iOS Backups for Data Loss Prevention, Data Extraction, Data Retention, Electronic Discovery and Data Migration in Enterprise & Institutional Environments

Last updated: **March 27th, 2023**
Author: **DigiDNA - Jérôme Bédat**

1. Introduction

iMazing is the most advanced solution for backing up and managing iOS device backups, as well as browsing or extracting data from them. Our team at DigiDNA has been a leader in iOS management since 2008, and we've developed a suite of solutions to manage Apple mobile devices. Our expertise is recognized worldwide, with millions of end-users and thousands of companies and institutions worldwide using our products. We were the first company to offer solutions for managing iOS devices, and all of our development is 100% Swiss made.

Our top priority is to provide our users with reliable solutions that offer the best possible user experience while taking great care to ensure user security and privacy.

Read more about our values here:

- About DigiDNA: https://imazing.com/about
- Security & Privacy: https://imazing.com/security-and-privacy
- Privacy Policy: https://imazing.com/privacy-policy

iOS backups are necessary in various situations, particularly in enterprise or institutional contexts. They help **prevent loss of device data**. In such cases, the data must be fully restorable to an iOS device. They are also useful in cases where **data retention or archiving** is needed for legal and regulatory compliance purposes, or for **e-discovery or forensic analysis**. Such data may not need to be restorable to a device, but **because iOS devices are extremely secure, a backup is necessary to access the user data**.
In this document, we will cover important technical questions and aspects related to iOS backups and iMazing.

iOS backups should be done from a computer, either a Mac or a PC. Typically, this is done on the end-user computer or from a server. However, due to technical and user experience reasons, the latter can be more challenging to achieve when working with Apple mobile devices. Once backed up, the data can be stored either locally on the end-user computer or remotely on a NAS or any cloud storage, depending on the use case.
DigiDNA's products do not host backups or user data on any servers or cloud infrastructure. Therefore, it is the responsibility of iMazing's business or institutional customers to determine where this data should be stored on their infrastructure, either locally on computers or remotely on a NAS or cloud storage. Our team can assist organizations to define their needs and understand the best practices for securely storing and safeguarding their data when using iMazing. However, **DigiDNA bears no responsibility for data storage**.

iMazing offers a range of features to enterprises and institutions that rely on iOS backups:

- iOS Backup to prevent data loss
- Data migration
- Data extraction
- Phone evidence for court
- Data retention for compliance
- Advanced forensics analysis
- Spyware detection

Before delving into these specific topics and use cases, it's important to understand the technical aspects and their implications for user experience and technical challenges.

Since the very beginning, Apple mobile devices have been designed to be extremely secure, and their data can only be accessed through dedicated protocols. This is because the iOS device file system is not directly accessible, as it would be with other non-iOS operating systems or standard external storage devices. Apple does not provide any documented API to back up or access iOS device data. Therefore, iMazing must use the same protocols as those used by Apple applications to manage iOS devices locally, such as iTunes/Finder on macOS or iTunes/Apple Devices on Windows.

iMazing works exactly the same way as the Apple applications listed above and respects end-to-end device and user data security. **iMazing does not circumvent Apple's security in any way.** Therefore, certain technical limitations and requirements, as well as user experience issues, should be taken into consideration when using backups or accessing data from Apple iOS devices.

2. iOS backups and data extraction with iMazing

In this chapter we'll cover important aspects of iOS local backups and how iMazing leverages the Apple iOS backup protocol and what should be taken into account when using iMazing to back up iOS devices.

2.1 iOS device and computer pairing

Upon first connection via USB of an iOS or iPadOS device to the host computer, the mobile OS displays a *Trust dialog* which the user needs to acknowledge before entering the device's passcode (no biometric auth).

Once pairing is established, iMazing can communicate with iOS devices via a USB cable or a local WLAN connection. Both the computer and device must be connected over the same local WLAN network for wireless communication to work.

