



DFIR Review Showcase: iOS Settings Display Auto-Lock & Require Passcode

By:

Scott Koenig (Nevada State Police)

From the proceedings of

The Digital Forensic Research Conference

DFRWS USA 2022

July 11-14, 2022

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment.

As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

<https://dfrws.org>

iOS Settings Display Auto-Lock & Require Passcode

A review of some iPhone settings and the corresponding property list (plist) that stores those settings

Scott Koenig

Digital Forensic Analyst with Nevada State Police



Background

- **A fellow analyst contacted me and asked if I've conducted research into setting files that store**
 - **iPhone display auto-lock setting; or**
 - **Setting that controls the amount of time that passes before the device requires a passcode**







Background

- The fellow analyst provided the file and location that might contain the setting he was interested in:

`\private\var\mobile\Library\UserConfigurationProfiles\PublicInfo\`

`PublicEffectiveUserSettings.plist`

After reviewing the file, it appeared to contain several device settings

Icon	FileName	FileExtension	FileSize_Bytes	FileSize_MegaBytes	LastModified
	MCMeta.plist	.plist	72	0	2022-02-25 17
	NamespacedUserSettings.plist	.plist	42	0	2022-07-03 12
	PublicEffectiveUserSettings.plist	.plist	9879	0	2022-04-27 09
	Truth.plist	.plist	10301	0	2022-07-03 12

```
PublicEffectiveUserSettings.plist
Tree View XML View Hex
0) intersection
1) restrictedBool
2) restrictedValue
  0) ratingMovies
  1) maxInactivity
     0) value
     | 120
     1) rangeMinimum
     | 30
  2) passcodeKeyboardComplexity
  3) allowedGameCenterOtherPlayerTypes
  4) minLength
  5) ratingApps
  6) enforcedSoftwareUpdateDelay
  7) ratingTVShows
  8) safariAcceptCookies
  9) simplePasscodeComplexity
 10) maxGracePeriod
     0) value
     | 0
     1) rangeMaximum
     | 14400
     2) rangeMinimum
     | 0
3) union
```

Background

- **Why was it important to conduct the research and publish the findings, via a Blog and via DFIR Review?**
 - **Validate analysis findings that would be included in a findings report**
 - **Confirms the storage location of the plist in different device models and iOS versions**
 - **Artifact could provide insight into how long a device screen was on and or unlocked**
 - **User locking the device or max time reached then locked**
 - **Vehicle collisions**
 - **Last device usage prior to a death**

Artifact Research

Artifact Research

- **Artifact research considerations:**
 - **Searching available resources for prior research**
 - <https://dfir.pubpub.org/>
 - <https://scholar.google.com/>
 - <https://discord.com/invite/digitalforensics>
 - <https://startme.stark4n6.com> – Kevin Pagano
 - <https://aboutdfir.com/>
 - <https://www.dfir.training/>
 - Other analyst public blogs and many other resources
 - **Asking questions on listservs or other forums**
 - **Communicating with others who might have unpublished research**



Google Groups



Data Collection

Data Collection

- **Data collection considerations:**
 - **Device model and operating systems available for research**
 - **Initial Research**
 - iPhone 6s Plus iOS 14.4.2 – included in the DFIR reviewed paper
 - **Supplemental Research – not included in the DFIR reviewed paper**
 - iPhone 7 iOS 15.1
 - iPhone X iOS 14.7
 - iPhone 12 iOS 16.0
 - **Forensic tools available for acquisition and analysis**
 - Cellebrite UFED 4PC & Physical Analyzer
 - Magnet AXIOM
 - Grayshift Graykey
 - ArtEx
 - Native file format viewers

iOS	14.4	iOS
14.0	14.4.1	15.0
	14.4.2	15.0.1
14.0.1	14.5	15.0.2
	14.5.1	15.1
14.1	14.6	15.1.1
	14.7	15.2
14.2	14.7.1	15.2.1
	14.8	15.3
14.2.1	14.8.1	15.3.1
		15.4
14.3		15.4.1
		15.5

