FastTrack Software

Admin By Request

DATA PRIVACY SETTINGS

The purpose of this document is to demonstrate how Admin By Request handles **Personally Identifiable Information** (**PII**) or personal data.

Table of Contents

Introduction

At Admin By Request, we value privacy.

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

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

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

The Privacy Settings page is found in the Admin By Request user portal, under **Settings > Windows / Mac Settings > Data**.

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.

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

About Privacy Settings

The Privacy Settings can be found within the Admin By Request user portal under **Settings > Windows / Mac Settings > Data.**

See item A in Appendix.

Privacy Settings and Descriptions

See below for the list of 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.

  It is important to note that once this setting is toggled **OFF**, the following three settings 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 Admin By Request user portal, or in Google maps via Admin By Request.

Adjusting Privacy Settings

It is important to note that when you adjust your Privacy Settings (enable or disable them using the **ON** / **OFF** toggles) the changes only apply to new data; it does not change or remove 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 user portal.

If you then disable this setting, *user X's* user name will remain in all of the appropriate 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.

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 Appendix.

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

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**
- Allow geo-tracking – **ON**

See item C in 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.

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 will detail where data is omitted from Requests, Auditlog, Inventory and Reports in the Admin By Request user portal when each Privacy Setting is disabled.

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 Admin By Request user portal. See items D, E and F in the Appendix.

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 Admin By Request user portal. See items D, E and F in the Appendix.

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 Admin By Request user portal. See items D, E and F in the Appendix.

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 Admin By Request user portal. See items D, E and F in the Appendix.

Collect inventory

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

Devices will still appear in the initial Inventory page under New Computers, however the sections in the subsequent page that display all inventory-related data will be missing from the right-hand menu.

These omitted sections are:

- **Overview**
- **Software**
- **Local Admins**

Disabling the Collect inventory setting essentially removes all sections that contain inventory-related data from the Inventory page.

See item F in the Appendix.

Allow geo-tracking

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

When disabled, user's IP addresses will not be mapped to their physical location.

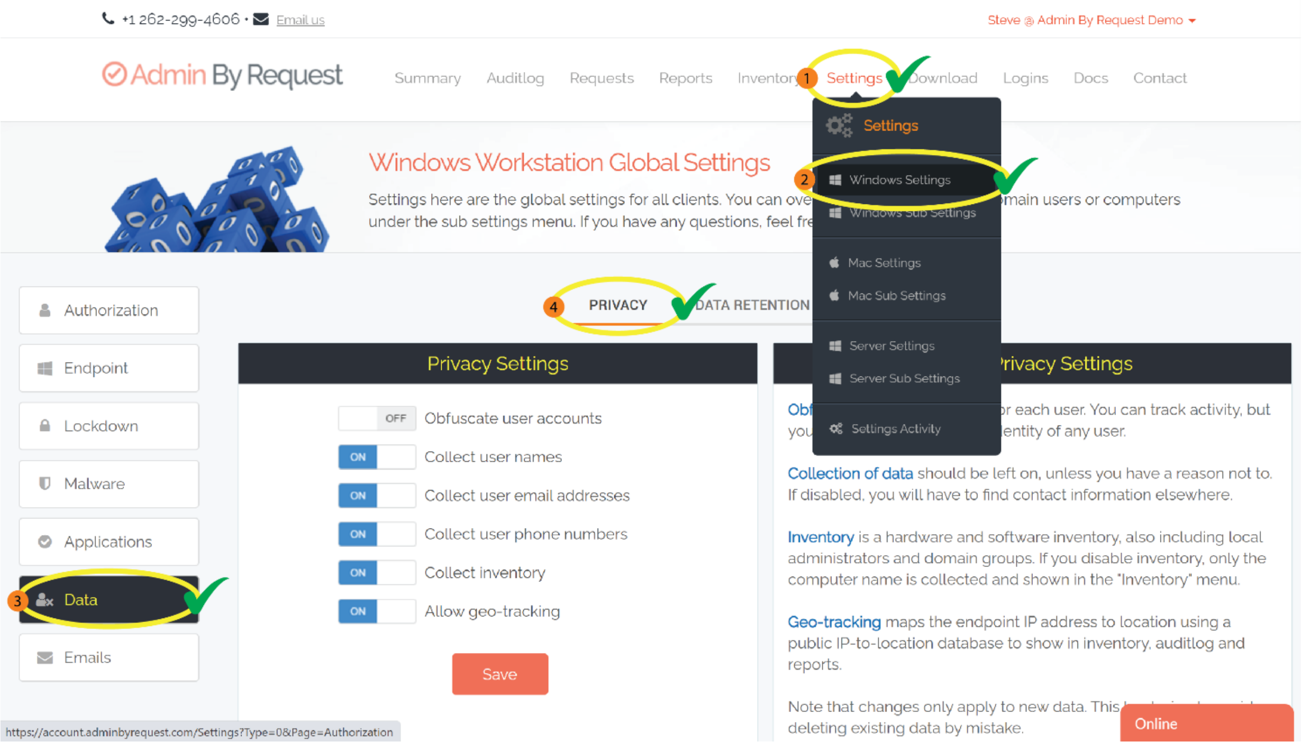
This means that in the Inventory page, under **Overview > Geographical location**, the City, Region and Country will be omitted.

