AD Lab 7.2 Release Notes

Document Date: 11/11/2019

Introduction

This document lists the new features, fixed issues, and known issues for this version. All known issues published under previous release notes still apply until they are listed under “Fixed Issues.”

What is New in 7.2

The following items are new and improved for this release:

Drive Decryption

- Volumes encrypted with McAfee Drive Encryption (MDE) can now be decrypted. (FC-44)
- Encrypted Apple File System (APFS) volumes (other than volumes encrypted by chip internal to Mac systems) can now be decrypted. (FC-4 / FC-228)

  For APFS volumes encrypted by the Apple T2 chip, the best practice would be to acquire the hard drive data while still internal to the system that encrypted it.

Database Integration

- The database schema utilized by the 7.2.x release is backwards compatible with the database schema of version 7.1.x. Therefore, FTK, AD Lab, and AD Enterprise 7.2.x can be configured to integrate with the AccessData eDiscovery or Summation v7.1.x application database as needed.

Evidence Image Exports

- Support for exporting to L01 format is now available. (FC-47)

LDAP Authentication

- When adding or deleting LDAP groups, an option has been added to select all groups listed. (FC-187)

Processing

- The “Event Audit Log” configuration can now be configured when creating a new Evidence Processing Profile template. (FC-37)
- ABBYY is now integrated as an optical character recognition (OCR) engine. (FC-38 / FC-263)

  For installation and configuration guidance, see KB article.

  Note: Quin-C Server must be running to run ABBYY OCR jobs. ABBYY jobs submitted in FTK at a time when the Quin-C server service is not running will be queued and no progress will be displayed in the processing status window.
- Information on all system browser cookies is now aggregated into node found on the “System Information” tab. (FC-251)

Registry Viewer Reports

- Registry Viewer reports have been updated to include registry keys from newer versions of Windows 10. (FC-54)

Viewer

- The old version of the Natural >> Web view tab has been restored to the list of content viewers. You can now toggle between the new Web (HTML5) tab view and the old Web view as appropriate. (FC-204)

Fixed Issues

The following items have been fixed in this release:

Administration

- Fixed group role permission inheritance for systems using Active Directory authentication (LDAP) integration. (FC-185)

Exports

- System Information Tab data now exports to a properly formatted XML file. (FC-52 / FC-161)
- Exports to Browser Briefcase in CoolHTML format have been fixed. (FC-282)
- Resolved issue where Browser Briefcase export in XML format was not being generated (FC-325)

Search

- “Files created between” date range index search option now returns expected results (FC-120)

User Interface

- Resolved list scrolling performance issues that affected systems with Windows Authentication integration (LDAP) and the “Label” column added to the file list. (FC-9)
- Fixed issue that caused FTK to crash when viewing certain SQLite DB files. (FC-128)
- Improved handling of search results pane after clicking the “CLEAR” option to remove previous live search results. (FC-123)
- Corrected issue that caused the Integrated Security setting to be automatically set to TRUE upon launching the application. (FC-158)
- Improved performance of application startup when using Network License Service (NLS). (FC-162)
- Fixed issue causing very slow application launch due to LDAP queries. (FC-163)
- Windows Authentication (LDAP) users who have logged out of the application are now able to log back in without having to sign out of Windows first. (FC-248)
- Fixed issue where custom column templates saved to your case could not be utilized by other cases. (FC-273)

Processing

- Improved parsing of long chat conversations from UFDR images. (FC-53)
- Improved processing of restore points (more than 31 (FC-64)

- Improved evidence path handling of cases with expanded Volume Shadow Copies (Restore Points) in the “Add / Remove Evidence” dialog. (FC-64)
- Improved recognition of evidence images containing exFAT file systems. (FC-156)
- Improved handling for certain UFDR image processing. (FC-159)
- Processing error that resulted in “Failure: Post-Processing: PopulateQuinCFamily failed” message now displays the correct error. (FC-169)
- Improved parsing of OneNote files so that they can be properly rendered in the viewer. (FC-202)
- Improved display functionality of emails subject line when invalid characters are detected. (FC-215)
- Improved handling of APFS partition detection and decryption of certain APFS images. (FC-228 / FC-234)

