

Connecting to SISLT Online

SISLT-Online Environment

SISLT is providing a space to host websites, and related assets, created during our online web development courses. The SISLT-Online hosting environment is setup similar to commercial web hosts, but how you connect and where your files may differ. The information in this document provides general connection instructions which will help you connect to the SISLT-Online server and upload your files.

You have a limited amount of space. Please do not upload extra files. This is not for storing files, it is for hosting your classwork, website, and related materials.

Questions

- If you experience difficulty connecting to the server please contact your instructor to ensure your account has been created. If you need to have an account created please have your instructor, or the SISLT student coordinator, send your name and PawPrint to Aaron D. Moss (mossad@missouri.edu).
- If you experience difficulty connecting to the VPN contact the Division of IT support desk (573-882-5000 or techsupport@missouri.edu) for additional assistance.
- If you receive a “Forbidden” error when trying to view your website please contact Aaron D. Moss (mossad@missouri.edu) and provide your URL.
- Your Mizzou login id is referenced as Single Sign On, Single Sing On ID, SSO, SSO ID, and PawPrint. These are equivalent: Single Sign On == SSO == SSO ID == PawPrint. Instructors and technical support personnel may use one or more of these terms when referring to your username on the server.

Quick Start

1. Connect to the VPN by visiting <https://anyconnect.missouri.edu/> in a web browser.
2. Use a SFTP client, like FileZilla, to connect to sislt-online.missouri.edu .
3. Change permissions on your **www** folder, see instructions below or email Aaron D. Moss (mossad@missouri.edu); you will see a 403 forbidden error or a 404 not found error until this is changed.
4. Upload files to your web directory; a folder named **www** .
5. View your website at <https://sislt-online.missouri.edu/~MyPawPrint/> .

Connection Settings

VPN (Virtual Private Network)

Before connecting to the SISLT Online server you'll need to connect to the Mizzou network; if you're on campus and using a wired connection you don't need to do this.

You will connect to the Mizzou network through a VPN using the Cisco AnyConnect Mobility Client available at <https://anyconnect.missouri.edu/> .

Web Server Hostname

Use the following hostname to connect to the SISLT-Online server:

- sislt-online.missouri.edu
-

Your Username

Your username on the server is based on the domain of your PawPrint. Most students will be in the TIGERS domain, and will not need to add the domain to their PawPrint. If you are an University of Missouri employee your SSO will be part of another domain. Please use the following to determine your domain:

- TIGERS: MyPawPrint
- UMC-USERS: MyPawPrint@col.missouri.edu
- UM-USERS: MyPawPrint@um.umsystem.edu
- UMH-USERS: MyPawPrint@umh.edu
- UMKC-USERS: MyPawPrint@kc.umkc.edu
- MST: MyPawPrint@mst.edu
- UMSL: MyPawPrint@stl.umsl.edu
- UMAC: MyPawPrint@umac.umsystem.edu
- UMAD: MyPawPrint@umad.umsystem.edu

If you're a student and your PawPrint is **abc123** then the username you use to login will be: **abc123**.

If you're a student attending from another University of Missouri campus, or a staff or faculty member, your username will have your domain included. If your PawPrint is **hopeb** and you're at MU then the username you use to login will be: **hopeb@col.missouri.edu**. If you're with UM System then **hopeb@um.umsystem.edu**. If UM Hospitals: **hopeb@umh.edu**. If KC: **hopeb@kc.umkc.edu**. If MST: **hopeb@mst.edu**. If UMSL: **hopeb@stl.umsl.edu**.

Your Password

Use your PawPrint password to log into SISLT-Online.

Your Website

Your website URL is based on your PawPrint; if you had to add a domain to your PawPrint to login on to the server you will need to add that domain to your URL.

URL: <https://sislt-online.missouri.edu/~MyPawPrint/>

URL: <https://sislt-online.missouri.edu/~MyPawPrint@col.missouri.edu/>

URL: <https://sislt-online.missouri.edu/~MyPawPrint@um.umsystem.edu/>

URL: <https://sislt-online.missouri.edu/~MyPawPrint@umh.edu/>

URL: <https://sislt-online.missouri.edu/~MyPawPrint@kc.umkc.edu/>

URL: <https://sislt-online.missouri.edu/~MyPawPrint@mst.edu/>

URL: <https://sislt-online.missouri.edu/~MyPawPrint@stl.umsl.edu/>

Note: *If you receive a “Forbidden” error when trying to view your website please contact Aaron D. Moss (mossad@missouri.edu) and provide your URL.*

Your Account

Your account is created the first time you log onto the server. When your account is created it doesn't have the correct permissions to allow your website to be viewed. Instructions for changing permissions are below, or you can send an email with your PawPrint to Aaron D. Moss (mossad@missouri.edu) who will make this change.