Please refer to section "*2.2 Device and Computer Pairing*" of our white paper "*iMazing in Enterprise & Institutional Environments*" to learn more about pairing and important other security questions. https://imazing.com/uploads/iMazing-in-Enterprise-and-Institutional-Environments.pdf

2.2 Apple iOS local backup format and protocol

Local iOS backups are based on Apple's proprietary backup format and protocol to efficiently back up user data from iOS devices to macOS or Windows computers. iOS backups are incremental, meaning that the first backup may take longer as all user data files are backed up. Subsequent backups are faster since only files that have been modified or added are backed up.

Apple iOS backups are not human-readable, but applications such as iMazing can read and extract data from them. If the backup is encrypted, the password must be known to decrypt the data. The backup encryption is extremely strong (AES-256) and cannot be brute forced (section *2.5*).

iOS is by design extremely secure and most data is by default not directly extractable. The only way to extract data from iOS devices is therefore to back up the device to a computer and extract data from the backup.

iOS backups are composed of many files named with a SHA-1 hash, which are referenced in metadata files. This means that the file and folder hierarchy of the device's file system is not simply copied to the computer.

The metadata for each file includes information such as the file's path, size, and modification date. For some files, it also includes a SHA-1 hash of the file's contents, which is used to ensure that the file has not been corrupted during the backup process.

iOS local backups are generated device side by iOS. An iOS service called the BackupAgent is in charge of all operations:

1. Comparing the files that are already backed up (if a backup for the same device already exists in the backup location).
2. Preparing files that need to be backed up.
3. Encrypting files if backup encryption is enabled.
4. Transfer files to the host computer so that iMazing can store them in the backup location.

By design, local backups of iOS devices always contain a full backup of all data; it is not possible to select which data to back up. However, iMazing now includes a "*Data Access Only*" feature that extracts only necessary data from a device by omitting photos and third-party app data. This reduces the amount of storage required to extract data from a device.
Fore more details about that read our guides:
https://imazing.com/guides/data-access-only-vs-full-backup-in-imazing

2.3 What data is included in an iOS backup?

Some files on the iOS device are not included in the backup process, such as system files, logs, and cached data. Some files are also not included when the backup encryption is not enabled.

The following datasets are backed up:

- Contacts
- Messages
- Call History
- Voicemail
- Notes
- Photos
- Safari History and Bookmarks (when backup encryption is enabled)
- Calendars
- Ringtones
- User accounts
- System settings and configurations
- Passwords and other data stored in the iOS keychain (requires backup encryption)

- Health data (when backup encryption is enabled)
- Third-party app data (if app developers didn't disable their app data from being backed up)

For more information please read our guide:
https://imazing.com/guides/what-data-is-included-in-an-ios-backup

2.4 USB and Wi-Fi connection

iMazing can connect to an iOS device via a USB cable or local Wi-Fi network. As explained in section *2.1*, to establish the initial pairing, the device must be connected to the host computer via USB. Once the pairing is established, iMazing will be able to reach the device if the computer and device are connected to the same WLAN subnet.

Please refer to section *3.* for more details about network technical requirements to allow iMazing to communicate with iOS devices over WLAN.

2.5 Backup encryption

To enable backup encryption, the user must define a password and enter the device passcode on the device. Backup encryption is enabled on the device and remains enabled until the device is erased.

When enabling backup encryption, some important details need to be taken into account:

- If a backup already exists on the host (computer) backup location, a full backup must be done and the previous backup will be overwritten.
- Changing the backup password requires the user to enter the previous password, define the new password, and enter the device passcode on the device. If a backup already exists on the host backup location, a full backup must be done and the previous backup will be overwritten.
- Disabling backup encryption requires the user to enter the previous password and enter the device passcode on the device. If a backup already exists on the host backup location, a full backup must be done and the previous backup will be overwritten.

