December 2018

Absolute 7.4 Release Notes

This document describes the software changes included in Absolute 7.4. It also describes the changes included in all hotfixes since the release of Service Pack 2 of Absolute 7.3.

These software changes introduce performance, security, data integrity, and usability improvements that enhance the responsiveness, reliability, and ease of use of the system. In addition, they also introduce enhancements, improvements, and fixes to existing features and functionality:

NOTE Depending on the Absolute licenses associated with your account, some of the following improvements and fixes may not be available to you.

Feature enhancements

This release introduces the following feature enhancements:

- ***Mac support***: Absolute now supports devices running version 10.14 of the macOS operating system.

  IMPORTANT Before upgrading your devices to macOS 10.14, note that Geolocation Tracking using Wi-Fi Positioning is not supported by this version of the operating system. If you want to upgrade your devices, you can ensure that device location information continues to be available in the Absolute console by enabling the Wi-Fi Networking setting in your Mac devices' System Services. For more information about configuring this setting, see *Absolute Geolocation Tracking on macOS Mojave (10.14)* in the Absolute Knowledge Base: https://community.absolute.com/s/article/Absolute-Geolocation-Tracking-on-macOS-Mojave-10-14.

  Note that Absolute will introduce a resolution to the Wi-Fi Positioning limitation in an upcoming release.

- ***Absolute agent for Mac***: To support devices running version 10.14 of the macOS operating system, the Absolute agent for Mac has been upgraded from a 32-bit to a 64-bit application. The new 64-bit agent is compatible with all supported versions (10.9 to 10.14) of the macOS operating system. The new agent is also more robust.

  In January 2019, all accounts that are configured for automatic agent upgrades will be upgraded to the new Mac agent. You'll see an announcement in the Absolute console when the Mac devices in your account are about to be upgraded.

  To download and install the agent on your devices now, go to the Administration > Download Packages page and download Agent Version **966** for Mac.

  For more information about installing the agent on your Mac devices, see the *Administrator's Guide for Absolute Agent* in the Help.

  NOTE After December 5th, 2018, the Mac agent package that you generate in the Administration > Agent Management area includes the new Mac agent.

- ***Application Persistence***: Application Persistence policies, which collect information about the functional status of third party applications installed on your Windows devices, now support persistence of the following applications:
  - Dell Advanced Threat Prevention
  - Dell Data Guardian

- Dell Encryption

When these policies are enabled in your policy groups, Application Persistence reports and widgets now show persistence information about these applications.

For more information, see the following topics in the online Help:

- *About Application Persistence: Dell Advanced Threat Prevention policies*
- *About Application Persistence: Dell Data Guardian policies*
- *About Application Persistence: Dell Encryption policies*

- ***Custom EDD Rules***: In the Data Protection > Endpoint Data Discovery > Rules area, you can now exclude an expression set's Match Score from a custom rule's total Match Score. Select the **Expression Set Options** > **Exclude from Match Score** option if a rule contains multiple expression sets and you don't want to inflate Match Scores unnecessarily. Note that the Match Scores associated with at least one expression set must be included in a rule's Match Score.

  For more information about when to use this option, see the section "Excluding an expression set's Match Score from a rule's total Match Score" in *Working with Expression Sets* in the online Help.

Improvements and fixes

Absolute 7.4 introduces the following improvements and fixes:

Feature/Area	Improvements and fixes
Absolute agent	● When the Absolute agent scans a Windows device for software information, the process no longer consumes up to 2GB of memory on the device if some of the files associated with the data upload are corrupted. ● To improve performance of the Absolute Monitoring Center, the value in the **Size (bytes)** field on a Mac device's Hardware > Memory page is now updated only after a *full* scan of the device's hardware information, not a delta scan.
Application Persistence (AP)	● An issue introduced in version 7.3.2 is now fixed. When the Absolute agent detects that a device's SCCM client is not installed, or the client isn't functioning correctly and a reinstallation is required to fix it, the agent now successfully reinstalls the SCCM client. ● In Application Persistence reports and widgets: ○ A device's 30-Day Reinstall Count is now accurate. Previously, if the Absolute agent needed to reinstall multiple components of a third-party application to bring it into compliance, each installation was included in the count. ○ Previously, when the **Report only** option was enabled in an AP policy, the value for 30-Day Repair Count sometimes indicated that repairs were completed when they were not even attempted. This issue is now fixed. ● In the Application Persistence Device Ranking widget: ○ When you click a bar to view a device's repairs or reinstallations, the sum of the individual items is now equivalent to the total shown at the top of the pop-up dialog. ○ The values for **Total Devices Repaired** and **Total Devices Reinstalled** are now based on the last 30 days, as expected. ● Previously, if a device was offline during a Microsoft SCCM status check, a status of Not Compliant, which is incorrect, may have been displayed in Application Persistence reports and widgets. In addition, the report's Status Details column erroneously indicated that the Not Compliant status was the result of an unsigned `ctccmdetect.exe` file. This issue is now fixed.

