AccessData KFF Installation Guide

Document Date: April 2, 2013

This document contains the following information about installing the Known File Filter (KFF).

Introduction to the New KFF Architecture

Starting with the 4.2 version of FTK, AD Lab, FTK Pro, and Enterprise, and the 2.2.3 version of CIRT, the implementation of KFF has changed. This document explains how to install and configure the new KFF components for these products.

There are two distinct components of KFF:

- The KFF Server - The KFF Server is an application that is used to process the KFF data against the evidence.
- The KFF Data - The KFF data are the hashes of the known files that are compared against the files in your case. The KFF data can be comprised of hashes obtained from pre-configured libraries or custom hashes that you configure your self.

Each component is installed separately. The KFF database is no longer stored in the shared evidence database but on the file system in EDB format.

About KFF Libraries

All of the pre-configured hash sets currently available for KFF come from three federal government agencies and are available in KFF libraries. You can download the following KFF libraries from the AccessData Downloads page:

- NDIC HashKeeper
- DHS
- NIST NSRL

  If you want to use the NSRL library, you do the following:

  - Install the complete library which includes data up through version 2.35
  - Install updates to bring the data up-to date.

  Important: In order to use the NSRL updates, you must first install the complete library.

It is not required to use a pre-configured KFF library in order to use KFF. You can configure or import custom hash sets.

For more information on KFF libraries and customizing or importing hash sets, see the Using KFF chapter in your product User Guide.

About Installing the KFF Server and KFF Libraries

In order to use KFF, you must now install the KFF Server application.

Where you install the KFF Server depends on the product you are using with KFF:

- For FTK and FTK Pro, the KFF Server is installed on the same computer that runs examiner.
- For AD Lab and Enterprise, the KFF Server can be installed on either the same computer that runs examiner or on a remote computer.
- For CIRT 2.2.3 and newer, the KFF Server can be installed on a remote computer.

When you install the KFF Server, you specify the location for both the KFF Server and the KFF data.

If you are upgrading from 4.1, you can use 4.1 to export your existing KFF groups and then import them into 4.2.x.

If you continue to use 4.1, you will use the 4.1 version of KFF, not the new KFF version for 4.2.x.

You do the following to install and add hash sets to KFF:

- Install the KFF Server
- Configure KFF Server settings
- (Optional) Install KFF libraries

About Installing the Known File Filter (KFF) Server for CIRT

Before you install or configure KFF hash data, you must install the KFF Server.

To install the KFF server for CIRT, follow the instructions in the CIRT documentation.

You can also check for and install KFF updates.

See KFF Updates on page 5.

Installing the Known File Filter (KFF) Server for FTK Products

Before you install or configure KFF hash data, you must install the KFF Server.

Use these instructions to install the KFF server for FTK, FTK Pro, LAB, or Enterprise versions 4.2 and later.

You can also check for and install KFF updates.

See KFF Updates on page 5.

See KFF Server 1.1.0.55 Update on page 6.

Note: If you have not yet installed the KFF Server, you can install the KFF Server update.

To install the KFF Server

Important: To install the KFF server, Microsoft .NET Framework 4 is required. If you do not have .NET installed, you will be prompted to install it. If you install .NET at this time, the computer must be restarted before installing KFF. On 32-bit computers, the installer will prompt you to do this, but on 64-bit computers, you may not be prompted and the KFF Server Setup Wizard opens. You must cancel the wizard and restart the computer manually before restarting the KFF Server installation.

1. Go to the AccessData Product Download website at: http://www.accessdata.com/support/product-downloads
2. On the *Product Downloads* page, expand *Forensic Toolkit (FTK)*, and click **Download**.
3. On the *Forensic Toolkit Download* page, click **Download Now** to download the following ISO file:
   Database (PostgreSQL) and KFF Installation Disc
   (AccessData recommends using a download manager program such as Filezilla.)
4. Mount the ISO and launch the Autorun.
5. Install the KFF Server.
   - **5a.** On the installation page, click **KFF Install**.
   - **5b.** Click **Install KFF Server**.
   - **5c.** Specify the location that you want to install KFF to
   - **5d.** Complete the installation wizard.
6. Configure the KFF settings.
   See Configuring KFF Settings on page 3.

Configuring KFF Settings

Before using KFF, you must configure the KFF Server settings. You can also view and edit the settings.

For FTK or FTK Pro, the *Configure KFF* dialog opens after the KFF Server installation is completed. You can also open this dialog manually. If you do not configure the KFF Server at this time, the dialog will be displayed the first time you attempt to manage KFF settings.

For AD Lab or Enterprise, if you installed the KFF Server on a remote computer, use the Configure KFF dialog to identify your KFF server. On the AD Lab or Enterprise computer, you can open this dialog manually or it will be displayed the first time you attempt to manage KFF settings. If you installed the KFF Server on the same computer, the *Configure KFF* dialog opens after the installation is completed. You can also open this dialog manually. If you do not configure the KFF Server, the dialog will be displayed the first time you attempt to manage KFF settings.

