



USER GUIDE

Device Collection Guide:

An Absolute Guide to Successfully Reclaiming
Your Devices with Ease

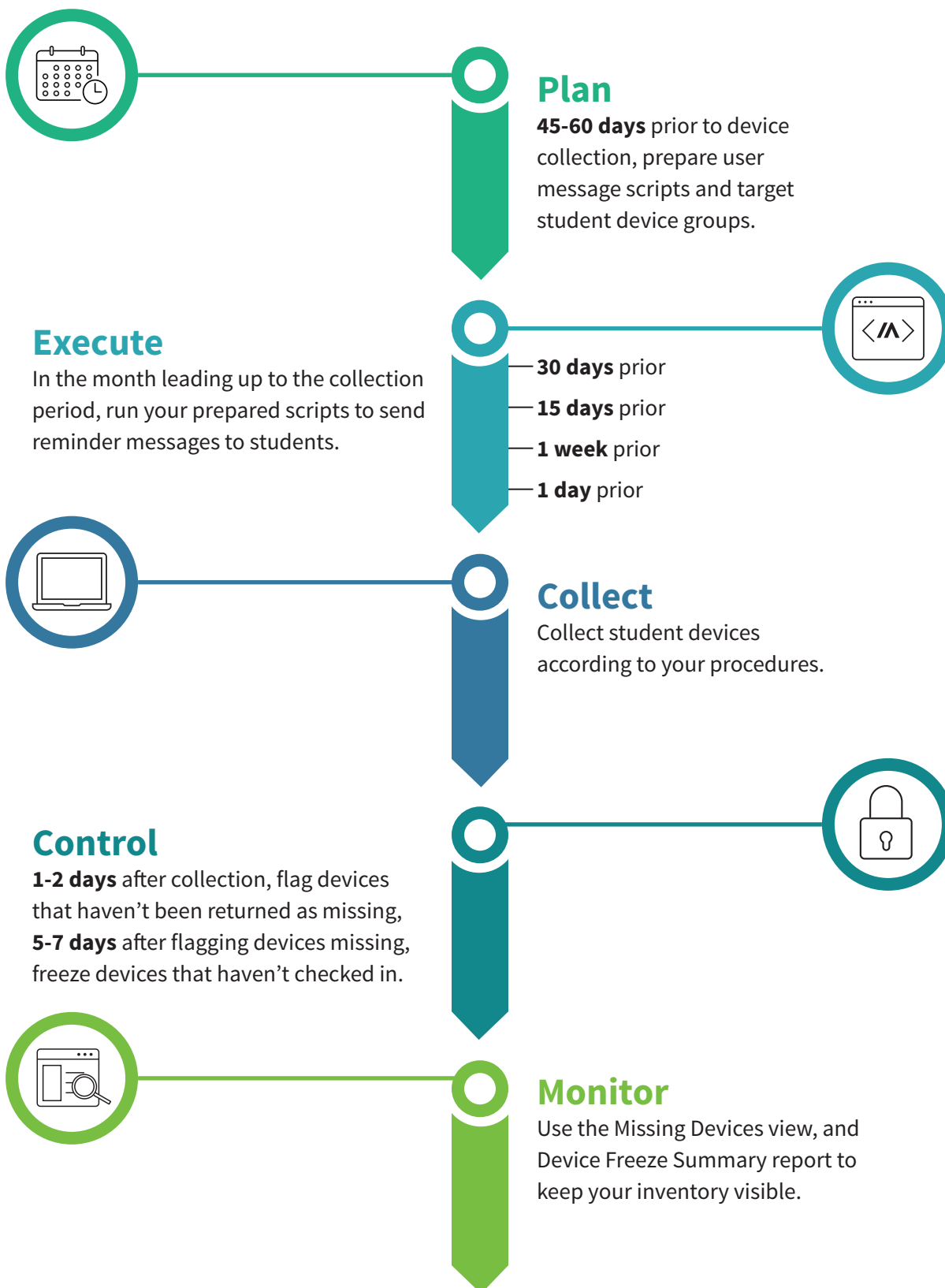
//ABSOLUTE®



CONTENTS

Summary	3
Plan	4
Execute	4
Collect	7
Control	8
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 organization's devices. Here is a summary:





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:

- Prepare the pre-built Reach script outlined in the Execute section.
- Create device groups (e.g. by school, 1:1 program, etc.) so that you can target specific return instructions to devices in the Execute phase.
- Coordinate with your colleagues for the Collect phase.
- Prepare device freeze messages for unreturned devices for the Control phase.

Execute



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

In the Execute phase, remind users about device collection and provide return instructions. Absolute Reach supports you in this task. This feature allows you to deploy PowerShell and Bash scripts to your Windows and Mac devices, respectively.

