

Directory Defender User Guide



Table of contents

Introduction	3
Welcome!	3
What is Directory Defender?	3
Installation.....	3
64 bit or 32 bit?	3
Hardware and Software Requirements	4
Running the Setup	4
Getting Help	4
Using Directory Defender	4
Install Directory Defender.....	4
Configure Defending Moves	5
Configure Defending Renames	8
Configure Defending Deletes.....	10
Add Exclusions.....	13
Set Up Email Alerts (optional)	13
Viewing the Log	14
Example of an Email Alert.....	15
About Blue Shoe Software	15

Introduction

© 2019 Blue Shoe Software LLC

ALL RIGHTS RESERVED.

No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher at the following address:

Blue Shoe Software LLC
Attn: Legal Dept.
424 East Central Boulevard
Suite720
Orlando, FL 32801

Ultimate Recycle Bin is a Trademark of Blue Shoe Software LLC.
Directory Defender is a Trademark of Blue Shoe Software LLC.
Blue Shoe Software is a Trademark of Blue Shoe Software LLC.
Trademarks may be registered in some jurisdictions.
All other trademarks are the property of their respective owners.

Welcome!

Thank you for choosing Directory Defender from Blue Shoe Software. Version 3 now includes the ability to not only block accidental folders moves, but also renames, and deletes. Configuration is much more flexible but still extremely quick and simple to set up. We would love to hear about your experiences using Directory Defender. Please find our contact information below.

What is Directory Defender?

Directory Defender is a unique tool brought to you by Blue Shoe Software.

How many times have you (or if you're a System Administrator, your users) accidentally moved a folder when clicking around in Windows Explorer? Too many to count?

We set out to solve this problem at the file server level. There is nothing to install or modify on your clients and your users can be running any operating system.

Install Directory Defender on your file server and configure it to block accidental folder moves, renames and deletes from network users. Problem solved!

Installation

64 bit or 32 bit?

Windows Vista, 7, and 8.x all come in 32 and 64 bit versions. We support both versions for each of these operating systems.

Beginning with Windows Server 2008 R2, only 64 bit versions are available. We provide a 32 bit and a 64 bit installation for Directory Defender. Don't worry, if you try to install on the wrong type, it won't let you. Just run the other type if you get an error installing.

Hardware and Software Requirements

Supported Windows Platforms

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008 (32-bit and 64-bit)
- Windows 10 (32-bit and 64-bit)
- Windows 8 / 8.1 (32-bit and 64-bit)
- Windows 7 (32-bit and 64-bit)
- Windows Vista (32-bit and 64-bit)

Running the Setup

The installer is very simple - just answer a few quick questions and the installer will do the rest. You should be all installed and running in a matter of minutes. No reboot necessary! Please be sure to pause anti-virus / anti-malware software prior to running the setup exe. Some anti-virus software, such as McAfee VirusScan Enterprise, will block the setup exe from launching and our drivers from installing properly.

Getting Help

If you run into any problems during installation, or after, please feel free to email our support team at support@blueshoesoftware.com

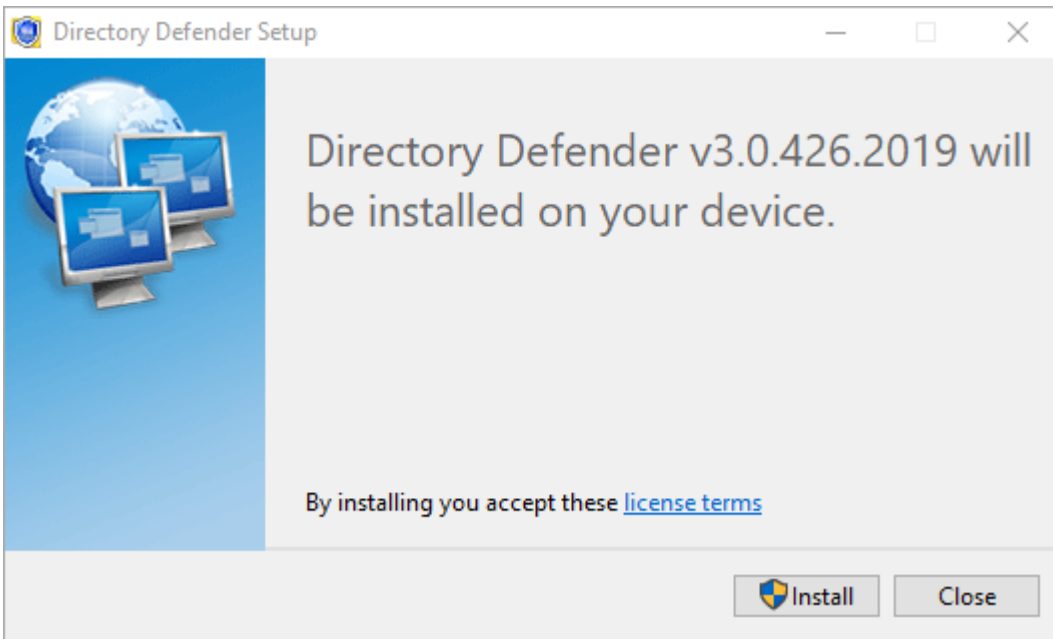
Plus, you can get more information and answers to frequently asked questions at our website: <http://www.blueshoesoftware.com>

