

Open Directory

Using Open Directory to authenticate users connecting to Rumpus.

Before You Start

Open Directory is Apple's directory and network authentication services architecture. Rumpus includes the ability to authenticate users via Open Directory, and therefore allow access to your Rumpus server based on local user accounts, accounts defined on a network LDAP server, or other Open Directory supported service.

Administering LDAP and other user account management services is well beyond the scope of this article, and it is assumed that you are experienced in managing directory services. For those without an existing Open Directory service, we strongly recommend using the built-in Rumpus user account management database, instead of Open Directory. For complete details, see the "Managing User Accounts" article in the "Helpful Info" folder of the Rumpus package.

Open Directory Considerations

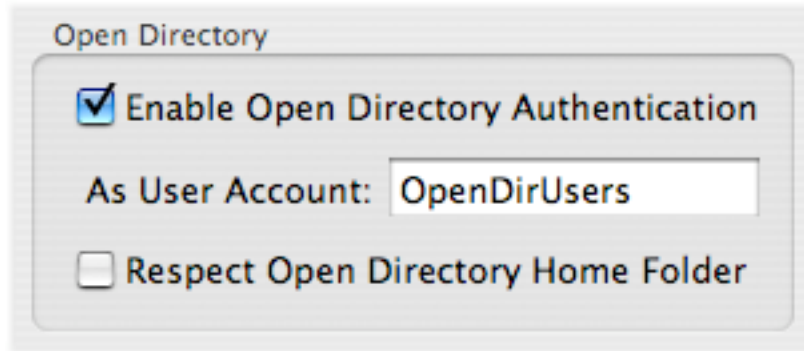
Because Rumpus uses the Open Directory framework to authenticate users, it is compatible with standard user authentication sources configured for use on the Rumpus computer. Use the Directory Access utility to select authentication services to be searched. Again, it is assumed that you are familiar with the Directory Access application in OS X, and that you have already configured the Rumpus server to search needed databases for user authentication information.

At this point, it is important to understand the difference between "authentication" and "authorization". "Authentication" refers to the act of confirming a user's identity, which in most cases (including all authentication done by Rumpus) means verifying that the user has entered the correct password. "Authorization", on the other hand, defines what the user is permitted to do. Rumpus will authenticate users via any Open Directory user account database, but for the most part, authorization (specifying what the Open Directory authenticated user is permitted to do) is defined within Rumpus.

You will therefore create a Rumpus user account, which will be applied to all Open Directory authenticated users, to define authorization privileges. This account will also be used to apply all other user-specific options, such as upload and download notices, account restrictions, and so on. Create the user account as you would any other Rumpus-defined account, and set the password to some suitably difficult to guess password (a long, random string of characters, for example) to ensure that the account is never used directly to access the server.

Configuring Rumpus

To have Rumpus authenticate users with locally configured Open Directory databases, open the “FTP Settings” window in Rumpus and switch to the “Security” tab. The “Open Directory” options group is shown below.



Check the “Enable Open Directory Authentication” checkbox, then enter the name of a user account defined in Rumpus in the “As User Account” field. The user account specified defines the authorization and other user-specific configuration options available in Rumpus. In other words, the privileges, Upload Notice, account restrictions, etc. configured on the Define Users window for the “As User Account” will be applied to all users authenticated via Open Directory.

The “Respect Open Directory Home Folder” determines whether or not Rumpus should use the user’s Open Directory home folder as their Rumpus home folder. Because the Open Directory home folder may not be valid on the Rumpus system, using this option can be complicated, so its use is described in the next section.

Specifying Home Folders

While any number of users can be authenticated via Open Directory, chances are each user needs to be granted access only to their own specific home folder. Because Rumpus provides a unique service that is distinct from other network resources, Rumpus does not automatically provide access to any particular folder on the Rumpus server or your file server. There are, however, a number of options that allow you to specify a home folder for users authenticated via Open Directory.

When All Users Should Share One Folder

If all users authenticated through Open Directory should be dropped into the same folder, then simply specify that folder for the selected user account in Rumpus. In this case, disable the "Respect Open Directory Home Folder" option, so that the folder chosen in Rumpus will be used as the home folder for all users.

When Each User Should Have A Home Folder On The Rumpus Server

If each authenticated user should be given their own home folder somewhere on the local Rumpus server, then specify a parent folder, followed by a tilde ("~") in the Home Folder field of the selected user account. Also, be sure to disable the "Respect Open Directory Home Folder".

In this configuration, Rumpus will replace the tilde in the home folder path with the user's account name, creating a unique path for each user. When users first log in, the home folder will be created if it doesn't already exist.

For example, if the user accounts "Bob", "Mary" and "Fred" are all authenticated using Open Directory, and the selected Rumpus user account has a home folder of "/Users/Shared/~", then each of these users will be assigned home folders of:

/Users/Shared/Bob
/Users/Shared/Mary
/Users/Shared/Fred

When Open Directory User Folders Are Correct Paths On The Rumpus Server

In some cases, such as defined users of the local system, the Open Directory user folder is a valid path on the Rumpus server and should be used as the user's Rumpus home folder. In this case, simply enable the "Respect Open Directory Home Folder", and set the selected user account home folder to a default path that can be used in case the Open Directory user folder is missing or can't be retrieved.

When The User Home Folder Exists On A Remote Volume

Rumpus can also handle the case where the Open Directory entry for each user account includes an accurate path to a folder on another server on your LAN. The remote server will need to be mounted as a volume on the Rumpus server's desktop at all times, so that Rumpus has access to the volume.

To set up this type of access, enable the "Respect Open Directory Home Folder" option, then open the Define Users window in Rumpus and choose the selected user account. Click the "Choose Folder" button next to the Home Folder field, and select the top level volume of the remote file server. Add a tilde ("~") to the end of the path, which tells Rumpus to append the users Open Directory user folder path to the path to the remote server.

For example, if the users "Bob", "Mary" and "Fred" all have user folders on a remote file server called "Server", set the selected user account home folder in Rumpus to "/Volumes/Server/~". If the user folder defined for each of those Open Directory Users were "/Users/Bob", "/Users/Mary" and "/Users/Fred" respectively, then Rumpus would map each user's home folder path to the correct local path on the Rumpus server:

/Volumes/Server/Users/Bob
/Volumes/Server/Users/Mary
/Volumes/Server/Users/Fred