Instructions for Managing Your Multifactor Authentication Devices

<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>After passing primary authentication for <strong>CAS, YaleConnect</strong> or <strong>VPN via the browser</strong> (typing <a href="https://access.yale.edu">https://access.yale.edu</a>), the Duo second factor screen displays.</td>
</tr>
</tbody>
</table>

- Select the left menu item “My Settings and Devices”
- Upon selecting the menu item “My Settings and Devices” a blue banner will appear at the bottom of the screen indicating that you must authenticate prior to managing your devices.
- Choose your authentication method.

**Note:** The blue banner will act as a status indicator in this screen of the device management process.
Upon successful authentication, you will be able to set your default device, and whether you want that default device to automatically receive a “push” or “phone call” when you log in.

In addition, you will see a listing of all your devices with a “Device Options” button for each one.

Upon selecting a “Device Options” button you will see a range of options that you can perform. These include:

- A “delete” function represented by a red button with a trash can.
- A “close” function represented by a grey button with an up arrow.
- A “Change Device Name” button
- Those devices that can run the Duo application will also have the option to “Activate Duo Mobile”.

The green banner will act as a status indicator in this screen of the device management process.

Users cannot manage devices through the VPN Client.

Users may remove (but not add) hardware tokens from the device management portal as well.

Notes

- Users cannot manage devices through the VPN Client.
- Users may remove (but not add) hardware tokens from the device management portal as well.