Using Directory Defender

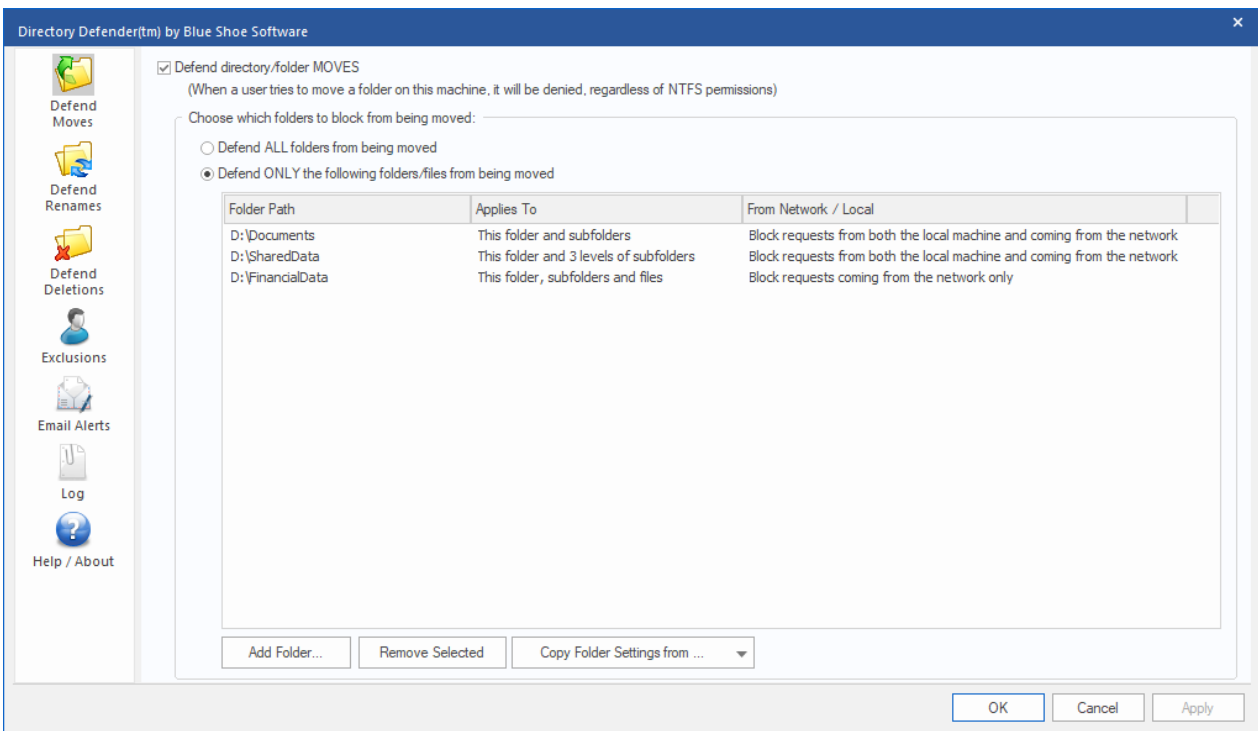
Install Directory Defender

Simply run the DirectoryDefenderSetup.exe on your Windows Server (2008 or later) or Windows Workstation (Vista or later).

Please be sure to pause anti-virus / anti-malware software prior to running the setup executable. Some anti-virus software, such as McAfee VirusScan Enterprise, will block the setup executable from launching and our drivers from installing properly.



Configure Defending Moves



Directory Defender allows you to specify specific folders to be protected from being moved. If you choose to "Defend ALL folders from being moved", this will block all folders on all volumes on the server. Best practice would be to choose "Add Folder..." and only add the folders which you would like to block.

Above, you can see that we've set up three folders, each with different "Applies To" scope and one only blocking requests that come from over the network (like from a workstation for example).

When you click "Add Folder..." you will be asked to choose a folder and where it applies to.

Select a folder to block from being moved...

Folder: C:\SharedData

Applies to: This folder, 'x' levels of subfolders and files (specify subfolder depth below)

Subfolder depth: 3 Subfolder depth of 1 is one level deep (C:\Folder\subfolder), 2 is two levels deep (C:\Folder\subfolder\subfolder), etc...

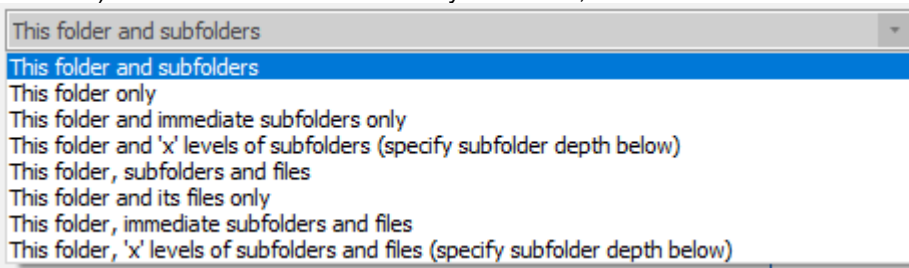
Network / Local: Block requests from both the local machine and coming from the network

Excluded Users: User/Group Exclusions
(for this rule only) BSS\ShareDataMoveGroup

OK Cancel

First, pick the folder, then the scope of the folders and files under that folder (Applies to:) and finally whether or not you want to block the request based on whether the request is made locally on the server itself, or coming from the network (like a user requesting to move a folder from her workstation). If you want a specific user or group to be excluded from this rule (so they can move folders), then add that user or group in the list of Excluded Users here. Instead of adding a group like "Domain Admins" to every folder rule, you can add them to the global Exclusions list on the main screen.

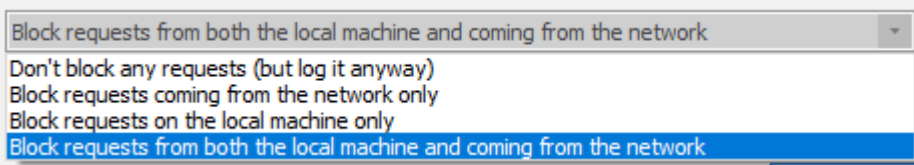
The scope this rule applies to now has eight separate options. The first four refer to folders only (no files included) and the last four are basically the same, but includes files as well.