Important Information

Supported Platforms

Windows Operating Systems Support

The following operating systems are supported:

- Windows 7
- Windows 10 Version 1709 (OS Build 16299.309) and 1809 (OS Build 17763.437)
- Windows Server 2012
- Windows Server 2016

Microsoft SQL Server Support

The following SQL databases are supported:

- SQL Server 2012
- SQL Server 2014
- SQL Server 2016

PostgreSQL Support

The following versions of PostgreSQL are supported:

- 9.6.3.5
- 11.2 (this is the version provided with the FTK installation files)

For Additional Information

Latest Documentation

The documentation is sometimes updated. For the latest documentation, see the product download page:

http://accessdata.com/product-download

or download the zip file from

www.accessdata.com/productdocs/ftk/ftk.zip

www.accessdata.com/productdocs/adlab/adlab.zip

Installation and Upgrade

- When installing 7.2.x to a system that has 7.1.x installed, the 7.1.x installation binaries will be automatically uninstalled and the case databases will be automatically upgraded to be compatible with 7.2.x. Once upgraded to 7.2.x cases upgraded as part of this process cannot be reverted to 7.1.x compatibility. (FC-272)

- The FTK Suite (FTK, AD Lab, AD Enterprise) no longer supports multiple products of the same version running on the same machine at the same time. The user can only install one of the three products of a specific version on a single machine. (29786, 30927)

Cloud Based Relational Database Services (RDS) Support

The AccessData Suite can now utilize the power and scale of Amazon Web Services™ managed relational database service (AWS RDS).

Users have the option to use the AWS™ provided PostgreSQL engine or the AWS Aurora™ service. AWS PostgreSQL RDS is wire-compatible with PostgreSQL 9.6.x.

AWS Aurora is an Amazon proprietary service that is PostgreSQL compatible offering up to 3x faster than a traditional PostgreSQL 9.6.x instance.

To use the amazon RDS Instance, you will need to set up your instance in your AWS console prior to installing the AccessData Suite. When selecting your RDS instance, make sure that the DB engine version for both Aurora and RDS is 9.6.x or higher. AccessData does not support PostgreSQL version 10 in this release.

You will also need to specify a "master" user. This is to work around the limitation that the RDS and Aurora PostgreSQL engine(s) will not allow users to have access to the "postgres" user within the DB engine. Please discuss this and all security implications with your network or database administrator(s).

Once you have selected and set up your database instance, you will use the "endpoint" on the status screen to connect your database.

Once this endpoint is available, you will be able to select "Cloud Based" on the UI of the "Add Database" screen for the AccessData Suite.

When prompted, enter both the Username and Password you provided during the RDS set up in your AWS console. Once complete, the database(s) for your products will be in the AWS cloud, alleviating the need for an on-premises Database server and instance.

Important: AccessData recommends not making the Database "Publically accessible" for security reasons. If using a VPN to connect to your cloud provider, you will need to update the rules for your security group to allow connections over your VPN.

AD Product Virtualization and Cloud Guidelines

Overview

This document outlines the support boundaries and procedures for supporting virtualized environments with AccessData software.

Introduction

While virtual machines have not traditionally been supported with AD Products; the fact is that most customers – small/medium business as well as large enterprise have rapidly moved away from a 1:1 server configuration for their workloads. Running virtual machines and sharing the resources have long been a way to maximize the investment of computing resources.

A virtual machine / virtualized environment that is properly configured will work as reliably, and perform essentially the same as a physical server with dedicated resources.