Run the Device Reclamation script to display return instructions

Run the pre-built Device Reclamation script from the Reach Script Library that prompts targeted devices to display return instructions in the users' default internet

browser. You will specify the return details such as location, collection date, and more before the script is executed.

To increase the likelihood of device returns, Absolute recommends that you run the script 30 days, 15 days, 1 week, and 1 day before device collection begins.

Here is an example of how the return instructions may appear to your users when the script is executed:



Device Return Notice

**Please be aware that you are in possession
of a device that must be returned
by June 1st**

Please return the device
to the following address:

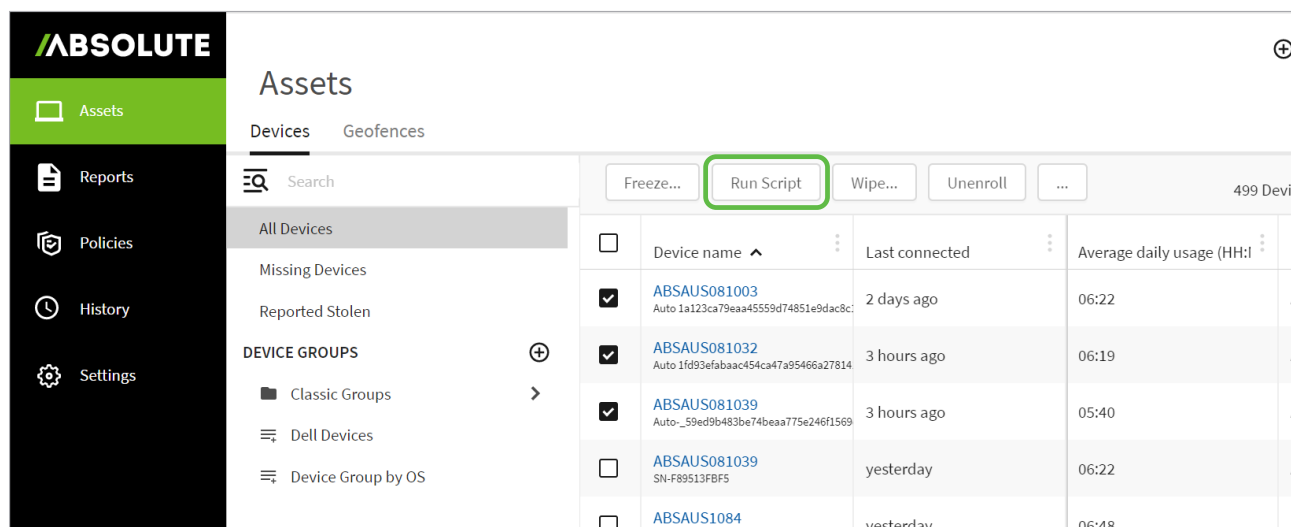
**1234 Funny Road, Apricot Town,
Maryland 12345**

If you have questions or issues returning
your device, please contact the
following individual:

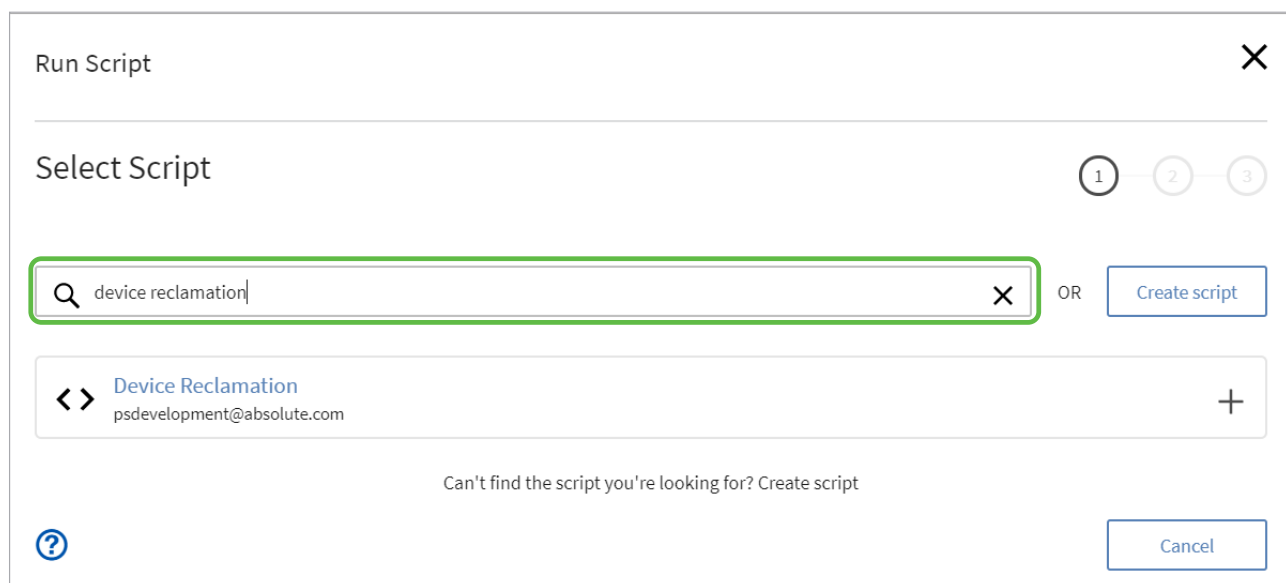
**Jane Doe
123-555-2213**

To run the pre-built script on your devices:

1. In the **Assets** area, select one or more devices from the **All Devices** view. You can use filters to target a specific device group.
2. Click **Run Script**.



3. In the dialog, type **Device Reclamation** in the field to search the Script Library.



4. Select **Device Reclamation** from the search results and click **Select Script**.

5. In the dialog, provide return instruction details in the fields. This includes Date, Address, Contact, and Phone. Optionally, include a logo.

Device Reclamation

End user message is displayed in users default browser with information about returning a device that is due to be returned.

Windows Mac

Script Variables ⓘ

.SYNOPSIS Launches HTML page in the users default browser with provided values for returning devices.

.DESCRIPTION This script launches an HTML template in a browser with filled in values for information about how

.NOTES This script must be run with logged in user rights.

Date

Required

Date that the devices should be returned by

Address

Required

Address for the devices to be returned to

Contact

Required

First and last name of person to contact for questions/issues during return of devices

Phone

Required

Phone number to contact for questions/issues during return of devices

Logo

Logo image link. Logo image should be 250x50 pixels in dimensions.

6. Under *Advanced Configuration Options*, specify these settings:

- **Rights:** Run with logged in user rights
- **Display Mode:** Hidden
- **Run Condition:** User is signed in
- **Maximum Run Time:** 10 Minutes

7. Ensure that you complete both the *Windows* and *Mac* sections, if applicable.

Device Reclamation

End user message is displayed in users default browser with information about returning a device that is due to be returned.

Windows Mac

8. Click **Next**.

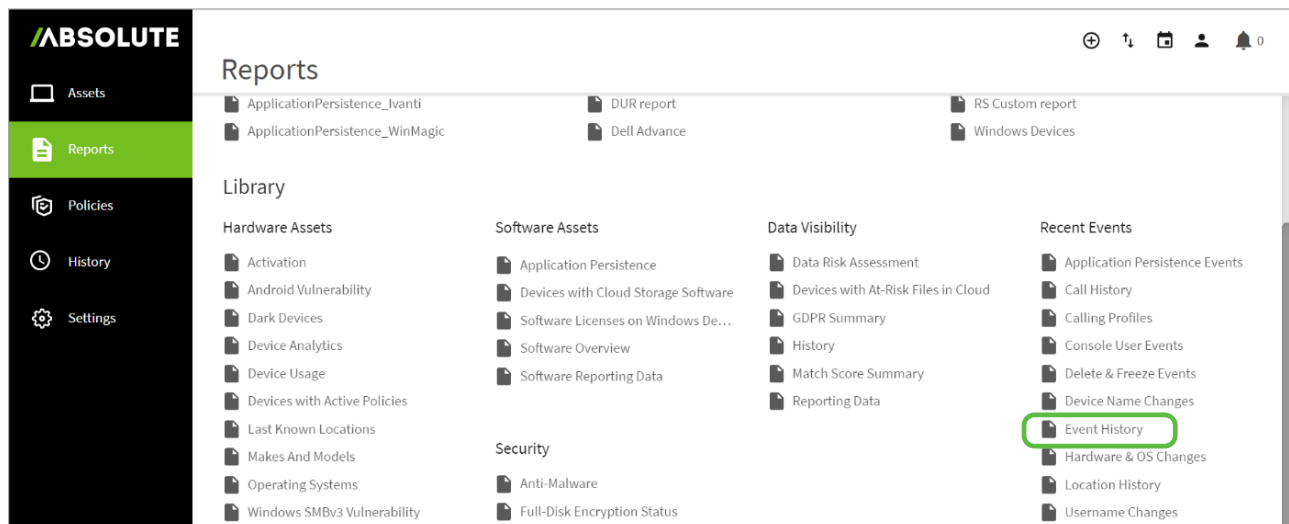
9. Confirm your devices. Click **Run Script**.


