Secure Shell (SSH)

If you would like to use a GUI (graphical user interface) to transfer files, please visit our SFTP page.

Logging in

In order to log in, you will need your Brandeis account username and password, as well as an authorization attribute for shell server access.

If you don't already have a Brandeis account, you can create one at https://identity.brandeis.edu.

To request authorization for your account to SSH into the shell servers, please go to https://identity.brandeis.edu/identity-manage and click on Enable/Disable shell access.

For Host Name, enter either:

- limpet.unet.brandeis.edu
- starfish.unet.brandeis.edu

Everyone has a choice of two servers to use. If one server happens to be down for maintenance, you can always try another.

For Username, enter your Brandeis username. This is the same as your e-mail address without the "@brandeis.edu."

Keep the default port number (22), and choose "Password" for the authentication method. Click connect.

Another box will prompt you for your password. Enter it, then click OK.

Windows SSH Client

Windows users can download PuTTY.exe for Windows.

Mac/Linux SSH Client

Mac and Linux users can simply type "ssh username@servername" from the Terminal (under Applications -> Utilities -> Terminal for Macs). For example, if your username was joeschmo, enter "ssh joeschmo@limpet.unet.brandeis.edu".

The first time you run SSH, you will get a message describing the host key sent by the server. Accept the key, provided that it matches the appropriate fingerprint:

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Fingerprint</th>
</tr>
</thead>
</table>

If you ever get a warning that the host key has changed, contact LTS immediately.

Related articles

- Remote Access Best Practices
- Secure Shell (SSH)
- Procedure to grant server access to consultants and vendors
• How to generate ssh key pairs and request ssh access to servers