In the Repots page, under **Dashboard > Where are my computers right now?**, devices that do not have this setting applied will not be pin-pointed on the map and the location details will not be listed upon clicking the **Drill down** button.

See items G & H in the Appendix.

Appendix

Item A: Navigating to the Privacy Settings page



Windows Workstation Global Settings

Settings here are the global settings for all clients. You can ove… …main users or computers under the sub settings menu. If you have any questions, feel fre…

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

…rivacy Settings

Obf… …r each user. You can track activity, but you… …entity of any user.

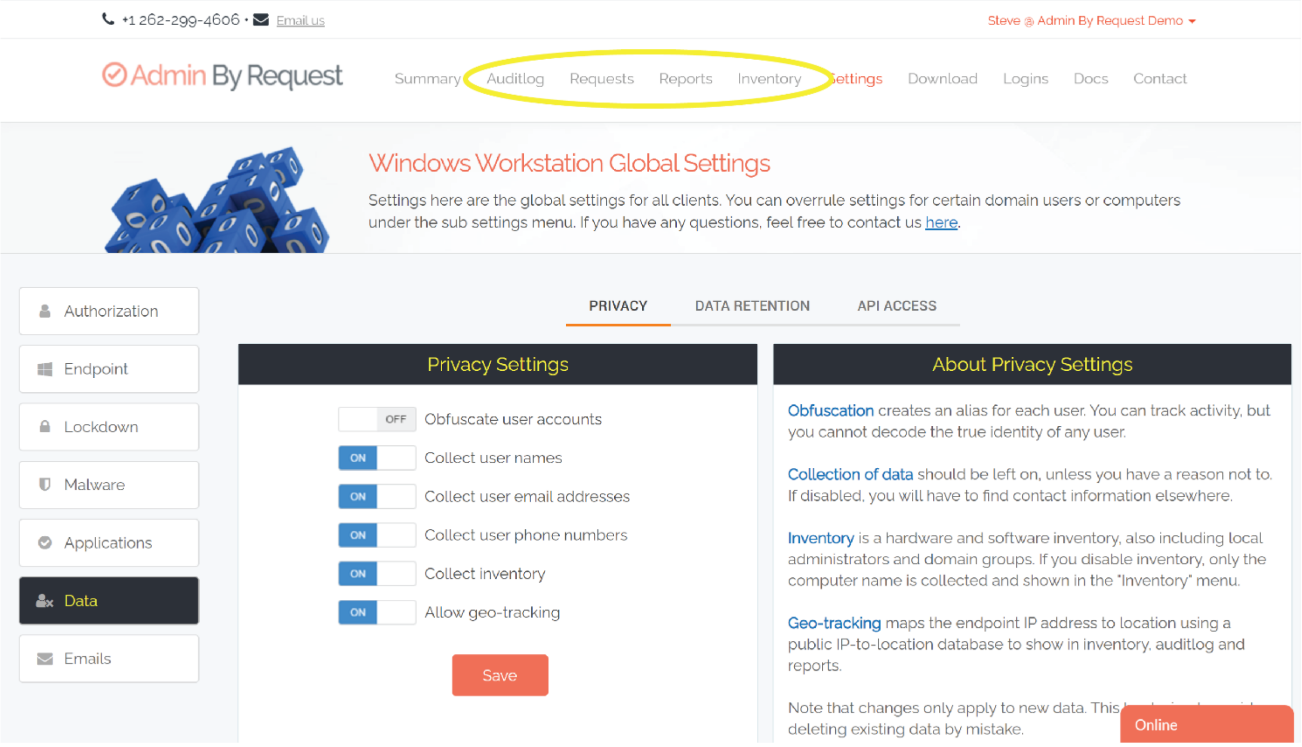
Collection of data should be left on, unless you have a reason not to. If disabled, you will have to find contact information elsewhere.

