Technical Note

Admin By Request
ZERO TRUST PLATFORM

Product Platform: **Windows**
Product Version: **8.0 +**
Document Date: **15 November 2024**
Document Version: **1.0**

AI Approval

Introduction

There are two main reasons for enterprises to remove their users' admin rights:

1. To prevent them from installing unwanted applications on company devices.
2. More importantly, for security reasons – to prevent malware infection and spread.

History and experience tells us that malware often comes attached to unknown, 'freebie' applications which users download for one-off use. For example, a user who has obtained an ISO file but has no way to extract it, may do a quick Google search for a tool which will help them complete the job; download, install – and find that their system is now infected.

So how can an organization easily distinguish between which apps are safe for approval, and which should be blocked or looked at more closely? With the Artificial Intelligence Auto-Approval feature in Admin By Request, you can let our AI engine decide which files are safe for approval, and which should be considered potentially dangerous and handled manually instead.

AI Approval – What Is It?

Large enterprises with thousands of users need to carefully balance productivity with security – manually approving each request for elevation would consume extensive resources, as would figuring out which applications are most used and creating enormous pre-approved lists to cover all possibilities.

The AI Approval feature is the safer, more efficient alternative as it allows organizations to make a rule that says any applications that are popular / known / elevated frequently will be automatically approved.

Behind the Feature

The idea behind this feature came from looking at trends in our massive database of applications and concluding that most of the applications run with elevated privileges are the same across the board – and these common apps are generally safe for elevation. So, the question arose, how could we use this data to help each customer?

We created a system that assigns an application two percentage scores between **0** and **100** based on (1) the application itself and (2) its vendor's popularity. A very well-known app from a reputable vendor (e.g., Microsoft Office) would score in the higher end of the scale, whereas a rarely used app from an unknown vendor would receive a low score.

The higher each of the scores, the more trustworthy the app is considered to be, and the less risk attached in allowing it to be automatically approved by the Admin By Request AI engine.

Very low scores (i.e., 0-1) indicate 'exotic' apps – rare software from unknown vendors that are much more likely to have malware attached. These exotic applications are those that you would not want to be auto-approved by the AI engine, and instead approved manually on a case-by-case basis.

How It Works

The idea with the scoring system is to allow customers to set a score of their choosing, and then enable AI Auto-Approval for every application that meets this score or higher – using the AI engine to approve applications that are very common, and therefore, likely safe.

For example, if you set both App and Vendor scores to **10**, and enable auto-approvals for both, all applications that meet the threshold for one of the scores will be automatically approved.

> **NOTE:**
> Only one of the scores (i.e., App OR Vendor) has to be met in order for an application to be Auto-Approved, and it is possible to only have one or the other enabled for the feature to work.

Any apps that score below the set value will not be AI Auto-Approved, and can be dealt with upon individual Request by users, or via Machine Learning – another feature of Admin By Request since version 8.0.

Configuring AI Approvals

Each organization can tailor the feature to suit their needs and preferences – but how do you know what to set your App and Vendor Auto-Approval scores to?

Within the Admin By Request portal, we've created a database of over 12 million known applications and their scores. This list can be used to gauge which applications have what score, and give each organization an idea of where to set their AI Auto-Approval thresholds.

Because of the huge size of the database, only a sample of the most common applications is presented. For the same reason, searching for a particular app is not possible (at the time of writing).

If the app you wish to approve via AI Approval is not listed in the sample, you can check it's current scores by installing it on an Admin By Request test computer. Once installed, go to the Auditlog and check the scores.

Example

We want to allow users to install two common apps using AI Approval and neither of these apps appears in the samples at the time of checking (although they might appear at a later date).

User installation may or may not require approval, depending on your tenant's App and Vendor scores.

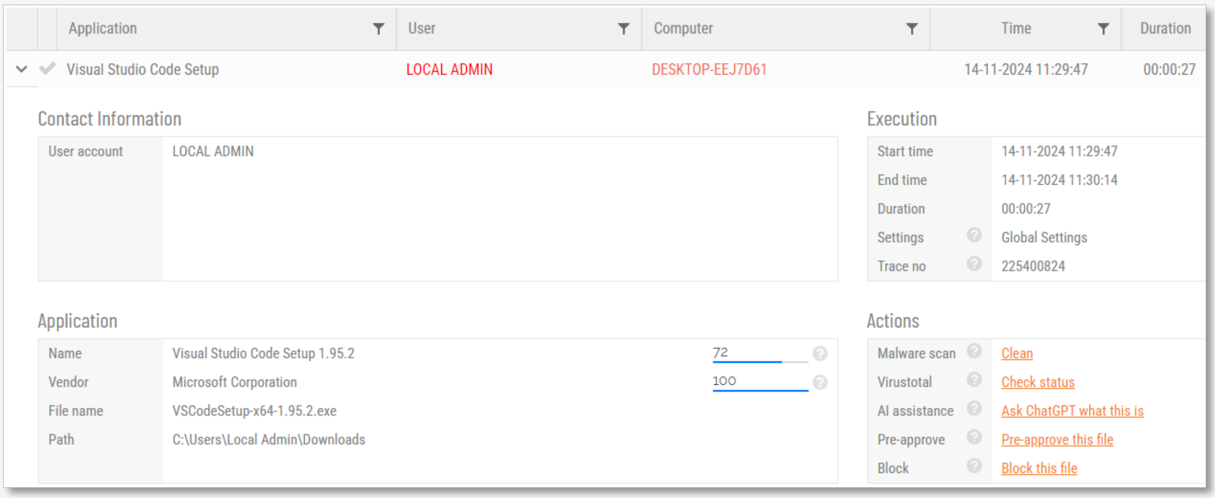
In this example, the apps are:

- Visual Studio Code Setup
- Zoom Meetings Installer

To check their current App and Vendor scores, make sure both App and Vendor auto-approval are **OFF** initially (i.e. not enabled). The AI Approval setting is found in the portal at **Endpoint Privilege Management > Settings > Windows Settings > App Control > AI APPROVAL**.

Using an admin account, install both apps on an Admin By Request test computer and then review the installation entries in the Auditlog:

- Visual Studio Code Setup - App Score **72**, Vendor Score **100**:



Application	User	Computer	Time	Duration
Visual Studio Code Setup	LOCAL ADMIN	DESKTOP-EEJ7D61	14-11-2024 11:29:47	00:00:27

Contact Information

User account	LOCAL ADMIN

Execution

Start time	14-11-2024 11:29:47
End time	14-11-2024 11:30:14
Duration	00:00:27
Settings	Global Settings
Trace no	225400824

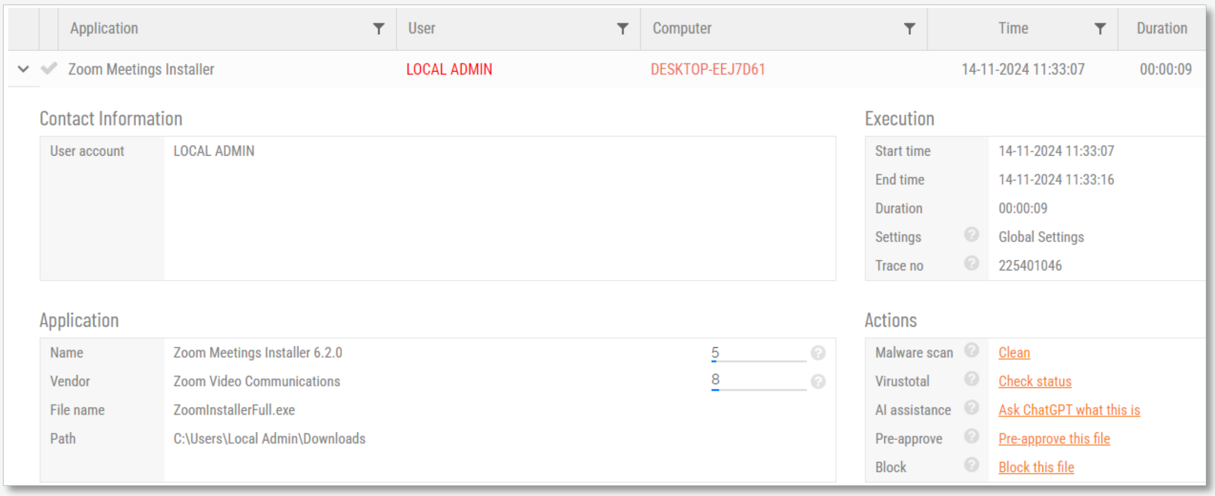
Application

Name	Visual Studio Code Setup 1.95.2	72
Vendor	Microsoft Corporation	100
File name	VSCodeSetup-x64-1.95.2.exe	
Path	C:\Users\Local Admin\Downloads	

Actions

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

- Zoom Meetings Installer - App Score **5**, Vendor Score **8**:



Application	User	Computer	Time	Duration
Zoom Meetings Installer	LOCAL ADMIN	DESKTOP-EEJ7D61	14-11-2024 11:33:07	00:00:09

Contact Information

User account	LOCAL ADMIN

Execution

Start time	14-11-2024 11:33:07
End time	14-11-2024 11:33:16
Duration	00:00:09
Settings	Global Settings
Trace no	225401046

Application

Name	Zoom Meetings Installer 6.2.0	5
Vendor	Zoom Video Communications	8
File name	ZoomInstallerFull.exe	
Path	C:\Users\Local Admin\Downloads	

Actions

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

VS Code Setup scores highly for both App and Vendor, while Zoom Meetings Installer does not score highly at all.