Check the status of executed scripts

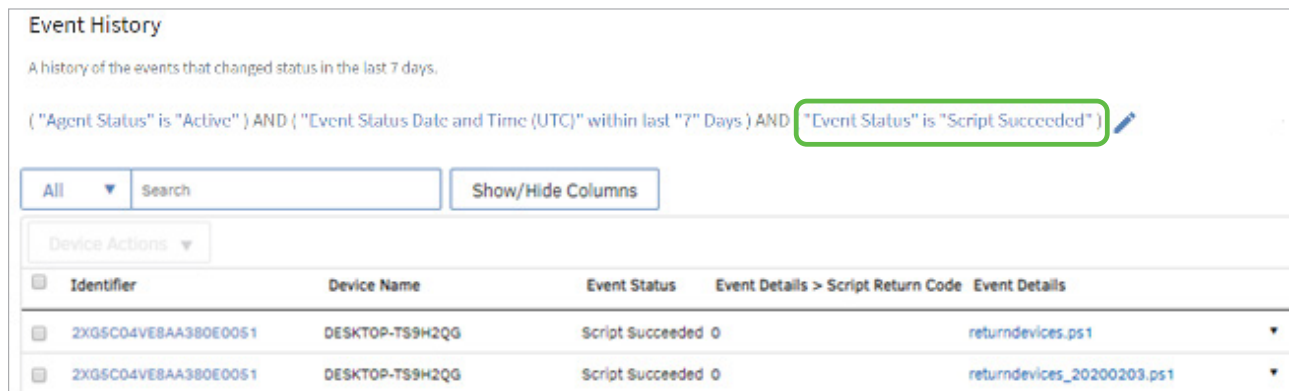
Use the Event History Report to check the status of your executed scripts.

To review this report:

1. In the **Reports** area, click **Event History** under **Recent Events**.



2. Click  to modify the Event Status variable in the filter to **Event Status is Script Succeeded**.



The report will show devices that have successfully executed the Device Reclamation script.

Collect



In this phase, collect devices according to your organization's procedures.



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


Track missing devices

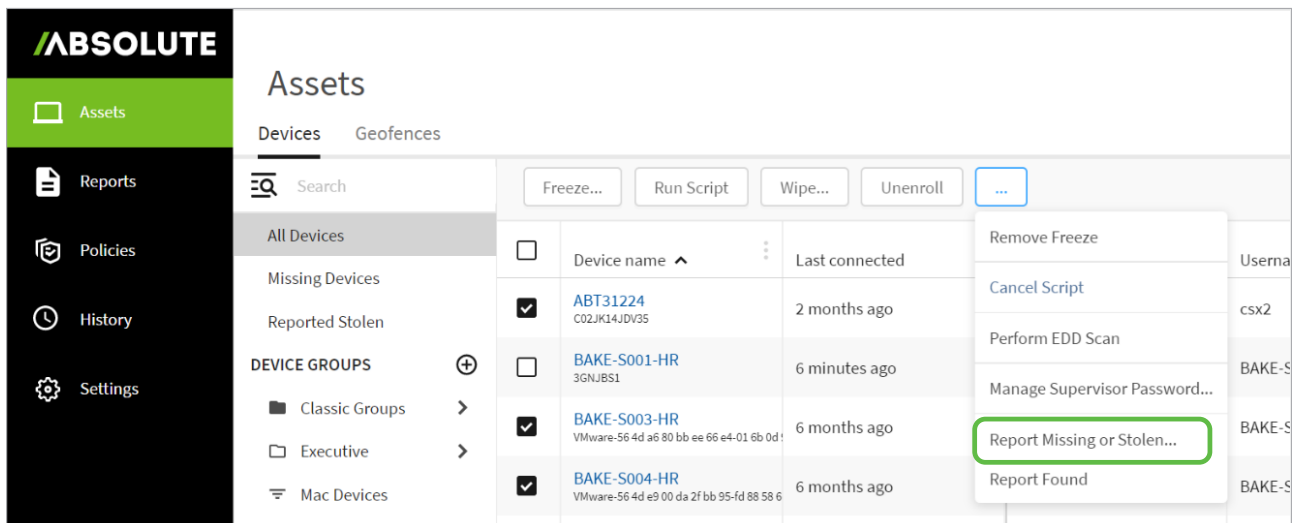
TIMELINE: 1-2 DAYS AFTER THE DEVICE COLLECTION PERIOD