- **This folder and subfolders:** The named folder will not be able to be moved. In addition, all subfolders *will not* be able to be moved (all the way down the tree).
- **This folder only:** The named folder will not be able to be moved. All subfolders of this folder *will* be able to be moved (all the way down the tree).
- **This folder and immediate subfolders only:** The named folder will not be able to be moved. In addition, all immediate subfolders will not be able to be moved. However, all subfolders below the immediate subfolder of named folder will be able to be moved. For example, if the named folder is C:\UserFolders, then C:\UserFolders\AUser will be blocked from being moved, but C:\UserFolders\AUser\MyDocuments will be able to be moved (as long as the user attempting to be moved has the rights to move this folder).
- **This folder and 'x' subfolders:** The named folder will not be able to be moved. In addition, all subfolders to a level specified as "Subfolder depth" will not be able to be moved.
- **This folder, subfolders and files:** This is the same as "This folder and subfolders", but it includes all the files as well.
- **This folder and its files only:** This is the same as "This folder only", but it includes the named folders' files as well. For example, if D:\Shared is the folder then a file like D:\Shared>List.txt will be blocked as well.

- **This folder, immediate subfolders and files:** This is the same as "This folder and immediate subfolders only", but it includes the files in the named folder and immediate subfolders only.
- **This folder, 'x' levels of subfolders and files:** This is the same as "This folder and 'x' subfolders", but it includes the files as well.

The "Network / Local:" setting includes three options.

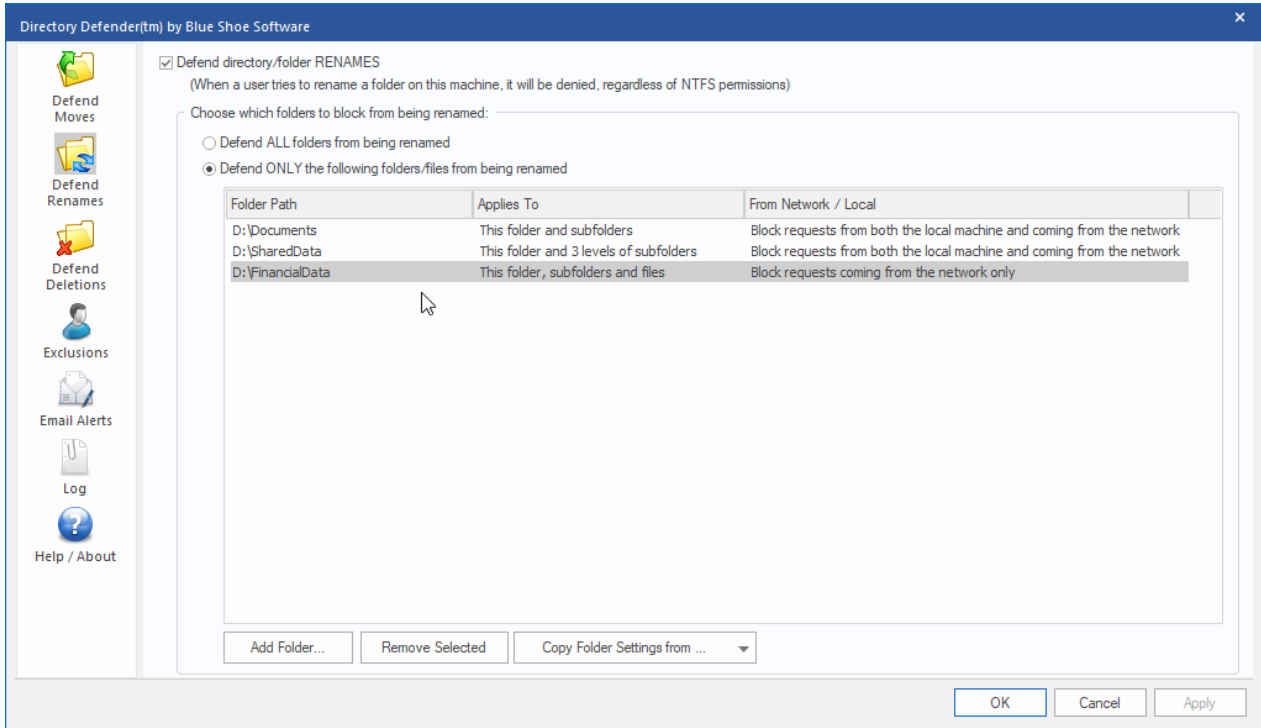


- **Don't block any requests:** This option will not actually block any request, but will log it as though it was blocked. We had several customers ask for a way to see how many users were actually moving, renaming and deleting folders without actually restricting them. This is that option.
- **Block requests coming from the network only:** If you want to be able to log into the server itself and make any change you want, but want to restrict users who are requesting to move, rename, or delete folders from a remote workstation or server, then this is the option for you.
- **Block requests on the local machine only:** If you want to do the opposite as above and restrict changes to local users and allow any changes for remote users, then this is the option for you.
- **Block requests from both the local machine and coming from the network:** This is the default option - this will block requests from both local users logged onto the machine locally, as well as restrict users who are making changes remotely such as from their workstation.

The "Copy Folder Settings from..." menu button allows you to copy all the folder settings from another tab. Sometimes, you may want to keep the same folders blocked from moves, renames, and deletes. You can add all the folders in the "Defend Moves" tab, and then when you go to the "Defend Renames" tab, for example, simply "Copy Folder Settings from 'Defend Moves' Page" and all the settings will be copied. There is a right-click "Copy" and "Paste" option to help keep these tabs in sync as well.

If you would like a user or group of users to be able to move any folder he/she has access to, then add them in the Excluded Users list here or the global [Exclusion](#) list.

