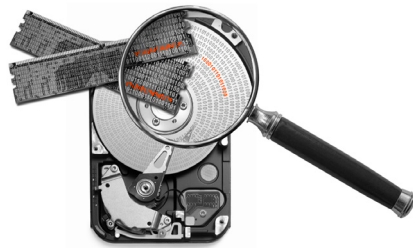


AccessData Triage



User Guide

Version: 1.1
Published: July 2011



AccessData[®]
A Pioneer in Digital Investigations Since 1987

AccessData Legal and Contact Information

Document date: July 26, 2011

Legal Information

©2011 AccessData Group, LLC All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

AccessData Group, LLC 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, LLC 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, LLC 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, LLC 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, LLC.
384 South 400 West
Suite 200
Lindon, Utah 84042
U.S.A.
www.accessdata.com

AccessData Trademarks and Copyright Information

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

A trademark symbol (®, ™, etc.) denotes an AccessData Group, LLC. trademark. With few exceptions, and unless otherwise notated, all third-party product names are spelled and

capitalized the same way the owner spells and capitalizes its product name. Third-party trademarks and copyrights are the property of the trademark and copyright holders. AccessData claims no responsibility for the function or performance of third-party products.

Third party acknowledgements:

- FreeBSD® Copyright 1992-2011. The FreeBSD Project .
- AFF® and AFFLIB® Copyright© 2005, 2006, 2007, 2008 Simson L. Garfinkel and Basis Technology Corp. All rights reserved.
- Copyright © 2005 - 2009 Ayende Rahien

Documentation Conventions

In AccessData documentation, a number of text variations are used to indicate meanings or actions. For example, a greater-than symbol (>) is used to separate actions within a step. Where an entry must be typed in using the keyboard, the variable data is set apart using [*variable_data*] format. Steps that required the user to click on a button or icon are indicated by **Bolded text**. This *Italic* font indicates a label or non-interactive item in the user interface.

A trademark symbol (®, ™, etc.) denotes an AccessData Group, LLC. trademark. Unless otherwise notated, all third-party product names are spelled and capitalized the same way the owner spells and capitalizes its product name. Third-party trademarks and copyrights are the property of the trademark and copyright holders. AccessData claims no responsibility for the function or performance of third-party products.

Registration

The AccessData product registration is done at AccessData after a purchase is made, and before the product is shipped. The licenses are bound to either a USB security device, or a Virtual CmStick, according to your purchase.

Subscriptions

AccessData provides a one-year licensing subscription with all new product purchases. The subscription allows you to access technical support, and to download and install the latest releases for your licensed products during the active license period.

Following the initial licensing period, a subscription renewal is required annually for continued support and for updating your products. You can renew your subscriptions through your AccessData Sales Representative.

Use LicenseManager to view your current registration information, to check for product updates and to download the latest product versions, where they are available for download. You can also visit our web site, www.accessdata.com anytime to find the latest releases of our products.

For more information, see Managing Licenses in your product manual or on the AccessData web site.

AccessData Contact Information

Your AccessData Sales Representative is your main contact with AccessData Group, LLC. Also, listed below are the general AccessData telephone number and mailing address, and telephone numbers for contacting individual departments.

Mailing Address and General Phone Numbers

You can contact AccessData in the following ways:

TABLE Contact-1 AD Mailing Address, Hours, and Department Phone Numbers

Corporate Headquarters:	AccessData Group, LLC. 384 South 400 West Suite 200 Lindon, UT 84042 USA <i>Voice:</i> 801.377.5410 <i>Fax:</i> 801.377.5426
General Corporate Hours:	Monday through Friday, 8:00 AM – 5:00 PM (MST) AccessData is closed on US Federal Holidays
State and Local Law Enforcement Sales:	<i>Voice:</i> 800.574.5199, option 1 <i>Fax:</i> 801.765.4370 <i>Email:</i> Sales@AccessData.com
Federal Sales:	<i>Voice:</i> 800.574.5199, option 2 <i>Fax:</i> 801.765.4370 <i>Email:</i> Sales@AccessData.com
Corporate Sales:	<i>Voice:</i> 801.377.5410, option 3 <i>Fax:</i> 801.765.4370 <i>Email:</i> Sales@AccessData.com
Training:	<i>Voice:</i> 801.377.5410, option 6 <i>Fax:</i> 801.765.4370 <i>Email:</i> Training@AccessData.com
Accounting:	<i>Voice:</i> 801.377.5410, option 4

Technical Support

Free technical support is available on all currently licensed AccessData products. You can contact AccessData Customer and Technical Support in the following ways:

TABLE Contact-2 AD Customer & Technical Support Contact Information

Domestic Support Americas/Asia-Pacific	
Standard Support:	Monday through Friday, 5:00 AM – 6:00 PM (MST), except corporate holidays. <i>Voice:</i> 801.377.5410, option 5 <i>Voice:</i> 800.658.5199 (Toll-free North America) <i>Email:</i> Support@AccessData.com
After Hours Phone Support:	Monday through Friday 6:00 PM to 1:00 AM (MST), except corporate holidays. <i>Voice:</i> 801.377.5410, option 5
After Hours Email-only Support:	Monday through Friday 1:00 AM to 5:00 AM (MST), except corporate holidays. <i>Email:</i> afterhours@accessdata.com
International Support Europe/Middle East/Africa	
Standard Support:	Monday through Friday, 8:00 AM – 5:00 PM (UK-London), except corporate holidays. <i>Voice:</i> +44 207 160 2017 (United Kingdom) <i>Email:</i> emeasupport@accessdata.com
After Hours Support:	Monday through Friday, 5:00 PM to 1:00 AM (UK/London), except corporate holidays. <i>Voice:</i> 801.377.5410 Option 5*.
After Hours Email-only Support:	Monday through Friday, 1:00 AM to 5:00 AM (UK/London), except corporate holidays. <i>Email:</i> afterhours@accessdata.com

TABLE Contact-2 AD Customer & Technical Support Contact Information (Continued)

Other	
<i>Web Site:</i>	http://www.AccessData.com/Support The Support web site allows access to Discussion Forums, Downloads, Previous Releases, our Knowledgebase, a way to submit and track your "trouble tickets", and in-depth contact information.
<i>AD SUMMATION</i>	Americas/Asia-Pacific: 800.786.2778 (North America). 415.659.0105. Email: support@summation.com
<i>Standard Support:</i>	Monday through Friday, 6:00 AM– 6:00 PM (PST), except corporate holidays.
<i>After Hours Support:</i>	Monday through Friday by calling 415.659.0105.
<i>After Hours Email-only Support:</i>	Between 12am and 4am (PST) Product Support is available only by email at afterhours@accessdata.com .
<i>AD Summation CaseVault</i>	866.278.2858 Email: support@casevault.com Monday through Friday, 8:00 AM – 6:00 PM (EST), except corporate holidays.
<i>AD Summation Discovery Cracker</i>	866.833.5377 Email: dcsupport@accessdata.com
<i>Support Hours:</i>	Monday through Friday, 7:00 AM – 7:00 PM (EST, except corporate holidays.

Note: All support inquiries are typically responded to within one business day. If there is an urgent need for support, contact AccessData by phone during normal business hours.

Documentation

Please email AccessData regarding any typos, inaccuracies, or other problems you find with the documentation:

documentation@accessdata.com

Professional Services

The AccessData Professional Services staff comes with a varied and extensive background in digital investigations including law enforcement, counter-intelligence, and corporate security. Their collective experience in working with both government and commercial entities, as well as in providing expert testimony, enables them to provide a full range of computer forensic and eDiscovery services.

At this time, Professional Services provides support for sales, installation, training, and utilization of FTK, FTK Pro, Enterprise, eDiscovery, and Lab. They can help you resolve any questions or problems you may have regarding these products

Contact Information for Professional Services

Contact AccessData Professional Services in the following ways:

TABLE Contact-3 AccessData Professional Services Contact Information

Contact Method	Number or Address
<i>Phone</i>	Washington DC: 410.703.9237
	North America: 801.377.5410
	North America Toll Free: 800-489-5199, option 7
	International: +1.801.377.5410
<i>Email</i>	adservices@accessdata.com

Table of Contents

AccessData Legal and Contact Information	i
Legal Information	i
AccessData Trademarks and Copyright Information	i
Documentation Conventions	ii
Registration	ii
Subscriptions	ii
AccessData Contact Information	ii
Mailing Address and General Phone Numbers	iii
Technical Support	iii
Documentation	iv
Professional Services	iv
Contact Information for Professional Services	v
Table of Contents	vi
Introduction	1
About AD Triage	1
Components of AD Triage	1
Installation	2
Prerequisites	2
Software Requirements	2
Hardware Requirements	2
Installing AD Triage Admin	3
Getting Started	6
Launching AD Triage Admin	6
Admin User Interface Overview	6
Triage Admin Main Window	6
Manage Collections Dialog	8
Manage Licenses Dialog	9
Profiles Dialog	10
File Filtering Dialog	11
Regular Expression Dialog	12
Keywords Dialog	12
Hash Filter Dialog	13

Default Collector Wizard Dialog	14
Custom Collector Wizard Dialog	15
Manage Triage Devices Dialog	16
Collection Interface Overview	18
Performing Basic Triage Tasks	20
About Triage Profiles	20
Creating a Profile	20
Managing Licenses	23
Creating a Triage USB Device	25
Creating a Standard Triage Device	25
Creating a Custom Triage Device	25
Creating a Bootable Disc	28
About Collecting Data on a Target System	28
Collecting Data from a Live System	29
Booting AD Triage on a Target System	29
Automatically Collecting Data on a Target System	30
Manually Collecting and Exporting Data on a Target System	30
Saving Collected Data	34
Managing Saved Collections	35
Filtering Saved Collections	35
Reviewing Saved Collections	36
Generating Reports for Saved Collections	37
Performing Advanced Triage Tasks	39
Advanced Profile Tasks	39
Copying a Profile	39
Editing a Profile	40
Deleting a Profile	41
About Custom Filters	41
Creating a Custom Filter	41
Creating a Keyword Group	44
Creating a Hash Group	45
Creating a Regular Expression Group	45
Advanced Saved Collections Tasks	46
Exporting Saved Collections	46
Deleting a Saved Collection	47
Importing a Saved Collection	47
Recovering a Remote Collection	47
Using the Triage Receiver	48
Mounting to a Remote Share	50

Appendix A Managing Security Devices and Licenses	51
AccessData Product Licenses	51
Installing and Managing Security Devices	51
Installing LicenseManager	59
Starting LicenseManager	61
Using LicenseManager	62
Updating Products	70
Sending a Dongle Packet File to Support	71
Virtual CodeMeter Activation Guide	71
Introduction	71
Preparation	71
Setup for Online Systems.	72
Setting up VCM for Offline Systems.	73
Creating a Virtual CM-Stick with Server 2003/2008 Enterprise Editions	75
Additional Instructions for AD LAB WebUI and eDiscovery	77
Virtual CodeMeter FAQs	77
Network License Server (NLS) Setup Guide.	79
Introduction	79
Preparation Notes	79
Setup Overview.	79
Network Dongle Notes	79
NLS Server System Notes	80
NLS Client System Notes.	80

Introduction

About AD Triage

AD Triage is designed to collect and review data/artifacts from a live or powered down target system and facilitate the transfer of that data to an administrator system. An AD1 logical image of the system's artifacts can then be written to the destination of your choice. From there, the data can be decrypted and imported into the administrator's interface for further review and reporting or can be consumed by FTK for more advanced analysis.

Components of AD Triage

AD Triage is made up of two interfaces, the *Admin* interface, and the *Collection* interface. The *Admin* interface is what you install on your machine. You will use this interface to review and store all the data that you collect.

The *Collection* interface is what you boot to on the target system. You can use this interface to collect and export data to a USB device or a specified computer on the same network as the target system.

Installation

This chapter contains all the information you need to install AD Triage.

Prerequisites

Before you install AD Triage, you must have the following items:

- A CodeMeter dongle that is licensed for AD Triage (see [Appendix A Managing Security Devices and Licenses](#) page 51)
- CodeMeter Runtime 4.2 installed on your system
- Microsoft .NET 3.5 SP1

Software Requirements

To run AD Triage, in addition to the hardware requirements, you need the following:

- An additional license with separate installation.
- Microsoft Windows OS platform on which AD Triage operates as a standalone product.
- AccessData FTK installed on your machine (if you intend to add the imaged data to a case for further investigation).

Images created by AD Triage are AccessData-proprietary AD1-type images. AD1 images can be imported back into AD Triage, and can be added as evidence to a case in any AD FTK-core product.

Hardware Requirements

AD Triage requires the following additional hardware:

- USB ports on your machine.
- CodeMeter USB or Virtual CmStick (with current licenses installed).
- A USB device for each profile you create in AD Triage.

Installing AD Triage Admin

To install AD Triage Admin

1. Insert installation disk into the CD/DVD drive.
2. Open the file for the installation disk.
3. Run the **SETUP.EXE** file.

FIGURE 2-1 Welcome Screen



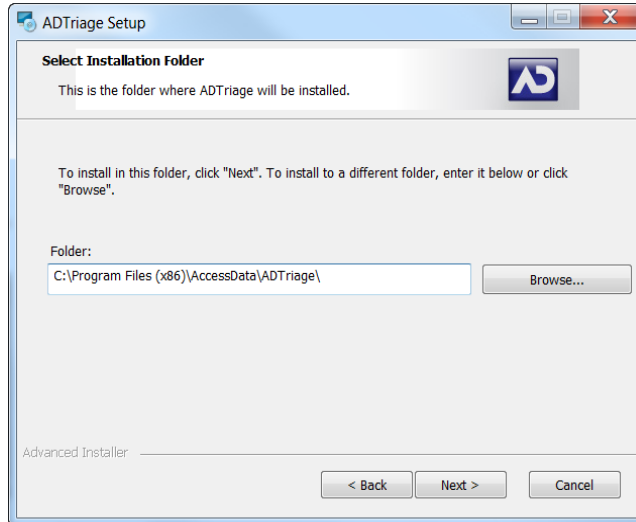
4. In the *Installation Wizard*, click **Next**.

FIGURE 2-2 End-User License Agreement



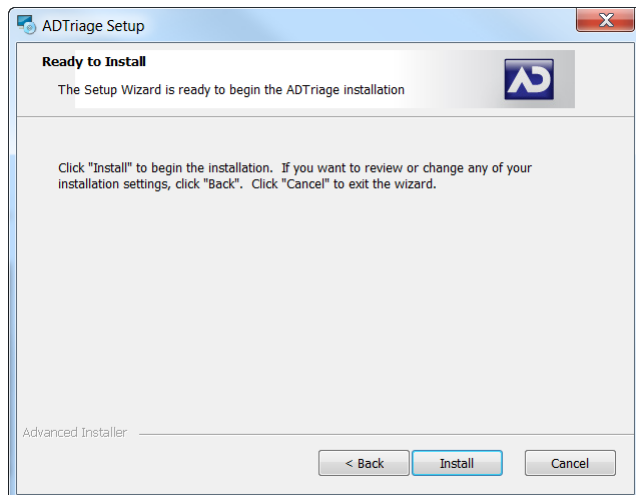
5. Mark the **I accept the terms in the License Agreement** and click **Next**.

FIGURE 2-3 Select Installation Folder Screen



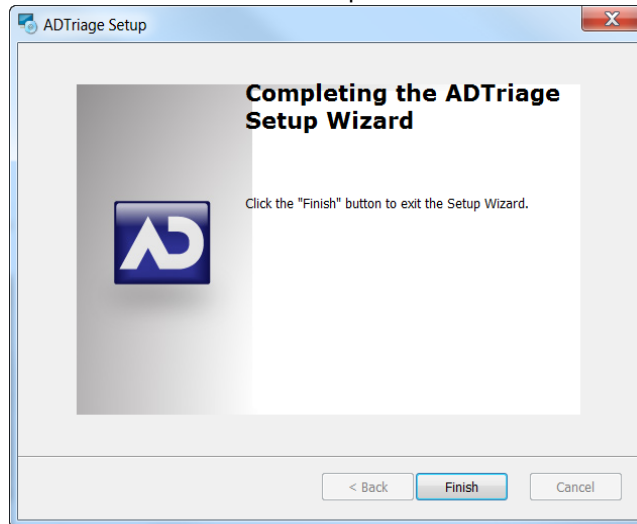
6. Browse to the location where you want to save your program files, select whether you want to install AD Triage for all users or just for the current user, and click **Next**.

FIGURE 2-4 Confirm Installation Screen



7. Click **Install** to begin the installation.

FIGURE 2-5 Installation Complete Screen



8. Click **Finish** to close the installation wizard.

Getting Started

This chapter introduces you to the features and interface of the *Admin* and *Collection* interfaces.

Launching AD Triage Admin

To launch AD Triage Admin

- ❖ Select **Start > Programs > AccessData > ADTriage > ADTriageAdmin.exe**.
The *Triage Admin* window opens.

Admin User Interface Overview

This section describes the elements of the *Admin* console. Use the following sections as a reference when using the *Admin* interface.

Triage Admin Main Window

The *Triage Admin* main window is the first thing you see when you open Triage (see [Launching AD Triage Admin](#) page 6). You can use the *Admin* main window to set up devices, create custom collection agent profiles, customize filters for profiles, manage licenses, and manage saved collections. Use the following figure and table to understand the elements found in the *Triage Admin* main window.

FIGURE 3-1 Triage Admin Main Window

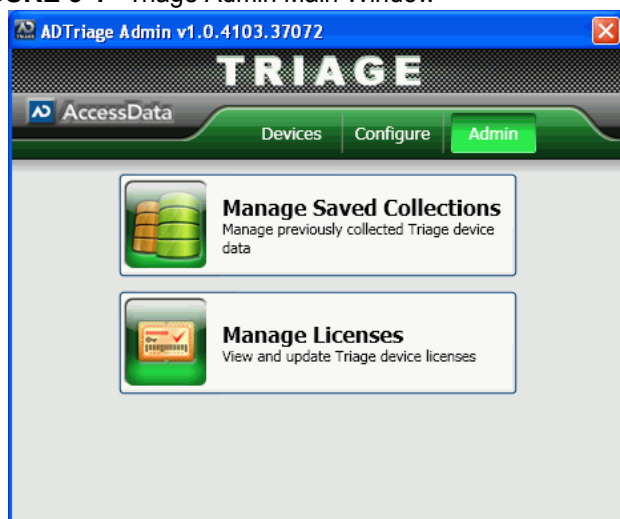


TABLE 3-1 Elements of the Triage Admin Main Window

Interface Element	Description
Admin Tab	<p>The following options are available on the Admin tab:</p> <ul style="list-style-type: none"> • Manage Saved Collections (see Manage Collections Dialog page 8) • Manage Licenses (see Manage Licenses Dialog page 9)
Devices Tab	<p>The following options are available on the Devices tab:</p> <ul style="list-style-type: none"> • Standard Triage Device (see Default Collector Wizard Dialog page 14) • Custom Triage Device (see Custom Collector Wizard Dialog page 15) • Manage Triage Devices (see Manage Triage Devices Dialog page 16)
Configure Tab	<p>The following options are available on the Profiles tab:</p> <ul style="list-style-type: none"> • Manage Profiles (see About Triage Profiles page 20) • Manage Custom Filters (see About Custom Filters page 41) • RegEx Groups (see Default Collector Wizard Dialog page 14) • Keyword Groups (see Regular Expression Dialog page 12) • Hash Groups (see Hash Filter Dialog page 13)

Manage Collections Dialog

Open the *Manage Collections* dialog by clicking the **Manage Saved Collections** button on the *Admin* tab. Use the following figure and table to understand the elements in the *Manage Collections* dialog.

FIGURE 3-2 Manage Collections Dialog

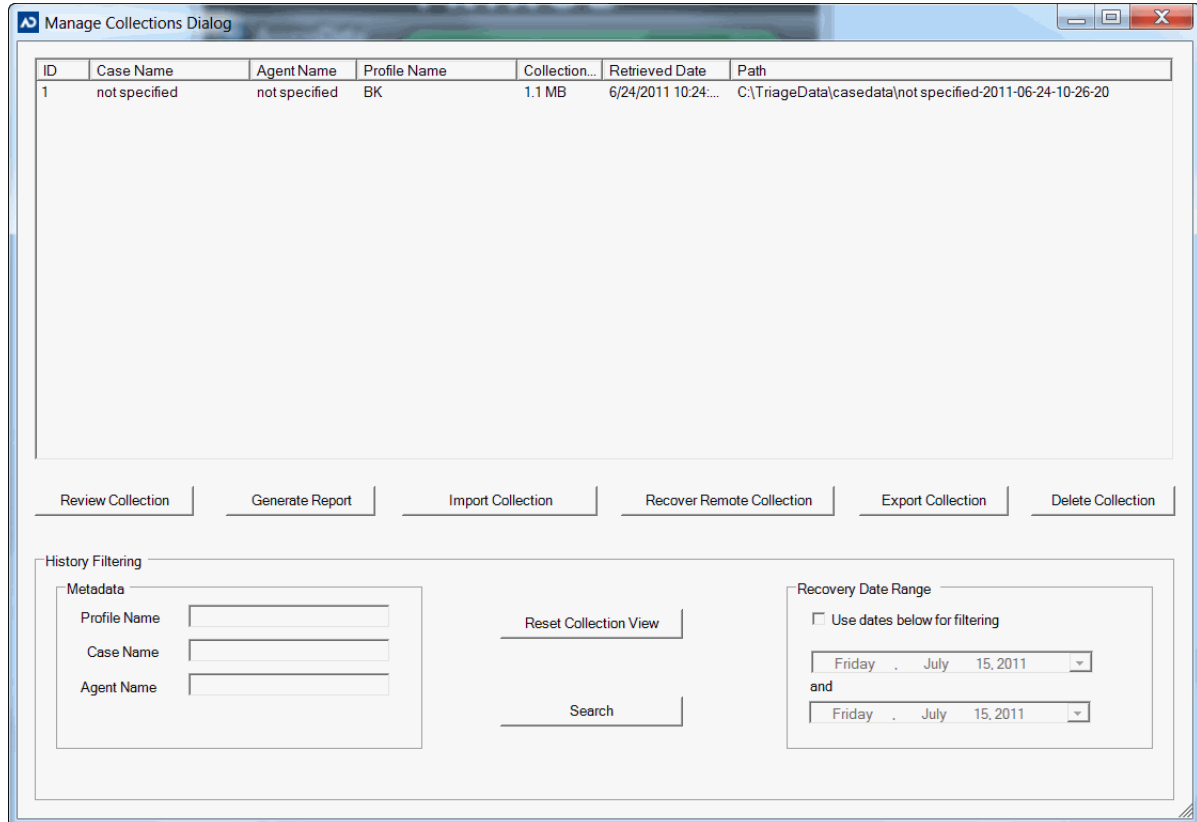


TABLE 3-2 Elements of the Manage Collections Dialog

Interface Element	Description
Manage Collections Pane	Lists recent actions performed in the <i>Triage Admin</i> main window. Click the column headings to sort by column. Double-click the ID number to open the evidence file.
Review Collection Button	Click to open the <i>Recover Evidence</i> dialog (see Reviewing Saved Collections page 36).
Generate Report Button	Click to open the <i>Generate Reports</i> dialog (see Generating Reports for Saved Collections page 37).
Import Collection Button	Click to import a collection from file. (see Importing a Saved Collection page 47).
Recover Remote Collection Button	Click to import a collection that was saved on a remote directory (see Recovering a Remote Collection page 47).
Export Collection Button	Click to create an AD1 image of the evidence (see Exporting Saved Collections page 46).

TABLE 3-2 Elements of the Manage Collections Dialog (Continued)

Delete Collection Button	Click to delete the selected evidence from the profile (Deleting a Saved Collection page 47).
Profile Name Field	Enter text to filter the <i>Manage Collections</i> pane by the <i>Profile Name</i> column.
Case Name Field	Enter text to filter the <i>Manage Collections</i> pane by the <i>Case Name</i> column.
Agent Name Field	Enter text to filter the <i>Manage Collections</i> pane by the <i>Agent Name</i> column.
Reset Collection View	Click to remove filters and return to the default collection view.
Use Dates Below for Filtering Check Box	Check to filter the <i>Manage Collections</i> pane by selected date range.
Search Button	Click to filter the <i>Manage Collections</i> pane by the criteria you entered.

Manage Licenses Dialog

Open the *Manage Licenses* dialog by clicking the **Manage Licenses** button on the *Admin* tab. Use the following figure and table to understand the elements in the *Manage Licenses* dialog.

FIGURE 3-3 Manage Licenses Dialog

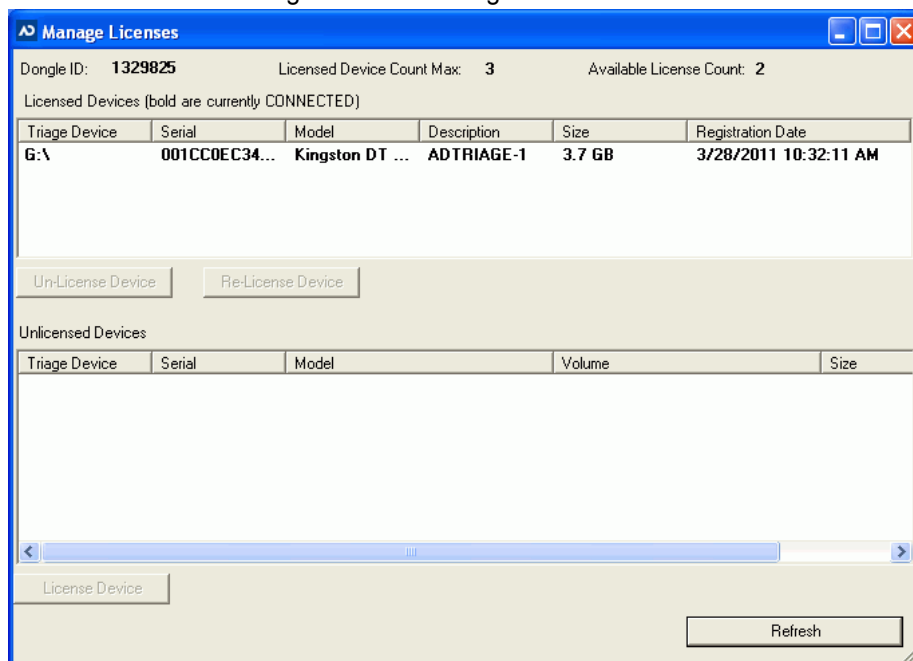


TABLE 3-3 Elements of the Manage Licenses Dialog

Dongle ID	Lists the number for the codemeter used for AD Triage.
Licensed Device Count Max	Lists the number of licenses for separate devices. Only visible if you signed up for a limited amount of device licenses, but unlimited amount of recoveries.

