



Feature Guide Removable Disks Security



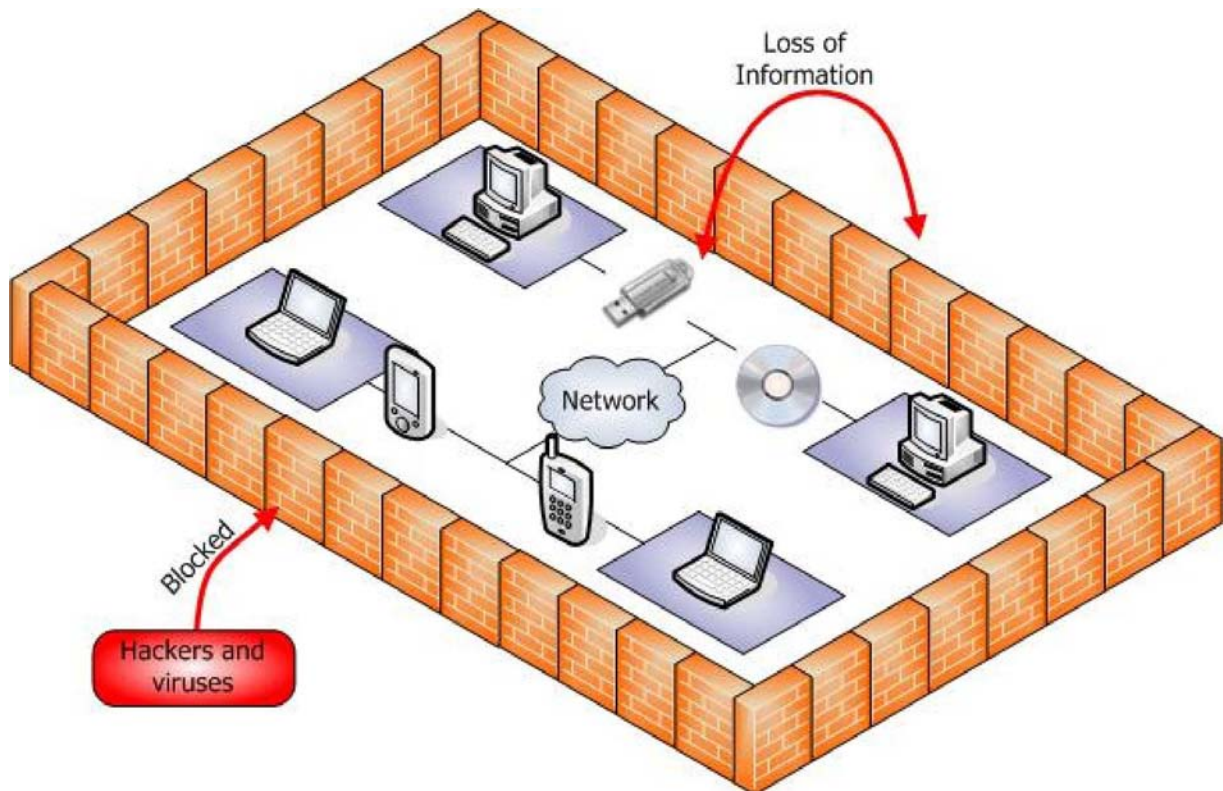
1 Introduction

Nowadays all companies equip their networks with firewalls, access control, and anti-virus solutions to protect themselves against threats like data theft, hackers, and virus attacks. These threats can cause loss of critical and confidential company information. However, in 80% of all cases this loss of information is caused by internal reasons. What are these reasons?

" A recent research from Ernst & Young found that 75% of the participated companies are forced to take measures within the next six months on the removable media used in their company. Removable media cause too many security leaks in their IT-environment."*

Technologies like USB and FireWire are a step forward in the development of new types of hardware and software, but are these technologies also a step forward for the security level that is required nowadays? Removable disks like memory sticks or digital cameras can be used on each computer. Because of their portable nature, they can cause loss of information and are an internal threat for each company.

Wouldn't it be great to manage and control all removable disks from a central point of administration? Real Enterprise Solutions created the management solution for this problem. This unique feature is called Removable Disks Security and is available in RES PowerFuse Edition 2005.



Loss of important company information is caused in 80% of the cases by internal reasons. Removable media is one of those reasons.

*Global Information Security Survey 2005, Ernst & Young.



2 Removable Disks Security in RES PowerFuse Edition 2005

How are removable media managed at this moment?

