Back to School Guide

USER GUIDE

An Absolute Guide to Successfully
Preparing For a New School Year

CONTENTS

Given the current situation with the COVID-19 pandemic, preparing for the school year is unlike any other. For many, understanding how students and teachers will interact is still unclear—there may be a full-time return to in-person learning, virtual classes for all, or a hybrid model that combines the two. However the new school year may look for you, this guide will help you prepare your device inventory.

01

Take Inventory

Know where your devices are and take action to locate any that are missing or unreturned.

02

Prepare Your Devices

Get your devices organized and up-to-date by remotely applying any necessary changes.

03

Initiate Device Monitoring

Set boundaries to track devices and turn on policies to monitor how they are being used.

04

Assign Your Team

Identify who will manage your devices and the actions they will perform in the console.

01 TAKE INVENTORY

Know where your devices are and take action to locate any that are missing or unreturned.

Secure unreturned devices that need to be collected.

- **Run the *Show a Return Device Notification* script** from the Reach Library to display return instructions to end users. Note: This script will not work on Chromebooks.
- **Flag unreturned devices as missing** to monitor them in the console. When they call in, you will receive a notification with details to help you identify their location. Once returned, mark devices found in the console.
- **Freeze devices** that exceeded the return deadline to prevent access to them. Provide a custom message with instructions for return.
- **Use the Geolocation report** to monitor the location of devices until they have been returned.
- **Create devices groups** to keep organized with reclaiming devices. Create device groups for devices that are:
  - Out of warranty and need to be retired and unenrolled.
  - Not expected to be returned.
  - Belonging to senior students and other individuals leaving.
  - Old and need to be recalled and replaced.
- **Follow the** device collection process to learn more about reclaiming devices.
- **Learn more** about addressing missing or stolen devices.

Confirm that devices are in the possession of the assigned users.

- **Use the Geolocation report** to determine if devices are calling in from their expected location (i.e. in state or local areas).
- **Sort the All Devices report by Device Name and Username** to identify data outside of the expected naming conventions. Save these views as custom reports.
- **Freeze devices** that aren't in the possession of the assigned user and take the appropriate actions.

02 PREPARE YOUR DEVICES

Get your devices organized and up-to-date by remotely applying any necessary changes.

Organize devices into groups.

- **Create a classic device group** for each campus and assign a representative (i.e. Tech Coordinator) from the campus to manage their group of devices. For each campus, create two device groups: one for student and staff devices and one for teacher devices. Separating devices in this way will help you with alerting and reporting.
- **Assign teacher/staff devices and student devices to different policy groups.** This allows you to configure devices separately so that you can accurately report on web usage and geolocation tracking of student devices.

Update devices with any necessary changes.

- **Freeze devices** that require critical software updates.
- **Run Reach scripts** to remotely update critical applications, install software, create desktop shortcuts to new websites or applications, manage browser settings, and more.

Identify unused devices.

- **Use the Dark Devices report** to monitor devices that have been offline longer than 30 days. Use this report to help identify unused devices and redistribute them to where they can be utilized.

Ensure that devices connecting to the school network are safe.

- **Use the Anti-Malware and Full-Disk Encryption Status reports** to check the anti-virus and encryption status of your devices.
- **Consider using a Reach script** to block firewall access to Remote Desktop Protocols (RDP).
- **Run an EDD scan on teacher/staff devices** to determine if sensitive personal and/or work related information is stored on the devices.

03 INITIATE DEVICE MONITORING

Set boundaries to track devices and turn on policies to monitor how they are being used.

Maximize the data collected in reports by turning on policies.

- **Hardware** policy collects all available hardware data about a device.
- **Software** policy collects information about the software applications installed on a device.
- **Device Usage** policy collects data about the time spent on a device.
- **Web Usage** policy collects data about the websites users visited most recently.
- **Application Persistence** collects information about the status and compliance of third party applications.

Review reports to ensure appropriate device use.

- **Use the Device Analytics report** to monitor device usage during a given time period. Use it to compare device usage between device groups (e.g. different schools in a district).
- **Use the Weekly Web Usage report** to monitor the time spent on websites and the **Rising Web Usage report** to identify trends in web activity on devices. Use these reports to identify sites that call for adjustments to web filtering and/or take administrative actions against users not using devices appropriately.
- **Compare web usage data** with device usage data to get a comprehensive understanding of how effectively devices are being used—that is, how much of device usage is spent on educational tools/websites.

Define boundaries for your devices and set alerts.

- **Set Geofences at the state/province level** to be notified when devices cross boundaries. Student devices are now permitted to leave campus and possibly the district; however, given current stay-at-home advisories, devices may not be allowed to leave the state/province. Set an alert to be notified when a device crosses a boundary so that it can be reported to administration and/or investigated as missing or stolen.
- **Set the Major Change alert** to be notified of devices that had changes made to their operating system, device name, username, and made a self-healing call. This alert is only triggered when all conditions are met, which may indicate that the device has been stolen.

04 ASSIGN YOUR TEAM

Identify who will manage your devices and the actions they will perform in the console.

Add your Tech Coordinators.

- Give Tech Coordinators access to only manage devices belonging to their campus device group.
- Assign Tech Coordinators to the Power User role. This will give them permissions to monitor asset reports, track down student devices that haven't connected for a period of time, perform hardware and software inventory checks, identify off-network devices, and flag devices as missing and monitor them until they call in.

Add your security team.

- Assign two or more users to the Security Power User or Security Administrator roles to manage device and data security when devices are missing or stolen.

Add your asset management team.

- Assign users to the Guest, Power User, or Administrator roles depending on the permission level they require. These roles enable users to review inventory and asset reports, track student device usage, and monitor suspicious alert events.
- Provide users with the added permission of unenroll to enable them to remove devices from your account when required. This will help keep your inventory up-to-date and remain license compliant.

WHAT'S NEXT?

To learn more about the console, visit The Learning Hub.

Need help with the device collection process or the console? Contact your Customer Success Manager, or Absolute Support.

ABSOLUTE®

ABOUT ABSOLUTE

Absolute is the leader in Endpoint Resilience™ solutions and the industry's only undeletable defense platform, embedded in over a half-billion devices. Enabling a permanent digital tether between the endpoint and the enterprise who distributed it, Absolute provides IT and Security organizations with complete connectivity, visibility, and control, whether a device is on or off the corporate network, and empowers them with Self-Healing Endpoint® security to ensure mission-critical apps remain healthy and deliver intended value. For the latest information, visit **absolute.com** and follow us on **LinkedIn** or **Twitter**.

EMAIL:
sales@absolute.com

SALES:
absolute.com/request-a-demo

PHONE:
North America: 1-877-660-2289
EMEA: +44-118-902-2000

WEBSITE:
absolute.com