Regulatory & Compliance

Data Privacy Settings

Document Information

Code:	**CD-DPS**	Created by:	**Steve Dodson**
Version:	**2.1**	Approved by:	**Lars Sneftrup Pedersen**
Date:	**30 September 2025**	Confidentiality:	**Public**

Admin By Request
ZERO TRUST PLATFORM

Copyright © 2025 Admin By Request

All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement (NDA). The software may be used or copied only in accordance with the terms of those agreements.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the customer's stated use without the written permission of Admin By Request.

San Francisco, Florida
Wisconsin, New York
(+1) 262 299 4600

Denmark, Norway,
Germany, Benelux
(+45) 55 55 36 57

United Kingdom, Spain
Switzerland, France
(+44) 20 3808 8747

Sweden, Thailand
Finland, New Zealand
(+46) 31 713 54 04

sales@adminbyrequest.com | support@adminbyrequest.com | www.adminbyrequest.com

Table of Contents

1 Introduction

1.1 Personally Identifiable Information (PII)

At Admin By Request, we value privacy.

That is why we give you complete control over what **PII** is stored in your portal.

You can collect all personal data, such as user names, locations and contact details, or none at all, depending on your organization's privacy policies and preferences.

1.2 Privacy Settings

Admin By Request has a dedicated Privacy Settings page within the portal for this exact purpose: so that no **PII** is collected without your explicit say-so.

The Privacy Settings page is found in the portal, under **Settings > Tenant Settings > Privacy > PRIVACY** (see Item A in the "Appendix" on page 6).

From here, you can make all of the appropriate adjustments to what personal information is collected so that you can implement privacy for your organization as you see fit.

1.3 Scope

This document covers the **PII** that you have the option to collect and demonstrate where, within the portal, this information is displayed or omitted when you toggle each of the Privacy Settings **ON** or **OFF**.

1.4 Related Documents

This document may refer to, and should be read in conjunction with, the following:

- Commitments and responsibilities in ABR's Data Processing Agreement
- Support provisions in ABR's Terms and Conditions and Customer Support Services
- Collection, use and disclosure of personal data in ABR's Privacy Policy.

Refer also to ABR's Trust Center documents.

This document is available online:

Data Privacy Settings

2 Privacy Settings and Descriptions

2.1 Privacy Settings

The following list describes settings that you can disable or enable using the **ON / OFF** toggles next to each setting, along with their explanations:

- **Obfuscate user accounts**
  This setting obfuscates the true identity of your users by creating an alias for each of them in the form of a random 32-digit string to stand as their username, and by not collecting their email addresses or phone numbers. When you toggle this setting **ON**, the following three privacy settings: *Collect user names*, *Collect user email addresses* and *Collect user phone numbers*, will be automatically toggled **OFF** and cannot be turned back on while *Obfuscate user accounts* is enabled.

  KEY POINT
  Once this setting is toggled **OFF**, the three settings below it will not be toggled back **ON** automatically. You will need to do this manually for each one.

- **Collect user names**
  This setting collects the full name of each user.
- **Collect user email addresses**
  This setting collects the email address of each user.
- **Collect user phone numbers**
  This setting collects the phone number of each user.
- **Collect inventory**
  This setting collects a range of software and hardware inventory within the following categories:
  - Computer information
  - User information
  - System information
  - Hardware
  - Geographical location
  - Operating system
  - Fastest network adapter
  - Primary monitor

  In addition to the above inventory categories and corresponding data, a list of the software that is installed on each user's device is also collected and displayed, as well as a list of the local administrators on the device in question.
- **Allow geo-tracking**
  This setting maps the IP address of each user's device to a location using a public IP-to-location database. These device locations can then be viewed in Inventory and Reports within your portal, or in Google maps via Admin By Request.

2.2 Adjusting Privacy Settings

KEY POINT
When you adjust your Privacy Settings (enable or disable them using the **ON / OFF** toggles), nothing happens to existing data - the changes apply only to new data and not to data that has already been collected prior to the adjustment being made.

For example, if you have the *Collect user names* setting enabled and user X makes a request, their user name will be collected and displayed in all of the appropriate places within the Admin By Request portal.

If you then disable this setting, user X's user name will remain in all of the relevant locations for the request they made with this setting toggled **ON**, but all further requests by user X and others will no longer collect and display the user name.

2.3 Where Privacy Settings Data is Displayed

PII and personal data collected by Admin By Request is displayed within the following four pages in the user portal:

- **Requests**
- **Auditlog**
- **Inventory**
- **Reports**

See item B in the Appendix.

Data that is collected could appear in all or only some of those pages within your portal, depending on the data in question.

2.3.1 Default Privacy Settings

The Default Privacy Settings, i.e., the settings automatically enabled / disabled when you first implement Admin By Request, are as follows:

- Obfuscate user accounts - **OFF**
- Collect user names - **ON**
- Collect user email addresses - **ON**
- Collect user phone numbers - **ON**
- Collect inventory - **ON** [1]
- Allow geo-tracking - **ON**

See item C in the Appendix.

In the Appendix of this document, all screenshots of the Requests, Auditlog, Inventory and Reports pages have been taken with the default settings applied.

1. Refer to IMPORTANT note in section 3.1.5.

3 Omitting Data

3.1 Where Privacy Settings Data is Omitted

As mentioned, we leave it entirely up to you to decide what **PII** and other personal data is collected by Admin By Request.

This section details where data is omitted from Requests, Auditlog, Inventory and Reports in the portal when each Privacy Setting is disabled.

3.1.1 Obfuscate user accounts

Obfuscate user accounts relates directly to the user name, user email address and user phone number.

When this setting is toggled **ON**, the user name will be replaced by a random 32-digit string as part of the alias created for that user.

For example, an obfuscated user name could read: **98492bd400b87fa8c414d5074cbb062d**.

In addition to obfuscating the user name, the user's email address and phone number will not be collected.

When *Obfuscate user accounts* is disabled (toggled **OFF**), user identities will not have an alias created for them, so user names, email addresses and phones numbers can be collected and displayed as normal, provided these settings are enabled.