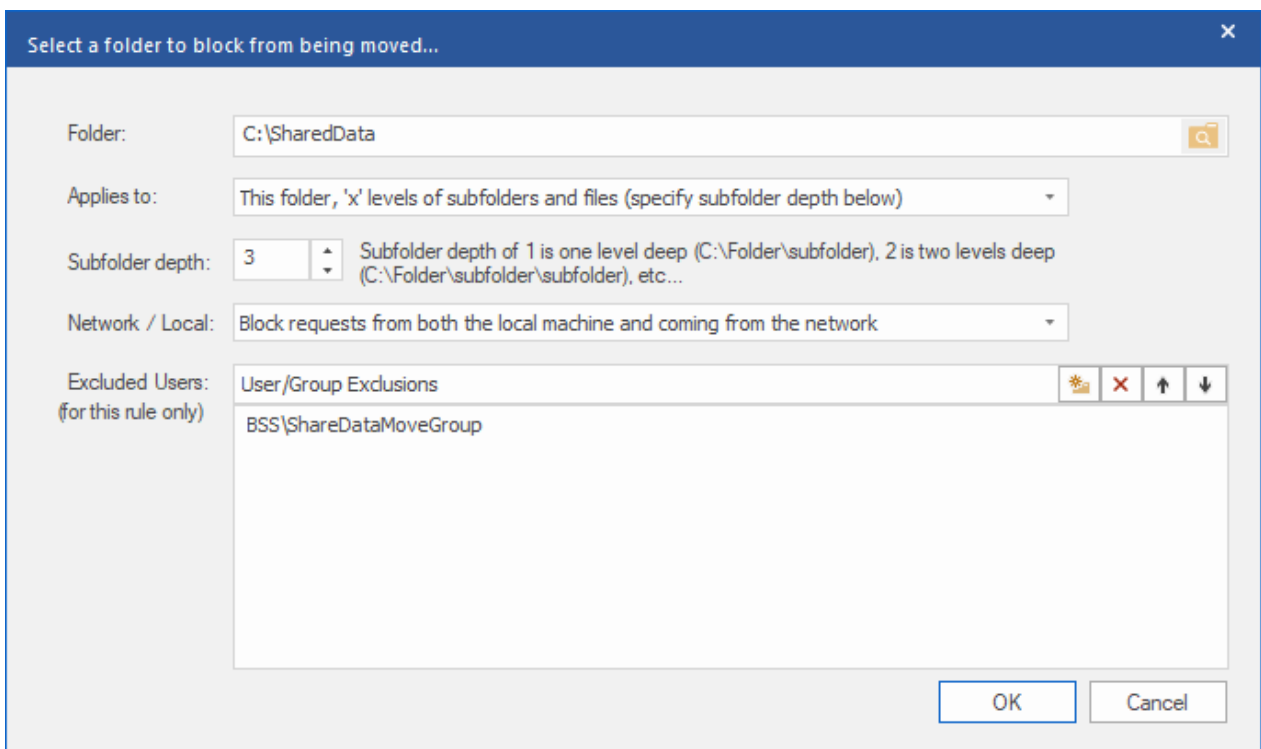
Configure Defending Renames



Directory Defender allows you to specify specific folders to be protected from being renamed. If you choose to "Defend ALL folders from being moved", this will block all folders on all volumes on the server. Best practice would be to choose "Add Folder..." and only add the folders which you would like to block.

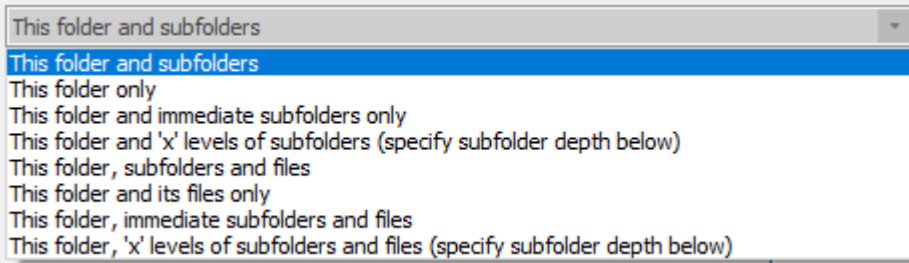
Above, you can see that we've set up three folders, each with different "Applies To" scope and one only blocking requests that come from over the network (like from a workstation for example).

When you click "Add Folder..." you will be asked to choose a folder and where it applies to.



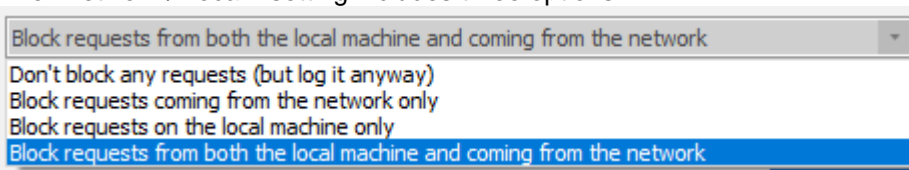
First, pick the folder, then the scope of the folders and files under that folder (Applies to:) and finally whether or not you want to block the request based on whether the request is made locally on the server itself, or coming from the network (like a user requesting to move a folder from her workstation). If you want a specific user or group to be excluded from this rule (so they can rename folders), then add that user or group in the list of Excluded Users here. Instead of adding a group like "Domain Admins" to every folder rule, you can add them to the global Exclusions list on the main screen.

The scope this rule applies to now has eight separate options. The first four refer to folders only (no files included) and the last four are basically the same, but includes files as well.



- **This folder and subfolders:** The named folder will not be able to be moved. In addition, all subfolders *will not* be able to be moved (all the way down the tree).
- **This folder only:** The named folder will not be able to be moved. All subfolders of this folder *will* be able to be moved (all the way down the tree).
- **This folder and immediate subfolders only:** The named folder will not be able to be moved. In addition, all immediate subfolders will not be able to be moved. However, all subfolders below the immediate subfolder of named folder will be able to be moved. For example, if the named folder is C:\UserFolders, then C:\UserFolders\AUser will be blocked from being moved, but C:\UserFolders\AUser\MyDocuments will be able to be moved (as long as the user attempting to be moved has the rights to move this folder).
- **This folder and 'x' subfolders:** The named folder will not be able to be moved. In addition, all subfolders to a level specified as "Subfolder depth" will not be able to be moved.
- **This folder, subfolders and files:** This is the same as "This folder and subfolders", but it includes all the files as well.
- **This folder and its files only:** This is the same as "This folder only", but it includes the named folders' files as well. For example, if D:\Shared is the folder then a file like D:\Shared\List.txt will be blocked as well.
- **This folder, immediate subfolders and files:** This is the same as "This folder and immediate subfolders only", but it includes the files in the named folder and immediate subfolders only.
- **This folder, 'x' levels of subfolders and files:** This is the same as "This folder and 'x' subfolders", but it includes the files as well.