Inventory is a hardware and software inventory, also including local administrators and domain groups. If you disable inventory, 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, auditlog and reports.

Note that changes only apply to new data. This… deleting existing data by mistake.

Item B: Admin By Request top menu – Pages that display data



Windows Workstation Global Settings

Settings here are the global settings for all clients. You can overrule settings for certain domain users or computers under the sub settings menu. If you have any questions, feel free to contact us here.

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

About Privacy Settings

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

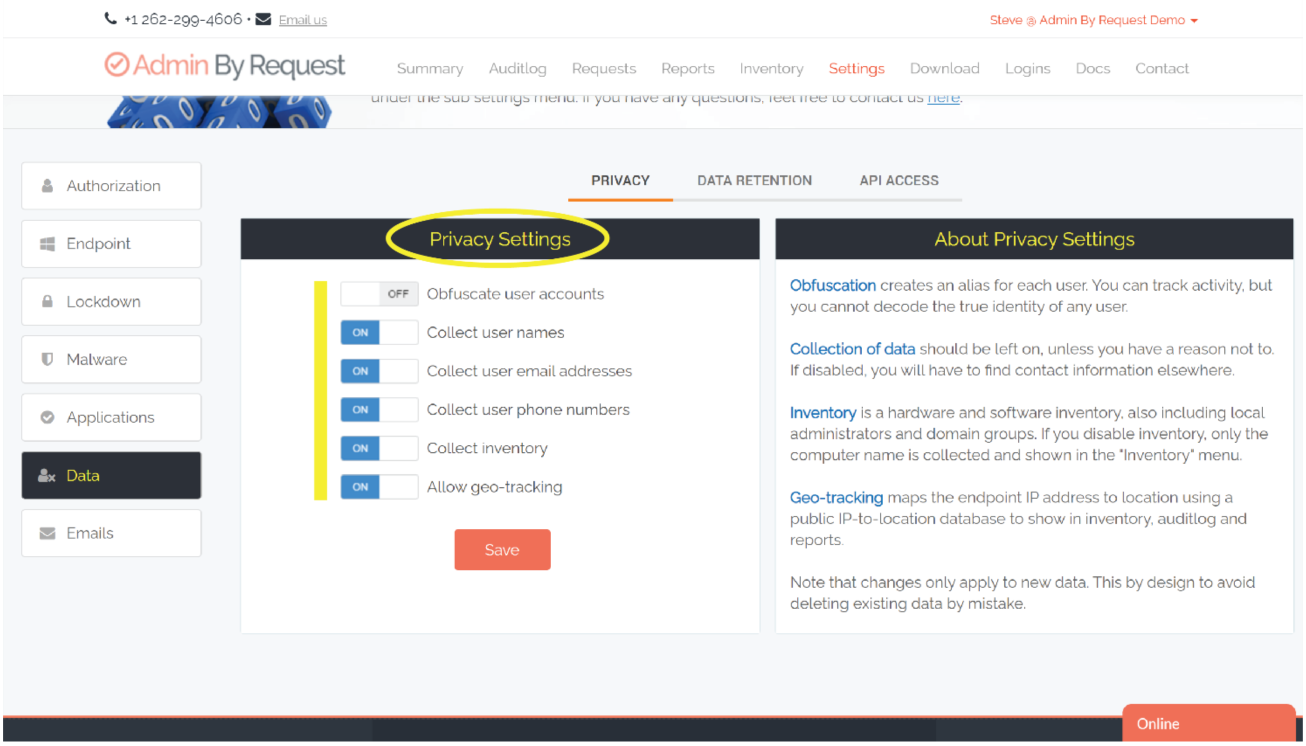
Collection of data should be left on, unless you have a reason not to. If disabled, you will have to find contact information elsewhere.

