AccessData

Known File Filter (KFF)

Installation Guide

AccessData®
A Pioneer in Digital Investigations Since 1987

AccessData Legal and Contact Information

Document date: November 21, 2013

Legal Information

AccessData Group, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Group, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, AccessData Group, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Group, Inc. reserves the right to make changes to any and all parts of AccessData software, at any time, without any obligation to notify any person or entity of such changes.

You may not export or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

AccessData Group, Inc.
588 W. 400 S.
Suite 350
Lindon, Utah 84042
U.S.A.

www.accessdata.com

AccessData Trademarks and Copyright Information

- AccessData® is a registered trademark of AccessData Group, Inc.
- AD Summation is a registered trademark of AccessData Group, Inc.
- Distributed Network Attack® is a registered trademark of AccessData Group, Inc.
- DNA® is a registered trademark of AccessData Group, Inc.
- Forensic Toolkit® is a registered trademark of AccessData Group, Inc.
- FTK® is a registered trademark of AccessData Group, Inc.
- Password Recovery Toolkit® is a registered trademark of AccessData Group, Inc.
- PRTK® is a registered trademark of AccessData Group, Inc.
- Registry Viewer® is a registered trademark of AccessData Group, Inc.

Chapter 8

Installing KFF

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

Introduction to the 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:

- KFF Server - The KFF Server is an application that is used to process the KFF data against the evidence.
- 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 Hash 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:

- NIST NSRL
  See About the NIST NSRL Data on page 4.
- NDIC HashKeeper (Sept 2008)
  See Installing the NDIC Hashkeeper Library on page 11.
- DHS (Jan 2008)
  See Installing the DHS Library on page 12.

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 the NIST NSRL Data

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

- Install the complete library.
- If updates are made available, install the updates to bring the data up-to date.

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

  When you install an NSRL update, you must keep the previous NSRL versions installed in order to maintain the complete set of NSRL data.

NSRL data release	Released	Information
version 2.40	May 2013	Contains the full NSRL library up through update 2.40. Install this library first. See Installing the NSRL Data Library on page 11.
version 2.39	April 2013	Contains NSRL updates 2.36 through 2.39.
version 2.35	Feb 2012	Contains the full NSRL library up through update 2.35.

About the KFF Server and Geolocation

In order to use the Geolocation Visualization feature in various AccessData products, you must do the following:

- Install the KFF Server 1.2.2 or later.
  You install the KFF server in the normal way.
  See Installing the KFF Server on page 6.

- Install the KFF Geolocation (GeoIP) Data (this data provide location data for evidence)
  On the KFF installation disc, there is also an option to install KFF Geolocation data.
  See Installing the Geolocation (GeoIP) Data on page 12.
  From time to time, there will be updates available for the GeoIP data.
  See Installing KFF Updates on page 12.

About Installing the KFF Server and KFF Libraries

In order to use KFF, you must first 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 must installed on the same computer that runs the Examiner.
- For all other AD products, the KFF Server can be installed on either the same computer or on a remote computer.

If you install the KFF Server on a deferent computer, you must configure the application with the location of the KFF Server.

After installing the KFF Server, before installing data or using KFF, you must configure KFF Server settings.

See Configuring KFF Settings on page 8.

If you are installing KFF in a distributed processing environment, when you configure the KFF Server location, you must specify the KFF server by its IP address and not use ‘localhost’. Otherwise you may get incorrect KFF counts.

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.

You can also check for and install KFF updates.

About the KFF Server Application versions

The KFF Server application is updated from time to time. It is best to use the latest version of the KFF Server.

KFF Server	Released	Installation Instructions
version 1.2.2	November 2013 with FTK 5.1	See Installing the KFF Server on page 6.
version 1.2.1.3	July 2013 with FTK 5.0.1	
version 1.2.0.115	May 2013 with FTK 5.0	
version 1.1.0.55	April 2013	
version 1.1.0.41	March 2013 with FTK 4.2.1	See the *FTK 4.2.x User Guide*.