The "Network / Local:" setting includes three options.

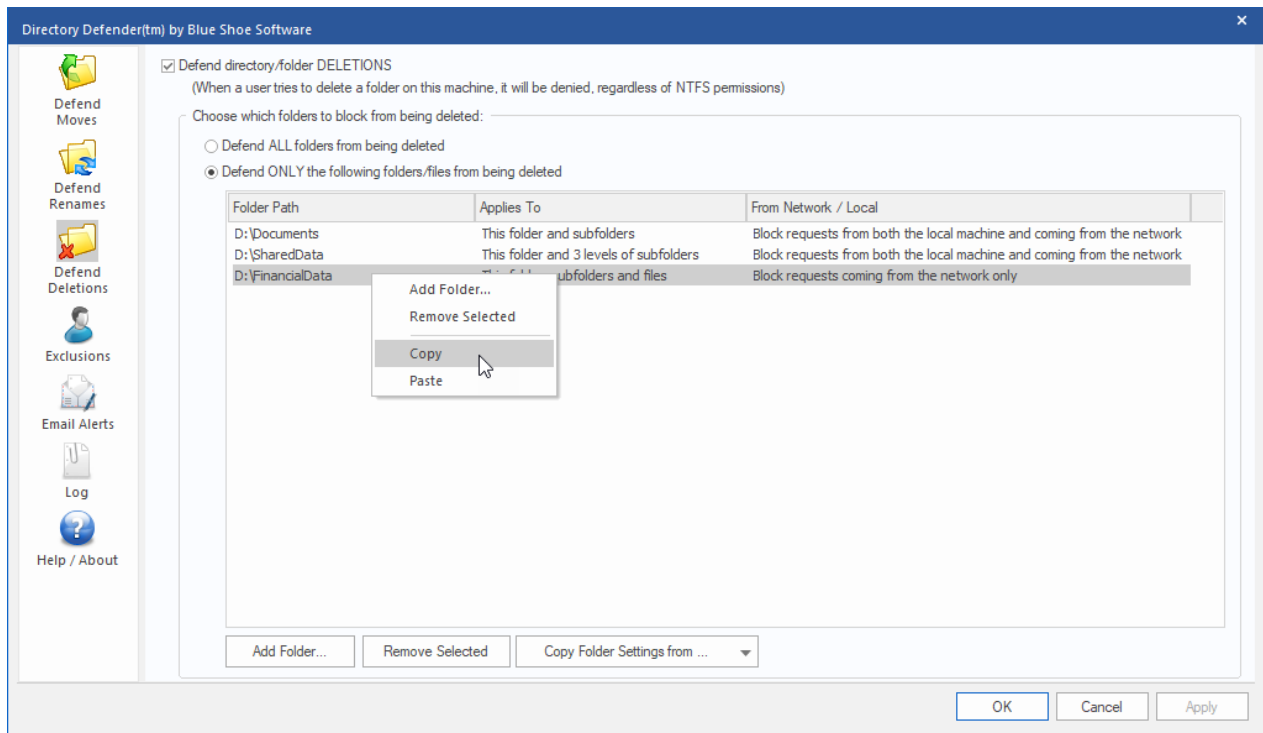


- **Don't block any requests:** This option will not actually block any request, but will log it as though it was blocked. We had several customers ask for a way to see how many users were actually moving, renaming and deleting folders without actually restricting them. This is that option.
- **Block requests coming from the network only:** If you want to be able to log into the server itself and make any change you want, but want to restrict users who are requesting to move, rename, or delete folders from a remote workstation or server, then this is the option for you.
- **Block requests on the local machine only:** If you want to do the opposite as above and restrict changes to local users and allow any changes for remote users, then this is the option for you.
- **Block requests from both the local machine and coming from the network:** This is the default option - this will block requests from both local users logged onto the machine locally, as well as restrict users who are making changes remotely such as from their workstation.

The "Copy Folder Settings from..." menu button allows you to copy all the folder settings from another tab. Sometimes, you may want to keep the same folders blocked from moves, renames, and deletes. You can add all the folders in the "Defend Moves" tab, and then when you go to the "Defend Renames" tab, for example, simply "Copy Folder Settings from 'Defend Moves' Page" and all the settings will be copied. There is a right-click "Copy" and "Paste" option to help keep these tabs in sync as well.

If you would like a user or group of users to be able to rename any folder he/she has access to, then add them in the Excluded Users list here or the global [Exclusion](#) list.