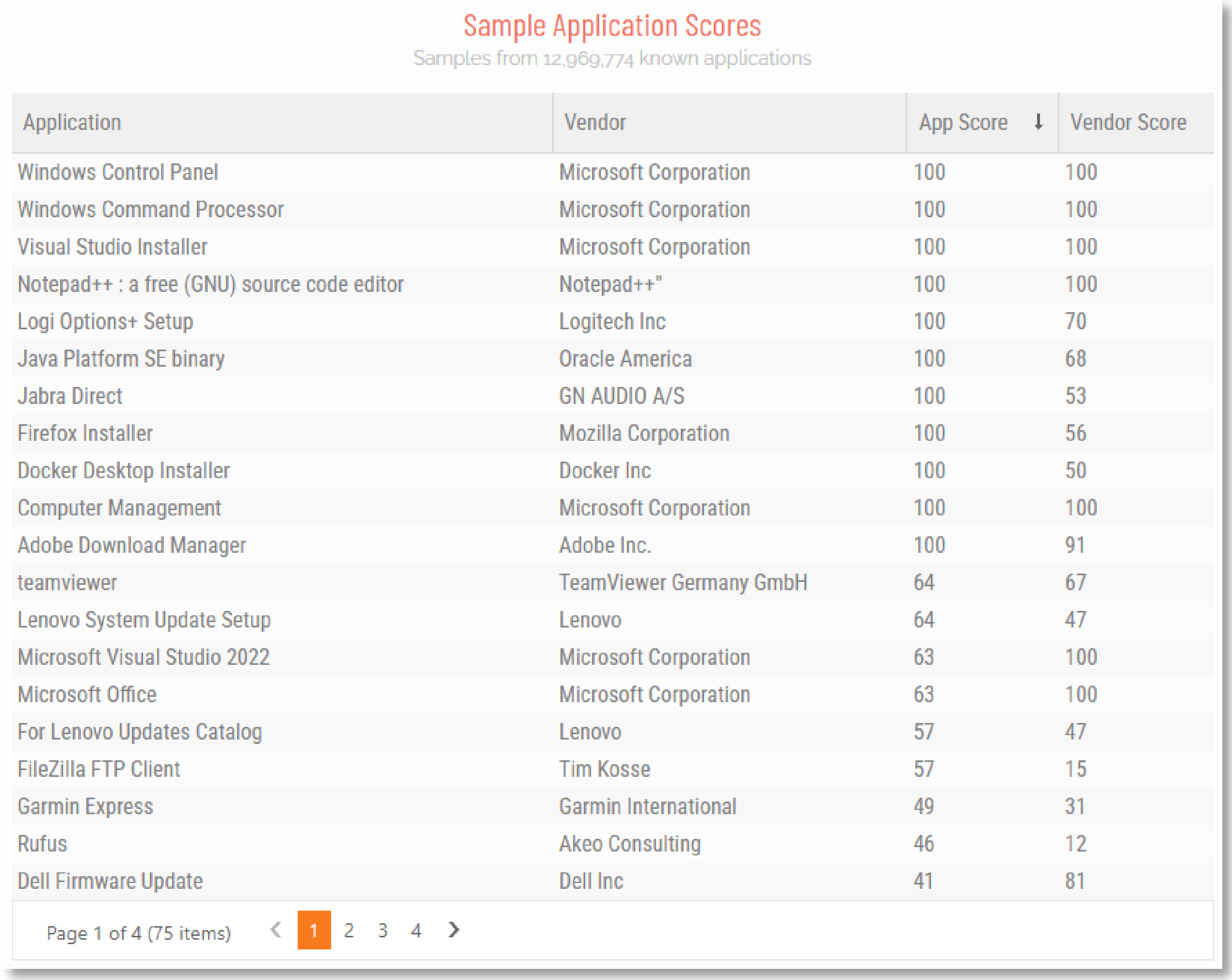
If we set our tenant scores to **45** and **90** for App and Vendor respectively, any app exceeding **either** of these will install without requiring approval, whereas any app falling below **both** values will require approval.

The following procedure describes how to do this.

To set AI Approval scores:

1. Navigate to **Endpoint Privilege Management > Settings > Windows Settings > App Control > AI APPROVAL** and check the *Sample Application Scores* table.