Inventory is a hardware and software inventory, also including local administrators and domain groups. If you disable inventory, 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, auditlog and reports.

Note that changes only apply to new data. This… deleting existing data by mistake.

Item C: Default Privacy Settings



+1 262-299-4606 • Email us
Steve @ Admin By Request Demo
Admin By Request
Summary Auditlog Requests Reports Inventory Settings Download Logins Docs Contact

under the sub settings menu. If you have any questions, feel free to contact us here.

Authorization
Endpoint
Lockdown
Malware
Applications
Data
Emails
PRIVACY DATA RETENTION API ACCESS

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

About Privacy Settings

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

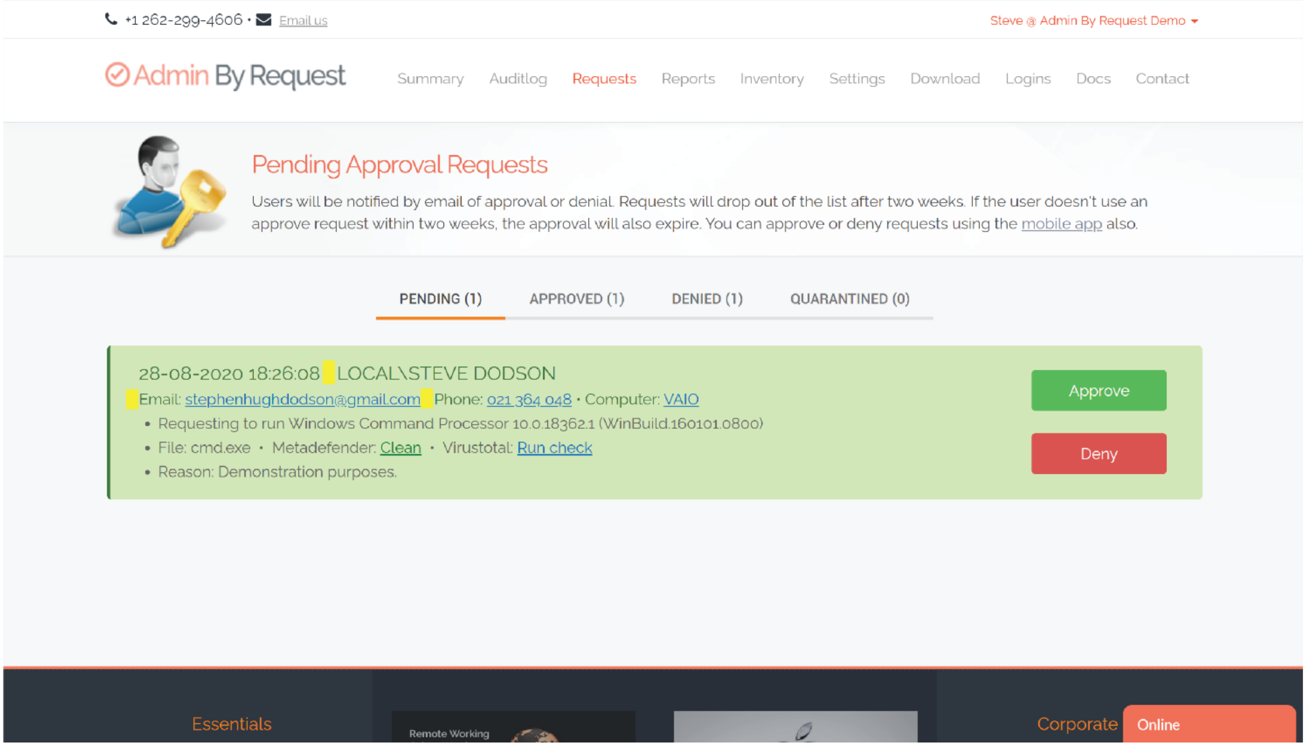
Collection of data should be left on, unless you have a reason not to. If disabled, you will have to find contact information elsewhere.