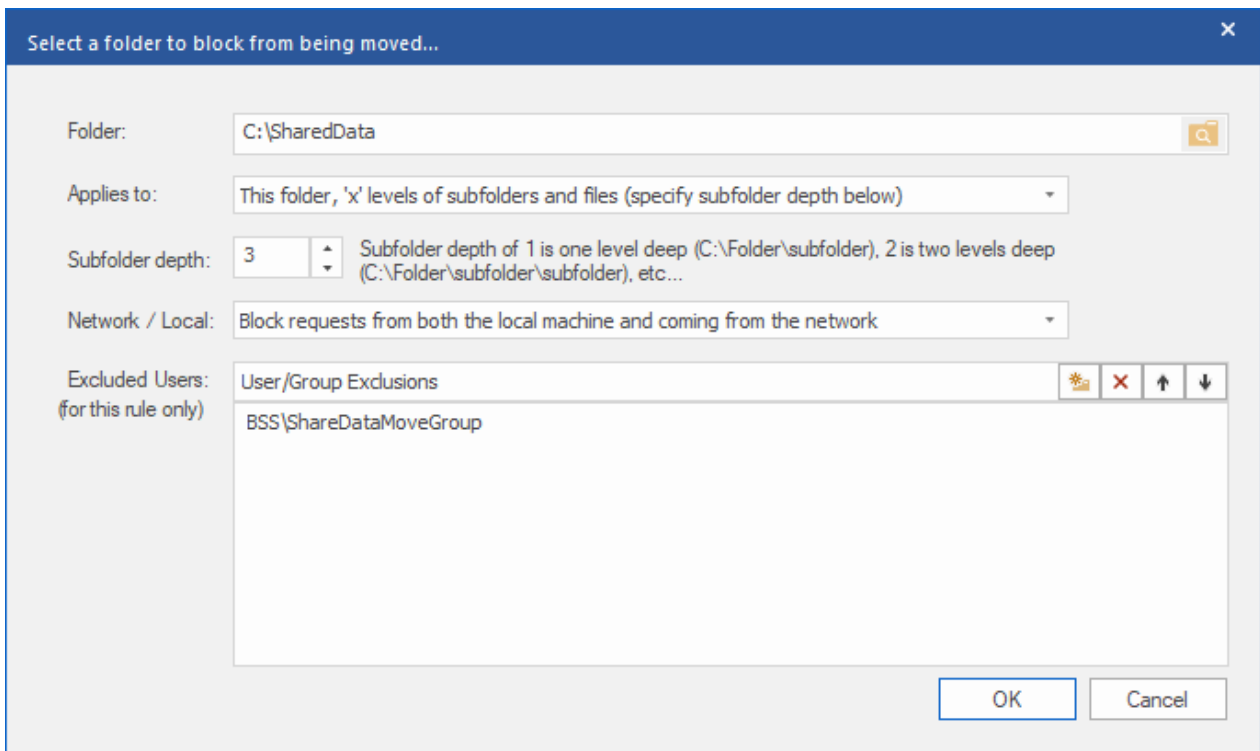
Configure Defending Deletes



Directory Defender allows you to specify specific folders to be protected from being deleted. If you choose to "Defend ALL folders from being moved", this will block all folders on all volumes on the server. Best practice would be to choose "Add Folder..." and only add the folders which you would like to block.

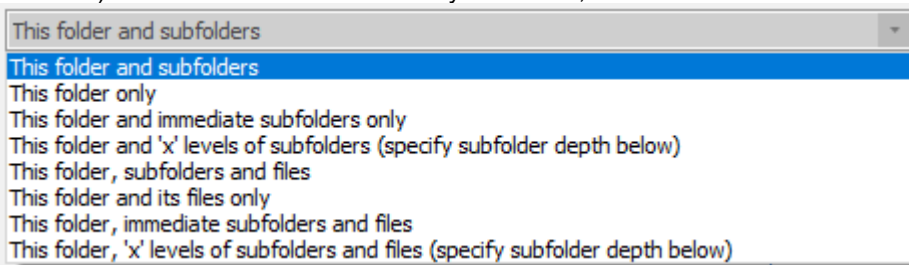
Above, you can see that we've set up three folders, each with different "Applies To" scope and one only blocking requests that come from over the network (like from a workstation for example).

When you click "Add Folder..." you will be asked to choose a folder and where it applies to.



First, pick the folder, then the scope of the folders and files under that folder (Applies to:) and finally whether or not you want to block the request based on whether the request is made locally on the server itself, or coming from the network (like a user requesting to move a folder from her workstation). If you want a specific user or group to be excluded from this rule (so they can delete folders), then add that user or group in the list of Excluded Users here. Instead of adding a group like "Domain Admins" to every folder rule, you can add them to the global Exclusions list on the main screen.

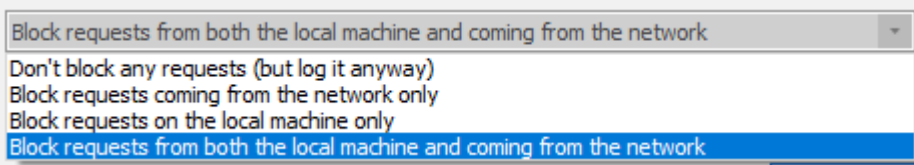
The scope this rule applies to now has eight separate options. The first four refer to folders only (no files included) and the last four are basically the same, but includes files as well.



- **This folder and subfolders:** The named folder will not be able to be moved. In addition, all subfolders *will not* be able to be moved (all the way down the tree).
- **This folder only:** The named folder will not be able to be moved. All subfolders of this folder *will* be able to be moved (all the way down the tree).
- **This folder and immediate subfolders only:** The named folder will not be able to be moved. In addition, all immediate subfolders will not be able to be moved. However, all subfolders below the immediate subfolder of named folder will be able to be moved. For example, if the named folder is C:\UserFolders, then C:\UserFolders\AUser will be blocked from being moved, but C:\UserFolders\AUser\MyDocuments will be able to be moved (as long as the user attempting to be moved has the rights to move this folder).
- **This folder and 'x' subfolders:** The named folder will not be able to be moved. In addition, all subfolders to a level specified as "Subfolder depth" will not be able to be moved.
- **This folder, subfolders and files:** This is the same as "This folder and subfolders", but it includes all the files as well.
- **This folder and its files only:** This is the same as "This folder only", but it includes the named folders' files as well. For example, if D:\Shared is the folder then a file like D:\Shared>List.txt will be blocked as well.

- **This folder, immediate subfolders and files:** This is the same as "This folder and immediate subfolders only", but it includes the files in the named folder and immediate subfolders only.
- **This folder, 'x' levels of subfolders and files:** This is the same as "This folder and 'x' subfolders", but it includes the files as well.

The "Network / Local:" setting includes three options.