Supported Virtual Environments

AccessData products are certified, and will work on the following Hypervisors and Cloud Based Environments:

Vendor/Service Provider	Version	Notes
VMware vSphere / ESXi	6.1 and higher	VMs must be Version 10 or higher
Microsoft Hyper-	V2012 R2 release and higher	VMs must be Generation 2
Amazon Web Services Elastic Compute Cloud (EC2)	AMIs running Windows Server 2016	AccessData recommends using c5/m5 compute fleets for AD Products.
Amazon Web Services Relational Database Services (RDS)	PostgreSQL Version 9.6.3 and higher. Aurora instances must not be version 10 or beyond.	AccessData recommends using db.m4 and db.r4 instances in your RDS deployment.
Microsoft Azure Compute Services	Azure Windows Virtual Machines running Windows Server 2016	AccessData recommends using Dsv2, Dsv3, Dv3 and Dv2 compute fleets for AD Products.

AccessData realizes there are other options for your cloud compute and virtualization infrastructure, however our products have not been tested on them for functionality and will not support providers and infrastructure outside of the guidance listed above.

Support Boundaries

AccessData will support its products in a virtual environment running on supported operating systems and environments by both the Vendor/manufacturer and AccessData.

Our software is designed and tested to work on various versions of Microsoft Windows, and our support strategy is based upon these being in compliance with vendor support and EOL Matrices.

AccessData does require that all of a customer(s) virtual resources are configured in alignment with our best practices and configuration work flow as outlined in our product documentation or as specified by our support team(s).

This includes ensuring that Virtual Machine resources are statically set and not dynamically set, nor controlled by the hypervisor – This applies specifically to the Processor Allocation, RAM, and Block Storage for a virtual machine to ensure they never go below a minimum threshold as outlined in our configuration guidelines.

Support Exclusions

- Underlying Network Performance problems on a Virtual switch
- Underlying disk performance problems on a virtual machine and/or host
- Connectivity to storage – beyond ensuring AccessData's products can connect to their resource(s)
- Non AccessData software issues (e.g. Microsoft SQL Server)
- Clustering / High Availability / Resiliency software
- Protocol specific errors, including but not limited to
    - iSCSI Protocol Errors
    - VLAN Tagging
    - Virtual Machine Queue(s) (VMQ) on 10 GB Networks
    - Attempting to mount volumes over Network File System(s) (NFS)
- Under provisioning/configuration errors on a virtual machine.

Links and Resources

Microsoft Windows Server Product Lifecycle:

https://support.microsoft.com/en-us/lifecycle/search/1163

VMware Lifecycle Product Matrix:

https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/product-lifecycle-matrix.pdf

Important: Not All products are guaranteed to work with all products from a specific vendor!

Running PostgreSQL on a Virtual Machine

If you run PostgreSQL on a virtual machine with a dynamically allocated virtual hard drive, you must manually stop the PostgreSQL service before rebooting the virtual machine. Otherwise, PostgreSQL will become corrupted.

If you run PostgreSQL on a virtual machine with a fixed size virtual hard drive, then PostgreSQL will not become corrupted when rebooting.

This does not apply to PostgreSQL instances hosted in a managed database service such as AWS Relational Database Service™.

MEMORY ANALYSIS

- The memory analysis tool is only available for use up to Windows 7, 64 bit.

KFF

- The KFF Server uses the Apache Cassandra database. The version of Cassandra being used requires 64-bit Java 8. No other version of Java (7 or 9) is currently supported.
    - To install Java, go to: https://java.com/en/download/windows-64bit.jsp
    - If you are using a 32-bit browser, your browser may automatically download the 32-bit version. You must use the 64-bit version.
- Make sure that you use the latest version of the KFF Server.
  See https://accessdata.com/product-download > Known File Filter 5.6 and up.
- When importing data using the KFF Import Utility, make sure that you get a confirmation that the import is complete before processing data using that KFF data. This is particularly important when importing NSRL data that takes several hours to import.
- Only the Project VIC and NSRL sets are locked/protected. All other sets in the KFF can be modified and archived.