About upgrading from FTK, FTK Pro, Lab, or Enterprise 4.1

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 or 5.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 or 5.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

KFF Server Prerequisites

- Microsoft .NET Framework

  Microsoft .NET Framework 4 is required. If the computer does not have it installed, you will be prompted to install it. If you install it at this time, the computer must be restarted before installing KFF.
- Microsoft Visual C++

  Microsoft Visual C++ 2010. If the computer does not have it installed, you will be prompted to install it.
- Recommended environment:
  - Operation System: 64-bit system
  - RAM: For computers doing heavy processing, 24 GB is recommended, but less can be used successfully.
  - CPU: Core i7

Installing the KFF Server

Installing the KFF Server

Use these instructions to install the KFF server for the following:

- FTK, FTK Pro, LAB, or Enterprise versions 4.2, 5.x, and later
- AD Insight, Summation, CIRT, eDiscovery 5.0 and later

See About Installing the KFF Server and KFF Libraries on page 5.

To install the KFF Server

1. Access the KFF Server installation files by doing one of the following:

- Access the setup file from the KFF Installation disc.
- Download the setup file from the web by doing the following:

  1a. Go to the AccessData Product Download website at: http://www.accessdata.com/support/product-downloads

  1b. On the *Product Downloads* page, expand *Known File Filter (KFF)*.

  1c. Click **Download** to download one of the following ISO files:

  KFF Server 1.2.2 (32-bit)
  KFF Server 1.2.2 (64-bit

  (AccessData recommends using a download manager program such as Filezilla.)

  1d. Mount the ISO.

2. Launch the Autorun.
3. Install the KFF Server.

   3a. Click **Install KFF Server**.

3b. Install pre-requisite software if needed.

3c. Specify the location that you want to install KFF to.

3d. Complete the installation wizard.

4. Configure the KFF settings.
   See Configuring KFF Settings on page 8.
5. (Optional) Install KFF data.
   See Installing KFF Data Libraries on page 11.

Installing the KFF Server for CIRT2.x

Before you install or configure KFF hash data for use with CIRT, 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 Installing KFF Updates on page 12.

Configuring KFF Settings

After installing the KFF Server, before using KFF you must configure KFF settings.

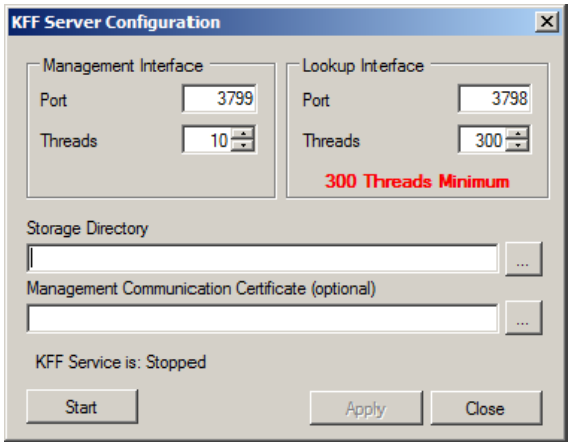
There are two places that you configure KFF settings:

Where to configure KFF Server Settings

Item	Description
The computer running the KFF Server	You mus configure settings for the KFF Server. See Configuring KFF Server Settings on page 8.
The computer running the application	On the computer running the application, such as FTK, Lab, Summation, or Insight , you configure the location of the KFF server. See Configuring the Location of the KFF Server on page 9.

Configuring KFF Server Settings

The *KFF Server Configuration* dialog opens after the KFF Server installation is completed. You can also open this dialog manually.



Important: To configure KFF, you must be logged in with Admin privileges.

KFF Server Settings

Item	Description
Interface port settings	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)

KFF Server Settings

Item	Description
Interface thread settings	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 threads is 300) **Important:** If you have too few Lookup Interface threads configured, it can result in KFF not working and generating the following error in the error log: "[Date] Failure on item ... Could not connect to KFF Server ..., token ..." If you get the error, increase the thread count.
Storage Directory	Specify the location where you want to store KFF data. If you install KFF data, this is the location it is stored to. The location must be configured before using KFF.
Management Communications Certificate	(Optional) If you want to encrypt the KFF data, specify a Management Communication Certificate
Start/Stop	You can manually start or stop the KFF Service.

