

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

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
1.1	Personally Identifiable Information (PII)	1
1.2	Privacy Settings	1
1.3	Scope	1
1.4	Related Documents	1
2	Privacy Settings and Descriptions	2
2.1	Privacy Settings	2
2.2	Adjusting Privacy Settings	3
2.3	Where Privacy Settings Data is Displayed	3
2.3.1	Default Privacy Settings	3
3	Omitting Data	4
3.1	Where Privacy Settings Data is Omitted	4
3.1.1	Obfuscate user accounts	4
3.1.2	Collect user names	4
3.1.3	Collect user email addresses	4
3.1.4	Collect user phone numbers	5
3.1.5	Collect inventory	5
3.1.6	Allow geo-tracking	5
4	Appendix	6
	Item A: Navigating to the Privacy Settings page	6
	Item B: Admin By Request top menu	7
	Item C: Privacy Settings	8
	Item D: Requests	9
	Item E: Auditlog	10
	Item F: Inventory	11
	Item G: Inventory (Geo-tracking)	12
	Item H: Reports > Dashboard	13
5	Document History	15

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:

The screenshot displays the Admin By Request web application. The top navigation bar features the 'Settings' link, which is highlighted with a red circle and the number 1. A dropdown menu is open from 'Settings', showing various configuration options, with 'Tenant Settings' highlighted by a red circle and the number 2. The left sidebar contains a 'Privacy' link, highlighted with a red circle and the number 3. The main content area shows the 'Privacy Settings' page, which is highlighted with a red circle and the number 4. The page includes a 'Save' button and a list of settings to be configured.

Privacy Settings

- ☐ OFF Obfuscate user accounts
- ☒ ON Collect user names
- ☒ ON Collect user email addresses
- ☒ ON Collect user phone numbers
- ☒ ON Collect inventory
- ☒ ON Allow geo-tracking

Obfuscation creates an alias for user accounts, but you cannot decode the true identity.

Collection of data should be enabled. If disabled, you will have to manually collect data.

Inventory is a hardware and software inventory. If disabled, only the computer name is collected and shown in the "Inventory" menu.

Geo-tracking maps the endpoint IP address to location using a public IP-to-location database to show in inventory and reports.

Note that changes only apply to new data. This is by design to avoid accidentally deleting existing data.

Item B: Admin By Request top menu

Pages that display data:

The screenshot shows the Admin By Request web interface. The top navigation bar includes the logo, a company logo placeholder, and a menu with items: Summary, Auditlog, Requests, Inventory, Reports, Settings (highlighted), Download, Logins, Docs, and Support. The main content area is titled 'Tenant Settings' and includes a sidebar with options: Identity, Auto-Update, Privacy (selected), Retention, API Keys, Webhooks, Email Domain, and Policies. The 'Privacy Settings' section is active, showing a list of settings: 'Obfuscate user accounts' (OFF), 'Collect user names' (ON), 'Collect user email addresses' (ON), 'Collect user phone numbers' (ON), 'Collect inventory' (ON), and 'Allow geo-tracking' (ON). A 'Save' button is at the bottom. To the right, an 'About Privacy Settings' section explains 'Obfuscation', 'Collection of data', 'Inventory', and 'Geo-tracking'.

Admin By Request Endpoint Privilege Management Eric Hastie @ Admin By Request Demo

YOUR Company Logo Summary **Auditlog** Requests Inventory Reports **Settings** Download Logins Docs Support

Tenant Settings

Settings here are global tenant settings on top of all other settings. If you have any questions, feel free to contact us [here](#).

- Identity
- Auto-Update
- Privacy**
- Retention
- API Keys
- Webhooks
- Email Domain
- Policies

Privacy Settings

Privacy Settings

- ☐ OFF Obfuscate user accounts
- ☒ ON Collect user names
- ☒ ON Collect user email addresses
- ☒ ON Collect user phone numbers
- ☒ ON Collect inventory
- ☒ ON Allow geo-tracking

Save

About Privacy Settings

Obfuscation creates an alias for each user. You can track activity, but you cannot decode the true identity of any user.

