## Instructions for Managing your second factor devices for Multifactor Authentication

<table>
<thead>
<tr>
<th>Step</th>
<th>Action/Result</th>
</tr>
</thead>
</table>
| 1    | After passing primary authentication for CAS, YaleConnect or VPN via the browser typing [https://access.yale.edu/mfa](https://access.yale.edu/mfa), the Duo second factor screen displays.  
Select the authentication type, changing the default device if needed, and then click on the “Manage Devices” button. If choosing to authenticate via smartphone or tablet, a message displays that a login request has been pushed to your phone; approve the request. Alternatively, choose another method of authentication.  
Clicking the **Manage Devices** button prompts the user to complete two-factor authentication, then displays the device management portal. |
| 2    | From this portal your users can:  
• enroll a new mobile phone, tablet, or landline by clicking “Enroll another Device”  
• rename an existing phone or tablet device via the actions button  
• activate Duo Mobile via the actions button  
• set a phone or tablet device as the default for Duo Push and phone call actions button  
• remove an existing device via the actions button |

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