Two Factor Authentication FAQ

- Basic information
  - When will O2 require two factor authentication?
  - Why is two factor authentication now required for logging to O2?
  - What do I need to do to set up two factor?
  - I already have two-factor set up using Duo for Harvard Key. Can I use this for authentication on O2?
  - How do I test logging in with two factor authentication to O2?
  - How do I add a new device or modify existing 2FA settings?
  - I'm getting the error “Your account has been locked out due to excessive authentication failures.” What do I do?

Examples
- ssh
- scp/sftp/rsync
- SFTP/SCP applications like Filezilla, WinSCP, and Transmit

Basic information

When will O2 require two factor authentication?

Since Monday, December 3rd, 2018, two factor authentication has been required to connect to O2 (o2.hms.harvard.edu), any O2 login host (e.g. login01.o2.rc.hms.harvard.edu), the transfer cluster (transfer.rc.hms.harvard.edu), or orchestra.med.harvard.edu (which simply redirects to the O2 cluster) from outside the HMS network. For a detailed list of where two factor authentication is required from, please reference the table here.

Why is two factor authentication now required for logging to O2?

Due to increased hacking attempts on O2, it is necessary to take increased security measures to protect user accounts and research data. We are following the industry standard of adding extra layer of authentication, as passwords can be compromised. Likewise, Harvard FAS’ Odyssey cluster has required 2-factor authentication for a number of years. We are using the Duo application to manage the two factor authentication process.

What do I need to do to set up two factor?

You'll need to register your device (mobile phone is recommended) with Duo for HMS to be able to authenticate using security codes. You can receive these security codes through a phone call, a text message, or through the Duo mobile app. If you already use Duo for the HMS VPN, then no action is needed. However, if you only use Duo with Harvard Key (not HMS), then you will need to set up a separate HMS Duo profile. First, connect via ssh to o2.hms.harvard.edu like you normally would, and you will receive a unique web address to register for HMS Duo:

```
DESKTOP:~$ ssh abc123@o2.hms.harvard.edu
Password: [input your account password]
Please enroll at https://api-2f8a17a9.duosecurity.com/portal?code=443789224a30udsihdj8a&akey=DAlUI3JAB2FHDJKS7MJRQ0G
```

You can copy your unique web address from the terminal application paste into the address bar of your web browser (e.g. Google Chrome), and follow the prompts to register.

Please contact us at rchelp@hms.harvard.edu if you have any trouble setting up Duo.

I already have two-factor set up using Duo for Harvard Key. Can I use this for
authentication on O2?

Unfortunately, no, we cannot use Harvard Key Duo profiles for two-factor authentication on O2. O2 cluster accounts use the HMS eCommons credentials, which are distinct from Harvard Key. To register your phone/device with Duo for HMS, you can ssh to o2.hms.harvard.edu, which will generate a web address that you can use to register for HMS Duo. See the previous answer for more detail.

How do I test logging in with two factor authentication to O2?

You can connect to o2.hms.harvard.edu to test your two factor authentication. If you have already enrolled in Duo for HMS, you will receive a “Duo two-factor login” message after entering your eCommons password. You can select from the available methods (push, phone call, SMS) to authenticate by. Detailed instructions are located here. If you have not enrolled in Duo for HMS, you will receive a unique link to register through.

Please contact us at rchelp@hms.harvard.edu if you encounter any errors using two factor authentication.

How do I add a new device or modify existing 2FA settings?

You can connect to https://secure.med.harvard.edu and authenticate with your regular credentials. When prompted for the two factor authentication step you will also be presented (on the left side of the screen) with option to add a new device or modify existing settings.

I’m getting the error "Your account has been locked out due to excessive authentication failures." What do I do?

If you have more than 10 consecutive failed Duo login attempts, such as through a script or some other automated task, your Duo account will be locked. The account will automatically be re-enabled in 60 minutes (1 hour), assuming you stopped the script/process that is trying to login multiple times. Otherwise, the account will keep locking and unlocking continuously.

Examples

ssh

On and after December 3rd, there is simply an additional step to connect via ssh to the O2 cluster at o2.hms.harvard.edu, any O2 login hosts (e.g. login01.o2.rc.hms.harvard.edu), or the transfer cluster at transfer.rc.hms.harvard.edu from outside of the HMS network. You can connect via ssh as you normally would; after entering your eCommons password you will now see a new message about "Duo two-factor login". This Duo message will prompt you to enter a passcode or to select which method to authenticate by. You can choose to authenticate via Duo Push (in the Duo mobile app), through a phone call, or by entering a passcode that is sent via SMS to your phone. After confirming your login by one of the previous methods, you will see the familiar “Welcome to O2 (Orchestra 2)!” message and will have finished logging into the cluster.
DESKTOP:~$ ssh abc123@o2.hms.harvard.edu
Password: [input your account password]
Duo two-factor login for abc123

Enter a passcode or select one of the following options:

1. Duo Push to XXX-XXX-1234
2. Phone call to XXX-XXX-1234
3. SMS passcodes to XXX-XXX-1234

Passcode or option (1-3): 1

Pushed a login request to your device...
Success. Logging you in...
Welcome to O2 (Orchestra 2)!

scp/sftp/rsync

Commands like scp, sftp, or rsync will still work as expected when using the transfer cluster transfer.rc.hms.harvard.edu. Once you submit the scp/sftp/rsync command to transfer data, you will receive a notification via your default Duo method (e.g. push, phone, sms) to authenticate if you are connecting from outside the HMS network. If you don’t have a default DUO Method setup, then all scp/sftp/rsync or similar non-interactive commands will just hang.

