CONNECTING TO THE IPSEC VPN USING MULTIFACTOR

It is now necessary for *all users* of the Pitt IPSec VPN service as of May 2017 to use the Duo Multifactor login. To use the Multifactor IPSec VPN, you need to have these things already in place:

- **A VPN role to access, such as "phyast_rsrch"**
  - If you do not already have this, e-mail phyast-itsupport@pitt.edu, stating which resources you need to access
  - Note: not all department resources are available via the IPSec VPN.
- **The PSK of the VPN role that you need to access**
  - This is also called a "Shared Secret" or "Group Password"
  - If you do not already have this, e-mail phyast-itsupport@pitt.edu, stating which VPN role you need to access
- **Multifactor already set up on your Pitt account**
  - If you do not already have this, see http://technology.pitt.edu/multifactor for more details, or contact the Pitt Help Desk

Duo hardware token (optional)

General instructions

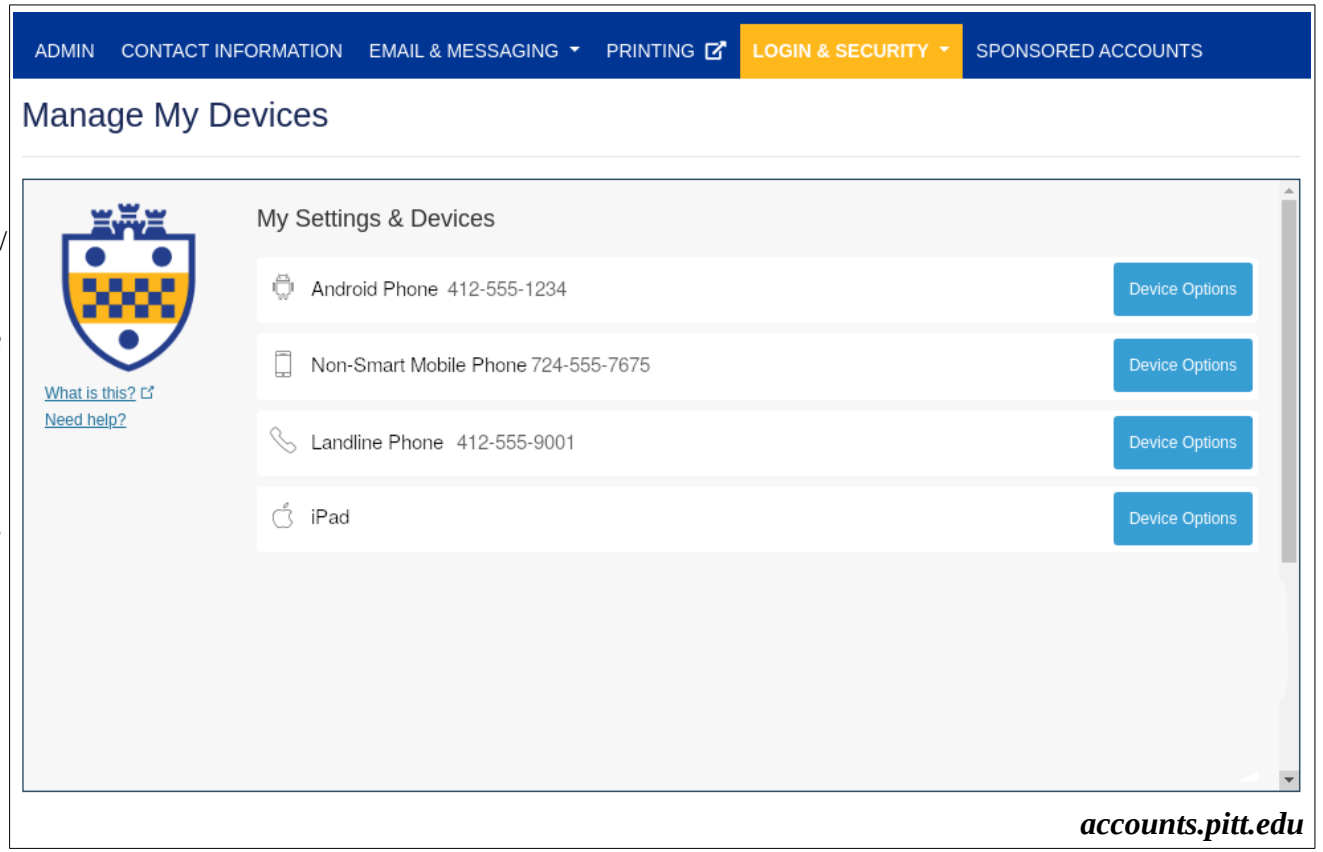
When you are asked for your Pitt password during the login to the IPSec VPN, you will need to add additional information to the end of your password to activate the Multifactor login. Here is what you need to type, depending on which method you wish to use:

