SchoolBooking LDAP Integration Guide

Before you start

This guide has been written to help you configure SchoolBooking to connect to your LDAP server. Please treat this document as a reference guide, your individual network / servers may need to be configured in a different manner than described within this document. You will also notice we use examples referring to Microsoft Active Directory. If you use another LDAP service such as OpenLDAP you may find that some of the wording / functions are slightly different from the guide.

Do not make changes to your network or servers unless you fully understand what you are doing.

Please read this guide thoroughly before trying to configure LDAP on your site.

Introduction

SchoolBooking supports the LDAP Protocol, this means that if your users are stored on a server that supports LDAP (such as a Microsoft Windows Server with Active Directory) SchoolBooking can connect directly to this over the internet.
By using an LDAP link to your server it is then possible for users logging into your SchoolBooking site to authenticate with your own server rather than setting up accounts on the SchoolBooking server.

There are many advantages for this method of access, two of the main ones being that users only need to remember their network username and password to gain access and very little user maintenance required by an admin.

The disadvantage is if your server or the connection goes down, your LDAP users will not be able to access the booking service, although local SchoolBooking users will still be able to connect.

Getting Started

You will need some knowledge of LDAP before being able to configure the settings within SchoolBooking. We strongly recommend you use a LDAP client tool to test your LDAP connection to your server both internally and then externally before trying to configure SchoolBooking to access your server. An LDAP client tool is likely to offer more detailed error messages whilst testing.
There are quite a few different products available for testing LDAP; a tool we recommend is Softerra LDAP Browser for Windows, this can be downloaded from http://www.ldapbrowser.com

Last updated 05-11-2017 MDB

There are plenty of other LDAP tools available for all major platforms; it's worth browsing Google for "LDAP test tool".

Technical overview

Protocols

SchoolBooking can support the use of both LDAP and LDAPS Protocol.
The LDAP protocol will send data in plain text to between the servers on port 389.
The LDAPS Protocol (known as secure LDAP) offers a layer of encryption, and operates on port 636.
It is up to you which protocol you use, however for testing we suggest you start with LDAP as it is much easier to setup as active Directory Servers are LDAP ready. Once you have a working LDAP connection we then recommend moving over to an LDAPS connection which offers better protection against network sniffing. LDAPS requires some additional configuration on your server including publishing security certificates. This level of instruction is outside of the scope of this document as different servers and situations would require different configuration. To find out more about LDAPS search for "LDAPS setup" from Google.

Firewall

As SchoolBooking is a cloud service, it will need to connect to your server through the internet. You will need to open the LDAP or LDAPS port to enable the SchoolBooking server to see your LDAP Server.
You will need to control who has access to this port, otherwise you will leave yourself open to possible misuse and security vulnerabilities from the outside world. We suggest that you only allow services that you trust to query to your server LDAP port.

To allow SchoolBooking to query your LDAP server you will need to create a firewall rule for your LDAP / LDAPS ports to allow communication to and from your LDAP server.

IP Addresses	Resolvable by A Record		
109.228.13.204	auth1.schoolbooking.com	< --------- > Ports 389 and/or 636	Your LDAP Servers External IP
109.228.58.225	auth2.schoolbooking.com		
77.68.90.197	auth3.schoolbooking.com		
77.68.89.113	auth4.schoolbooking.com		

Note that All IP's or A Records listed above will need to be allowed to talk with your LDAP server as we load balance requests between multiple servers during busy periods and at times of server maintenance.

What SchoolBooking needs to know

Before proceeding you should work these settings out by using the LDAP test tool before entering details into SchoolBooking.

Server Address

This is the address of your server, it needs to start with either LDAP:// or LDAPS:// followed by either an external hostname or an external IP Address.
An example of this address would be: LDAP://mytestserver.mydomain.com.

