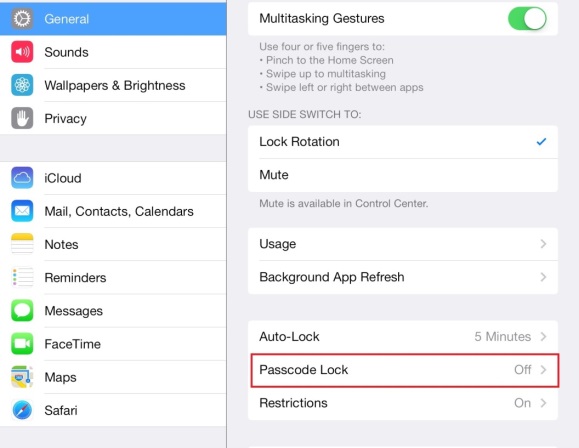
* + 1. The ABA Model Rules of Professional Conduct require lawyers to use technology competently and to consider the risk and sensitivity of the way confidential client information is handled.
    2. Many legal professionals have incorporated iOS devices into their daily workflows, whether simply to manage their email and contacts or to perform more extensive document work.
    3. To help protect against the loss of firm, client, or personal information, it’s a best practice to enable a number of security measures on your iOS devices.

# Implement a Strong Passcode

* + 1. The strong passcode option on your iPhone\* and iPad\* allows you to create a passcode that incorporates letters, numbers, and even special characters. Adding a strong passcode to your device helps strengthen protection against unauthorized access.
    2. To create a strong passcode:
       1. Open the **Settings** app on the iOS device.
       2. To display the passcode options, from the **General** settings, tap **Passcode Lock**.



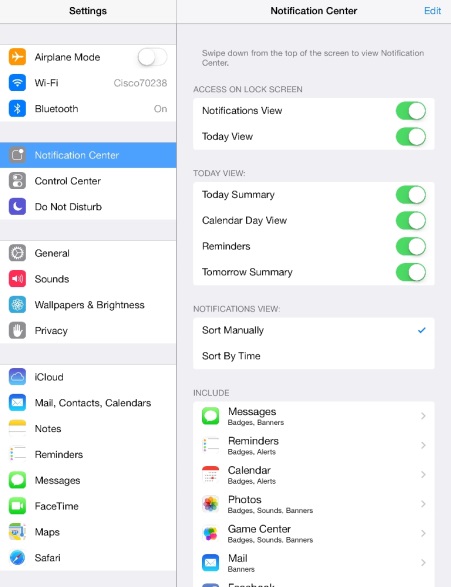
* + - 1. To create a more secure passcode, begin by turning off **Simple Passcode** by sliding the button to the left.



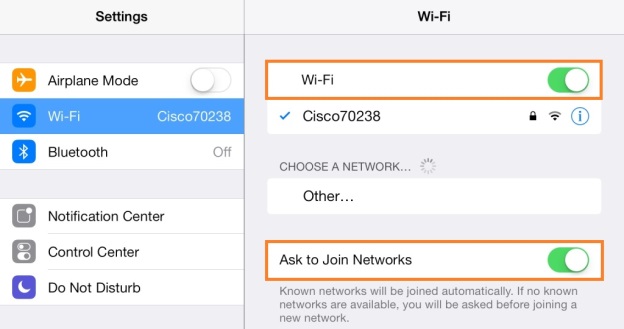
* + - 1. Tap **Turn Passcode On** and enter a longer passcode containing a combination of upper and lower case letters, numbers, and special characters.
      2. Tap **Next**, reenter the passcode, and tap **Done** when finished.
    1. To further strengthen the passcode settings on your iOS device:
* Tap the **Require Passcode** setting and select **Immediately**.
* Slide the **Erase Data** button to the right to enable automatic data erasure after 10 failed passcode attempts.
* From the **General** settings, tap **Auto-Lock** and select the lowest number to lock the device when inactive.

# Disable Notifications, Wi-Fi, Bluetooth, and Siri

* + 1. Even when locked, an iOS device can display a variety of sensitive information. If your device isn’t within your control, or the screen is visible to others, this feature can inadvertently disclose confidential information.
    2. To ensure that your device doesn’t automatically connect to an unsecure location or limit the possibility of unauthorized access to your device, turn off Wi-Fi and Bluetooth when not in use. Change Siri settings to prevent bypassing a locked screen to access information.
    3. To disable locked screen notifications:
       1. Open the **Settings** app and select **Notification Center**.
       2. Slide the **Today View** button to the left.

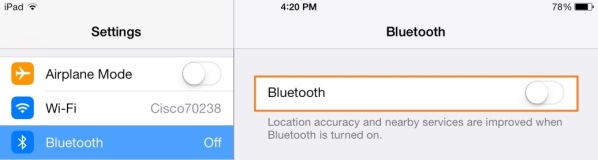


* Individual components of the **Today View** can be customized by sliding the selected button to the left in the **Today View** category.
* To customize the information shown by individual apps, select the app and disable notifications in the **Alerts** category.
  + 1. To turn off Wi-Fi:
* Open the **Settings** app , select **Wi-Fi**, and slide the **Wi-Fi** button to the left.