1. Connect to the VPN by visiting <https://anyconnect.missouri.edu/> in a web browser.
2. Use a SFTP client, like FileZilla, to connect to sislt-online.missouri.edu .
3. Change permissions on your **www** folder, see instructions below or email Aaron D. Moss (mossad@missouri.edu); you will see a 403 forbidden error or a 404 not found error until this is changed.
4. Upload files to your web directory; a folder named **www** .
5. View your website at <https://sislt-online.missouri.edu/~MyPawPrint/> .

VPN

Before connecting to the SISLT Online server you'll need to connect to the Mizzou network; if you're on campus and using a wired connection you don't need to do this.

You will connect to the VPN using the Cisco AnyConnect Mobility Client available at <https://anyconnect.missouri.edu/> .

Install

If you have not installed the Cisco AnyConnect Mobility Client follow the instructions below to install it. If you have already installed the VPN client, then you may skip directly to the Connect instructions.

1. Go to <https://anyconnect.missouri.edu/> .
2. Choose your group. Students choose ****Generic**, employees choose ***Employee**.
3. Enter your PawPrint SSO.
4. Enter your password for your PawPrint.
5. Click **Login**.
6. You will be prompted to verify your identity. You can choose to Enter a time-based passcode or enter one of the following numbers to verify using that method:
 - Enter a time-based passcode
 - 1 for SMS/TEXT MESSAGE.
 - 2 for PHONE.
 - 3 for EMAIL.
 - 4 for Send Passcode to Phone APP.
 - 5 for Send Accept to Phone APP.
 - If you haven't installed the OTP app on a mobile device you may not see options 4 and 5.
7. Click **Continue** to submit your contact choice.

8. If you have multiple phone numbers or devices associated:
 1. For **Response** type the number beside the chosen phone number or device.
 2. Click **Continue**.
9. You are prompted for the passcode: *Please enter OTP or use '0' to try a different option*
10. For **Response** type the passcode.
11. Click **Continue**.
12. You will be redirected to a page with a link to download the Cisco AnyConnect software.

Instructions for downloading and installing the software can be found on the download page, just click **Instructions** to expand the installation instructions.

A button with a plus sign icon and the text "Instructions".

Connect

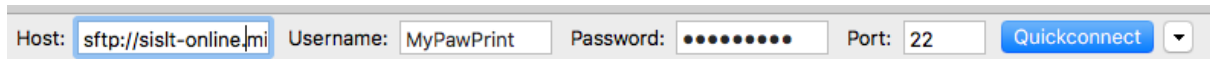
1. Open Cisco AnyConnect Secure Mobility Client. On Windows this is a shortcut on the desktop, or in the Start menu. On Mac this is in the Applications folder.
2. In the text box type **anyconnect.missouri.edu**.
3. Click the **Connect** button.
4. In the Group dropdown choose:
 1. ****Generic**, if you're a student.
 2. ***Employee**, if you're an employee.
5. In the **Username** field type your University username (PawPrint or SSO).
6. In the **Password** field type your University password.
7. Click **OK**
8. You will be prompted to verify your identity. You can choose to Enter a time-based passcode or enter one of the following numbers to verify using that method:
 - Enter a time-based passcode
 - 1 for SMS/TEXT MESSAGE.
 - 2 for PHONE.
 - 3 for EMAIL.
 - 4 for Send Passcode to Phone APP.
 - 5 for Send Accept to Phone APP.
 - If you haven't installed the OTP app on a mobile device you may not see options 4 and 5.
9. Click **Continue** to submit your contact choice.
10. If you have multiple phone numbers or devices associated:
 1. For **Response** type the number beside the chosen phone number or device.
 2. Click **Continue**.
11. You are prompted for the passcode: *Please enter OTP or use '0' to try a different option*
12. For **Response** type the passcode.
13. Click **Continue**.
14. You are now connect to the University of Missouri (Mizzou) VPN.

You can visit Mizzou's knowledge base for instructions on installing and connecting to the VPN (login with your PawPrint and password): <https://missouri.rightanswers.com/portal/app/portlets/results/viewolution.jsp?solutionid=150910121324401&page=1&position=1> .