Base DN including users

A Base DN is the top level of the LDAP directory tree. A minimum example of a Base DN would probably look something like:-
DC=school, DC=test, DC=server, DC=sch, DC=uk

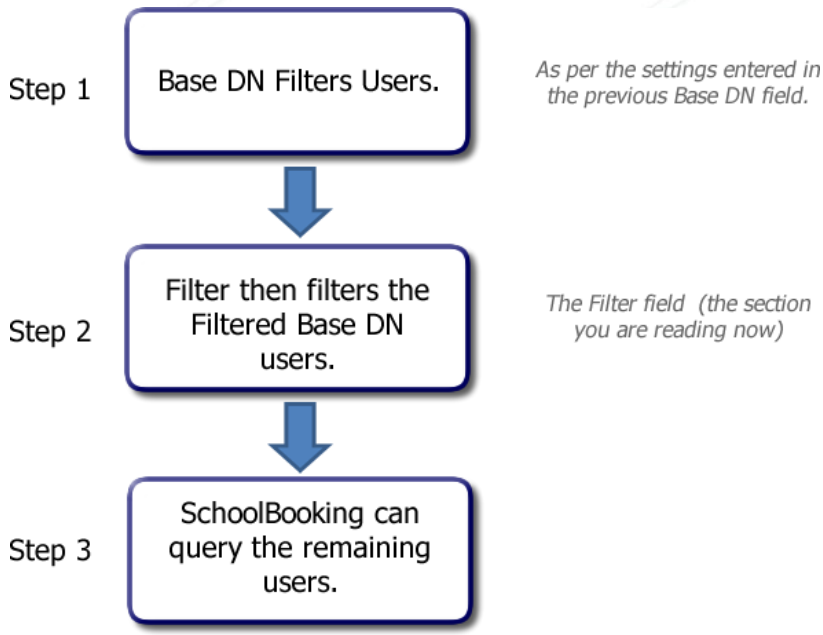
Again you will need to find these settings out using the LDAP client previously mentioned in the "Getting Started" section.
If you use active directory, it is likely that your users will be held in an Organisation unit (it looks like a folder) We suggest you also include a path to your users Organisational Unit within your Base DN as it will increase performance when SchoolBooking authenticates, and can also allow you to include / exclude users from accessing SchoolBooking.
If you specify a particular Organisational Unit, only users within that Organisational Unit and any child Organisational Unit will be seen by SchoolBooking.
For our example, if my server had an Organisational Unit named "my users" with a child Organisational Unit named "staff", the path I would specify would be:
OU=staff, OU= my users, DC=school, DC=test, DC=server, DC=sch, DC=uk
Note that OU = Organisational Unit.

Watch out for the default "users" folder on Active Directory!
A standard Active Directory installation has a "users" folder within the root/base of active directory. It looks like an Organisational Unit but is instead a Common Name. If we tried to specify it in the above example it would fail, instead we need to reference it using the CN abbreviation and not an OU abbreviation, See the example below.

CN= users, DC=school, DC=test, DC=server, DC=sch, DC=uk.

Filter

We have already looked at ways of filtering out users to increase performance and limit users by specifying Organisational Units within the Base DN. The filter field will filter whatever is left after Base DN has done its job.
For SchoolBooking to know what to look for, we have to write a filter. It is worth Googling, but as an example the following filter would allow all users within your specified Base DN. :-
(&(objectCategory=person)(objectClass=user))
Note: - if you leave the filter field blank the above bare minimum filter will automatically be applied.



Example of the Filter Process

There are more powerful filters you can easily implement, one of which is the use of Active Directory Membership Groups. If you create a new Membership Group in Active Directory called “SchoolBooking” and then assigned that group to a selection of users, SchoolBooking would only allow those selected user’s access. Of course you could do it with an existing group for example if your staff were already allocated a Staff Membership Group, you could specify this.
To create a filter that looks at users with a security group we have to specify the path to the Membership Group, similar to our Base DN example.
For example if our Membership Group was created within the “users” folder we would reference as followed:-
(&(objectCategory=person)(objectClass=user)(memberOf=CN=SchoolBooking,CN=users, DC=test,DC=server))
Note how we have combined the basic filter and added the additional Membership filter to it.