TABLE 3-3 Elements of the Manage Licenses Dialog (Continued)

Available License Count	Lists the number of licenses still available for use. Only visible if you signed up for a limited amount of device licenses, but unlimited amount of recoveries.
Upper Device Pane	Lists the devices currently in use.
Un-License Device Button	Click to remove the license from the selected device.
Re-License Device Button	Click to reattach a license to the selected device.
Lower Device Pane	Lists un-licensed devices that are connected to the computer.
License Device Button	Click to attach a license to the selected device (see Managing Licenses page 23).
Refresh Button	Click to refresh the lists of devices.

Profiles Dialog

Open the *Profiles* dialog by clicking the **Manage Profiles** button on the *Configure* tab. Use the following figure and table to understand the elements in the *Profiles* dialog.

FIGURE 3-4 Profiles Dialog

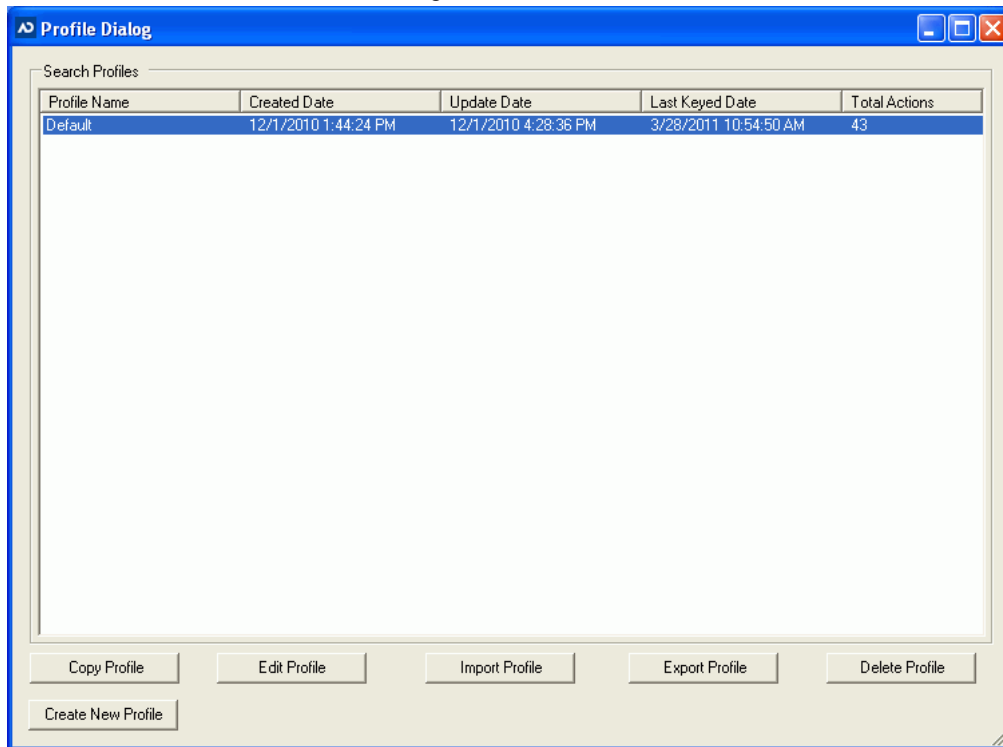


TABLE 3-4 Elements of the Profile Dialog

Profile Pane	Lists the current profiles.
Copy Profile Button	Click to copy the selected profile.
Edit Profile Button	Click to edit the selected profile.
Delete Profile Button	Click to delete the selected profile.

TABLE 3-4 Elements of the Profile Dialog (Continued)

Create New Profile Button	Click to create a new profile (see Creating a Profile page 20).
---------------------------	---

File Filtering Dialog

Open the *File Filtering* dialog by clicking the **Manage Custom Filters** button on the *Configure* tab. Use the following figure and table to understand the elements in the *File Filtering* dialog.

FIGURE 3-5 File Filtering Dialog

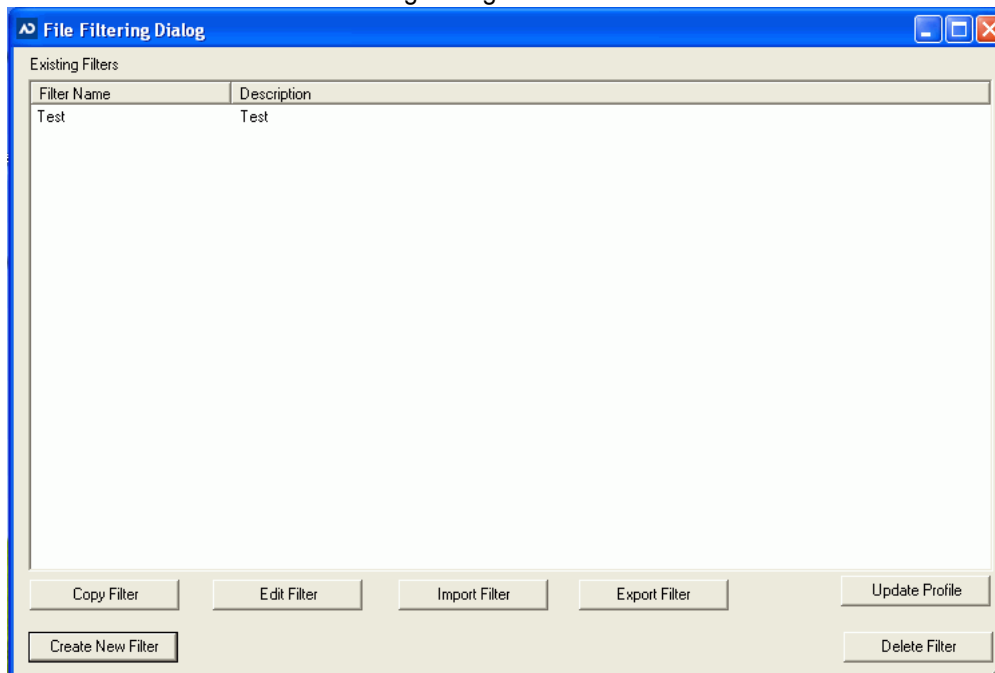


TABLE 3-5 Elements of the File Filtering Dialog

Interface Element	Description
Existing Filters Pane	Lists the existing filters. Click the column header to sort the list by that column.
Create New Filter Button	Click to create a new custom filter (see Creating a Custom Filter page 41).
Delete Filter Button	Click to delete the selected filter.
Update Profile Button	Click to add the selected filter to a profile.
Copy Filter Button	Click to copy the selected filter.
Edit Filter Button	Click to edit the selected filter.
Import Filter Button	Click to import a filter from a file.
Export Filter Button	Click to export the selected filter.

Regular Expression Dialog

Open the *Regular Expression* dialog by clicking the **RegEx Groups** button on the *Configure* tab. Use the following figure and table to understand the elements in the *Regular Expression* dialog.

FIGURE 3-6 Regular Expression Dialog

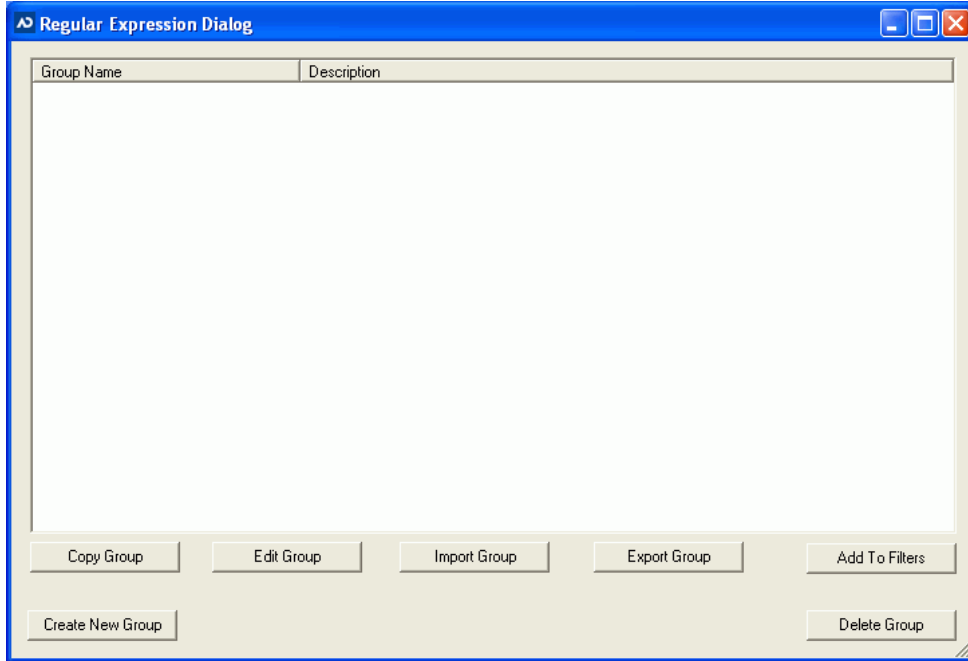


TABLE 3-6 Elements of the Regular Expression Dialog

Interface Element	Description
Regular Expression Pane	Lists existing groups.
Copy Group Button	Click to copy the selected group.
Edit Group Button	Click to edit the selected group.
Import Group Button	Click to import a group from file.
Export Group Button	Click to export the selected group to a file.
Add to Filters Button	Click to add filters to the selected group.
Delete Group Button	Click to delete the selected group.
Create New Group Button	Click to create a new Regular Expression group (see Creating a Regular Expression Group page 45).

Keywords Dialog

Open the *Keywords* dialog by clicking the **Keyword Groups** button on the *Configure* tab. Use the following figure and table to understand the elements in the *Keywords* dialog.

FIGURE 3-7 Keywords Dialog

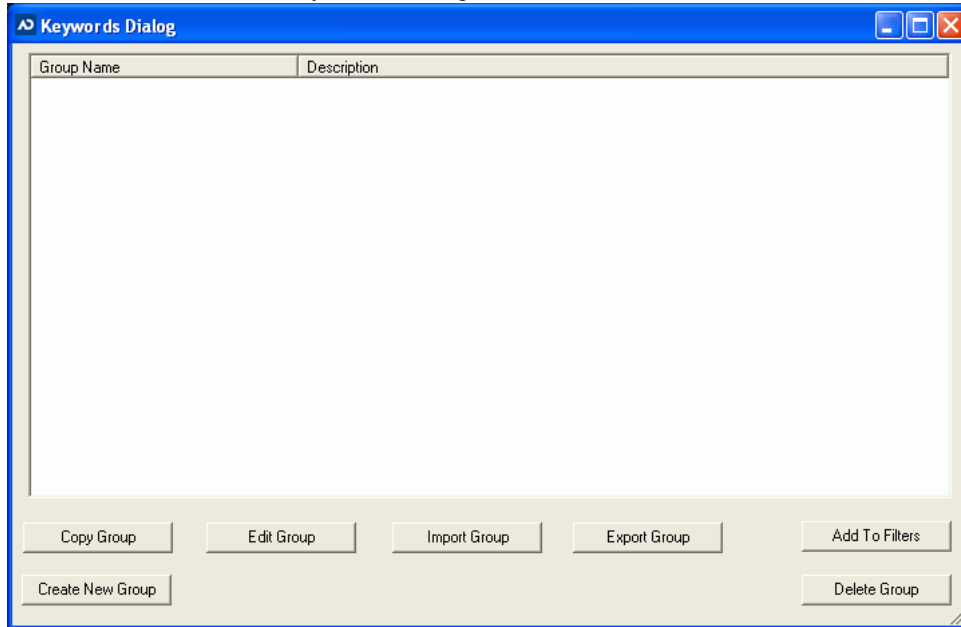


TABLE 3-7 Elements of the Keywords Dialog

Interface Element	Description
Keywords Pane	Lists existing filters.
Copy Group Button	Click to copy the selected group.
Edit Group Button	Click to edit the selected group.
Import Group Button	Click to import a filter from file.
Export Group Button	Click to export a group to a file.
Add to Filter Button	Click to add filters to the selected group.
Delete Group Button	Click to delete the selected group.
Create New Group Button	Click to create a new Keyword group. (see Creating a Keyword Group page 44)

Hash Filter Dialog

Open the *Hash Filter* dialog by clicking the **Hash Groups** button on the *Configure* tab. Use the following figure and table to understand the elements in the *Hash Filter* dialog.

FIGURE 3-8 Hash Filter Dialog

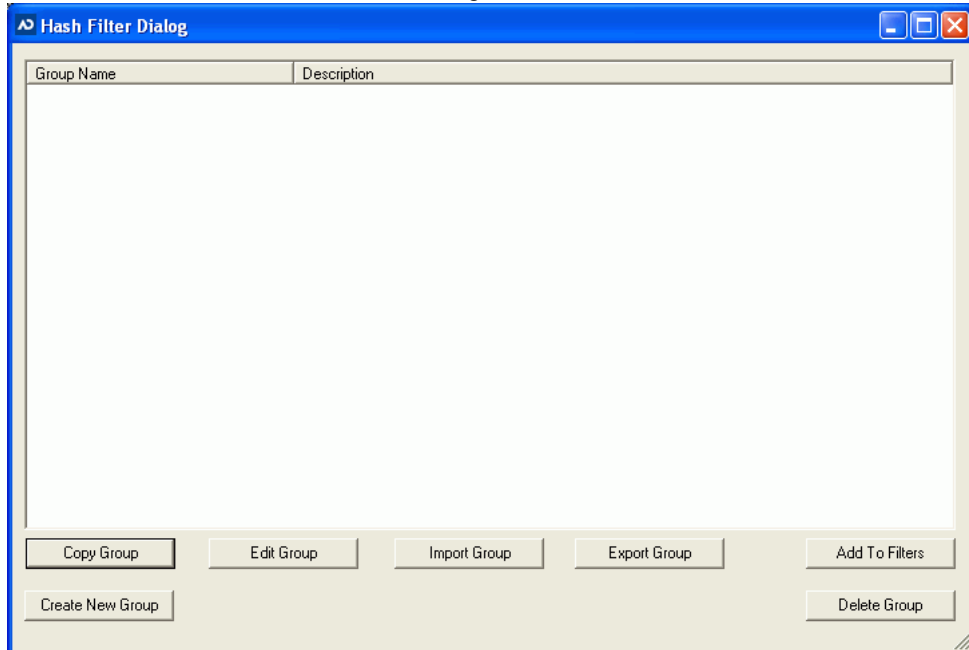


TABLE 3-8 Elements of the Hash Filter Dialog

Interface Element	Description
Hash Filter Pane	Lists existing groups. Click the column header to sort the list by that column.
Copy Group Button	Click to copy the selected group.
Edit Group Button	Click to edit the selected group.
Import Group Button	Click to import a group from an existing file.
Export Group Button	Click to export the selected group to a file.
Add to Filters Button	Click to add filters to the selected group.
Delete Group Button	Click to delete the selected group.
Create New Group Button	Click to create a new Hash Filter Group (see Creating a Hash Group page 45).

Default Collector Wizard Dialog

Open the *Default Collector Wizard* dialog by clicking the **Standard Triage Device** button on the *Devices* tab of the *Admin* window. Use this dialog to apply the Default profile to a licensed USB device (see [Creating a Standard Triage Device](#) page 25). Use the following figure and table to understand the elements in the *Default Collector Wizard* dialog.

FIGURE 3-9 Default Collector Wizard Dialog

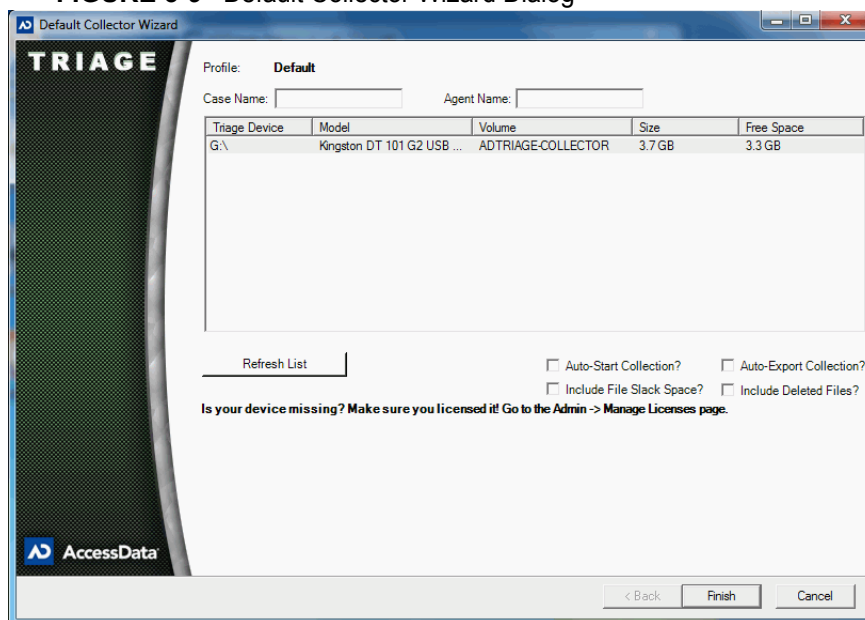


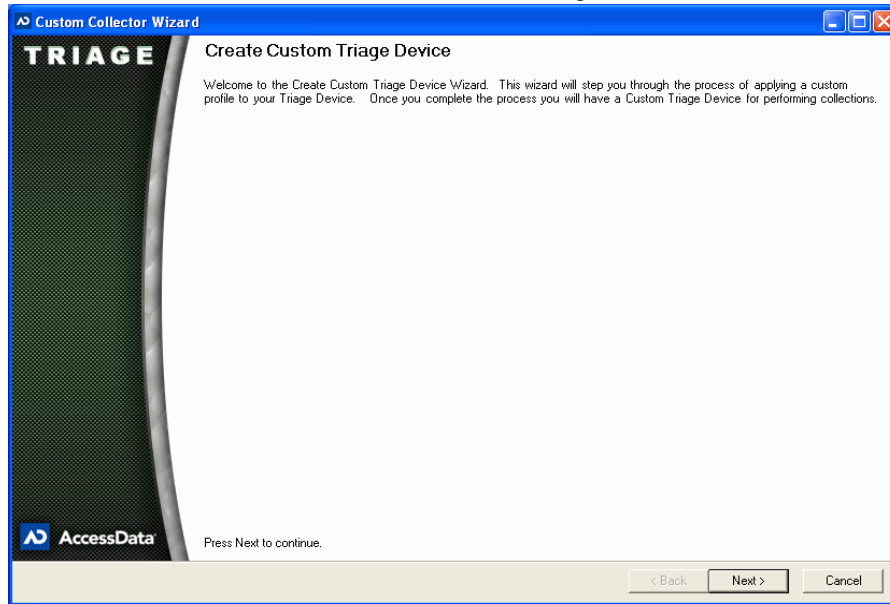
TABLE 3-9 Elements of the Default Collector Wizard Dialog

Interface Element	Description
Case Name Field	Enter the name of the case (optional).
Agent Name Field	Enter the name of the agent (optional).
Select USB Device Pane	Select the USB to which you want apply the Default profile.
Refresh List Button	Click to refresh the list of available devices.
Auto-Start Collection Check Box	Check to automatically start collection when booting to the target system.
Auto-Export Collection Check Box	Check to automatically export collected data to the USB device.
Finish Button	Click to make the selected USB device a Triage device.

Custom Collector Wizard Dialog

Open the *Custom Collector Wizard* dialog by clicking the **Custom Triage Device** button on the *Devices* tab of the Admin window. Use this wizard to apply one of your custom profiles to a licensed USB device (see [Creating a Standard Triage Device](#) page 25).

FIGURE 3-10 Custom Collector Wizard Dialog



Manage Triage Devices Dialog

Open the *Manage Triage Devices* dialog by clicking the **Manage Triage Devices** button on the *Devices* tab of the *Admin* window. Use this window to save collected evidence, review collected evidence, generate reports, and delete collected evidence (see [Saving Collected Data](#) page 34). Use the following figure and table to understand the elements in the *Manage Triage Devices* dialog.

FIGURE 3-11 Manage Triage Devices Dialog

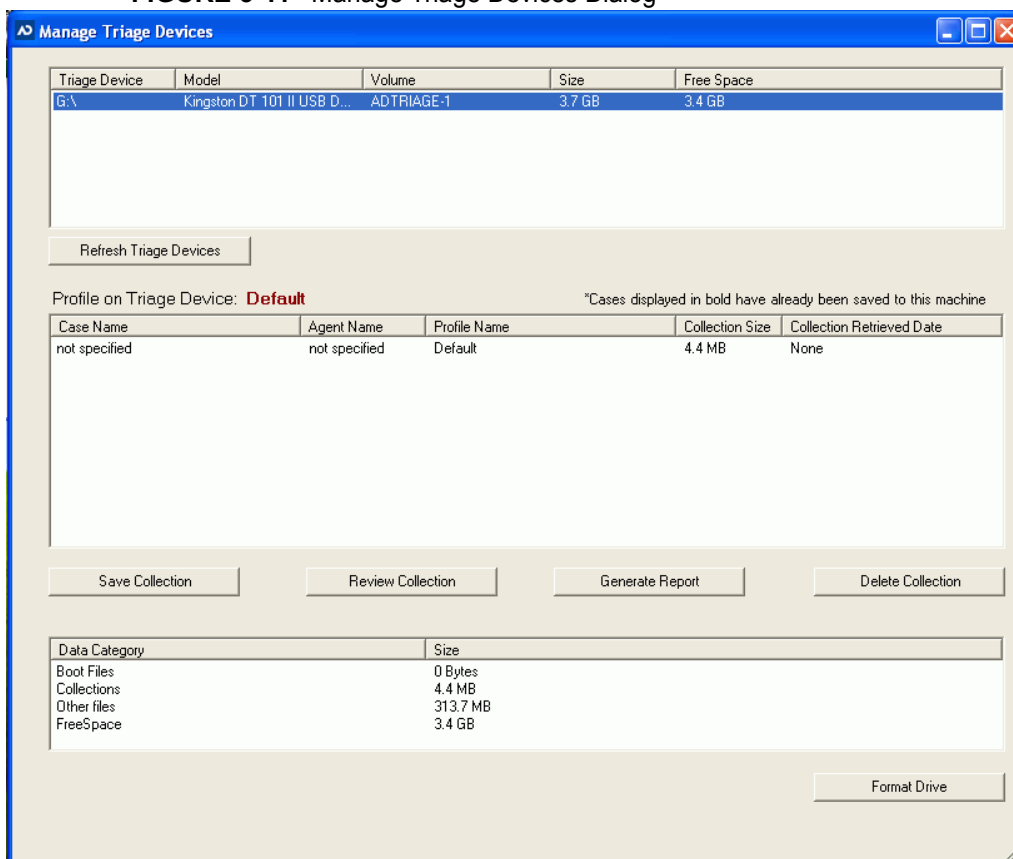


TABLE 3-10 Elements of the Manage Triage Devices Dialog

Devices Pane	Lists the connected Triage USB Devices.
Refresh Triage Devices Button	Click to refresh the Devices pane.
Profile on Triage Device	Lists the name of the profile on the selected Triage device.
Collection Pane	Lists the Case Name, Agent Name, Profile Name, Collection Size, and Collection Retrieved Date for each collection on the selected Triage device.
Save Collection Button	Click to save the selected collection in the Triage files.
Review Collection Button	Click to review the selected collection.
Generate Report Button	Click to generate a report of the selected collection.
Delete Collection Button	Click to delete the selected collection from the USB device.
Evidence Pane	Lists file sizes for the selected USB device.
Format Drive Button	Click to reformat the selected USB device. This will delete all existing data on the device.
License Count	This will appear at the bottom of the dialog if you signed up for an unlimited amount of devices license, but a limited amount of recoveries. The count of total and available licenses are listed here.

Collection Interface Overview

The *Collection* interface is the what you see when you are collecting data on a target system. You can either boot this interface from a shutdown system or launch the interface from a Triage USB device on a live system. Use the following sections as a guide when working with the *Collection* interface.

