Absolute DDS 6.1 Release Notes

Release 6.1 of Absolute Data & Device Security (DDS) is an incremental feature release that builds on Release 6.0 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.

- ***Reports***: The following predefined reports are now available in the Reports area:
  - ***Device Analytics***: Use this report to compare device membership across selected Device Groups and Roll-Up Folders.

    The report consists of two components: a bar chart and a results grid. You can add bars to the bar chart to visually compare the number of devices in two or more device groups or folders. The list of devices that are members of the selected groups and folders show in the results grid.

    For more information about creating this report, see *Device Analytics report* in the DDS 6 Help.
  - ***Devices with At-Risk Files in Cloud***: Use this report to view information about file content, detected by the Endpoint Data Discovery policy, that may be at risk of being shared using a cloud storage service. The report uses a simple set of filters to show detected EDD data that resides in a folder typically created by one of the following cloud storage applications:
    - iCloud Drive®
    - Box Sync®
    - Dropbox
    - Microsoft OneDrive®

    For more information about this report, see *Devices with At-Risk Files in Cloud report* in the DDS 6 Help.
  - ***Devices with Cloud Storage Software***: Use this report to view your Windows and Mac devices with one or more of the following cloud storage applications installed:
    - iCloud Drive
    - Box Sync
    - Dropbox
    - Microsoft OneDrive
    - Google Drive™ online storage service

    For more information about this report, see *Devices with Cloud Storage Software report* in the DDS 6 Help.
- ***Encryption Status reporting***: A new device policy, Full-Disk Encryption Status, is now available. You can activate the policy to enable the Absolute DDS agent to collect encryption status information from your Windows devices. You can view the collected information by adding **Encryption** columns to the Active Devices report or the Devices with Active Policies report. You can then save your changes to create a customized report.

For more information about activating the Full-Disk Encryption Status policy, see *Activating device policies* in the DDS 6 Help. For more information about creating a customized Full-Disk Encryption Status report, see *Types of customized reports* in the DDS 6 Help.

- ***Anti-Malware reporting***: The Absolute DDS agent now detects information about the anti-malware software installed on your Windows devices. You can view the detected information by adding **Anti-Malware** columns to the Active Devices report or the Devices with Active Policies report. You can then save your changes to create a customized report.

  For more information about creating a customized Anti-Malware report, see *Types of customized reports* in the DDS 6 Help.

- ***Freezing devices from a report***: You can now select multiple devices from any of the following reports and submit a single Device Freeze request in DDS 5 to freeze the devices:
  - Active Devices report
  - Devices with Active Policies report
  - Endpoint Data Discovery Match Score Summary report
  - a customized report based on any of the above listed predefined reports

  For more information, see *Freezing devices* in the DDS 6 Help.

- ***Policy status reporting***: Policy status columns are now available on the Active Devices report and the Device with Active Policies report. The columns contain status icons that let you view, at a glance, the status of the Hardware, Software, and Endpoint Data Discovery policies on your devices.

  The new status icons are also included on each device's Policy tab.

  For more information about the different policy status icons and their definitions, see *Active Devices report* in the DDS 6 Help.

- ***IP Address reporting***: A device's last detected **Local IP Address** and **Public IP Address** are now available in the System Information section of the device's Device Details tab. For more information, see *Viewing device details* in the DDS 6 Help.

  In Reports, you can now add **Local IP Address** and **Public IP Address** columns to the Active Devices report and the Device with Active Policies report. You can also use these data points to filter the reports.

  For more information about working with these reports, see *Active Devices report* and *Devices with Active Policies report* in the DDS 6 Help.

- ***Endpoint Data Discovery report enhancement***: You can now add the **File Path** column to the Endpoint Data Discovery History report and the Endpoint Data Discovery Reporting Data report. Use **Show/Hide Columns** to add this column to the report. You can then filter the data in these reports by file path.

  For more information about adding columns to a report, see *Managing report columns* in the DDS 6 Help.

- ***Endpoint Data Discovery Match Score Summary report enhancement***: You can now add the following columns to the Endpoint Data Discovery Match Score Summary report:
  - Make
  - Model
  - Device Name
  - Serial Number
  - Username

Use **Show/Hide Columns** to add these columns to the report. You can then use these data points to filter the report.

For more information about adding columns to a report, see *Managing report columns* in the DDS 6 Help.

- ***Endpoint Data Discovery scan improvements***:
  - EDD scans will no longer falsely detect matches to the Credit Card rule in files with the `.obj` or `.dae` file extension. These files are typically used by 3D graphics programs.
  - The EDD policy will no longer attempt to scan the following files on devices with PGP Desktop Encryption installed:
    - C:\PGPWDE01
    - C:\PGPWDE02

    These files are unscannable.
- ***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 feature enhancements may not be available to you.

- ***Absolute Customer Service Account Access***: A new setting, Absolute Customer Service Account Access, is now available on the Account Settings page. An Administrator can enable this setting to let Absolute customer service staff log in to the account to troubleshoot issues and provide technical support. Note that logged-in Absolute customer service staff can't perform security actions, such as Data Delete.

  For more information about configuring this new setting, see "Editing Account Settings" in the *Absolute DDS 5 User Guide*.

  NOTE After you enable this setting, all login and logout events performed by Absolute customer service staff are logged to the User Event Report. For more information, see "User Event Report" in the *Absolute DDS 5 User Guide*.

- ***Integration with Splunk***: Absolute DDS now supports direct integration with Splunk Enterprise and Splunk Cloud through the Absolute SIEM Connector.

  This integration includes the Absolute Data & Device Security (DDS) App for Splunk, which you download from the Splunk Store and install. The app includes a custom report and four dashboards to help you view and analyze the alerts generated in Absolute DDS.

  You can also submit an Absolute DDS Device Freeze request directly from Splunk to freeze an at-risk device.

  For more information about the Absolute SIEM Connector and Splunk integration, see the *Absolute SIEM Connector Install Guide*.

- ***Device Freeze enhancement for Android devices***: You can now include a contact phone number in a custom Device Freeze message, which allows the user of a frozen Android device to tap the hyperlinked phone number and place a call. This feature is intended to allow users to use their frozen Android device to call for assistance, even though their device is otherwise unusable.

  For more information, see "Including Phone Numbers in Custom Device Freeze Messages" in the *Absolute DDS 5 User Guide*.

- ***Full-Disk Encryption Status Report improvements***:
  - A new column, **Detected Date**, is now available on the Full-Disk Encryption Status report. The column shows the date and time when the encryption information was detected on the device.
  - The value in the **Algorithm** column now shows the correct key size; the two digits that were appended to the value are removed.
- ***Support for Self Healing Call Alert on Android devices***: The predefined alert, **Self Healing Call**, is now triggered when the Absolute DDS agent on an Android device is tampered with or removed.

  For more information, see "About Predefined Alerts" in the *Absolute DDS 5 User Guide*.

- ***Security Posture Report improvements***:
  - In the DDS console, when you click **Close** on the Data export in progress dialog, your exported report is now saved to My Reports, as expected.
  - In the Security Posture Report Template, when you edit the value for **Months since last agent call to be considered too old** on the Variables and Lookups page, and then refresh the report, the data on the report's Summary page is now accurate.
- ***Report improvement***: The Anti-Malware Report now shows the same device count as the Installed Programs by Account Report, for a given anti-malware software application.
- ***Default User Language and Locale***: The default language that you select in your User Profile is now applied consistently to all pages in the DDS console. Specifically, all items in drop-down fields are now shown in the correct language.

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 6.1 Release Notes—Documentation Release 1