Backup encryption is done device side by the iOS BackupAgent; **iMazing is not in charge of encrypting the backup**. The backup encryption algorithm used by Apple is AES-256.

iMazing needs to know the backup encryption password to be able to compare new incremental backups with backups previously done in the same location to create its snapshots. Please refer

to section *2.7* of this guide to learn more about the iMazing backup archiving feature in charge of creating the backup snapshots.

Backup encryption passwords can optionally be saved in the macOS keychain or Windows Credentials when enabling the encryption so that the user doesn't need to enter it at every backup.

For more details about backup encryption, read:

- https://imazing.com/guides/backup-encryption-in-imazing
- https://imazing.com/guides/backup-options-in-imazing#backup-encryption
- https://imazing.com/blog/ios-10-2-introduces-safer-backups

2.6 Backup location

iMazing can back up devices to external drives or network drives (NAS) mounted on macOS or Windows.

Backing up to a network drive is typically slower than backing up to the computer's local drive or to an external drive connected to the computer via USB or Thunderbolt cable. The speed of the backup process will depend on multiple factors, which are described in detail in the following article: https://imazing.com/guides/understanding-and-fixing-slow-iphone-or-ipad-backups

Disabling backup archiving options (snapshots, section *2.7*) can speed up backups made to a network drive.

Please refer to iMazing user manual for more details about backup location:
https://imazing.com/guides/backup-options-in-imazing#backup-location

2.7 Backup archiving (snapshots)

iMazing's backup archiving system can keep multiple snapshots of the same device and automatically optimizes disk usage to only use the space necessary to store each snapshot.

iMazing's archiving system can be configured to store backups for a certain period of time and automatically remove the older ones.

Enabling backup archiving on the local computer drive or with an external drive is dependent on the filesystem format supporting hard links. The backup can be slower and will take some extra

space on file systems such as FAT which are not supporting hardlinks. We advise to use only file systems supporting hardlinks when enabling this feature.

For more details about available options please refer to:
https://imazing.com/guides/backup-options-in-imazing#archival-options

2.8 iOS device user passcode

The iOS device user defined passcode is important at different levels when working with iOS local backup.

The user must enter the device passcode on the device when prompted for the following operations:

- To establish the initial pairing between the host computer and the iOS device
- To enable, disable backup encryption and to change the backup encryption password
- Since iOS 16.1 and iOS 15.7.3, Apple has changed the local iOS backup process. **It is now required to enter the device passcode every time iMazing launches a backup operation.** You will find more details about this in our blog article: https://imazing.com/blog/ios-backup-passcode-prompt

2.9 Automatic backups with iMazing Mini

Mini is iMazing's companion app. It is available from the iMazing main menu *Tools*.
You can configure in iMazing Preferences in the *General* tab to launch iMazing Mini automatically with the option *Launch iMazing Mini at login*.

From iMazing device options, you can configure automatic backup to run:

- Daily
- Every 2 days
- Every 3 days
- Weekly
- Every two weeks
- Monthly

You can also configure a preferred time frame or prevent iMazing Mini from backing up a device if its battery charge percentage is too low.

For more details about iMazing Mini, please read user manual and guides:

- https://imazing.com/guides/getting-started-with-imazing-mini
- https://imazing.com/guides/how-to-backup-iphone-automatically
- https://imazing.com/guides/backup-options-in-imazing#automatic-backups

2.10 Supervised iOS devices

On devices supervised by your MDM solution or locally supervised with iMazing Configurator or Apple Configurator, you can enforce backup encryption. To do so create an Apple configuration profile (.mobileconfig) with a “Restrictions” payload (com.apple.applicationaccess), and check the option “Force encrypted backups” (forceEncryptedBackup).

You can create and edit Apple configuration profiles with iMazing Profile Editor:

- https://imazing.com/profile-editor
- https://imazing.com/configurator
- https://imazing.com/guides/getting-started-with-imazing-profile-editor
- https://imazing.com/guides/ios-configuration-profiles-intro
- https://imazing.com/guides/how-to-supervise-iphone-ipad
- https://imazing.com/guides/how-to-manage-supervised-iphone-ipad

2.11 iMazing Configurator: back up and manage devices in bulk

iMazing Configurator is a powerful tool to manage, provision and configure devices in bulk.