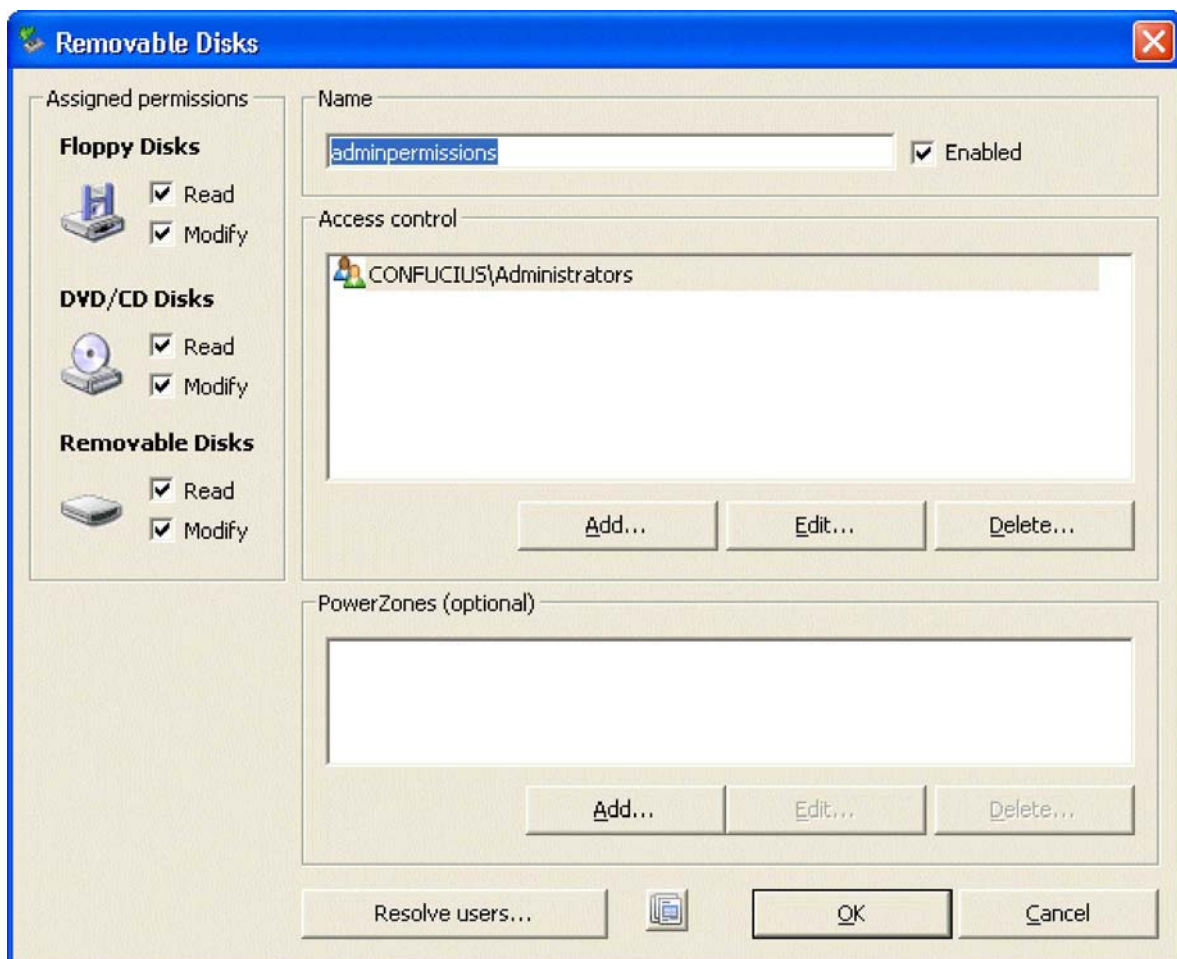
Removable disks like memory sticks and external hard drives are easy to use, but difficult to manage in an IT-environment. Every user can connect his own memory stick and copy critical and confidential files to it or accidentally infect the system with viruses and worms. The same issue exists with external hard drives. How can this be prevented?

USB and FireWire ports can be closed at the local client, but then a simple USB mouse or keyboard or an application that uses an USB license key cannot be used. The floppy drive or CD/DVD-ROM drive can be removed from all computers, but this is time-consuming and not a proper solution. In addition, there are always users that need to use their floppy drive or DVD/CD-ROM drive in their daily work.

At this moment, Microsoft does not offer a solution to manage and control removable media in Windows. The consequence is that removable media may cause the loss or theft of critical and confidential company information or infection of the system with viruses and worms. This is a security leak for each company using Microsoft Windows at its local clients.

Removable Disks Security in RES PowerFuse Edition 2005

With the Removable Disks Security feature in RES PowerFuse Edition 2005, the use of removable disks can be configured for specific people on specific computers or locations. Different levels of permissions can be assigned to use floppy disks, DVD/CD disks, and other removable media. This is controlled by AppGuard technology, a local system driver that is also used for the unauthorized use of applications, files, and folders.



The Removable Disks Security feature has three security modes. The feature can be Disabled, Enabled or configured in Learning mode. This last option is very useful when configuring this feature: All illegal actions will be logged but not blocked. With the information in this log file, the configuration can be tuned before enabling Removable Disks



Security. This prevents many help desk calls from displeased users.

Multiple Removable Disks Security entries can be created with all their specific configurations. For each entry, different levels of permissions, Access Control and PowerZones can be used. With this type of configuration, exceptions can be made for specific users, computers, and locations.

Other removable media like mobile phones, PDA's (Personal Digital Assistants), and CD/DVD burners need a software program to communicate with the computer. The use of this software program can be managed with Application Management in PowerFuse.

