



Configuring Global RES PowerFuse Settings for Specific Users

RES PowerFuse 2008

Disclaimer

Whilst every care has been taken by RES Software to ensure that the information contained in this publication is correct and complete, it is possible that this is not the case. RES Software provides the publication "as is", without any warranty for its soundness, suitability for a different purpose or otherwise. RES Software is not liable for any damage which has occurred or may occur as a result of or in any respect related to the use of this publication. RES Software may change or terminate this publication at any time without further notice and shall not be responsible for any consequence(s) arising there from. Subject to this disclaimer, RES Software is not responsible for any contributions by third parties to this publication.

Copyright Notice

Copyright © 1998-2008 RES Software, The Netherlands. RES®, PowerFuse®, Wisdom®, Orchestra®, Insight® and the RES logo are either registered trademarks or trademarks of RES Software in Europe, the United States and other countries. Microsoft and Windows are either registered trademarks of Microsoft Corporation in the United States and/or other countries. All other product and company names mentioned may be trademarks and/or service marks of their respective owners.

Copyright © RES manuals, training materials and software 1998-2008 Real Enterprise Solutions Development BV, The Netherlands. Patents Pending.

Any rights not expressly granted herein are reserved by RES Software or Real Enterprise Solutions Development BV.

1. Background

Many, but not all, configuration settings in RES PowerFuse 2008 offer Access Control and Workspace Control security. This makes those settings flexible and easy to configure.

For the RES PowerFuse settings that do not contain Access Control and Workspace Control, you can still configure exceptions for specific (groups of) users. For this purpose you can use a Windows registry setting in RES PowerFuse.

This white paper explains how to do this.

Please note that the recommended way to work with RES PowerFuse is to use the RES PowerFuse Management Console. Use the registry setting method as described in this white paper only when there is no other option.



Warning:

Incorrectly editing the Windows registry may severely damage your system. Before making changes to the Windows registry, you should back up any valued data on your computer.



Terminology:

Some well-known terms from RES PowerFuse 7.03 have changed in RES PowerFuse 2008:

- The Real Enterprise Manager is now called the **RES PowerFuse Management Console**.
- Computers that run RES PowerFuse are now called **RES PowerFuse Agents**.
- The RES PowerFuse database is now called the **RES PowerFuse Datastore**.
- The RES Service (res.exe) is now called the **RES PowerFuse Agent Service**.

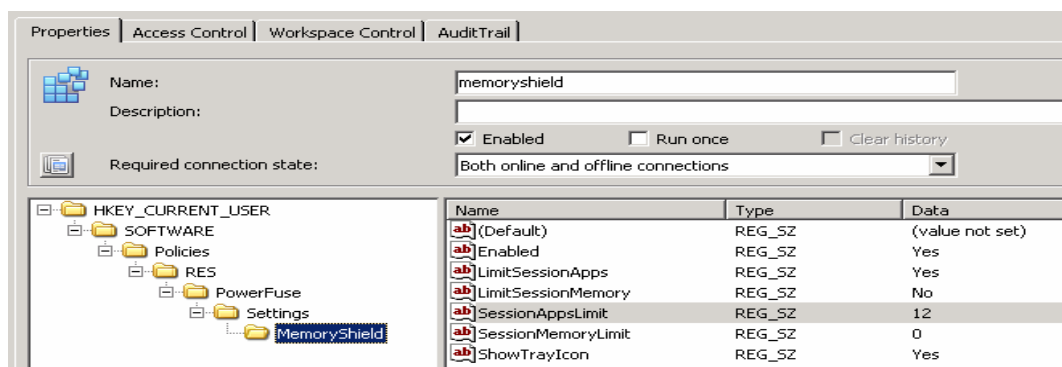
2. An example case

You may need to use Workspace Control and Access Control for a setting such as MemoryShield, for instance to give Terminal Servers different MemoryShield settings than other RES PowerFuse agents in your environment.