[About Collecting Data on a Target System](#) page 28

[Collecting Data from a Live System](#) page 29

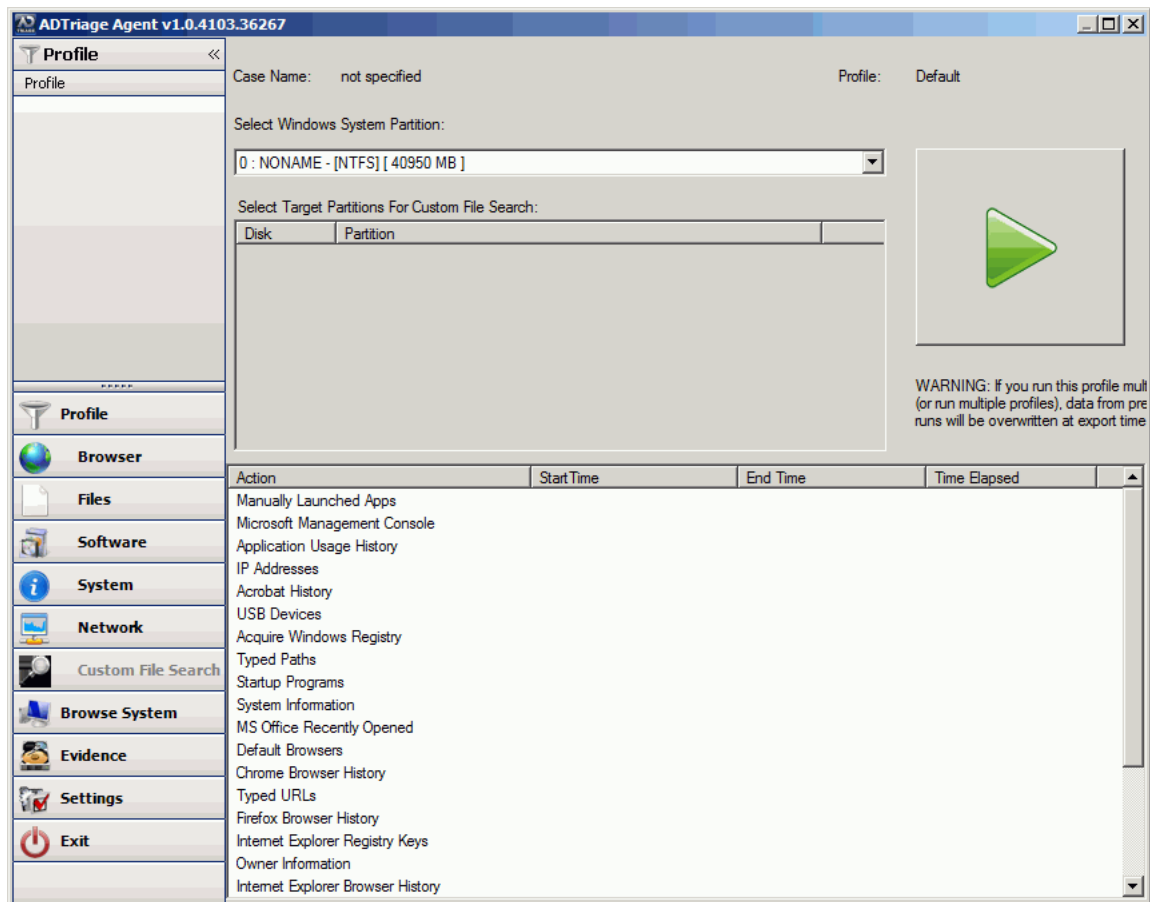
[Booting AD Triage on a Target System](#) page 29

[Automatically Collecting Data on a Target System](#) page 30

[Manually Collecting and Exporting Data on a Target System](#) page 30

Use the following figure and table to understand the elements of the Triage *Collection* interface.

FIGURE 3-12 Collection Interface Profile Tab



The tabs of the *Collection* interface can appear in the following colors:

- Black: Indicates that collection has not yet begun.
- Orange: Indicates that collection is in process.
- Green: Indicates that collection is complete.
- Red: Indicates that user action is still required.

TABLE 3-11 Elements of the Collection Interface

Case Name	Name saved to the Triage USB device when it was created.
-----------	--

TABLE 3-11 Elements of the Collection Interface (Continued)

Profile	Name of the profile applied to the Triage USB device.
Select Windows System Partition Drop-down	Expand drop-down to select a Windows system partition.
Select Users for User-specific Action Data Pane	Check the items from which you want to collect data.
Play Button	Click to start collection.
Action Pane	Lists the actions that will be performed during collection.
Log of Profile Runs Pane	Lists the date and time information for actions performed during collection.
Browser Tab	Displays the status of collection of Browser files.
Files Tab	Displays the status of collection of computer files.
Software Tab	Displays the status of collection of software files.
System Tab	Displays the status of collection of system files.
Network	Displays the status of collection of network files.
Browse System Tab	Click to select specific collected data and create AD1 and RAW files.
Evidence Tab	Click to export collected data, or to view the status of exported collected data.
Settings Tab	Click to view and edit the settings of the <i>Collection</i> interface.
Exit	Click to close the <i>Collection</i> interface.

Performing Basic Triage Tasks

This chapter explains the basic tasks that you can perform with Triage.

About Triage Profiles

Triage profiles allow you to hold and track all the collections for a single case. You can create a new profile for every case and collect multiple target systems for each profile. You can only have one profile on a USB device at a time. You must have a different USB device for every profile.

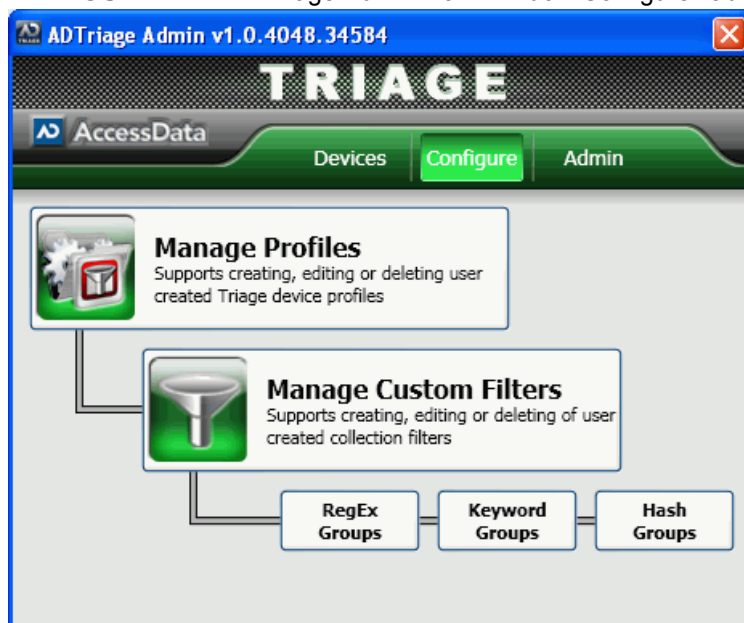
Creating a Profile

Profiles are used to hold collections. Profiles can contain multiple collections. You can create a new profile for each of your cases.

To create a profile

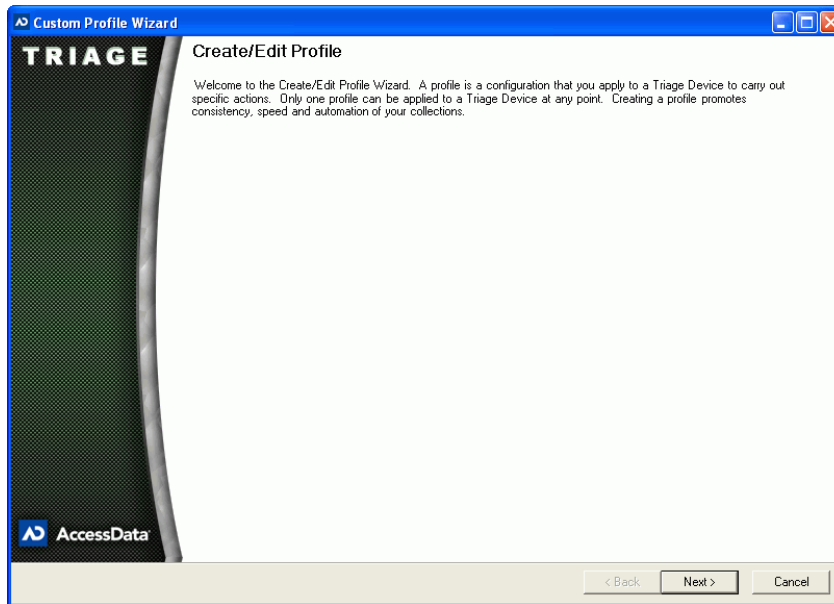
1. Open the *AD Triage Admin* main window (see [Launching AD Triage Admin](#) page 6).
2. Select the **Configure** tab.

FIGURE 4-1 AD Triage Admin Main Window Configure Tab



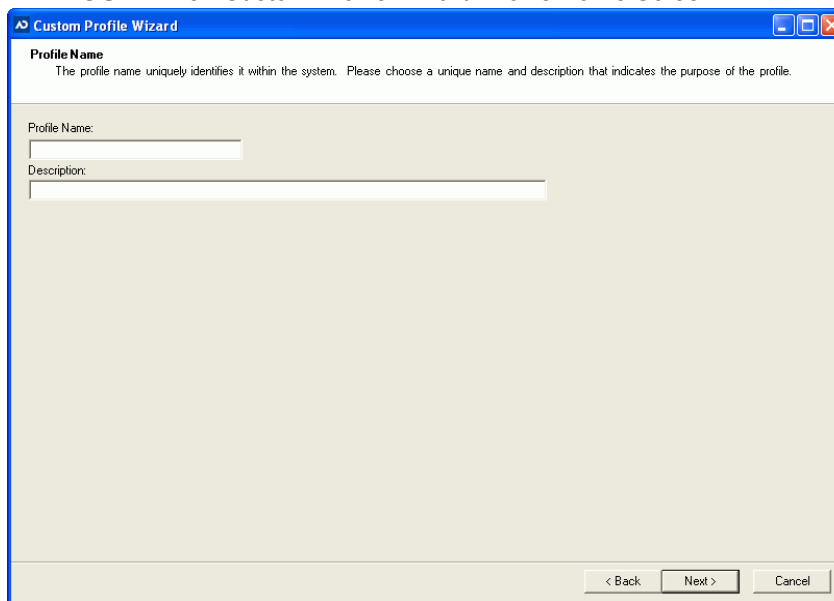
3. Click **Manage Profiles** (see [Profiles Dialog](#) page 10).
4. In the *Profiles* dialog, click **Create New Profile**.

FIGURE 4-2 Custom Profile Wizard Welcome Screen



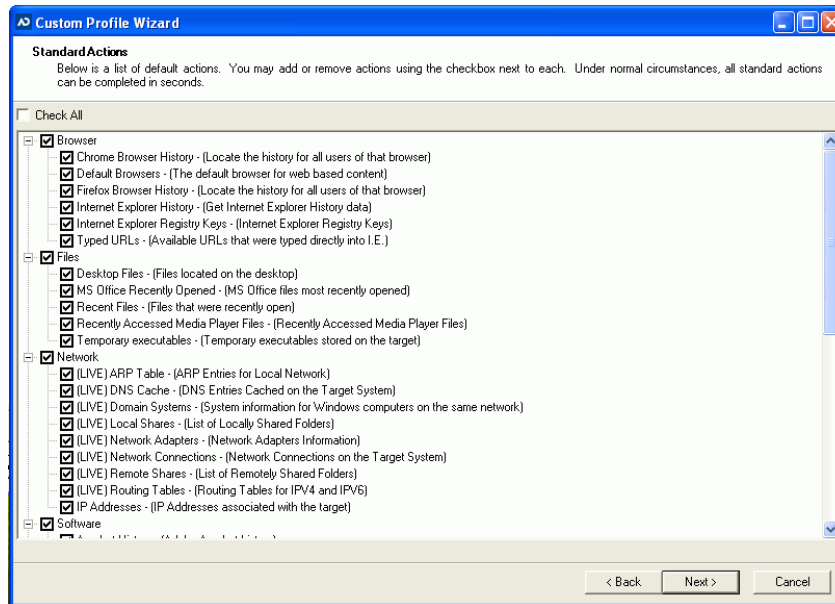
5. Click **Next**.

FIGURE 4-3 Custom Profile Wizard Profile Name Screen



6. In the *Profile Name* screen, enter a name and description for the profile and then click **Next**.

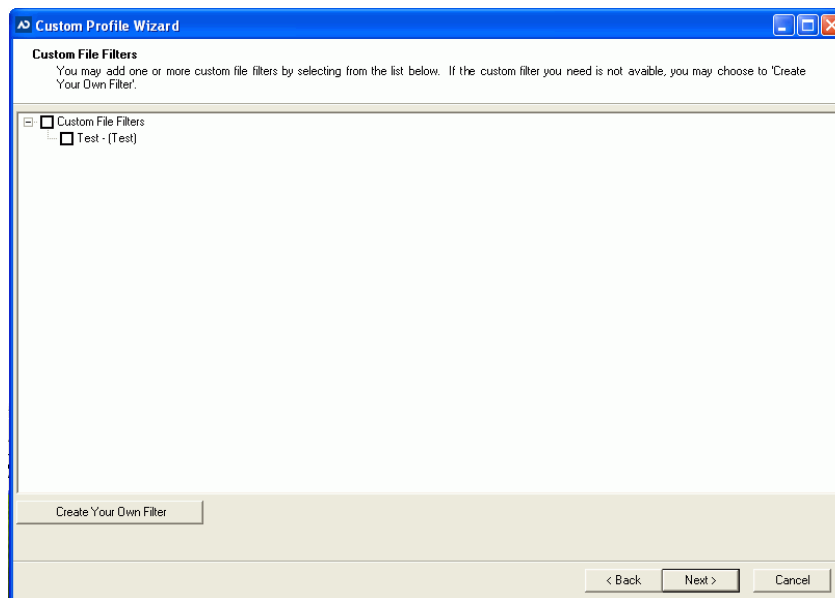
FIGURE 4-4 Custom Profile Wizard Standard Actions Screen



7. In the *Standard Actions* screen, check the actions from the default list that you want the profile to perform during collection and then click **Next**.

Note: All standard actions are selected by default.

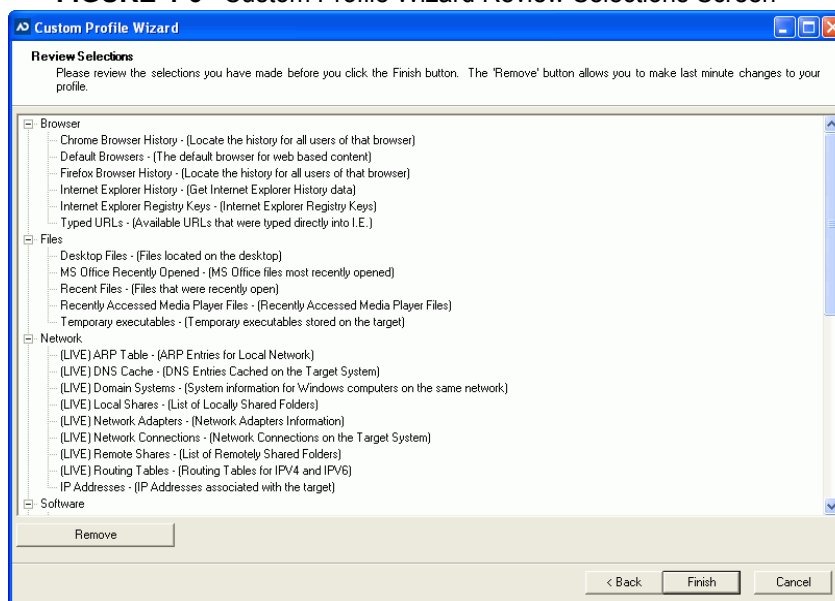
FIGURE 4-5 Custom Profile Wizard Custom File Filters Screen



8. In the *Custom File Filters* screen, check the custom filters that you want the profile to apply during collection and then click **Next**.

Note: You may, at this time, create a custom filter by clicking the **Create Your Own Filter** button. See [Creating a Custom Filter](#) page 41 for more information on how to do this.

FIGURE 4-6 Custom Profile Wizard Review Selections Screen



9. In the *Review Selections* screen, review the actions you have selected to ensure that you want them applied to the profile. If you want to remove any of the actions, highlight the item and click the **Remove** button.
10. Click **Finish**.
11. Click **Yes**.

Managing Licenses

Before you can apply a profile to a device for collection, you must first license the device. You can use one license per device and one profile per device.

See [Appendix A Managing Security Devices and Licenses](#) page 51.

Note: Though you can only apply one profile to a device, devices can carry multiple collections.

Triage provides a single licensed USB device. There is no limit to number of collections or volume of data per collection

Note: Multiple licenses can be associated with a single admin console for large organizations

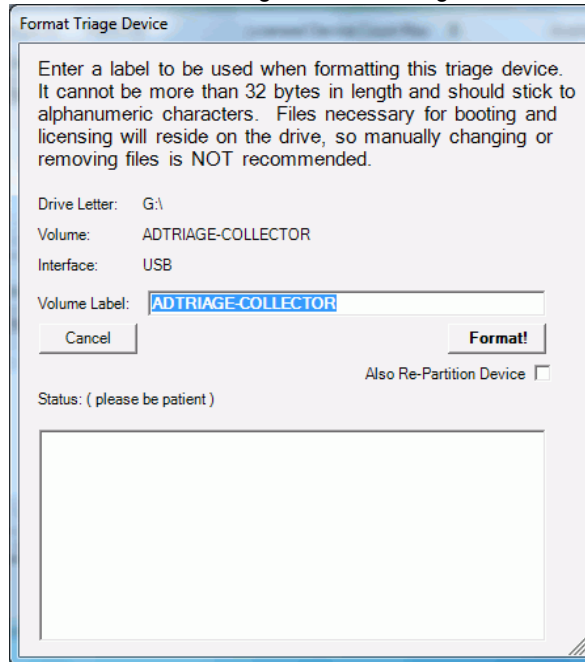
If you have a license that limits the number of USB devices you can license, the available license count appears at the top of the *Manage Licenses* dialog.

Note: If you run out of licenses for USB devices, contact the AccessData sales team for information on how to get more licenses.

To license a device

1. On the *Admin* tab, click **Manage Licenses** (see [Manage Licenses Dialog](#) page 9).
2. In the *Manage Licenses* dialog, select the device you want to license from the lower pane and click **License**.

FIGURE 4-7 Format Triage Device Dialog



3. In the *Format Triage Device* dialog, name the USB device in the *Volume Label* field.
4. Click the **Format!** button.

Triage will format the device. You can view the status of the device in the *Status* pane. If an error occurs, follow the steps in the *Status* pane and attempt the format again. Or, check **Also Re-Partition Device** and try to format the device again if formatting fails. Formatting does the following things to the USB device:

 - Formats the device as a single NTFS partition
 - Makes the device bootable
 - Adds a license file

Important: Formatting a USB device will remove all media currently on the device. Make sure that you don't have any wanted data on the USB device. You cannot save more than one profile to a USB device. Each profile must have its own device. However, you can collect multiple target systems to one USB device.

Note: Formatting the device makes the device bootable. So, when booting to a target system, you can boot to the USB device and it will run the Triage collection console. (See [Booting AD Triage on a Target System](#) page 29 for more information on booting to a USB device.)
5. Click **OK**.

The USB device should now appear in the upper license pane of the *Manage License* dialog.

Creating a Triage USB Device

When you create a Triage USB device, you save the profile and all of the actions associated with the profile to the USB device. This allows you to collect data from a target system using the criteria you set up on the selected profile.

There are two types of Triage device creation:

- *Standard Triage Device*: This uses the Default profile automatically.
- *Custom Triage Device*: This allows you to select a profile to save to the device.

Note: You can only create Triage USB devices using devices that you have already licensed. See [Managing Licenses](#) page 23 for information on how to license your device.

Creating a Standard Triage Device

The *Standard Triage Device* option uses the Default profile when initializing the USB device. Any actions applied to the Default profile will be applied to the USB device. There can only be one profile on a device at a time. Putting a new profile on a device with an existing profile will delete any data you have on the device.

You can change the Default profile by using the *Manage Profiles* feature (see [About Triage Profiles](#) page 20).

Note: Although you can edit the Default profile, you cannot change the name of the profile.

To create a standard USB device

1. In the *AD Triage* main window, click on the **Devices** tab.
2. Click on the **Standard Triage Devices** button (see [Default Collector Wizard Dialog](#) page 14).
3. In the *Default Collector Wizard* dialog, enter a **Case Name** and **Agent Name** (optional).
4. Select the USB device that you want to make into a Triage device.
Note: If you do not see the device that you are looking for, ensure that the device is attached to the computer. Then, ensure that the device is licensed (see [Managing Licenses](#) page 23).
5. Check **Auto-start collection** if you want Triage to automatically collect data on the target system upon start up.
Note: When a user selects the Auto-Start option, and the target has multiple partitions, the Triage Agent will use the Registry from the partition with the most used space and will use all partitions when performing custom file searches.
6. Check **Auto-export** if you want Triage to automatically export collected data to the USB device.
7. Check **Include File Slack Space** to include slack-space on files during collection.
8. Check **Include Deleted Files** to include deleted files during collection.
9. Click **Finish**.
Note: If you already have a profile on the device, a message appears asking you if you want to copy over the existing profile. Click **Yes** to delete the existing profile on the device and apply the new one.
10. In the confirmation message that appears, click **OK**.

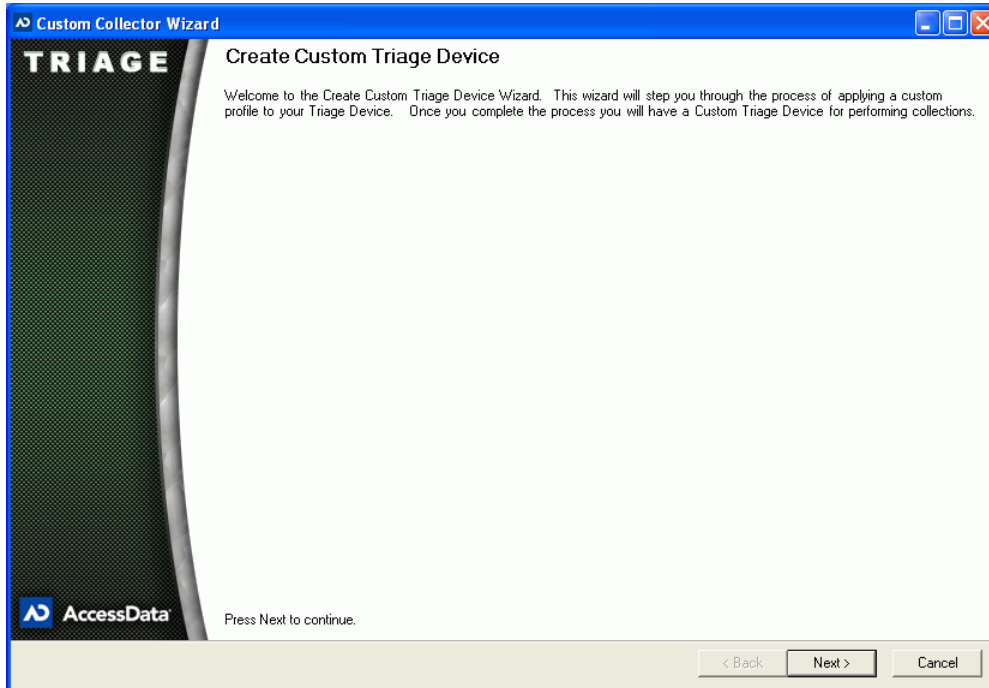
Creating a Custom Triage Device

The Custom Triage Device option allows you to select a custom profile that you want to use for the USB device.

To create a custom USB device

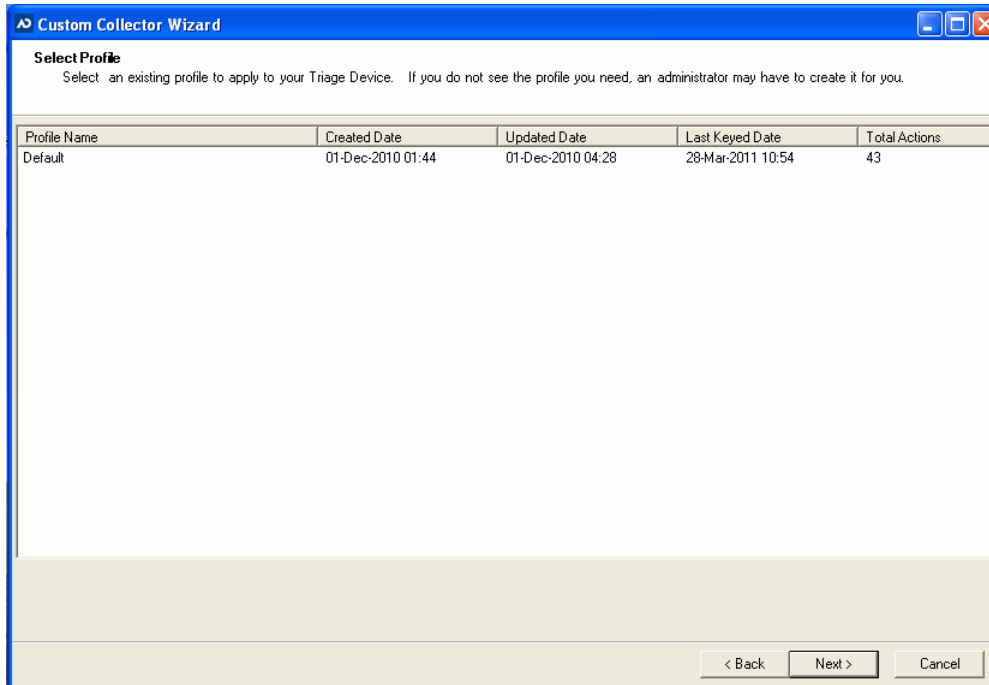
1. In the *AD Triage* main window, click on the **Devices** tab.
2. Click on the **Custom Triage Devices** button.

FIGURE 4-8 Custom Collector Wizard Welcome Screen



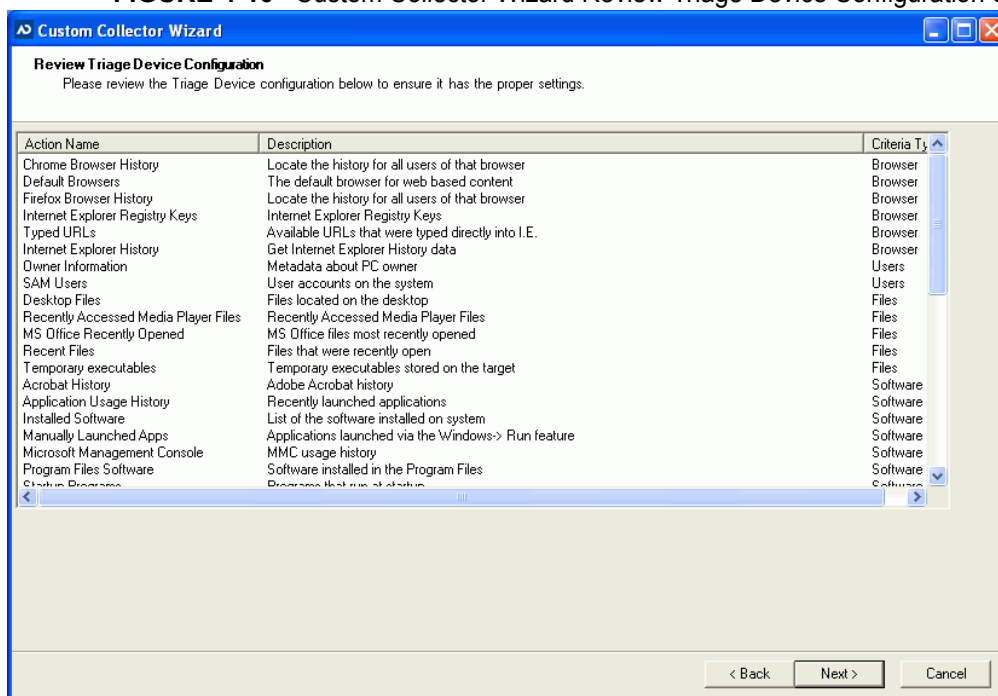
3. In the *Custom Collector Wizard Welcome* screen, click **Next**.

