

## Absolute 7.0 Release Notes

---

Absolute 7.0 is a major release offering a redesigned console with many new features and enhancements. It is the first major feature release following Absolute Data and Device Security (DDS) 6.4.

### Product name change

This release introduces a change to the name of our product: Absolute Data and Device Security (DDS) is now **Absolute**.

All references to the prior product name in the console and the online Help are updated to "Absolute".

### Redesigned Absolute console

Absolute 7 introduces a redesigned console with an exciting new look and feel.

If you used the Absolute console in a previous release, you'll notice that the console includes a new navigation bar showing a collection of icons instead of links. Click the icons to access the newly defined areas within the console. These areas are no longer divided into DDS 6 and DDS 5 functionality; the entire system is restructured to bring together related features and functionality. For example, DDS 6 device-related reports and all DDS 5 reports (now named Classic Reports) reside in a single area called *Find Devices*.

To learn where to now find the DDS 6 and DDS 5 features you're familiar with, see [Navigating the new console](#) near the end of this document.

#### Quick access toolbar

The new console includes a new quick access toolbar near the top of each console page. You can use the menus on the toolbar to perform the actions you use most, such as create a new device group or request a security authorization code.



### Features and enhancements

The current release of Absolute introduces the following new features and feature enhancements:

---

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

---

- **Absolute Reach:** You can use the new Absolute Reach feature to upload a script to the Absolute console and run the script on selected Windows or Mac devices. The following script formats are supported:
  - PowerShell script (.ps1): for Windows devices
  - Bash shell script (.sh): for Mac devices

Each script format has its own set of configuration options you can set, such as the maximum allowed run time for the script. You can view the status of your submitted Script requests on the new Event History report or on a device's Event History page.

If you need to cancel a Script request that you've submitted, you can submit a Cancel Script request, as long as the status of the original Script request has not changed from *Script Requested*.

---

For more information about submitting Script requests, see *Running scripts on devices* in the online Help. For more information about canceling a request, see *Canceling scripts requested for devices* in the online Help.

- **User Awareness:** You can use the new User Awareness area to see a history of the devices used by your domain users and the potential data risk posed by those users as a result of the devices they've accessed.

The User Awareness area includes the following pages:


- **Dashboard:** Use the dashboard's User Data Access Risk widget to see the ten users that pose the greatest data access risk to your organization. The widget displays a Risk Score for each user, which is a sum of the Endpoint Data Discovery (EDD) Match Scores from all devices they've accessed.
- **Activity:** View a timeline of the Windows, Mac, and Chromebook devices that a user has logged in to.

---

**NOTE** To view data in the User Awareness area, a number of prerequisites must be met.

---

For the list of prerequisites, and more information about working in the User Awareness area, see the topics under *User Awareness* in the online Help.

- **Application Persistence:**
  - **Application Persistence policy:** The Report and Repair policy has been renamed to "Application Persistence policy" and the policy has been enhanced. Administrators can now configure the policy to reinstall the application if the Absolute agent detects that the application is missing or failed to be repaired.  
In addition, Application Persistence policies now support the following third party applications installed on your devices:
    - F5 BIG-IP Edge Client™
    - Ziften ZenithFor more information, see *Getting started with Application Persistence policies* in the online Help.
  - **Application Persistence report:** A new predefined report is available in the Find Devices area. The Application Persistence report shows the status of your persisted applications. You can also add columns to the report to view details about applications that have been repaired or reinstalled on a device.  
For more information, see *Application Persistence report* in the online Help.
  - **Persistence page:** For authorized users, the Persistence page in the Applications area provides an overview of the third party applications that you can track, repair, and reinstall by activating the Application Persistence policy. For those applications that are eligible for activation, the current status and configuration of the Application Persistence policy shows. From this page, you can configure and activate policies for eligible applications.  
For more information, see *Persistence* in the online Help.
- **User Management:** The Users area in DDS 5 is replaced by a new area for managing users in Absolute 7. You can access the new User Management area by clicking  on the navigation bar and clicking **User Management** on the sidebar. The User Management area includes two sections: Users and Roles.

