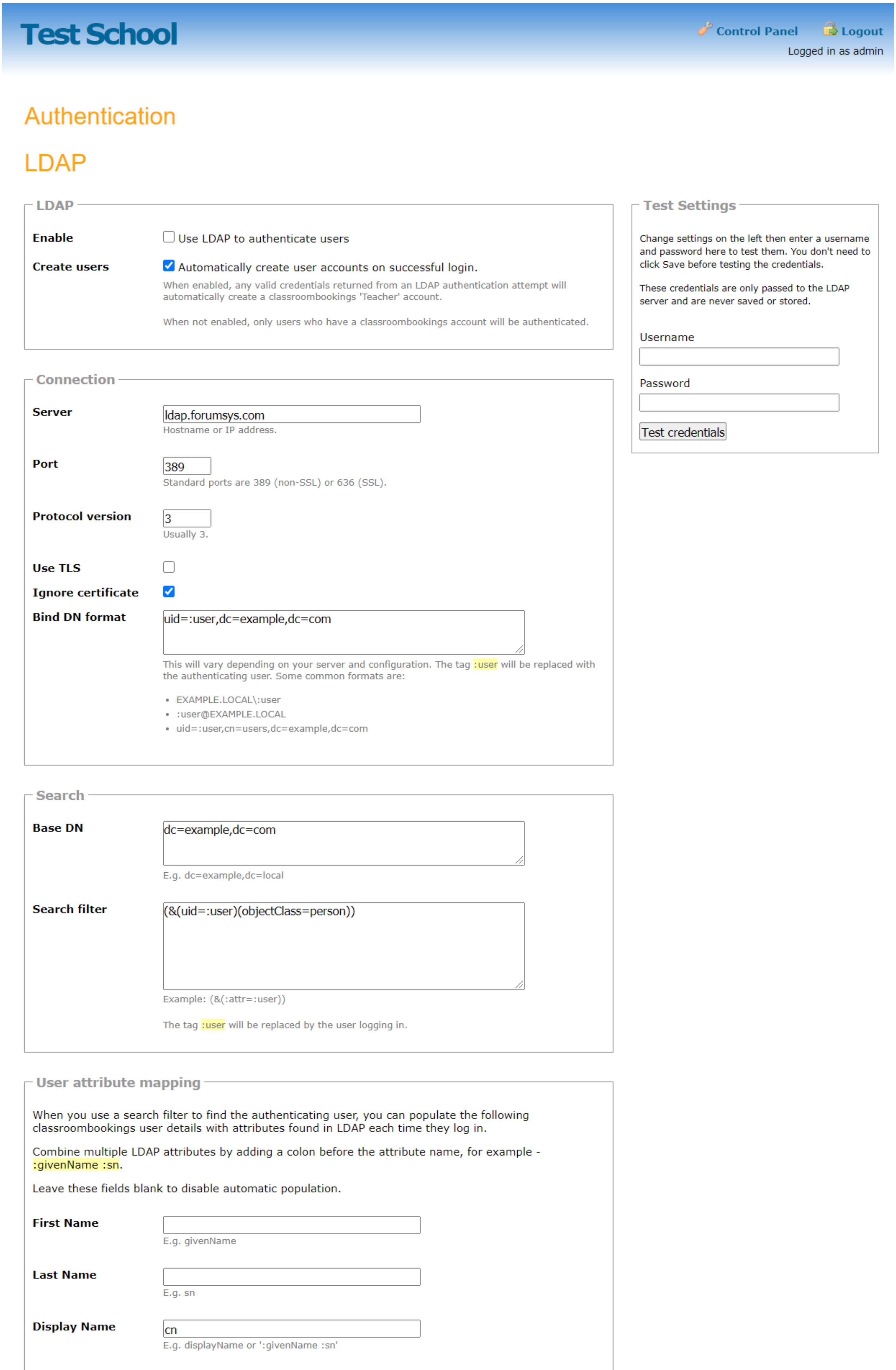
LDAP Authentication

You can use LDAP Authentication to authenticate users against an Active Directory (AD) or LDAP server.

> Support for this functionality requires that the PHP installation has the **ldap** extension enabled.



Authentication

LDAP

LDAP

Enable ☐ Use LDAP to authenticate users

Create users ☑ Automatically create user accounts on successful login.