Inventory is a hardware and software inventory, also including local administrators and domain groups. If you disable inventory, 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, auditlog and reports.

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

Item D: Requests with default Privacy Settings applied



+1 262-299-4606 • Email us
Steve @ Admin By Request Demo
Admin By Request
Summary Auditlog Requests Reports Inventory Settings Download Logins Docs Contact

Pending Approval Requests

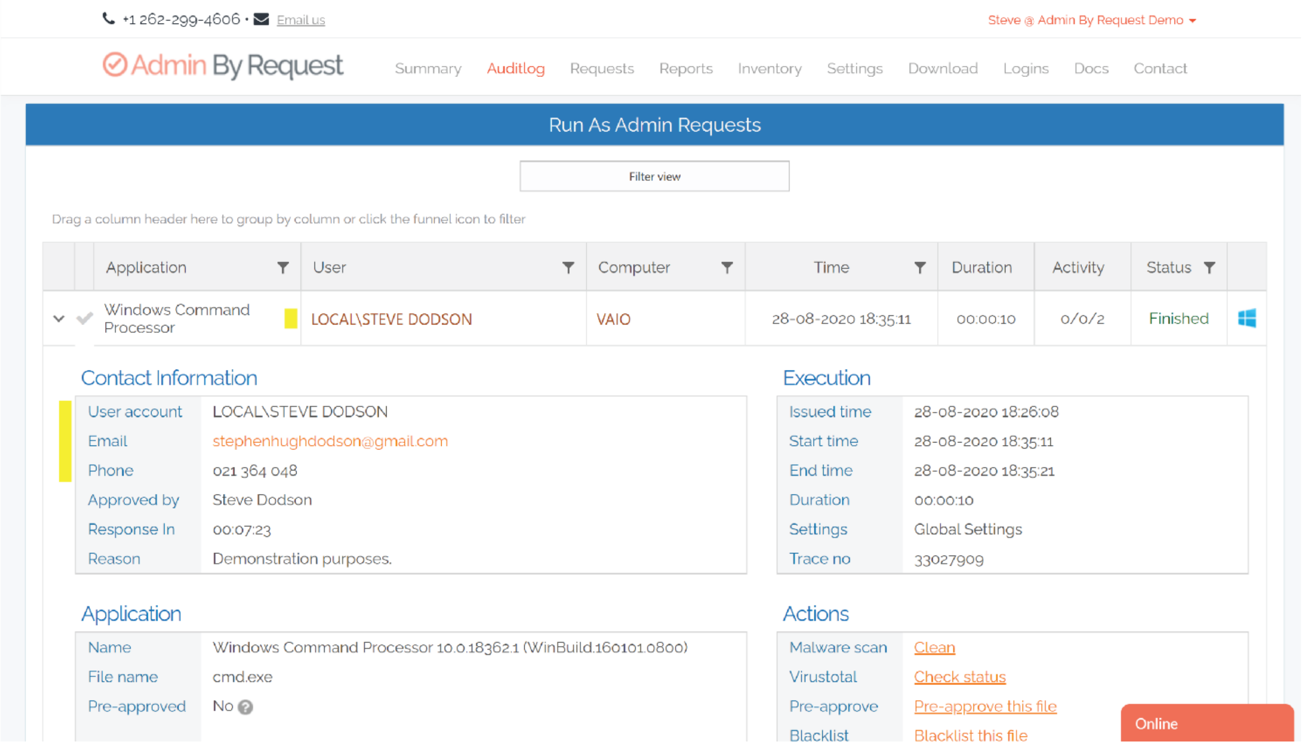
Users will be notified by email of approval or denial. Requests will drop out of the list after two weeks. If the user doesn't use an approve request within two weeks, the approval will also expire. You can approve or deny requests using the mobile app also.

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

28-08-2020 18:26:08 LOCAL\STEVE DODSON
Email: stephenhughdodson@gmail.com Phone: 021 364 048 • Computer: VAIO

- Requesting to run Windows Command Processor 10.0.18362.1 (WinBuild.160101.0800)
- File: cmd.exe • Metadefender: Clean • Virustotal: Run check
- Reason: Demonstration purposes.

