Absolute DDS 6.2 Release Notes

Release 6.2 of Absolute Data & Device Security (DDS) is an incremental feature release that builds on Release 6.1 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.

- ***Dashboard***: A new "Dashboard" link is added to the DDS 6 navigation pane.
  Click this link to see a collection of widgets that provide an overview of the reports and metrics you care about most.

  The Dashboard includes an overview widget and one or more of the following widgets:

  - Anti-Malware
  - Full-Disk Encryption
  - SCCM

  NOTE Depending on the Absolute products associated with your account, the Dashboard, or some of its widgets may not be available.

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

- ***Device Policies***: Two new policies are now available in the Device Policies area:
  - **Device Usage**: Activate this policy to begin collecting data about the usage of your Windows devices. Device usage is based on user events, which occur when a user logs in to or unlocks a device. The policy also collects the number of minutes a device is in use per day. You can analyze the collected data by generating a Device Analytics report or viewing a device's Usage Event Details page.

    For more information about the Device Usage policy, see *Getting started with Device Usage policies* in the DDS 6 Help.

  - **SCCM Status**: If you use System Center Configuration Manager (SCCM) to manage your Windows devices, activate this policy to collect status information about the SCCM clients installed on your Windows devices. You can view the collected information in the new SCCM Status report in DDS 6.

    For more information about this policy, see *Getting started with SCCM Status policies* in the DDS 6 Help.

- ***Device Analytics report*** : The Device Analytics report is enhanced. After you activate the new Device Usage policy, you can now use this report to see the Windows devices in your account that were in use during a particular time period. You can also compare device usage across your device groups.

  For more information about this report, see *Device Analytics report* in the DDS 6 Help.

- ***Usage Event Details***: A new page, Usage Event Details, is added to a Windows device's Device Details. Open this page to view details about the individual user events collected from a device by the Device Usage policy.

For more information about the Usage Event Details page, see *Viewing a device's usage* in the DDS 6 Help.

- ***Predefined reports***: The following predefined reports are now available in the Reports area:
  - **Anti-Malware**: Use this report to view information about the anti-malware applications installed and detected on your Windows and Mac devices.

    For more information about viewing this report, see *Anti-Malware report* in the DDS 6 Help.
  - **Full-Disk Encryption Status**: After you activate the Full-Disk Encryption Status policy, use this report to view information about the full-disk encryption products detected on your Windows and Mac devices. The report also shows the encryption status of each device's system drive.

    For more information about this report, see *Full-Disk Encryption Status report* in the DDS 6 Help.
  - **SCCM Status**: After you activate the new SCCM Status policy, use this report to view information about the status of each SCCM client installed on your Windows devices.

    For more information about this report, see *SCCM Status report* in the DDS 6 Help.
- ***Mac Support***:
  - The Mac version of the Absolute DDS agent is now supported on devices running Mac OS X version 10.12.
  - The Mac version of the Absolute DDS agent now detects anti-malware applications installed on Mac devices. You can view this information in the new Anti-Malware report. The agent also detects full-disk encryption products installed on Mac devices, and detects if the device's system drive is encrypted. You can view this information in the new Full-Disk Encryption Status report.
- ***Device Freeze***:
  - Depending on the configuration of your account, a new Device Freeze wizard may be available in DDS 6.

    The wizard simplifies the Device Freeze workflow by walking you through the steps to submit a request. In addition, you can now:

    – Specify the character length of the Unfreeze code associated with the request. Values between 4 (recommended for Android devices) and 8 digits are supported.
    – Create a new freeze message while you're submitting your request and save the message for future use.

    If you are logged in to DDS 6 as a Security Administrator or Security Power User, and your account includes the required configuration, you can access the Device Freeze wizard from a device's Device Details page or from one of the following reports:

    – Active Devices report
    – Devices with Active Policies report
    – Endpoint Data Discovery Match Score Summary report
    – A customized report based on one of the above listed predefined reports
  - Two new options are now available in the Device Options menu on the Device Details page:
    – **Cancel Freeze Request**
    – **Unfreeze Device**

If you are logged in to DDS 6 as a Security Administrator or Security Power User, you can now cancel a Device Freeze request directly from a device's Device Details page. Alternatively, if the device is already frozen, you can unfreeze it.

For more information about these tasks, see *Canceling a Device Freeze request* and *Unfreezing a frozen device* in the DDS 6 Help.

- ***Remediation of At-Risk Files using Data Delete***: The Data Delete feature in DDS 6 is enhanced. For *Windows* devices, you can now select individual at-risk files on either of the pages and submit a Data Delete request:
  - Device Details > Endpoint Data Discovery Summary
  - Device Details > Endpoint Data Discovery History

  For more information, see *Deleting data from a device* in the DDS 6 Help.
- ***Endpoint Data Discovery Rules***:
  - **Expressions**: EDD rule expressions now support two new operators for masking confidential content:
    - @Mask_After
    - @Mask_Upto

    The following operators, which are used to validate account numbers or identifiers, are also supported:

    - @Luhn
    - @NHSNumber
    - @JPIDNumber

    For more information about the new operators, see *Expression syntax guidelines* in the DDS 6 Help.
  - **Templates**:The following expression set templates are now available in Endpoint Data Discovery (EDD) Rules:
    - Credit Card
    - UK National Health Service
    - UK National Insurance Number
    - Japanese My Number

    The templates use the new @Mask_After operator to mask confidential content. You can use these templates to build custom EDD rules to scan your devices for confidential or at-risk data.

