

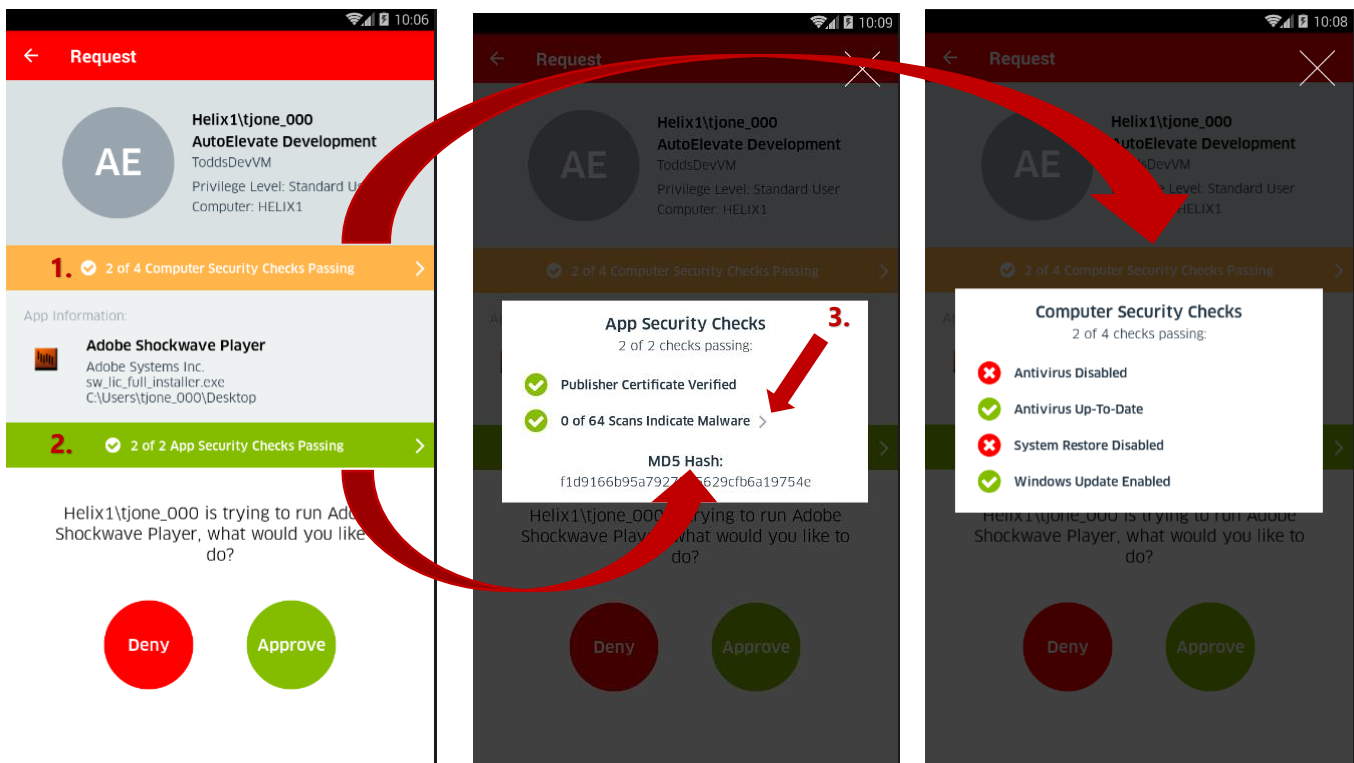


VirusTotal Integration Enhancements

AutoElevate’s commercially licensed integration with VirusTotal brings a powerful analysis tool to the fingertips of your Engineers as part of AutoElevate’s core product at no additional charge. VirusTotal inspects items with over 70 antivirus scanners and services, in addition to a myriad of tools to extract signals from the studied content. AutoElevate has summarized this file intelligence with easy to understand color signaling so that engineers can easily see the disposition and reputation of items that are being requested quickly with a glance.

Additionally, as part of the integration changes have been made in separation of the Computer security information and the Application security information. This gives the engineer the ability to make decisions based on the disposition of the machine where the request is taking place and based on what’s being requested.

In the Mobile Apps:



1. Computer Security Banner – Summarizes basic security information related to the disposition of the machine. The banner changes color from Green, Yellow, to Red depending on the number of checks failed giving engineers a quick and clear visual indication as to the status. By clicking into the banner additional information be displayed.

2. Application Security Banner – Summarizes application security information related to the disposition of the application/process being requested for elevation. The banner changes color from Green, Yellow, to Red depending on the number of checks failed giving engineers a quick and clear visual indication as to the status. By clicking into the banner additional information be displayed including the VirusTotal summary information.

3. VirusTotal Summary Banner – Summarizes the information from VirusTotal as to how many anti-virus software manufacturers or services have record of the MD5 hash and how many have scanned it as either good or malicious. Since false positives can exist from any given anti-virus manufacturer or service either 1 or 2 sources showing the item to be malicious would result in a 'yellow' or caution banner which would be good to investigate further, 3 or more would result in a Red banner indicating that extreme caution should be taken along with further research. The VirusTotal Summary can be clicked which will automatically launch a browser taking you to the VirusTotal information for that item so that further research can be done.

In the Admin Portal Request Screen:

The screenshot displays a 'Request' screen with a red header. It is divided into two main sections: 'Company/Location/User Info' and 'App Info'. Below these are security check results and a confirmation dialog.

Company/Location/User Info	
Username	Helix1\tjone_000
Company	AutoElevate Development
Location	ToddsDevVM
Privilege Level	Standard User
Computer	HELIX1

App Info	
App Name	Adobe Shockwave Player
Publisher Name	Adobe Systems Inc.
Filename	sw_lic_full_installer.exe
Path	C:\Users\tjone_000\Desktop
MD5 Hash	f1d9166b95a7927565629cfb6a19754e

2. App Security Checks: 2 of 2 Passing

Publisher Cert Verified	✓
0 of 64 Scans Indicate Malware 🔗	✓

3. Computer Security Checks: 2 of 4 Passing

Antivirus Enabled	✗
Antivirus Up-To-Date	✓
System Restore Enabled	✗
Windows Update Enabled	✓

Helix1\tjone_000 is trying to run Adobe Shockwave Player, what would you like to do?

DENY **APPROVE**

VirusTotal Summary in Tickets:

Notes

SCHEDULE ME ASSIGN ME ^

Discussion 2 Internal 0 Resolution 0 All 2 Customer Has Updated

Descending v ^ v

1.

API Member ?
Fri 12/21/2018 9:56 AM UTC-05
0 of 64 Scans Indicate Malware: <https://www.virustotal.com/file/597fcc52570600f33fff2a9db19d7c68349131d6e637b1b776b86ac368bf9064/analysis/1507750289/>

API Member ?
Fri 12/21/2018 9:56 AM UTC-05

General Information
Company Name: AutoElevate Development
Computer Name: HELIX1
Logged In User: Helix1\tjone_000
Privilege Level: Standard User

App Information
Name: Adobe Shockwave Player
Description: Adobe Shockwave Player
Vendor: Adobe Systems Inc.
Version:
Path: C:\Users\tjone_000\Desktop\sw_ljic_full_installer.exe

1. **VirusTotal Summary Banner** – An additional time entry now is entered into the ticket which summarizes the information from VirusTotal as to how many anti-virus software manufacturers or services have record of the MD5 hash and how many have scanned it as either good or malicious. The VirusTotal Summary can be clicked which will automatically launch a browser taking you to the VirusTotal information for that item so that further research can be done.

[The rest of this page left intentionally blank]