***Testing &
Interpretation of Data***

Testing & Interpretation of Data

- **Testing & interpretation of the data considerations:**
 - **Locating artifact source file**
 - This step could take a considerable amount of time to complete
 - Community benefit of having these types of writeups published on DFIR Review
 - **Number of tests needed for repeated results in source file**
 - This could cause the research to have limitations during testing and the number of conclusions that could be made during the findings

Testing & Interpretation of Data

During research and testing, I made changes to the device settings six times. Below are the device settings followed by the values listed in the property list:

Test One

No passcode

Display Auto-Lock = 2 minutes

Require Passcode = not set

maxInactivity value = 120

maxGracePeriod value = 0

Test Two

6-digit passcode

Display Auto-Lock = 30 seconds

Require Passcode = immediately

maxInactivity value = 30

maxGracePeriod value = 0

Test Three

6-digit passcode

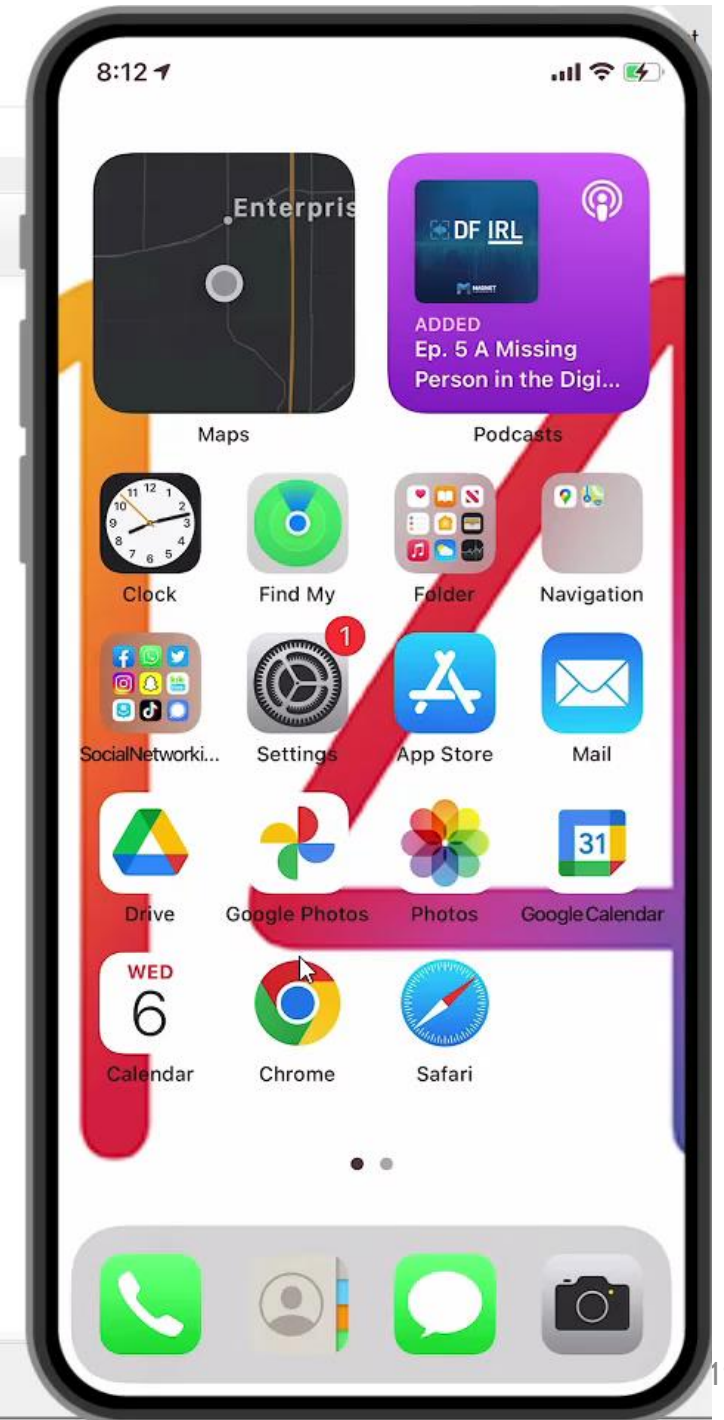
Display Auto-Lock = never

Require Passcode = 1 minute

maxInactivity value = 2147483647

maxGracePeriod value = 60

```
x PublicEffectiveUserSettings.plist
Tree View XML View Hex
0) intersection
1) restrictedBool
2) restrictedValue
0) maxGracePeriod
0) value
  | 14400
1) rangeMaximum
  | 14400
2) rangeMinimum
  | 0
1) maxInactivity
0) value
  | 120
1) rangeMinimum
  | 30
2) passcodeKeyboardComplexity
3) allowedGameCenterOtherPlayerTypes
4) minLength
0) value
  | 4
1) rangeMinimum
  | 4
5) ratingApps
6) enforcedSoftwareUpdateDelay
7) ratingTVShows
8) safariAcceptCookies
9) simplePasscodeComplexity
10) ...
\restrictedValue\ratingMovies
```



Testing & Interpretation of Data

During research and testing, I made changes to the device settings six times. Below are the device settings followed by the values listed in the property list:

Test One

No passcode

Display Auto-Lock = 2 minutes

Require Passcode = not set

maxInactivity value = 120

maxGracePeriod value = 0

Test Two

6-digit passcode

Display Auto-Lock = 30 seconds

Require Passcode = immediately

maxInactivity value = 30

maxGracePeriod value = 0

Test Three

6-digit passcode

Display Auto-Lock = never

Require Passcode = 1 minute

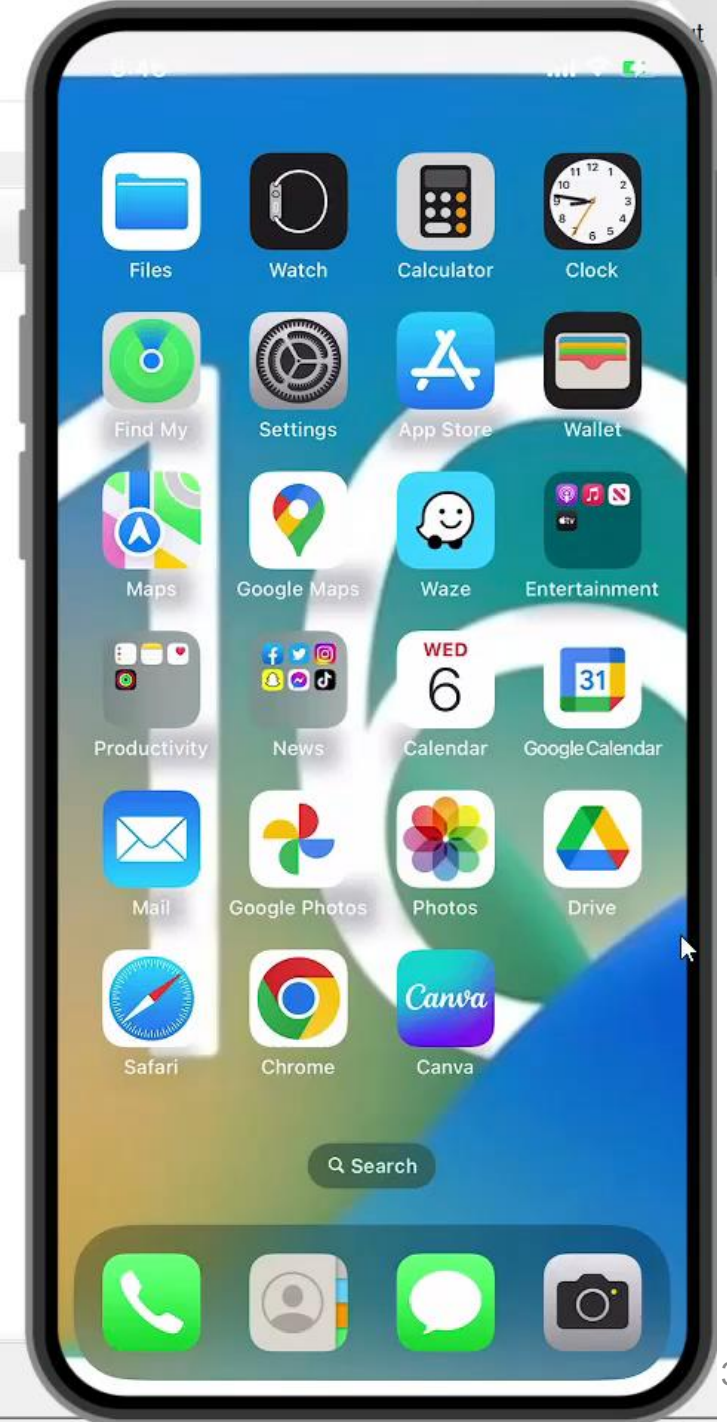
maxInactivity value = 2147483647

maxGracePeriod value = 60

008101-001814CC0E88001E

```
PublicEffectiveUserSettings.plist
Tree View XML View Hex
0) intersection
1) restrictedBool
2) restrictedValue
  0) maxGracePeriod
    0) value
      60
    1) rangeMaximum
      14400
    2) rangeMinimum
      0
  1) maxInactivity
    0) value
      2147483647
    1) rangeMinimum
      30
  2) passcodeKeyboardComplexity
  3) allowedGameCenterOtherPlayerTypes
  4) minLength
  5) ratingApps
  6) enforcedSoftwareUpdateDelay
  7) simplePasscodeComplexity
  8) ratingTVShows
  9) safariAcceptCookies
  10) ratingMovies
3) union
```

\restrictedValue\maxGracePeriod\rangeMinimum\0



Testing & Interpretation of Data

During research and testing, I made changes to the device settings six times. Below are the device settings followed by the values listed in the property list:

Test Four

6-digit passcode

Display Auto-Lock = 1 minute

Require Passcode = 5 minute

maxInactivity value = 60

maxGracePeriod value = 300

Test Five

6-digit passcode

Display Auto-Lock = 3 minutes

Require Passcode = 4 hours

maxInactivity value = 180

maxGracePeriod value = 14400

Test Six

No passcode

Display Auto-Lock = 2 minutes

Require Passcode = 5 minutes

maxInactivity value = 120

maxGracePeriod value = 300

```
