Two Factor Authentication on O2

As of Dec 3, 2018, all O2 cluster logins from outside of the HMS network require two-factor authentication.

The Two Factor Authentication FAQ has quick answers to your more specific questions.
Or read below for a broader overview of 2-factor authentication.

<table>
<thead>
<tr>
<th>If logging into O2 from...</th>
<th>Will two factor authentication be required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>HMS wired network connection in an HMS on-campus building</td>
<td>No</td>
</tr>
<tr>
<td>(Note that this may exclude certain cases where labs from HMS affiliates have office space in an HMS building like the NRB)</td>
<td></td>
</tr>
<tr>
<td>HSDM and HSPH networks</td>
<td>No</td>
</tr>
<tr>
<td>When logged into the HMS VPN - from anywhere</td>
<td>No</td>
</tr>
<tr>
<td>(Please do NOT copy large files to/from O2 when on VPN.)</td>
<td></td>
</tr>
<tr>
<td>&quot;HMS Private&quot; wireless network</td>
<td>No</td>
</tr>
<tr>
<td>&quot;HMS Public&quot; wireless network</td>
<td>Yes</td>
</tr>
<tr>
<td>Other Harvard networks (FAS, etc)</td>
<td>Yes</td>
</tr>
<tr>
<td>Networks at all other HMS affiliates (hospitals, etc)</td>
<td>Yes</td>
</tr>
<tr>
<td>Any other external network (home, etc), NOT using the HMS VPN</td>
<td>Yes</td>
</tr>
<tr>
<td>an HMS system (even on campus) which has a public-facing IP address</td>
<td>Yes</td>
</tr>
<tr>
<td>(This is mostly for web and other application servers, not your desktop)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>within O2...</th>
<th>Will two factor authentication be required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssh/copy from O2 login nodes to transfer.rc.hms.harvard.edu</td>
<td>Yes</td>
</tr>
<tr>
<td>ssh from one login node to another login node</td>
<td>Yes</td>
</tr>
<tr>
<td>ssh from one transfer node to another transfer node</td>
<td>No</td>
</tr>
<tr>
<td>ssh/copy from compute node to transfer.rc.hms.harvard.edu</td>
<td>No</td>
</tr>
<tr>
<td>copy from interactive job to/from transfer.rc.hms.harvard.edu</td>
<td>No</td>
</tr>
<tr>
<td>copy batch job to/from transfer.rc.hms.harvard.edu</td>
<td>No</td>
</tr>
</tbody>
</table>

Summary

- Previously, O2 only required a password login using your eCommons ID.
- Security has been dramatically increased for the data and account credentials on O2. Over time, there have been increased hacking attempts.

With this change, two factor authentication will be required to access both regular login servers and file transfer servers:
- o2.hms.harvard.edu
Includes all O2 login servers: login01.o2.rc.hms.harvard.edu, login02.o2.rc.hms.harvard.edu, etc...
- transfer.rc.hms.harvard.edu
- orchestra.med.harvard.edu (which now just redirects to O2)

With two-factor authentication, your O2 login additionally requires a secondary validation such as a security code sent to your cell phone or a code generated by an application such as Duo Mobile.

- Harvard already requires two factor authentication for Harvard Key and the FAS Odyssey HPC Cluster.
- HMS requires it for resetting your eCommons ID password and other services such as the HMS VPN.

Setting up the DUO application for HMS

If you already use DUO with the HMS VPN, then you are all set for O2.

If you use DUO with Harvard Key but not HMS yet, you still need to set up a separate DUO HMS profile.

The easiest way is to try logging into O2 via ssh. If you are not yet registered, you will be prompted to register with a unique URL, as shown below:

```
DESKTOP:~$ ssh abc123@o2.hms.harvard.edu
Password: [input your account password]
Please enroll at https://api-2f8a17a9.duosecurity.com/portal?code=443789224a30udsihdj8a&akey=DAIUI3JAB2FHDJKS7MJRQ0G
```

You can also visit the following page for how to register your device/phone for use with DUO at HMS.

Once you are enrolled in DUO for HMS:

Login (using an SSH application as usual) to O2: o2.hms.harvard.edu

- Follow instructions for inputting your security code:
  - Enter either "1" or "push" to authenticate via DUO
  - Enter either "2" or "phone" to authenticate via response to a voice call
  - Enter either "3" or "sms" to get a code via a SMS text message

The example below is for user "abc123" using the "Duo Push" method.
To test SFTP / SCP / rsync logins:

The process is the same as above no matter which application you use (e.g. command line sftp or apps like FileZilla), except that you will not be prompted with a choice for "push | phone | sms".