When enabled, any valid credentials returned from an LDAP authentication attempt will automatically create a classroombookings 'Teacher' account.

When not enabled, only users who have a classroombookings account will be authenticated.

Connection

Server ldap.forumsys.com

Hostname or IP address.

Port 389

Standard ports are 389 (non-SSL) or 636 (SSL).

Protocol version 3

Usually 3.

Use TLS ☐

Ignore certificate ☑

Bind DN format uid=:user,dc=example,dc=com

This will vary depending on your server and configuration. The tag :user will be replaced with the authenticating user. Some common formats are:

- EXAMPLE.LOCAL\:user
- :user@EXAMPLE.LOCAL
- uid=:user,cn=users,dc=example,dc=com

Search

Base DN dc=example,dc=com

E.g. dc=example,dc=local

Search filter (&(uid=:user)(objectClass=person))

Example: (&(:attr=:user))

The tag :user will be replaced by the user logging in.

User attribute mapping

When you use a search filter to find the authenticating user, you can populate the following classroombookings user details with attributes found in LDAP each time they log in.

Combine multiple LDAP attributes by adding a colon before the attribute name, for example - :givenName :sn.

Leave these fields blank to disable automatic population.

First Name

E.g. givenName

Last Name

E.g. sn

Display Name cn

E.g. displayName or ':givenName :sn'

Test Settings

Change settings on the left then enter a username and password here to test them. You don't need to click Save before testing the credentials.

These credentials are only passed to the LDAP server and are never saved or stored.

Username

Password

You can choose to have classroombookings automatically create accounts upon successful authentication with the server, or only allow access to accounts that already exist.

When LDAP is enabled and a user successfully logs in, their password is hashed and stored in the classroombookings database, just like local users. This enables those users to log in even if the LDAP server is temporarily unavailable or the LDAP setting is turned off.

Connection

Firewall

The AD/LDAP server must be accessible over the network from the server that classroombookings is running on. Depending on your setup, this may involve opening and/or forwarding ports on firewalls.

If you are using the hosted cloud service, you will need to allow access to the port from the following IP address:

- `94.237.60.222`.

Server

This is the hostname or IP address of the AD/LDAP server to authenticate with. Currently, only one server is supported.

Port

The port number that the AD/LDAP server is running on.

Protocol version

The protocol version number that the AD/LDAP connection should use.

Use TLS

Specify whether to use TLS for the connection.

Ignore certificate

Choose this option to ignore any certificate errors when using a TLS connection. If you do not use this option, you may need to install and/or accept your AD/LDAP server's certificate on the classroombookings server.

Bind DN Format

Specify the format that the authenticating user will use when attempting to connect to the LDAP server. This will vary depending on your AD/LDAP server configuration and version. The keyword `:user` will be replaced by the username entered by the user.

Common formats are:

- `EXAMPLE.LOCAL\:user`
- `:user@EXAMPLE.LOCAL`
- `uid=:user,cn=users,dc=example,dc=com`

Search

You can specify a search criteria to ensure that the authenticating user matches the given cirteria here.

If you don't use this, any user who successfully authenticates can log in. Most organisations will want to enter a search criteria to ensure only a certain tree or group of users can log in to classroombookings, and deny another set.

Base DN

This is the Base DN that the search will start at.

Search filter

This is the AD/LDAP search filter used to find the user. The keyword `:user` will be replaced by the authenticating username.

Match user with a keyword in their description:

`(&(uid=:user)(description=staff))`

Match user that has an email address AD/LDAP field:

`(&(uid=:user)(|(description=staff)(email=*)))`

Match user that is a member of a given group:

```
(&(uid=:user)(memberof=CN=Teachers,OU=Users,DC=Example,DC=com))
```

You can read more about the LDAP query syntax here: Search Filter Syntax.

User attribute mapping

When you use a search filter to find the authenticating user, you can populate the following classroombookings user profile fields with their attributes found in LDAP each time they log in.

You can combine multiple AD/LDAP attributes by adding a colon before the attribute name, for example - `:givenName :sn`. If you are just specifying a single field, you do not need to include the colon.

If you leave the field blank, classroombookings will not attempt to populate those user details.

