AccessData AD Enterprise 6.5 Release Notes

Document Date: 06/19/2018

Introduction

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

Supported Platforms

The followng platforms are supported for running AD Enterprise:

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

New and Improved in 6.5

The following items are new and improved for this release:

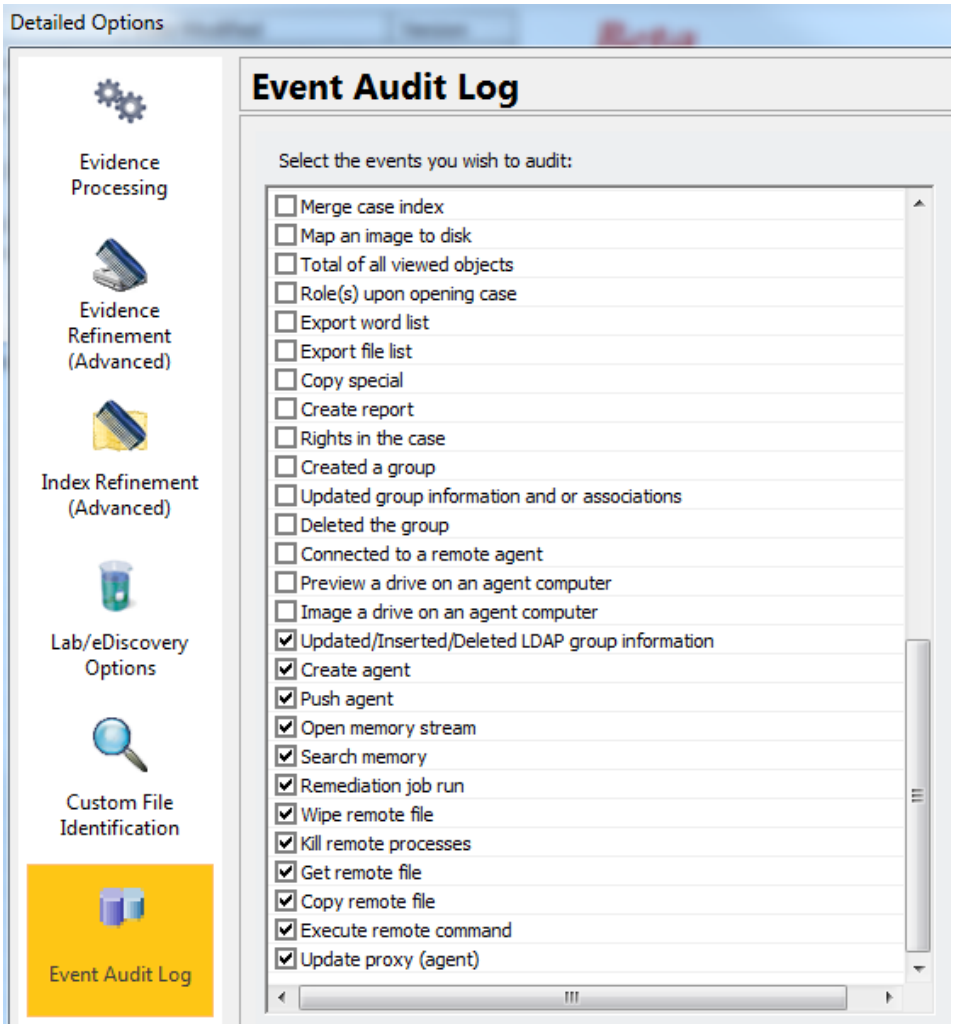
Removal of ADMS

ADMS functionality has been integrated within the Case Manager and Examiner interfaces.

For example:

- Users are managed from the Case Manager under Database > Administer Users.