Here is a non-exhaustive list of scenarios where you could use iMazing Configurator to back up a fleet of devices:

- Enroll a fleet of unmanaged devices to a MDM solution while preserving your users data.
- Migrate from one MDM solution to another while preserving your users data.
- Back up multiple devices before reconfiguring or refurbishing devices

For more details about what iMazing Configurator, contact us or read our documentation:

- https://imazing.com/configurator
- https://imazing.com/guides/configurator-overview
- https://imazing.com/guides/configurator-quick-start
- https://imazing.com/guides/configurator-blueprints
- https://imazing.com/guides/configurator-operation-dispatcher

2.12 iMazing CLI: command line interface

iMazing CLI is a command line tool for advanced interaction with iOS devices and backups. It allows for file transfer, data extraction, backup/restore, and updating iOS. All iMazing features are fully scriptable from an app or script. The CLI tool works on macOS and Windows, and can be deployed in any environment easily.

For more details about iMazing CLI, you can read:

- https://imazing.com//cli
- https://imazing.com/guides/getting-started-with-imazing-cli
- https://imazing.com/uploads/iMazing-CLI.pdf

2.13 iMazing task delegation system (coming 2023 Q2)

We are currently working on a task delegation system, allowing admins to delegate tasks to their users from our iMazing Account platform.

In short, end-users will receive a notification by email to click a button that will launch iMazing on their computer. iMazing will then run in kiosk mode and execute the task without any other user interaction, except entering the device passcode when required. Admins will then be able to track tasks status and send reminders to their users manually or automatically. The admin will also be able to configure precisely all backup options such as:

- Encryption password
- Backup location
- Backup archiving

This system will also let admins configure iMazing settings remotely.

2.14 Network and iOS backups over WLAN

iMazing relies on Apple Mobile Device drivers to communicate with iOS devices via USB or Wi-Fi.

After an iOS device has been initially paired to a host computer using a USB cable, Apple Mobile Devices drivers allow communication with the device over WLAN, when the computer and device are connected to the same local subnet.

Device discovery is managed by protocols mDNS/Bonjour (ZeroConf). mDNS is implemented using multicasting, and multicast packets.

To make sure Bonjour operates properly, in your firewall and router settings, make sure that TCP ports 123 and 3689, and *UDP* ports 123 and 5353 are open and not blocked by the router or firewall.

Depending on the network configuration of your organization, it can sometimes be difficult to set up.

Limitations

- We have observed that in some cases, Wi-Fi mesh networks negatively impact wireless backups due to a lack of stability.
- Bonjour may not be acceptable in high-security corporate environments.
- Backing up many devices wirelessly to a single computer can lead to spotty results and connection issues. 10 devices should work fine, but probably not 50. The maximum number of simultaneous backups can be configured in iMazing Mini's preferences window.

It is possible in theory to communicate with iOS devices and back them up over VPN connections and even different subnets. However, we have not yet tested these scenarios at DigiDNA, and we are not specialized enough in networking to provide guidance or support in this area.

Here are two threads that cover these topics:

- https://serverfault.com/questions/892341/how-to-make-bonjour-mdns-work-over-openvpn
- https://serverfault.com/questions/136133/bonjour-mdns-broadcast-across-subnets

2.15 Deploying iMazing in Enterprise & Institutional Environments

iMazing can be deployed in complex enterprise or institutional environments, please read our dedicated whitepaper:
https://imazing.com/uploads/iMazing-in-Enterprise-and-Institutional-Environments.pdf

2.16 Security and Privacy

All iMazing features work locally, which means that user data remains on the local computer or network drive of the user, or infrastructure of the organization. DigiDNA does not have access to its user data and does not upload data to any cloud, except in cases where organizations back up or extract data to their own cloud.