To view or edit KFF configuration settings

1. In the *Case Manager*, click **Tools > Preferences > Configure KFF**.
2. Configure the KFF settings.
   - **2a.** You can set or view the address of the KFF Server.
     - If you installed the KFF Server on the same computer, this value will be localhost.
     - If you installed the KFF Server on a different computer, identify your KFF server.
   - **2b.** Use the default interface port settings unless you want to use different ports for your environment:
     - KFF Management Interface is used to view KFF groups and sets. (Default port is 3799)
     - The KFF Lookup Interface is the port used to lookup KFF hashes. (Default port is 3798)
   - **2c.** Specify the number of threads.
     - KFF Management Interface is used to view KFF groups and sets. (Default threads is 10)
       In most cases you will not need to modify the number of Management Interface threads.
     - The KFF Lookup Interface is the port used to lookup KFF hashes. (Default port is 3798)

Important: If you have too many or too few of threads configured, it could slow down performance. To calculate an appropriate number of threads, multiply the number of cores that the computer has by four. For example, if the KFF Server computer has 4 cores, you should use 16 threads.

   - **2d.** (Optional) If you want to encrypt the KFF data, specify a Management Communication Certificate.
   - **2e.** Click **Close**.

NIST NRSL Library

After you install the KFF Server, you can install NSRL data. After you install NRSL data, you can view the installed hash sets and groups.

With the 4.2.0 and 4.2.1 versions of FTK, FTK Pro, LAB, or Enterprise, NSRL data up through version 2.35 (Feb 2012) is available for installation.

You can also check for and install KFF updates.

See KFF Updates on page 5.

W A R N I N G: There is an issue that if you install NSRL data, then uninstall it, it will prevent KFF from working.If you install NSRL data, you must keep it installed.

To install the NRSL 2.35

1. Go to the AccessData Product Download website at: http://www.accessdata.com/support/product-downloads
2. On the *Product Downloads* page, expand *Forensic Toolkit (FTK)*, and click **Download**.
3. On the *Forensic Toolkit Download* page, click **Download Now** to download the following ISO file:
   Database (PostgreSQL) and KFF Installation Disc
   (AccessData recommends using a download manager program such as Filezilla.)
4. Mount the ISO and launch the Autorun.
5. Install the NSRL data.
   - **5a.** On the installation page, click **KFF Install**.
   - **5b.** Click **Install KFF Data**.
   - **5c.** Complete the installation wizard.

NDIC Hashkeeper 9.08 Library

You can install the Hashkeeper 9.08 library to work with versions 4.2.x of FTK, FTK Pro, Lab, and Enterprise as well as version 2.2.3 and newer of CIRT.

To install the Hashkeeper library

1. Go to the AccessData Product Download website at: http://www.accessdata.com/support/product-downloads
2. On the *Product Downloads* page, expand **Known File Filter (KFF)**.
3. Download and run the NDIC Hashkeeper 9.08 installation file.

DHS 1.08 Library

You can install the DHS 1.08 library to work with versions 4.2.x of FTK, FTK Pro, Lab, and Enterprise as well as version 2.2.3 and newer of CIRT.

To install the DHS library

1. Go to the AccessData Product Download website at: http://www.accessdata.com/support/product-downloads
2. On the *Product Downloads* page, expand **Known File Filter (KFF)**.
3. Download and run the DHS 1.08 installation file.

KFF Updates

From time to time, AccessData will release updates to the KFF Server and the KFF data libraries.

Some of the KFF data updates may require you to update the version of the KFF Server.

To check for updates, do the following:

1. Go to the AccessData Product Download website at: http://www.accessdata.com/support/product-downloads
2. On the *Product Downloads* page, expand **Known File Filter (KFF)**.
3. Check for updates.

The following updates have been released:

- KFF Server 1.0.0.55 - See KFF Server 1.1.0.55 Update on page 6.
- NIST NSRL 2.39 - See NSRL 2.39 Update on page 6.

KFF Server 1.1.0.55 Update

This KFF Server update includes enhancements for the NSRL 2.39 Update.

KFF Server 1.1.0.55 Prerequisites

This release of KFF Server supports only the following product versions and later:

- CIRT 2.2.3
- 4.2.1 version of
  - FTK
  - FTK Pro
  - AD Lab
  - Enterprise

  If you have version 4.2.0, you must upgrade to 4.2.1.

To install the KFF Server update

1. Go to the AccessData Product Download website at: http://www.accessdata.com/support/product-downloads
2. On the *Product Downloads* page, expand **Known File Filter (KFF)**.
3. Download and run the KFF Server 1.1.0.55 installation file.

NSRL 2.39 Update

This update includes the following NSRL updates:

- NSRL_236.edb
- NSRL_237.edb
- NSRL_238.edb
- NSRL_239.edb

The data files are installed in the folder that you designated as the Storage Directory when you installed the KFF Server. If you do not remember the location of your KFF data, you can run **KFF_Config.exe** from *\Program Files\AccessData\KFF*.

NSRL 2.39 Prerequisites

This NSRL 2.39 update supports only the following product versions and later:

- CIRT 2.2.3
- 4.2.1 version of
  - FTK
  - FTK Pro
  - AD Lab
  - Enterprise

  If you have version 4.2.0, you must upgrade to 4.2.1.

  If you are using version 4.1.x or older of FTK, FTK Pro, AD Lab, or Enterprise, you cannot update the NSRL data at this time.

In order to use this NSRL update, you must first do the following:

- Install the KFF Server 1.0.55 Update - See KFF Server 1.1.0.55 Update on page 6.
- Install the main NSIST NSRL library - See NIST NRSL Library on page 4.

W A R N I N G: There is an issue that if you install NSRL data, then uninstall it, it will prevent KFF from working.If you install NSRL data, you must keep it installed.

To Install the NSRL 2.29 Update

1. Go to the AccessData Product Download website at: http://www.accessdata.com/support/product-downloads
2. On the *Product Downloads* page, expand **Known File Filter (KFF)**.
3. Download and run the NSRL 2.39 Update installation file.