Preparing Collection Keys

Introduction

This guide covers how to prepare USB Collection Keys that can be used to scan target computers directly.

This document applies to the following applications		
ADFPRO Mobile & Computer Triage	DEI Digital Evidence Investigator	

What is a Collection Key?

A Collection Key is a USB storage device that is used directly on a target computer to collect data. One Collection Key is provided with the ADF product but you can also use your own to scan multiple targets on-scene, provided they match these requirements:

- USB external storage drive.
- Size of at least 16GB and up to 2TB when using the MBR (Master Boot Record) or greater when using GPT (GUID Partition Table).
- Fast read and write speed is highly recommended (the ADF Collection Key can read up to 1050 MB/sec and write up to 1000 MB/sec on USB 3.2 Gen 2 (10 Gbps))
- 512 byte native sector size, or
- 4096 byte sector size with logical 512 byte emulation. Drives with 4096 byte native sector size are not supported at this time.
- The Collection Key will be formatted with NTFS.

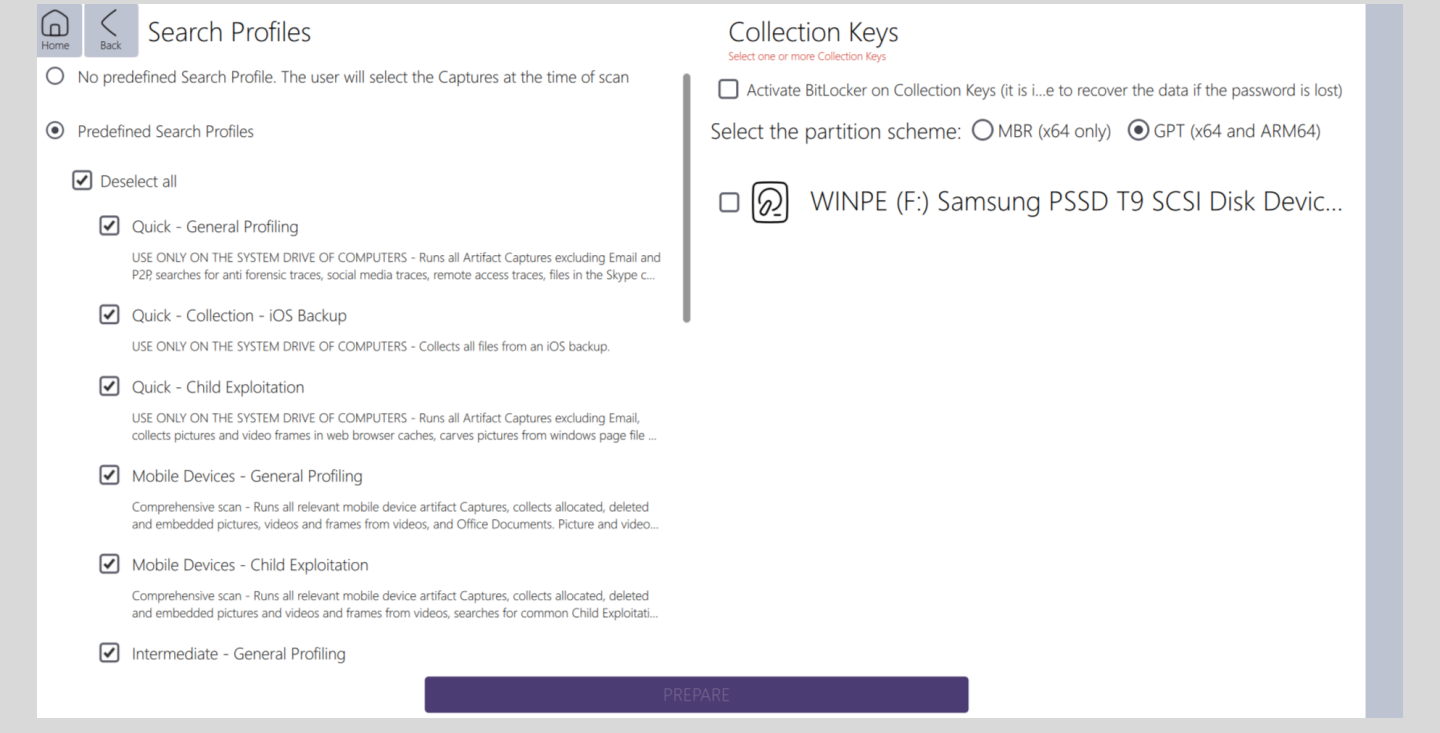
Collection Keys have to be prepared before they can be used. This process involves copying all the files needed to execute the ADF application. Once completed, the Collection Key is Windows bootable allowing the ADF application to conduct a boot scan, and it also contains the files necessary to conduct a live scan and a remote agent scan. Starting with version 6.4.0, a Collection Key prepared with the GPT partition scheme can boot both x64 (Intel and AMD) computers and ARM64 computers, such as laptops with Qualcomm Snapdragon processors, including when the Collection Key is protected with BitLocker.