- Roles are managed from the Case Manager under Database > Administer Roles.
  Roles include many rights. The new Enterprise specific rights are:
  - Agent - Acquire
  - Agent - Drive Preview
  - Agent - Remediation
  - Agent - Push
- The Change Network Tree functionality is now called the Agent List.
  The Agent List is available in the Case Manager under Tools > Preferences > Agent Configuration.
- The Audit Logs have been incorporated into the Event Audit Log.
  The Event Audit Log is configured through the Event Log Processing Options. These are available in the Evidence Processing Options when creating a new case.



AD CyberForensics Initial Triage

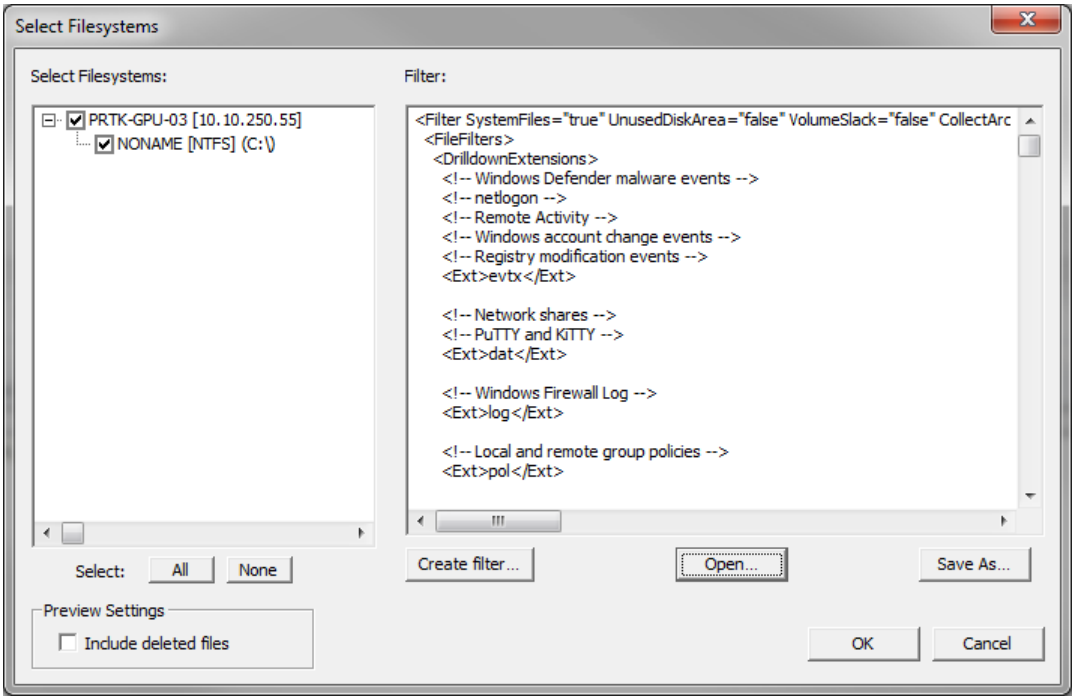
Use this targeted, prebuilt filter to quickly preview common areas of interest to determine the severity of a breach. Determine the scope of the incident and what was impacted in the system.

The filter is named AD_Cyber_Forensics_Initial_Triage_Filter.xml and can be found at the following path:

ProgramData > AccessData > Products > Forensic Toolkit > 6.x

You can do the following:

- Investigate suspected systems to determine the scope and root cause of an incident.
- Determine whether a machine has been compromised or has compromised others.
- Use predefined or personalized filters to create targeted data collections for up to 50 nodes.