To view or edit KFF Server configuration settings

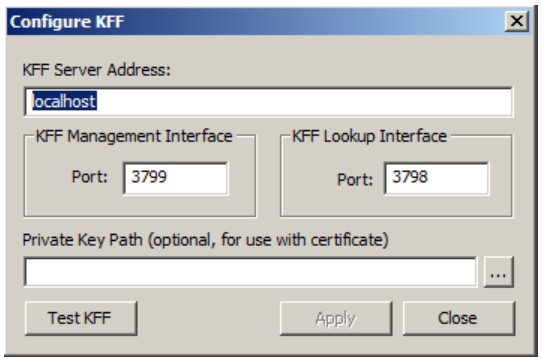
1. On the computer where the KFF Server is installed, click **Start** > **All Programs** > **AccessData KFF Server** > **KFF Server Configuration**.
2. Configure the KFF settings.
3. Click **Apply**.

Configuring the Location of the KFF Server

On the computer running the application, after installing the KFF Server, you must specify the location of the KFF Server.

Configuring KFF Settings on FTK computers.

Before using KFF with FTK, FTK Pro, Lab, or Enterprise, with KFF, you must configure the KFF settings.



Important: To configure KFF, you must be logged in with Admin privileges.

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

Configuring the KFF Server Location on Web-based Products

If you are using Summation, CIRT, eDiscovery, or Insight, so the following to specify the location of the KFF Server.

1. On the computer running the application (for example, the server running Summation), go to C:\Program Files\AccessData\Common\FTK Business Services.
2. Open AdgWindowsServiceHost.exe.config.
3. Modify <add key="kffHostname" value="localhost" />.
4. Change localhost to be the location of your KFF server (you can use hostname or IP).
5. Save and close file.
6. Restart the business services common service.

Installing KFF Data Libraries

Note: If you install either DHS data or NDIC data after previously installing KFF Geolocation (GeoIP) data, you will get an error that a newer version is already installed and will need to be uninstalled first. Workaround: Uninstall the GeoIP data, install the DHS and/or NDIC data, then re-install the GeoIP data.

Installing the NSRL Data Library

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

You start by installing the full NSRL library up to version 2.40. You can then install any updates.

See About the NIST NSRL Data on page 4.

You can also check for and install KFF updates.

See Installing KFF Updates on page 12.

To install the NSRL 2.40 library and updates

1. Access the NSRL 2.40 installation files by doing one of the following:

- Access the setup file from the KFF Installation disc.
- Download the setup file from the web by doing the following:

1a. Go to the AccessData Product Download website at: http://www.accessdata.com/support/product-downloads

1b. On the *Product Downloads* page, expand *Known File Filter (KFF)*.

1c. Click **Download** to download one of the following ISO files:

KFF Server 1.2.2 & Cum. NRSL 240 Data (32-bit)
KFF Server 1.2.2 & Cum. NRSL 240 Data (64-bit

(AccessData recommends using a download manager program such as Filezilla.)

1d. Mount the ISO.

2. Launch the Autorun.
3. Click **Install NSRL Full Data 2.40** and complete the installation wizard.
4. Close the installation window.

Installing the NDIC Hashkeeper 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.

Installing the DHS 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.

Installing the Geolocation (GeoIP) Data

Geolocation (GeoIP) data is used for the Geolocation Visualization feature of several AccessData products.

See About the KFF Server and Geolocation on page 4.

You can also check for and install KFF updates.

See Installing KFF Updates on page 12.

To install the Geolocation Data

1. Access the KFF installation files by doing one of the following:

- Access the setup file from the KFF Installation disc.
- Download the setup file from the web by doing the following:

1a. Go to the AccessData Product Download website at: http://www.accessdata.com/support/product-downloads

1b. On the *Product Downloads* page, expand *Known File Filter (KFF)*.

1c. Click **Download** to download one of the following ISO files:

KFF Server 1.2.2 & Cum. NRSL 240 Data (32-bit)
KFF Server 1.2.2 & Cum. NRSL 240 Data (64-bit

(AccessData recommends using a download manager program such as Filezilla.)

1d. Mount the ISO.

2. Launch the Autorun.
3. Click **Install Geolocation** and complete the installation wizard.
4. Close the installation window.

Installing 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.
   - See About the KFF Server Application versions on page 5.
   - See About the NIST NSRL Data on page 4.