Collection of data should be left on unless you have a reason not to do this. If disabled, you will have to find contact information elsewhere.

Inventory is a hardware and software inventory. If disabled, only the computer name is collected and shown in the 'Inventory' menu.

Geo-tracking maps the endpoint IP address to location using a public IP-to-location database to show in inventory and reports.

Note that changes only apply to new data. This is by design to avoid accidentally deleting existing data.

Item C: Privacy Settings

Default privacy settings:

Admin By Request Endpoint Privilege Management Eric Hastie @ Admin By Request Demo

Summary Auditlog Requests Inventory Reports **Settings** Download Logins Docs Support

Tenant Settings
Settings here are global tenant settings on top of all other settings. If you have any questions, feel free to contact us [here](#).

Identity Auto-Update **Privacy** Retention API Keys Webhooks Email Domain Policies

Privacy Settings

Privacy Settings

☐ OFF Obfuscate user accounts
☒ ON Collect user names
☒ ON Collect user email addresses
☒ ON Collect user phone numbers
☒ ON Collect inventory
☒ ON Allow geo-tracking

Save

About Privacy Settings

Obfuscation creates an alias for each user. You can track activity, but you cannot decode the true identity of any user.

Collection of data should be left on unless you have a reason not to do this. If disabled, you will have to find contact information elsewhere.

Inventory is a hardware and software inventory. If disabled, only the computer name is collected and shown in the 'Inventory' menu.

Geo-tracking maps the endpoint IP address to location using a public IP-to-location database to show in inventory and reports.

Note that changes only apply to new data. This is by design to avoid accidentally deleting existing data.

Obfuscate user accounts:

Admin By Request Endpoint Privilege Management Eric Hastie @ Admin By Request Demo

Summary Auditlog Requests Inventory Reports **Settings** Download Logins Docs Support

Tenant Settings
Settings here are global tenant settings on top of all other settings. If you have any questions, feel free to contact us [here](#).

Identity Auto-Update **Privacy** Retention API Keys Webhooks Email Domain Policies

Privacy Settings

Privacy Settings

☒ ON Obfuscate user accounts
☐ OFF Collect user names
☐ OFF Collect user email addresses
☐ OFF Collect user phone numbers
☒ ON Collect inventory
☒ ON Allow geo-tracking

Save

About Privacy Settings

Obfuscation creates an alias for each user. You can track activity, but you cannot decode the true identity of any user.

Collection of data should be left on unless you have a reason not to do this. If disabled, you will have to find contact information elsewhere.

Inventory is a hardware and software inventory. If disabled, only the computer name is collected and shown in the 'Inventory' menu.

Geo-tracking maps the endpoint IP address to location using a public IP-to-location database to show in inventory and reports.

Note that changes only apply to new data. This is by design to avoid accidentally deleting existing data.

Item D: Requests

Default privacy settings:

Admin By Request Endpoint Privilege Management Eric Hastie @ Admin By Request Demo

Summary Auditlog **Requests** Inventory Reports Settings Download Logins Docs Support

Pending Approval Requests

Users will be notified by email of approval or denial. Requests will drop out of the list after two weeks. If a user does not use an approved request within two weeks, the approval will expire. You can approve or deny requests using the [mobile app](#) also.

PENDING (1) APPROVED (0) DENIED (0) QUARANTINED (0)

20-11-2024 15:32:58 • Elliott Frame

Requesting to run Uninstall Programs 8.4.2.0 from Admin By Request

- Email: elliottf@abrnzdemo.com • Phone: 555 123456 • Computer: DESKTOP-67KF4TH
- File: AdminByRequest.exe • App: 15/100 • Vendor: 32/100 • Metadefender: [Clean](#) • Virustotal: [Run check](#)
- Reason: Testing the uninstall process via Tray Tools

Approve Deny AI Assistance

Obfuscate user accounts:

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

Admin By Request Endpoint Privilege Management Eric Hastie @ Admin By Request Demo

Summary Auditlog **Requests** Inventory Reports Settings Download Logins Docs Support

Pending Approval Requests

Users will be notified by email of approval or denial. Requests will drop out of the list after two weeks. If a user does not use an approved request within two weeks, the approval will expire. You can approve or deny requests using the [mobile app](#) also.