Toggling this setting affects data within the Requests, Auditlog and Inventory pages of the portal.

See items C, D, E & F in the Appendix.

3.1.2 Collect user names

When *Collect user names* is disabled, user names will be replaced with a random 32-bit string (as is the case for the user name when *Obfuscate user accounts* is enabled).

Toggling this setting affects data within the Requests, Auditlog and Inventory pages of the portal.

See items D, E & F in the Appendix.

3.1.3 Collect user email addresses

When Collect user email addresses is disabled, email addresses will not appear within Requests, Auditlog or Inventory.

Toggling this setting affects data within the Requests, Auditlog and Inventory pages of the portal.

See items D, E & F in the Appendix.

3.1.4 Collect user phone numbers

When *Collect user phone numbers* is disabled, email addresses will not appear within Requests, Auditlog or Inventory.

Toggling this setting affects data within the Requests, Auditlog and Inventory pages of the portal.

See items D, E & F in the Appendix.

3.1.5 Collect inventory

When *Collect inventory* is disabled, the Inventory page in the portal omits the related **PII** and personal data.

Devices will still appear in the Inventory page in the Computer column, but the Inventory left menu item is missing, along with the sections on that page:

- **Computer**
- **User**
- **System**
- **Hardware**
- **Geographical Location**
- **Primary Network Adapter**

See item F in the Appendix.

IMPORTANT
If you want to record device owners for endpoints, *Collect inventory* must be **ON**.

This is because there is no way to identify the device owner if no inventory data is collected. Therefore, if *Collect inventory* is **OFF** (portal menu **Settings > Tenant Settings > Privacy > PRIVACY**), setting *Lock device to owner* (portal menu **Endpoint Privilege Management > Settings > [OS] Settings > Lockdown > OWNER**) has no effect.

3.1.6 Allow geo-tracking

The *Allow geo-tracking* setting affects **PII** within the Inventory and Reports pages in the portal.

When disabled, users' IP addresses will not be mapped to their physical locations.

This means that in the Inventory page for a device, under **Geographical Location**, the *City*, *Country* and *Hour offset* fields will be omitted. The link "Show on Google Maps" will also be unavailable.

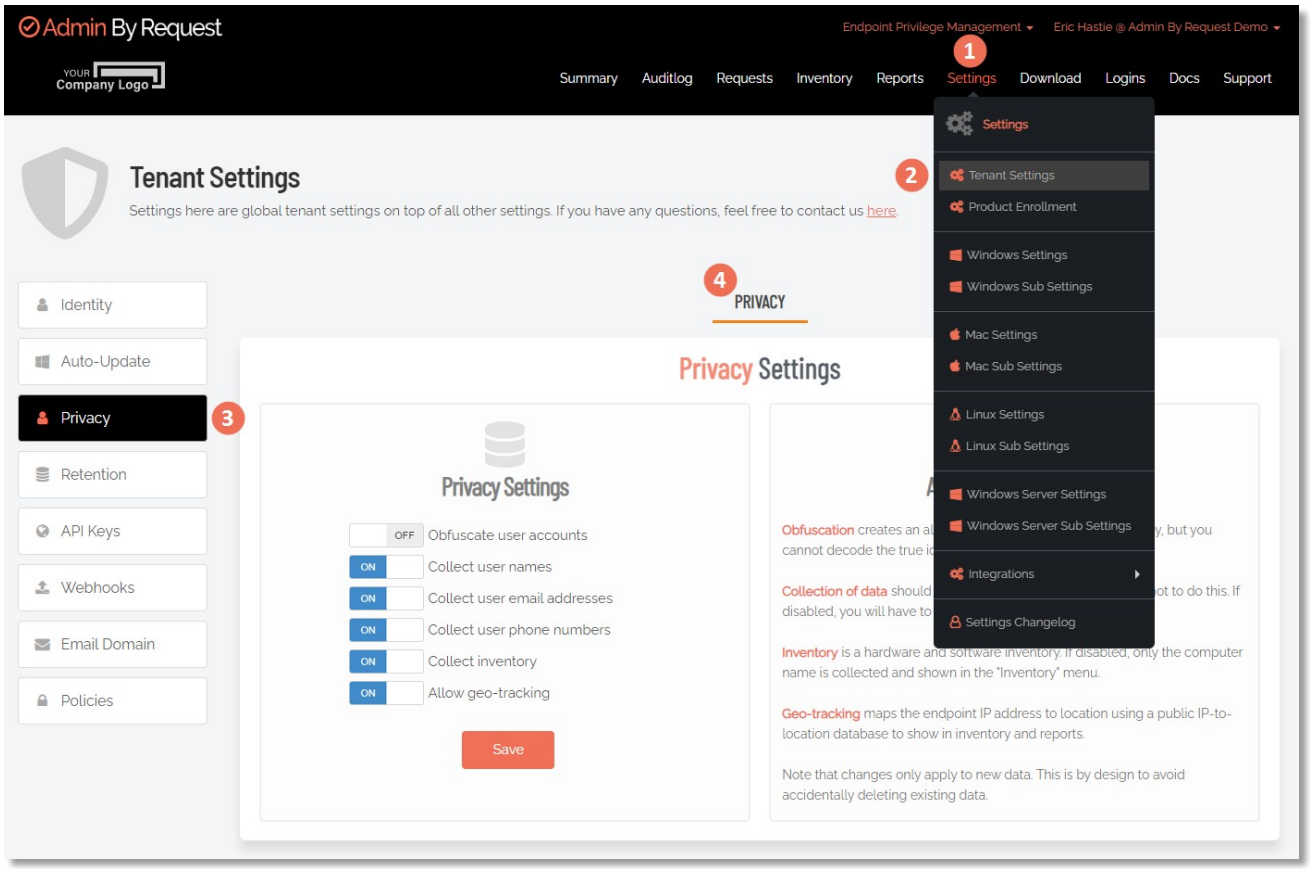
In the Reports page, under **Dashboard**, the "Where are my computers right now?" section does not display.

