Managing Your Passwords

Dan Pucillo on January 14, 2020

Managing Your Passwords

Strong password management practices are critical to keeping you, your work, and UCSF secure. Most systems at UCSF (email, wireless, Pulse VPN, and many applications) use your network login and/or email credentials to authenticate. UCSF provides tools to help you manage your passwords, to keep you safe and working. Learn more about:

- UCSF Password Management Tool
- Password Change Instructions
- Keeper Password Vault

UCSF Password Management Tool

Use the UCSF Password Management Tool to change your password and unlock your account in the event of a lock out. You can also enroll a mobile device to unlock your accounts while you are off the UCSF network.

- About the UCSF Password Management Tool [1]
- How to Enroll in and Use the UCSF Password Management Tool [2]
- Logging into your UCSF account for the first time [3]
- Password FAQ [4]

REMINDER: Once you have updated your network password, sign in as soon as possible to all your mobile devices, and use your new password to sign in to your WiFi and mobile email apps. Doing so will help prevent getting locked out of your account. For complete instructions on how to do this on either a Windows machine or a Mac, please see below. For information on specific applications, please see the list of links to the left.
Password Change Instructions

1. Be prepared to complete the process in one sitting without interruption. Gather your mobile devices.
2. Think about what you want your new passphrase to be?a short sentence that?s easy to remember but hard to guess and meets the new requirements: at least 12 characters from 3 of 4 categories (uppercase, lowercase, numbers, symbols). This is the passphrase you will use any time you connect to the UCSF network?Windows or Mac each time you log into your machine, Pulse VPN when you work remotely, MyAccess, etc.
3. On your computer, enroll in the UCSF Password Management Tool [7] by setting up your security questions. You?ve successfully enrolled if you make it to the Password Tool main menu. (You can find comprehensive enrollment steps in this guide under ?Enroll and log in [2].?)
4. From the Password Tool main menu, select ?Register mobile device.? In the Apple App Store or Google Play app search for ?Hitachi ID Mobile Access App? and download the app to your phone.
5. OPTIONAL - Link your mobile device by using the Hitachi ID Mobile Access app to scan the QR code generated by the Password Tool. On your computer screen, you will see a message telling you your device has been activated. (You can find comprehensive mobile steps in this guide under ?Register your mobile device [2].?). Linking your mobile device will allow you to manage your UCSF password using the app on your device, but you are also able to manage your password without using the stand-alone app.
6. Close all programs on your computer (Outlook, etc.) except for the Password Tool. Close all apps on your phone and/or tablet.
7. Put your mobile devices into Airplane Mode.
8. Go back to the Password Tool main menu and select ?Change passwords.? Enter and confirm your new 12-character passphrase.
9. Hit Ctrl+Alt+Delete on Windows or Shift-Opt-Cmd-Q on Mac and sign out of your computer.
10. Sign back in with your new 12-character passphrase. If you have the option to ?Use my Windows user account? check that box.
11. Now you need to update your password in several places to avoid being locked out of your UCSF account.
   1. UCSFwpa WiFi. Follow these instructions for Windows [8] or Mac [5].
   2. Outlook. Open Outlook and enter your new passphrase when prompted.
   3. Any other programs that require your UCSF account such as Jabber [8] or Pidgin [9].
   4. We also recommend clearing your cache and cookies across browsers and deleting passwords you?ve saved in browsers. Find comprehensive guides on the left sidebar under ?Related Pages [10].?
12. Take your phone off airplane mode. You need to update your password on your mobile devices now to avoid being locked out.
   1. UCSFwpa WiFi. If your device was previously connected to UCSFwpa under your old password, you will need to start by selecting ?Forget this Network.? Reconnect with your new passphrase. Follow ?UCSFwpa Instructions ? iPhone/iPad [11]? or ?UCSFwpa Instructions ? Android
2. UCSF email on your phone. See the Email Online Mobile page for information.
3. Any other apps that require your UCSF account.
13. Repeat the process for each of your devices as you take them off airplane mode one at a time.
14. Congrats! You’re done. Use your new passphrase any time you connect to the UCSF network? Windows or Mac each time you log into your machine, Pulse VPN when you work remotely, MyAccess, etc.
15. Contact the IT Service Desk if you have questions or become locked out: 415/514-4100 or help.ucsf.edu or itservicedesk@ucsf.edu.
   ○ If you are a BCHO customer, contact the BCHO Help Desk: 510.428.3885 x4357

Keeper Password Vault

Use Keeper Password Vault free of charge to manage your passwords simply and intuitively by setting up one Master Password. Keeper also generates strong passwords, auto-fills passwords across your apps and sites, and organizes passwords on all platforms and devices.

Please note: Keeper is intended for UCSF work purposes only. If you do use it for personal accounts, when you separate from UCSF, this information will be immediately removed and irretrievable.

- About Keeper Password Vault at UCSF
- How to Enroll in and Use Keeper Password Vault