PENDING (2) APPROVED (1) DENIED (0) QUARANTINED (0)

20-11-2024 15:48:08 • 4e47a184aade21f55d8b10b7b4f6dade

Requesting to run Rufus 4.5.2180 from Akeo Consulting

- Computer: DESKTOP-67KF4TH
- File: [rufus-4.5.exe](#) • App: 46/100 • Vendor: 12/100 • Metadefender: [Clean](#) • Virustotal: [Run check](#)
- Reason: Another program needed for dev work

Approve Deny AI Assistance

20-11-2024 15:44:16 • 4e47a184aade21f55d8b10b7b4f6dade

Requesting to run an administrator session

- Computer: DESKTOP-67KF4TH
- Reason: Further testing required

Approve Deny

Item E: Auditlog

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

Default privacy settings:

Uninstall Programs
Elliott Frame
DESKTOP-67KF4TH
20-11-2024 16:06:15
00:00:36
0/1/1
Finished

Contact Information

User account Elliott Frame
Email elliottf@abnzdemo.com
Phone 555 123456
Approved by Eric Hastie
Response In 00:15:57
Reason Testing the uninstall process via Tray Tools

Application

Name Uninstall Programs 8.4.2.0 15
Vendor Admin By Request 32
File name AdminByRequest.exe
Path C:\Program Files (x86)\FastTrack Software\Admin By Request

Installed or uninstalled software

Action	Application	Version	Publisher
Uninstall	WinZip	76.9.16251	Corel Corporation

Programs executed using elevated privileges

Program	File	Vendor	Version				
Windows® installer	MsiExec.exe	Microsoft Corporation	5.0.17134.1 (WinBuild.160101.0800)	Check			

Execution

Issued time 20-11-2024 15:32:58
Start time 20-11-2024 16:06:15
End time 20-11-2024 16:06:51
Duration 00:00:36
Settings Global Settings
Trace no 226834536

Actions

Malware scan Unknown
Virusotal Check status
AI assistance Ask ChatGPT what this is
Pre-approve Pre-approve this file
Block Block this file

We're Online!

Obfuscate user accounts:

Rufus
4e47a184aade21f55d8b10b7b4f6dade
DESKTOP-67KF4TH
20-11-2024 16:07:35
00:00:58
0/0/2
Finished

Contact Information

User account 4e47a184aade21f55d8b10b7b4f6dade
Approved by Eric Hastie
Response In 00:19:13
Reason Another program needed for dev work

Application

Name Rufus 4.5.2180 46
Vendor Akeo Consulting 12
File name rufus-4.5.exe

Installed or uninstalled software

No software was installed or uninstalled.

Programs executed using elevated privileges

Program	File	Vendor	Version				
➤ Rufus	rufus-4.5.exe	Akeo Consulting	4.5.2180	Check	Path	Approve	Block

Execution

Issued time 20-11-2024 15:48:08
Start time 20-11-2024 16:07:35
End time 20-11-2024 16:08:33
Duration 00:00:58
Settings Global Settings
Trace no 226836177

Actions

Malware scan Clean
Virusotal Check status
AI assistance Ask ChatGPT what this is
Pre-approve Pre-approve this file
Block Block this file

30 September 2025

4 Appendix

PAGE 10

Item F: Inventory

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

Default privacy settings:

The screenshot shows the 'Hardware Inventory' section for the computer 'DESKTOP-67KF4TH'. The interface includes a sidebar with navigation options like 'Inventory', 'PIN Code', 'Local Admins', 'Break Glass', 'Events', 'Auditlog', 'Sub Settings', and 'Owner'. The main content area displays details for the Computer, User, System, and Hardware.