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

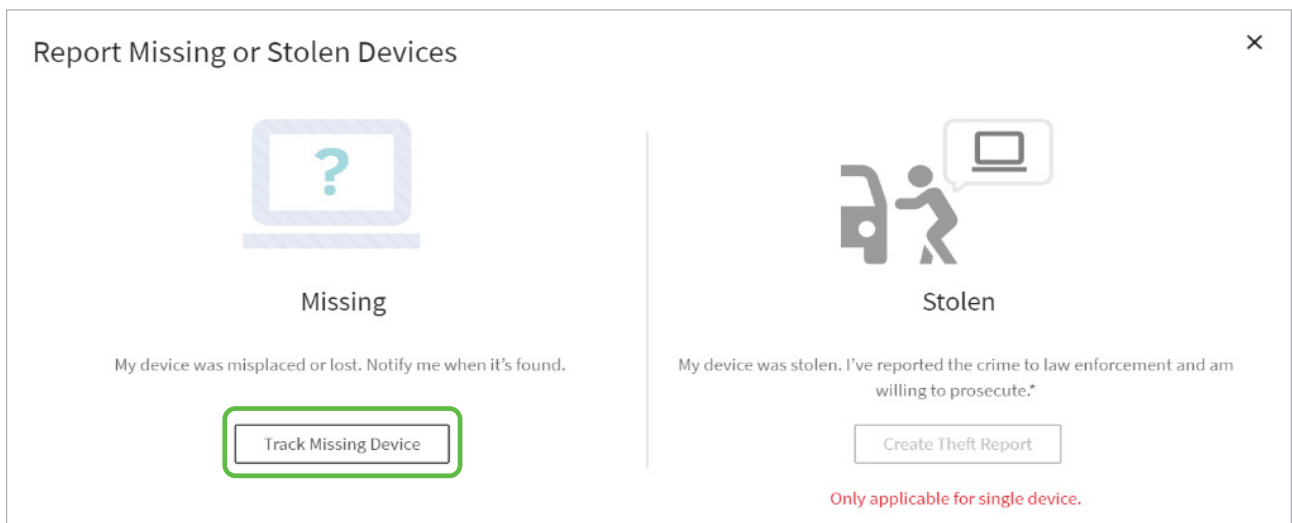
To flag a device as missing:

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**.



The screenshot shows the Absolute console interface. On the left is a sidebar with navigation options: Assets (selected), Reports, Policies, History, and Settings. The main area is titled 'Assets' and has tabs for 'Devices' and 'Geofences'. Under 'Devices', there's a search bar and a list of device groups: All Devices, Missing Devices, and Reported Stolen. Below these are 'DEVICE GROUPS' including Classic Groups, Executive, and Mac Devices. A table of devices is displayed with columns for checkboxes, Device name, and Last connected. A context menu is open over the table, showing options like 'Remove Freeze', 'Cancel Script', 'Perform EDD Scan', 'Manage Supervisor Password...', 'Report Missing or Stolen...' (highlighted with a green box), and 'Report Found'.

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



The screenshot shows a dialog box titled 'Report Missing or Stolen Devices'. It has two main sections. The left section is for 'Missing' devices, featuring a laptop icon with a question mark and the text 'My device was misplaced or lost. Notify me when it's found.' Below this is a button labeled 'Track Missing Device' which is highlighted with a green box. The right section is for 'Stolen' devices, featuring an icon of a person running with a laptop and the text 'My device was stolen. I've reported the crime to law enforcement and am willing to prosecute.*' Below this is a button labeled 'Create Theft Report'. At the bottom right, there is a red note: 'Only applicable for single 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.

