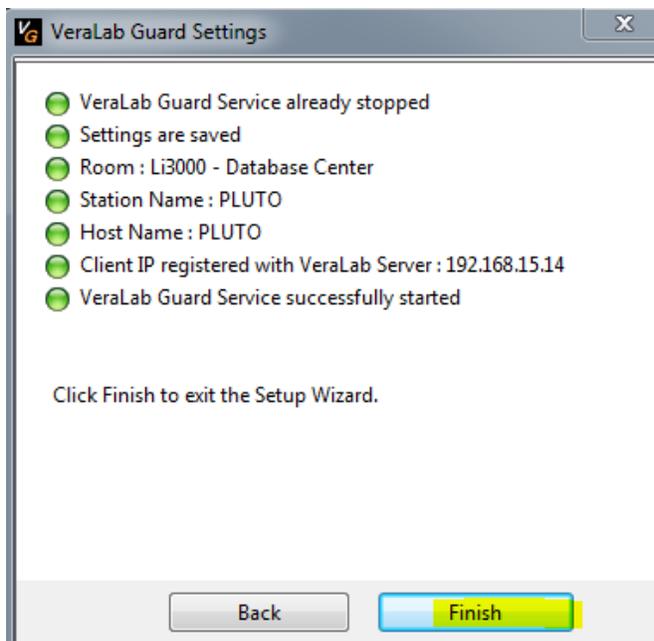
- Download LDAP-enabled client from our web site www.veralab.com. LDAP-enabled client package comes with two files. Open Autologon.ini and enter your local account credentials, same as you used in step 1. Save that file and exit.

```
[autologon]
username=labadmin
password=welcome1
```

- Run exe package. Both files, veralab_cleint_setup_ldap.exe and Autologon.ini, must be in the same directory when you start client installation. You must install VeraLab client as a user with administrator privilege.
- Once installation is done a new window will automatically pop-up where you need to enter VeraLab server connection details, e.g. server name or IP address and Screen Unlock password. Screen unlock password was designed primarily for counter sign on scenarios and is rarely used when LDAP authentication for client stations is enabled.



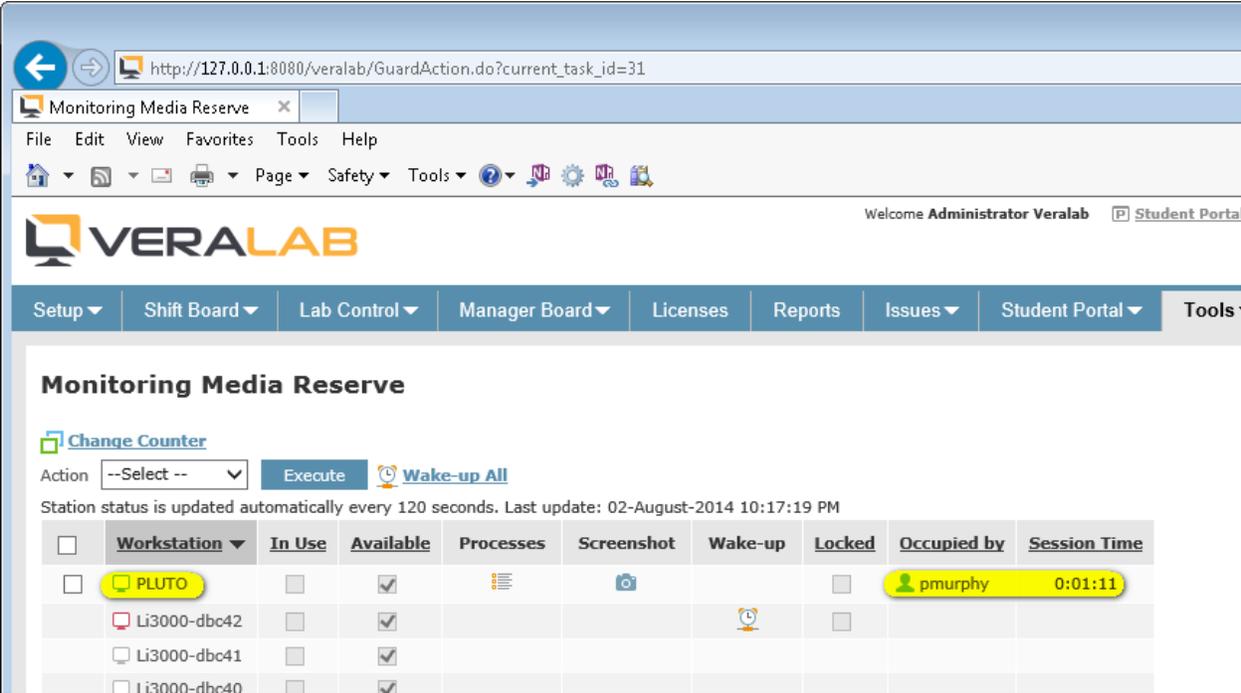
9. Register Client with the server by selecting Room, Model, Image and click Finish. Please refer to VeraLab Administrator's Guide for more information how to setup your VeraLab environment.



10. Now if you logout or reboot your client, you should be able to use LDAP credentials to log on to Windows session. You will be presented with VeraLab custom login screen.



11. You can see client sessions via **Monitoring** page if you login to VeraLab web application and go to Tools->Monitoring.



If you have any questions about LDAP configuration, please contact VeraLab Support:

CONTACT US

 **1-855-VERALAB (1-855-837-2522)**

 Support: support@veralab.com
Sales: sales@veralab.com

 Twitter |  You Tube