Using predefined filter settings, you can investigate the following items:

- System files
- Installed programs
- Registry information

Preview of live data (a collection of metadata with a link to the live file) can include the following options:

- Antivirus trigger logs for Windows Defender and McAfee
- Socket lists
- Creation or modification of escalated (administrative) credentials
- Remote group policies (those synced through Active Directory)
- Local Group Policies
- Out-of-the-box Windows group policy registry keys

- Remote access events monitoring
- Communication between systems
- Absolute path matching
- Windows firewall logs

Filters, Parsers, & Filesystems

- Windows Defender Antivirus event log: filter
- Net Logon events: filter
- Remote Login (Remote Activity) events: filter
- Network shares: filter
- Windows Registry Modification events: filter
- Windows Registry out-of-the-box registry policies: filter
- Windows Group Policy (Registry.pol): filter, parser, and filesystem
- McAfee Antivirus Log: filter, parser, and filesystem
- Windows Firewall Log: filter, parser, and filesystem
- SSH - PuTTY and KiTTY: filter
- SSH - MobaXterm: filter and parser
- SSH - XShell: filter and parser
- SSH - OpenSSH known_hosts file: filter, parser, and filesystem

Memory Analysis

- Static Memory Analysis and additional Live Memory Analysis are supported for the following operating systems:
  - 32- and 64-bit Windows 10
  - 64-bit Windows Server 2016
  - 64-bit Windows Server 2012 and 2012 R2
  - 32- and 64-bit Windows 8, 8.1, and 8.1 Update 1
  - 32- and 64-bit Windows 7 (all service packs)
  - 32- and 64-bit Windows Server 2008 (all service packs)
  - 64-bit Windows Server 2008 R2 (all service packs)
  - 32- and 64-bit Windows Crash Dump

Important: Windows 10 version 1709 and newer is **not** supported for memory analysis.