By default, scp/sftp/rsync will choose your default method in DUO to authenticate.

How to setup default DUO Method using DUO_PASSCODE environment variable

By default non-interactive commands like scp/sftp/rsync or applications like FileZilla/WinSCP/MobiKwik etc. will not work if you don't have a default DUO Method. They simply hang forever or timeout after a few seconds.

You can setup a default DUO setting by doing any of the two following methods.

using o2

- to be set on your o2 cluster .bashrc or .bash_profile
- values: phone, push, sms, sms1, phone1, push1, sms2, push2, phone2.
- If you set DUO_PASSCODE variable as mentioned below, then you will not be prompted for any type of login either ssh or scp/sftp/rsync etc.
- It is not recommended to use sms with DUO_PASSCODE variable, because you won't be given a prompt to enter sms code, so the login attempt will fail.
- NOTE: By choosing this method, you'll not be prompted for regular ssh commands as well, if you just want auto push for non-interactive commands choose the other method for setting default DUO.

Example:
#login to o2 normally
DESKTOP:-$ ssh abc123@o2.hms.harvard.edu
Welcome to O2 (Orchestra 2)!
...
[abc123@login06]:~
$
# THIS HAS TO BE DONE ONLY ONCE
[abc123@login06]:~
$ echo 'export DUO_PASSCODE=phone' >> $HOME/.bashrc

#CHECK WHETHER .bashrc IS UPDATED
[abc123@login06]:~
$ tail -1 $HOME/.bashrc
export DUO_PASSCODE=phone

#now logout from o2
[abc123@login06]:~
$ logout
Connection to o2.hms.harvard.edu closed.

#NOW, TRY SCP/SFTP/RSYNC
DESKTOP:-$ sftp abc123@o2.hms.harvard.edu
Connected to o2.hms.harvard.edu.
sftp> quit
quit

#NOW, TRY SSH TO A SERVER
DESKTOP:-$ ssh o2.hms.harvard.edu
Reading $DUO_PASSCODE...

Calling your phone...
Dialing XXX-XXX-1234...
Answered. Press 1 on your phone to log in.
Success. Logging you in...
Welcome to O2 (Orchestra 2)!
...
[abc123@login06]:~
$

using secure.med.harvard.edu

login to secure.med.harvard.edu using any browser of your choice, after entering your ecommons and password, you'll be landed on a page shown like below,

Click cancel at the bottom of the prompt so that you don't get re-directed.
Now click My Settings & Devices on the left hand side bar, now you've to approve/accept your 2fa so that you'll land on a page something like this below.

Now you can choose your default method and save it. That should do it!

The next time you do scp/sftp/any non-interactive commands you'll get a default prompt on your default chosen method.

- **NOTE:** By choosing this method, you'll still get prompted for regular ssh commands, if you just want auto push for ssh commands as well choose the o2 method for setting default DUO.

**For Windows Users:**

To set up your DUO_PASSCODE environment variable, consult a page like this: [https://www.computerhope.com/issues/ch000549.htm](https://www.computerhope.com/issues/ch000549.htm) (this may require administrator access on your local machine).

This may be a good time for you to transition away from PuTTY if that is your primary method of connection to O2. We have been recommending "native" terminal emulator applications such as MobaXterm, or for savvy Windows 10 users, Windows Subsystem for Linux. The reason for this is that setting the above environment variable (DUO_PASSCODE) is somewhat involved on Windows as opposed to on OS X or other *nix systems due to there not being easy access to a terminal (and cmd.exe and powershell.exe are not suitable replacements most of the time). Applications such as MobaXterm superimpose a *nix-like terminal over your Windows installation, and you can navigate your system much like you would navigate O2. Once you have one of these types of applications set up, you can follow the above example verbatim instead of having to do complex menu navigation to accomplish the equivalent result. MobaXterm also has a built-in X server, so you no longer need a separate program running to perform X11 forwarding (e.g. Xming), as well as a built in ftp browser, so you don't need programs like Filezilla or WinSCP either. We recommend any of the following over PuTTY:

**EASY**

- **MobaXterm** - [https://mobaxterm.mobatek.net/](https://mobaxterm.mobatek.net/) (the free version should be all you need)

**MEDIUM/HARD (but far more flexible)** -
Windows Subsystem for Linux (for Windows 10 only) - https://docs.microsoft.com/en-us/windows/wsl/install-win10

Cygwin - https://www.cygwin.com/

WSL and Cygwin require some level of user competence to configure, so if that is not of interest, we definitely recommend MobaXterm as the drop-in replacement.

Support

Please let HMS Research Computing know if you experience any trouble with using two-factor authentication: rchelp@hms.harvard.edu