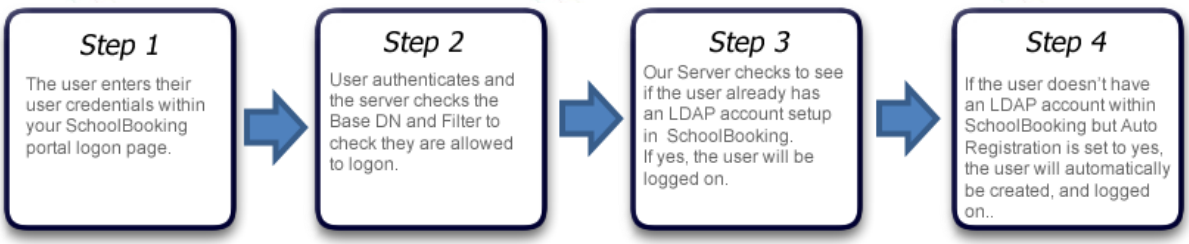
Domain

When a user logs into your network they probably have to specify a domain. On older versions of Windows this was done with a drop down box where the domain could be specified
When your users authenticate with SchoolBooking your server will expect them to provide a domain. So that your users don’t need to provide the domain name along with their username when logging on to SchoolBooking, you need to specify the domain name for them within this Domain field.
If my domain was called testdomain I would simply enter testdomain within the Domain field.

Example of Windows XP Logon Domain (it is harder to view the domain on Windows 10)

Auto Register

Auto register allows SchoolBooking to automatically create accounts as a user’s logon occurs.
As long as you’re Base DN / filter within the previous sections is set correctly you should enable this setting as it cuts out the need for you or the user to manually create / import their user account.

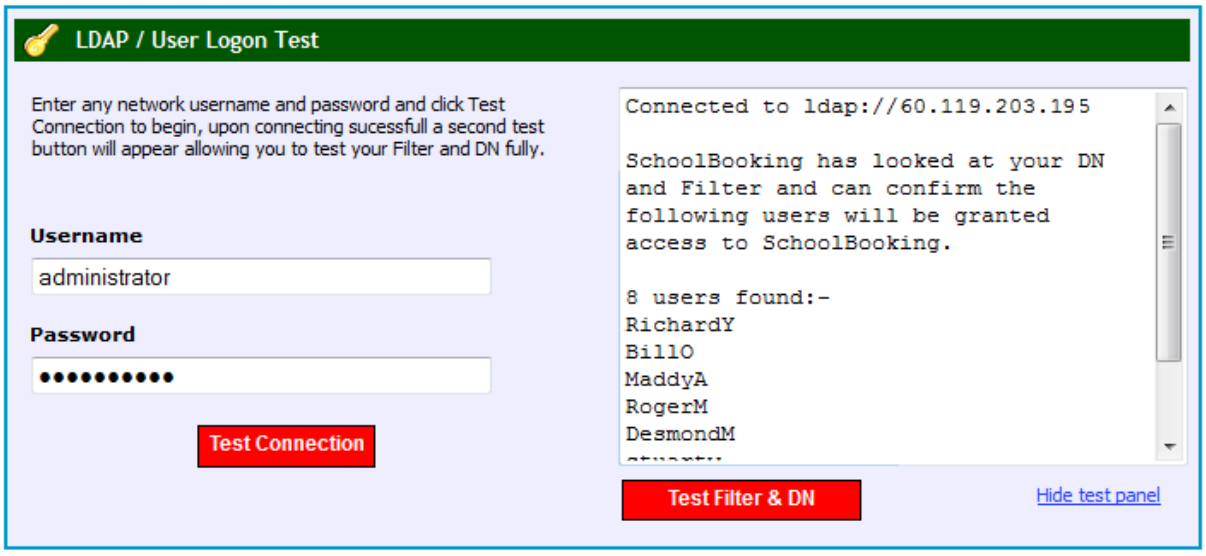


The Auto Registration Process

If Auto Register is set to “No” and a new user tries to login they will be rejected with the error message “You are not allowed to logon”. For the user to be able to login an Admin would need to enter the users details within SchoolBooking user manager ensuring that the username entered matches the network user name and then select YES under the LDAP option.