---

In the Users section, authorized users can create a new user account, assign a user role, and invite the associated user to create their login password. They can also search for existing users by name, email address, or the status of their user account.

In the Roles section, authorized users can view the permissions associated with each default user role and assign one or more users to these roles. Depending on the configuration of your account, authorized users may also be able to view and assign *custom roles* to users. Custom roles are available only if your Absolute account is configured with a System Administrator role, which is a new "superuser" role available in this release. System Administrators create a custom role by selecting a base role and then adding individual permissions to the role. To add the System Administrator role to your account, submit a Support case. For more information, see *Contacting Global Support* in the online Help.

For more information about working with users and roles, see the topics under *User Management* in the online Help.

- **Unenroll Device:** To disable a device in the Absolute console and free up the device's license, you now submit an Unenroll Device request instead of an Agent Removal request. Authorized users can select one or more devices from one of the following reports or pages and submit an Unenroll Device request:
  - Active Devices report
  - Application Persistence report
  - Devices with Active Policies report
  - Endpoint Data Discovery Match Score Summary report
  - Event History report
  - A customized report based on one of the above listed predefined reports
  - Device Group page
  - A device's Device Details page

When you submit an Unenroll Device request, an item is added to the Notifications area, which you can open from the console's quick access toolbar. You can also view your pending Unenroll Device requests on the new Event History report or a device's Event History page.

For more information about unenrolling a device, see *Unenrolling devices from your account* in the online Help.

- **Event History report:** To support the Absolute Reach and Unenroll Devices features, a new predefined report is now available in the Find Devices area. Authorized users can use the Event History report to see a history of the devices with one or more new, pending, or completed Script requests, Cancel Script requests, and Unenroll Device requests. By default, the report shows information for the past seven days, but you can update the report's filters to show more or less data. You can also view the history of an individual device's events on its Event History page.

For more information, see *Event History report* and *Viewing the event history for a device* in the online Help.

- **Policies:** The Policy Groups area has been redesigned. After you open a policy group, the work area is now divided onto the following two pages, which you can toggle between:
  - **Devices:** shows the list of devices assigned to a policy group. From this page you add more devices to a policy group or remove devices.
  - **Settings:** shows the activation status of the policy group's policies all on a single page. From this page you can set policy configurations (where applicable), and activate and deactivate policies.

- **Integration with Azure Information Protection (AIP):** The AIP Status field is now included on the dialog that shows when you click a file name on any of the following pages:
  - Endpoint Data Discovery History report
  - Endpoint Data Discovery Reporting Data report
  - Device Details: Endpoint Data Discovery Summary page
  - Device Details: Endpoint Data Discovery History page

For more information, see *Viewing a file's EDD matches* in the online Help.

- **Reset Password:** The process for changing your password has been improved to be more secure. Instead of emailing you a system generated password, we now send an email containing a Reset Password link. The link opens a dialog that contains an additional security feature, and fields to enter and confirm your new password. For more information, see *Resetting your password* in the online Help.
- **Last Connected (UTC):** You can now use the Last Connected (UTC) filter to filter device reports and smart device groups by the date and time when a device's Absolute agent last connected to the Absolute Monitoring Center. You can also add the Last Connected (UTC) column to a report.
- **Absolute Mobile for Android:** A new version of the Android agent is now available. You can download agent version 3238 from the Download Packages page in the Administration area.


## Improvements and fixes

Absolute 7 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.