See items G & H in the Appendix.

4 Appendix

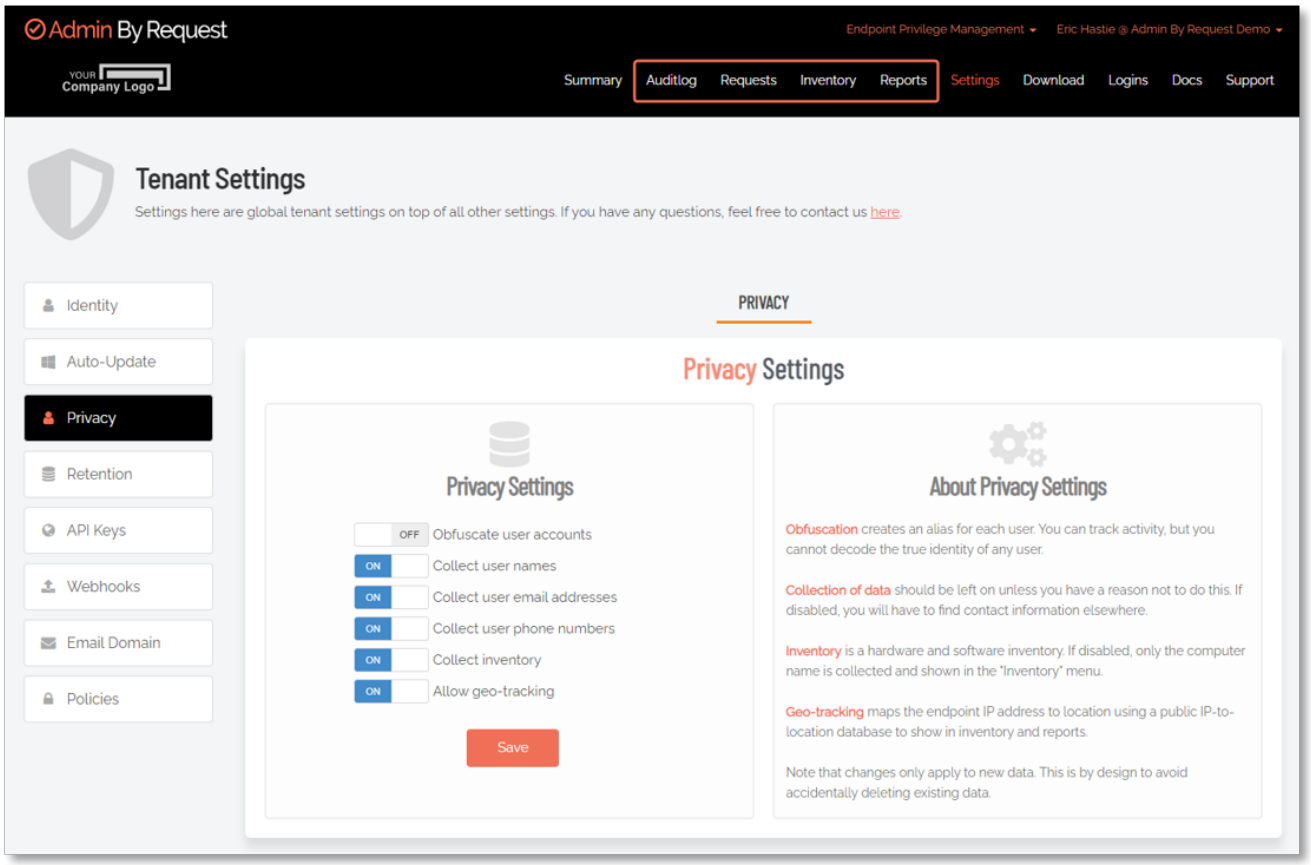
Item A: Navigating to the Privacy Settings page

Settings > Tenant Settings > Privacy > PRIVACY:



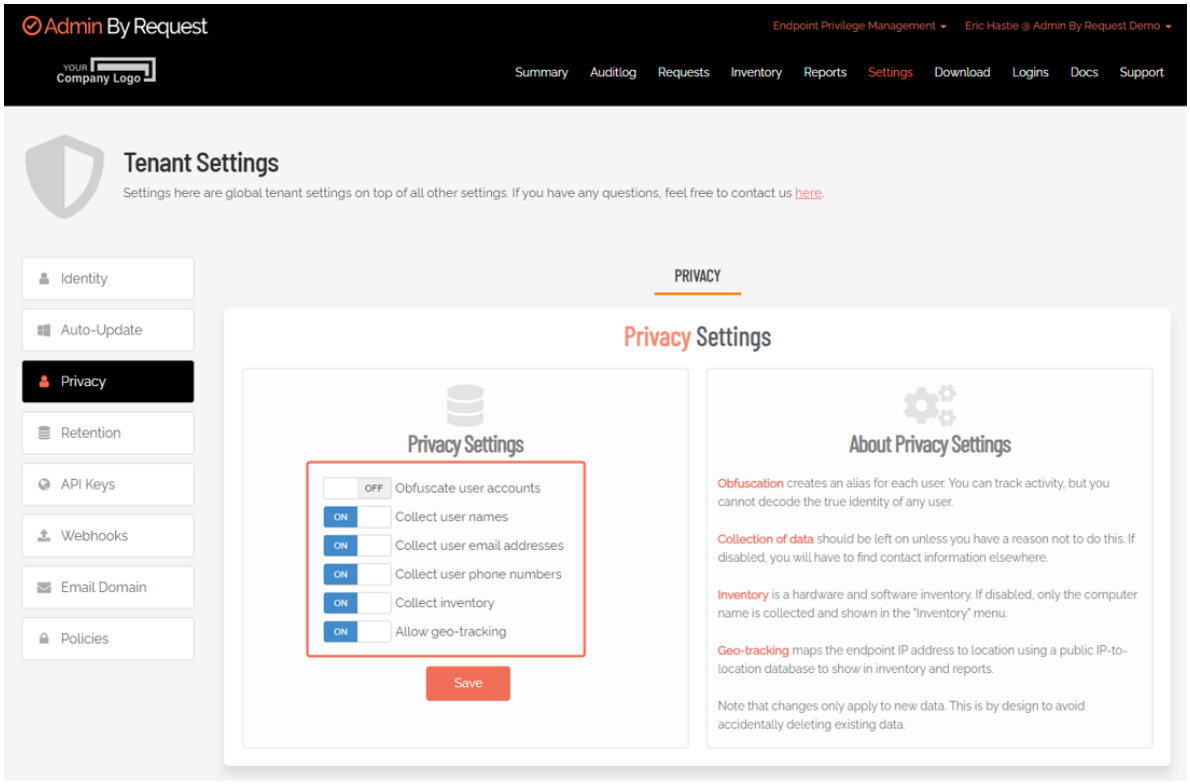
Item B: Admin By Request top menu

Pages that display data:

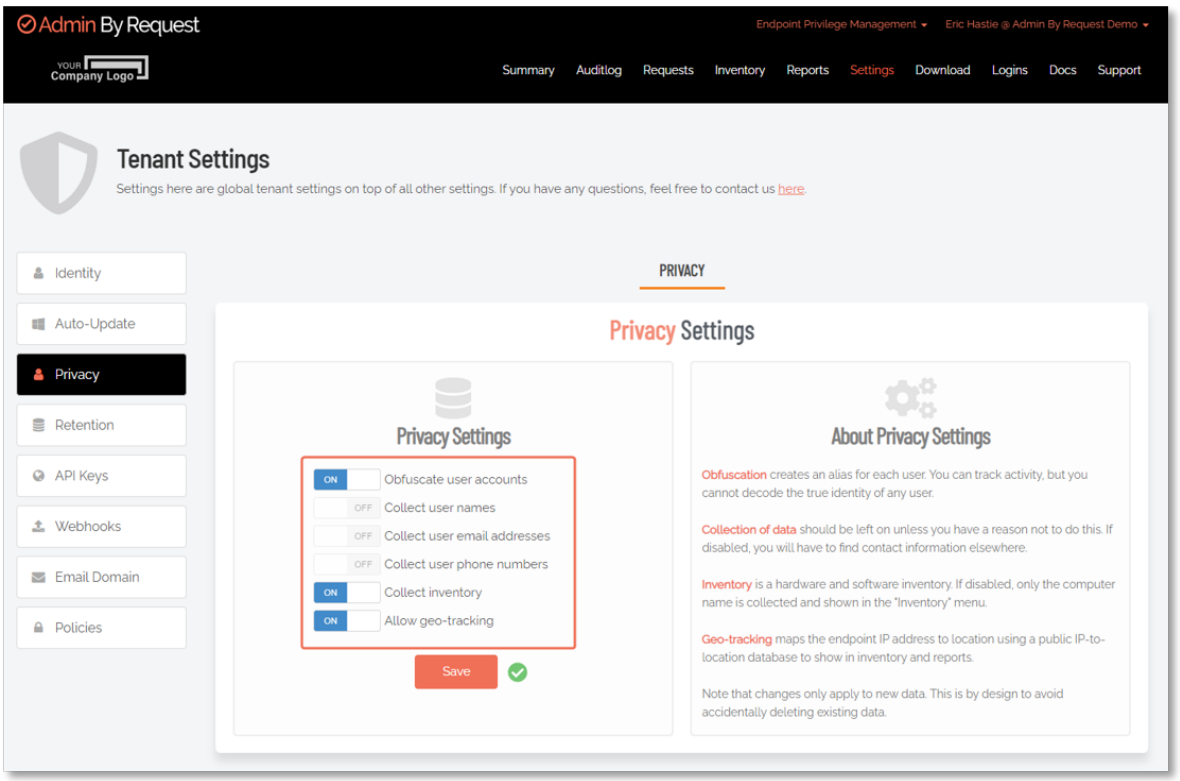


Item C: Privacy Settings

Default privacy settings:

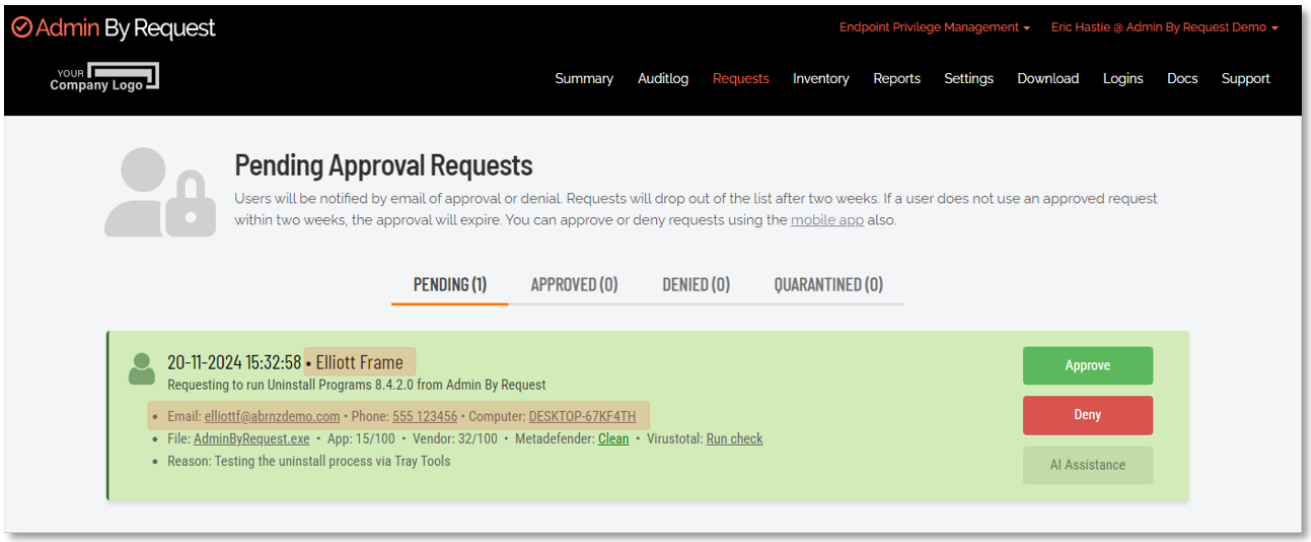


Obfuscate user accounts:



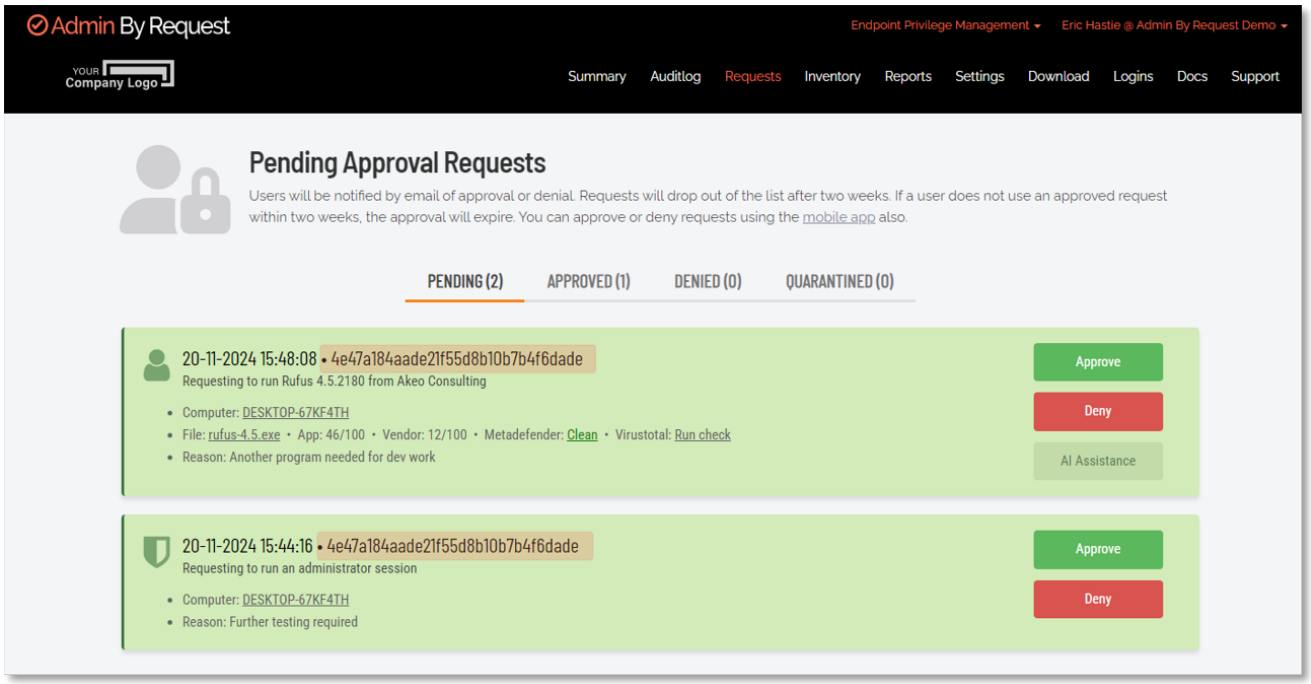
Item D: Requests

Default privacy settings:



Obfuscate user accounts:

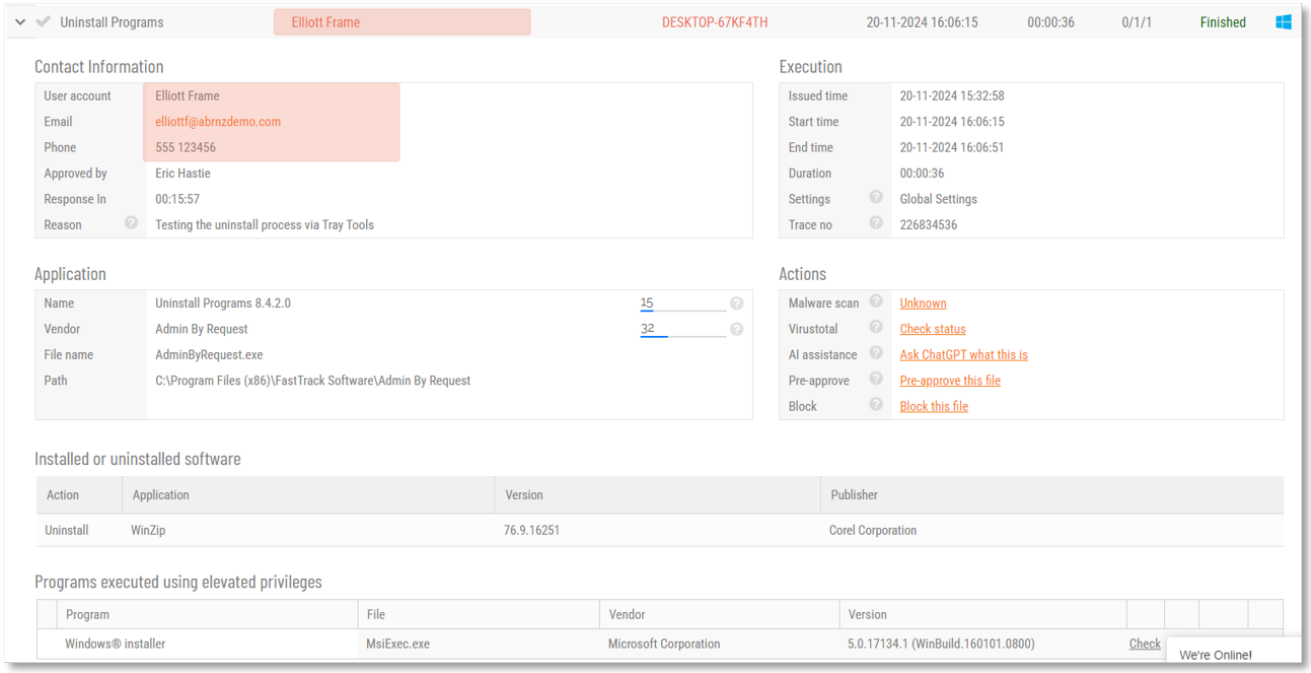
1. First request - RUN AS ADMIN (file **rufus-4.5.exe**)
2. Second request - ADMIN SESSION