   The App Score and Vendor Score columns show each application's score in the database. In the image below, the list is ordered based on *highest* App Score (simply click the column heading to toggle ascending or descending) and we can see that the top scoring applications are all well-known:



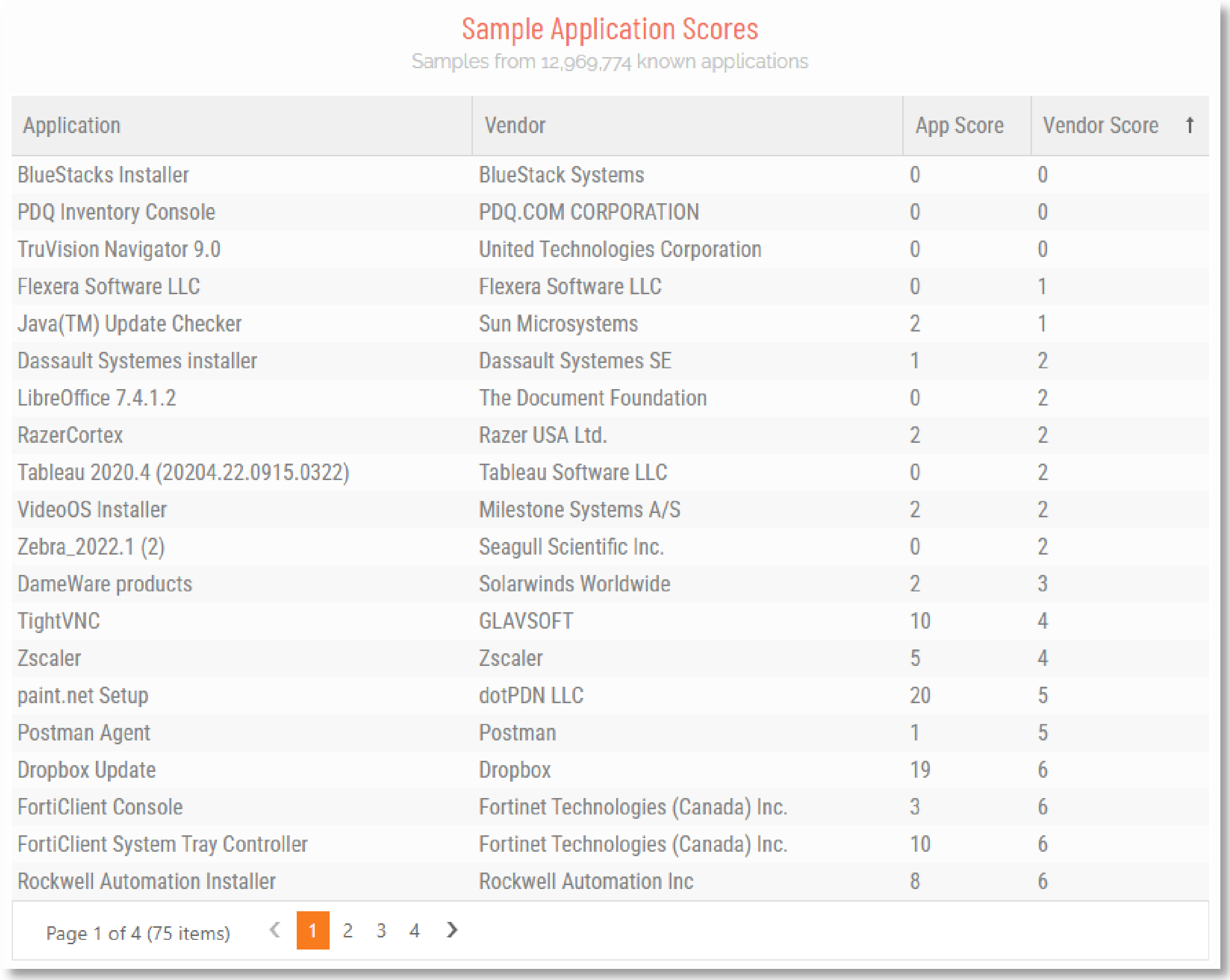
Sample Application Scores

Samples from 12,969,774 known applications

Application	Vendor	App Score ↓	Vendor Score
Windows Control Panel	Microsoft Corporation	100	100
Windows Command Processor	Microsoft Corporation	100	100
Visual Studio Installer	Microsoft Corporation	100	100
Notepad++ : a free (GNU) source code editor	Notepad++"	100	100
Logi Options+ Setup	Logitech Inc	100	70
Java Platform SE binary	Oracle America	100	68
Jabra Direct	GN AUDIO A/S	100	53
Firefox Installer	Mozilla Corporation	100	56
Docker Desktop Installer	Docker Inc	100	50
Computer Management	Microsoft Corporation	100	100
Adobe Download Manager	Adobe Inc.	100	91
teamviewer	TeamViewer Germany GmbH	64	67
Lenovo System Update Setup	Lenovo	64	47
Microsoft Visual Studio 2022	Microsoft Corporation	63	100
Microsoft Office	Microsoft Corporation	63	100
For Lenovo Updates Catalog	Lenovo	57	47
FileZilla FTP Client	Tim Kosse	57	15
Garmin Express	Garmin International	49	31
Rufus	Akeo Consulting	46	12
Dell Firmware Update	Dell Inc	41	81