Item E: Auditlog with default Privacy Settings applied > [select details arrow to the left of an item]



Run As Admin Requests

Filter view

Drag a column header here to group by column or click the funnel icon to filter

Application	User	Computer	Time	Duration	Activity	Status
Windows Command Processor	LOCAL\STEVE DODSON	VAIO	28-08-2020 18:35:11	00:00:10	0/0/2	Finished

Contact Information

User account	LOCAL\STEVE DODSON
Email	stephenhughdodson@gmail.com
Phone	021 364 048
Approved by	Steve Dodson
Response In	00:07:23
Reason	Demonstration purposes.

Execution

Issued time	28-08-2020 18:26:08
Start time	28-08-2020 18:35:11
End time	28-08-2020 18:35:21
Duration	00:00:10
Settings	Global Settings
Trace no	33027909

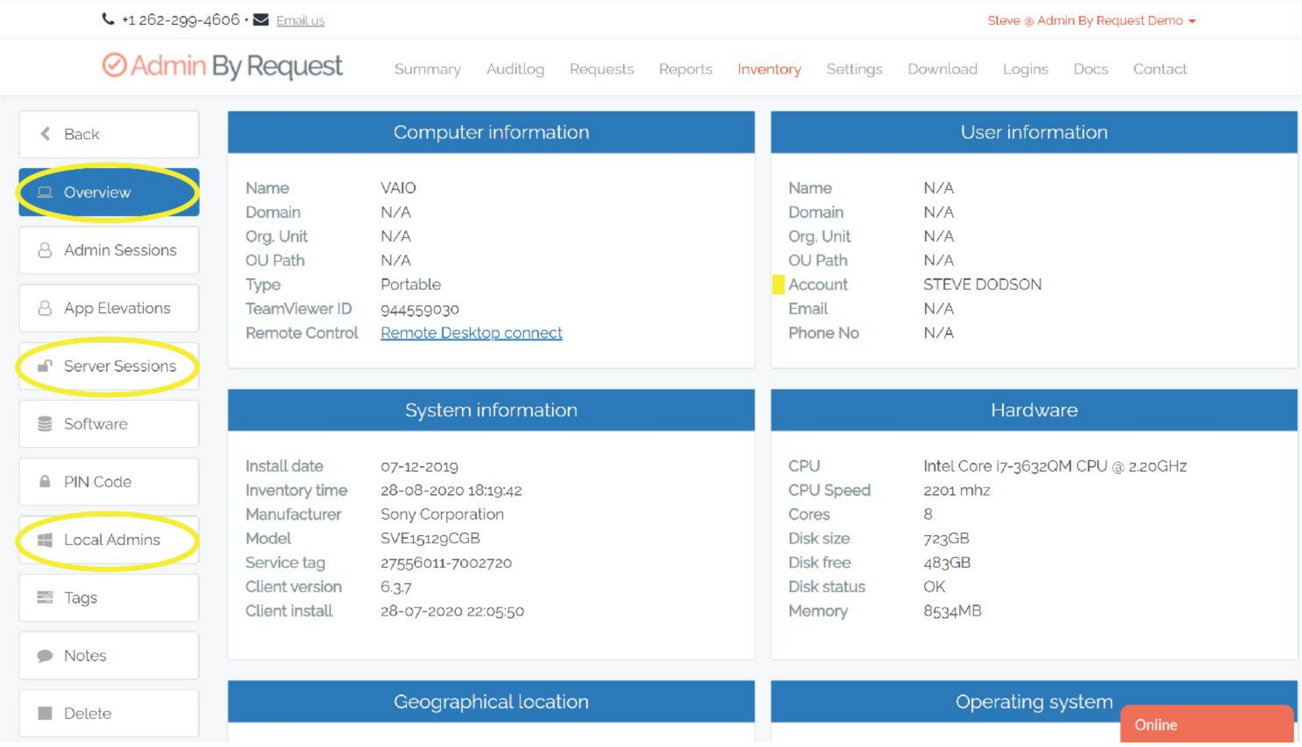
Application

Name	Windows Command Processor 10.0.18362.1 (WinBuild.160101.0800)
File name	cmd.exe
Pre-approved	No

