AutoElevate
freedom users want, control admins need

# Web Admin Portal Overview

The Web Admin Portal consists of 5 main areas – Dashboard, Computers, Events, Requests, and Rules.

Aside from the Dashboard, each page contains a data grid that is designed to allow you to find, sort, and view data quickly and easily. Column headers can be dragged to the top which then groups all data by that data type. You can group as many headers together as you would like. Change the grouping by changing the order in the header. You can also sort each column in ascending/descending or descending/ascending order by clicking the column header. Each column can be filtered by any letters, words, numbers or text by typing into the spot at the top or each column that says “filter”. Each column can be ordered in the grid by clicking the column header and dragging it back and forth in the list for the desired order.

## Dashboard

The Dashboard is divided into 3 sections - Security, Agent Deployment, and 30 Day Results. All sections display results from the past 30 days.

### Security

- **Systems with UAC Off** - Systems with UAC Off represent a security risk. With the UAC in an Off state Windows systems do not generate any UAC events or dialog boxes and therefore AutoElevate has nothing to track or intercept.
- **Systems with UAC Low** - This number is a combination of the previous number (Systems with UAC Off) as well as machines that have the UAC set to Level 1. With the UAC set to this level Windows systems do not generate any UAC events or dialog boxes and therefore AutoElevate nothing to track or intercept.
- **Operating with Admin Privileges** - Machines checking in within the last 30 days which are either actively logged in with a user operating with Admin privileges or were last logged in with an Admin user.

### Agent Deployment

- **Systems in Audit Mode** - Systems with AutoElevate operating in Audit Mode. In Audit mode system state and UAC events are logged but the user experience is not altered.
- **Systems in Live Mode** - Systems with AutoElevate operating in Live mode. In Live mode UAC events are intercepted, users are given the opportunity to initiate real time approval, and rules are automatically applied.
- **Systems Ready to Go Live** - Systems that have the UAC On and users which are operating with Standard privileges.

### 30 Day Results

- **Requests Fulfilled** - Real-Time requests that were responded to by technicians within the last 30 days.

- **Rules Applied** - Instances in the last 30 days where an established rule elevated privileges for the end user without technician intervention.
- **Rules Missed (in Audit Mode)** - UAC events that took place on machines operating in Audit mode when the UAC event matched an existing rule. This indicates an instance where automatic elevation (or denial) could have taken place automatically had the agent been in Live mode.

# Computers

Each line in the Computer data grid is a computer that an agent is installed and collecting data on. The following is the list of data currently available for each Computer:

- **Company** – Company Name – This information is pulled from the registry of each machine and communicated back to the Web Admin Portal. If the Company does not exist when the agent 1st checks in the Company will be created automatically in the Web Admin Portal.
- **Location** – Location Name – This information is pulled from the registry of each machine and communicated back the Web Admin Portal. If the Location does not exist when the agent 1st checks in it is created automatically. Locations can be used to organize computers into groups which are specifically location based. For instance you could create Locations of Atlanta, Denver, New York for a Company or you could make one called Main Office and Laptops or any combination that you desire.
- **Name** – Name of the computer. When an agent is 1st installed it is assigned a unique identifier by AutoElevate which is how it is identified by the Web Admin Portal. When a computers name is changed the Web Admin Portal is aware of that change and updates the computer automatically.
- **Operating System** – Operating system, version, and build of the computer.
- **UAC Status** – "On" or "Off". Displays if the UAC is on or off for the given computer. If the UAC is changed the machine must be rebooted for Windows UAC functionality to behave properly.
- **UAC Admin Level** – Displays the UAC Admin Level of 1, 2, 3, or 4.
- **UAC User Level** – Displays the UAC User Level of 1, 2, 3, or 4.
- **Active User Name** – Displays the name of any user that is currently logged into the machine. If it is blank that indicates the machine is logged out.
- **Active User Privilege Type** – Displays the privilege level of the currently logged in user.
- **Domain Member?** – "TRUE/FALSE" - Displays if the currently logged in user is a Domain Member ("TRUE") or a local user ("FALSE").
- **Anti-Virus Enabled?** – "TRUE/FALSE" – Displays if the Anti-Virus is enabled or disabled.
- **Anti-Virus Up-To-Date?** - "TRUE/FALSE" – Displays if the Anti-Virus is up to date.
- **System Restore Enabled?** - "TRUE/FALSE" – Displays if the Windows System Restore is enabled or disabled.

