GL

GL is the name of our general access Unix systems here at UMBC, managed by DoIT. Anyone with a UMBC account can access GL.

Accessing the GL Servers

To connect to GL you’ll need an SSH client. For Windows, we recommend using PuTTY; the Bitvise SSH client is an alternative option. For Mac and Linux, we recommend the `ssh` command in the Terminal. Below is the connection info for GL:

<table>
<thead>
<tr>
<th>Host:</th>
<th>gl.umbc.edu</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port:</td>
<td>22 (This is the default for SSH)</td>
</tr>
<tr>
<td>Protocol (Connection Type):</td>
<td>SSH</td>
</tr>
</tbody>
</table>

You authenticate to the GL systems using your myUMBC username (all lowercase!) and password.

Windows

Connect using your SSH client. They usually have a connection dialog where you can specify the host, port, and protocol information listed above.

Mac/Linux

Run `ssh yourusername1@gl.umbc.edu` in the Terminal.

Other information

Quotas

All UMBC accounts have a quota of 500MB. If you exceed your quota, you will have issues running programs, etc. You can check your quota by running “fs lq” in your home directory.

Host Authenticity

When you first connect to an unknown server over SSH, your client will typically present the server’s host key fingerprint so that you can verify its authenticity. These are the current host key fingerprints (as of 8/23/2018) for the GL servers:

- **ECDSA**
- **ED25519**
- **RSA**
  - SHA256: OsVzgoPEGqlaxINCqUX/3881WavHkT1ASDSOX0TBs4 MD5: c4:35:6:ab:3:6:4d:79:8:0:ab:2c:63:44

Common Questions

**Can I add an SSH key to my GL account?**

Sorry, but given the nature of our infrastructure, the GL servers do not support SSH public key authentication for normal users. We understand that might be frustrating to some of our more security-minded students, so here’s why:

The GL servers use a secure network authentication protocol called Kerberos for logins, and home directories are served from a network filesystem called AFS. AFS uses your Kerberos credentials to grant access to your home directory during the login process.

In a typical SSH public key authentication setup, the keys that are allowed to authenticate for a user are listed in a file in their home directory which--in our setup--the SSH process doesn’t have access to until you’ve already authenticated to Kerberos.

In other news, the GL systems do allow GSSAPI authentication. If you’re a power user, handy with Google and reading software documentation, you're welcome to take a look at Configuring Kerberos for the UMBC realm.

⚠️ Help requests for configuring Kerberos, GSSAPI, and SSH on personal systems are outside the scope of our support. But it's really not that hard. You can do it--we believe in you!