Increase the security at the local client

The most important benefit is the increase of the security at the local clients. USB and FireWire ports are still open and can be used, but not for removable devices like memory sticks or external hard drives. The floppy drive and CD/DVD-ROM drive are still enabled, but the user will need permissions to use these drives. The Removable Disks Security feature increases the security of the entire IT-environment, because it prevents local use of removable disks. It helps safeguard your company against the loss of critical and sensitive company information.

Different levels of permissions

In some situations, a user needs permissions to read data from a floppy disk or a memory stick, but he should not have permissions to modify data. This configuration is possible with the Removable Disk Security feature in PowerFuse edition 2005. For each entry, different levels of permissions can be assigned to the floppy disks, CD/DVD disks and other removable disks. The configuration options are No permissions, Read-only permissions, and Read/Modify permissions. These different levels of permissions enable the system administrator to refine the Removable Disks Security entries.

Full control for the system administrator

The system administrator has complete control over the use of floppy disks, CD/DVD disks and other removable disks from one central point of administration. The combination of different levels of permissions, Access control and PowerZones enables the system administrator to configure and control the use of these disks. When a user without permissions tries to use removable disks, a message will be displayed and a log is created for the system administrator.

With these options, the system administrator has full control and is able to protect the entire IT-environment against the security threats of removable disks.

Time	File	Process	Computer	Username	S...	Operation	Action
16:16:29.797	a:\	pexplor...	RES\Q...	RES\luijt...	0	16448 - rea...	BLOCK
16:16:29.797	a:\	pexplor...	RES\Q...	RES\luijt...	0	68 - open re...	BLOCK
16:16:10.062	a:\	pexplor...	RES\Q...	RES\luijt...	0	68 - open re...	BLOCK
16:16:10.046	a:\	pexplor...	RES\Q...	RES\luijt...	0	16448 - rea...	BLOCK
16:16:08.451	a:\	pexplor...	RES\Q...	RES\luijt...	0	260 - open g...	BLOCK
16:16:08.451	a:\	pexplor...	RES\Q...	RES\luijt...	0	260 - open g...	BLOCK
16:16:08.435	a:\	pexplor...	RES\Q...	RES\luijt...	0	260 - open g...	BLOCK
16:16:07.184	a:\desкто...	pexplor...	RES\Q...	RES\luijt...	0	260 - open g...	BLOCK
16:16:05.824	a:\	pexplor...	RES\Q...	RES\luijt...	0	68 - open re...	BLOCK



3 Conclusion

Managing and controlling removable media has become a major security issue for each company nowadays. As mentioned in the introduction this security issue can cause loss or theft of critical and confidential company information that will lead to irrecoverable damage to a company. The Removable Disks Security feature in RES PowerFuse Edition 2005 is the solution for this issue.

From one central point of administration, the use of removable disks can be managed and controlled. The options Access control, PowerZones, and different levels of permissions can be configured for each Removable Disks entry. All unauthorized attempts to use floppy disks, CD/DVD disks, and other removable media will be displayed in the log file. This makes the feature easy to use and reliable.

New technologies mean new risks. The Removable Disks Security feature in RES PowerFuse Edition 2005 will manage and control removable disks and decrease the risks that are created by using them. This feature is indispensable for each company that wants to solve all current security issues that are created by removable media.



DISCLAIMER

RES created this guide to supply information that assists you with the installation of the RES PowerFuse product and framework. Although the greatest care has been taken to make this document as accurate as possible, Real Enterprise Solutions Nederland B.V. (The Netherlands), RES EMEA B.V. (Europe), and Real Enterprise Synergy Inc. (USA) cannot guarantee the complete accuracy of the information provided in this publication. This publication and the RES PowerFuse program can be changed or terminated at any given time without further notice. Real Enterprise Solutions Nederland B.V. (Netherlands), RES EMEA B.V. (Europe), and Real Enterprise Synergy Inc. (USA) disclaim any loss directly or indirectly due to using RES PowerFuse and its features or the information that is presented in this publication. This information is not warranted for any purpose.

Real Enterprise Solutions Nederland B.V. (Netherlands), RES EMEA B.V. (Europe), and Real Enterprise Synergy Inc. (USA) disclaim any loss which could directly, indirectly, or seemingly be related to the use of RES PowerFuse, the RES Subscriber, upgrade packs, PowerPacks, any other RES-supplied software, or the use of information provided by Real Enterprise Solutions Nederland B.V. (Netherlands), RES EMEA B.V. (Europe), or Real Enterprise Synergy Inc. (USA) through any other documents.

COPYRIGHT

Copyright © 1998-2006 Real Enterprise Solutions Development B.V., All rights reserved, patents pending. RES, PowerFuse, and the PowerFuse Logo are registered trademarks of Real Enterprise Solutions Development B.V. Windows is a registered trademark of the Microsoft Corporation in the United States and all other countries. All other product names, company names, marks, logos, and symbols are trademarks of their respective owners.

⚠ WARNING: *RES PowerFuse is protected by copyright law and international treaties. Unauthorized reproduction, distribution, reverse engineering, or decompiling of the program or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.*