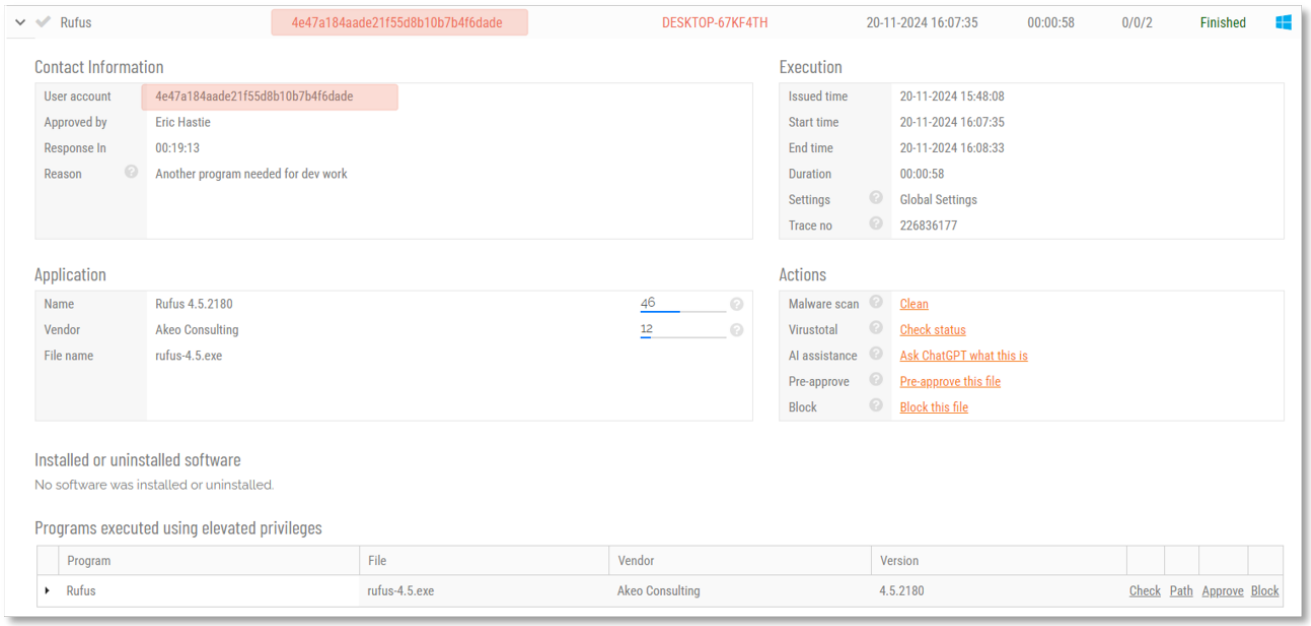
Item E: Auditlog

Select the "expand" arrow (**>**) to the left of an entry to drill-down.

Default privacy settings:



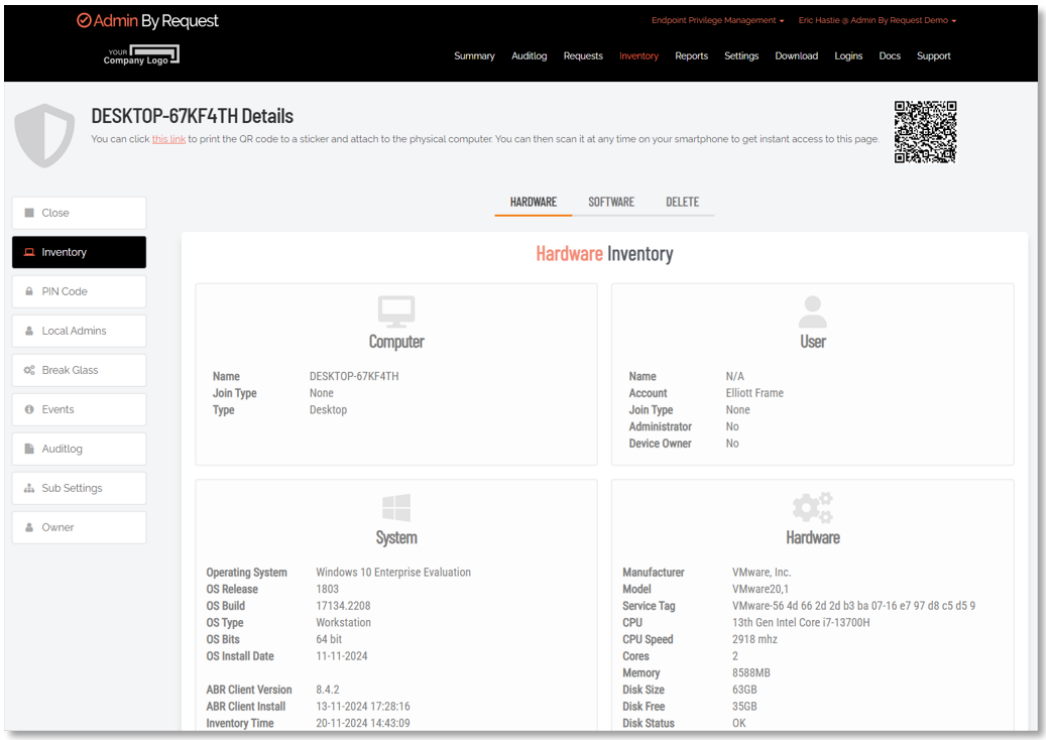
Obfuscate user accounts:



