Chromebook Collection Guide

An Absolute Guide to Successfully Reclaiming Student Devices with Ease
CONTENTS

Summary .............................................................................................................. 3

Plan ..................................................................................................................... 4

Execute .............................................................................................................. 4

Collect ............................................................................................................... 7

Control .............................................................................................................. 7

Monitor ............................................................................................................. 11

What’s Next? ..................................................................................................... 13
This guide takes you through the device collection process and highlights the Absolute features that can assist you in successfully reclaiming your district’s devices. Here is a summary:

**Plan**

45-60 days prior to device collection, prepare user message scripts and target student device groups.

**Execute**

In the month leading up to the collection period create custom alerts and reports to categorize devices by desired return date.

- 30 days prior
- 15 days prior
- 1 week prior
- 1 day prior

**Collect**

Collect student devices according to your procedures.

**Control**

1-2 days after collection, flag devices that haven’t been returned as missing, 5-7 days after flagging devices missing, freeze devices that haven’t checked in.

**Monitor**

Use the Missing Devices view, and Device Freeze Summary report to keep your inventory visible.
**Plan**

**TIMELINE: 45-60 DAYS PRIOR TO THE DEVICE COLLECTION PERIOD**

Get organized for the phases that lie ahead. Read about the other phases in this guide and make any necessary preparations so that you can successfully collect your devices.

Preparation tasks may include:

- Create device groups (e.g. by school, 1:1 program, etc.)
- Create custom alerts and reports by required date of return in the Execute phase
- Coordinate with your colleagues for the Collect phase
- Prepare custom Device Freeze messages to elicit a response from students who have not returned devices on time in the Control phase

**Execute**

**TIMELINE: 30 DAYS, 15 DAYS, 1 WEEK, AND 1 DAY PRIOR TO THE DEVICE COLLECTION PERIOD**

In the Execute phase, identify and categorize devices by desired return date, and create alerts for before and after the return date to help you stay organized.

Absolute’s custom report fields and alerts help you in this task. Identify the devices that you want returned by creating a custom reports device field for the date the device(s) should be returned. Use this date value to create custom reports and alerts for devices approaching or past their return date. Please see Help for more information on populating custom device fields with more information.
Create a Custom Device Field to Categorize Devices by Return Date

1. Navigate to Settings → Data → Manage Device Fields
2. Click Create a Custom Device Field and name the field Device Return Date (or custom) to be used for reporting and alert purposes. Set the Field Type to Date and click Save.

Set Up Return Date Alerts

1. Set up an email alert for this group of devices to trigger prior to and after the return date.
2. Go to Policies → Alerts → Create and Edit Alerts.
3. Select the **Device Return Date** field and how many days in advance you would like the alert. Here, we suggest 14 days.

---

**Set Up Return Date Reports**

Use your Device Return Date report to see all the Chromebooks that need to be returned.

1. Navigate to Assets → All Devices
2. Click the Menu Options Icon → Select **Edit Columns**

---
3. Search for the **Device Return Date** Item on the Left Pane and Add to the Right Pane.

4. Save the report with a custom name such as **Assets List with Return Dates**

Use these reports to track your device returns in the Collect phase. Additional custom reports and alerts can be created based on your requirements, such as devices that have passed their return date.

**Collect**

In this phase, collect devices according to your District’s procedures.

**Control**

In the Control phase, flag unreturned Chromebooks as missing in the console to attempt retrieval. If this is unsuccessful, freeze the devices.

**Track missing devices**

**TIMELINE: 1-2 DAYS AFTER THE DEVICE COLLECTION PERIOD**

Absolute monitors devices that you have flagged as missing. When they come online, you are notified and provided with details such as username, public and local IP. Using this information, you can determine the device location and contact the user to collect the device. When collected, mark the device as found in the console.

**Flag an unreturned device as missing**

To flag a device as missing:

1. In the **Assets** area, select one or more devices (maximum: 100 devices) from the **All Devices** view.
2. Expand the menu and select **Report Missing or Stolen**.

