AutoElevate
freedom users want, security admins need

Audit Guide

By default when a new agent is installed it is set into “Audit” mode, which is designed not to change the user experience but will allow you to examine the security disposition of all the machines in your environment so that you can put together a Plan Of Action to tighten up security and begin using AutoElevate in Live mode. The following document considers some questions that would be good to review as part of your process and includes how to use the AutoElevate Admin Portal to gather the necessary information and how to use specific Labtech scripts to make necessary adjustments.

How many machines have their security set in a way that puts you at risk and makes them vulnerable to a business ending security breach?

Best practice is for UAC to be turned on

To determine if UAC turned off or on do the following from the Admin Portal:

From the Computers Screen:

- Drag “UAC Status” column header to the top
- To set the UAC on/off do the following:
  - Check off the box next to the computer(s) that you want to set change the UAC setting on
  - Then click on the 'Actions' menu (near the top of the screen)
  - Select to set UAC to one of the following settings (under the UAC Settings heading):
    - Set to On (Not Dimmed)
    - Set to On (Dimmed)
    - Set to On (Maximum)
    - Set to Off

Notes About Changing UAC Status:

Our system does not initiate a system reboot but one is necessary for Windows to change the UAC from On to Off or vice versa, this is regardless of whether it is changed via our system, your RMM, or directly from Windows.

AutoElevate will give you status on whether the system has been rebooted since requesting the change and the status of whether or not it has been changed and has been rebooted in the

SuperUser Software, Inc. dba. AutoElevate; 777 Brickell Ave #500-9319; Miami, FL 33131
© 2017 SuperUser Software, Inc. dba. AutoElevate – ALL RIGHTS RESERVED

"UAC Status" column on the Computer screen.

Once one of the computers is in an "On" state and has been rebooted, it can be changed to any of the other "On" states without requiring a reboot (i.e. changing from On (Not Dimmed) to On (Dimmed) etc.). Once the system agent checks in with the Admin Portal the change will take place immediately.

There are some subtle differences in UAC settings when manually logging in and changing the sliders in Windows so we have consolidated those settings down to 3 options which can be set in AutoElevate which then set the appropriate settings for all types of users for the machine. The UAC settings are:

- **"Not Dimmed"** - means that the Windows UAC dialog boxes are being launched in the logged in users desktop session and therefore is possible for applications or processes running in that desktop session to potentially interact with the UAC dialogs.
- **"Dimmed"** - means that the Windows UAC dialog boxes are being launched in a special private and isolated desktop session which is separate from the user and therefore prevents applications or processes running as the user from interacting with the UAC dialogs which is a more secure method.
- **"Maximum"** - is a setting which applies specifically to users that are logged in as an Administrator. Maximum UAC will make it so that Administrators are both "Dimmed" and get prompted not just for application installs or file elevations but also for administrative tasks.

Best practice is for users to be only running as “Standard Users”

To determine if users are running as Admins or as Standard Users look in the Admin Portal:

From the Computers Screen:

- Drag “Active User Privilege Type” column header to the top, this will sort machines by what type of privilege level machines are running. Take note of users that are running as Administrators and make arrangements to get into the machine and change the users permissions level. If user must run as Administrator make sure UAC is on and UAC Admin Level is set to 3 or preferably 4.

Best practice is for UAC User Level 3 or 4 and UAC Admin Level to be set to 2 or higher

By settings the UAC On and either Dimmed or Not Dimmed from the Admin Portal these settings are set appropriately for you and are then reflected in the UAC User Level & UAC Admin Level columns.

SuperUser Software, Inc. dba. AutoElevate; 777 Brickell Ave #500-9319; Miami, FL 33131
© 2017 SuperUser Software, Inc. dba. AutoElevate – ALL RIGHTS RESERVED

Are your best practices being followed and implemented at your client sites?

- **Is System Restore on?**
- **Is Anti-Virus enabled?**
- **Is Anti-Virus up-to-date?**
- **Is Windows update enabled?**
    - Evaluate the security disposition of the machines at each Company and Location
        - Drag each of the following column headers to the top, to examine machines by each group that may need adjustments
        - Drag “System Restore Enabled” column header to the top
        - Drag “Anti-Virus Enabled” column header to the top
        - Drag “Anti-Virus Up-to-date” column header to the top

What machines under your management would be targeted by hackers with the latest malware because end users are working with too many privileges?

- Look for machines that have a large number of users which are part of the Admin group
    - Close “Company” and “Location”
    - Click on the “Admin Users” header to sort by computers with the highest number of admin users

Are users REALLY being inconvenienced by not having admin privileges? How many users have them? How often do they need them? And for what?

- Once you have UAC turned on and the agents installed run the client machines for a period of time in “Audit” mode to monitor and determine how many times machines are having UAC events and what is being requested

- From the Events Screen
- Drag the “Computer Name” column header to the top to group Events by Computer
- Drag either the “Vendor” or “Name” column header to the top to see most common requests

SuperUser Software, Inc. dba. AutoElevate; 777 Brickell Ave #500-9319; Miami, FL 33131
© 2017 SuperUser Software, Inc. dba. AutoElevate – ALL RIGHTS RESERVED