FIGURE 4-9 Custom Collector Wizard Select Profile Screen



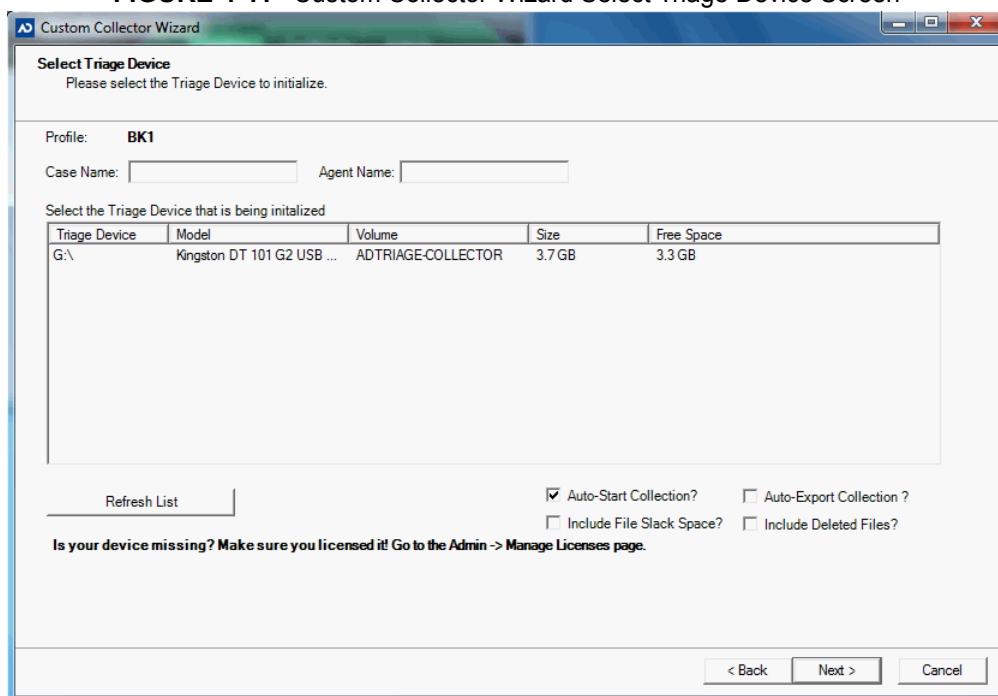
4. In the *Select Profile* screen, select the profile that you want to use during collection.

FIGURE 4-10 Custom Collector Wizard Review Triage Device Configuration Screen



5. Review the Triage device configuration and click **Next**.

FIGURE 4-11 Custom Collector Wizard Select Triage Device Screen



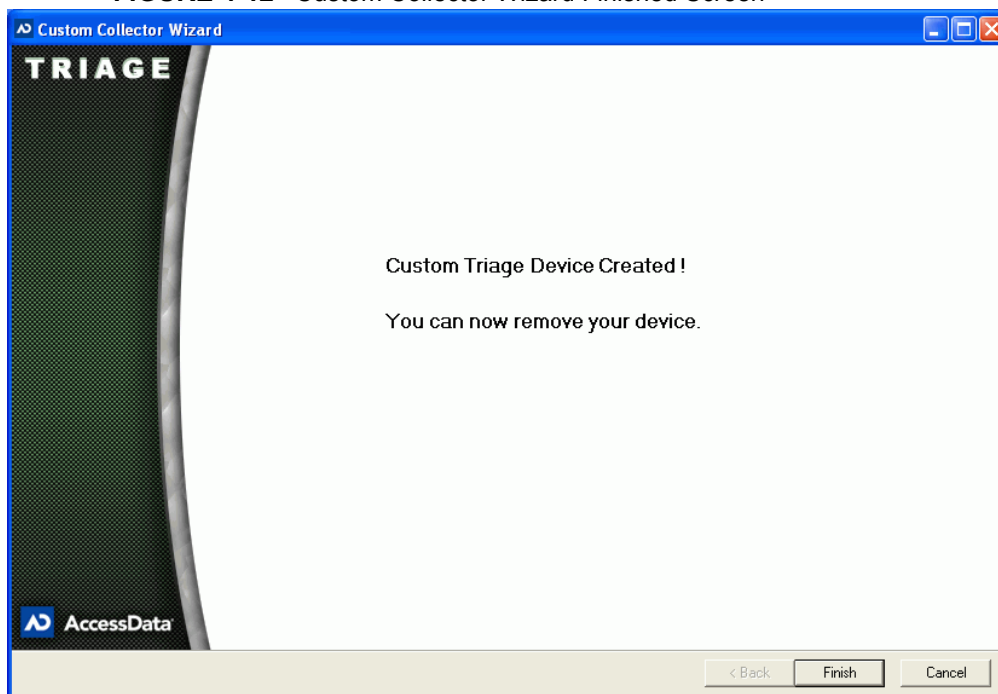
6. In the *Select Triage Device* screen, enter a *Case Name* and *Agent Name* for the device.

7. Select the USB device that you want to make into a Triage device.

Note: If you do not see the device that you are looking for, ensure that the device is attached to the computer. Then, ensure that the device is licensed (see [Managing Licenses](#) page 23).

8. Check to **Auto-start collection** if you want Triage to automatically collect data on the target system upon start up.
- Note:** When a user selects the Auto-Start option, and the target has multiple partitions, the Triage Agent will use the Registry from the partition with the most used space and will use all partitions when performing custom file searches.
9. Check **Auto-export** if you want Triage to automatically export collected data to the USB device.
10. Check **Include File Slack Space** to include slack-space during collection.
11. Check **Include Deleted Files** to include deleted files during collection.
12. Click **Next**.

FIGURE 4-12 Custom Collector Wizard Finished Screen



13. Click **Finish**.

Creating a Bootable Disc

If you are collecting data in the field, it is important to have not only a bootable USB device, but also a bootable copy of the Triage ISO on a disk. It is recommended that you use a disc burning application to burn the Triage ISO to a disc. Use the ADTriageBootable.iso (found on the disc you received with your software) to create a bootable disc.

About Collecting Data on a Target System

When you collect data on a Target System, you must have a USB device that is formatted as a Triage USB device. You must perform the steps in [Managing Licenses](#) page 23 and [Creating a Triage USB Device](#) page 25 to have a USB device that will collect data on a target system.

Additionally, if you are collecting data in the field, it is recommended that you burn the Triage ISO to a disk, and use the disk in the event that you cannot boot to your USB device. See [Creating a Bootable Disc](#) on page 28.

Once you have completed those tasks, you are ready to collect data on a target system. Triage is designed to collect data from a shut down or live system.

To collect data from a live system, see [Collecting Data from a Live System](#) page 29.

To perform a collection from a shut down system, you must first make the target system boot to the USB device or a bootable CD/DVD. See [Booting AD Triage on a Target System](#) page 29 for information on how to boot to the USB or CD/DVD drive.

After you have set the target system to boot to the USB device or CD/DVD drive, you can then restart the system and collect data. See [Automatically Collecting Data on a Target System](#) page 30 for information on what occurs during automatic collection.

Collecting Data from a Live System

You can use Triage to collect data from a live target system. To do this, you must have a bootable USB device or bootable Triage disk. Use the following sections for information on how to obtain these items:

[Managing Licenses](#) page 23

[Creating a Triage USB Device](#) page 25

[Creating a Bootable Disc](#) page 28

To collect data on a live system

1. Insert the Triage USB device into target system.
2. Do one of the following:
 - In the Windows prompt, select to run **AD Triage**.
 - Open the devices folder and run the **TriageAgent**.
3. In the Collection window, perform one of the following tasks:
 - Data will automatically be collected and exported if you selected Auto-Start Collection and Auto-Export Collection. See [Automatically Collecting Data on a Target System](#) page 30.
 - Manually collect the data from the target system. See [Manually Collecting and Exporting Data on a Target System](#) page 30.

Booting AD Triage on a Target System

You can use Triage to collect data from a shut down system, but to do this, you will need to boot the system to a Triage USB device, or a Triage disk. Use the following sections for information on how to obtain these items:

[Managing Licenses](#) page 23

[Creating a Triage USB Device](#) page 25

[Creating a Bootable Disc](#) page 28

This section describes how to set up the target system to boot to the USB device or disk.

To boot AD Triage on a target system

1. Insert the bootable disk or bootable USB device. (See [Creating a Bootable Disc](#) page 28 for more information on how to make a bootable disk.)
2. Start the target system and enter the BIOS.
Note: On Intel system boards, press **F2** or **F12** during start up to enter the BIOS. On non-Intel systems, press **Delete** or **Esc** during start up to enter the BIOS.
3. Edit the BIOS boot sequence to one of the following:
 - Make the CD/DVD drive boot before the hard drive if you are booting using a disk.
 - Make the USB boot before the hard drive if you are booting using the USB device (see [Managing Licenses](#) page 23 for making a bootable USB device).

4. Save and exit the BIOS.

Note: Press **CTRL > ALT > Delete** if the system has trouble booting. If this does not work, hold down the power button for 4 to 5 seconds.

Automatically Collecting Data on a Target System

The following steps occur after you have set the target system to boot to the USB device or CD/DVD drive, and you have restarted the target system:

1. The target system boots into Windows.
2. The AD Triage collection application launches.
3. AD Triage detects drives.
4. AD Triage collects the data for the profile on the USB device (if **Auto-Start Collection** was selected when creating a Triage USB).
5. AD Triage exports the data to the USB device (if **Auto-Export Collection** was selected when creating a Triage USB).
6. Close the *Collection* window and shut down the system.

Manually Collecting and Exporting Data on a Target System

If you did not check to Auto-start collection when you created your Triage USB device, you will need to manually start collection when on the target system.

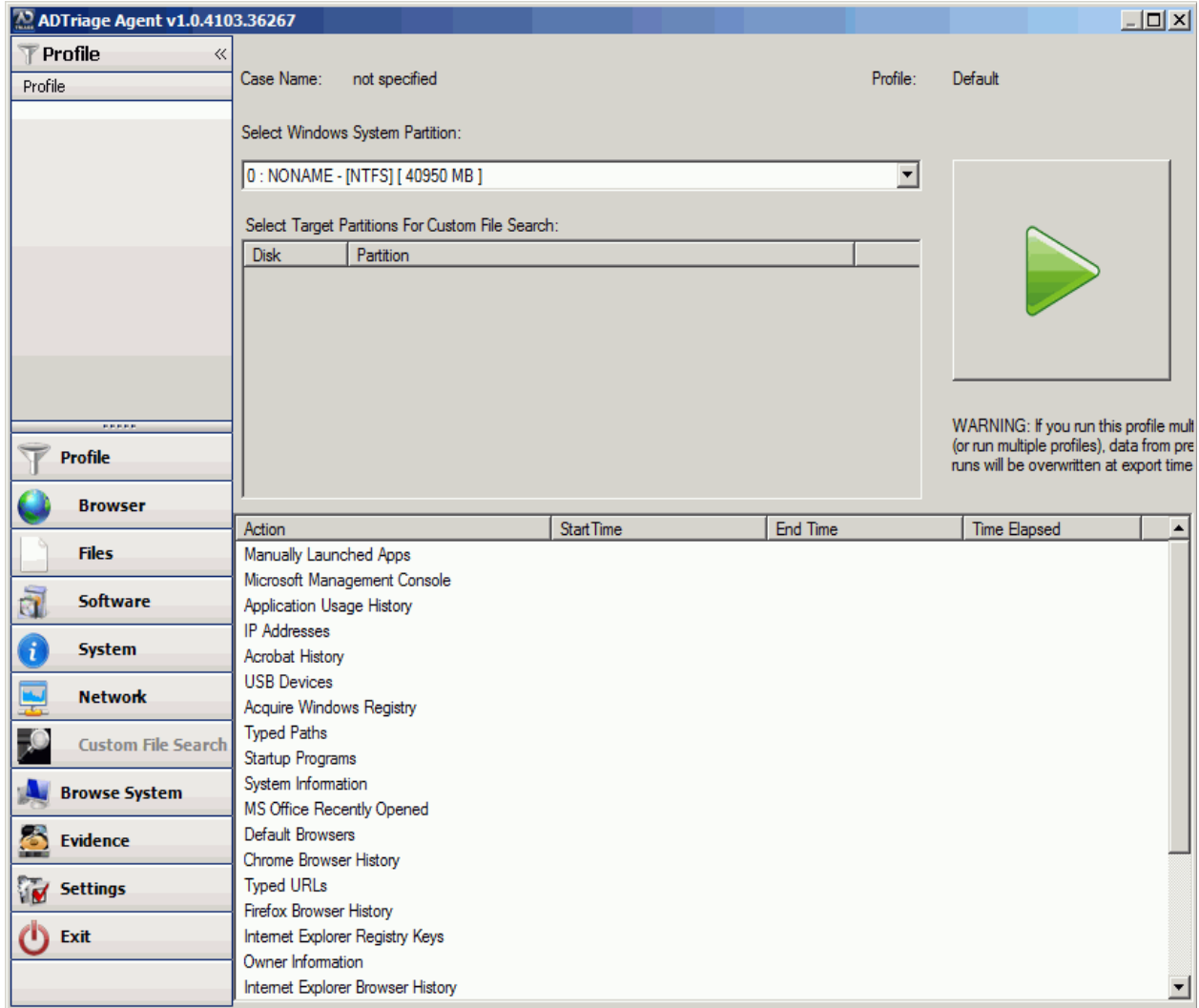
To manually collect data from a target system

1. After setting up the target system to boot to the USB device or CD/DVD drive, restart the computer.

The *AD Triage Collections* window opens.

Note: If the screen says that *No Profiles Were Found*, ensure that the licensed USB (with a profile on it) is connected and click the **Refresh Drives** button on the **Settings** tab.

FIGURE 4-13 Collection Interface

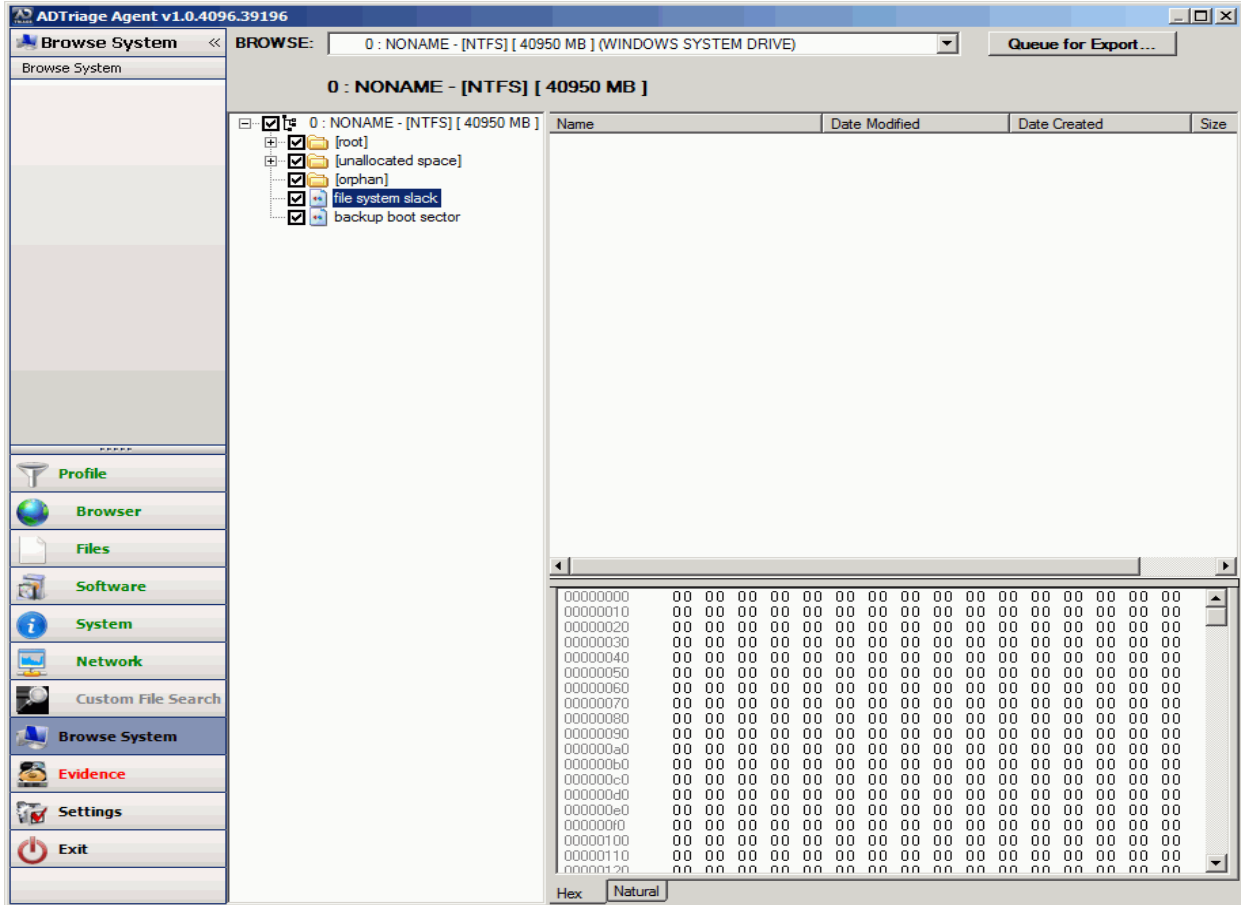


2. Click the **play** button on the *Profiles* tab.

Collection begins. You can identify the progress of the collection by the colors of the words on the tabs. Green indicates that the action has been completed.

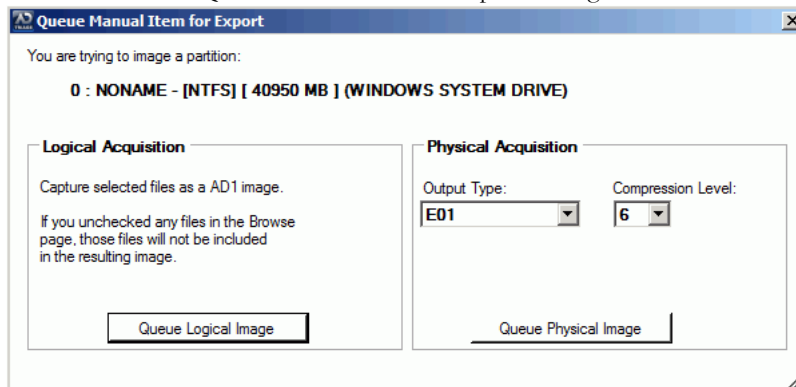
Note: If you checked to **Auto-Start Collection** when creating a Triage USB device, AD Triage will automatically collect data on the target system upon boot up. And the play button will not be available.

FIGURE 4-14 Collection Interface Browse System Tab



3. After collection is complete, you can select the Browse System tab and select the specific system drives that you want to acquire and click Queue for Export (optional).

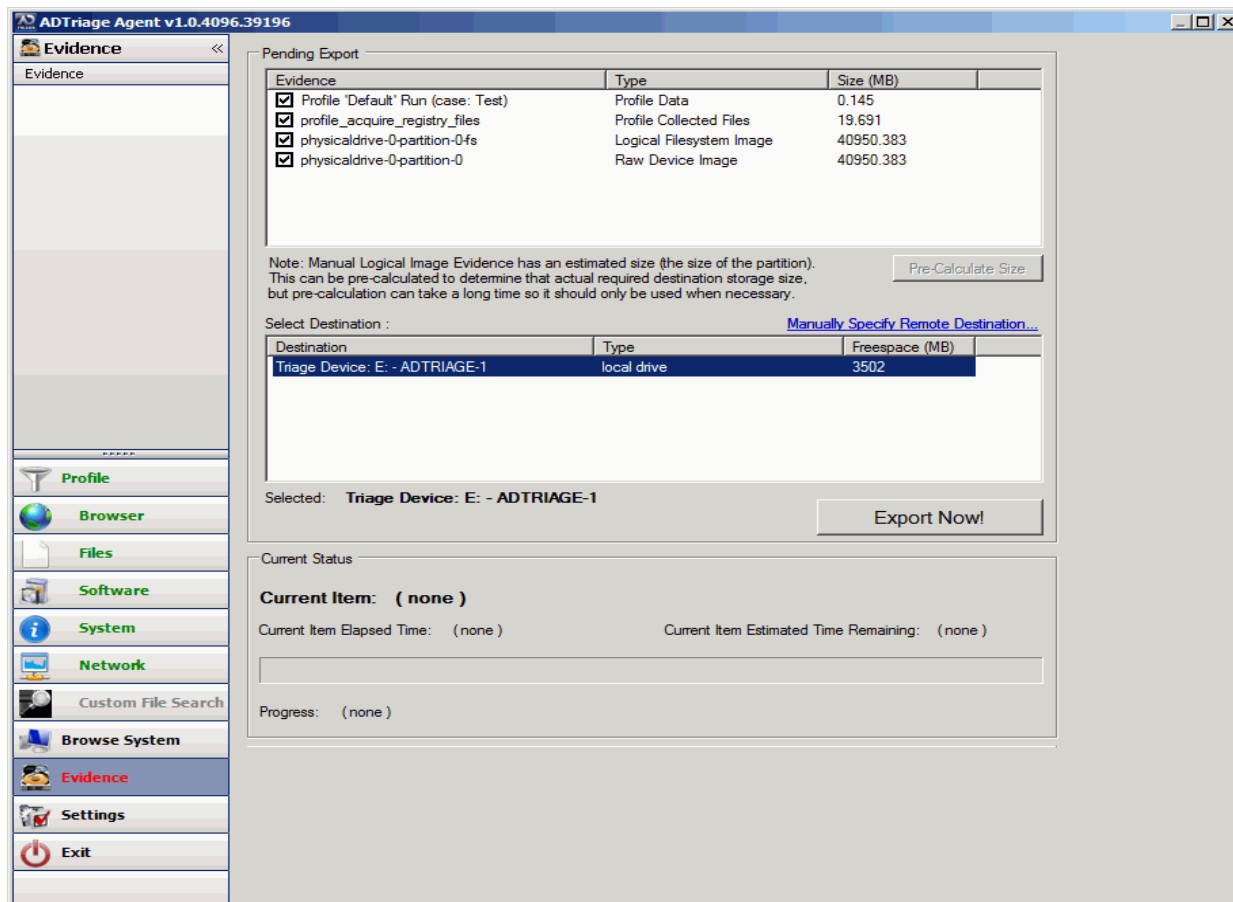
FIGURE 4-15 Queue Manual Item for Export Dialog



- 3a. In the Queue Manual Item for Export, do one of the following (optional):
 - In the Logical Acquisition group box, click Queue Logical Image to capture the selected files as an AD1 image. Exit the dialog.
 - In the Physical Acquisition group box, select the Output Type (E01, SMART, or RAW) and Compression Level that you want to acquire and click Queue Physical Image to create a physical evidence item. Exit the dialog.

- If there is data that has not been exported, the *Evidence* tab appears in red. Click on the **Evidence** tab.

FIGURE 4-16 Collection Interface Evidence Tab



- All data that still needs to be exported appears in the *Pending Export* pane. Select the items you want to export, select the location where you want to export the data, and click **Export Now!**.
Collected data and AD1 files are exported to the selected device/location. Data that was successfully exported appears in the *Successfully Exported* pane. When all the evidence has been exported, the *Evidence* tab appears in green.
- After you have exported your data, you can pre-calculate the estimated size of the export to determine the actual required destination storage size. But, pre-calculation can take a long time, so it should only be used when necessary. Click **Pre-Calculate Size** to perform this task.
- Click **Exit** to close the *Collection* window. If you have not exported all your evidence, you will be alerted that you have pending evidence.
- Shut down the system.
Note: Remember to reset the BIOS on the target system to boot from the hard drive first after you are done collecting data.

Using Kanguru and IronKey Encrypted Devices

If you are using a Kanguru and IronKey encrypted device when collecting data, the process differs slightly from non-encrypted keys. To use an encrypted key on a shutdown system, you must boot from a burned CD.

Collecting data using an encrypted key

1. Boot to the target system using a burned CD. See [Creating a Bootable Disc](#) on page 28.
2. Navigate to the helper application found on the cd-partition of the Kanguru or IronKey device and run it to decrypt the device.
Note: You may receive warning messages following this step, but the message will not prevent you from using the device. Close the message and continue to the next step.
3. Click **Rescan Drives**.
4. In the Triage Collection window, start the collection. See [Manually Collecting and Exporting Data on a Target System](#) on page 30.
5. After the collection is complete, click the **Settings** tab.
6. On the *Settings* tab, click **Run Program**.
7. Export the data to the device. See [Manually Collecting and Exporting Data on a Target System](#) on page 30.