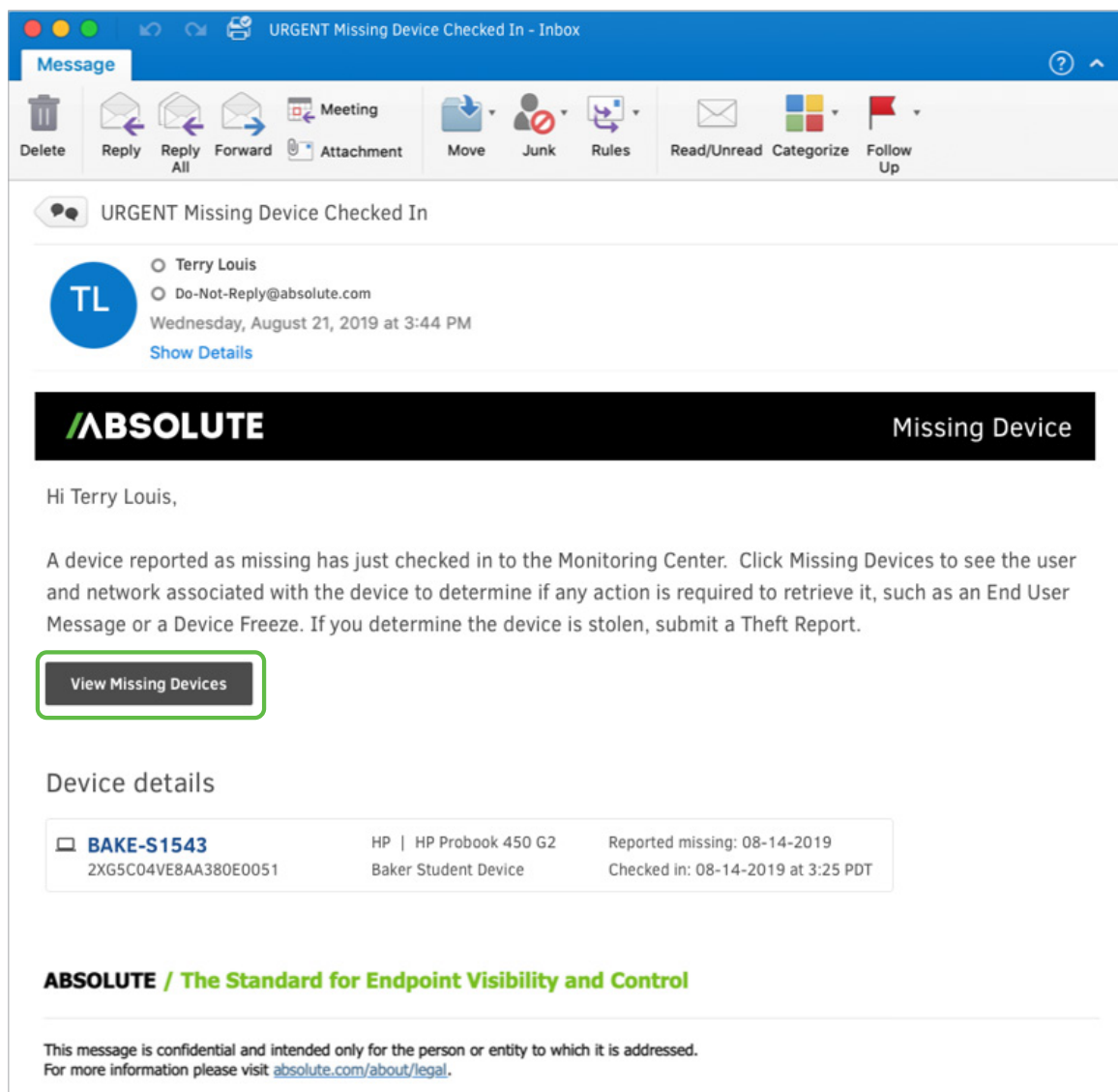


The dialog box is titled "Report Missing Devices" with a close button (X) in the top right corner. Below the title, it says "Track these 3 devices" and "Notify me when they check in". There is a text input field labeled "Email" containing two email addresses: "psmith@absolute.com" and "tjones@absolute.com", each followed by a small 'x' icon to indicate removal. A third empty input field is to the right. At the bottom left is a help icon (question mark in a circle), and at the bottom right is a "Save" button.

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.