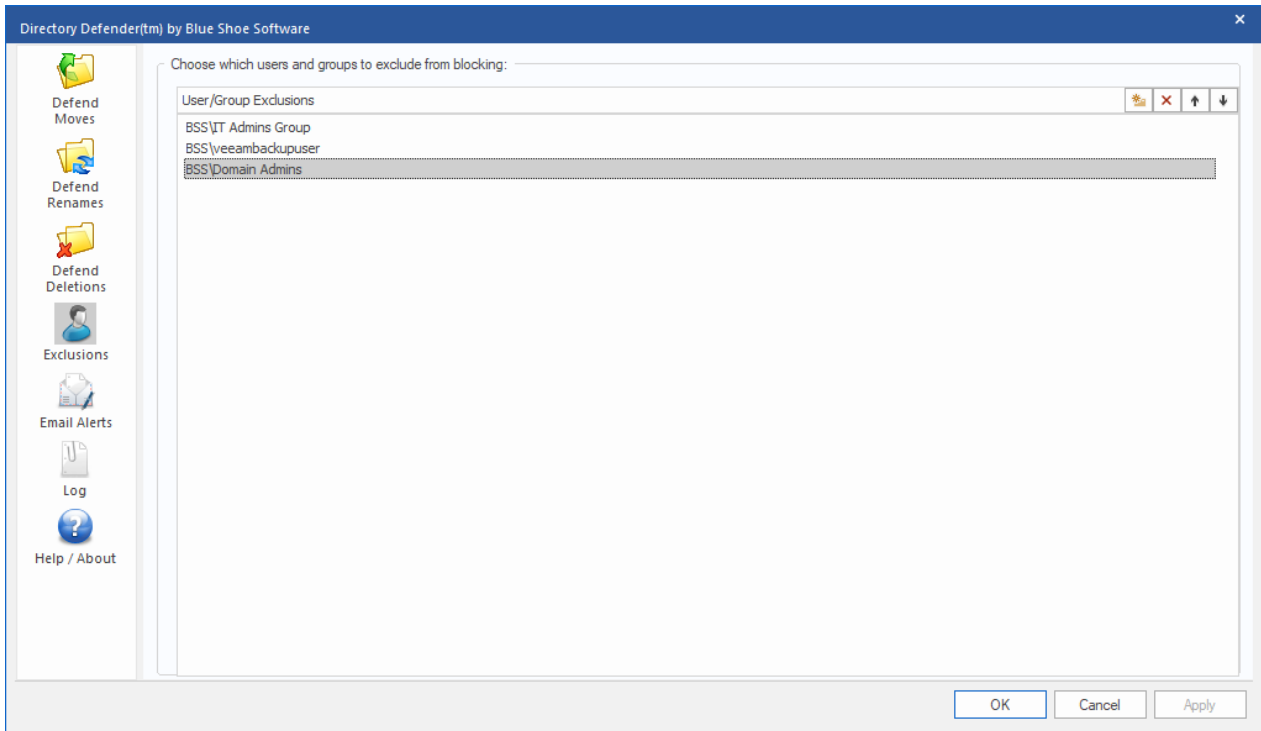


- **Don't block any requests:** This option will not actually block any request, but will log it as though it was blocked. We had several customers ask for a way to see how many users were actually moving, renaming and deleting folders without actually restricting them. This is that option.
- **Block requests coming from the network only:** If you want to be able to log into the server itself and make any change you want, but want to restrict users who are requesting to move, rename, or delete folders from a remote workstation or server, then this is the option for you.
- **Block requests on the local machine only:** If you want to do the opposite as above and restrict changes to local users and allow any changes for remote users, then this is the option for you.
- **Block requests from both the local machine and coming from the network:** This is the default option - this will block requests from both local users logged onto the machine locally, as well as restrict users who are making changes remotely such as from their workstation.

The "Copy Folder Settings from..." menu button allows you to copy all the folder settings from another tab. Sometimes, you may want to keep the same folders blocked from moves, renames, and deletes. You can add all the folders in the "Defend Moves" tab, and then when you go to the "Defend Renames" tab, for example, simply "Copy Folder Settings from 'Defend Moves' Page" and all the settings will be copied. There is a right-click "Copy" and "Paste" option to help keep these tabs in sync as well.

If you would like a user or group of users to be able to delete any folder he/she has access to, then add them to an [Exclusion](#) group.