---

















- **Reports:** When the Absolute agent successfully collects hardware, software, or EDD data from a device, the correct status icon now shows in the applicable policy status column in a device report, such as the Active Devices report. Previously, the *Unable to send data* icon (▲) showed in some cases.
- **Device Freeze:** On the Device Freeze Summary Report page, any edits you make to the Requested Date filter are now saved when you click  to save your report filters. To reuse your saved filters, go to Find Devices > Classic Reports > My Content > My Filters.
- **Device Groups:**
  - When you use the *within last* or *not within last* Date filter to create a smart device group, the filter is now applied correctly each time the device group is generated.
  - When you add a new device to your Absolute account, the device now shows in the device groups you've assigned it to, in all cases.
- **Integration with Azure Information Protection (AIP):**
  - After you remove AIP Protection from a file, the file no longer shows *Unsupported File Type* in the AIP Status column on the Endpoint Data Discovery Match Score Summary page. Now, the AIP Status column is blank indicating that the file is once again eligible for protection using AIP.
  - When you select the option to remove AIP Protection from a file, a dialog now shows asking you to confirm that you want to perform this action.
- **Licensing:** Absolute DDS Premium Editions now includes the Application Persistence (formerly Report and Repair) feature, as expected.




















- **Application Persistence (formerly Report and Repair):**
  - When you add the Repair Status column to a report, a status of **Unknown Option** no longer shows in the column for some devices. Instead, the applicable status now shows.
  - All instances of the application name, "Ivanti (LANDESK) Management Suite", are updated to its new product name, "Ivanti Endpoint Manager".
- **Account Settings:** Administrators no longer need to configure password complexity settings for their account on the Account Settings page. Password complexity requirements are now included by default and are defined as follows:
  - Passwords must contain between 8 and 20 characters and include at least two alphabetic characters and one special character.
  - Reuse of the user's last five passwords is not permitted.
- **Investigation Report:** You can now submit an Investigation Report for a device with an Asset Number that exceeds 30 characters in length.
- **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.










## Navigating the new console

Use the following table to learn where to now find the features you're familiar with from Absolute DDS 6.4.

Feature in Absolute DDS 6.4	Where to find this feature in Absolute 7
<b>DDS 6</b>	
Explore	This page is deprecated.
Reports	<ul style="list-style-type: none"> <li>● For device reports: On the navigation bar, click . Select a report from the Find Devices sidebar.</li> <li>● For software reports: On the navigation bar, click . Click <b>Software Reports</b> and select a report from the sidebar.</li> <li>● For Endpoint Data Discovery (EDD) reports: On the navigation bar, click . Click <b>Endpoint Data Discovery</b> and select a report from the sidebar.</li> </ul>
Dashboard	To view all available dashboard widgets, click  on the navigation bar to show the Home page.
Device Groups	To view and edit existing device groups, click  on the navigation bar. Click <b>Device Groups</b> and select a device group or folder on the Device Groups sidebar. To add a new device group, click  on the quick access toolbar and then click <b>Smart Device Group</b> or <b>Static Device Group</b> .

Feature in Absolute DDS 6.4	Where to find this feature in Absolute 7
Device Policies	To view and edit existing policy groups, click  on the navigation bar. Click <b>Policy Groups</b> and select a policy group on the Policy Groups sidebar. To add a new policy group, click  on the quick access toolbar and then click <b>Policy Group</b> .
Administration	
Endpoint Data Discovery Rules	On the navigation bar, click  . Click <b>Endpoint Data Discovery</b> and click <b>Rules</b> on the sidebar.
Software Catalog	On the navigation bar, click  . Click <b>Software Reports</b> and click <b>Software Catalog</b> on the sidebar.
Support	On the navigation bar, click  and click <b>Support</b> .
Training	On the navigation bar, click  and click <b>Training</b> .
<b>DDS 5</b>	
Home	This page has been replaced by the Home dashboard. On the navigation bar, click  .
Reports	On the navigation bar, click  and click <b>Classic Reports</b> on the sidebar.
Administration	
Alerts	To view existing alerts and alert events, click  on the navigation bar and click <b>Alerts</b> on the sidebar. To add an alert, click  on the quick access toolbar and then click <b>Alert</b> .
Data	On the navigation bar, click  and click <b>Data</b> on the sidebar.
Departments	On the Data sidebar, click <b>Departments</b> .
Export Data	To export data, click  on the quick access toolbar and click <b>Export Data</b> . To view the status of Export requests, on the navigation bar, click  and click <b>Import/Export</b> .
Import Data	To import data, click  on the quick access toolbar and select an option from the shortcut menu. To view the status of Export requests, on the navigation bar, click  and click <b>Import/Export</b> .
Custom Device Fields	On the Data sidebar, click <b>View and Edit Custom Device Fields</b> or <b>Manage Custom Device Fields</b> .
End-User Messaging	On the Data sidebar, click <b>End User Messaging</b> . Click the <b>Import/Export</b> link and click <b>Export Data Status</b> to open this page.
Geofences	To view existing geofences, click  on the navigation bar and click <b>Geofences</b> .
Groups	