Actions

Malware scan	Clean
Virustotal	Check status
Pre-approve	Pre-approve this file
Blacklist	Blacklist this file

Item F: Inventory with Default Privacy settings applied > [select computer]



Computer information

Name	VAIO
Domain	N/A
Org. Unit	N/A
OU Path	N/A
Type	Portable
TeamViewer ID	944559030
Remote Control	Remote Desktop connect

User information

Name	N/A
Domain	N/A
Org. Unit	N/A
OU Path	N/A
Account	STEVE DODSON
Email	N/A
Phone No	N/A

System information

Install date	07-12-2019
Inventory time	28-08-2020 18:19:42
Manufacturer	Sony Corporation
Model	SVE15129CGB
Service tag	27556011-7002720
Client version	6.3.7
Client install	28-07-2020 22:05:50

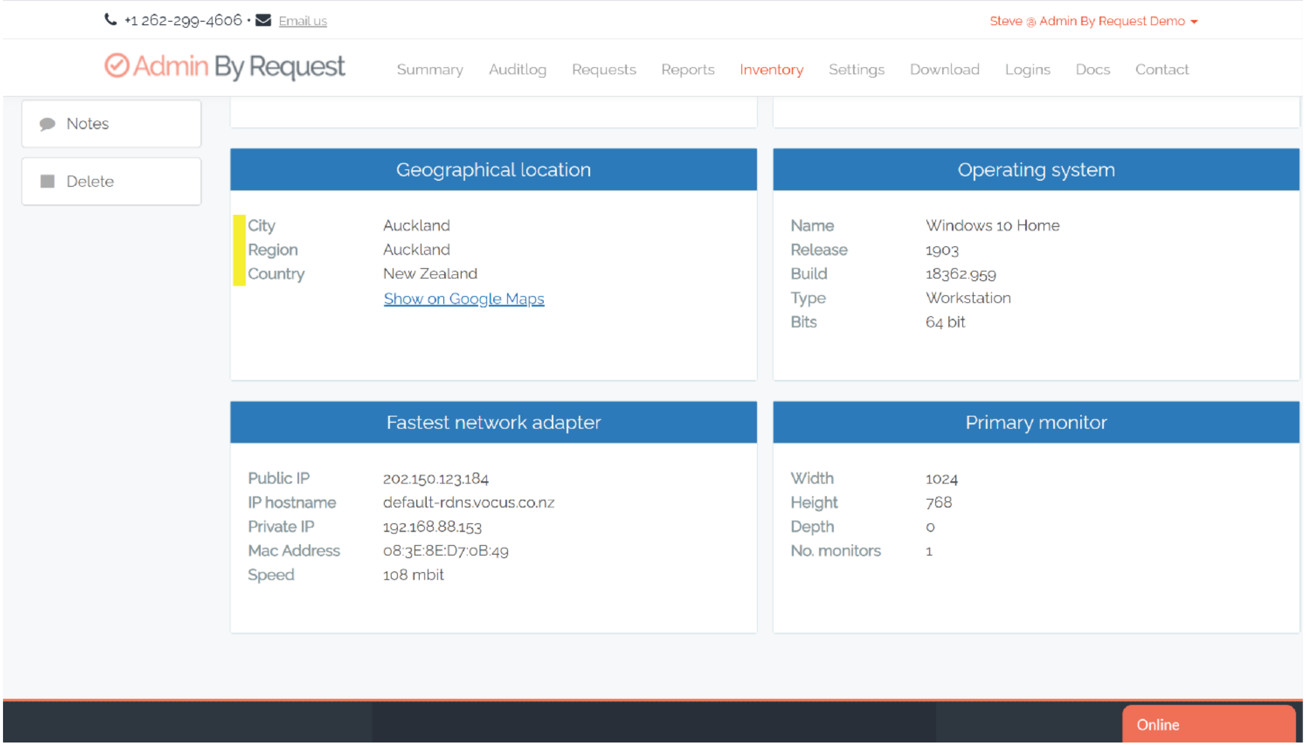
Hardware

CPU	Intel Core i7-3632QM CPU @ 2.20GHz
CPU Speed	2201 mhz
Cores	8
Disk size	723GB
Disk free	483GB
Disk status	OK
Memory	8534MB