Recommendations

- Cerberus writes binaries to the AD Temp folder momentarily in order to perform the malware analysis. Upon completion, it will quickly delete the binary. It is important to ensure that your antivirus is not scanning the AD Temp folder. If the antivirus deletes/quarantines the binary from the temp, Cerberus analysis will not be performed.
- If you choose to have a case's database files placed in the case folder, do not move your case folder without first archiving and detaching the case.
- When creating a Custom Data View, the available filter list should not include: Checked Files, Unchecked Files (checked status is not available across users), Bookmarked Files, Labeled Files (too broad and will include all bookmarks or labels). These filters have been removed from the list. (6533)
- Difference in file handling when using Belkasoft parsing:

- If a SQLite database is encountered in the evidence that could have been handled by the Belkasoft parser but the Belkasoft All-in-One processing option was not checked, that SQLite database will get expanded using a generic SQLite expansion that shows tables and rows.
- Any evidence processed in this manner that is later re-processed (using Additional Analysis) with the Belkasoft All-in-One expansion option will NOT be expanded using Belkasoft technology but will remain with the original expanded items.
- To expand a SQLite database using Belkasoft technology that has already been expanded as a generic SQLite database, it must be added as a new, different piece of evidence, or a new case must be created.

Known Issues in 7.2

Chats

- The Belkasoft option is for parsing chat messages and using AccessData's parsing, and when available, will result in additional extracted data.
- If you use the All Communications processing profile and you have Belkasoft marked, Viber and Hangouts information is not parsed correctly. Only chat messages are returned. (17155)

Database

- If you have cases created in v7.1.0.290 or earlier, opening any of those cases in v7.2 or newer will cause the application to auto-upgrade the case's database schema and therefore the case will no longer open in v7.1.0.290 AccessData has released a v7.1.2.6 patch that resolves this issue and allows the case to be opened in either v7.1.0.290 or v7.2. (FC-168)
- When installing 7.2.x to a system that has 7.1.x installed, the 7.1.x installation binaries will be automatically uninstalled and the case databases will be automatically upgraded to be compatible with 7.2.x. Once upgraded to 7.2.x cases upgraded as part of this process cannot be reverted to 7.1.x compatibility. (FC-272)

Decryption

- When adding an image encrypted with FileVault2 on Mac 10.11 or later, you are not prompted for a password and as a result, the image data is not recognized. (17440)

Distributed Processing Manager

- When using a Distributed Processing Manager, and creating a project using a local path, you may receive an error that it cannot find ProcessingHost.exe. (9104)

  Workaround: Manually change the case path and/or evidence path to UNC.

Forensic Image Support

- Image integrity verification of L01 formatted images is not supported and will result in an error. When exporting to L01 format from the examiner interface the image will export successfully, however selecting the option to "Add image to case when completed" will result in an error stating that image verification failed.

Python Script Wizard

- If you open the Python Script Wizard, and you don't have a Python environment installed, in the Python Environment field, instead of a clear message, you will see a message the says "The system cannot find the specifiedExit Code : -98765". (17563)
- Python 2 environments will not have access to some features due to restrictions of the software

Processing

- A user with the Project/Case Administrator role can restore/attach any case, not just the cases that the user has rights to. However, if the user does not have rights to a case that is restored/attached, they still cannot see it in the Case List. (15804)
- Deleted files in APFS file systems are able to be recovered during processing by selecting the "Meta Carve" option. It is recommended to exclude duplicates from your case as this process will likely create numerous duplicate files. (FC-228 / FC-239 / FC-322)
- L01 files encrypted by FTK are not supported. If you need to encrypt the logical image you are creating, create an encrypted AD1 image. (FC-337)

Viewers

- In Examiner and in the Web HTML 5 viewer, if you are viewing web content that has an Adobe SWF files in it, the SWF file will not be displayed. (17554)

Windows 10 Mail

- When viewing Windows 10 Mail (Unistore Database) evidence, Submit Date data is not available. (14165)

Comments?