Saving Collected Data

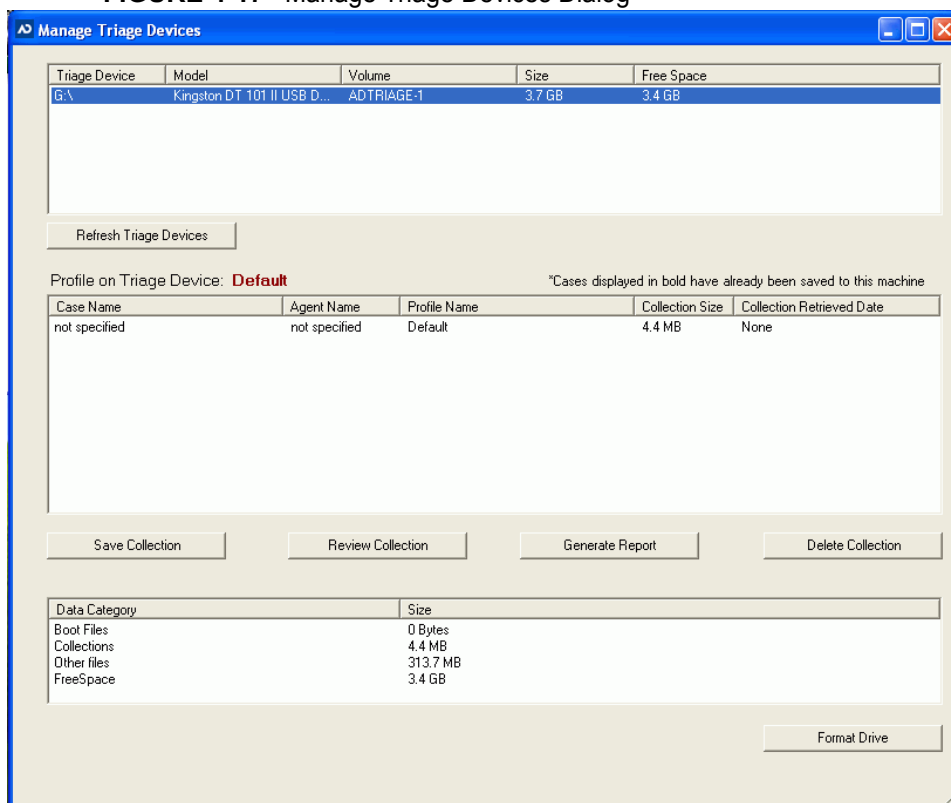
If you exported your collected data from a target system to your Triage USB device, you can save the data in Triage Admin, review the data, and generate reports.

Before saving a collection, ensure that you have enough available disk space on your Admin computer. If you do not have sufficient disk space, collections will not import completely.

To save collected data

1. Ensure that the USB device is connected to the computer.
2. In the *Triage Admin* console, click the **Devices** tab.
3. Click **Manage Triage Devices**.

FIGURE 4-17 Manage Triage Devices Dialog



4. Select the USB device that contains the collections that you want to save from the upper pane.
5. Collections appear in the middle pane, select the collection that you want to save.
Note: You can review collections, generate reports and delete collections from this dialog. More information on performing these tasks are covered in [Managing Saved Collections](#) page 35.
6. Click **Save Collection**.
7. In the Save Collection dialog, browse to the location where you want the case data to save.
The collection is saved in the designated location.
8. Close the dialog.

Managing Saved Collections

Once you have saved your collected data, you can then review it, generate reports, and export the collection from the *Manage Collections* dialog. You can view a list of all the saved collections in the *Manage Collections* dialog. This section will help you filter and manage all your saved collections.

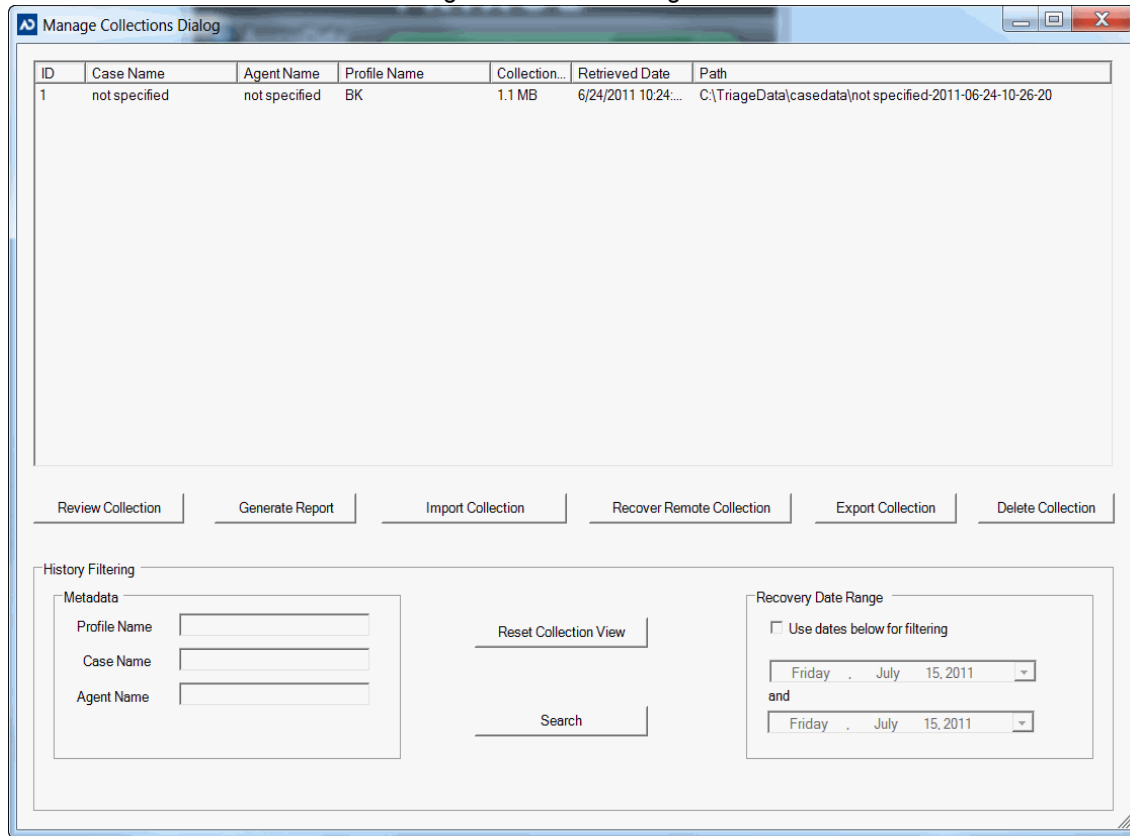
Filtering Saved Collections

The list of collections in the *Manage Collections* dialog is a list of ALL the collections saved to AD Triage. If you are looking for a specific collection, you may need to filter the list to find the collection you are looking for.

To filter saved collections

1. In the *Admin* console, click the **Admin** tab (see [Triage Admin Main Window](#) page 6).
2. Click the **Manage Saved Collections** button.

FIGURE 4-18 Manage Collections Dialog



3. In the *Manage Collections* dialog, you can filter the list of collections by specifying the name of the profile, the name of the case, the name of the agent, and/or a specified date range. Enter your filtering criteria and click **Search**.
4. Once you have found the collection(s) you are looking for, you can perform the following actions:
 - Review the collection [Reviewing Saved Collections](#) page 36
 - Generate a report [Generating Reports for Saved Collections](#) page 37
 - Export the collection [Exporting Saved Collections](#) page 46
 - Delete the collection [Deleting a Saved Collection](#) page 47
 - Import a collection [Importing a Saved Collection](#) page 47
 - Recovering a Remote Collection [Recovering a Remote Collection](#) page 47

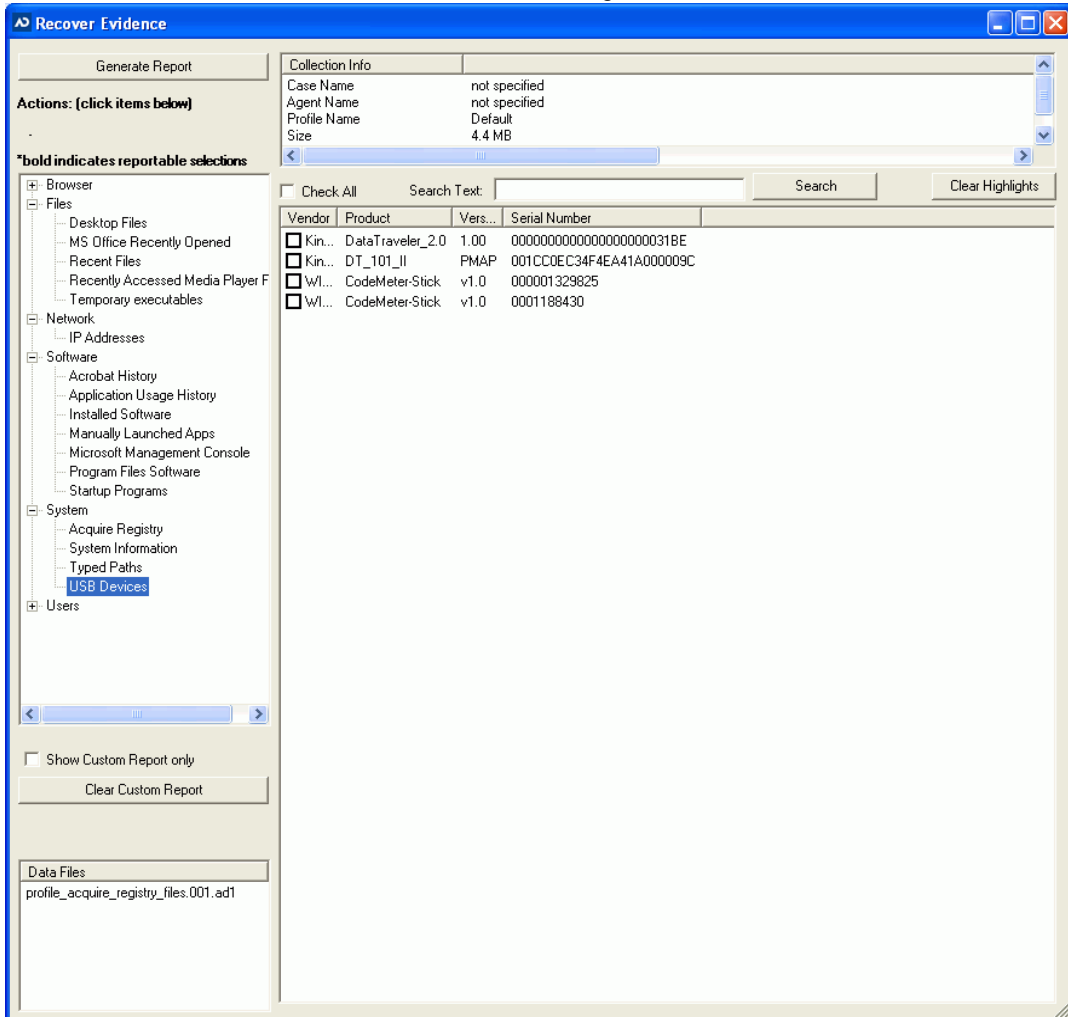
Reviewing Saved Collections

Once you have found the collection/s you are looking for in the *Manage Collections* dialog using the filters (see [Filtering Saved Collections](#) page 35), you can then review the collected data.

To review saved collections

1. In the *Manage Collections* dialog, select the collection that you want to review (see [Filtering Saved Collections](#) page 35).
2. Click **Review Collection**.

FIGURE 4-19 Recover Evidence Dialog



3. In the *Recover Evidence* dialog, use the left panes to navigate the collected data and the AD files created during collection. Check the files that you would like to include in a custom report.
4. Click **Generate Report** to create a report of the collection, then follow the steps found in [Generating Reports for Saved Collections](#) page 37.
5. Close the *Recover Evidence* dialog.

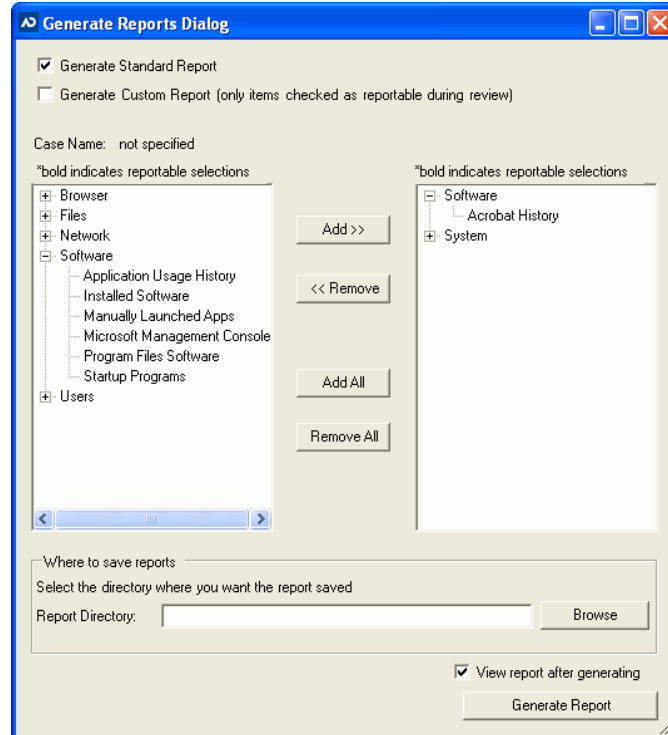
Generating Reports for Saved Collections

Once you have found the collection/s you are looking for in the *Manage Collections* dialog using the filters (see [Filtering Saved Collections](#) page 35), you can then generate a report of the collected data.

To generate a report for a saved collection

1. In the *Manage Collections* dialog, select the collection for which you want to generate a report (see [Filtering Saved Collections](#) page 35).
2. Click **Generate Report**.

FIGURE 4-20 Generate Reports Dialog



3. Check whether you want to generate a *Standard* or *Custom Report*.
4. Highlight the collected data that you want to include in your report and click **Add**.
Note: Items in bold are those items that you selected when you reviewed your data.
5. **Browse** to the location where you would like to save the generated report.
6. Check **View report after generating** to open the report after it has been generated.
7. Click **Generate Report**.
8. Click **OK**.
If you checked to view the report, it opens in an internet browser.

Performing Advanced Triage Tasks

This chapter describes advanced tasks that can be performed using AD Triage.

Advanced Profile Tasks

In addition to creating a new profile ([Creating a Profile](#) page 20), you can also perform the following tasks:

- Copy a Profile [Copying a Profile](#) page 39
- Edit a Profile [Editing a Profile](#) page 40
- Delete a Profile [Deleting a Profile](#) page 41

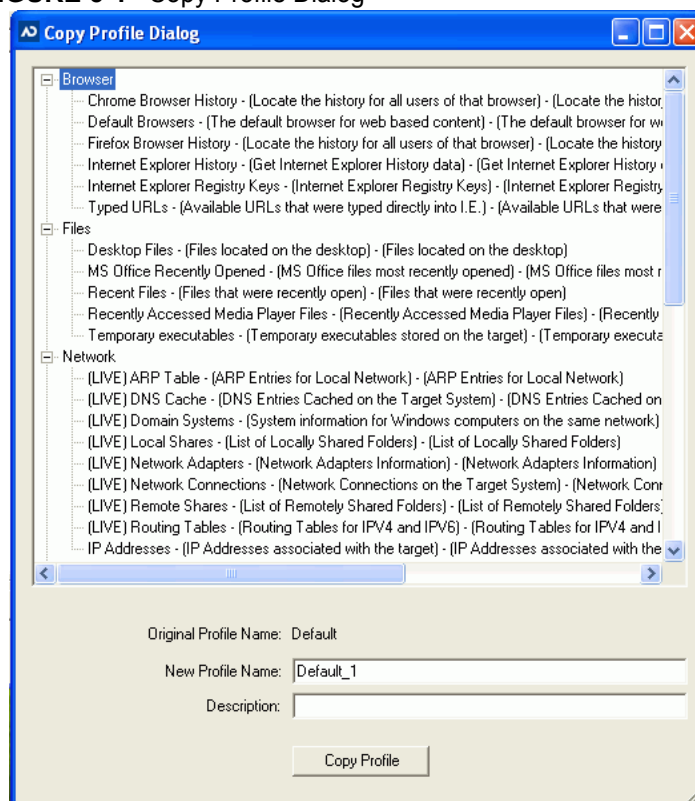
Copying a Profile

If you want to create a profile that is very similar to an existing profile, but you don't want to have to go through the process of creating a new profile, you can use the copy profile feature.

To copy a profile

1. Open the *AD Triage Admin* main window (see [Launching AD Triage Admin](#) page 6).
2. Select the **Configure** tab (see [AD Triage Admin Main Window Configure Tab](#) page 20).
3. Click **Manage Profiles** (see [Profiles Dialog](#) page 10).
4. In the *Profile* dialog, select the profile that you want to copy and then click **Copy Profile**.

FIGURE 5-1 Copy Profile Dialog



5. In the *Copy Profile* dialog, review the actions for the profile and enter a **New Profile Name** and **Description**.
6. Click **Copy Profile**.
7. Click **OK**.

Editing a Profile

You may want to edit an existing profile to remove or add actions to the profile.

Note: You can edit the actions of the *Default* profile, but you cannot edit the profile name.

To edit an existing profile

1. Open the *AD Triage Admin* main window (see [Launching AD Triage Admin](#) page 6).
2. Select the **Configure** tab (see [AD Triage Admin Main Window Configure Tab](#) page 20).
3. Click **Manage Profiles** (see [Profiles Dialog](#) page 10).
4. In the *Profile* dialog, select the profile that you want to edit and click **Edit Profile** (see [Custom Profile Wizard Welcome Screen](#) page 21).
5. Click **Next** (see [Custom Profile Wizard Profile Name Screen](#) page 21).
6. Edit the **Profile Name** or **Description** if desired, and click **Next** (see [Custom Profile Wizard Standard Actions Screen](#) page 22).
7. Edit the standard actions that you want included with the profile and click **Next** (see [Custom Profile Wizard Custom File Filters Screen](#) page 22).
8. Edit the custom file filters that you want included with the profile and click **Next** (see [Custom Profile Wizard Review Selections Screen](#) page 23).
9. Review the actions applied to the profile and click **Finish**.
10. Click **Yes**.

Deleting a Profile

If you want to remove a profile from Triage, you can delete it as long as it is not the default profile.

To delete a profile

1. Open the *AD Triage Admin* main window (see [Launching AD Triage Admin](#) page 6).
2. Select the **Configure** tab (see [AD Triage Admin Main Window Configure Tab](#) page 20).
3. Click **Manage Profiles** (see [Profiles Dialog](#) page 10).
4. In the *Profile* dialog, select the profile that you want to delete and click **Delete Profile**.
5. Click **Yes**.

About Custom Filters

In the *AD Triage Admin* console, you can create custom filters, create and add custom conditions to the filters, and add your custom filters to profiles as actions to be performed during collection.

Note: Triage only supports binary / plain text keyword searching. Which means any compound or compressed file will most likely not produce the desired results since these files are searched from a binary perspective. FTK supports archive expansion and filtered text searching of compound documents.

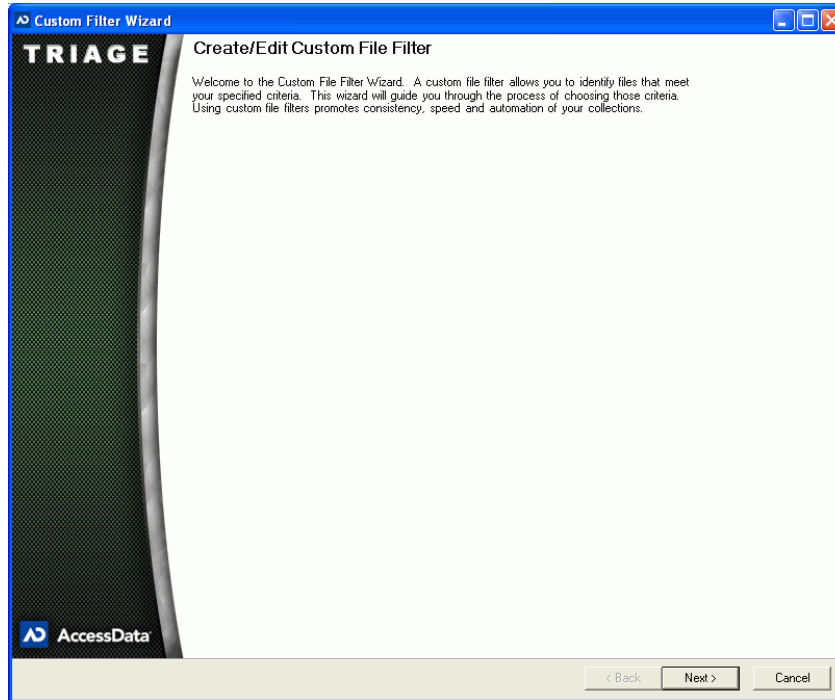
Creating a Custom Filter

Custom filters look for files that contain specified attributes when collecting data. You can apply custom filters to profiles before creating a Triage device.

To create a custom filter

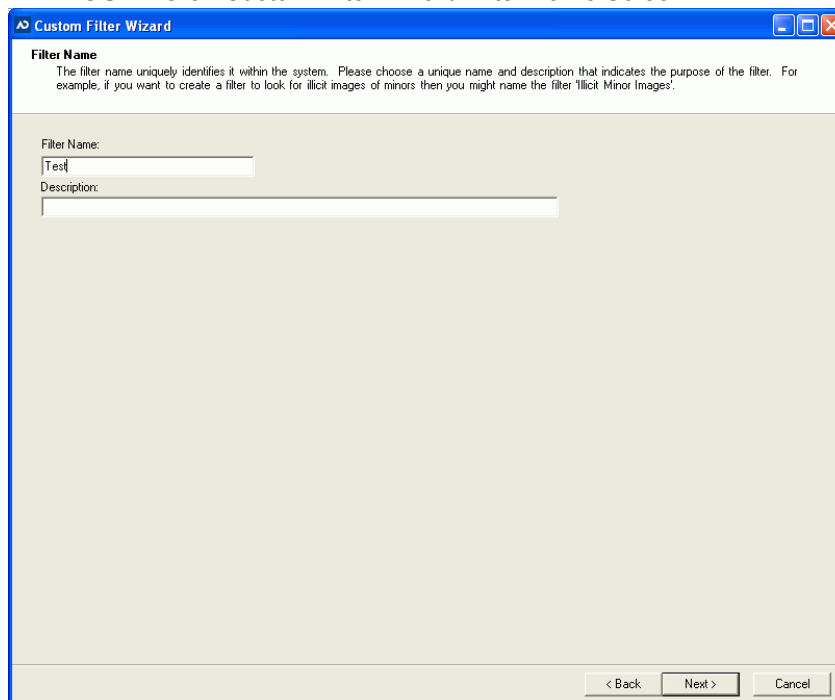
1. Open the *AD Triage Admin* main window (see [Launching AD Triage Admin](#) page 6).
2. Select the **Configure** tab (see [AD Triage Admin Main Window Configure Tab](#) page 20).
3. Click **Manage Custom Filters** (see [File Filtering Dialog](#) page 11).
4. In the *File Filtering* dialog, click **Create New Filter**.

FIGURE 5-2 Custom Filter Wizard



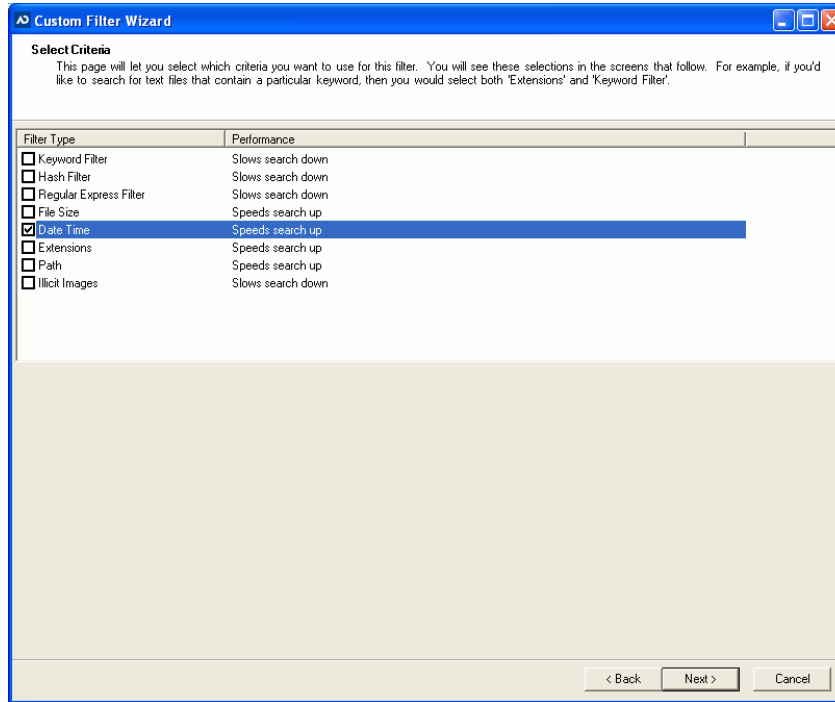
5. In the *Custom Filter Wizard*, click **Next**.

FIGURE 5-3 Custom Filter Wizard Filter Name Screen



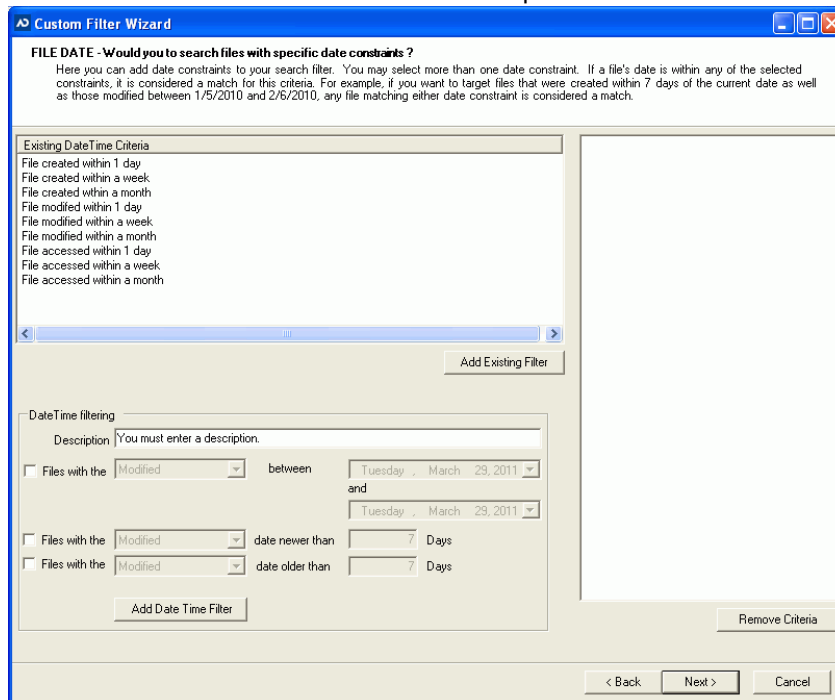
6. In the *Filter Name* screen, enter a name and description for the filter and then click **Next**.