3. In the dialog, click **Track Missing Device**.

4. In the dialog, specify the email addresses of those who should be notified when the device calls in. Separate email addresses by pressing **Enter** on the keyboard. Email addresses can include non-console users.

5. Click **Save**.

When a missing device comes online and calls in, a notification will be sent to the specified email addresses.
The notification email provides a link to the Missing Devices view in the console. This view is discussed further in the Monitor section.

Mark a missing device as found

When you have collected a missing device, mark it as found:

1. In the Assets area, select one or more devices from the All Devices view or Missing Devices view.
2. Expand the menu and select Report Found.
Freeze missing devices

TIMELINE: 5 DAYS AFTER THE DEVICE COLLECTION PERIOD

If a missing device does not call-in, freeze it to display a full-screen message. The user is unable to bypass the message to use the device.

The steps to follow may not apply if you are using the alternate version of device freeze. If you’re using the alternate version, follow the steps provided in the Help to submit an on-demand freeze request.

To freeze devices:

1. In the Assets area, select one or more devices from the All Devices view or Missing Devices view.
2. Click Freeze.

   You are taken to the Request Device Freeze page.

3. On the page, complete each of the sections as follows:
   i. Request Authorization Code: Click Request Code.
      The authorization code is sent to the email address associated with your console login. You are required to provide this code later.
   ii. Device Freeze Request Name: Name your device freeze request. This name appears in reports.
   iii. Select Devices: Ignore this section since you have already selected your devices.
   iv. Select a Message: Create a device freeze message or select an existing message from the list.
   v. Schedule Freeze Date: Select On next agent call.
      This will freeze the selected devices on their next call-in.
   vi. Select a Passcode Option:
      • Select Code Length: Specify your preferred unfreeze code length.
      • Passcode Options: Select Generate a different random passcode for each device.
   vii. Email Notification: To receive freeze status notifications, provide your email address in the field and select the checkbox.
   viii. Select whether a Reboot is to be Forced: Select Force reboot before freezing device (Windows devices only).
      This logs the user out of the device before the device freeze takes effect.
   ix. Consent to Install Software: Select the checkbox to consent to the terms.

4. Click Submit.
Monitor

TIMELINE: ONGOING. AT YOUR DISCRETION.

In the Monitor phase, use the Missing Devices view and Device Freeze Summary report to maintain visibility into your unreturned Chromebooks.

**Missing Devices view**

When missing devices call in, you will receive a notification email with a link to the Missing Devices view. However, you can access this view at any time to check the status of your missing devices.

To view details about your missing devices:

1. In the **Assets** area, click **Missing Devices** from the sidebar of the **Devices** section.

You are provided with details that can help you with retrieving devices.

**Device Freeze Summary report**

Use the Device Freeze Summary report to identify whether devices have been successfully frozen.

The steps to follow may not apply if you are using the alternate version of device freeze. If you’re using the alternate version, follow the steps provided in the **Help**.

To run the Device Freeze Summary report:

1. In the **Settings** area, click **Device Freeze** from the sidebar.
2. Select **Device Freeze Summary Report** from the sidebar.

3. On the page, specify the time period for when the freeze requests were made.

4. Specify the freeze request statuses that you are interested in. These are most commonly used in device collection:
   - Select **Freeze Requested** to see devices that have not come online to process the freeze request
   - Select **Frozen by Request** to see devices that have been successfully frozen
5. Click **Show Results**.

You are provided with a report that includes device information, and device freeze details.

---

**What’s Next?**

With the assistance of the Absolute console, you are more easily able to manage the phases of the device collection process.

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](#).
ABOUT ABSOLUTE
Absolute empowers more than 12,000 customers worldwide to protect devices, data, applications and users against theft or attack — both on and off the corporate network. With the industry’s only tamper-proof endpoint visibility and control solution, Absolute allows IT to enforce asset management, endpoint security, and data compliance for today’s remote digital workforces. Patented Absolute Persistence™ is embedded in the firmware of Dell, HP, Lenovo, and 26 other manufacturers’ devices for vendor-agnostic coverage, tamper-proof resilience, and ease of deployment. See how it works at absolute.com and follow us at @absolutecorp.