ABSOLUTE™

May 2018

Absolute 7.3 Release Notes

Absolute 7.3 is an incremental feature release that builds on Absolute 7.2 and offers new features, feature enhancements, improvements, and fixes.

Features and enhancements

Absolute 7.3 introduces the following new features and feature enhancements:

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

- ***Authentication enhancements***:
  - **Single Sign-On**: Absolute now supports single sign-on using any of the following third party SAML identity providers (IdP):
    - Azure Active Directory
    - ForgeRock®
    - Okta
    - OneLogin
    - PingFederate®
    - PingOne®

    To configure single sign-on, you need to add configurations to the new Account Settings > Single Sign-On area in the Absolute console. You also need to add Absolute to your chosen IdP as a new service provider. After single sign-on is enabled, users can enter their credentials on the IdP login page and then access the Absolute console without logging in again.

    For more information about configuring Single Sign-On in the Absolute console, see *Setting up Single Sign-On for your Absolute account* in the online Help.
  - **Two-Factor Authentication**: To enhance the security of your Absolute account, you can now enable Two-Factor Authentication (2FA) for all users. After 2FA is enabled, users need to enter a verification code along with their email address and password when they log in to the Absolute console. Verification codes are generated on the user's iOS or Android mobile device using the Google Authenticator app, which they can download from their respective app store.

    For more information about Absolute's Two-Factor Authentication solution, see *Enabling Two Factor Authentication for your account* in the online Help. For more information about configuring the Google Authenticator app so you can log in to the Absolute console, see *Setting up Two-Factor Authentication on your mobile device* in the online Help.
  - **Login page**: In support of the new Single Sign-On and Two-Factor Authentication features, the Login page has a new look and feel and the workflow is updated. To log in, you now enter only your email address before clicking **Next**. If you are using the Absolute IdP, the page refreshes to allow you to enter your password and a verification code (if 2FA is enabled). If you are using a third party IdP, you're redirected to the configured IdP login page to log in.
- ***License management***: A new default policy group, the **Unlicensed policy group**, is now available in the Policy Groups area. Devices in this policy group do not consume a base license, meaning that none of Absolute's licensed features are available to the policy group's devices.

The unlicensed policy group helps you manage your base licenses by acting as a staging area when licenses are unavailable. Devices are automatically added to this policy group when a base license expires, or when you add new devices to your account when no base licenses are available. After you renew or purchase licenses, the devices are automatically moved to their respective policy group.

You can also add devices to the unlicensed policy group manually. If you need to retire some devices, you can free up base licenses by moving the devices to the unlicensed policy group while you unenroll them from your account. Similarly, if a base licenses is oversubscribed, you can move devices to the unlicensed policy group while you purchase more licenses.

For more information about working with the unlicensed policy group, see *About the unlicensed policy group* in the online Help. We also recommend that you review *Best Practice for Maintaining License Compliance*, which you can access from *Supplemental and technical documents* in the online Help.

- ***Risk Analysis***: If your Absolute license includes the Investigations feature, you can now submit a Risk Analysis request to determine if the data on a lost or stolen device is at risk. From the submitted request, the new Absolute Risk Response Team prepares a Risk Analysis file, which includes a summary of the identified risks and a recommended course of action to secure the device. Note that it may take up to 72 hours to complete this process.

  When the Risk Analysis file is ready, a copy is emailed to you. You can also download a PDF of the Risk Analysis file from the Risk Analysis page in the Device Management > Investigations area.

  For more information, see *Requesting risk analysis for devices* and *Working with Risk Analysis requests* in the online Help, or review the training video in the Learning Hub.

- ***Endpoint Data Discovery***:
  - **EDD rules**: To support General Data Protection Regulation (GDPR) compliance for customers within the EU, new Personally Identifiable Information (PII) templates are available. In Data Protection > Endpoint Data Discovery > Rules, you can now use the following templates to build custom EDD rules:
    - Taxpayer ID Number (Germany)
    - Social Security Number (Germany)
    - Social Security Number (France)
    - Personal ID Number (Estonia)
    - Personal ID Number (Finland)
    - Personal ID Number (Norway)
    - Personal ID Number (Sweden)
    - Civil Registration System (Denmark)
    - DNI Number (Spain)
    - Tax Code ID (Italy)

    In addition, the following templates are enhanced:

    - National Health Service (UK)
    - National Insurance Number (UK)

    For more information, see *Getting started with rules* in the online Help.