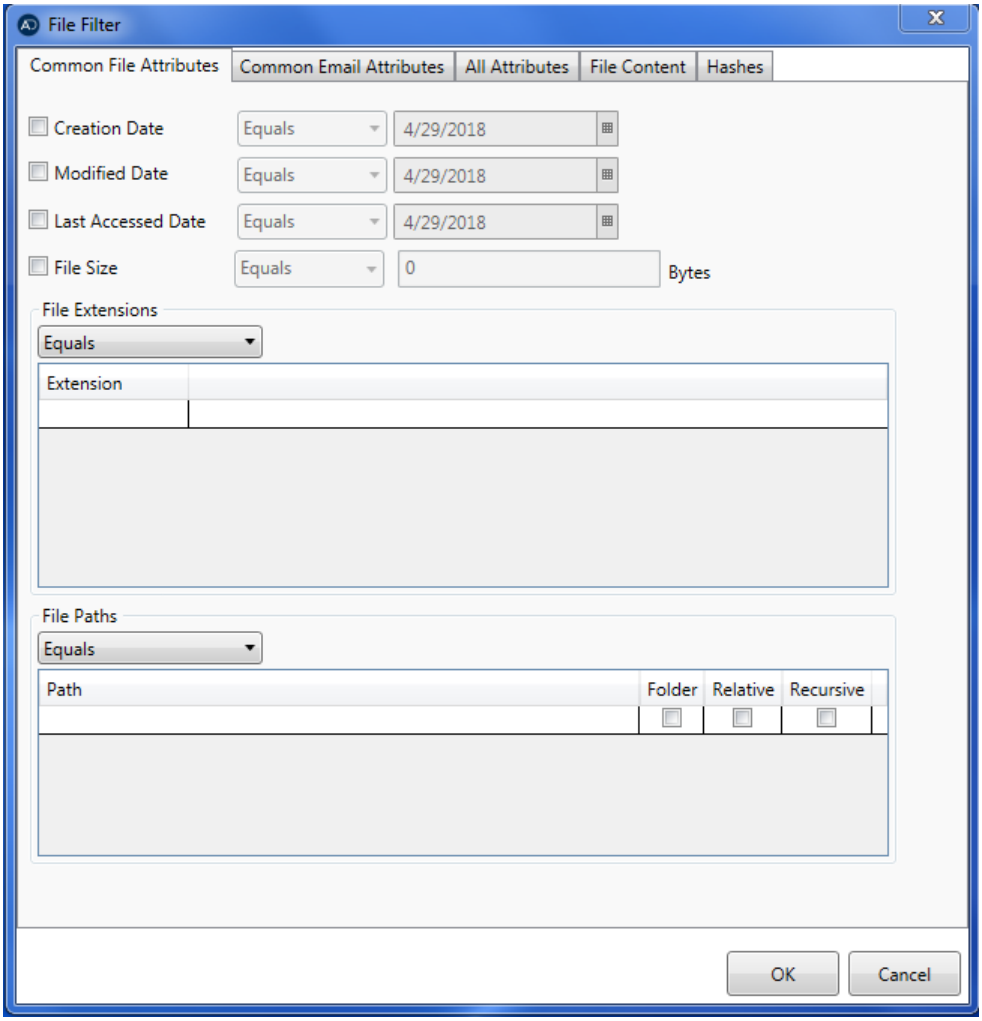
Filter Builder

The filter builder tool allows you to create complex filters for use within the *Select Filesystems* collection dialog.

Note: File content searches use the ECMA script.

Options inlcude:

- Include and Exclude filters
- Common File Attributes
- Common Email Attributes
- Customized Attribute Selections
- File Content
- Hashes



Agent

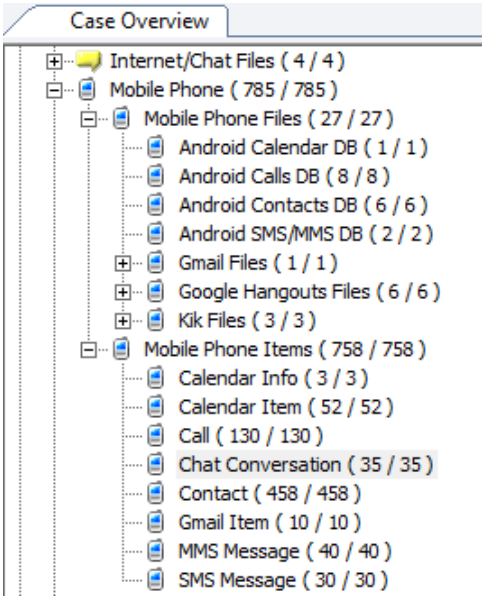
- Parse into compound files, matching inner items
- Ability to match arbitrary attributes
- Ability to match using absolute paths
- Preview up to 10 times faster using absolute paths

Mobile Phone Support

Android

Parsers have been added for the following data:

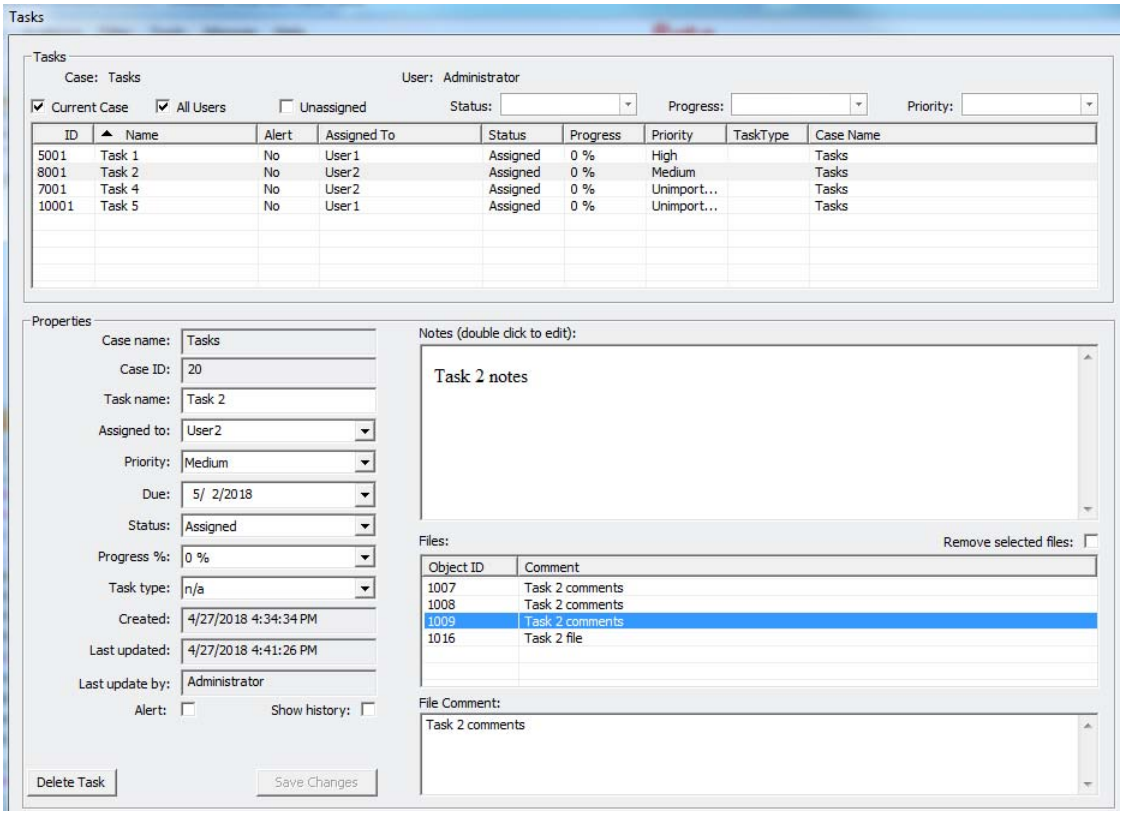
- Phone Contacts from the Address Book
- SMS/MMS messages from the Android Messages app
- Calendar
- Call Log
- Google Hangouts for Android
- Kik for Android
- Gmail for Android



Tasks

A new task feature has been added which lets you do the following:

- Administrators and users can create tasks within a case and assign them to users.
- As users review case data, they can assign evidence items to a task.
- Users can report the status and progress of a task as well as add notes.
  Administrators and users can view the status of tasks and the files associated with the tasks.



Fixed Issues in 6.5

- Enhancements for absolute paths (12832)
- Memory Analysis now works for modern operating systems (12612)
- The Company column now populates for Mobile Phone Contacts (13054)
- The SRC (source) column now works correctly when processing XRY files (13123)
- The import utility server address no longer reverts back to localhost every time it closes (13163)
- Generate Common Video File option is now functional for all cases (13815)
- Loading times for copy previous case for MSSQL has been improved (13090)
- Agent list will now refresh automatically when adding new nodes (13210)
- Adding hashes to the KFF from the volatile screen no longer fails (13951)

Important Information

Latest Documentation

- **To access the latest AD Enterprise Release Notes and documentation:**
  Download the zip file from www.accessdata.com/productdocs/adenterprise/adenterprise.zip.

Installation and upgrade

- If you install AD Enterprise on a Windows 2003 64-bit computer, you must configure the ASP .NET service extension. To configure this, do the following:
  - Open the Microsoft Internet Information Services (IIS) Manager.
  - In the left pane, click Web Service Extensions.
  - In the extensions list, click ASP.NET v4.x.
  - Click Allow.
- 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)
- AD Enterprise supports Distributed Processing Engines (DPEs).
- Using the AD Enterprise 6.5 Agent with eDiscovery 6.3 SP2.

WARNING: eDiscovery 6.3 SP2 can use the Enterprise 6.5 agent. However, because they use different database versions, do not install Enterprise 6.5 on an eDiscovery 6.3 server. Only install products together when they are the same version. Otherwise, installing Enterprise will upgrade the eDiscovery database and you cannot revert that change without a database restore.

Agent Support

- Official Support for Red Hat Linux 6.x and 7.x
  The 6.2 Linux Agent requires GLIBC 2.17 or newer. Collection from a system running on an older GLIBC version can be attempted using the 6.1 version of the Agent, which can be obtained by contacting AccessData Support. A system's GLIBC version can be determined by running the following command: `ldd -version`.