Please visit this page on how to setup default duo method. For more information on transferring data to/from O2, please reference this page.

DESKTOP:~$ sftp abc123@transfer.rc.hms.harvard.edu
Password: [input your account password]
# now Duo will contact you via your preferred method
# once you’ve successfully authenticated, you will be connected:
Connected to abc123@transfer.rc.hms.harvard.edu.
sftp>

Additionally, when using scp or sftp from the command line, you can also configure ssh parameters as well. This is useful for if you need to set up keep-alives to hold the process open, for example (see below for graphical options):

DESKTOP:~$ scp -o TCPKeepAlive=yes abc123@transfer.rc.hms.harvard.edu

For more keep-alive options, you can try some settings on this page (use them with -o in the above command).

SFTP/SCP applications like Filezilla, WinSCP, and Transmit

Transferring data to or from O2 using the transfer cluster (transfer.rc.hms.harvard.edu) via an SFTP/SCP application like Filezilla will require two factor authentication from outside of the HMS network. For information on transferring data to/from O2, please reference this page.

When you connect to transfer.rc.hms.harvard.edu with Filezilla or an equivalent program, your default Duo method will be used to authenticate. If Duo push is your preferred method, then you’ll get a notification from the Duo app, or if a phone call is your preferred method, you’ll get a call, etc. Once you have confirmed via Duo, you will be able to transfer files using your SFTP/SCP application.

In order to reduce the number of times you need to authenticate via Duo, you can enable the keep-alive option in your SFTP/SCP application. In FileZilla, this is located under Settings > Connection > FTP. Click the “Send FTP keep-alive commands” checkbox to enable sending keep-alive commands to retain your FileZilla connection for longer periods of time (and prevent needing to authenticate with Duo for your next transfer):
The equivalent option for enabling keep-alive commands in WinSCP is under the Advanced Site Settings menu, under Connection:

- **Transfer Mode**
  - Passive (recommended)
  - Active
  - Allow fallback to other transfer mode on failure

If you have problems to retrieve directory listings or to transfer files, try to change the default transfer mode.

**FTP Keep-alive**
- Send FTP keep-alive commands

A proper server does not require this. Contact the server administrator if you need this.

Transmit requires modification of several settings to reduce the number authentication requests via Duo. Under Preferences > Advanced, select "Try to keep idle connections alive", as well as Preferences > Advanced > Advanced Server Settings > select "Tickle server during long transfers". You can also increase the number of seconds specified in "Connect Timeout" under Advanced Server Settings.
Additionally, Transmit takes advantage of Mac's App Nap, which can extend your battery life by putting inactive applications into a suspended state where they aren't able to use system resources. If App Nap is enabled for Transmit and the application is put into the background, you will get a Duo two-factor authentication request once you move Transmit to the foreground and try to transfer files to or from O2. You can prevent Transmit from using App Nap by running in your local terminal:

```
$ defaults write com.panic.Transmit NSAppSleepDisabled -bool YES
```

Caveat:

It's worth noting that all of these tools (and probably more) will behave as expected only if you are doing typical drag-and-drop activities inside the open session. If you are a user that uses a file manager to make edits to files in order to circumvent having to use a terminal-based text editor, if you perform some action such as right-click edit, then save your edits afterward to re-upload to O2, you WILL be prompted to authenticate every single time you do this. This is because these programs typically open brand new connections to deal with such operations, which the cluster interprets to be brand new log-ins. The workaround to this is obviously to only perform drag-and-drop operations, as these use the existing open connection.

Of particular note, MobaXterm will prompt you for re-authentication every time even though you are performing a drag-and-drop activity.

We are looking into potential configuration settings or alternate offerings that may change the above behavior, and will modify this page accordingly if anything is found.

If your workflow is impacted by this (e.g. a local edit/re-upload workflow), it is strongly recommended that you find some alternate means of file editing that you are comfortable with. `nano` is a solid entry-level terminal-based text editor, but is much less feature-rich than other programs such as `vim` or `emacs`, which have non-trivial learning curves. If you absolutely must use the mouse in your editing, you can download certain text
editors with Linux support directly to O2 (such as Sublime Text), and use them over an active X11 connection. You will experience some latency, especially as the file you are looking at increases in size, but you will be able to edit your file and have full mouse capabilities. If you have questions about this option, please contact us (see below) and we can assist you in setting this up in your local cluster environment).

Other use cases not detailed here

If your use case was not illustrated above and you would like guidance on how to prepare for the O2 two factor rollout, please contact us at rchelp@hms.harvard.edu ASAP. For example, if you have an automated script that copies data to O2, or is ssh-ing to O2 to run scripts or submit jobs, your scripts will likely break Monday, December 3rd.