PublicEffectiveUserSettings.plist
Tree View XML View Hex
0) intersection
1) restrictedBool
2) restrictedValue
  0) maxGracePeriod
    0) value
      | 300
    1) rangeMaximum
      | 14400
    2) rangeMinimum
      | 0
  1) maxInactivity
    0) value
      | 60
    1) rangeMinimum
      | 30
  2) passcodeKeyboardComplexity
  3) allowedGameCenterOtherPlayerTypes
  4) minLength
  5) ratingApps
  6) enforcedSoftwareUpdateDelay
  7) simplePasscodeComplexity
  8) ratingTVShows
  9) safariAcceptCookies
  10) ratingMovies
3) union
```

\restrictedValue\maxInactivity



Testing & Interpretation of Data

During research and testing, I made changes to the device settings six times. Below are the device settings followed by the values listed in the property list:

Test Four

6-digit passcode

Display Auto-Lock = 1 minute

Require Passcode = 5 minute

maxInactivity value = 60

maxGracePeriod value = 300

Test Five

6-digit passcode

Display Auto-Lock = 3 minutes

Require Passcode = 4 hours

maxInactivity value = 180

maxGracePeriod value = 14400

Test Six

No passcode

Display Auto-Lock = 2 minutes

Require Passcode = 5 minutes

maxInactivity value = 120

maxGracePeriod value = 300

```
PublicEffectiveUserSettings.plist
Tree View XML View Hex
0) intersection
1) restrictedBool
2) restrictedValue
  0) maxGracePeriod
    0) value
      | 14400
    1) rangeMaximum
      | 14400
    2) rangeMinimum
      | 0
  1) maxInactivity
    0) value
      | 180
    1) rangeMinimum
      | 30
  2) passcodeKeyboardComplexity
  3) allowedGameCenterOtherPlayerTypes
  4) minLength
  5) ratingApps
  6) enforcedSoftwareUpdateDelay
  7) simplePasscodeComplexity
  8) ratingTVShows
  9) safariAcceptCookies
  10) ratingMovies
3) union
```