  - **Scan Levels**: A new scan level is now available on the Configure EDD dialog. Select the **Extended** scan level option to scan virtually all Internet Media Types in *all* directories, with a few exceptions (some system directories are excluded). Note that Extended scans tend to take more time and resources to complete than the other options, and they may significantly increase the number of false positives.

    For more information, see *Overview of EDD configuration* in the online Help.

- ***User Awareness***:
  - **User Awareness policy**: A new policy is now available in the Policies and Alerts > Policies area. Activate the User Awareness policy on your Windows devices to collect user activity information, including login and logout events, application usage, Internet usage, and USB file transfer activity. You can view the collected information in the User Awareness area.

    For more information, see *Getting started with User Awareness policies* and *Configuring User Awareness policies* in the online Help.
  - **User Awareness Tech Preview**: After you enable the new User Awareness policy, you can preview the information collected from your Windows devices on the following new or updated pages in the User Awareness area:
    - **Dashboard**: review the User Risk widget and the User Endpoint Data Discovery Match Scores widget to see which users may pose a risk to your organization, based on their device activity
    - **Users**: view summarized activity information for a particular user, averaged over the past 30 days. The User's page has four subtabs: Devices Used, Applications, Internet activity, and Events.
    - **Applications**: view summarized application activity for all users in your account
    - **Events**: view user activity events that deviate from your users' normal activity levels

    For more information, see *Getting started with User Awareness* in the online Help, or review the training video in the Learning Hub.

- ***Application Persistence***:
  - The **Application version** field is now available in policy configurations for all third party applications. Use this field to specify which version of the application you expect to be running on your devices. If a different version is detected on a device, a status of Not Compliant shows in Application Persistence reports and widgets.
  - For the following third party applications, if you select the **Report, repair and reinstall** option, you can now configure a 32-bit installer *and* a 64-bit installer in the same policy group:
    - ESET® Endpoint Antivirus
    - Microsoft BitLocker® Drive Encryption
    - Pulse Connect Secure
    - WinMagic SecureDoc™

    When an application needs to be reinstalled on a device, the device automatically downloads the appropriate installer for its operating system.

- ***User Management***: To support features added in release 7.3, the following permissions are now available on the Permissions page in Roles:
  - **Authentication**: required to enable Two-Factor Authentication and Single Sign-On. By default, this permission is assigned to the System Administrator role only

- ○ **Risk Analysis**: required to submit a Risk Analysis request and view the risk Analysis page in the Investigations area. By default, this permission is assigned to all roles.
- ○ **Dashboard Security**: required to view the following Dashboard widgets:
  - – Device Activity
  - – Endpoint Data Discovery Match Scores
  - – User Endpoint Data Discovery Match Scores
  - – User Risk

  By default, this permission is assigned to all Administrator roles.
- ○ **Dashboard Inventory**: required to view all other widgets. By default, this permission is assigned to all roles.

> **NOTE** If you have created any custom roles, these permissions may need to be added to those roles. For more information, see *Default user roles and their permissions* and *Creating a custom role* in the online Help.

Improvements and fixes

Absolute 7.3 introduces numerous performance, security, and usability improvements that enhance the responsiveness, reliability, and ease of use of the system.

This release also 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.

Feature/Area	Improvements and fixes
Absolute agent	● When a new version of the Absolute agent for Android is released, but no Persistence technology exists on a device, the user is now prompted to accept the upgrade on the next connection to the Absolute Monitoring Center. Once it's accepted, all Absolute components on the device are upgraded. ● When you generate a Windows or Mac agent package for download, you can now refer to the Notifications indicator in the main toolbar to determine if the package is generated. ● On the Agent Management page, prior agent versions that are not available to be assigned to your account no longer show on the page.
Account Settings	● In the Administration area, a new Account Settings link and page are available. The page includes configurations for two new features: Two-Factor Authentication and Single Sign-On. The old Account Settings is now labeled **Classic Account Settings**. Also, when you click 👤 ▾ > **Account Settings**, the new Account Settings page opens instead of the Classic Account Settings page. ● When Event Calling is enabled on one or more devices, the correct device count now shows in both the Call Settings area of the Account Settings page *and* the dialog that shows when you click the **View** link in this area.
Android support	● In Device Details for an Android device, the following pages related Endpoint Data Discovery, which is not supported on Android devices, no longer show: ○ Endpoint Data Discovery Summary ○ Endpoint Data Discovery History