- **Push method**
  - Type your password, then a comma, then the word "**push**" (no quotes, no spaces).
  - If you have the Duo app installed on your smartphone, and it is the primary device set up on your account for Multifactor, you will receive the Push notification on that phone.
  - Once you approve the notification, you will be logged into your VPN role.
- **Phone call method**
  - Type your password, then a comma, then the word "**phone**" (no quotes, no spaces).
  - You will receive a phone call from the Multifactor phone service on the primary phone number set up on your account for Multifactor, regardless of whether it is a landline or a mobile phone.
  - Once you hit "1" on your phone to approve the login, you will be logged into your VPN role.
- **SMS method**
  - Type your password, then a comma, then the letters "**sms**" (no quotes, no spaces).
  - The password prompt will re-appear, and possibly suggest that the authentication attempt has failed. *This is normal*.
  - You will receive a text message from the Multifactor service containing a code on the primary mobile phone number set up on your account for Multifactor.
  - Proceed to the next method…
- **Code method**
  - You can generate a numeric code four ways:
    - SMS (see above)
    - The Duo App on your smartphone
    - The Duo hardware token
    - A 24-hour emergency key as given by the Pitt Help Desk (412-624-4357)
  - Type your password, then a comma, then your code (no spaces).
  - If your password and code is correct, you will be logged into your VPN role.
- **Don't-add-anything**
  - If you do not put a comma and a method or code after your password, it will attempt a Push method to the first Push-capable device in your list of Multifactor devices.

– Gracie Jane Gollinger, phyast-itsupport@pitt.edu

Advanced instructions

It is possible to work with multiple multifactor devices in a manner similar to what is stated above.



- **Checking Your Multifactor Devices**
  - Log into accounts.pitt.edu.
  - Click on “Login & Security”, then select “Add/ Modify Pitt Passport Devices”.
  - You will find the list of devices, with their order, in a manner similar to the graphic on the right.
- **Different phone call method**
  - Type your password, then a comma, then the word “**phone2**” (no quotes, no spaces).
  - You will receive a phone call from the Multifactor phone service on the second phone number set up on your account for Multifactor, regardless of whether it is a landline or a mobile phone.
  - In the example given to the right, a call will be received on the “Non-Smart Mobile Phone” instead of the first “Android Phone”.
  - If instead the word “**phone3**” were entered, a call would be received at the “Landline Phone”.
  - If the word “**phone4**” were entered given the setup above, the authentication will fail, and the connection would have to be re-established, because there is no fourth phone call-capable device listed.
- **SMS method**
  - Type your password, then a comma, then the letters “**sms2**” (no quotes, no spaces).
  - The password prompt will re-appear, and possibly suggest that the authentication attempt has failed. *This is normal*.
  - You will receive a text message from the Multifactor service containing a code on the second mobile phone number set up on your account for Multifactor.
  - In the example shown above, a text would be received on the “Non-Smart Mobile Phone” instead of the default “Android Phone”.
  - Proceed to the Code Method as listed on the first page.
  - If “**sms3**” were entered as above, the authentication will fail, and the connection would have to be re-established, because there is no third text-capable phone listed.
- A Push method currently only works for the first Push-capable device. Therefore, assuming the “Android Phone” has the Duo app installed and is set up for a Duo Push notification, the “iPad” would not be able to receive a Push from this method.
- YubiKeys and other U2F devices are not supported.

– Gracie Jane Gollinger, phyast-itsupport@pitt.edu