Geographical location

Operating system

Item G: Inventory with Default Privacy Settings applied > Overview > [Geographical location]



Geographical location

City	Auckland
Region	Auckland
Country	New Zealand
	Show on Google Maps

Operating system

Name	Windows 10 Home
Release	1903
Build	18362.959
Type	Workstation
Bits	64 bit

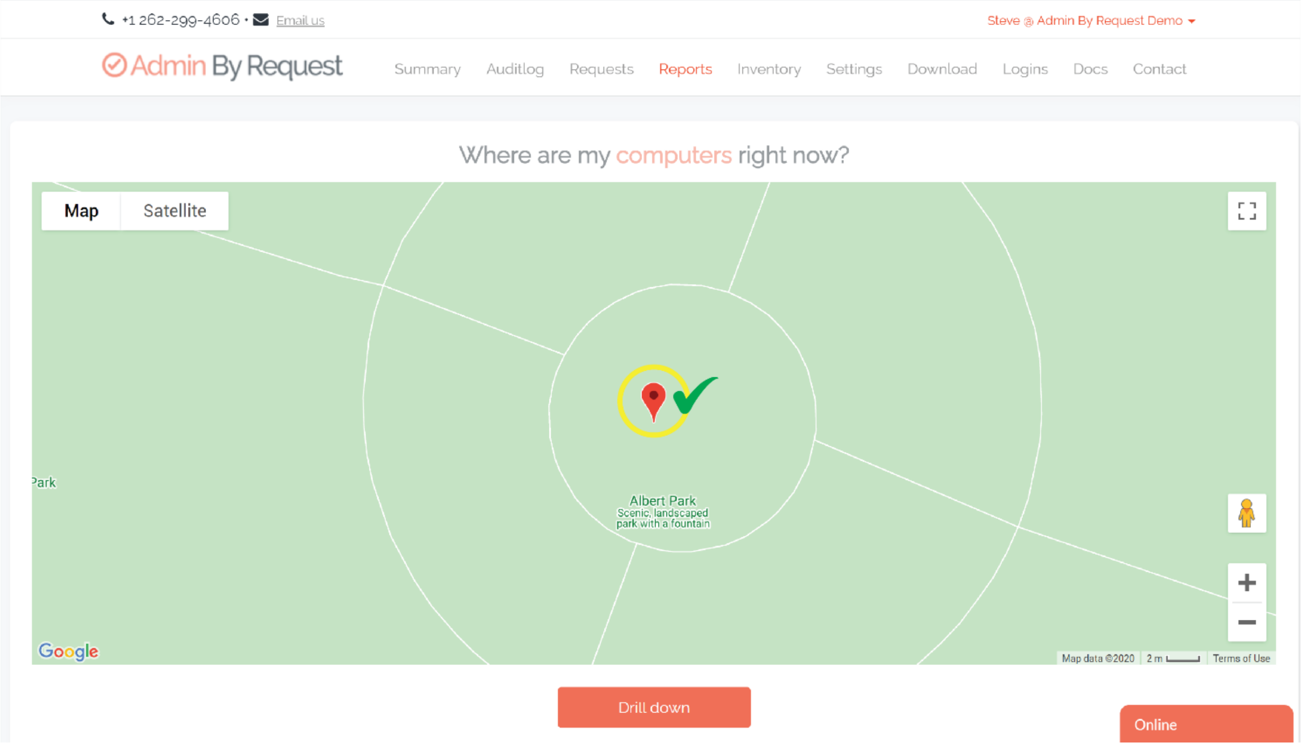
Fastest network adapter

Public IP	202.150.123.184
IP hostname	default-rdns.vocus.co.nz
Private IP	192.168.88.153
Mac Address	08:3E:8E:D7:0B:49
Speed	108 mbit

Primary monitor

Width	1024
Height	768
Depth	0
No. monitors	1

Item H: Reports > Dashboard > Where are my computers right now?



Where are my computers right now?