Page 1 of 4 (75 items)

When we order the list by lowest scoring app Vendors (click Vendor Score column heading), most of the low-scoring applications are not particularly well-known:



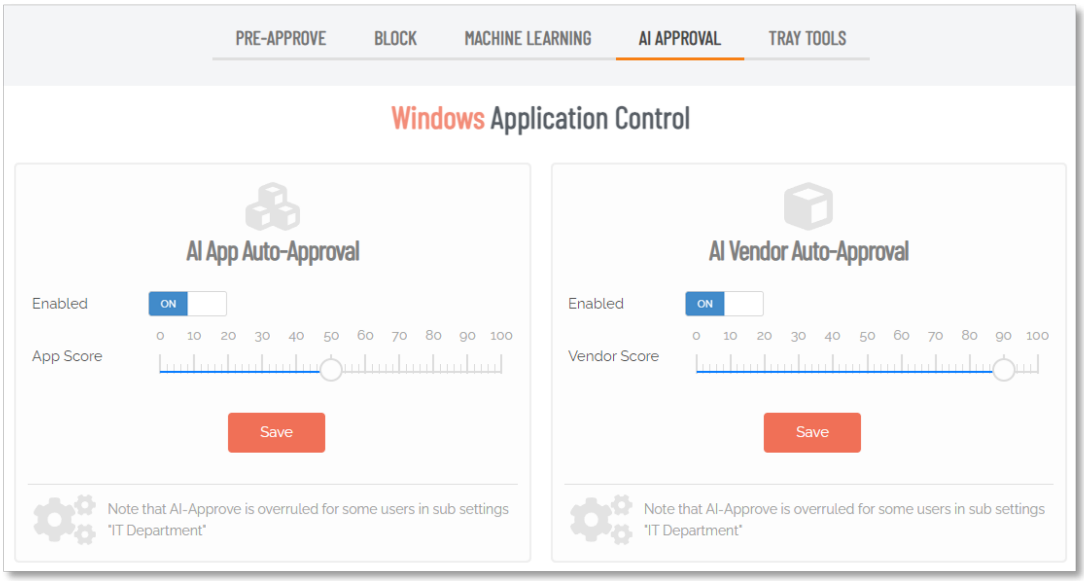
Sample Application Scores

Samples from 12,969,774 known applications

Application	Vendor	App Score	Vendor Score ↑
BlueStacks Installer	BlueStack Systems	0	0
PDQ Inventory Console	PDQ.COM CORPORATION	0	0
TruVision Navigator 9.0	United Technologies Corporation	0	0
Flexera Software LLC	Flexera Software LLC	0	1
Java(TM) Update Checker	Sun Microsystems	2	1
Dassault Systemes installer	Dassault Systemes SE	1	2
LibreOffice 7.4.1.2	The Document Foundation	0	2
RazerCortex	Razer USA Ltd.	2	2
Tableau 2020.4 (20204.22.0915.0322)	Tableau Software LLC	0	2
VideoOS Installer	Milestone Systems A/S	2	2
Zebra_2022.1 (2)	Seagull Scientific Inc.	0	2
DameWare products	Solarwinds Worldwide	2	3
TightVNC	GLAVSOFT	10	4
Zscaler	Zscaler	5	4
paint.net Setup	dotPDN LLC	20	5
Postman Agent	Postman	1	5
Dropbox Update	Dropbox	19	6
FortiClient Console	Fortinet Technologies (Canada) Inc.	3	6
FortiClient System Tray Controller	Fortinet Technologies (Canada) Inc.	10	6
Rockwell Automation Installer	Rockwell Automation Inc	8	6

Page 1 of 4 (75 items)

2. Now, in the portal, configure your tenant's App and Vendor **Enabled** toggles and score their values as desired. Following our example, we use App Score **45** and Vendor Score **90**:



Windows Application Control

AI App Auto-Approval

Enabled: ON

App Score

Note that AI-Approve is overruled for some users in sub settings "IT Department"

