June 2017

Absolute DDS 6.4 Release Notes

Release 6.4 of Absolute Data & Device Security (DDS) is an incremental feature release that builds on Release 6.3 and offers new features and enhancements.

DDS 6 features and enhancements

DDS 6 introduces the following features and enhancements:

NOTE Depending on the Absolute products associated with your account, some of the following features and feature enhancements may not be available to you.

- ***Language support***: The DDS 6 user interface is now available in the following languages, in addition to English:

  - French
  - German
  - Italian
  - Japanese
  - Korean
  - Portuguese
  - Spanish
  - Simplified Chinese
  - Traditional Chinese
  - Turkish

  The DDS 6 Help is also available in these languages.

  You can set your language preference for the DDS console in your User Profile, if you have not already done so. For more information, see "Editing your User System Settings" in the *DDS 5 User Guide*.

- ***Enhanced support for Android devices***:
  - The Device Details: Hardware pages for Android devices are updated. For example, the following pages, which do not apply to the Android platform, are no longer visible:
    - CD-ROM
    - Sound Device
    - Input
    - Storage
    - Printing
    - USB

    In addition, some pages, sections, and data points are relabeled to more accurately reflect Android hardware terminology.

    For more information, see *Viewing a device's hardware information* in the DDS 6 Help.
  - An Android device's IMEI now shows next to the Identifier in the header of all Device Details pages.
  - Software policies now support Android devices. You can view information about the software installed on your Android devices in the following reports and pages:
    - Software Overview report
    - Software Reporting Data report
    - Device Details: Software page

- ○ A new predefined report, **Android Vulnerability**, is now available in the Reports area. This report shows a vulnerability rating for each active Android device in your account. The rating is based on enhanced hardware information collected from Android devices. You can also view details about specific vulnerabilities detected on a device on its Android Vulnerability page in Device Details.

  For more information, see *Android Vulnerability report* and *Viewing vulnerability details for a device* in the DDS 6 Help.

  NOTE To view information in the Android Vulnerability report, your Android devices need to be running version 3232 of the Absolute agent for Android. You can find your devices' agent version on the Asset Report in DDS 5.
  To upgrade the agent on your Android devices, contact Absolute Global Support at www.absolute.com/support.

- ***Endpoint Data Discovery enhancements***:
  - ○ Administrators can now select one or more devices and request a one-time, immediate EDD scan for at-risk file content. For example, you may want to run an EDD scan to verify that the user of a device has "cleaned up" the at-risk files that were reported during a prior EDD scan.

    The **Perform EDD Scan** option is available from the following reports and pages:

    - – Active Devices report
    - – Devices with Active Policies
    - – Endpoint Data Discovery Match Score Summary
    - – A customized report based on one of the above listed predefined reports
    - – Devices page within a device policy

    After the request is submitted, the EDD scan runs on each device on the next agent connection.

    For more information, see *Scanning a device for at-risk file content* in the DDS 6 Help.

  - ○ If your organization uses one of the following Microsoft® Azure Information Protection (AIP) products to create and manage rights-protected content, you can now apply protection to at-risk files directly from the Absolute DDS console:

    - – Azure Information Protection
    - – Active Directory Rights Management Services

    When this feature is enabled in an EDD policy, Administrators can select individual files on a device's Endpoint Data Discovery Summary page and submit a request to apply one of your organization's pre-configured AIP policy templates to the files on the device. In this way, files that contain at-risk content can be protected should the files be distributed outside your organization or to unauthorized users.

    NOTE Before you can protect files in Absolute DDS, you need to ensure that your organization's deployment of Microsoft AIP meets the prerequisites for this feature.

    For more information about prerequisites, and how to assign AIP policy templates to files from the DDS console, see *Protecting at-risk files using Azure Information Protection* in the DDS 6 Help.

- ***Report and Repair policy enhancement***:

The Report and Repair policy in the Device Policies area is enhanced. You can now configure the policy to collect information about the functional status of the following third party applications installed on your devices:

- WinMagic SecureDoc
- Ivanti (LANDesk) Management Suite

Depending on the Absolute products associated with your account, the agent may also be able to attempt to repair these applications if they are non-functional.

You can view the information collected by each application's Report and Repair policy by adding columns to the Active Devices report or the Devices with Active Policies report to create a customized Report and Repair report.

For more information, see *Getting started with Report and Repair policies* and *Creating a Report and Repair status report* in the DDS 6 Help.