Upgrading CodeMeter

- AD Enterprise 5.6.1 and later include an updated version of CodeMeter Runtime Kit (5.21).
  - If this is a new installation of AD Enterprise you do not need to do anything and the latest version of CodeMeter is installed.
  - If you are upgrading to AD Enterprise 5.6.1, be aware that a security vulnerability has been detected in Codemeter 4.5. However, if you simply upgrade from CodeMeter 4.5 to 5.21, the vulnerability remains. To fix the vulnerability, you must manually uninstall 4.5 before installing 5.21.

    If you are upgrading to AD Enterprise 5.6.1, manually uninstall CodeMeter first and then install AD Enterprise 5.6.1 which will install a clean CodeMeter 5.21. Otherwise, after upgrading to AD Enterprise 5.6.1, manually uninstall CodeMeter 4.5 and then manually install CodeMeter 5.21.

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.

KFF

- The KFF Server now 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, you may automatically download the 32-bit version. You must use the 64-bit version.
- 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.
- Deleting NDIC, DHS, and NSRL KFF libraries.

  As of 6.3, you can delete NDIC, DHS, and NSRL libraries from within the AD Enterprise application.

  Important: Deleting these libraries from the application can take from one to several hours. We recommend that you delete these libraries using the KFF Import Utility.
- Only the Project VIC and NSRL sets are locked/protected. All other sets in the KFF can be modified and archived.
- NDIC or DHS sets cannot be migrated and must be imported into the 6.4 or later version of KFF.

Recommendations

- 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 the manner that is later re-processed (using Additional Analysis) with the Belkasoft All-in-One expansion option will NOT be expanded using Belksoft 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.

Windows build used for testing this release

- Windows 10 Version 1709 (OS Build 16299.309)

New AD1 files and Imager 3.4.x

Any AD1 file created by FTK or Summation 6.0 or later can only be opened with Imager 3.4.0 or later.

Imager 3.4 can be freely download from the AD website:

http://accessdata.com/product-download

Using an older version of Imager will result in an “Image detection failed” error.

This happens because the AD1 format was enhanced to support forward compatibility between AccessData products. Newer AD1s have a version 4 in the header instead of 3. A hex editor can be used to quickly determine if your AD1 is v3 or v4.

Known Issues in 6.5

Known Issues

Enterprise Roles and Rights for seeing tabs in the Examiner

- Agent - Drive Preview

  The Agent - Drive Preview right replaced the Browse right in previous versions. When configuring Roles and Rights in Enterprise 6.5 for non-administrators, in order for a user to see the *Explore*, *Graphics*, *Live Search*, and *Index Search* tabs in the Examiner, their role must include the *Agent-Drive Preview* right. Otherwise, when users access the Examiner, those tabs are not visible. (15099)

Tasks

- Task and Bookmark notes: When attempting to change a font in a note, some text must be selected first. If you change the font without pre-selecting text, you will get an error. (14923)

Android phone support

- When viewing Android phone Contact information in the *Overview* tab, on the *File Content* > *Natural* tab, the *Display Name* is displayed twice. (14946)

Volatility

- Windows 10 version 1709 is not supported for memory analysis (13967)

Where to get more information

Use the following documentation resources to learn more about this product. Each document is available in PDF format.

Document	Description
User Guide	Information about how to use this product, including detailed technical information and instructions for performing tasks. Download the latest documentation zip file from www.accessdata.com/productdocs/adenterprise/adenterprise.zip.
KFF Quick Install Guide and KFF installation files	For the most current KFF Server and KFF data installation files, as well as the *KFF Quick Install Guide*, visit the AccessData Product Downloads page: http://accessdata.com/product-download Expand the *Known File Filter (KFF)* section and then the *KFF Server* section.

Comments?

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