At DigiDNA, we hold a deep respect for our users' data security. Our company, which has been active since 2008, and is based and owned in Switzerland. Safeguarding the privacy of our users has been a fundamental aspect of our core values since the very beginning.

We always prioritize and uphold Apple's security mechanisms from end-to-end.

Please have a look to our "*Security & Privacy*" page: https://imazing.com/security-and-privacy

For further details, or read section *2.* of our whitepaper "*iMazing in Enterprise & Institutional Environments*":
https://imazing.com/uploads/iMazing-in-Enterprise-and-Institutional-Environments.pdf

3. Use cases

In this chapter, we will cover five common use cases where iOS backups are necessary in enterprise and institutional environments. We will describe what iMazing can and cannot do, as well as the technical requirements and potential limitations for each case.

3.1 End-user iOS device backups

An organization wishes to back up end-users' devices to their own computers. This is a common scenario and is easy to set up, as it does not require any complex infrastructure.

iMazing Mini, the backup agent of iMazing, can be installed on the end-user's computer to perform automatic backups on a daily, weekly, or monthly basis.

Our task delegation system, available on iMazing Account, allows administrators to optionally monitor backup status and notify users when a backup is due (coming soon).

For this use case, the appropriate license is the "iMazing Business" license, which requires one license per seat/user.

Read sections *2.9* and *2.13* for more details on how it works.

- https://imazing.com/backup-iphone-ipad
- https://imazing.com/guides/how-to-backup-an-iphone-ipad-or-ipod-touch-to-your-mac-or-pc-computer
- https://imazing.com/guides/how-to-backup-iphone-automatically
- https://imazing.com/guides/how-to-backup-iphone-ipad-to-external-drive-or-another-location

3.2 End-user data transfer to new iOS devices

An organization's end-users may need to transfer their data from one device to another using their computers.

iMazing's data transfer feature can help with backing up and restoring data to another device easily, while keeping a backup of the source device. Users can customize which data they want to transfer, if they don't want to transfer all their data.

- https://imazing.com/transfer-all-data-to-any-other-iphone-or-ipad
- https://imazing.com/guides/how-to-transfer-data-from-an-iphone-ipad-or-ipod-touch-to-another-device

3.3 Centralized iOS backups

If an organization would like to back up their end-users' devices to a centralized storage, users can either use their own computers to back up devices to a centralized network drive (NAS), or a server running iMazing Mini is needed at the location where the user is located if they don't have a computer.

Backing up devices to a network drive is easy to set up with iMazing Mini or our task delegation system on end-user computers. However, the network infrastructure and NAS storage must be sufficient to support such usage. Bandwidth is very important in this case, please refer to section *2.6* and *3*.

When a centralized server is needed to back up users' devices, some technical and user experience challenges need to be taken into account:

1. Since iOS 16.1 and 15.7.3, a new device backup passcode prompt has been introduced by Apple. This means that when the server triggers a backup, the user needs to enter the device passcode. If users are not aware that a backup will run, they may miss the passcode prompt on the device and the backup will be canceled. Also, if users are using the device, they will be interrupted by this passcode prompt. This makes iOS backups from a server impractical in real day-to-day scenarios. In the future, our task delegation system will send notifications to users via email so that they can proactively accept the backup operation and be ready to enter their device passcode. Refer to section *2.8*for more details.
2. iOS devices must be physically connected via USB to the backup server to establish the initial pairing. Users must also enter their passcode to allow pairing, which can be impractical in some scenarios. Refer to section *2.1* for more details.
3. The network infrastructure must support mDNS/Bonjour to allow device discovery over WLAN. It can be challenging to set up a network so that Bonjour works over VPN or different subnets. It is recommended to have one backup server per local subnet. See section *3*.

For all these reasons, we currently recommend organizations rely on iMazing Mini and one computer per end-user for centralized backup scenarios.