FIGURE 5-4 Custom Filter Wizard Select Criteria Screen



7. In the *Select Criteria* screen, check the types of groups you want included in your custom filter and then click **Next**.

FIGURE 5-5 Custom Filter Wizard Groups Screen



8. Depending on the groups that you checked, the next screen allows you to add the specific criteria for each group to the custom filter. The following screens may appear:

- Keyword (see [Creating a Keyword Group](#) page 44)
- Hash (see [Creating a Hash Group](#) page 45)
- Regular Expression (see [Creating a Regular Expression Group](#) page 45)
- File Size

Note: When applying a *File Size* filter, the filter will search for the “Size on Disk” file capacity rather than the “Size” capacity when collecting data. Increase the size of your file search accordingly to accommodate this.

- Date Time
- Extensions
- Path
- Illicit Images

Note: Multiple conditions added under a single group name are considered an “OR” condition. Each separate group name added is considered an “AND” condition.

9. Add your criteria for each group and click **Next** until you reach the *Review Custom File Filter Constraints* screen.
10. Click **Finish**.
11. Click **OK**.

Note: To add the filter to a profile, click the **Update Profile** button on the *File Filtering* dialog.

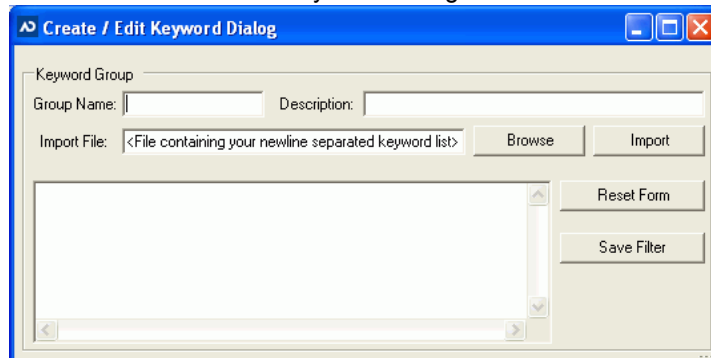
Creating a Keyword Group

The keyword feature allows you to create a keyword group that can then be added to a custom filter. Keyword conditions search for a specific word or term during collection.

To create a new keyword group

1. In the *Configure* tab, click **Keyword Groups** (see [Keywords Dialog](#) page 12).
2. In the *Keywords* dialog, click **Create New Group**.

FIGURE 5-6 Create/Edit Keyword Dialog



3. Enter a **Group Name** and **Description**.
4. (Optional) Enter an **Import File** path or browse to a file that contains the keywords you want to add to the group. Once found, click **Import** to add the keywords to the list.
5. Enter the keywords you want added to the condition in the keyword pane.

Note: Enter each keyword search term on its own line.
6. Click **Save Filter**.
7. Click **OK** to add the keyword to the existing filters list.
8. Click **Yes** to create another keyword group or **No** to close the dialog.
9. Add the group to a filter by following the steps in [Creating a Custom Filter](#) page 41.

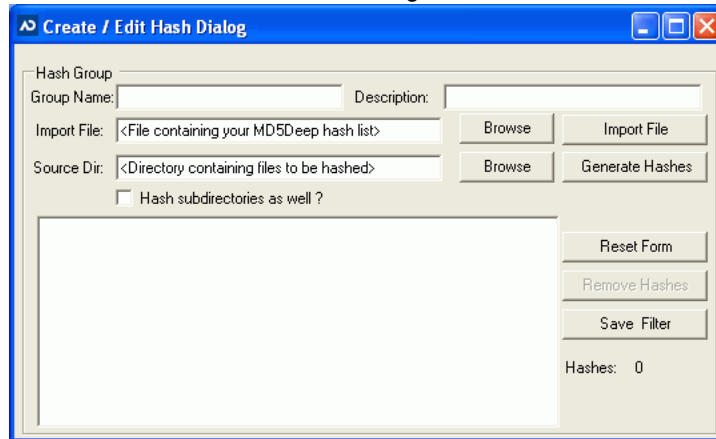
Creating a Hash Group

The Hash feature allows you to create a hash group that can then be added to a custom filter. Hash conditions search for specified hashes during collection.

To create a hash group

1. In the *Configure* tab, click **Hash Groups** (see [Hash Filter Dialog](#) page 13).
2. In the *Hash Filter* dialog, click **Create New Group**.

FIGURE 5-7 Create/Edit Hash Dialog



3. In the *Create/Edit Hash* dialog, enter a **Group Name** and **Description** for the group.
4. Click the **Import File Browse** button to browse to the known file on your system. Then, click **Import File** to add the file to the *Hash* pane.
5. Click the **Source Dir Browse** button to browse to the directory containing files to be hashed.
6. Check the **Hash Subdirectories as well** check box to include child files for the selected known file.
Note: Selecting a known file greatly increases the speed of the hashing when collecting data.
7. Click **Generate Hashes** to add the hashes to the *Hash* pane.
Note: Clicking the **Reset Form** button clears all the fields in the dialog.
8. Click **Save Filter**.
9. Click **Yes**.
10. Click **Yes** again if you want to create a new *Hash* group or **No** to return to the *Hash Filter* dialog.
11. Add the group to a filter by following the steps in [Creating a Custom Filter](#) page 41.

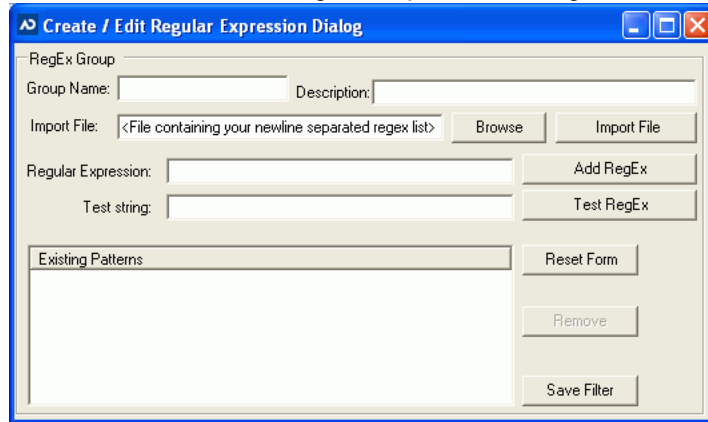
Creating a Regular Expression Group

The *Regular Expression* feature allows you to create a regular expression condition that can then be added to a custom filter. Regular expression conditions search for a specified expression during collection.

To create a regular expression group

1. In the *Configure* tab, click **RegEx Groups** (see [Regular Expression Dialog](#) page 12).
2. In the *Regular Expression* dialog, click **Create New Group**.

FIGURE 5-8 Create/Edit Regular Expression Dialog



3. In the *Create/Edit Regular Expression* dialog, enter a **Group Name** and **Description** for the group.
4. Click the Import File **Browse** button and select a known file. Then, click **Import File** to add the regular expression to the *Regular Expression* pane.
5. Enter an expression in the **Regular Expression** field.
6. Enter a **Test String** for the regular expression.
7. Click **Test Regular Expression** button to test if the expression matches the string.
8. Click **Add Regular Expression**.
Note: Clicking the **Reset Form** button clears all the fields in the dialog.
9. Click **Save Filter**.
10. Click **Yes**.
11. Click **Yes** again if you want to create a new *Hash* group or **No** to return to the Hash Filter dialog.
12. Add the group to a filter by following the steps in [Creating a Custom Filter](#) page 41.

Advanced Saved Collections Tasks

Once you have saved a collection, you can use the Manage Saved Collections feature to perform the following advanced tasks:

- Export Saved Collections [Exporting Saved Collections](#) page 46
- Delete Saved Collections [Deleting a Saved Collection](#) page 47
- Import Saved Collections [Importing a Saved Collection](#) page 47

Exporting Saved Collections

Once you have found the collection/s you are looking for in the *Manage Collections* dialog using the filters (see [Filtering Saved Collections](#) page 35), you can then export the collection to a designated location. This makes a copy of the collection and saves it in the location you select. You can then use the exported file and import it into another *AD Triage Admin* system for others to review.

To export a saved collection

1. On the *Admin* tab of the *Admin* console, click **Manage Saved Collections** (see [Manage Collections Dialog](#) page 8).
2. In the *Manage Collections* dialog, select the collection that you want to export (see [Filtering Saved Collections](#) page 35).
3. Click **Export Collection**.
4. Browse to the location where you want to save the exported file.
5. Click **OK**.

Deleting a Saved Collection

Once you have found the collection/s you are looking for in the *Manage Collections* dialog using the filters (see [Filtering Saved Collections](#) page 35), you can then delete the collected data from your saved collection file. This will not remove the collected data from the USB device that it originated from.

To delete a saved collection

1. On the *Admin* tab of the *Admin* console, click **Manage Saved Collections** (see [Manage Collections Dialog](#) page 8).
2. In the *Manage Collections* dialog, select the collection that you want to delete (see [Filtering Saved Collections](#) page 35).
3. Click **Delete Collection**.
4. Click **OK**.

Importing a Saved Collection

If you want to import a collection that is saved from another *Triage Admin* console, you can use the *Import Collection* feature.

To import a saved collection

1. On the *Admin* tab of the *Admin* console, click **Manage Saved Collections** (see [Manage Collections Dialog](#) page 8).
2. In the *Manage Collections* dialog, click **Import Collection**.
3. Browse to the file that you want to import and click **OK**.
4. In the *Import Collection* dialog, select the collection(s) that you want to import and click **Import Collections**.
5. In the message box that appears, click **Yes**.
The collection is added to your saved collections.

Recovering a Remote Collection

If you want to recover a collection that is saved on a remote share, you can use the *Recover Remote Collection* feature.

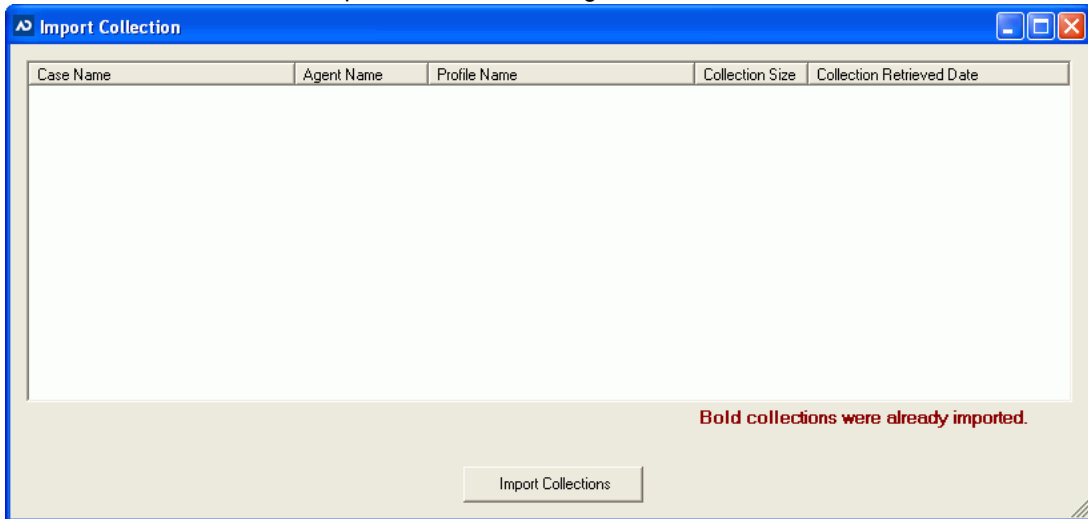
Note: You can only use this feature with collections you have mounted to a remote share. This feature will not work for data collected using the Triage Receiver.

To import a remote collection

1. On the *Admin* tab of the *Admin* console, click **Manage Saved Collections** (see [Manage Collections Dialog](#) page 8).
2. In the *Manage Collections* dialog, click **Recover Remote Collection**.
3. Browse to the location of the remote directory and click **OK**.

Note: To import data from a remote directory, the directory must have the following folder structure: triage > remote > casedata. Triage will not recognize directories that have an altered folder structure naming convention.

FIGURE 5-9 Import Collections Dialog



4. In the *Import Collections* dialog, select the collection(s) that you want to import and click **Import Collections**.
5. In the message box that appears, click **Yes**.
The collection is imported.

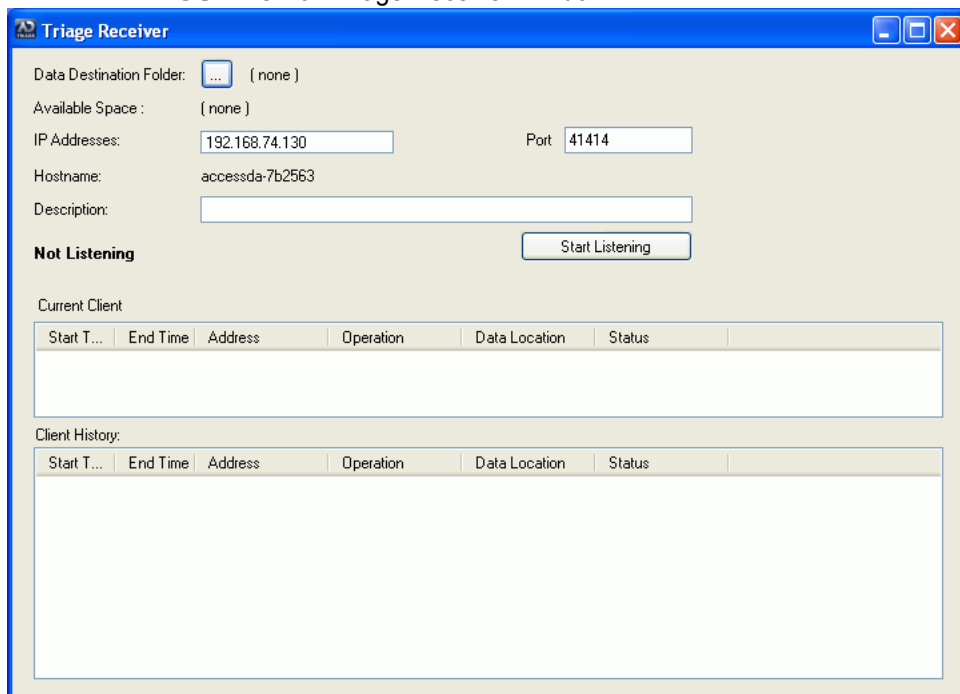
Using the Triage Receiver

The *Triage Receiver* can be used to export collected data directly from the target system to a designated location on the same network, using the *Triage Receiver*.

To export data to a designated location

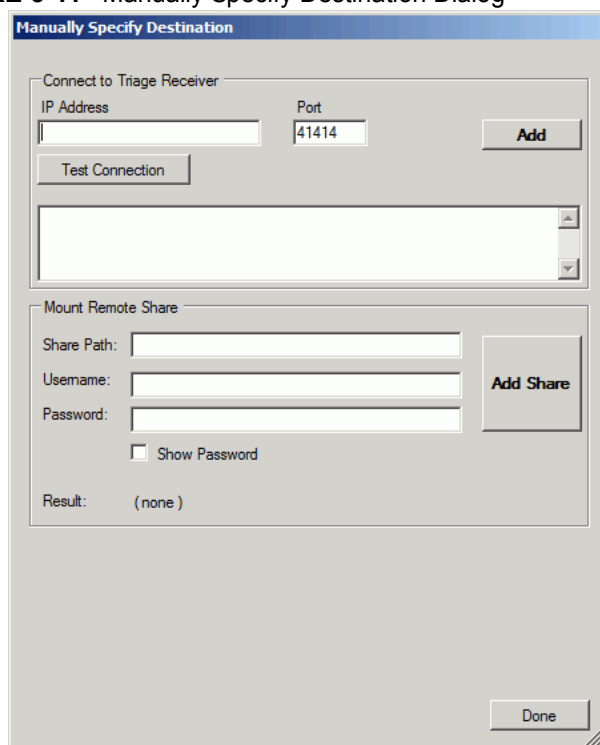
1. Select **Start > Programs > AccessData > ADTriage >TriageReceiver.exe**.

FIGURE 5-10 Triage Receiver Window



2. In the *Triage Receiver*, click the **Data Destination Folder** browse button.
3. Select the location where you want to save the collection.
4. Click the **Start Listening** button.
5. Collect data from the target system, but do not export it yet (see [Manually Collecting and Exporting Data on a Target System](#) page 30).
6. In the *Collection* interface, click the **Evidence** tab.
7. Click the **Manually Specify Remote Destination...** link.

FIGURE 5-11 Manually Specify Destination Dialog



8. Enter the **IP Address** of the computer where you want to export the collection.
 9. Enter the **Port** number where you want to export the collection.
 10. Click **Test Connection**.
The pane below the *Test Connection* button displays whether or not the connection is a success. You can also see the connection status in the *Triage Receiver* window.
 11. If the test connection worked, click **Add**.
 12. Click **Done**.
 13. Select the computer in the *Select Destination* pane.
 14. Click **Export Now!**
The data is exported to the location that you designated.
- Note:** To import the collection into the Triage Admin console, see [Importing a Saved Collection](#) page 47.

Mounting to a Remote Share

When you are manually specifying a destination to export your collection, you can mount exported data to a remote share before bringing the data into the Admin console.

To mount collected data to a remote share

1. Run the *Triage Collection* interface on the target system with your Triage USB device (see [Manually Collecting and Exporting Data on a Target System](#) page 30).
2. Collect data from the target system, but do not export it yet (see [Manually Collecting and Exporting Data on a Target System](#) page 30).
3. In the *Collection* interface, click the **Evidence** tab.
4. Click the **Manually Specify Remote Destination** link.
5. Enter the Share Path of the remote share folder where you want to export the collection.
6. Click **Add Share**.

Appendix A Managing Security Devices and Licenses

This chapter expands on the licensing information needed to run AccessData products, including AccessData product licenses, Virtual CodeMeter activation, and Network License Server configurations.

AccessData Product Licenses

This section acquaints you with managing AccessData product licenses. Here you will find details regarding the LicenseManager interface and how to manage licenses and update products using LicenseManager.

Installing and Managing Security Devices

Before you can manage licenses with LicenseManager, you must install the proper security device software and/or drivers. This section explains installing and using the Wibu CodeMeter Runtime software and USB CmStick, as well as the Keylok USB dongle drivers and dongle device.

Installing the Security Device

As discussed previously, AccessData products require a licensing security device that communicates with the program to verify the existence of a current license. The device can be the older Keylok dongle, or the newer WIBU-SYSTEMS (Wibu) CodeMeter (CmStick). Both are USB devices, and both require specific software to be installed prior to connecting the devices and running your AccessData products. You will need:

- The WIBU-SYSTEMS CodeMeter Runtime software with a WIBU-SYSTEMS CodeMeter (CmStick), either the physical USB device, or the Virtual device.
- The WIBU-SYSTEMS CodeMeter Runtime software, and the AccessData Dongle Drivers with a Keylok dongle

Note: Without a license security device and its related software, you can run PRTK or DNA in Demo mode only.

The CmStick or dongle should be stored in a secure location when not in use.

You can install your AccessData product and the CodeMeter software from the shipping CD or from downloadable files available on the AccessData website at www.accessdata.com.

Click **Support > Downloads**, and browse to the product to download. Click the download link and save the file locally prior to running the installation files.

Installing the CodeMeter Runtime Software

When you purchase the full PRTK package, AccessData provides a USB CmStick with the product package. The green Keylok dongles are no longer provided, but can be purchased separately through your AccessData Sales Representative.

To use the CmStick, you must first install the CodeMeter Runtime software, either from the shipping CD, or from the setup file downloaded from the AccessData Web site.

Locating the Setup File

To install the CodeMeter Runtime software from the CD, you can browse to the setup file, or select it from the Autorun menu.

To download the CodeMeter Runtime software

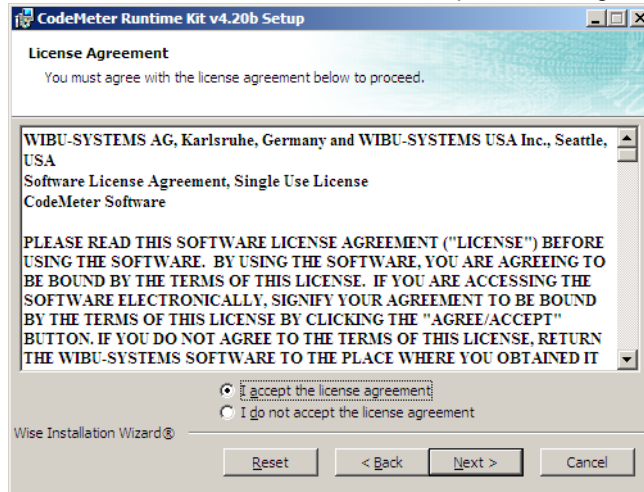
1. Go to www.accessdata.com and do the following:
2. Click **Support > Downloads**.
3. Find one of the following, according to your system:
 - CodeMeter Runtime 4.20b (32 bit)
MD5: 2e658fd67dff9da589430920624099b3
(MD5 hash applies only to this version)
 - CodeMeter Runtime 4.20b (64 bit)
MD5: b54031002a1ac18ada3cb91de7c2ee84
(MD5 hash applies only to this version)
4. Click the **Download** link.
5. Save the file to your PC and run after the download is complete.

When the download is complete, double-click on the **downloaded file**.

To run the CodeMeter Runtime Setup

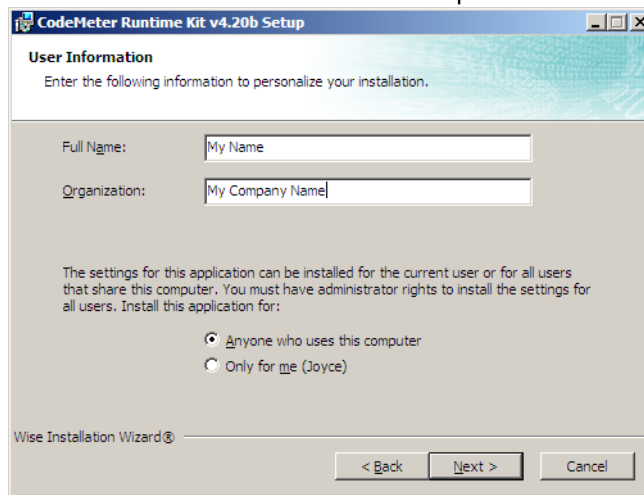
1. Double-click the CodeMeterRuntime[32 or 64]_4.20b.exe.
2. In the Welcome dialog, click **Next**.
3. Read and accept the License Agreement

FIGURE A-1 CodeMeter Runtime Setup: License Agreement.



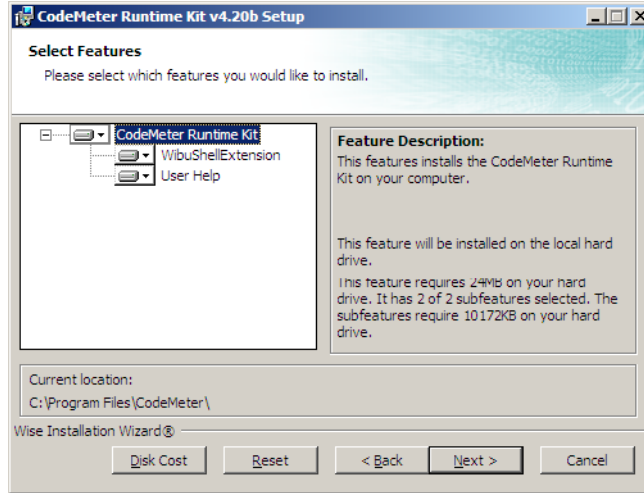
4. Click **Next**.
5. Enter User Information.

FIGURE A-2 CodeMeter Runtime Setup: User Information



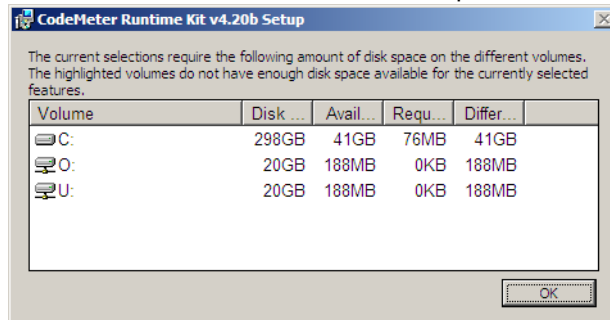
6. Specify whether this application should be available only when you log in, or for anyone who uses this computer.
7. Click **Next**.

FIGURE A-3 CodeMeter Runtime Setup: Select Features



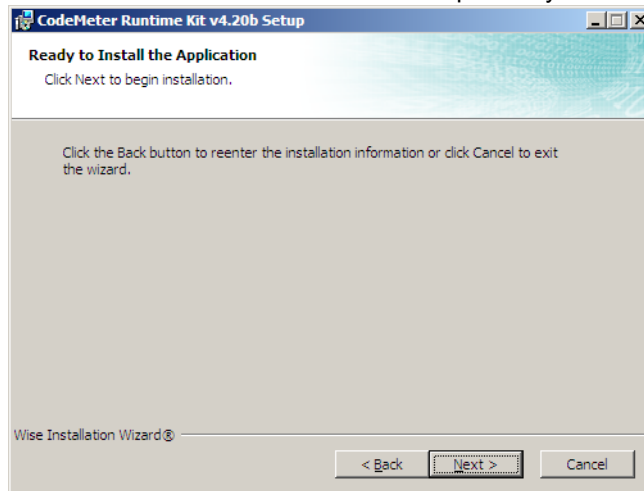
8. Select the features you want to install.
9. Click **Disk Cost** to see how much space the installation of CodeMeter software takes, and drive space available. This helps you determine the destination drive.

FIGURE A-4 CodeMeter Runtime Setup: Disk Cost



10. Click **OK**.
11. Click **Next**.

FIGURE A-5 CodeMeter Runtime Setup: Ready to Install



12. When you are satisfied with the options you have selected, click **Next**.

FIGURE A-6 CodeMeter Runtime Setup: Successfully Installed



13. Installation will run its course. When complete, you will see the “CodeMeter Runtime Kit v4.20b has been successfully installed” screen. Click **Finish** to exit the installation.

