



Password security starts with a strong password. Ascension requires all associates to create and protect a new 12 character password to log into the Ascension network. This initiative is crucial in enhancing our defenses against potential cyber threats and ensuring the protection of our valuable information.

IMPORTANT: It is highly recommended that you change your password at the end of the day. Once the password is changed, there could be up to a 90 minute timeframe for applications to sync with the new password and you may not be able to access these applications during this time.

New password requirements

- **Length** : At least 12 characters.
- **Complexity**: Includes three of the following:
 - lowercase letters
 - uppercase letters
 - Numbers (0 - 9)
 - Special characters (!, \$, #, %).
- **Expiration** : Passwords must be changed at least every 90 days.
- **Re-use** : Do not re-use your password. Create a new one every time.
- **Tips**:
 - Use passphrases instead of words (for example, let'stlunch@11?)
 - Make it hard to guess. Avoid information easily found on public documents or social media profiles. • Avoid using the same password across multiple sites.
 - Don't write down or share your password with anyone.
 - Strong passwords are unique; don't use common phrases.

How to change your password

Scenario 1: Use for Ascension-issued Windows devices

Follow these steps to change your password if you are the sole user of your device:

1. Log in and ensure you are connected to the Ascension network
 - a. If onsite, connect to your facility's network.
 - b. If remote, connect following these **VPN instructions**.
2. Press CTRL+ALT+DEL at the same time on your keyboard.
3. Click **Change a Password**.
4. Enter your current password, then create and confirm a new one.

Scenario 2: Use in all other cases

Follow these steps if you use a MacOs device, a shared workstation, auto-logon device or another non-assigned device common in patient care areas

1. Open the Ascension Health Password Manager (AHPM) tool. Most computers have a desktop shortcut, or visit <https://ahpm.ascension.org/> .
2. Enter your Ascension email address and current password.

3. Select your domain (if you are unsure, choose one closest to your work location).
4. Complete the Captcha.
5. Click the blue Login button.
6. If this is your first time using the password manager tool, you will be prompted to answer four security questions and enroll.
7. You will be prompted to accept the DUO Multi-factor authentication on your phone.
 - a. You will need to be enrolled in Duo to proceed.
 - b. For more details on Duo, visit the Duo multifactor authentication site and FAQ document or contact the Service Desk (ensure you are on the Ascension network or VPN to access these links).
8. Change your password by entering your old password and the new one.
9. Click Change Password .

IMPORTANT Reminder for mobile device users: Log in to Wi-Fi

After changing your password, if you are using a mobile device at an Ascension location, you MUST re-login to Ascension's Wi-Fi on your mobile device to avoid account lockouts.

1. On your phone, go to Settings > Wi-Fi .
2. Tap the info button next to the network.
3. Select Forget This Network and confirm.
4. Reconnect to the network using your new credentials.

Service Desk Assistance – 877-635-0532:

- The Service Desk can only provide assistance for password or Duo Multi-factor Authentication by phone
- It is highly recommended to have DUO Multi-factor Authentication established to ensure a seamless password reset process. If you do not have DUO established, these options are available:
 - Google video call - Service Desk will send an email invite to a corporate or personal email address so that you may show the Service Desk analyst a form of identification such as your corporate badge, driver's license, state issued ID, passport or military ID.
 - Login to a computer with a camera and select Google video link email.
 - Login on your mobile device and select Google video link email.
 - Badge Selfie
 - Take a selfie holding your badge and email to the Service Desk
 - Authentication may not occur if badge does not accurately reflect name (ie nicknames, maiden/married name changes)