WHITE PAPER

“Get Audit-Ready Guide” with Absolute

This guide will help you prepare for your audits by reviewing how to create and share custom reports

Audits and technology go hand in hand. You need to be able to readily provide data on where funds have been spent and how resources are being used. With the introduction of the CARES Act, the American Rescue Plan, and other federal funding, it is now even more important to have a centralized place for all the data points required for an audit.

The good news is that a lot of the information needed for an audit is readily available within your Absolute console. Absolute collects many data points about your devices and offers you the ability to import data unique to your organization.

This guide will help you prepare for your audits by reviewing how to create and share custom reports containing data points that matters most to you, in a time-efficient manner.

/ABSOLUTE®

Data points collected by the Absolute agent

- Average Device usage
- Device Freeze Status
- Device Name
- Domain Name
- Identifier
- Last Connected
- Local IP Address
- Make
- Missing or Stolen
- Model
- OS Installation Date
- Policy Group Name
- Public IP Address
- Serial Number
- Username

Fixed Device Fields

- Asset Tag/Number
- Cost Centre/Code
- Department
- Device Purchase Date
- Purchase Order Ref
- School

Custom Device Fields

- Paid Date
- Received Date
- Student Number

For a complete list of data points collected by the Absolute agent, refer to the **Help**.

Identify data for your report

The Absolute agent collects most of the device-related data needed for your reports. However, there can be certain data points specific to your devices or your organization that the agent does not collect (e.g., student number or school). You may need to include these unique data points in your regular device audits. To centralize your asset management, you can import these data points into the Absolute console using Device Fields.

Device fields

There are two types of device fields available in the console called Fixed Device Fields and Custom Device Fields. You can use these to identify the device fields that you need to add or create for your audit reports.

Users with the permission level of Administrator or higher can manage device fields. System Administrators can grant permission to any custom roles to manage device fields.

Fixed Device Fields

- Absolute provides a list of predefined device fields included by default in every account.
- These fields are non-editable and can't be deleted.
- Go to Settings > Data > Manage Device Fields to review the list of fixed device fields. You can also find the list in the **Help**.

Custom Device Fields

- If you want to store information in the console that is relevant to your device or organization but not covered by one of the Fixed Device Fields, you can create a Custom Device Field. Absolute allows you to create up to 20 Custom Device Fields.
- The Custom Device Fields can be text, a date, or a selection from a drop-down list of options.
- To create a Custom Device Field, go to **Settings > Data > Manage Device Fields > Create Custom Device Field**.

To learn more about managing device fields, refer to the **Help**.

Update device field data

When you add new device fields to your console, you need to assign data values to them. You can add data values to an individual device or to all devices in a device group.

Users with the permission levels higher than a Guest user can edit and update device fields, whereas a Guest user can only view the data values.

Add data values to an individual device or device group

- Go to **Settings > Data > View and Edit Device Fields > Actions > Choose device or Choose device group**.
- You cannot choose a device or a device group containing a device that is reported stolen in the console.
- Enter new data values or update existing data values in the Field Data field.
- The data value entered for a device group is applied to all the devices in the device group. If you want to add different data values, choose devices individually.
- While working with device groups, some devices may have different existing values for the same device field. In this case, a Multiple Values button is available under the Field Data field. If you choose to override the existing values, click the button and update the field.

To learn more about updating device field data, refer to the **Help**.

Import device field data

Use Import Data to bulk upload data values for multiple devices at the same time.

- Go to **Assets > All Devices**. Use edit columns to include the device fields to which you want to add data. Export the report in CSV file format with column names.
- Alternatively, you can also create your own CSV file. The column names you enter must match with the device field names in the console.
- **Identifiers** must be the first column in the CSV file.
- Add data values and update the CSV file. The format of the data values you enter must match with the data types defined in the console.
- Go to **Settings > Data > View and Edit Device Fields > Import Data** and import the updated file to the console.
- Once the uploaded file is processed, an update will appear in the Notifications area of the console.

To learn more about importing data, refer to the **Help**.

Create a custom report

Every audit process is unique and requires different information. You can create custom reports to include the data points that are required for your audit report.

- Go to **Assets > All Devices**. Apply filters and add or remove columns necessary for your audit report. Save the custom report by giving it a suitable name
- You can also create a custom report by modifying any default or existing custom report in the **Reports** page.
- You can find the custom reports in the **Reports** page, under **Custom**.
- Custom reports are user specific. You cannot view custom reports created by other users unless they export it and share with you.

Share your report

As part of the audit process, you may want to share your custom reports with others. To share a custom report, you can either export it or schedule it to automatically share with your colleagues in and outside your organization, on an ongoing cadence.