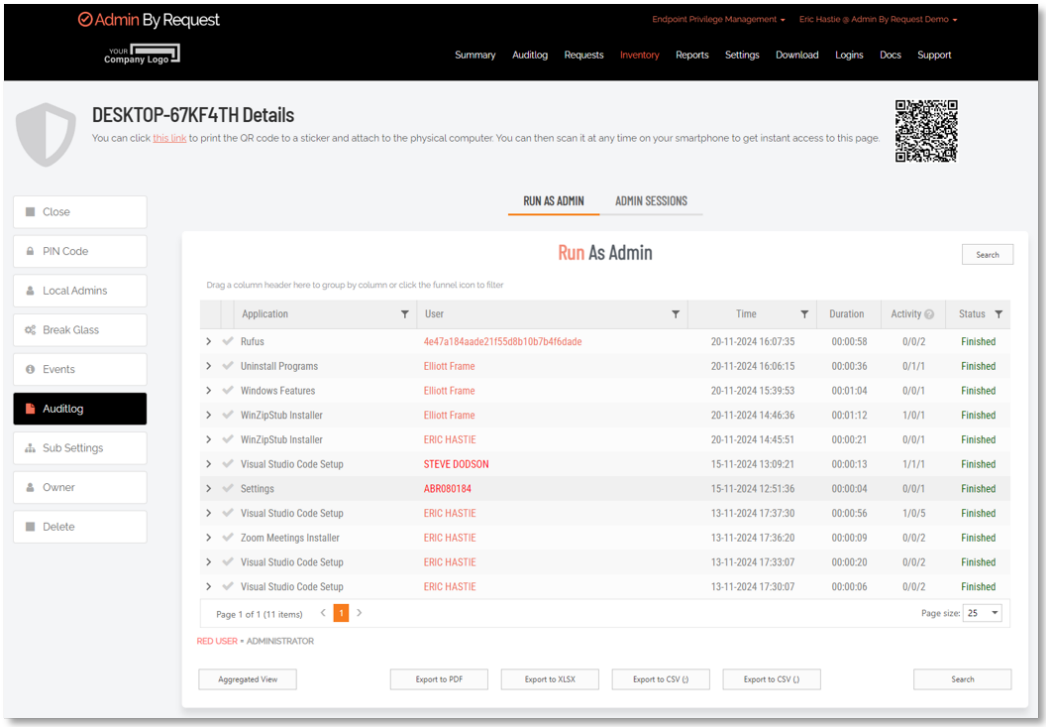
Item F: Inventory

Select either the "Computer name" link or the "Details" link for an entry to drill-down.

Default privacy settings:



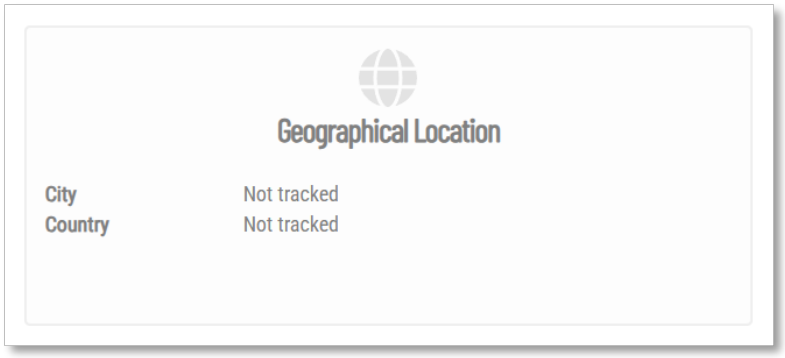
Collect inventory **OFF**:



Item G: Inventory (Geo-tracking)

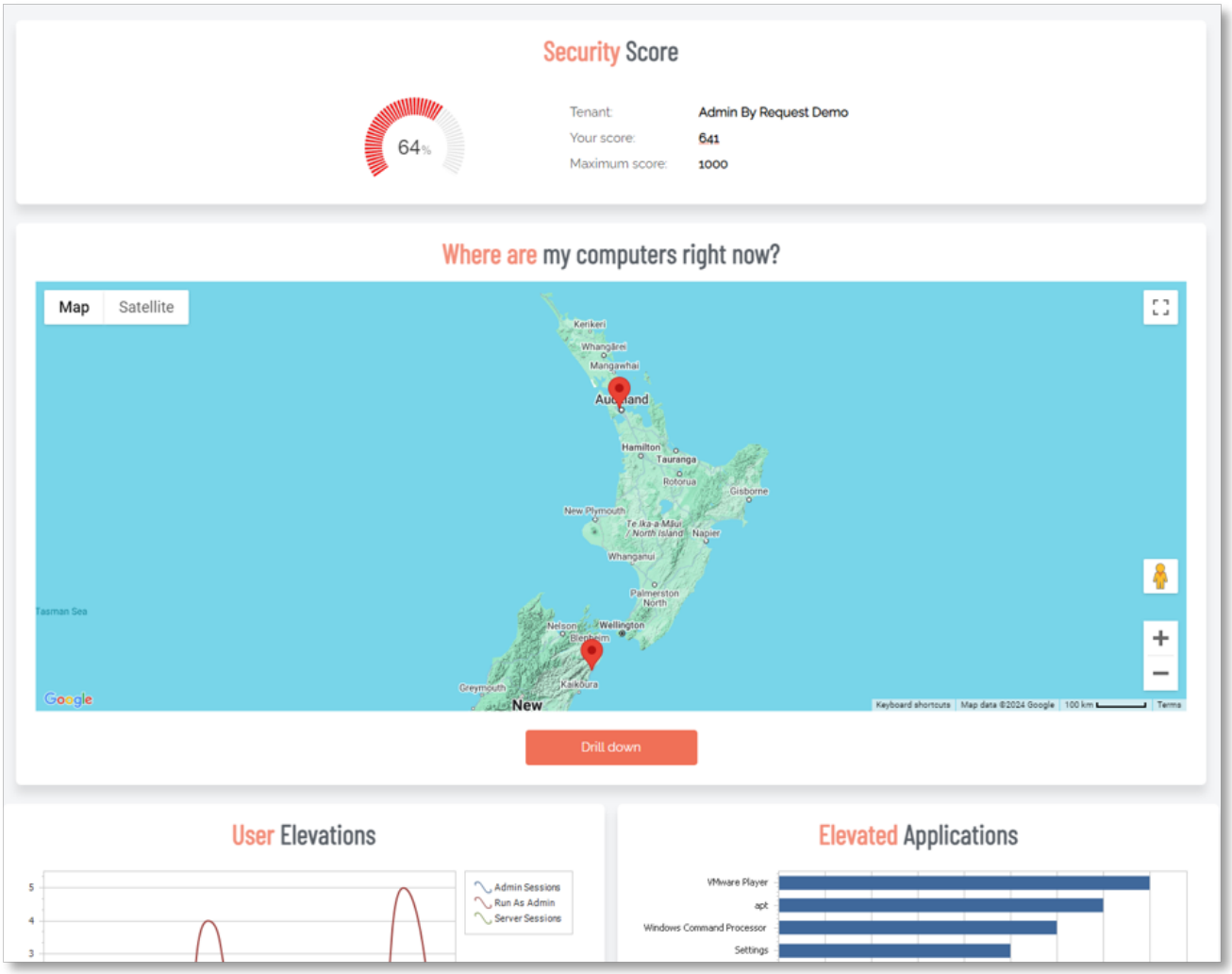
Default privacy settings:

Allow geo-tracking **OFF**:

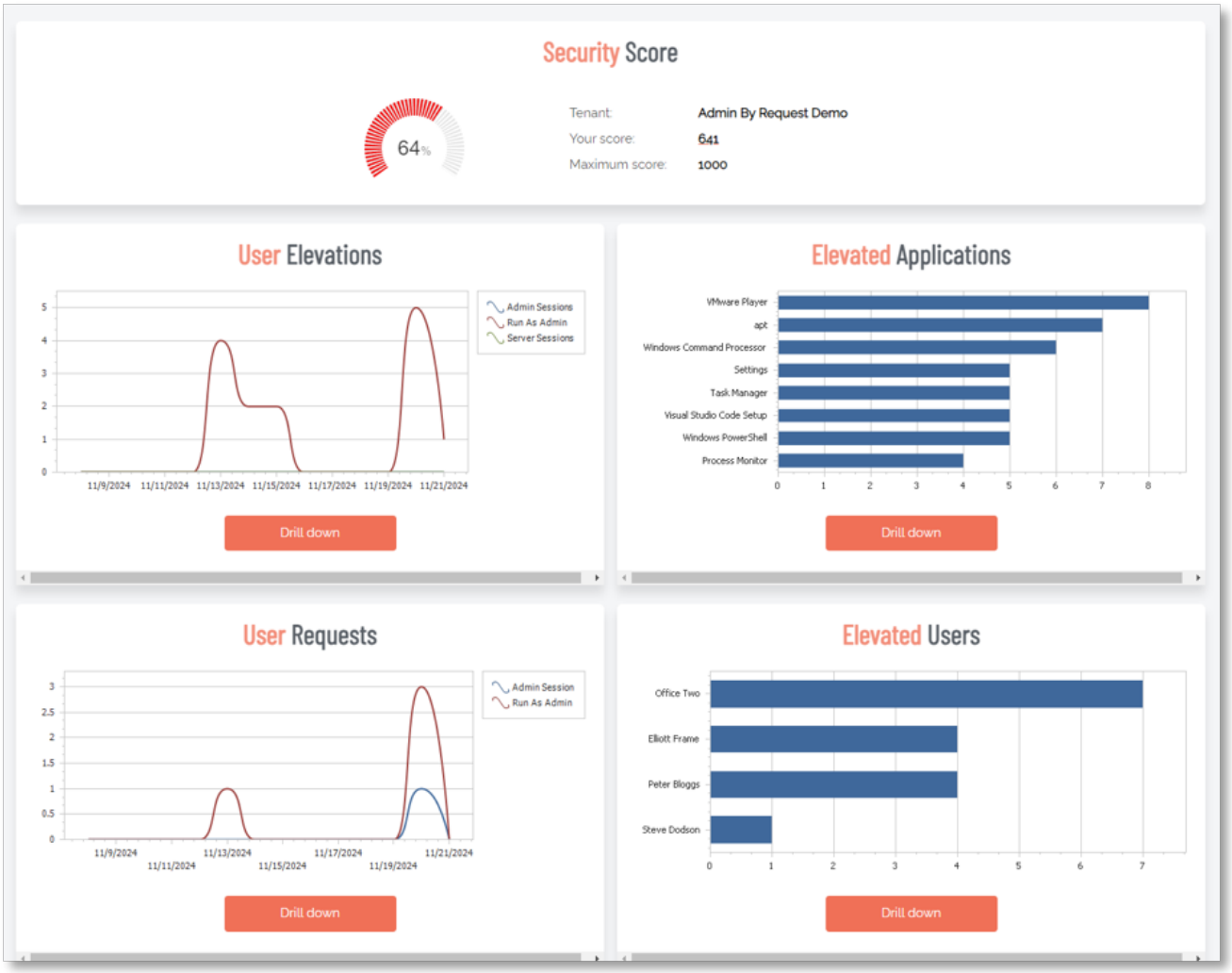


Item H: Reports > Dashboard

Default privacy settings:



Allow geo-tracking **OFF**:



5 Document History

Version	Author	Changes
25 March 2023 **1.0**	Sophie Alice Dodson	Initial document release.
15 November 2024 **1.1**	Steve Dodson	Incorporated v1.0 Data Privacy Settings PDF into Document Management System. Updated *Settings* paths to reflect new portal menu structure.
14 February 2025 **1.2**	Steve Dodson	Added *Privacy Settings*, *Scope* and *Reference* headings to chapter "Introduction". Updated styles so that headings in online pages have the same numbering as printable PDFs.
8 August 2025 **2.0**	Steve Dodson	Applied latest template, aligned with Terms & Conditions and Data Processing Agreement documents. Added IMPORTANT note about *Device Owner* dependence on *Collect Inventory* setting.
30 September 2025 **2.1**	Steve Dodson	Added Related Documents section to "Introduction".