    For more information about the new templates, see *Getting started with customized EDD rules* in the DDS 6 Help.
- ***IP range filtering***: Filters for reports, device groups, and policy groups are updated. The **between** filter condition is now available when you filter by Local IP Address or Public IP Address, so you can filter devices by IP range.

  For more information filtering in DDS 6, see *Working with filters* in the DDS 6 Help.

  NOTE IP range filtering is not supported in the Device Analytics report. Also, the **contains** and **not contains** filter conditions are no longer available when you filter by IP Address.

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.

- ***Endpoint Data Discovery (EDD) improvements and fixes***:
  - When you export an Endpoint Data Discovery Match Score Summary report, the column headers for any customized EDD rules now show the correct rule name.
  - You now see an error message if you attempt to publish a customized EDD rule that does not contain any expressions sets.
  - You can now filter the following reports by customized EDD rule name:
    - Endpoint Data Discovery History report
    - Endpoint Data Discovery Reporting Data report
  - Characters with diacritical marks, such as those used in the Latin character set (á, è, ç, etc.), are now supported in EDD Rules. That is, when you enter sample text to test a rule that contains expressions with Latin characters, matches are found as expected.
- ***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.

- ***Contacting Global Support***: Absolute Global Support is now using a new customer relationship management (CRM) platform to manage customer submitted Support cases. As a result, you'll see a new interface when you click **Support** on the DDS console navigation pane and click **Submit a Support Case**. You'll also use the new My Cases page to view and update your existing cases.

  NOTE The My Cases page shows only the Support cases that you've submitted. You can no longer view Support cases submitted by other users in your account.

  For more information about submitting and updating a Support case, see "Contacting Absolute Global Support" in the *Absolute DDS 5 User Guide*.
- ***Device Freeze improvement***: A new section, **Schedule Freeze Date**, is now available on the Request Device Freeze page. This section lets Security Administrators and Security Power Users specify whether a Device Freeze occurs on the next agent call or on a future date (within one year of the current date).

  For requests that are scheduled to occur in the future, there are three new Device Freeze statuses:
  - **Scheduled Freeze Pending**

    The submitted Device Freeze request is scheduled to occur on or after a future date. When the scheduled date is reached, the status changes to Freeze Scheduled.

- **Freeze Scheduled**

  The current date equals or exceeds the date on which the device is scheduled to be frozen. After the device makes a successful call to the Monitoring Center, the device is frozen.

- **Frozen by Scheduled Freeze**

  The device was frozen by a Device Freeze request that was scheduled to occur on or after a specified date.

These statuses show on the Device Freeze Summary Report. They also show on the Device Freeze Details page for a scheduled Device Freeze request.

For more information about creating and viewing scheduled Device Freeze requests, see "Requesting a Device Freeze" and "Tracking Device Freeze Status" in the *Absolute DDS 5 User Guide*.

- ***Password Policy Settings***: A new section, Password Policy Settings, is now available on the Account Settings page. An Administrator can configure this section's settings for all users within the account to enforce password complexity requirements, such as minimum length, character mix, and expiration.

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

  NOTE Password requirements are now set at the account level. As a result, the following password settings are no longer available on the Create and Edit User page:
  - **User must change password every <#> days**
  - **Require strong password**

- ***Android device support***:
  - When you are submitting a Device Freeze request, you can now use **IMEI** to filter the list of devices on the Select devices dialog.
  - The following device information is now available on the Create and View Agent Removal Requests page:
    - IMEI
    - Subscriber Id
    - Phone Number

    You can also now upload a file of device IMEIs for Agent Removal.
  - The following device information is now available on the Device Freeze Summary Report page and the Device Freeze Details page:
    - Subscriber Id
    - Phone Number
  - If a device is running Android operating system 5.*x* or higher, the device's passcode is now cleared when you use an Unfreeze request to unfreeze the device, which leaves the device unlocked. If the device is encrypted, the encryption passcode is also cleared.

    NOTE This enhancement does not apply to Android devices without Absolute Persistence.

- ***Full-Disk Encryption Status Report***: The report now shows the correct encryption status when Microsoft Bitlocker is installed on a Window 10 device and the device's system drive is encrypted.

- ***RTT-IP status icons***: The icons that show a device's RTT-IP status are no longer available on the following pages in DDS 5:
  - Asset Report
  - Device Summary
  - Account Settings > Devices that have the RTT-IP feature turned on

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 6.2 Release Notes—Documentation Release 4