AI Vendor Auto-Approval

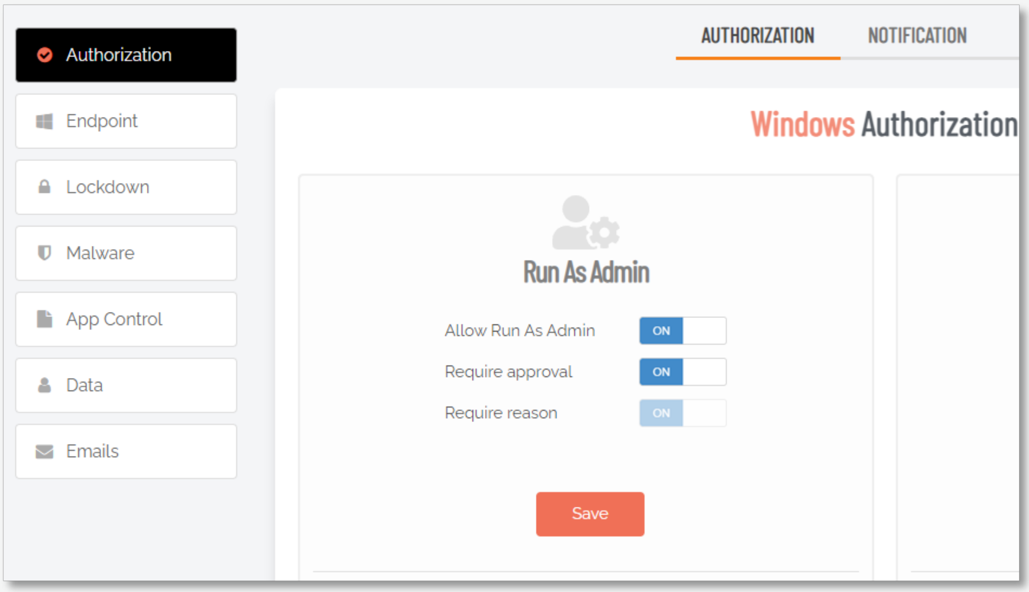
Enabled: ON

Vendor Score

Note that AI-Approve is overruled for some users in sub settings "IT Department"

KEY POINT:

AI Approval will have no effect unless you have **Require approval** toggled **ON** under **Endpoint Privilege Management > Settings > Windows Settings > Authorization > AUTHORIZATION**:

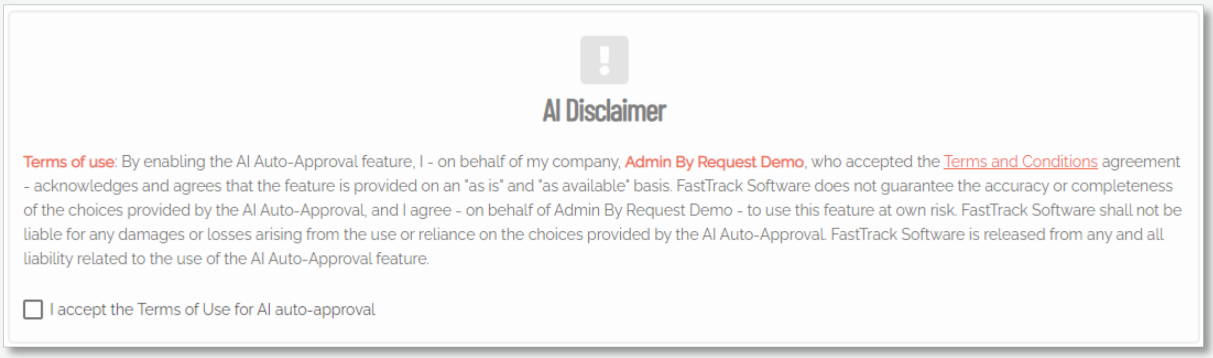


Allow Run As Admin ON

Require approval ON

Require reason ON

Regardless, you must accept the AI Disclaimer that pops up when either App or Vendor auto-approval is enabled:



AI Disclaimer

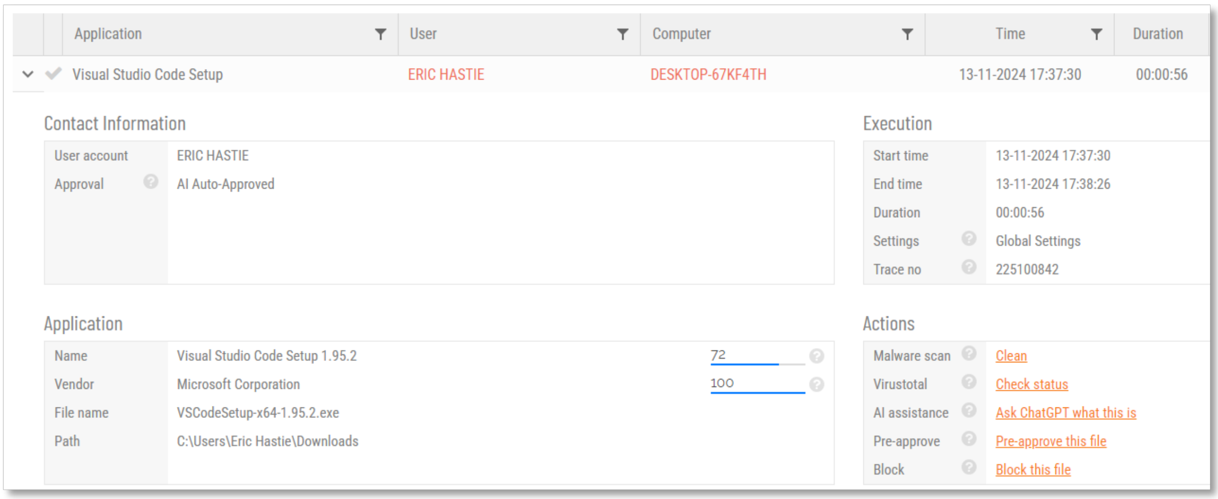
Terms of use: By enabling the AI Auto-Approval feature, I - on behalf of my company, Admin By Request Demo, who accepted the Terms and Conditions agreement - acknowledges and agrees that the feature is provided on an "as is" and "as available" basis. FastTrack Software does not guarantee the accuracy or completeness of the choices provided by the AI Auto-Approval, and I agree - on behalf of Admin By Request Demo - to use this feature at own risk. FastTrack Software shall not be liable for any damages or losses arising from the use or reliance on the choices provided by the AI Auto-Approval. FastTrack Software is released from any and all liability related to the use of the AI Auto-Approval feature.

