

Connecting to Cat5 via SSH from macOS

If this is your first time to connect to Cat5 via SSH, start with the **First Time Only Steps** below.

Connecting to Cat5

1. Open the "Terminal" app. (If it's not in your Dock, find it in Finder → Applications → Utilities.)
2. At Terminal's command prompt, type `ssh cat5` and press Return.
3. If SSH complains that "The authenticity of host ... can't be established," then please check [Cat5 Host Key Fingerprints](#) on the DES website for how to proceed.
4. Otherwise, type your Cat5 password (it will not be visible) and press Return.

```
Terminal -- -bash -- 80x24
$ ssh cat5
[redacted]@cat5.envsci.rutgers.edu's password:
Warning: No xauth data; using fake authentication data for X11 forwarding.
Last login: Thu Sep 13 14:43:46 2018 from 173.10.101.20
[redacted]@cat5 ~]$
```

(Ignore the warning about "No xauth data.")

You are now connected!

Disconnecting from Cat5

1. To close your SSH session to Cat5, type `exit` at Cat5's command prompt.
2. (Optional) Type `exit` again to quit the Terminal session, then close the Terminal window.

First Time Only Steps

Install XQuartz

You must have the "XQuartz" X-Window system installed before you use SSH. You may have already installed it, for example for use with X2Go. If you are not sure, open Finder, go to Applications, and then the Utilities folder. If XQuartz is shown in this folder, then you can proceed to configuring SSH. If not, then follow these steps to install XQuartz:

1. Go to this page in your web browser: <https://www.xquartz.org/>
2. In the middle of the page, click on "XQuartz-X.Y.Z.dmg" to download, where "X", "Y", and "Z" are version numbers. Save the file.

Download	Version	Released	Info
XQuartz-2.7.9.dmg	2.7.9	2016-05-05	For OS X 10.6.3 or later

License Info

(Continued on next page)

Install XQuartz (Continued)

3. Open the saved file from step 2. A window will open. Double-click on the XQuartz package shown in this new window.
 - a. Click “Continue” three times.
 - b. Read and agree to the license.
 - c. Click “Install”
 - d. When done, “eject” the “XQuartz-X.Y.Z” device in Finder.

Configure SSH for Cat5

SSH is built-in to macOS, so you don’t need to install it. Follow these steps to setup convenient access to Cat5:

1. Open the “Terminal” app.
 - a. To find it, open Finder, go to Applications, and then open the Utilities folder. Terminal is in that folder.
 - b. You will use Terminal every time you connect via SSH. To make it easier to get to, you may (optionally) drag the Terminal icon from the Finder into your Dock.
2. You will need to edit the SSH configuration file, but you may not have one to edit yet. The steps below will check if you have the file and make one if needed. Type the specified commands (written in orange) at the Terminal command prompt, and press Return after each command.
 - a. Check if you have an “.ssh” directory, which stores the configuration for the SSH program, by typing this command:

```
ls -a ~/.ssh
```
 - b. If the “.ssh” directory exists, then the above command will show you the contents of that directory. In that case, skip to step “c”. If the “.ssh” directory does not exist, the “ls” command will complain, saying “No such file or directory.” If that happens, create the missing directory like so:

```
mkdir -m 700 ~/.ssh
```
 - c. Change into the “.ssh” directory with this command:

```
cd ~/.ssh
```
 - d. If you created the directory in step “b”, then no files exist within it yet; skip to step “e” to create one. Otherwise, test if the “config” file exists with this command:

```
ls config
```

If “ls” responds with “No such file or directory” then proceed to step “e” to create it. Otherwise, jump to step 3.
 - e. Create an empty configuration file and set its permissions with these commands:

```
touch config  
chmod 600 config
```
3. Edit the configuration file (~/.ssh/config) with your favorite text editor. If you don’t have a favorite yet, type this command to open the file in TextEdit (the default editor in macOS):

```
open -a TextEdit ~/.ssh/config
```

(Continued on next page)

Configure SSH for Cat5 (continued)

4. Add the following lines to the bottom of the “~/.ssh/config” file, replacing `username` with your actual user name on Cat5 (usually the same as your Rutgers NetID). All lines after the “Host cat5” line should be indented a couple of spaces:

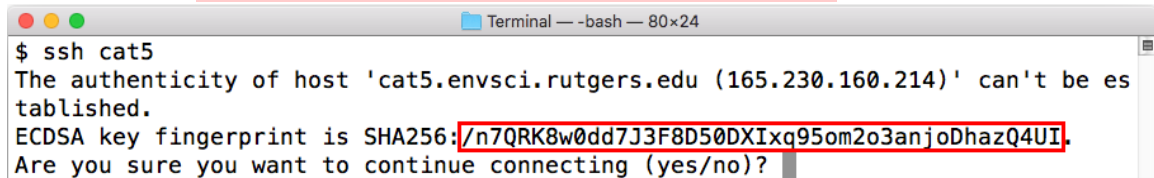
```
Host cat5
  ForwardX11          yes
  ForwardX11Trusted  yes
  HostName            cat5.envsci.rutgers.edu
  User                username
```

5. Save the file and close the editor.
6. Your SSH is now configured. Proceed to connecting for the first time.

Connect to Cat5 for the First Time

The first time you connect, a few things will be different from subsequent connections.