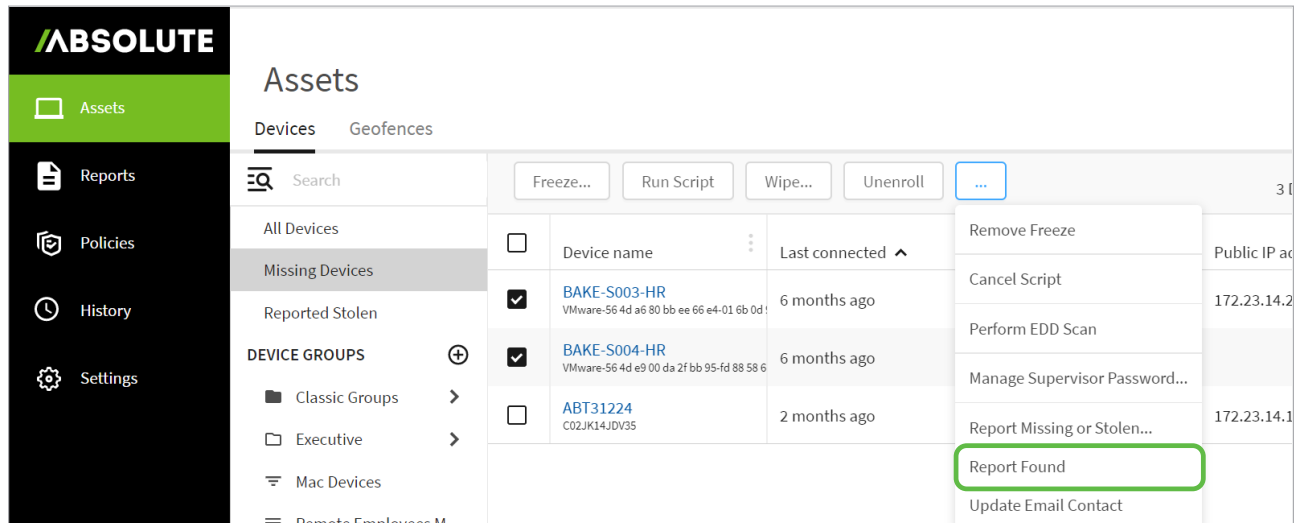


The screenshot shows an email client interface. The subject line is "URGENT Missing Device Checked In - Inbox". The email header shows it's from "Terry Louis" (TL) to "Do-Not-Reply@absolute.com" on Wednesday, August 21, 2019 at 3:44 PM. The email body has a black header with the "ABSOLUTE" logo and "Missing Device". The text says: "Hi Terry Louis, A device reported as missing has just checked in to the Monitoring Center. Click Missing Devices to see the user and network associated with the device to determine if any action is required to retrieve it, such as an End User Message or a Device Freeze. If you determine the device is stolen, submit a Theft Report." Below this is a button labeled "View Missing Devices" which is highlighted with a green border. The "Device details" section shows: "BAKE-S1543" (ID: 2XG5C04VE8AA380E0051), "HP | HP Probook 450 G2" (Baker Student Device), and "Reported missing: 08-14-2019" (Checked in: 08-14-2019 at 3:25 PDT). The footer includes the "ABSOLUTE / The Standard for Endpoint Visibility and Control" logo and a confidentiality disclaimer.

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

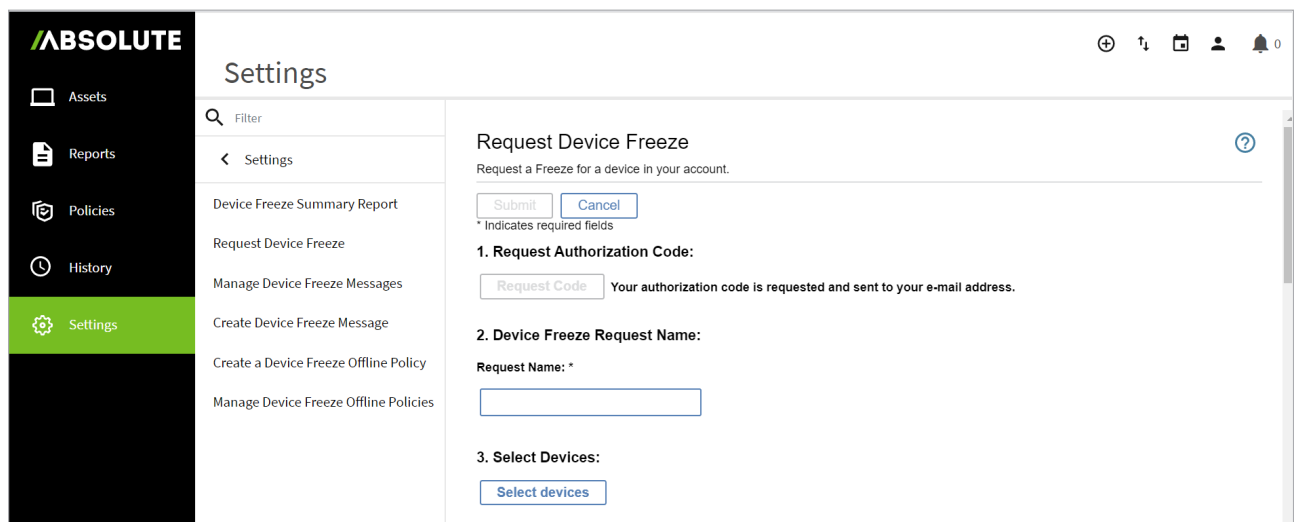
If a missing device does not call-in, freeze it to display a full-screen message. The user is unable to bypass the message to use the device.

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 devices.

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.

The screenshot shows the 'Assets' section of the Absolute software interface. The left sidebar has a green header with the Absolute logo and a 'Missing Devices' button highlighted with a green box. The main content area is titled 'Assets' and has tabs for 'Devices' and 'Geofences'. Below the tabs is a search bar and filters for 'Agent status' (Active) and 'Missing status' (Missing). A table displays the details of missing devices. The table has columns for Device name, Last connected, Username, Public IP address, Local IP address, and MISSING Reported date. One device is listed: ABSAUS081003, last connected 2 days ago, with username ABS/crawfordv and IP addresses 109.252.118.130 and 193.168.1.78. The reported date is Jan 29, 2020, 12:06 PM PST.

Device name	Last connected	Username	Public IP address	Local IP address	MISSING Reported date
ABSAUS081003 <small>Auto 1a1230ca79eaa45559d74851e9d9dc8c</small>	2 days ago	ABS/crawfordv	109.252.118.130	193.168.1.78	Jan 29, 2020, 12:06 PM PST