☐ I accept the Terms of Use for AI auto-approval

3. When AI auto-approval is enabled, users installing applications may or may not need approval, depending on your tenant's App and Vendor scores.

In our example, when a non-admin user installs these apps, the following entries are logged in the Auditlog:

- Visual Studio Code Setup: App Score **72**, Vendor Score **100**. Required scores from settings: App Score **45**, Vendor Score **90** => no approval required (see *AI Auto-Approved* below):



	Application	User	Computer	Time	Duration
✓	Visual Studio Code Setup	ERIC HASTIE	DESKTOP-67KF4TH	13-11-2024 17:37:30	00:00:56

Contact Information

User account	ERIC HASTIE
Approval	AI Auto-Approved

Execution

Start time	13-11-2024 17:37:30
End time	13-11-2024 17:38:26
Duration	00:00:56
Settings	Global Settings
Trace no	225100842

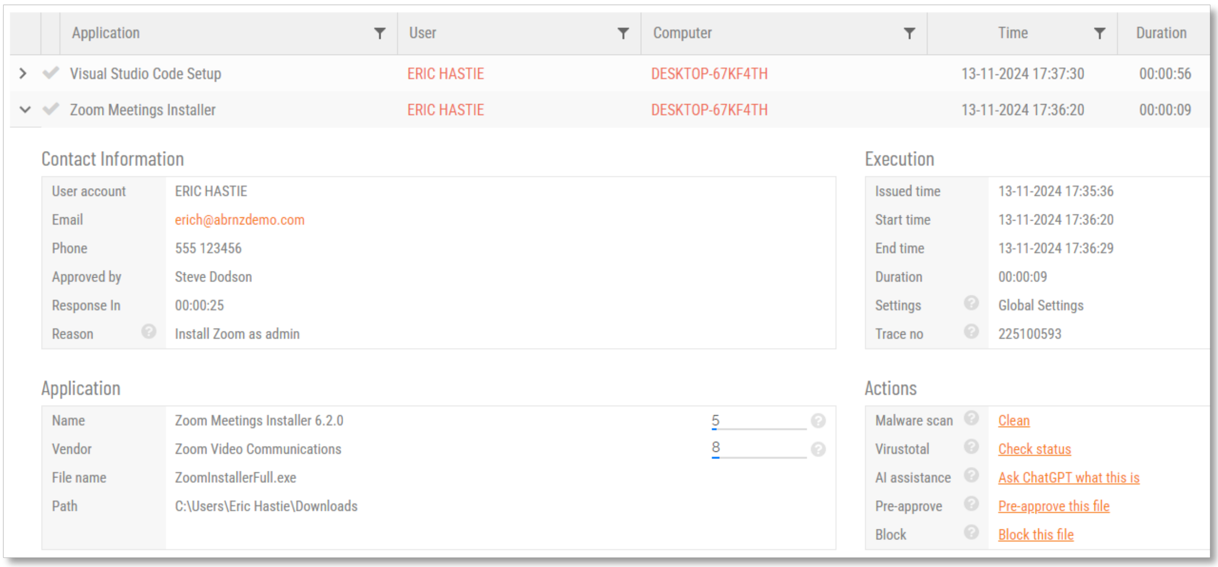
Application

Name	Visual Studio Code Setup 1.95.2	72
Vendor	Microsoft Corporation	100
File name	VSCodeSetup-x64-1.95.2.exe	
Path	C:\Users\Eric Hastie\Downloads	

Actions

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

- Zoom Meetings Installer - App Score **5**, Vendor Score **8**. Required scores from settings: App Score **45**, Vendor Score **90** => approval required (see *Approved by* below):