1. Open the “Terminal” app. (If it’s not in your Dock, find it in Finder → Applications → Utilities.)
2. At Terminal’s command prompt, type `ssh cat5` and press Return.
3. Since this is your first time to connect, the SSH program does not recognize Cat5. It will warn you that “The authenticity of host ... can’t be established” and ask if it should really connect. **This is not a trivial question, so do not answer blindly!**



```
Terminal -- -bash -- 80x24
$ ssh cat5
The authenticity of host 'cat5.envsci.rutgers.edu (165.230.160.214)' can't be es
tablished.
ECDSA key fingerprint is SHA256:/n7QRK8w0dd7J3F8D50DXIxq95om2o3anjoDhazQ4UI.
Are you sure you want to continue connecting (yes/no)?
```

4. To ensure a secure connection, check that the provided “fingerprint” (outlined in red above) *exactly* matches one of these lines:
 - /n7QRK8w0dd7J3F8D50DXIxq95om2o3anjoDhazQ4UI
 - 25:ea:b6:1d:75:17:9e:ea:48:61:50:09:4d:80:57:17
 - ee:05:33:ed:1e:5c:31:84:86:b9:8c:11:15:1a:9d:6f

If it matches one of those, then type `yes` to connect. Proceed to step 6 on the next page.

5. **If the fingerprint does not match** any of those, then please check [Cat5 Host Key Fingerprints](#) on the DES website for more possible fingerprints. **Do not accept an unverified fingerprint!** If you find a matching fingerprint in that list, continue to step 6 on the next page. Otherwise, stop here and contact help@envsci.rutgers.edu for assistance before proceeding.

Connect to Cat5 for the First Time (continued)

6. At this point, you will be asked to enter your password. If your Cat5 account is new, then you were given a Temporary Password, which you are forced to change upon your first login. If you have already changed your password (e.g. by connecting via X2Go or via SSH from another computer) then you can enter your normal Cat5 password here. Proceed to step 8.

❶ Important: Passwords **will not be visible** on the screen while you type them.

7. Otherwise, follow these steps to update your password:

```

Terminal — -bash — 80x24
$ ssh cat5
The authenticity of host 'cat5.envsci.rutgers.edu (165.230.160.214)' can't be es
tablished.
ECDSA key fingerprint is SHA256:/n7QRK8w0dd7J3F8D50DXIqx95om2o3anjoDhazQ4UI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'cat5.envsci.rutgers.edu,165.230.160.214' (ECDSA) to
the list of known hosts.
[REDACTED]@cat5.envsci.rutgers.edu's password: a ← Temporary Password
Warning: No xauth data; using fake authentication data for X11 forwarding.
X11 forwarding request failed on channel 0
You are required to change your password immediately (root enforced)
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for [REDACTED].
Changing password for [REDACTED].
(current) UNIX password: b ← Temporary Password (again)
New password: c ← Your New Password
Retype new password: d ← Your New Password (again)
passwd: all authentication tokens updated successfully.
Connection to cat5.envsci.rutgers.edu closed.
$ e ← You can now log in again with your new password
  
```

- At the first password prompt, type the **Temporary Password** and press Return.
 - After the announcement about changing your passwords, at the “(current) UNIX password:” prompt, type the **Temporary Password** (yes, again) and press Return. If you type the Temporary Password incorrectly here, the process will abort, and Cat5 will disconnect. You will have to start over at step 2 (skipping steps 3-5).
 - At the “New password” prompt, type a **new, made-up password for Cat5**. No one else may know this password. You should be able to remember it, but people should not be able to easily guess what it is. **Don't use a dumb password such as “password” or someone's name or birthday.** If your password is too simple, Cat5 will complain and you will have to come up with something else. Press the Return key when done typing.
 - At the next prompt, type your **new password** again (to verify that you typed it correctly since you cannot see it), and press Return. If you did not type your new password the same as the first time, this process will abort, and you will have to start over at step 2.
 - After successfully changing your password, Cat5 will disconnect. Your new password is now your regular Cat5 password. You do not need the Temporary Password any more.
8. The next time you connect to Cat5, you will log in normally (as shown on page 1) using your normal Cat5 password.

Congratulations, you are now completely setup to connect to Cat5 via SSH! Enjoy!