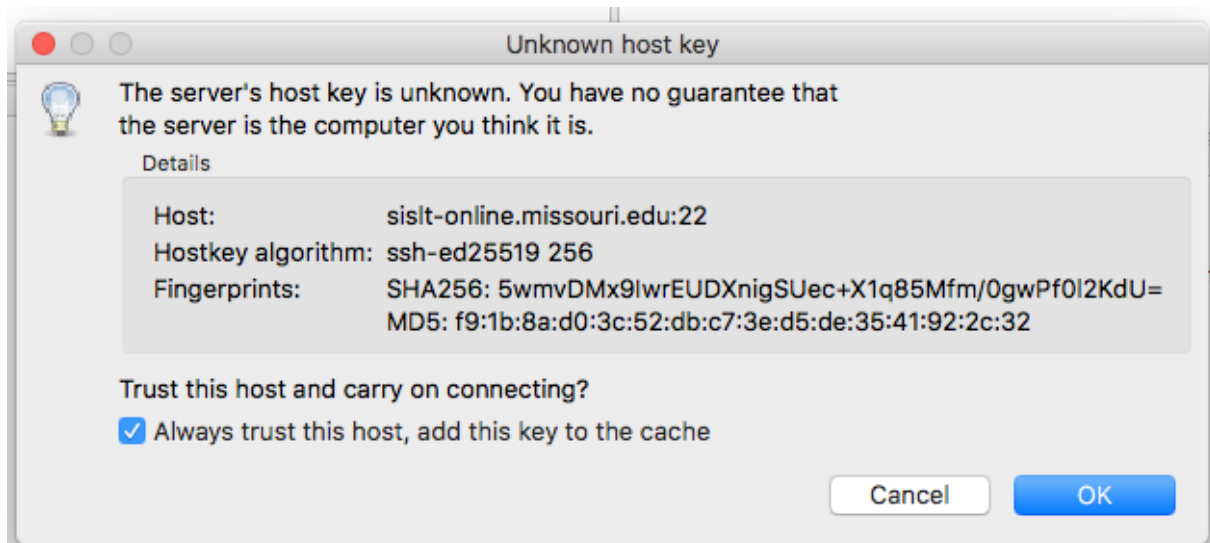
Note: *If you experience difficulty connecting to the VPN contact the Division of IT support desk (573-882-5000 or techsupport@missouri.edu) for additional assistance.*

FileZilla

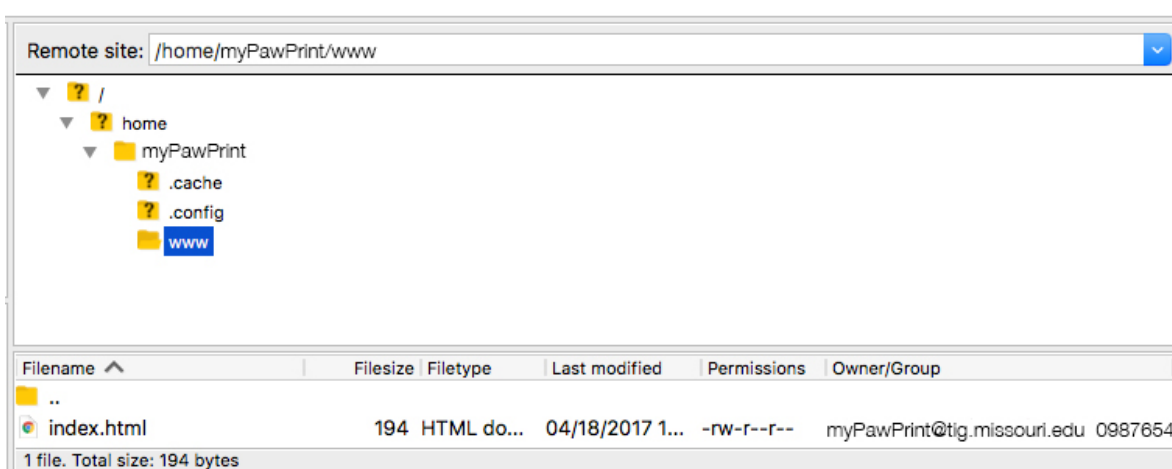
1. Download and install FileZilla. <https://filezilla-project.org/>
2. Open FileZilla.
3. In the Quick Connect tool bar enter the following:
 - Hostname: sftp://sislt-online.missouri.edu
 - Username: MyPawPrint
 - Password: Your PawPrint password.
 - Port: 22



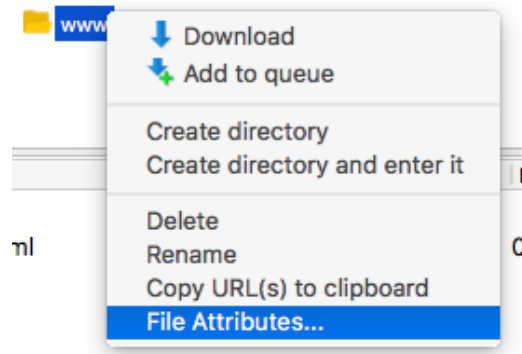
4. Click **Quickconnect**.
5. If “Unknown host key” check “Always trust this host, add this key to the cache” and click **OK**.