The SchoolBooking Settings and LDAP Test Panel

Once you have successfully tested your LDAP connection using the LDAP client tool specified in the Getting Started Section, we can then move on to entering the details into the SchoolBooking LDAP section.
Once you have entered your details click on the “Open Test Panel” button.
A new window will appear with some authentication fields on the left and a response window on the right.
Enter a network username and password; you should be able to use any network account within your Active Directory to authenticate as LDAP should be viewable by any of your users.
Once you have successfully authenticated a further button will appear at the bottom of the response window, allowing you to test your DN and Filter.
If you click the Test DN & Filter button, you will be able to see who will really be able to access SchoolBooking. The test looks at the Base DN and the Filter and then displays what SchoolBooking can see.
You can go back and forth between the Test Panel and the settings to specify and try different filters and Base DN and test them – again we do recommend doing this in an LDAP client tool.



Example of a response from the server after click the Test DN & Filter button.

If you get the list of users you were expecting, hide the test panel and click the X in the corner of the LDAP window. You will then be asked to save; after which you can then enable LDAP.
Note that SchoolBooking has a deliberate limit time out set on this tool so if your server / request takes longer than 1 minute to return the list of users, the tool will time out. This may occur if you have a lot of users within your Active Directory. If you believe the filter to be correct but are unable to test due to the time out, try enabling LDAP and then logging on with a user from your sites login portal.

Frequently Asked Questions

Why can't my LDAP users change their Username or Password from within SchoolBooking?

Any user who logs into SchoolBooking using LDAP will not be able to change their username or password as SchoolBooking only queries (reads) your LDAP server and does not write to it.

What happens to my existing users once I enable LDAP?

Nothing will happen to your users they will continue to Login as they have done using their local SchoolBooking account.

How can I allow my existing local users to be able to logon with LDAP?

Simply logon as a SchoolBooking Administrator and go to user manager, edit the existing user you want to switch to use LDAP and under the LDAP option change it from No to Yes.
You must also ensure that their SchoolBooking username matches up with their network Username.
You can also use Bulk LDAP management tool to update multiple users at once – this can be found within the Bulk tools section of user management.

How does it work?

SchoolBooking will connect using the settings you specify, it passes the username and password entered by the user from your SchoolBooking portal page and passes it over to your LDAP server. It is then up to your LDAP server to respond with either a simple yes or no to whether the user can logon.

What information does School Booking store about the user?

SchoolBooking only queries the users who successfully authenticate and pass your filter requirements. The details we pull from your LDAP server are based upon the users initial authentication; the fields we query are their Username, Forename, Surname and Email Address. These details will be used to populate the user within SchoolBooking.
It is important to note that SchoolBooking does not store LDAP passwords.

How quickly can I expect a user to login?

Our tests have shown that an average LDAP user will authenticate in less than 1 second but it will of course be dictated by the speed of your internet connection and other outside factors.
The connection between the SchoolBooking authentication servers and the internet is 100 Mbps.

Can SchoolBooking help me configure my LDAP server?

We can offer advice about your server / network setup and are happy for you to pass over your settings for us to look at and test. We unfortunately cannot remote into your server and change your server or network configuration.

How does LDAP affect my SchoolBooking User license?

We recommend that whilst configuring your Base DN / Filter you also consider your SchoolBooking user license. By default, if an LDAP user exceeds your sites user license limit they will still be allowed to connect. However, when an administrator visits the user management page they will not be allowed to make changes until they lower the enabled user count. We may also contact you to ask for you to lower your user count.