Preparing a Collection Key

To prepare a Collection Key, navigate to **Home** > **Scan Setup & Key Management** > **Prepare Collection Keys**.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.

The left-hand side shows the available Search Profiles to be deployed onto the Collection Key, and the right-hand side shows the connected devices that can be prepared.



Here are the instructions to prepare one or more Collection Keys:

1. On the left-hand side of the screen, you can select the Search Profiles to deploy onto the Collection Keys. These profiles will then be available at the time of the scan. Selecting all the Search Profiles at once is possible but will increase the time it takes to prepare the Collection Key.
2. You can also choose not to deploy any Search Profile, in which case all the Captures will be available at scan time and can be selected then. Note that if you have very large Captures (those containing large amounts of hash values for example), preparing the Collection Key can take time.
3. On the right-hand side of the screen, you can select to encrypt the Collection Keys with BitLocker and input a password just before preparing the keys. It is possible to force the use of BitLocker with an option in the configuration file (see the Encrypt the Collection Key section of the Configuring the ADF Application guide).



It is not possible to encrypt a Collection Key with BitLocker on Windows 7 and 8.1. We recommend using Windows 10 or newer. Starting with version 6.4.0, a Standard User can also activate BitLocker on Collection Keys.

4. Choose how the Collection Key will be formatted using the MBR (x64 only) or GPT (x64 and ARM64) radio buttons. GPT is selected by default.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.



GPT is supported by computers using UEFI boot mode, including ARM64 computers, and allows full use of USB storage devices larger than 2TB. A GPT Collection Key boots both x64 and ARM64 computers, so it is the recommended choice.
Use MBR only for older computers that cannot start in UEFI mode (legacy BIOS). An MBR Collection Key boots x64 computers only, and the MBR partition scheme limits the drive to 2TB even if the drive storage capacity is greater. When MBR is selected, a warning is displayed: click Use MBR to confirm, or Keep GPT to go back to GPT.

5. You can also select one or more removable storage devices to be prepared as Collection Keys.



Ensure the correct removable storage devices are selected as all existing data will be deleted.

6. When ready, click on **PREPARE**.



The first Collection Key preparation can be time consuming (up to 40 minutes) as the bootable Windows image for x64 and ARM64 computers is created. Without the Windows ADK, a Collection Key can only be prepared for live scans.

7. Unplug the Collection Keys when prompted. On some occasions it is not possible to eject the removable storage device, a warning message will be displayed in these instances. The Collection Key is now prepared.

Copyright ©2016-2026 ADF Solutions, Inc. All rights reserved. U.S. Pat. No. 8,219,588 and 7,941,386. ADF PRO, Digital Evidence Investigator and Mobile Device Investigator are trademarks or registered trademarks of ADF Solutions, Inc. All other trademarks referenced herein are the property of their respective owners.