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		
ADF PRO	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:

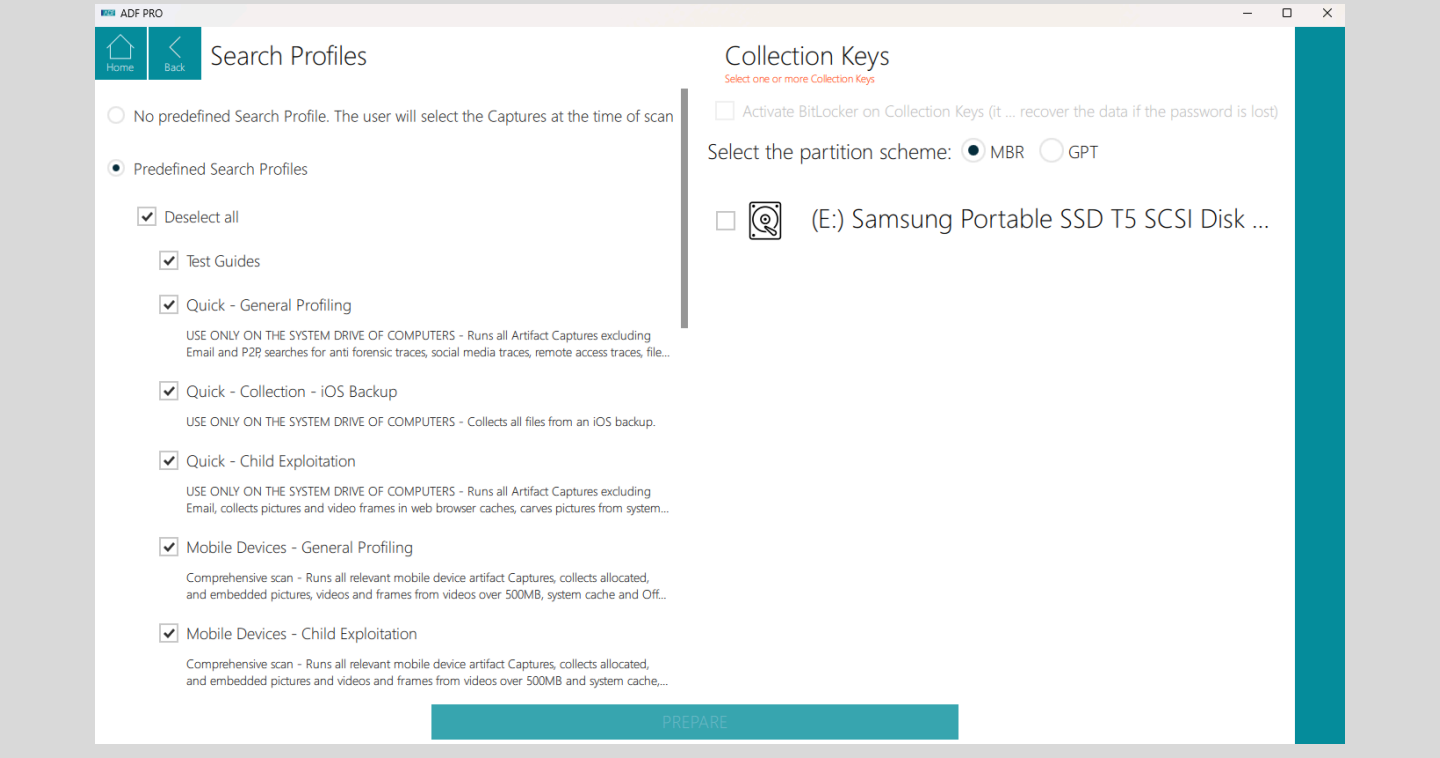
- USB external storage drive.
- Size of at least 16GB and up to 2TB when using the MBR (Master Boot Record) or greater when using GPT (GUID Partition Table).
- Fast read and write speed is highly recommended (the ADF Collection Key can read up to 1050 MB/sec and write up to 1000 MB/sec on USB 3.0)
- 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.

Preparing a Collection Key

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

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.

4. Choose how the Collection Key will be formatted using the MBR (Master Boot Record) or GPT (GUID Partition Table) radio buttons.

Using the MBR partition scheme limits that drive to 2TB even if the drive storage capacity is greater. The advantage of MBR is that legacy BIOS all support booting from that type of drives for a boot scan. So it is generally a safer approach to select MBR when preparing a Collection Key.

GPT is supported by modern computers using UEFI boot mode and allows full use of USB storage devices larger than 2TB.

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 30 minutes) as the bootable Windows image is created.

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.