- https://preview.imazing.com/uploads/case-studies/imazing-case-study-redding-construction.pdf

3.4 Data retention and archiving for compliance

In this scenario, an organization would like to archive its user data in a centralized storage or vault for data retention or archiving purposes. The data does not need to be restorable to an iOS device, but it must be stored in a human-readable or machine-parsable format for indexing.

iMazing's "Export all data" feature is designed to extract data from users' devices to various file formats, depending on the dataset: PDF, CSV, excel, various media formats etc.

- https://preview.imazing.com/export-all-data
- https://preview.imazing.com/guides/how-to-easily-export-all-iphone-data-to-mac-or-pc

Our task delegation system (coming soon), available on our platform "iMazing Account", allows for the delegation of extraction tasks to end-users. The system sends notifications to users and runs the task in "kiosk" mode in iMazing, transferring the extracted data automatically to centralized storage with minimum user interaction (see section *2.13*).

- https://preview.imazing.com/uploads/case-studies/imazing-case-study-redding-construction.pdf

3.4 Extract any type of data from iOS devices and backups

iMazing enables forensics teams, law enforcement agencies, or IT professionals to efficiently browse and extract various types of data from iOS devices and backups.

iMazing's "Extract all data" feature offers a data extraction wizard that allows users to select which datasets they want to extract. The datasets are then neatly organized into separate folders, with subfolders for each Messages and WhatsApp conversation, and with locations and dates for the photo library. The data is presented in readable formats such as PDF, Excel, CSV, photos, videos, and other media files.

iMazing's "Extract raw data" feature allows professionals to extract all data stored on the device file system or from a backup, including SQLite DBs, .plist files, and media files, while preserving the files and folders structure.

iMazing also offers a file browser that enables users to browse and extract files from both encrypted and unencrypted iOS backups.

See section *2.3* to learn more about what data can be extracted.

- https://preview.imazing.com/guides/how-to-easily-export-all-iphone-data-to-mac-or-pc

- https://imazing.com/guides/how-to-extract-files-and-data-from-an-encrypted-iphone-backup

3.5 Phone evidence and e-discovery

Law firms often need to extract data from their clients' iOS devices, especially call logs, Messages (SMS, iMessages) and WhatsApp chats, photos or other media files, with the associated metadata.

iMazing is an advanced solution for extracting data from iOS devices and is widely used by many law firms.

For law firms wanting to delegate data extraction to their clients, "iMazing Phone Evidence" is the best solution. It allows firms to send invitations and instructions to their clients via our iMazing Account platform, enabling clients to extract the required data on their own computers at home.

When extracting data from the office, the "iMazing Station" license is the best option. It enables law firms and agencies to extract data in the same way as the "Phone Evidence" license, but the task is performed at their office rather than being delegated to clients.

See section *2.3* to learn more about what data can be extracted.

- https://preview.imazing.com/enterprise/phone-evidence
- https://preview.imazing.com/export-all-data
- https://preview.imazing.com/guides/how-to-easily-export-all-iphone-data-to-mac-or-pc
- https://preview.imazing.com/guides/how-to-print-messages-and-whatsapp-chats-for-legal-purposes
- https://preview.imazing.com/guides/getting-started-with-imazing-phone-evidence
- https://preview.imazing.com/uploads/case-studies/imazing-case-study-federal-defender.pdf
- https://preview.imazing.com/uploads/case-studies/imazing-case-study-craig-ball.pdf

3.6 Mobile device management and data migration

iMazing Configurator has been used by numerous organizations seeking to enroll their users' devices to Mobile Device Management (MDM) solutions, either to supervise them or to migrate from one MDM provider to another. iMazing enables bulk migration of fleets of iOS devices while preserving user data, and supports both local supervision or Automated Device Enrollment (ADE/DEP).

See section *2.11* for more details.

- https://preview.imazing.com/configurator
- https://preview.imazing.com/uploads/case-studies/imazing-case-study-university-of-utah.pdf
- https://preview.imazing.com/uploads/case-studies/imazing-case-study-compu-hire.pdf
- https://preview.imazing.com/uploads/case-studies/imazing-case-study-mda.pdf