March 2017

Absolute DDS 6.3 Release Notes

Release 6.3 of Absolute Data & Device Security (DDS) is an incremental feature release that builds on Release 6.2 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.

- ***Chromebook support***:
  - The Hardware policy now collects enhanced hardware information from Chromebook devices. You can view this information in the Active Devices report, the Devices with Active Policies report, and the Device Details: Hardware page of a Chromebook device.
  - The Device Usage policy now supports Chromebooks, meaning you can view device usage information for these devices in the Device Analytics report.
- ***Mac support***: The Device Usage policy now supports Mac devices, meaning you can view device usage information for these devices in the Device Analytics report.
- ***Device Policies***: A new device policy, **Report and Repair**, is now available in the Device Policies area. Administrators can configure and activate this policy to collect information about the functional status and compliance of Microsoft BitLocker® Drive Encryption on your devices. Depending on the Absolute products associated with your account, the DDS agent may also be able to repair BitLocker if it is non-functional or non-compliant.

  You can view the collected BitLocker status information 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.
- ***Endpoint Data Discovery reporting***: A new predefined report, **Data Risk Assessment**, is now available in the Reports area. You can use this report to view the calculated level of risk, or Risk Score, associated with the file content detected during an Endpoint Data Discovery scan. File content will have an elevated Risk Score if it was found in a cloud storage folder and therefore may be at risk of being shared in the cloud.

  NOTE With the release of DDS 6.3, a device's Risk Score will show in the Data Risk Assessment report as zero (0) until the actual Risk Score can be calculated by a full EDD scan.
  Since a device's next full EDD scan may not occur for another three months, Absolute is releasing a service pack on March 3, 2017 to update any Risk Scores that have not been recalculated by a full EDD scan.

  This report also shows each device's Estimated Cost Exposure, which is the estimated cost to your organization should a data breach occur on the device.

  For more information, see *Data Risk Assessment report* in the DDS 6 Help.
- ***Dashboard enhancements***: Two new widgets, which provide summarized Endpoint Data Discovery information, are now available on the Dashboard:

- **Risk Exposure**: This widget is based on the new Data Risk Assessment report. It shows the average Risk Score and the total Estimated Cost Exposure across all devices in your account. The five devices with the highest Risk Scores are also shown.

  NOTE With the release of DDS 6.3, the widget's average Risk Score and each device's individual Risk Score is set to zero (0) until actual Risk Scores can be calculated by a full EDD scan.
  Since a device's next full EDD scan may not occur for another three months, Absolute is releasing a service pack on March 3, 2017 to update any Risk Scores that have not been recalculated by a full EDD scan.

- **Endpoint Data Discovery Match Scores**: This widget is based on the Endpoint Data Discovery Match Score Summary report and shows the policy groups with the highest total Match Scores.

For more information about these new widgets, see *Dashboard* in the DDS 6 Help.

- ***Device Analytics report enhancements***:
  - You can now view device usage information for Mac and Chromebook devices in this report.
  - Device group information is now available in the report's results grid. Click a link in the **Device Group** column to see the list of device groups that a device belongs to.
  - A new Event Type, **Keyboard and Mouse Activity**, is now available when you create the report's Series. Select this event type if you want to see the total amount of keyboard and mouse activity per device group.
  - A new filter, **Event Time**, is now available when you create the report's Series. Use this filter to show only those device usage events that occurred on specific days of the week and hours of the day during the report's defined date range.
  - Two new columns, **Login and Unlock Event Count** and **Keyboard and Mouse Activity (dd:hh:mm)**, are now available in the report's results grid.
  - The bar chart now has two new display options in addition to Device Count:
    - The Keyboard and Mouse Activity option shows the total number of minutes, hours, or days of keyboard and mouse activity, per device group, during the date range
    - The Login and Unlock Events option shows the total number of device login and unlock events, per device group, during the date range

  For more information about these enhancements, see *Device Analytics report* and *Working with customized Device Analytics reports* in the DDS 6 Help.

- ***Device Freeze enhancements***:
  - The Device Freeze wizard now includes an enhanced HTML editor for creating Device Freeze messages. Security Administrators and Security Power Users can use the tools in the new editor to format message text, add font and background colors, and insert images.

    For more information about the new editor, see step 3 of *Freezing devices* in the DDS 6 Help.

    NOTE The following features, which are available in DDS 5, are currently not supported in DDS 6:
    - Scheduled Device Freeze
    - Custom Action Fields
    - Device Freeze Offline Policies

- Security Administrators and Security Power Users can now cancel Device Freeze requests, and unfreeze one or more frozen devices, from the following reports:
  - Active Devices
  - Devices with Active Policies
  - Endpoint Data Discovery Match Score Summary
  - A customized report based on one of the above listed predefined reports

  For more information, see *Cancelling Device Freeze requests* and *Unfreezing frozen devices* in the DDS 6 Help.

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.

- ***Report improvements and fixes***:
  - For all reports, the Show Filter button has been removed and each report's current filters are now visible by default under the report title. To edit a report's filters, click the new icon next to the filters.
  - In the Software Licenses on Windows Devices report, license names for Microsoft Visio and Microsoft Project now include the version, such as:
    - Microsoft Visio Professional 2013
    - Microsoft Project Standard 2010
  - When you add a filter to a Device Analytics report, the list of filter criteria in the Data field no longer extends beyond the bottom of the screen obscuring part of the list.
  - Devices no longer show in the Anti-Malware report or dashboard widget if the DDS agent could not detect the name of the anti-malware application installed on the device.
- ***Custom Field improvement***: When you update a value in a Custom Device Field in DDS 5, the update is now synced as expected with the corresponding Custom Field in DDS 6.
- ***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.

- ***Device Freeze improvements***:
  - To improve support for Android devices, a new field, **Select code length**, is now available in the Select a Passcode Option area of the Request Device Freeze page. Security Administrators and Security Power Users can use this field to specify the length of the passcode. Options are **4 digits**, which is the recommended option for Android devices, and **8 digits**.

- A new filter, **Requested Date**, is now available in the Search Criteria area of the Device Freeze Summary Report. This filter includes options to let Security Administrators and Security Power Users filter the results based on the date the Device Freeze was requested.
- To improve support for Android devices, Security Administrators and Security Power Users can now use Subscriber ID or Phone Number to search for devices when they submit a Device Freeze request.

For more information about these improvements, see "Requesting a Device Freeze" in the *Absolute DDS 5 User Guide*.

- ***Report improvements***:
  - To improve support for Android devices, the following information is now available in the Call History Report, the Suspicious Devices report, and the Activation Report:
    - IMEI
    - Subscriber ID
    - Phone Number

    You can also use these criteria to filter the Call History Report and the Activation Report.
  - You can now filter the Software By Device Report based on IMEI.
  - A new filter option, **at any time**, is now available in the Search Criteria area of the SCCM Status Report. Select this option if you *don't* want to filter the report based on the devices' last call.

  For more information about these improvements see the applicable section in the *Absolute DDS 5 User Guide*.
- ***User Profile improvements***: You can now add primary and secondary contact phone numbers to your user profile. In addition, Administrators are now required to add primary contact information when they create or edit a user.

  For more information, see "Editing Your User Details" and "Creating New Users" in the *Absolute DDS 5 User Guide*.

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 6.3 Release Notes—Documentation Release 3