This document describes an example of such a situation, based on a fictional company called D-Energy with 400 workplaces in the New York head office. These 400 RES PowerFuse agents form a mixed environment: Terminal Servers, workstations and laptops. The office has a central Datastore on an SQL server. A workspace has been created for the Terminal Servers in this company.

For standard workstations, the maximum number of applications has been limited to 5 and the amount of memory per session to 50MB. The system administrator wants to configure different MemoryShield settings for all users within the OU: **D-Energy.local\USA\New York\Administration**. This Organizational Unit contains all Terminal Servers in New York. The administrator wants to set the maximum number of running applications per session to 12. He also wants to allow an unlimited amount of memory per session for this group of Terminal Servers.

The administrator creates a Registry settings file and imports it into the PowerLaunch node of RES PowerFuse by selecting "Import Registry File...". RES PowerFuse recognizes the key settings as an HKLM key and will change it to HKCU. The setting of the SessionAppsLimit String Value is then changed from 5 to 12.



The changed setting is then restricted to the relevant users and the relevant computers:

- On the Access Control tab, at the Identity section, the Administration OU in New York is selected. This OU contains all users that should receive this setting.
- On the Workspace Control tab the Workspace **Terminal Servers NY** is selected.

This is saved as a PowerLaunch Registry setting.

The configuration is now complete. Users located in the OU D-Energy.local\USA\New York\Administration who start a RES PowerFuse session on a Terminal Server within the **Terminal Servers NY** Workspace will be able to run twelve applications simultaneously in their session.

Step-by-step instructions of this procedure are given in the next chapter.

3. Step by Step

Summarizing, here are step-by-step instructions for using registry settings in RES PowerFuse.

1. On a RES PowerFuse Agent, open the Windows Registry by running the command "regedit".
2. Navigate to the registry line HKLM\SOFTWARE\Policies\RES PowerFuse\Settings\Xxx (where Xxx represents the key to be exported, *e.g.* MemoryShield).
3. Click **File > Export**.
4. Save the file: choose a location and enter a file name (*e.g.* MemShSetting.reg).
5. In the RES PowerFuse Management Console, go to: Configuration Management > PowerLaunch > User Registry.
6. Click the **Add Registry** button.
7. In the menu **Registry**, click on **Import registry file**.
8. Browse to the .reg file that you have saved earlier (see step 4) and open it.
9. Click **No** when you are asked: "... Do you want to ignore these keys?".
10. Click the **Properties** tab and change all settings as needed.
11. Click the **Access Control** tab to configure the Access Control criteria of the registry setting:
 - a) In the Identity area, click **Add** to select groups, users security roles or languages to which the setting applies. This will open the **Identity** window.
 - b) Click **Resolve users** to retrieve information about the users that you assigned. This will open the **Assigned users** window.
 - c) In the Location area, click **Add** to limit the setting to a PowerZone. This will open the **Location** window.
 - d) Alternatively, click **Edit** or **Delete** to modify existing entries.
12. Click the **Workspace Control** tab and indicate to which workspace(s) the registry setting applies.

4. Conclusion

Some RES PowerFuse settings that do not have Access Control and Workspace Control options in the RES PowerFuse Management Console are configurable by importing settings into the User Registry. In this white paper we have described how to use the Windows registry to configure RES PowerFuse settings in PowerLaunch.

Below is an overview of the registry settings that can be configured that way:

- Desktop configuration & Lockdown
- ScreenSaver
- Start Menu & Taskbar
- WebTop
- MemoryShield
- Directory Maintenance
- Security Management

Recommended reading:

This white paper is part of a series of white papers. Recommended reading order:

1. "The Architecture of RES PowerFuse 2008".
2. "How to increase the Manageability of Your RES PowerFuse Environment".
3. "Configuring Global RES PowerFuse Settings for Specific Users".
4. "The RES PowerFuse Replication Model".

You can download these white papers from the download section of the RES Software website: <http://www.ressoftware.com/downloads>.