The CodeMeter Control Center

When the CodeMeter Runtime installation is complete, the CodeMeter Control Center pops up. This is a great time to connect the CmStick and verify that the device is recognized and is Enabled. Once verified, you can close the control center and run your AccessData product(s).

When the software is installed, but the CmStick is not connected, you will see a system tray icon that looks like this:



When the software is installed, and the CmStick is connected and recognized, you will see a system tray icon that looks like this:



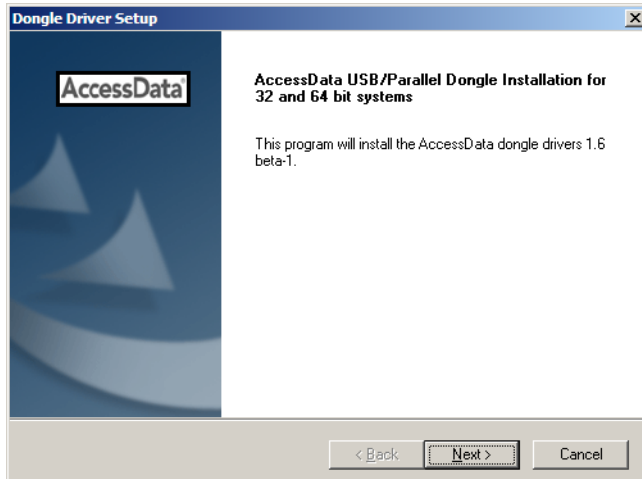
For the most part there is nothing you need to do with this control center, and you need make no changes using this tool with very few exceptions. If you have problems with your CmStick, contact AccessData Support and an agent will walk you through any troubleshooting steps that may need to be performed.

Installing Keylok Dongle Drivers

To install the Keylok USB dongle drivers

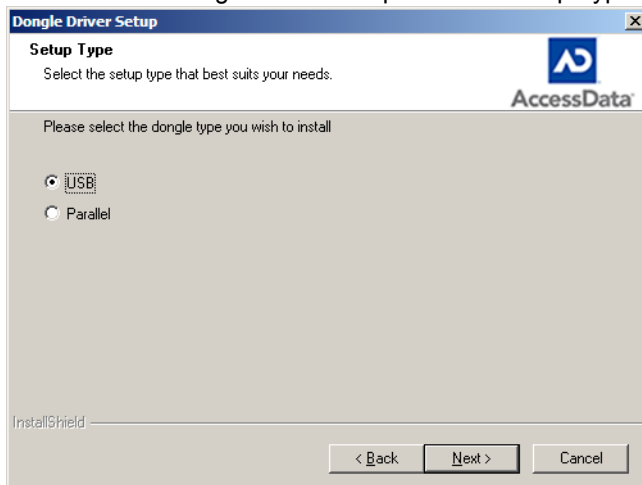
1. Choose one of the following methods:
 - If installing from CD, insert the CD into the CD-ROM drive and click **Install the Dongle Drivers**.
If auto-run is not enabled, select **Start > Run**. Browse to the CD-ROM drive and select **Autorun.exe**.
 - If installing from a file downloaded from the AccessData Web site, locate the **Dongle_driver_1.6.exe** setup file, and double-click it.

FIGURE A-7 Dongle Driver Setup



2. Click **Next**.

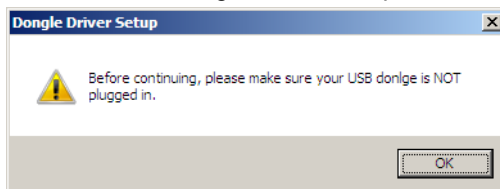
FIGURE A-8 Dongle Driver Setup: Choose Setup Type for Dongle



3. Select the type of dongle to install the drivers for.

4. Click **Next**.

FIGURE A-9 Dongle Driver Setup: Ensure USB Device is not Plugged In

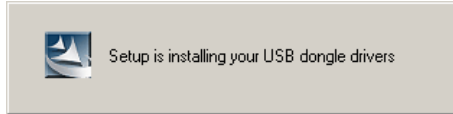


5. If you have a USB dongle, verify that it is not connected.

6. Click **OK**.

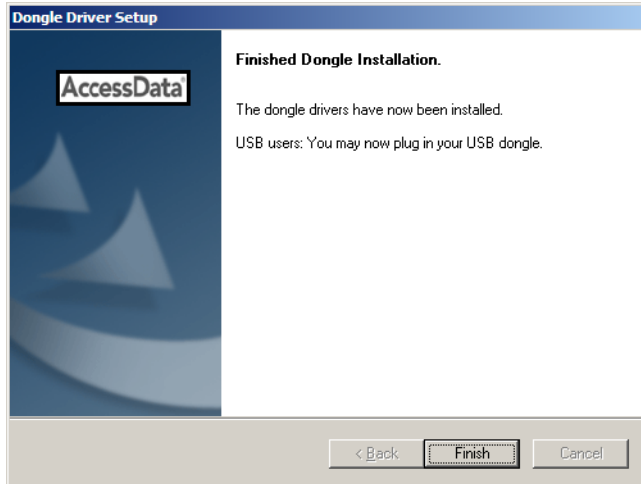
A message box appears telling you that the installation is progressing.

FIGURE A-10 Setup Progress Message Box.



7. When you see the Dongle Driver Setup window that says, "Finished Dongle Installation," click **Finish**.

FIGURE A-11 Dongle Driver Setup: Finished



8. Connect the USB dongle. Wait for the Windows Found New Hardware wizard, and follow the prompts.

Important: If the Windows Found New Hardware wizard appears, complete the wizard. Do not close without completing, or the dongle driver will not be installed.

Windows Found New Hardware Wizard

When you connect the dongle after installing the dongle drivers, you should wait for the Windows Found New Hardware Wizard to open. It is not uncommon for users to disregard this wizard, and then find that the dongle is not recognized and their AccessData software will not run.

To configure the dongle using the Found New Hardware Wizard

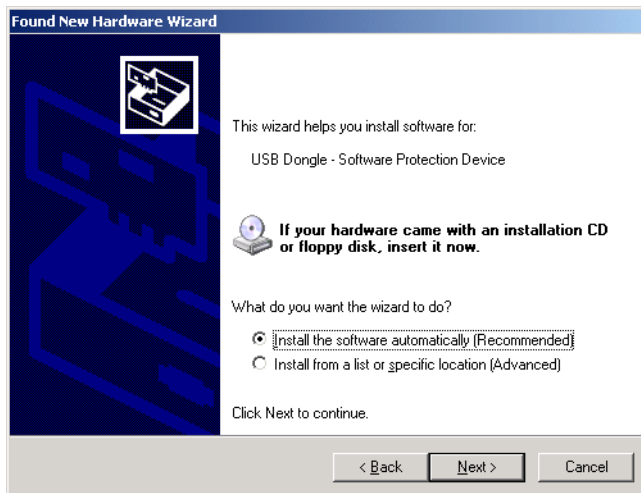
1. When prompted whether to connect to Windows Update to search for software, choose, “No, not this time.”

FIGURE A-12 Found New Hardware Wizard: Welcome



2. Click **Next**.
3. When prompted whether to install the software automatically or to install from a list of specific locations, choose, “Install the software automatically (Recommended).”

FIGURE A-13 Found New Hardware Wizard: Install Automatically



4. Click **Next**.
5. Click **Finish** to close the wizard.

FIGURE A-14 Found New Hardware Wizard: Complete



Once you have installed the dongle drivers and connected the dongle and verified that Windows recognizes it, you can use LicenseManager to manage product licenses.

Installing LicenseManager

LicenseManager lets you manage product and license subscriptions using a security device or device packet file.

To download the LicenseManager installer from the AccessData web site

1. Go to the AccessData download page at:
<http://www.accessdata.com/downloads.htm>.
2. On the download page, click the **LicenseManager Download** link.
3. Save the installation file to your download directory or other temporary directory on your drive.
 - 3a. The current version information is as follows:
 - License Manager version 3.1.1 (**LicenseManager_3.1.1.exe**)
 - Release Date: March 25, 2010
 - MD5: 2e645ca8b0ca57aafbc156213be2147f (for this version only)

To install LicenseManager

1. Navigate to, and double-click the installation file.
2. Wait for the *Preparing to Install* processes to complete.
3. Click **Next** on the Welcome screen

FIGURE A-15 LicenseManager Setup: Welcome.



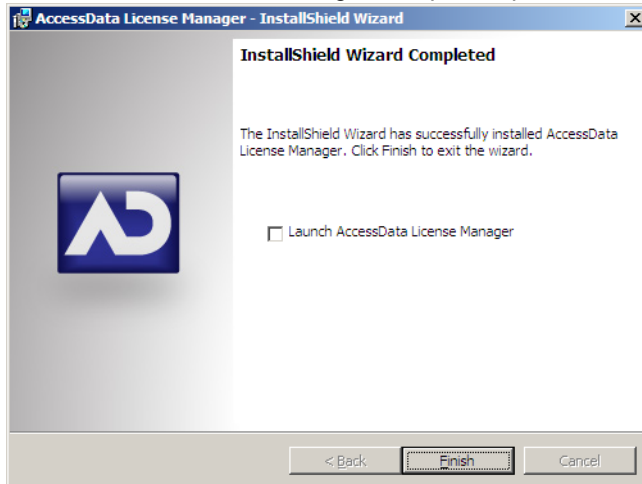
4. Read and accept the License Agreement
5. Click **Next**.

FIGURE A-16 LicenseManager Setup: License Agreement.



6. Accept the default destination folder, or select a different one.
7. Click **Next**.
8. In the Ready to Install the Program dialog, click **Back** to review or change any of the installation settings. When you are ready to continue, click **Install**.
9. Wait while the installation completes.
10. If you want to launch LicenseManager after completing the installation, mark the **Launch AccessData LicenseManager** check box.


FIGURE A-17 LicenseManager Setup: Completed



11. Select the **Launch AccessData LicenseManager** check box to run the program upon finishing the setup.
12. Click **Finish** to finalize the installation and close the wizard.

Starting LicenseManager

To launch LicenseManager



1. Launch LicenseManager in any of the following ways:
 - Execute **LicenseManager.exe** from **C:\Program Files\AccessData\Common Files\AccessData LicenseManager**.
 - Click **Start > All Programs > AccessData > LicenseManager > LicenseManager**.
 - Click or double-click (depending on your Windows settings) the **LicenseManager** icon on your desktop .
 - From some AccessData programs, you can run LicenseManager from the **Tools > Other Applications** menu. This option is not available in PRTK or DNA.

When starting, LicenseManager reads licensing and subscription information from the installed and connected WIBU-SYSTEMS CodeMeter Stick, or Keylok dongle.

If using a Keylok dongle, and LicenseManager either does not open or displays the message, “Device Not Found”

1. Make sure the correct dongle driver is installed on your computer.
2. With the dongle connected, check in Windows Device Manager to make sure the device is recognized. If it has an error indicator, right click on the device and choose Uninstall.
3. Remove the dongle after the device has been uninstalled.
4. Reboot your computer.
5. After the reboot is complete, and all startup processes have finished running, connect the dongle.
6. Wait for Windows to run the Add New Hardware wizard. If you already have the right dongle drivers installed, do not browse the internet, choose, “No, not this time.”
7. Click **Next** to continue.
8. On the next options screen, choose, “Install the software automatically (Recommended)”
9. Click **Next** to continue.
10. When the installation of the dongle device is complete, click Finish to close the wizard.
11. You still need the CodeMeter software installed, but will not need a CodeMeter Stick to run LicenseManager.

If using a CodeMeter Stick, and LicenseManager either does not open or displays the message, “Device Not Found”

1. Make sure the CodeMeter Runtime 4.20b software is installed. It is available at www.accessdata.com/support. Click Downloads and browse to the product. Click on the download link. You can **Run** the product from the Website, or **Save** the file locally and run it from your PC. Once the CodeMeter Runtime software is installed and running, you will see a gray icon in your system tray: .
2. Make sure the CodeMeter Stick is connected to the USB port. When the CmStick is then connected, you will see the icon change to look like this: .

If the CodeMeter Stick is not connected, LicenseManager still lets you to manage licenses using a security device packet file if you have exported and saved the file previously.

To open LicenseManager without a CodeMeter Stick installed

1. Click **Tools > LicenseManager**.
LicenseManager displays the message, “Device not Found”.
2. Click **OK**, then browse for a security device packet file to open.

Note: Although you can run LicenseManager using a packet file, AccessData products will not run with a packet file alone. You must have the CmStick or dongle connected to the computer to run AccessData products that require a license.

Using LicenseManager

LicenseManager provides the tools necessary for managing AccessData product licenses on a WIBU-SYSTEMS CodeMeter Stick security device, a Keylok dongle, a Virtual Dongle, or in a security device packet file.

LicenseManager displays license information, allows you to add licenses to or remove existing licenses from a dongle or CmStick. LicenseManager, and can also be used to export a security device packet file. Packet files can be saved and reloaded into LicenseManager, or sent via email to AccessData support.

In addition, you can use LicenseManager to check for product updates and in some cases download the latest product versions.

LicenseManager displays CodeMeter Stick information (including packet version and serial number) and licensing information for all AccessData products. The Purchase Licenses button connects directly to the AccessData website and allows you to browse the site for

information about products you may wish to purchase. Contact AccessData by phone to speak with a Sales Representative for answers to product questions, and to purchase products and renew licenses and subscriptions.

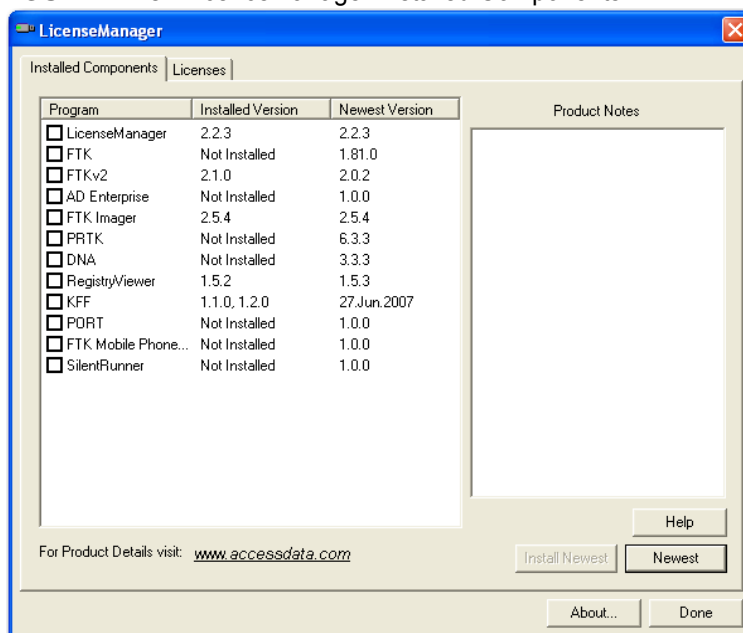
The LicenseManager Interface

The LicenseManager interface consists of two tabs that organize the options in the LicenseManager window: the Installed Components tab and the Licenses tab.

The Installed Components Tab

The Installed Components tab lists the AccessData programs installed on the machine. The Installed Components tab is displayed in the following figure.

FIGURE A-18 LicenceManager Installed Components



The following information is displayed on the Installed Components tab:

TABLE A-1 LicenseManager Installed Components Tab Features

Item	Description
Program	Lists all AccessData products installed on the host.
Installed Version	Displays the version of each AccessData product installed on the host.
Newest Version	Displays the latest version available of each AccessData product installed on the host. Click Newest to refresh this list.
Product Notes	Displays notes and information about the product selected in the program list.
AccessData Link	Links to the AccessData product page where you can learn more about AccessData products.

The following buttons provide additional functionality from the Installed Components tab:

TABLE A-2 LicenseManager Installed Components Buttons

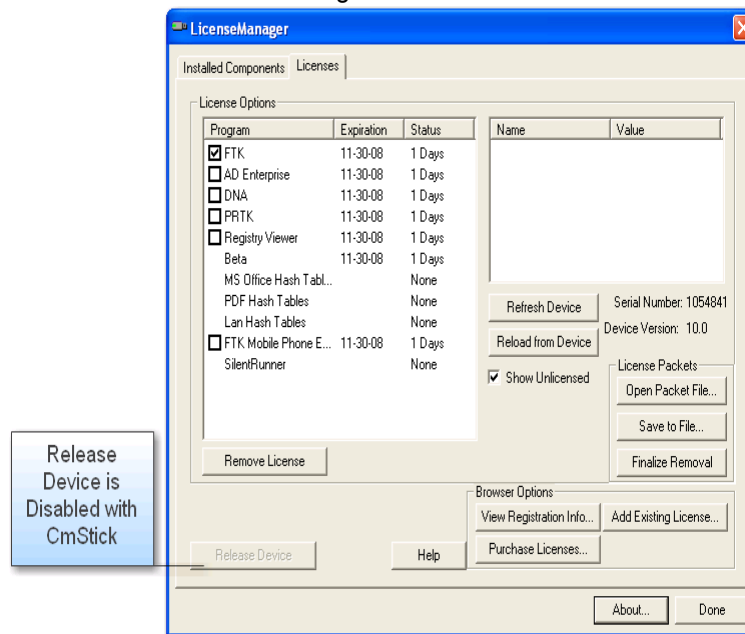
Button	Function
Help	Opens the LicenseManager Help web page.
Install Newest	Installs the newest version of the programs checked in the product window, if that program is available for download. You can also get the latest versions from our website using your Internet browser.
Newest	Updates the latest version information for your installed products.
About	Displays the About LicenseManager screen. Provides version, copyright, and trademark information for LicenseManager.
Done	Closes LicenseManager.

Use the Installed Components tab to manage your AccessData products and stay up to date on new releases.

The Licenses Tab

The Licenses tab displays CodeMeter Stick information for the current security device packet file and licensing information for AccessData products available to the owner of the CodeMeter Stick, as displayed in the following figure.

FIGURE A-19 LicenseManager Licenses Tab



The Licenses tab provides the following information:

TABLE A-3 LicenseManager Licenses Tab Features

Column	Description
Program	Shows the owned licenses for AccessData products.
Expiration Date	Shows the date on which your current license expires.

TABLE A-3 LicenseManager Licenses Tab Features (Continued)

Column	Description
Status	Shows these status of that product's license: <ul style="list-style-type: none"> • None: the product license is not currently owned • Days Left: displays when less than 31 days remain on the license. • Never: the license is permanently owned. This generally applies to Hash Tables and Portable Office Rainbow Tables.
Name	Shows the name of additional parameters or information a product requires for its license.
Value	Shows the values of additional parameters or information a product contained in or required for its license.
Show Unlicensed	When checked, the License window displays all products, whether licensed or not.

The following license management actions can be performed using buttons found on the License tab:

TABLE A-4 License Management Options

Button	Function
Remove License	Removes a selected license from the Licenses window and from the CodeMeter Stick or dongle. Opens the AccessData License Server web page to confirm success.
Refresh Device	Connects to the AccessData License Server. Downloads and overwrites the info on the CodeMeter Stick or dongle with the latest information on the server.
Reload from Device	Begins or restarts the service to read the licenses stored on the CodeMeter Stick or dongle.
Release Device	Click to stop the program reading the dongle attached to your machine, much like Windows' Safely Remove Hardware feature. Click this button before removing a dongle. This option is disabled for the CodeMeter Stick.
Open Packet File	Opens Windows Explorer, allowing you to navigate to a .PKT file containing your license information.
Save to File	Opens Windows Explorer, allowing you to save a .PKT file containing your license information. The default location is My Documents.
Finalize Removal	Finishes the removal of licenses in the unbound state. Licenses must be unbound from the CmStick or dongle before this button takes effect.
View Registration Info	Displays an HTML page with your CodeMeter Stick number and other license information.
Add Existing License	Allows you to bind an existing unbound license to your CodeMeter Stick, through an internet connection to the AccessData License Server.
Purchase License	Brings up the AccessData product page from which you can learn more about AccessData products.
About	Displays the About LicenseManager screen. Provides version, copyright, and trademark information for LicenseManager.
Done	Closes LicenseManager.

Opening and Saving Dongle Packet Files

You can open or save dongle packet files using LicenseManager. When started, LicenseManager attempts to read licensing and subscription information from the dongle. If you do not have a dongle installed, LicenseManager lets you browse to open a dongle packet file. You must have already created and saved a dongle packet file to be able to browse to and open it.

To save a security device packet file

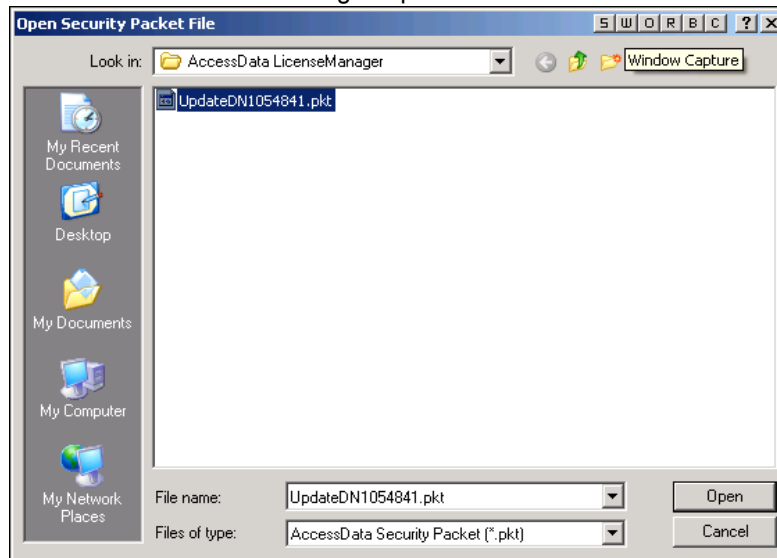
1. Click the **Licenses** tab, then under License Packets, click **Save to File**.
2. Browse to the desired folder and accept the default name of the .PKT file; then click **Save**.

Note: In general, the best place to save the .PKT files is in the AccessData LicenseManager folder. The default path is C:\Program Files\AccessData\Common Files\AccessData LicenseManager\.

To open a security device packet file

1. Select the **Licenses** tab.
2. Under License Packets, click **Open Packet File**.
3. Browse for a dongle packet file to open. Select the file and click **Open**.

FIGURE A-20 LicenseManager Open Packet File



Adding and Removing Product Licenses

On a computer with an Internet connection, LicenseManager lets you add available product licenses to, or remove them from, a dongle.

To move a product license from one dongle to another dongle, first remove the product license from the first dongle. You must release that dongle, and connect the second dongle before continuing. When the second dongle is connected and recognized by Windows and LicenseManager, click on the Licenses tab to add the product license to the second dongle.

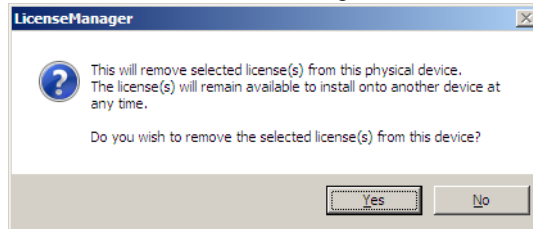
Removing a License

To remove (unassociate, or unbind) a product license

1. From the Licenses tab, mark the program license to remove.
This action activates the Remove License button below the Program list box.

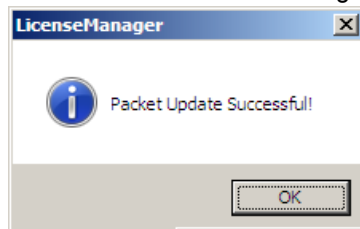
2. Click **Remove License** to connect your machine to the AccessData License Server through the internet.
3. When you are prompted to confirm the removal of the selected license(s) from the device, click **Yes** to continue, or **No** to cancel.

FIGURE A-21 LicenseManager Confirm License Release



4. Several screens appear indicating the connection and activity on the License Server, and when the license removal is complete, the following screen appears.

FIGURE A-22 LicenseManager Packet Update Successful



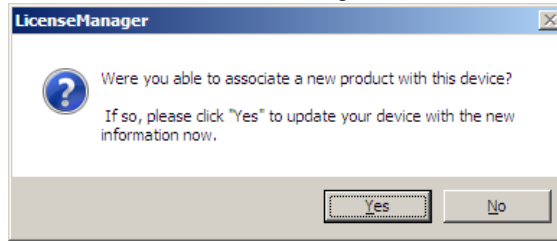
5. Click **OK** to close the message box.
 Another internet browser screen appears from LicenseManager with a message that says, "The removal of your license(s) from Security Device was successful!" You may close this box at any time.

Adding a License

To add a new or released license

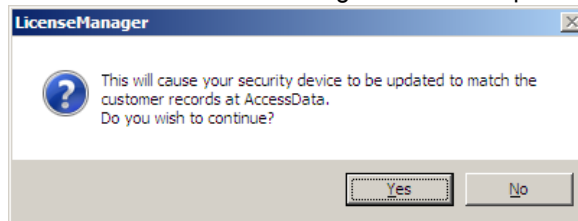
1. From the Licenses tab, under Browser Options, click **Add Existing License**.
 The AccessData LicenseManager Web page opens, listing the licenses currently bound to the connected security device, and below that list, you will see the licenses that currently are not bound to any security device. Mark the box in the Bind column for the product you wish to add to the connected device, then click **Submit**.
2. An AccessData LicenseManager Web page will open, displaying the following message, "The AccessData product(s) that you selected has been bound to the record for Security Device nnnnnn within the Security Device Database.
 "Please run LicenseManager's "Refresh Device" feature in order to complete the process of binding these product license(s) to this Security Device." You may close this window at any time.

FIGURE A-23 LicenseManager: Associate Successful?



3. Click **Yes** if LicenseManager prompts, "Were you able to associate a new product with this device?"
4. Click **Refresh Device** in the Licenses tab of LicenseManager. Click **Yes** when prompted.

FIGURE A-24 LicenseManager: Continue Updating Security Device?



You will see the newly added license in the License Options list.

Adding and Removing Product Licenses Remotely

While LicenseManager requires an Internet connection to use some features, you can add or remove licenses from a dongle packet file for a dongle that resides on a computer, such as a forensic lab computer, that does not have an Internet connection.

If you cannot connect to the Internet, the easiest way to move licenses from one dongle to another is to physically move the dongle to a computer with an Internet connection, add or remove product licenses as necessary using LicenseManager, and then physically move the dongle back to the original computer. However, if you cannot move the dongle—due to organization policies or a need for forensic soundness—then transfer the packet files and update files remotely.