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

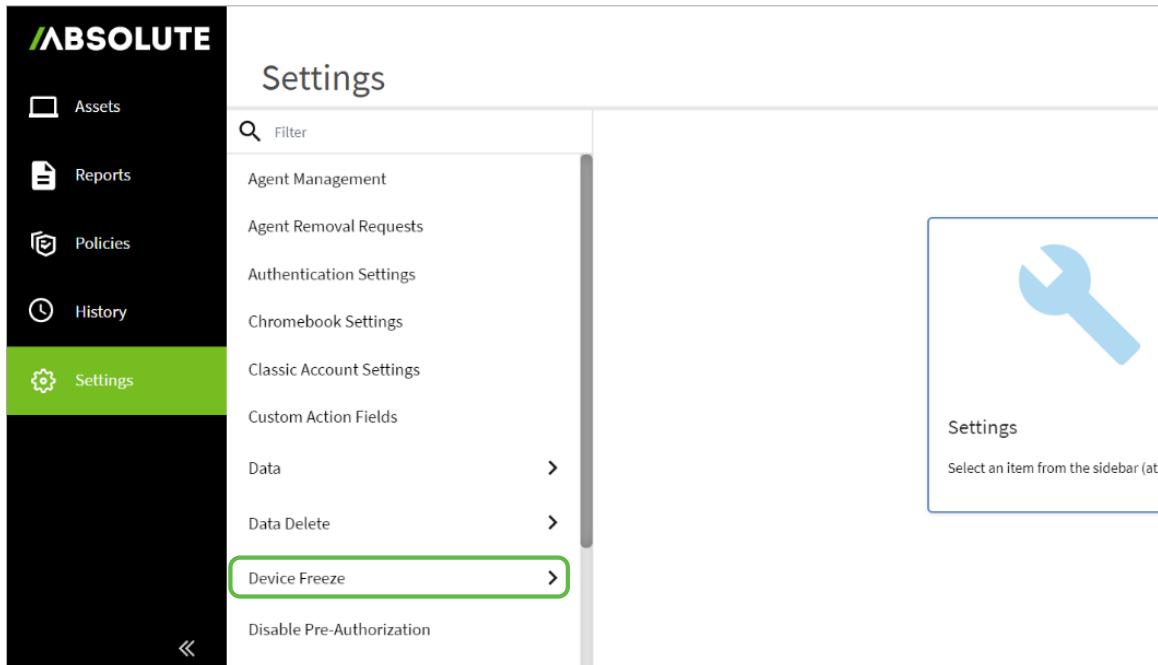
Device Freeze Summary report

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.

Device Freeze Summary Report

View a list of devices for which a Device Freeze request or offline policy exists.

Search Criteria

Show all Devices where...

the Group is:

and the field: is or contains

and the Request Name or Policy Name is or contains:

and the Requested Date ☒ in the last days [?](#)

☐ between and

Note - only 1 year of data is stored online.
The greater the date range, the longer it may take to generate results.

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

and the Device Freeze Status is:

<input checked="" type="checkbox"/> Freeze Requested	<input checked="" type="checkbox"/> Frozen By Request
<input checked="" type="checkbox"/> Unfreeze Requested	<input checked="" type="checkbox"/> Frozen By Policy
<input checked="" type="checkbox"/> Request Cancelled	<input checked="" type="checkbox"/> Unfrozen With Agent Call
<input checked="" type="checkbox"/> Pending	<input checked="" type="checkbox"/> Unfrozen With Passcode
<input type="checkbox"/> Policy Assigned	<input checked="" type="checkbox"/> Processing
<input type="checkbox"/> Freeze Scheduled	<input checked="" type="checkbox"/> Frozen by Scheduled Freeze
<input type="checkbox"/> Scheduled Freeze Pending	

5. Click **Show Results**.

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

The screenshot shows the Absolute console interface. On the left is a sidebar with navigation links: Assets, Reports, Policies, History, and Settings (highlighted). The main area is titled 'Settings' and contains a 'Device Freeze Summary Report' section. This section includes a 'Request Device Freeze' button and a 'Manage Device Freeze Messages' button. Below these is a table of device freeze requests.

Identifier	Request ID	Request Name /Policy Name	Make	Model	Serial Number	IMEI	Subscriber Id	Phone Number	Requested on	R
1KA2UE9R09AA2YK20023	cdc56fc3-5857-4777-ac78-11db563ce271	Device Freeze - Apr 20, 2020	VMware, Inc.	VMware Virtual Platform	VMWARE 56 4D E4 7F 8A 05 D1 60 C6 16 AF C0 A3 BB D				4/20/2020 9:35:52 AM	1
1KA2UE9R09AA2YK20023	15c8b0f-c4cd-4cdc-a362-0b951c79a836	Device Freeze - Apr 20, 2020	VMware, Inc.	VMware Virtual Platform	VMWARE 56 4D E4 7F 8A 05 D1 60 C6 16 AF C0 A3 BB D				4/20/2020 9:08:04 AM	1
1KA2UE9R09AA2YK20024	514feb2-	Device Freeze - Apr 20,	VMware,	VMware	VMWARE 56				4/20/2020	1

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](https://twitter.com/absolutecorp).



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