\restrictedValue\enforcedSoftwareUpdateDelay



Testing & Interpretation of Data

During research and testing, I made changes to the device settings six times. Below are the device settings followed by the values listed in the property list:

Test Four

6-digit passcode

Display Auto-Lock = 1 minute

Require Passcode = 5 minute

maxInactivity value = 60

maxGracePeriod value = 300

Test Five

6-digit passcode

Display Auto-Lock = 3 minutes

Require Passcode = 4 hours

maxInactivity value = 180

maxGracePeriod value = 14400

Test Six

No passcode

Display Auto-Lock = 2 minutes

Require Passcode = 5 minutes

maxInactivity value = 120

maxGracePeriod value = 300

The screenshot shows a plist file viewer interface. The title bar reads 'PublicEffectiveUserSettings.plist'. The interface includes a toolbar with icons for file operations and a search box. Below the toolbar, there are tabs for 'Tree View', 'XML View', and 'Hex'. The 'Tree View' is selected, displaying a list of settings:

- 0) intersection
- 1) restrictedBool
- 2) restrictedValue
- 3) union

The background of the viewer shows a faint grid pattern. At the bottom right of the viewer, there is a legend for data types: Dictionary (blue), Array (green), Number (red), Text (purple), Boolean (orange), Data (pink), and Date (grey).

***Consider details not
researched***

Consider details not researched

- **Consider details not researched or included in the write-up:**
 - **Acquisition restrictions**
 - For the initial research I was using a jailbroken device and focused on full filesystem acquisitions and tool-based acquisitions. The DFIR reviewer mentioned in their comments that they also located the artifact plist in a normal iPhone back also.
 - **Settings not tested**
 - Initially, I did not use every variation possible and missed the fact the Face-ID switch being ON affected the number of options given for when a passcode is required. This again was picked up by the DFIR Reviewer and mentioned in their comments.
 - **Future work**
 - Updates to the research based on new devices & new operating systems.
 - When I was previously demonstrating the testing results, I mentioned I was using a device with iOS 16 which matched my original results from iOS 14 and 15, validating the article again with the new iOS
- **Use blogs to add onto the original DFIR reviewed material for community use**

DFIR Review

DFIR Review

- **Why did I use DFIR Review?**
 - **Encouraged by DFIR community mentor to have research peer reviewed**
 - **I must thank Heather Mahalik for pressuring me to do more. She pushed me to validate and then share. I would not have the knowledge or currant motivation that I now have without her being a true mentor. Thanks!!**
 - **DFIR Review allows the research to be published via blog prior to review**
 - **Given the frequency of mobile device and application updates it can be critical to get research into the hands of other analyst for their investigations**

DFIR Review

- **Why did I use DFIR Review?**
 - **Reviewers provide accurate and detailed comments and critiques**
 - **Reviewers provided feedback about my tests indicating that I only mentioned “Touch ID & Passcode” settings & that they could be “Face ID & Passcode” depending on the model of device and iOS installed**
 - **Also mentioned that I should also test on iPad**
 - **This was mentioned earlier about have availability of test devices to use during research**
 - **Last but not least...**
 - **Very self-rewarding to know that hours of work was accurate**

DFIR Review

- I would like to thank the reviewers for their time and dedication to the community. Without them this process would not be possible! Thanks everyone!!
- **Eric Eppley** (Methodology Review)
- **Anthony Knutson** (Methodology Review, Validated Review Using Reviewer Generated Datasets)
- **Johann Polewczyk** (Methodology Review, Validated Review Using Reviewer Generated Datasets)
- **Aurèle Scoundrianos** (Methodology Review, Validated Review Using Reviewer Generated Datasets)

Scott Koenig
bskoenig3347@gmail.com

Blog: <https://theforensicscooter.com/>



Twitter: @Scott_Kjr