Category	Property	Value
Computer	Name	DESKTOP-67KF4TH
	Join Type	None
	Type	Desktop
User	Name	N/A
	Account	Elliott Frame
	Join Type	None
	Administrator	No
	Device Owner	No
System	Operating System	Windows 10 Enterprise Evaluation
	OS Release	1803
	OS Build	17134.2208
	OS Type	Workstation
	OS Bits	64 bit
	OS Install Date	11-11-2024
ABR Client	ABR Client Version	8.4.2
	ABR Client Install	13-11-2024 17:28:16
	Inventory Time	20-11-2024 14:43:09
Hardware	Manufacturer	VMware, Inc.
	Model	VMware20,1
	Service Tag	VMware-56 4d 66 2d b3 ba 07-16 e7 97 d8 c5 d5 9
	CPU	13th Gen Intel Core i7-13700H
	CPU Speed	2918 mhz
	Cores	2
	Memory	8588MB
	Disk Size	63GB
Disk Free	35GB	
Disk Status	OK	

Collect inventory **OFF**:

The screenshot shows the 'Run As Admin' section for the computer 'DESKTOP-67KF4TH'. The interface includes a sidebar with navigation options like 'Inventory', 'PIN Code', 'Local Admins', 'Break Glass', 'Events', 'Auditlog', 'Sub Settings', and 'Owner'. The main content area displays a table of 'Run As Admin' sessions.

Application	User	Time	Duration	Activity	Status
> ✓ Rufus	4e47a184aade21f5508b10b7b4f6dade	20-11-2024 16:07:35	00:00:58	0/0/2	Finished
> ✓ Uninstall Programs	Elliott Frame	20-11-2024 16:06:15	00:00:36	0/1/1	Finished
> ✓ Windows Features	Elliott Frame	20-11-2024 15:39:53	00:01:04	0/0/1	Finished
> ✓ WinZipStub Installer	Elliott Frame	20-11-2024 14:46:36	00:01:12	1/0/1	Finished
> ✓ WinZipStub Installer	ERIC HASTIE	20-11-2024 14:45:51	00:00:21	0/0/1	Finished
> ✓ Visual Studio Code Setup	STEVE DOOSON	15-11-2024 13:09:21	00:00:13	1/1/1	Finished
> ✓ Settings	ABR090184	15-11-2024 12:51:36	00:00:04	0/0/1	Finished
> ✓ Visual Studio Code Setup	ERIC HASTIE	13-11-2024 17:37:30	00:00:56	1/0/5	Finished
> ✓ Zoom Meetings Installer	ERIC HASTIE	13-11-2024 17:36:20	00:00:09	0/0/2	Finished
> ✓ Visual Studio Code Setup	ERIC HASTIE	13-11-2024 17:33:07	00:00:20	0/0/2	Finished
> ✓ Visual Studio Code Setup	ERIC HASTIE	13-11-2024 17:30:07	00:00:06	0/0/2	Finished

Page 1 of 1 (11 items) | Page size: 25

RED USER - ADMINISTRATOR

Buttons: Aggregated View, Export to PDF, Export to XLSX, Export to CSV (I), Export to CSV (I), Search

Item G: Inventory (Geo-tracking)

Default privacy settings:



Geographical Location

City

Country

Hour offset

Auckland

New Zealand

UTC +13 hours

[Show on Google Maps](#)

Allow geo-tracking **OFF**:



Geographical Location

City

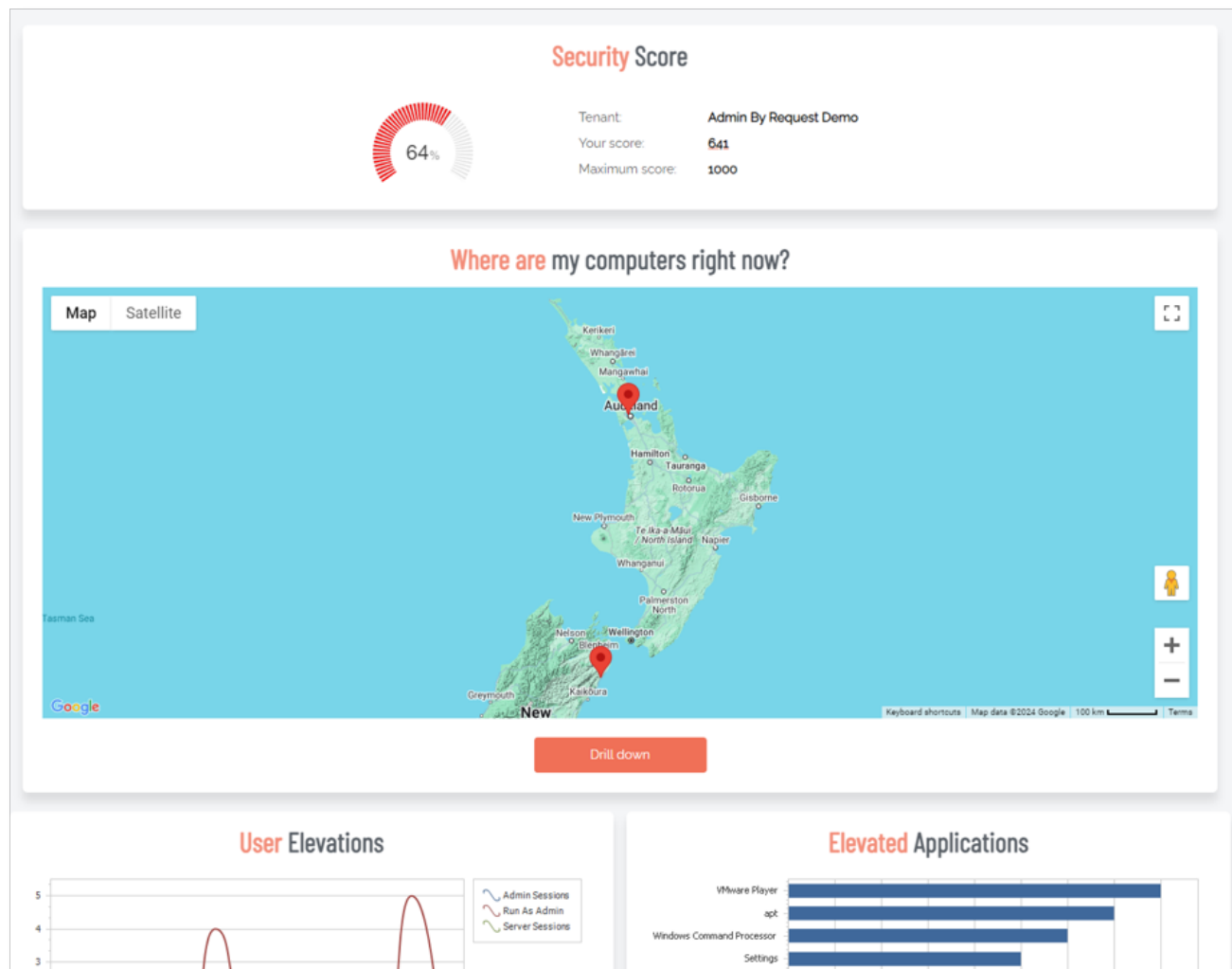
Country

Not tracked

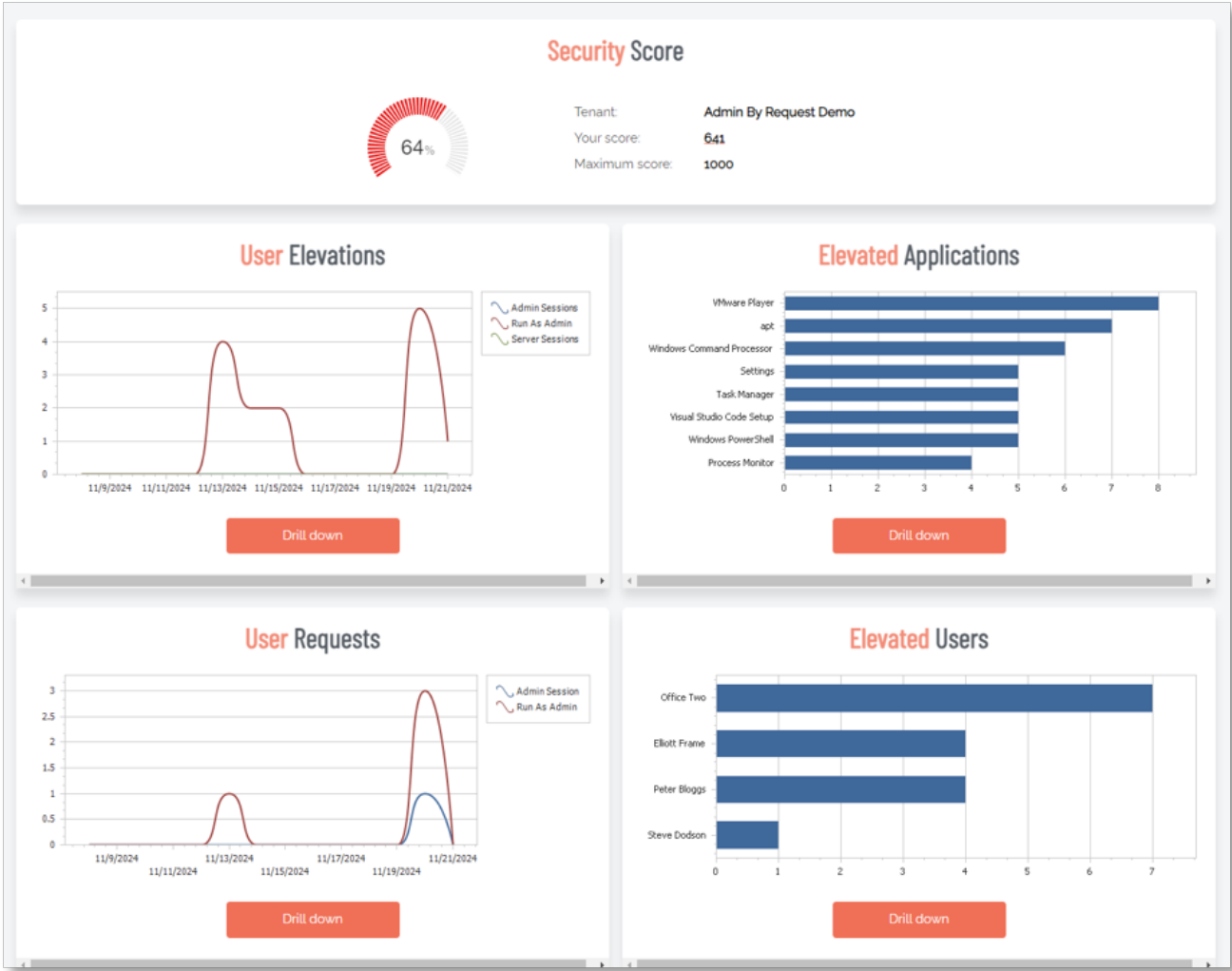
Not tracked

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 <i>Settings</i> paths to reflect new portal menu structure.
14 February 2025 1.2	Steve Dodson	Added <i>Privacy Settings</i> , <i>Scope</i> and <i>Reference</i> 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 <i>Device Owner</i> dependence on <i>Collect Inventory</i> setting.
30 September 2025 2.1	Steve Dodson	Added Related Documents section to "Introduction".