- ***Contacting Global Support***: the Support page that is available in DDS 5 is now available in DDS 6. On the navigation pane, click the **Support** link under DDS 6 to open a page containing links to Global Support.
- ***Learning Hub***: a new training portal is now available. To open the Learning Hub, click the **Training** link on the navigation pane under DDS 6. From this page you can view videos and interactions about using the following features in DDS 6:
    - Reports
    - Device Groups
    - Device Policies
    - Endpoint Data Discovery

DDS 6 improvements and fixes

DDS 6 introduces the following improvements and fixes to existing features:

NOTE Depending on the Absolute products associated with your account, some of the following feature enhancements may not be available to you.

- ***Data collection improvements***:
    - When a device's hardware, software, or full-disk encryption information changes, those changes are now consistently reflected in the Absolute DDS console after the device's next agent connection.
    - For Windows devices, the SDC (software data collection) component of the Absolute DDS agent no longer crashes unexpectedly, generating a Windows Application Error that is visible to the device user.
    - If Microsoft Office 2013 or Microsoft Office 2016 is installed on a Windows device, the application is now reported in the Software Licenses for Windows devices report.
- ***Device group improvements***:
    - In the Edit Filter dialog for a smart device group, the **Device Name equal to** filter is no longer case sensitive. As a result, the group's device list is now generated correctly, regardless of the case used to enter a device's Device Name.
    - The Local IP Address for a Chromebook is now detected successfully at each agent connection. As a result, Chromebooks no longer become disassociated from smart device groups that are based on an IP range filter.

    - From the Device Groups page, you can now delete two device groups in succession without receiving a "Resource not found" error message when you try to delete the second device group.

- ***Endpoint Data Discovery improvement***: When a device user deletes a file that was detected during an EDD scan, the device's EDD Match Score is now always updated to reflect that the file is removed.
- ***Report and Repair: BitLocker policy fixes***:
    - When a status of *Not compliant* is reported for a device, the **Status Details** report column now always contains details about each BitLocker component that is non-compliant.
    - The **Last Status Check (UTC)** report column now always shows the date and time when a device's BitLocker status was last verified, regardless of whether the status changed or not.
- ***General improvements and fixes***: This release also introduces numerous performance, security, and usability improvements that enhance the responsiveness, reliability, and ease of use of the system.

DDS 5 improvements and fixes

DDS 5 introduces the following improvements and fixes to existing features:

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

- ***User interface improvements and fixes***:
    - Longer Device Names are no longer truncated to 14 characters on the Create and View Agent Removal Requests page in **Administration** > **Account**.
    - After you upload a list of devices to a device group, the **Request Code** button is no longer grayed out when you navigate to either of the following pages to perform a security action:
        - Request Data Delete page
        - Request Device Freeze page
    - On the Activation Report page, the text that inaccurately states that data is stored for only one year is now removed.
- ***Security Posture Report improvement***: If WinMagic SecureDoc™ is installed on your devices, the Encryption Health page of the Security Posture Report now shows information for this application.
- ***Chromebook support***:
    - On the Select Organizational Units dialog in Account Settings, you can now select sub organizational units.
    - If you remove the Google account from the Account Settings page in the DDS console, the associated Chromebooks now remain Active and continue to connect to the Absolute Monitoring Center.

    NOTE If you want to disable these devices in Absolute DDS, submit an Agent Removal request and then use the Google Admin console to remove the Chromebook extension from each device. For more information, see the *Absolute for Chromebooks Extension Install Guide*.

- ***Feature support***: If the Absolute MTM Premium for Chromebooks (MTMPRMCHR) product is associated with your account, the following features are now available, as expected:
  - Software Assets reports
  - Alerts
- ***Device Freeze improvements***:
  - When you include an image in a Device Freeze message, the URL in the <img src> HTML tag needs to be surrounded by quotation marks. If you omit the quotation marks or use them incorrectly, the system now corrects these errors allowing the device to be frozen as expected.
  - Using an Unfreeze request to unfreeze an Android device no longer clears the device's screen lock PIN (or password) leaving the device unlocked.

    NOTE For an Android device with no PIN or password set, the device's PIN is now automatically set to 1234 when the device is frozen. After the device is unfrozen, the user is notified that they need to enter `1234` to unlock the device. They can then go to Settings to remove or reset the PIN.

Contacting Global Support

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

Copyright Information

Absolute DDS 6.4 Release Notes—Documentation Release 3

©2017 Absolute Software Corporation. All rights reserved. Absolute, Computrace, and Persistence are registered trademarks of Absolute Software Corporation. LoJack is a registered trademark of LoJack Corporation, used under license by Absolute Software Corporation. LoJack Corporation is not responsible for any content herein. All other trademarks are property of their respective owners.

For a list of patents issued to Absolute Software Corporation, see www.absolute.com/patents.