To ensure you do not automatically connect to an unsecure network, open the **Settings** app, select **Wi-Fi,** and enable **Ask to Join Networks** by sliding the button to the right.

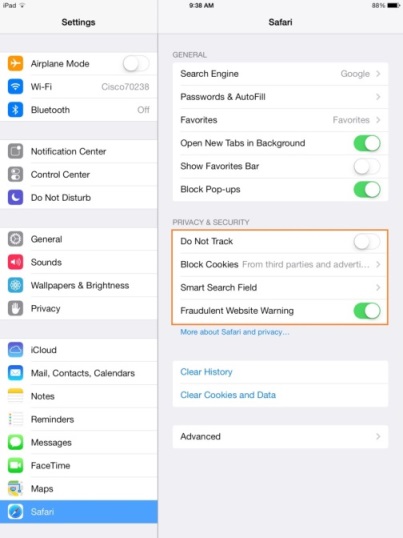
* + 1. To turn off Bluetooth:
* From the Settings screen, tap **Bluetooth** and slide the **Bluetooth** button to the left.



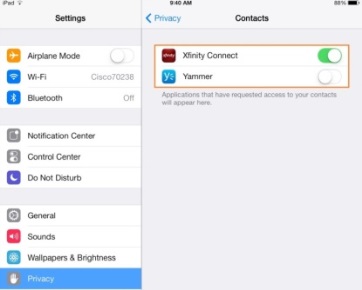
* + 1. To block Siri from bypassing the screen lock passcode:
* From the **Settings** app, tap **General**, select **Passcode Lock,** and slide the Siri button to the left.
  + 1. To turn off Siri:
* From the **General** screen, tap **Siri** and slide the **Siri** button to the left.

# Keep Data Private

* + 1. Additional security measures to consider when using an iOS device include keeping your Internet browsing private, turning off location tracking, and managing the privacy settings on all apps, including social media apps.
    2. To secure Internet browsing to prevent history tracking, block cookies, and warn of potentially fraudulent websites:
       1. Tap the **Settings** app and from the Settings category, select **Safari**.
       2. In the Privacy & Security section, set security settings preferences for using the browser.

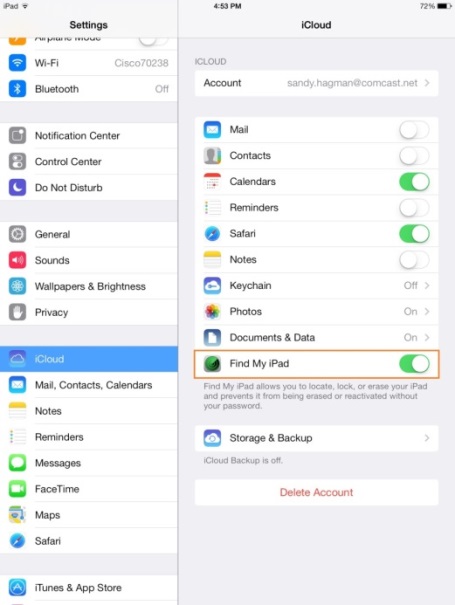


* + 1. Many apps use your GPS location to provide you with location-based information. Location tracking can be turned off globally for all apps or managed for apps individually.
    2. To set location services:
       1. Open the **Settings** app, select **Privacy,** and tap **Location Services**.
       2. To turn off location services for all apps, slide the **Location Services** button to the left.
       3. To turn off location services for a specific app, slide the appropriate button to the off position.
    3. To ensure that work-related emails are always sent from the correct account, designate your firm mail account as the default.
    4. To designate a default mail account:
       1. From the **Settings** app, tap **Mail, Contacts, Calendars**.
       2. Under the Mail category, tap **Default Account** and select an account.
    5. To control which apps have access to your contact information:
       1. Tap the **Settings** app, select **Privacy**, and tap **Contacts.**
       2. To turn off access to contacts, select an app and slide the button to the left.



# Find iPhone or iPad

* + 1. If an iOS device goes missing, use iCloud or the Find My iPhone or iPad app to display the location of the missing device on a map.
    2. To activate the Find My iPhone or iPad app:
       1. Open the **Settings** app , select **iCloud**, and slide the **Find My iPad** (or iPhone) button to the right.



# Enable Restrictions

* + 1. Use the **Restrictions** option on your iOS devices to lock down automatic launching of Safari, FaceTime, and other applications. Restrictions can also prevent the installation or deletion of apps or changes to an account. Because a passcode is needed to apply or remove restrictions, device security is further enhanced.
    2. To enable restrictions:
       1. Open the **Settings** app, select **General** and tap **Restrictions**.



* + - 1. To turn on restrictions, tap **Enable Restrictions**, enter a passcode, and confirm it.
      2. Set restrictions for access to apps, allowed content, and privacy.

# Update Software

* + 1. Keep your iPhone and iPad up-to-date with the latest iOS software and patches. Operating system updates often include bug fixes, address security holes, and include additional functionality related to security protections.