Adding a License Remotely

To remotely add (associate or bind) a product license

1. On the computer where the security device resides:
 - 1a. Run LicenseManager.
 - 1b. From the **Licenses** tab, click **Reload from Device** to read the dongle license information.
 - 1c. Click **Save to File** to save the dongle packet file to the local machine.
2. Copy the dongle packet file to a computer with an Internet connection.
3. On the computer with an Internet connection:
 - 3a. Remove any attached security device.
 - 3b. Launch LicenseManager. You will see a notification, “No security device found”.
 - 3c. Click *OK*.
 - 3d. An “Open” dialog box will display. Highlight the .PKT file, and click **Open**.
 - 3e. Click on the **Licenses** tab.
 - 3f. Click **Add Existing License**.
 - 3g. Complete the process to add a product license on the Website page.
 - 3h. Click **Yes** when the LicenseManager prompts, “Were you able to associate a new product with this dongle?”
 - 3i. When LicenseManager does not detect a dongle or the serial number of the dongle does not match the serial number in the dongle packet file, you are prompted to save the update file, [serial#].wibuCmRaU.
 - 3j. Save the update file to the local machine.
4. After the update file is downloaded, copy the update file to the computer where the dongle resides:
5. On the computer where the dongle resides:
 - 5a. Run the update file by double-clicking it. ([serial#].wibuCmRaU is an executable file.)
 - 5b. After an update file downloads and installs, click *OK*.
 - 5c. Run LicenseManager.
 - 5d. From the Licenses tab, click **Reload from Device** to verify the product license has been added to the dongle.

Removing a License Remotely

To remotely remove (unassociate, or unbind) a product license

1. On the computer where the dongle resides:
 - 1a. Run LicenseManager.
 - 1b. From the Licenses tab, click **Reload from Device** to read the dongle license information.
 - 1c. Click **Save to File** to save the dongle packet file to the local machine.
2. Copy the file to a computer with an Internet connection.
3. On the computer with an Internet connection:
 - 3a. Launch LicenseManager. You will see a notification, “No security device found”.
 - 3b. Click *OK*.
 - 3c. An “Open” dialog box will display. Highlight the .PKT file, and click **Open**.
 - 3d. Click on the Licenses tab.
 - 3e. Mark the box for the product license you want to unassociate; then click **Remove License**.
 - 3f. When prompted to confirm the removal of the selected license from the dongle, click **Yes**.

- 3g. When LicenseManager does not detect a dongle or the serial number of the dongle does not match the serial number in the dongle packet file, you are prompted save the update file.
- 3h. Click **Yes** to save the update file to the local computer.
- 3i. The Step 1 of 2 dialog details how to use the dongle packet file to remove the license from a dongle on another computer.
- 3j. Save the update file to the local machine.
4. After the update file is downloaded, copy the update file to the computer where the dongle resides.
5. On the computer where the dongle resides:
 - 5a. Run the update file by double-clicking it. This runs the executable update file and copies the new information to the security device.
 - 5b. Run LicenseManager
 - 5c. On the Licenses tab, click **Reload from Device** in LicenseManager to read the security device and allow you to verify the product license is removed from the dongle.
 - 5d. Click **Save to File** to save the updated dongle packet file to the local machine.
6. Copy the file to a computer with an Internet connection.

Updating Products

You can use LicenseManager to check for product updates and download the latest product versions.

Checking for Product Updates

To check for product updates, on the Installed Components tab, click **Newest**. This refreshes the list to display what version you have installed, and the newest version available.

Downloading Product Updates

To install the newest version, mark the box next to the product to install, then click **Install Newest**.

Note: Some products, such as FTK 2.x, Enterprise, and others, are too large to download, and are not available. A notification displays if this is the case.

To download a product update

1. Ensure that LicenseManager displays the latest product information by clicking the Installed Components tab. Click **Newest** to refresh the list showing the latest releases, then compare your installed version to the latest release.
If the latest release is newer than your installed version, you may be able to install the latest release from the AccessData website.

2. Ensure that the program you want to install is not running.
3. Mark the box next to the program you want to download; then click **Install Newest**.
4. When prompted, click **Yes** to download the latest install version of the product.
 - 4a. If installing the update on a remote computer, copy the product update file to another computer.
5. Install the product update. You may need to restart your computer after the update is installed.

Purchasing Product Licenses

Use LicenseManager to link to the AccessData website to find information about all our products.

Purchase product licenses through your AccessData Sales Representative. Call 801-377-5410 and follow the prompt for Sales, or send an email to sales@accessdata.com.

Note: Once a product has been purchased and appears in the AccessData License Server, add the product license to a CodeMeter Stick, dongle, or security device packet file by clicking **Refresh Device**.

Sending a Dongle Packet File to Support

Send a security device packet file **only** when specifically directed to do so by AccessData support.

To create a dongle packet file

1. Run LicenseManager
2. Click on the Licenses tab.
3. Click **Load from Device**.
4. Click **Refresh Device** if you need to get the latest info from AD's license server.
5. Click **Save to File**, and note or specify the location for the saved file.
6. Attach the dongle packet file to an e-mail and send it to:
support@accessdata.com.

Virtual CodeMeter Activation Guide

Introduction

A Virtual CodeMeter (VCM) allows the user to run licensed AccessData products without a physical CodeMeter device. A VCM can be created using AccessData License Manager, but requires the user to enter a Confirmation Code during the creation process.

The latest revision of this guide can be found at:

http://accessdata.com/downloads/media/VCM_Activation_Guide.pdf

Preparation

- Contact your AccessData sales rep to order a VCM confirmation code.
- Install CodeMeter Runtime 4.10b or newer (available on the AccessData download page).
- Install the latest release of License Manager (available on the AccessData download page).

- The following steps are to be run on the system where you want to permanently attach the VCM.
Note: Once created, the VCM cannot be moved to any other system.
- AD LAB WebUI and eDiscovery administrators, please also follow steps outlined under in [Additional Instructions for AD LAB WebUI and eDiscovery](#) (page 77) in order to enable VCM licensing on the AccessData License Service.

Setup for Online Systems

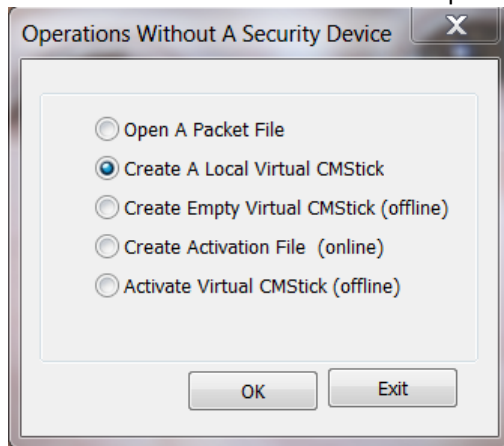
To set up a Virtual CodeMeter

1. Unplug any AccessData dongles you currently have connected.
2. Launch License Manager.

Note: When creating a VCM on Windows Server 2003 or 2008, please refer to the special set of steps written for those platforms. See [Creating a Virtual CM-Stick with Server 2003/2008 Enterprise Editions](#) (page 75).

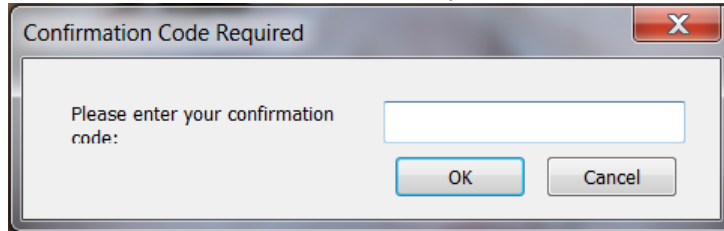
3. Select **Create A Local Virtual CMStick**.

FIGURE A-25 Virtual CodeMeter Setup: Create a Local Virtual CmStick



4. Click **OK**.
The Confirmation Code Required dialog appears.

FIGURE A-26 Virtual CodeMeter Setup: Confirmation Code Required



5. Enter your confirmation code.
6. Click **OK**, AccessData License Manager will automatically synchronize with the License Server over the Internet.
7. Click **OK** when the update completes. License Manager will then create the VCM on your system.
8. At this point, AccessData License Manager now displays a serial number for the VCM on the Licenses tab and the VCM can now operate in a similar way to a hardware CodeMeter device.

Setting up VCM for Offline Systems

You can setup a Virtual CodeMeter on a system that is not connected to the internet (offline). You must also have one machine that connects to the internet to perform certain steps. This section details what to do on which machine.

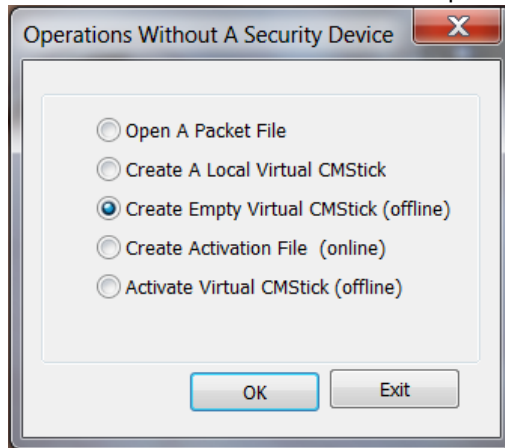
Perform these steps on the Online system

1. Unplug any AccessData dongles you currently have connected.
2. Launch License Manager.

Note: When creating a VCM on Windows Server 2003 or 2008 Enterprise Edition, please refer to the special set of steps written for those platforms. See [Creating a Virtual CM-Stick with Server 2003/2008 Enterprise Editions](#) (page 75).

3. Select **Create Empty Virtual CMStick (offline)**.

FIGURE A-27 Virtual CodeMeter Setup: Create Empty Virtual CMStick (offline)

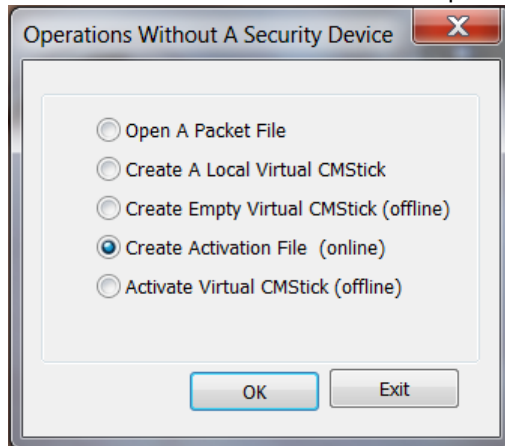


4. Click **OK**.
5. The resulting dialog prompts you to save the *.wibucmrau file. Enter a name and path for the file, then click **Save**.
6. Transfer the *.wibucmrau to the Online system.

Perform these steps on the Online system

7. Unplug any AccessData dongles you currently have connected.
8. Launch License Manager.
9. Select **Create Activation File (online)**.

FIGURE A-28 Virtual CodeMeter Setup: Create Activation File (online)



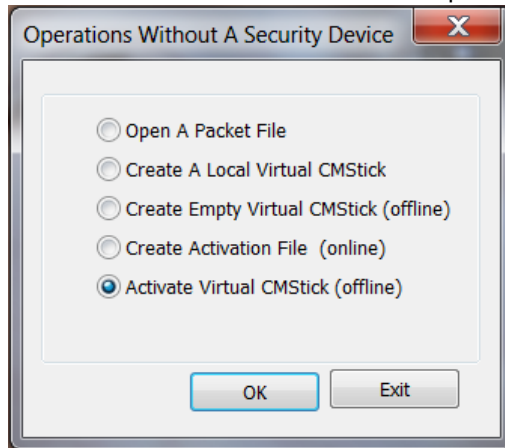
10. Click **OK**.
The Confirmation Code Required dialog appears.

11. Enter your confirmation code and click **OK**.
12. AccessData License Manager will automatically synchronize with the License Server over the internet. Data synchronized from the server will be written to the *.wibucmrau file. Click **OK** when the update completes.
13. Transfer *.wibucmrau back to the offline system.

Perform these steps on the Offline system

14. Unplug any AccessData dongles you currently have connected.
15. Launch License Manager.
16. Select **Create Activate Virtual CMStick (offline)**.

FIGURE A-29 Virtual CodeMeter Setup: Activate Virtual CMStick (offline)



17. Click **OK**.
18. The resulting dialog prompts you to browse to the location of the newly updated *.wibucmrau file. Locate the file, then click **Open**. License Manager creates the VCM on your system.
19. At this point, AccessData License Manager should now display a serial number for the VCM on the "Licenses" tab and the VCM can now operate in a similar way to a hardware CodeMeter device.

Creating a Virtual CM-Stick with Server 2003/2008 Enterprise Editions

This section contains special instructions for using a VCM with Windows Server 2003 or 2008 Enterprise Editions. Complete each section in order.

To Create an Empty CodeMeter License Container

1. On the Server 2003/2008 machine, unplug any CodeMeter devices.
2. Open the CodeMeter Control Center. Make sure the window on the License tab is, empty indicating that no licenses are currently loaded.
3. Select **File > Import License**.
4. Browse to the License Manager program files directory.
 - 32 bit systems: C:\Program Files\AccessData\LicenseManager\
 - 64 bit systems: C:\Program Files (x86)\AccessData\LicenseManager\

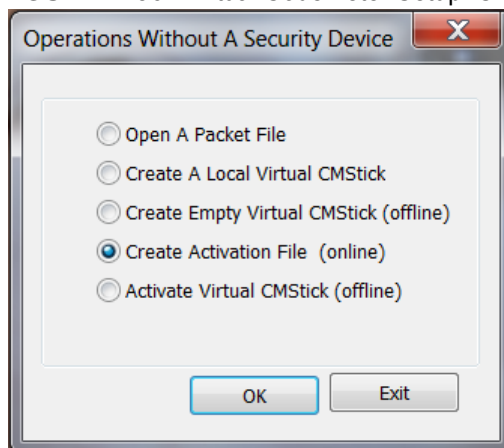
5. Highlight the `TemplateDisc5010.wbb` file, then click **Import**.
6. Click the **Activate License** button.
7. When the *CmFAS Assistant* opens, click **Next**.
8. Select **Create license request**, and click **Next**.
9. Confirm the desired directory and filename to save `.WibuCmRaC`. (Example: `Test1.WibuCmRaC`)
10. Click **Commit**.
11. Click **Finish**.

To Copy to another machine

1. Copy the new `.WibuCmRaC` to another machine that is not running Windows Server 2003/2008 Enterprise.

Note: The destination system must have an active internet connection.
2. Unplug any AccessData dongles you currently have connected.
3. Launch *License Manager*.
4. Select **Create Activation File (online)**.

FIGURE A-30 Virtual CodeMeter Setup: Create Activation File (online)



5. Click **OK**.
6. In the Confirmation Code Required dialog enter your confirmation code and click **OK**.
7. AccessData License Manager will automatically synchronize with the License Server over the internet. Data synchronized from the server will be written to the `*.wibucmrau` file. Click **OK** when the update completes.

To Finish the activation on the Windows Server 2003/2008 Enterprise system

1. Copy the activated `.WibuCmRaC` file to the Server 2003/2008 machine.
2. On the Server 2003/2008 machine, unplug any CodeMeter devices.
3. Open the CodeMeter Control Center. Make sure the window on the License tab empty indicating that no licenses are currently loaded.
4. Select **File > Import License**.
5. Browse to the location where the activated `.WibuCmRaC` is stored. Click **Import**.
6. AccessData License Manager now displays a serial number for the VCM on the Licenses tab and the VCM can now operate in a similar way to a hardware CodeMeter device.

Additional Instructions for AD LAB WebUI and eDiscovery

This section provides additional information for enabling the Web User Interface to recognize a VCM.

To enable AD Lab WebUI and eDiscovery to use VCM

1. Open Registry Editor.
2. Navigate to the following key:
HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products
3. Add the following DWORD registry string to the key and set the value to 1:
HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products | EnableACTTest

FIGURE A-31 Registry Editor: Add a DWORD String

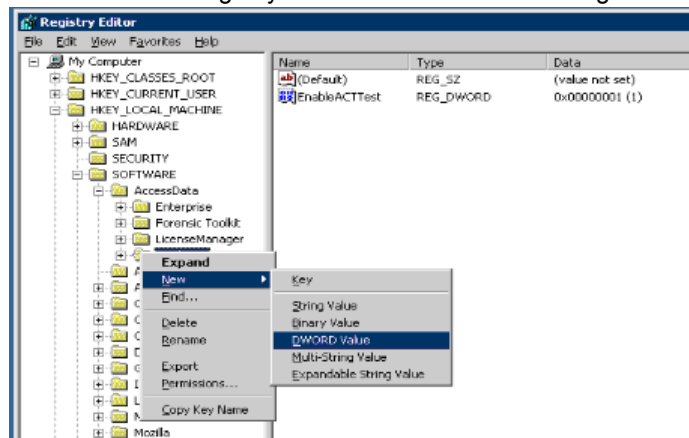
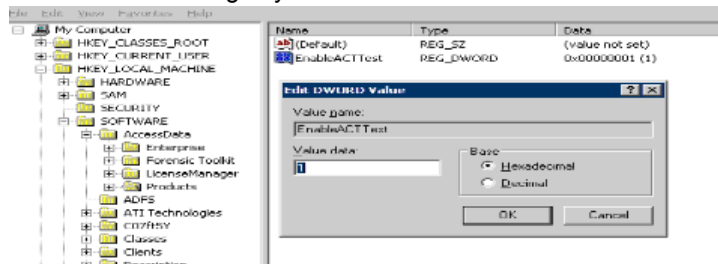


FIGURE A-32 Registry Editor: Add a DWORD Value



The *AccessData License Service* will know to expect a VCM when *EnableACTTest* is set to "1."

Virtual CodeMeter FAQs

Q: How do I get a Virtual CodeMeter (VCM)?

A: Contact your AccessData product sales representative. They will provide you with a VCM confirmation code.

Q: How do VCMs work?

A: A VCM operates in almost exactly the same way as a hardware CodeMeter device, except that they exist as a file stored on the hard disk. During activation, the VCM file (named with a WBB extension) is tied to the hardware of the system using unique hardware identifiers. Those unique identifiers make VCMs non-portable. When AccessData License Manager is launched, it will automatically load the VCM and display its license information. From there, you can refresh, remove, add existing licenses, etc just the same you would with a hardware security device.

Q: Are VCMs supported on virtual machines (VM)?

A: No. Due to the fact that virtual machines are portable and VCMs are not, VCMs are not supported on virtual machines. Currently it is recommended to use AccessData Network License Service (NLS) to license systems running as virtual machines. [CLICK HERE](#) for more information.

Q: Does the AccessData Network License Service (NLS) support VCMs?

A: The current release of NLS does not support using VCM as a network dongle. AccessData is considering this support for a future release.

Q: How can I "unplug" a VCM?

A: If you want to prevent License Manager from automatically loading the VCM you can "unplug" it by stopping the CodeMeter Runtime Service server and then moving (cut and paste) the WBB file to a new location (renaming the file does not suffice). By default the WBB file is located at:

32 bit systems:

C:\Program Files\CodeMeter\CmAct\

64 bit systems:

C:\Program Files (x86)\CodeMeter\CmAct\

Q: I have activated a VCM on my system, but now I need to activate it on a different system. What should I do?

A: Since a VCM is uniquely tied to the system on which it is activated, it cannot be moved to any other system. If you need to activate a VCM on a different system, you need to contact your AccessData Sales Representative.

Q: What if I need to reinstall Windows, format my drive, change my system's hardware, or back up my VCM in case of a disaster? Will the VCM still work?

A: The VCM can be backed up by simply copying the WBB file to a safe location. It can be restored by copying the WBB file to the CmAct folder. The VCM cannot be restored without a WBB file. If you do not have a back up of your WBB file, you will need to get a new confirmation code from your AccessData Sales Representative.

Q: My AccessData product does not seem to recognize the license stored on a VCM. What am I doing wrong?

A: VCMs are supported by the following versions of AccessData products:

- FTK 1.81.6 and newer
- FTK 3.1.0 and newer
- PRTK 6.5.0 and newer
- DNA 3.5.0 and newer
- RV 1.6.0 and newer
- eDiscovery 3.1.2 and newer
- AD Lab 3.1.2 and newer
- AD Enterprise 3.1.0 and newer
- MPE+ 4.0.0.1 and newer

Ensure that the version of the product you are running support VCMs. If the version you are running is listed as supported, verify that according to License Manager, the release date of the version you are running falls before the expiration date of the license.

Network License Server (NLS) Setup Guide

Introduction

This section discusses the installation steps and configuration notes needed to successfully setup an AccessData Network License Server (NLS).

Note: Click on this link to access the latest version of this guide:

[Network License Server \(NLS\) Setup Guide.](#)

Preparation Notes

- CodeMeter Runtime 3.30a or newer must be installed on all Client and Server systems
- AccessData License Manager must be used to prepare the network dongle. The system running License Manager must have internet access and have CodeMeter Runtime installed.
- The current release of NLS supports the following versions of Windows:
 - Windows XP 32/64 bit
 - Windows Server 2003 32/64 bit
 - Windows Vista 32/64 bit
 - Windows Server 2008 R1 32/64 bit
 - Windows 7 32/64 bit
 - Windows Server 2008 R2 64 bit

Setup Overview

To setup NLS

1. Download the latest release of NLS located in the utilities section of the AccessData download page.
2. Extract contents of ZIP to a folder of your choice.
3. On the NLS server system, run through the NLS Installation MSI and accept all defaults.
4. Prepare network dongle:
 - 4a. Provide the serial number to AD Support and request to have the “Network Dongle Flag” applied.
 - 4b. Migrate any additional licenses to the network dongle
 - 4c. Refresh the network dongle device using AccessData License Manager.
5. Launch the AccessData product on the NLS client system.
6. Enter the NLS server configuration information:
 - IP address or hostname of NLS server system
 - Port 6921
7. Click, **OK**.

If you encounter any problems, please read the notes below for troubleshooting information.

Network Dongle Notes

- AccessData License Manager 2.2.6 or newer should be installed in order to manage licenses on the network dongle.

- Network dongles can hold up to 120 physical licenses. Each License has a capacity to hold thousands of sub licenses (i.e. Client count or worker count).
- Contact AccessData Technical Support to have your CodeMeter device flagged as a Network Dongle (required for NLS).

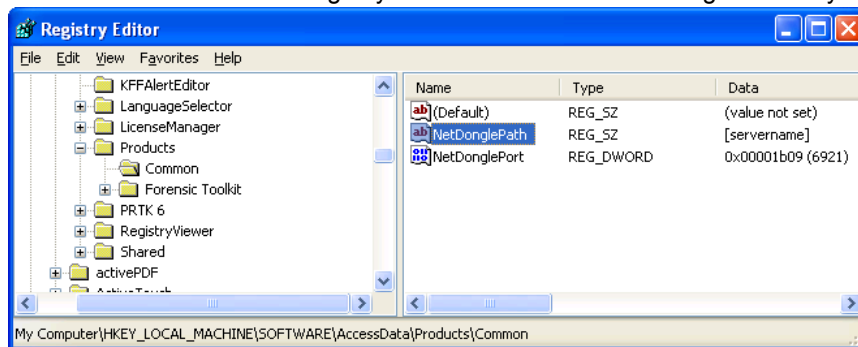
NLS Server System Notes

- Make sure the CodeMeter device is flagged as Network Dongle (i.e. License Manager will show the serial as "1181234N". To have this flag set on your CodeMeter device, please contact AccessData Technical Support).
- Server system must be configured to allow incoming and outgoing traffic on TCP port 6921.
- A web interface to view and revoke licenses all licenses is accessible at <http://localhost:5555>
This page can be reached only from a web browser running locally on the NLS server system.
- A Network Dongle cannot be used to run AccessData products locally unless the NLS server is running locally.
- Some versions of Windows may not find a local NLS server when the DNS hostname of the server is provided. In those cases, it is recommended to use a static IP address.
- When using the NLS across domains, users must have permissions to access resources on both domains (either by dual-domain membership or cross-domain trust).
- When running NLS on Windows Server 2008, Terminal Services must be installed and accepting connections. If Terminal Services is not configured it will not open the port and share out the licenses correctly.
- The name of the service according to Windows is "AccessData Network License Service."

NLS Client System Notes

- When launched, any NLS client application that needs to lease a license from the NLS server will automatically check for the following values within the Windows Registry.

FIGURE A-33 Windows Registry Editor: AccessData NetDonglePath Key



- **NetDonglePath:** The IP address or DNS hostname of the system hosting the Network License Server service which is found in the following registry key on the client system:
`HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products\Common`
- **NetDonglePort:** The TCP port number through which the client and server systems have been configured to use. This value is located in the same key as NetDonglePath.

- **uniqueid**: In order to lease a license from the server, the client system must first possess a unique identification value. This value is automatically generated by applications such as FTK 3, PRTK, or DNA. (Registry Viewer and FTK 1.x cannot be used setup initial client NLS configuration at this time.)

You can find the each client system's uniqueid by inspecting the following registry key: **HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Shared**

- The Client system must be configured to allow all incoming and outgoing traffic on TCP port 6921.
- The following products support the ability to lease a license from a NLS server:
 - FTK 2.2.1 and newer
 - FTK 1.81.2 and newer
 - FTK Pro 3.2 and newer
 - PRTK 6.4.2 and newer
 - DNA 3.4.2 and newer
 - Registry Viewer 1.5.4 and newer
 - AD Enterprise 3.0.3 and newer
 - AD Lab 3.0.4 and newer
 - AD Lab Lite 3.1.2 and previous
 - Mobile Phone Examiner 3.0 and newer
 - Explicit Image Detection (EID) Add-on
 - Glyph Add-on
- Use AccessData License Manager (ver. 2.2.4 or newer) to migrate licenses off other devices and onto a network device.
- When running AccessData products on Windows Vista, 7, or Server 2008 you must choose **Run as administrator** at least once in order to lease a license from a NLS server.
- If the NLS client application is having trouble leasing a license either from the NLS server, AccessData recommends that you reset the licensing configuration to default.
- To reset the licensing configuration, delete and recreate the NLS registry key located at: **HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products\Common**