Export a report

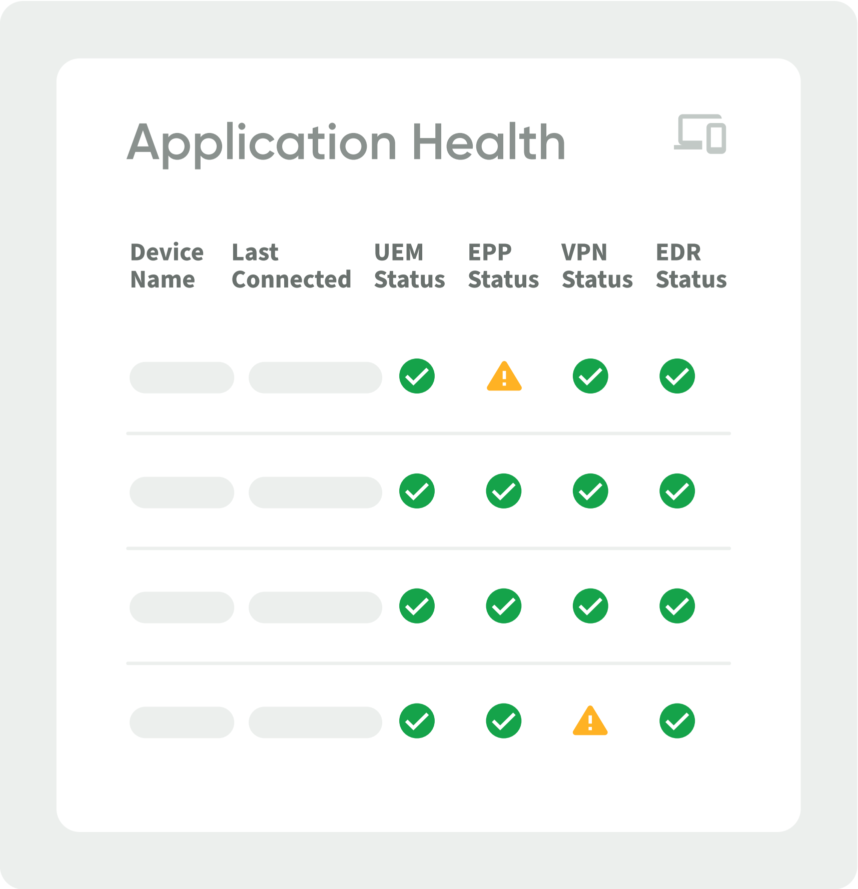
- Go to **Reports** and open a custom report that you created for your audit.
- Depending on the report you're exporting, click either or **Report options** and export the report to your computer in your preferred format.

Schedule a report

- Go to **Reports** and open a custom report that you created for your audit.
- Click and click **Schedule**. Schedule the report to automatically generate on a daily, weekly, or monthly basis.
- • You can choose a preferred file format for the report and send to email addresses that belongs to both inside and outside your organization.
- To learn more about working with reports, refer to the **Help**.

> “Some of the largest security breaches involving school districts include data not just about current students and staff, but those who might have interacted with the district five or 10 years ago.”

DOUG LEVIN,
K-12 CYBERSECURITY RESOURCE CENTER,



Application Health

Device Name	Last Connected	UEM Status	EPP Status	VPN Status	EDR Status
		✓	⚠	✓	✓
		✓	✓	✓	✓
		✓	✓	✓	✓
		✓	✓	⚠	✓

How Absolute can help

The Absolute Platform for Endpoint Resilience® helps schools and districts ensure that their devices and security controls maintain a secure operational state automatically, without the need for user intervention. Here are three ways that Absolute can help schools protect their networks and data more effectively.

Endpoint security and device recovery

Lost or stolen devices can be exploited by bad actors to gain access to networks or data. Absolute's software includes tools that enable schools to wipe or freeze devices that go missing, as well as tools that aid in tracking and recovering lost or stolen devices.

Application functionality

Encryption, anti-virus, and anti-malware software can only provide protection if they're working effectively. If these programs are disabled or not functioning, then school networks and data are vulnerable to an attack. Often, when hackers gain access to a computer system, they'll disable the software protecting the rest of the network. According to Absolute's "Endpoint Trends in K12 Education 2021-22" report, only 53% of the anti-virus applications studied were operating effectively.[3]

If Absolute's software detects that an endpoint device's security solutions have been uninstalled or aren't working correctly, it will reinstall these solutions automatically. By ensuring the integrity of security applications, Absolute's software removes the burden from IT staff to check and maintain these systems manually.

Scanning for sensitive information

Often, educators aren't even aware they are storing sensitive information on endpoint devices and other vulnerable locations. Nearly one-third of the education devices studied for Absolute's "Endpoint Trends in K12 Education 2021-22" report contained sensitive data such as Social Security numbers and student health information.[4]

Absolute's software helps schools determine whether they are at risk from unencrypted data. The software scans devices to look for personal health information, Social Security numbers, financial information, and other sensitive data stored on these machines. K-12 leaders can schedule and run regular reports to see which devices contain unprotected data, so they can take steps to secure this information.

[1] K-12 Cybersecurity Resource Center (2021). "The State of K-12 Cybersecurity: 2020 Year in Review."

[2] Goodhue, David (2021). "Hackers breach Broward schools' computer system. They're demanding millions in ransom," The Miami Herald.

[3] Absolute Software (2021). "Endpoint Trends in K12 Education 2021-22."

[4] Ibid.

eSchool News.com

This white paper was produced by eSchool News, the online platform that delivers daily technology news and information to K-12 education administrators, educators, and technology professionals, and dedicated to the advancement and wise use of technology to improve teaching and learning for all. eSchool News offers ed-tech decision makers a wide range of informative content — including newsletters, webinars, case studies, white papers, websites, and more — that provide in-depth coverage of the latest innovations, trends, and real-world solutions impacting the education community. Explore more at www.eSchoolNews.com.

ABSOLUTE®

Absolute Software makes security **work**. We empower mission-critical performance with advanced cyber resilience. Embedded in more than 600 million devices, our cyber resilience platform delivers endpoint-to-network access security coverage, ensures automated security compliance, and enables operational continuity. Nearly 21,000 global customers trust Absolute to protect enterprise assets, fortify security and business applications, and provide a frictionless, always-on user experience.

Request a Demo