	Application	User	Computer	Time	Duration
✓	Visual Studio Code Setup	ERIC HASTIE	DESKTOP-67KF4TH	13-11-2024 17:37:30	00:00:56
✓	Zoom Meetings Installer	ERIC HASTIE	DESKTOP-67KF4TH	13-11-2024 17:36:20	00:00:09

Contact Information

User account	ERIC HASTIE
Email	erich@abrnzdemo.com
Phone	555 123456
Approved by	Steve Dodson
Response In	00:00:25
Reason	Install Zoom as admin

Execution

Issued time	13-11-2024 17:35:36
Start time	13-11-2024 17:36:20
End time	13-11-2024 17:36:29
Duration	00:00:09
Settings	Global Settings
Trace no	225100593

Application

Name	Zoom Meetings Installer 6.2.0	5
Vendor	Zoom Video Communications	8
File name	ZoomInstallerFull.exe	
Path	C:\Users\Eric Hastie\Downloads	

Actions

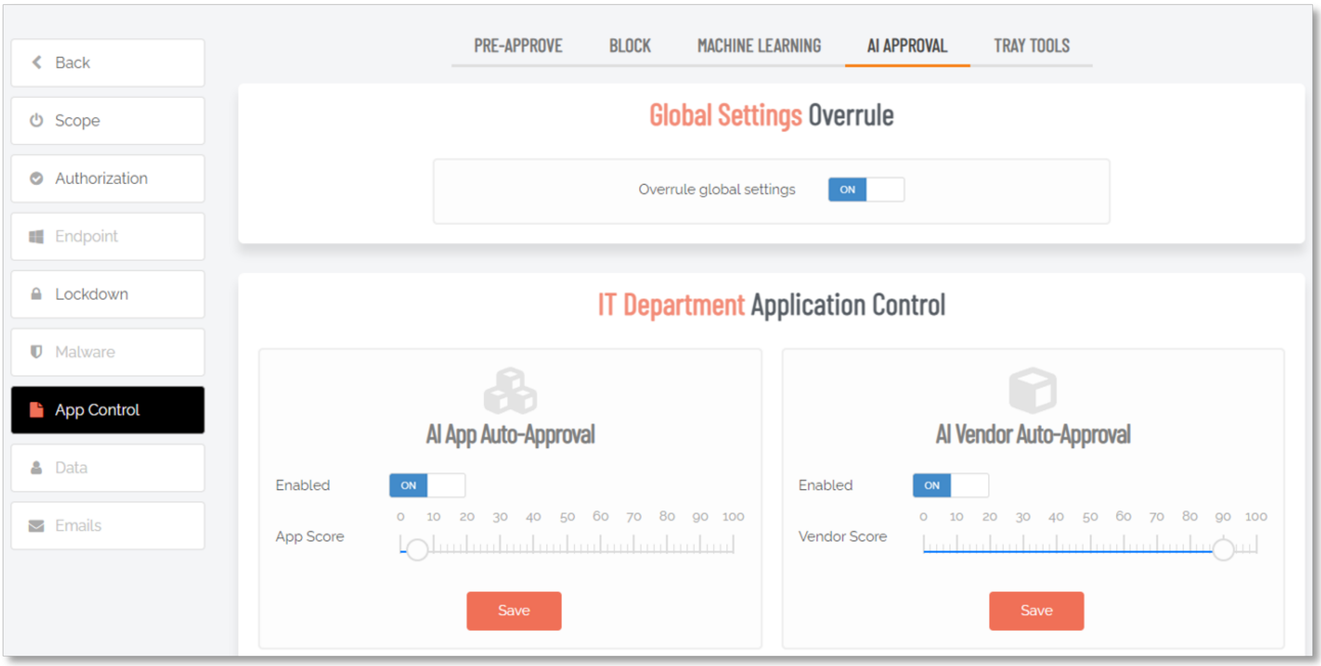
Malware scan	Clean
Virustotal	Check status
AI assistance	Ask ChatGPT what this is
Pre-approve	Pre-approve this file
Block	Block this file

Sub-Settings

Like all Admin By Request features, you can set Global settings to apply to all users, and create Sub-Settings as 'exceptions to the rule'. The same goes for AI Approvals.

A use case for a Sub-Settings could be members of the **IT Department**, who are more likely to require 'exotic' applications from time to time – not just the common apps used frequently by other users.

For this Sub-Setting, you could override Global Settings and set the auto-approve App score to a lower value, e.g., **5**, so that auto approvals include less-common applications. For all other users (outside of the Sub-Setting scope), the App Score threshold would remain at **45**:



Global Settings Overrule

Overrule global settings ON

IT Department Application Control

AI App Auto-Approval

Enabled ON

App Score

AI Vendor Auto-Approval

Enabled ON

Vendor Score

Refer to Windows Settings > App Control > AI Approval tab for settings information.