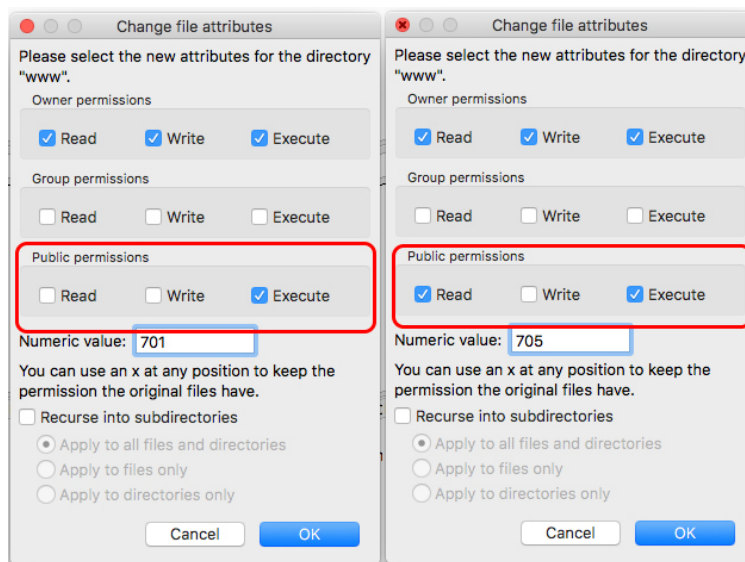
6. Remote site pane should populate with your home directory at /home/myPawPrint/. If this is not the directory path you see in the remote pane, you will need to navigate to your /home/myPawPrint/ directory before continuing.



7. Right click on the **www** directory and select **File Attributes...** from the menu.



8. Change the attributes on the **www** directory to allow the public to read and execute; check the boxes next to read and execute under **Public permissions** to and click **OK** to save.



9. Your web site will be stored in the **www** directory on the server. Drag files from the local pane to the **www** directory in the remote pane to upload files to your website in SISLT-Online.
10. View your website at <https://sislt-online.missouri.edu/~mypawprint/> where mypawprint is your SSO (PawPrint).

Note: If you receive a “Forbidden” error when trying to view your website please contact Aaron D. Moss (mossad@missouri.edu) and provide your URL.

Save a Backup: Drag files from the remote pane to a directory on the local pane to download files to your computer.

HELP! Troubleshooting Errors

Errors happen. Please try the following.

Connection time out after 20 seconds

1. *Did you enter the hostname correctly?*

- **Check to ensure the hostname *sislt-online.missouri.edu* for the server is correctly entered into the Host field of FileZilla.**

2. *Did you enter your username correctly?*

- **Your username is your PawPrint if you're enrolled through the Columbia campus.**
- **Your username is your PawPrint plus your domain if you're enrolled through another University of Missouri campus. Please see the *Your Username* section above for examples of PawPrint plus domain.**

3. *Did you connect to the Mizzou VPN? If not, you might see the following in the status window of FileZilla:*

```
Status:      Connecting to sislt-online.missouri.edu...
Response:    fzSftp started, protocol_version=8
Command:     open "mypawprint@sislt-online.missouri.edu" 22
Error:       Connection timed out after 20 seconds of inactivity
Error:       Could not connect to server
```

- **Connect to the Mizzou VPN and then connect to the server using FileZilla.**

Terminal/Command Line SSh

1. On the command line type one of the following depending on your domain:
 - `ssh mypawprint@sislt-online.missouri.edu`
 - `ssh mypawprint@col.missouri.edu@sislt-online.missouri.edu`
 - `ssh mypawprint@um.umsystem.edu@sislt-online.missouri.edu`
 - `ssh mypawprint@umh.edu@sislt-online.missouri.edu`
 - `ssh mypawprint@kc.umkc.edu@sislt-online.missouri.edu`
 - `ssh mypawprint@mst.edu@sislt-online.missouri.edu`
 - `ssh mypawprint@stl.umsl.edu@sislt-online.missouri.edu`
2. Enter your PawPrint password when prompted.
3. You may be asked to save the Host Key for the server. If you know the host and trust it you should allow the connection.

You have a limited amount of space. Please do not upload extra files. This is not for storing files, it is for hosting your classwork, website, and related materials.