We value all feedback from our customers. Please contact us at support@accessdata.com, or send documentation issues to documentation@accessdata.com.

AccessData Legal Information

Document date: November 11, 2019

Legal Information

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

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

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

AccessData Group, Inc.
603 E. Timpanogos Circle
Building H
Orem, UT 84097 USA

AccessData Trademarks and Copyright Information

The following are either registered trademarks or trademarks of AccessData Group, Inc. All other trademarks are the property of their respective owners

.

AccessData®	AD Summation®	Mobile Phone Examiner Plus®
AccessData Certified Examiner® (ACE®)	Discovery Cracker®	MPE+ Velocitor™
AD AccessData™	Distributed Network Attack®	Password Recovery Toolkit®
AD eDiscovery®	DNA®	PRTK®
AD RTK™	Forensic Toolkit® (FTK®)	Registry Viewer®
LawDrop®	Summation®	

A trademark symbol (®, ™, etc.) denotes an AccessData Group, Inc. 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:

- AFF® and AFFLIB® Copyright® 2005, 2006, 2007, 2008 Simson L. Garfinkel and Basis Technology Corp. All rights reserved.
  Copyright © 2005 - 2009 Ayende Rahien
- FreeBSD ® Copyright 1992-2011. The FreeBSD Project.
- BSD License:
  Copyright (c) 2009-2011, Andriy Syrov. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer; Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution; Neither the name of Andriy Syrov nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- WordNet License:
  This license is available as the file LICENSE in any downloaded version of WordNet.
- WordNet 3.0 license: (Download)
  WordNet Release 3.0 This software and database is being provided to you, the LICENSEE, by Princeton University under the following license. By obtaining, using and/or copying this software and database, you agree that you have read, understood, and will comply with these terms and conditions.: Permission to use, copy, modify and distribute this software and database and its documentation for any purpose and without fee or royalty is hereby granted, provided that you agree to comply with the following copyright notice and statements, including the disclaimer, and that the same appear on ALL copies of the software, database and documentation, including modifications that you make for internal use or for distribution. WordNet 3.0 Copyright 2006 by Princeton University. All rights reserved. THIS SOFTWARE AND DATABASE IS PROVIDED "AS IS" AND PRINCETON UNIVERSITY MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PRINCETON UNIVERSITY MAKES NO REPRESENTATIONS OR WARRANTIES OF MERCHANT- ABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE LICENSED SOFTWARE, DATABASE OR DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. The name of Princeton University or Princeton may not be used in advertising or publicity pertaining to distribution of the software and/or database.

Title to copyright in this software, database and any associated documentation shall at all times remain with Princeton University and LICENSEE agrees to preserve same.

- XMLmind XSL-FO Converter Professional Edition Developer License Agreement:
  Distribution
  Licensee may not distribute with the Application any component of the Software other than the binary class library (xfc.jar) for the JavaTM version and the Dynamic Link Library file (xfc.dll) for the .NET version.
  Licensee shall include the following copyright notice: "XMLmind XSL-FO Converter Copyright © 2002-2009 Pixware SARL", with every copy of the Application. This copyright notice may be placed together with Licensee's own copyright notices, or in any reasonably visible location in the packaging or documentation of the Application.
  Licensee may use, distribute, license and sell the Application without additional fees due to Licensor, subject to all the conditions of this License Agreement.
- "Amazon Web Services", "AWS" "AWS Aurora" "AWS Relational Database Service" are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries and is used with permission https://aws.amazon.com/aispl/trademark-guidelines/.
- Apache(r), Apache Cassandra and the flame logo is a registered trademark of the Apache Software Foundation in the United States and/or other countries. No endorsement by the Apache Software Foundation is implied by the use of these marks.