Feature in Absolute DDS 6.4	Where to find this feature in Absolute 7
Device Groups	On the navigation bar, click  . Click <b>Device Groups</b> and then click <b>Classic Groups</b> on the sidebar.
Import Group	To import groups, click  on the quick access toolbar and select an option from the menu. To view the status of Group Import requests, on the navigation bar, click  . On the sidebar, click <b>Import/Export</b> and click an option on the Import/Export sidebar.
Export Groups	To export groups, click  on the quick access toolbar and select an option from the menu. To view the status of Group Export requests, on the navigation bar, click  . On the sidebar, click <b>Import/Export</b> and click an option on the Import/Export sidebar.
Software Policy	On the navigation bar, click  . Click <b>Policy Groups</b> and click <b>Software Policies</b> on the sidebar.
Users	To view existing users, click  on the navigation bar and click <b>User Management</b> on the sidebar. To add a user, click  on the quick access toolbar and then click <b>User</b> .
Account	
Account Settings	Do one of the following: <ul style="list-style-type: none"> <li>On the navigation bar, click  and click <b>Account Settings</b> on the sidebar.</li> <li>On the quick access toolbar, click  and click <b>Account Settings</b>.</li> </ul>
Add Licenses	On the navigation bar, click  and click <b>Add Licenses</b> on the sidebar.
Download Packages	On the navigation bar, click  and click <b>Download Packages</b> on the sidebar.
System Notifications	On the navigation bar, click  and click <b>System Notifications</b> on the sidebar.
Disable Pre-Authorization	On the navigation bar, click  and click <b>Disable Pre-Authorization</b> on the sidebar.
Agent Removal Requests	To submit a new request to remove the agent from a device, on the quick access toolbar click  and click <b>Unenroll Device</b> . To view pending Agent Removal Requests that were submitted before the release of Absolute 7, on the navigation bar, click  and click <b>Agent Removal Requests</b> on the sidebar.
Data and Device Security	
Security Authorization	To request an authorization code, click  on the quick access toolbar and click <b>Authorization Code</b> .
Data Delete	On the navigation bar, click  and click <b>Data Delete</b> on the sidebar.
Device Freeze	On the navigation bar, click  and click <b>Device Freeze</b> on the sidebar.

Feature in Absolute DDS 6.4	Where to find this feature in Absolute 7
Intel® Anti-Theft Technology	On the navigation bar, click  and click <b>Intel® Anti-Theft Technology</b> on the sidebar.
File List	To submit a File List request, click  on the quick access toolbar and click <b>Request File List</b> . To view the status of File List requests, on the navigation bar, click  and click <b>File List Summary Report</b> on the sidebar.
Remote File Retrieval	To submit a File Retrieval request, click  on the quick access toolbar and click <b>Request File Retrieval</b> . To view the status of File Retrieval requests, on the navigation bar, click  and click <b>File Retrieval Summary Report</b> on the sidebar.
Custom Action Fields	On the navigation bar, click  and click <b>Custom Action Fields</b> on the sidebar.
Investigations	On the navigation bar, click  and click <b>Investigations</b> .
Documentation	On the navigation bar, click  and click <b>Documentation</b> .
Support	On the navigation bar, click  and click <b>Support</b> .

For more information about working with the new console, see *Navigating the console* in the online Help.

## Contacting Global Support

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

## Copyright Information

Absolute 7.0 Release Notes—Documentation Release 1

©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](http://www.absolute.com/patents).