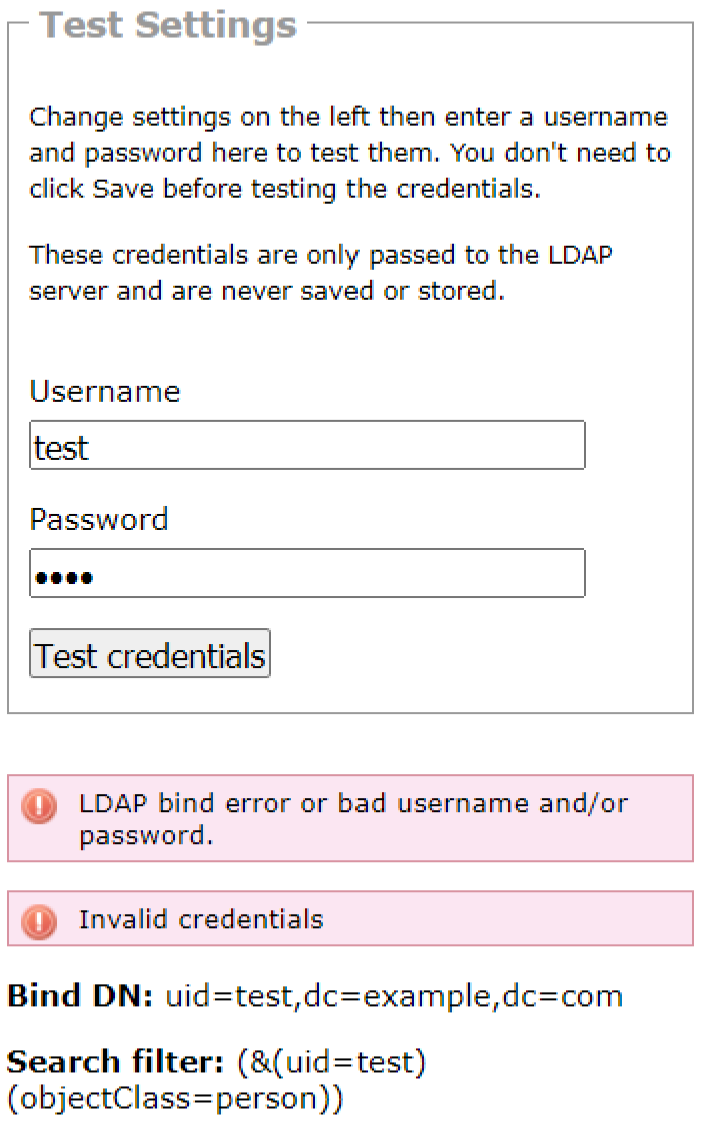
Testing the settings

You can check if the AD/LDAP settings entered on this page will work by using the *Test Settings* box on the right side of the page.

This is useful to test that a connection can be made and only the desired user accounts can successfully authenticate.

The connection settings on the page are used every time you click **Test credentials**, so you don't need to click Save before testing.

Any error or success messages will be displayed under the box.



Change settings on the left then enter a username and password here to test them. You don't need to click Save before testing the credentials.

These credentials are only passed to the LDAP server and are never saved or stored.

Username

test

Password

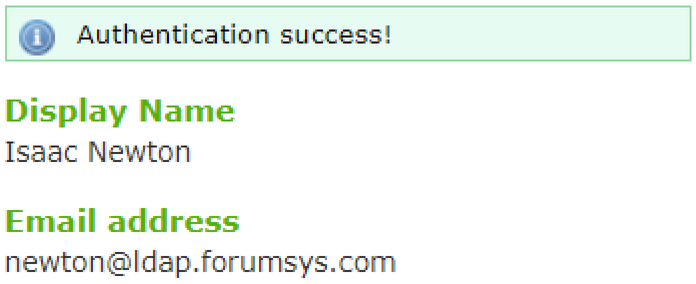
●●●●

LDAP bind error or bad username and/or password.

Invalid credentials

Bind DN: uid=test,dc=example,dc=com

Search filter: (&(uid=test)(objectClass=person))



Authentication success!

Display Name
Isaac Newton

Email address
newton@ldap.forumsys.com

Revision #7

Created Sun, Dec 27, 2020 3:40 PM by Craig Rodway

Updated Fri, Jan 1, 2021 3:34 PM by Craig Rodway