Feature/Area	Improvements and fixes
Device Freeze	● If a user is logged in when a Device Freeze request is deployed to a Windows device, the user is now immediately logged out of their current session and the Freeze message is displayed. A device reboot is no longer required to freeze a Windows device. As a result of this change, the following setting no longer shows on the Freeze dialog: **Force reboot before freezing device (Windows Devices Only)** ● In the Event History report, a status of Freeze Armed no longer shows for On-demand Freeze requests.
Device Groups	● On a device's Device Groups page, you can now click a device group name to navigate to the device group and view its list of devices or edit the group. ● In the Device Management > Device Groups area, you can now select devices in a Smart Device Group, Static Device Group, or Roll-Up Folder and perform a device action, such as Run Script or Unenroll Device. In addition, the "Select All" checkbox is now available in the results grid header of a Smart Device Group or Roll-Up Folder. ● On the View and Edit Device Fields page in Administration > Data area, you can now select a Static Device Group when you click **Actions** > **Choose device group**. ● If you delete a device group that is being used to filter a report, the device group name now shows in red text with a strikethrough (for example, ~~device group 1~~) in the report's filter area.
Endpoint Data Discovery (EDD)	● The Encryption > Status column is now included by default in the following reports: ○ History ○ Reporting Data ○ Devices with At-Risk Files in Cloud You can also filter these reports by the devices' Full-Disk Encryption Status. ● The maximum number of custom EDD rules that you can create within your account has increased from 20 to 50 rules. ● Disabled devices no longer show in EDD reports. ● When you activate an EDD policy that includes the Personal Health Information policy rule, file content is now scanned for Medicare Beneficiary Identifiers (MBI) in addition to Social Security Numbers (SSN). You can also use the following operator in a custom rule to find MBIs in your devices' files: ○ @US_MBI For more information about using this operator, see *Expression syntax guidelines* in the online Help. ● You can now use the following operators in custom EDD rule expressions to find numeric dates, in supported date formats, in your devices' files: ○ @Date_Any_Numeric (<locale parameter>) ○ @Date_Any_Numeric (all) ○ @Date_Specific_Numeric (<locale parameter>; YYYY: MM; DD) For more information about using these operators, see *Expression syntax guidelines* in the online Help. ● When you view a file from a device's Endpoint Data Discovery Summary page, the name of the matched expression set now shows in the Details column instead of a system generated identifier.

Feature/Area	Improvements and fixes
Endpoint Data Discovery (EDD) continued	● Error messaging is now improved when you create a custom EDD rule that contains invalid content. ● When you rename a policy group, the new name now shows immediately in the Policy Group column in EDD reports. ● When you protect a .pdf file from the Absolute console using Azure Information Protection (AIP) and then immediately remove AIP protection from the file, its AIP Status now updates to Remove Protection Pending on the device's Endpoint Data Discovery Summary page. ● A warning now shows on the Endpoint Data Discovery Summary page if a device's EDD policy configuration has changed, but the information on the page is unchanged because a new EDD scan hasn't completed yet.
Full-Disk Encryption Status	● If your devices use TrueCrypt for file encryption and one of the following applications for full disk encryption, the devices' encryption status is now reportedly correctly in the Full-Disk Encryption Status report. ○ Dell Encryption ○ Microsoft BitLocker Drive Encryption ● For devices with Trend Micro Encryption Management for Microsoft BitLocker, encryption status is now reported correctly in the Full-Disk Encryption Status report.
Navigation	● The sidebar is now divided into two sections: **Default** and **Custom**. This change affects the following areas in the console: ○ Find Devices ○ Applications > Reports ○ Data Protection > Endpoint Data Discovery For example, in the Find Devices area, all default reports now show on the sidebar under Default, in alphabetical order. Any reports that you save as a custom report show under Custom, in alphabetical order. ● In the Administration > Script Library area, the sidebar is now divided into **Absolute** and **Custom** sections. All scripts authored by Absolute now show on the sidebar under Absolute, in alphabetical order. Any scripts that you've uploaded show under Custom, in alphabetical order.
Policy Groups	● When you view a policy group, you no longer need to scroll to the end of the device list to prompt the "Select All" checkbox in the results grid header to be enabled. ● When you remove tens of thousands of devices from a policy group using the "Select All" checkbox, the system no longer times out before the process completes.

Feature/Area	Improvements and fixes
Script Library	● The following Absolute scripts, which you can run on your Windows devices, are now available in the Script Library in the Administration area: ○ Add Firewall Port Rule ○ Change OS Licensing from MAK to KMS ○ Clear SCCM Cache ○ Enable or Disable User Account on Computer ○ Enables or Disables USB Removable Media ○ Force SCCM Check-in ○ Force System Center Endpoint Protection / Windows Defender Checkin ○ Mute Computer ○ Share a Windows Folder ○ Start Processes with Optional Arguments ○ Start / Stop / Restart Windows Service ○ Start Windows application

Contacting Technical Support

If you have difficulty using the Absolute console or any of its components, contact Absolute Technical Support. We welcome your questions, comments, and feature requests. Visit us at www.absolute.com/en/support and follow the instructions on the page to contact Technical Support in your region.

Copyright Information

Absolute 7.4 Release Notes—Documentation Release 2