- **Windows Update Enabled?** - "TRUE/FALSE" – Displays if the Windows System Update is enabled or disabled.
- **Agent Mode** – "Audit", "Live", or "Technician" – When an agent is installed for the 1st time it automatically is installed in "Audit" mode which is designed to gather information about the machine and UAC events without changing the user experience. "Live" mode turns the AutoElevate agent into an active state in which is actively looks for and intercepts UAC events. "Technician" mode is an audit mode which is initiated directly from the machine so that a technician working on the machine locally can temporarily prevent AutoElevate from intercepting UAC events.
- **Agent Version** – The build version of the AutoElevate agent.
- **Last Ping** – Date and time that the agent has last checked in with the Web Admin Portal.

# Events

Each line in the Events data grid is a UAC event that was recorded from a computer that has an agent that is installed and turned on. The UAC event data is collected regardless of whether the machine is in Audit, Live, or Technician mode as long as the UAC is on. The following is the list of data currently displayed in the Event screen for each UAC event:

- **Company** – Name of your client which the computer is registered under.
- **Location** – Location Group of the computer.
- **Computer Name** – Name of computer on which the UAC event took place.
- **Vendor** – The name of the software manufacturer (i.e. “Microsoft”)
- **Name** – The name of the application that initiated the UAC event
- **Version** – Version number of the application collected from the application properties
- **Description** – Application description collected from the application properties
- **Path** – Path on the machine where the file is located.
- **Publisher Cert Verified** – Displays if the application publisher certificate is valid and verified.
- **Anti-Virus Enabled?** – Displays if the Anti-Virus was enabled when the UAC event took place.
- **Anti-Virus Up-to-Date?** Displays if the Anti-Virus was Up-to-date when the UAC event took place.
- **System Restore Enabled?** Displays if Windows System Restore was enabled when the UAC event took place.
- **Windows Update Enabled?** Displays if Windows Update was enabled when the UAC event took place.
- **MD5 Hash** – the unique MD5 hash calculation for the application.
- **Date Created** – Date/Time when the UAC event was created or occurred.

# Requests

Each request represents an UAC event in which the user specifically requested the installation. Each line in the Requests screen represents an interaction with a user. The following is the list of data currently displayed in the Request Screen:

- **Company** – Name of your client which the computer is registered under.
- **Location** – Location Group of the computer.
- **Computer Name** – Name of the computer where the user made the request.
- **Name** – Name of the application being requested.
- **Active User Name** – Name of the user that was logged into the computer when the Request was made.
- **Active User Privilege Type** - Displays the privilege level of the user making the request.
- **Date Created** – Date / Time of the request.

# Rules

The Rules screen displays any rules that have been made for either Approval or Denial and shows if they are a Global, Company, Location, or Computer rule. Clicking on the “trash can” icon next to each rule asks you to confirm if you wish to delete the rule. Currently rules can’t be moved from one level to another, they must be deleted and re-created at the new level.

- **Company** – Name of your client which the computer is registered under.
- **Location** – Location Group of the computer.
- **Computer Name** – Name of the computer where the user made the request.
- **Name** – Name of the application being requested.
- **Trigger Identifier - MD5 Hash** – the unique MD5 hash calculation for the application.

- **Approved?** – "TRUE/FALSE" – indicates whether the rule is Approved = True, or Denied = False.
- **Created By?** – Name of the AutoElevate user that made the rule.
- **Date Created** – Date and Time when the rule was created.