Feature/Area	Improvements and fixes
Announcements	• When you click the 📅▾ icon on the quick access bar, the **All Announcements** button is now available below the calendar even if there are no unread announcements in the current month.
Application Persistence	• On an Application Persistence policy configuration page, clicking the **Application Persistence Terms and Conditions** link to review the terms and conditions no longer automatically selects the checkbox indicating that you acknowledge the terms and conditions. • On an Application Persistence policy configuration page, the SHA-256 Hash field is now a required field.
Authentication	• When system generated Absolute emails contain links (such as the Reset Password email), the URL of the link is also provided in the email. This means that if you are viewing the email in plain text you can copy the URL and paste it in a browser.
Chromebook support	• The username associated with a Chromebook device in the Google Admin console now shows in the Absolute console in the Username field instead of the Assigned Username field.
Custom Device Fields	• When you move Custom Device Field values to a new device, the correct date format is now applied to the following fields: Lease End Date, Service Contract End Date, and Warranty End Date.
Dashboard	• On the Home and Device Management Dashboards, the correct time now shows when you click the 🕓 icon in the Device Activity widget. • On the Home and Applications Dashboards, the data in the Application Persistence Summary widget is now consistently refreshed every 15 minutes, as expected.
Data collection	• When the Absolute agent performs hardware data collection on a Mac device running macOS 10.10.5, performance of the device is no longer negatively impacted, the `hdc` folder no longer shows in the Dock, and the device can be restarted.
Device groups	• In the quick access toolbar, you can now use the **Upload File for Bulk Device Action** option to add devices to an existing static device group. • When you're adding more devices to a device group, the devices that are already members of the group are no longer available for selection in the Add Devices dialog. • You can now successfully create a device group when the device group name contains a question mark (?). • If you add a child Default Folder to a Roll Up Folder that already contains one or more device groups, the list of devices included in the Roll Up Folder now show as expected when you open the Roll Up Folder.
Device Usage reporting	• When the Device Usage policy is enabled on a device, a device usage value of "0" is reported each day that the device is unused. Previously, no value was reported for these days until the device was used, at which time a value of "No data" was reported for each day with no usage.

Feature/Area	Improvements and fixes
Endpoint Data Discovery	● When the EDD component finds a match on a Mac device in a gzip (.gz) file, the File Type is now reported correctly in EDD reports as application/x-gzip, instead of incorrectly as application/msword. ● All predefined Endpoint Data Discovery reports now include Username, Device Name, and Serial Number columns by default. ● If your user role is not granted Publish permissions for Endpoint Data Discovery, you no longer see the Perform EDD Scan option in the Device Actions menu on reports and a device's Device Details page. ● When you export the Endpoint Data Discovery Match Scores report, all devices with no detected matches now show a value of "0" in the Total Match Score column. Previously the column in the exported report was empty. ● On a Windows device, if a file is moved after a full scan, the file is now reported in its new location during the subsequent delta scan.
Full-Disk Encryption	● The Absolute agent now detects Microsoft BitLocker Drive Encryption on devices running the Windows 10 Education N operating system.
Geolocation	● The **Last known location** of a device that shows on the (Classic) Device Summary > Call Tracking tab now matches the device's most recent location that shows on the Device Location History Report.
Language support	● When you view the Absolute console in a language other than English and you export a report that includes the following columns, the column headers now show in the correct language: ○ Hardware > Status ○ Software > Status ○ EDD > Status ● When you view the Absolute console in French, the **Configuration Options** section now shows in the Call Settings area of the Classic Account Settings page.
Policies	● If the Hardware policy in your global policy group is set to Inactive you can now activate the policy. However, note that after the policy is activated you can't deactivate it. ● The Policies page for a device now shows a warning if an error occurs while the system is trying to protect a file using Azure Information Protection (AIP).
Public APIs	● If authentication to an Absolute public API fails, you can now turn on authentication debugging on the API Token Management page in the Absolute console and then submit a Support case. Absolute Technical Support will review the generated log file and help you resolve the authentication issue.
Report improvements	● You can now add the Enrolled Date (UTC) column to reports. This column shows the date and time when a device made its first connection to the Absolute Monitoring Center. For devices that were enrolled prior to the release of Absolute 7.0, this column shows the device's Activation Date. ● You can now successfully export an extremely large report (> 1 million records). Note that the file must be in CSV format; XML and XSL formats are not available.
User Management	● If your account has not been upgraded to Absolute 7 Device Freeze, Freeze Device permissions are now correct when you view a role's Permissions page.
User Awareness	● On the Users page in the User Awareness area, you can now search for users by name or username.

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/support and follow the instructions on the page to contact Technical Support in your region.

Copyright Information

Absolute 7.3 Release Notes—Documentation Release 1

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