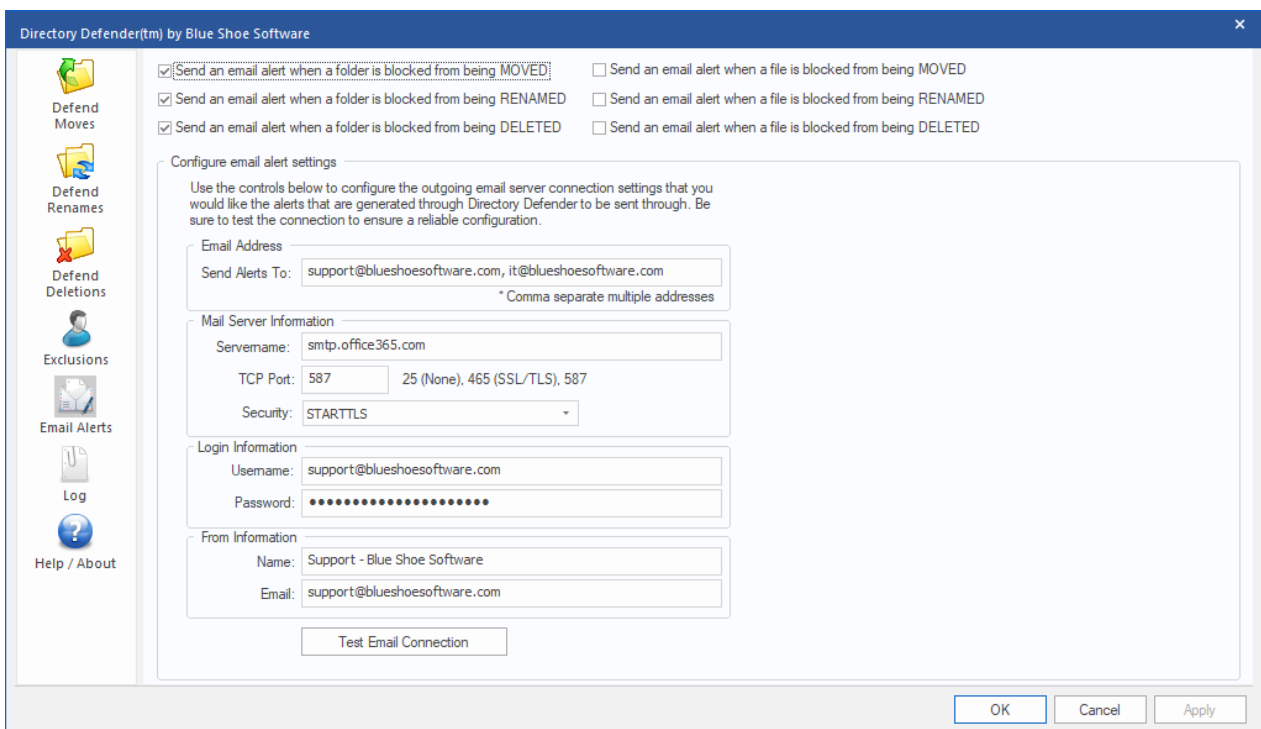
Add Exclusions



Directory Defender allows you to exclude any user or group from being blocked when moving, renaming or deleting folders.

This way, you can add the Domain Admins group or any specific users, for example. If any user is listed specifically or is a member of a group in this list, they will not be blocked from moving, renaming, or deleting any folder on the server. This list is global - if you prefer to just allow a group of users to be excluded from a specific folder structure, add them when adding the folder rule.

Set Up Email Alerts (optional)

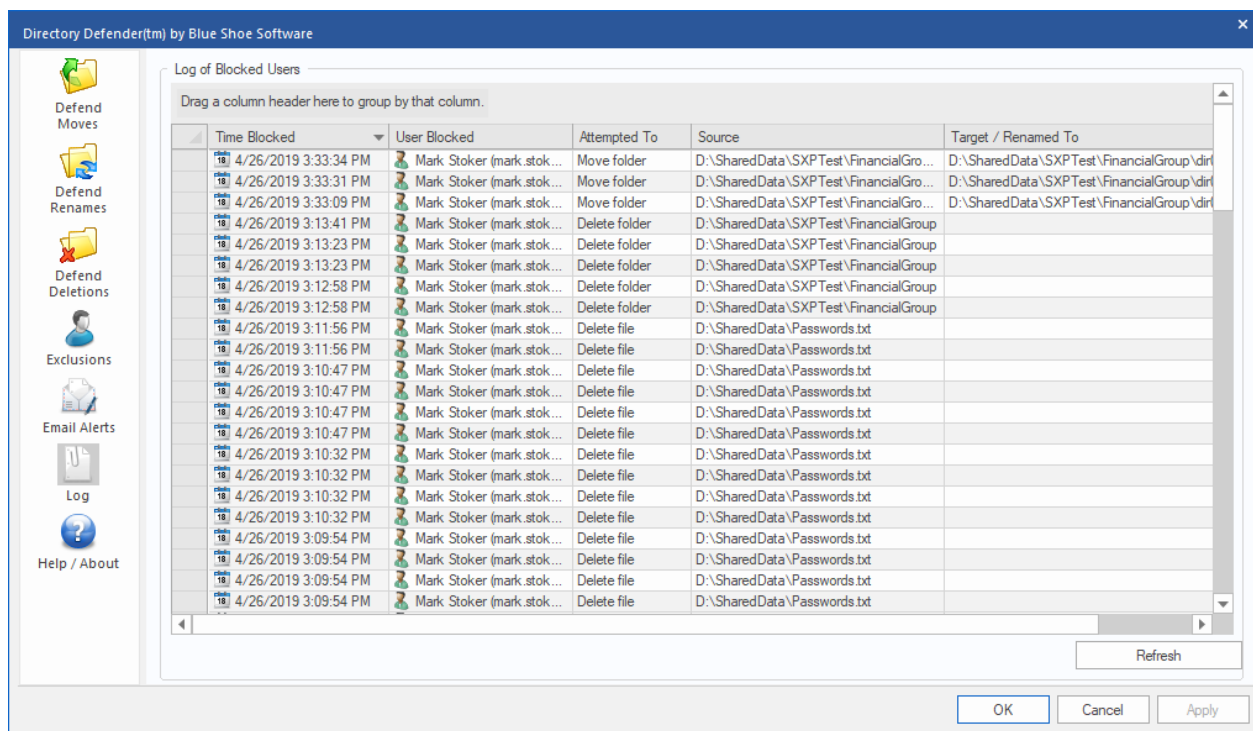


Directory Defender allows you to send an alert to one or more email addresses when a user is blocked from moving, renaming, or deleting either a folder or a file. This way a system administrator can keep track of who is being blocked and make a determination on whether or not they need to be added to an Exclusion group.

- **Email Address (Send Alerts To):** Add the email address where you want the alert to be sent. You can add multiple email addresses by comma separating the address. For example: email@domain.com, email2@domain.com
- **Servername:** This is the SMTP host name that you have access to send email through.
- **TCP Port:** This is the SMTP Port number that the email client will connect to when sending the alert. Typically this port is dependent on what type of Security is used to send the email.
- **Security:** Directory Defender supports three types of email security. None (no authentication), SSL/TLS (used when mail server accepts encrypted connection, typically port 465), and STARTTLS (Office 365 uses this - upgrades the SMTP connection to use encryption, typically port 587) Check with your SMTP Host provider for proper Security and Port settings.
- **Login Username:** Since many SMTP Hosts no longer support relaying emails, you will have a username and password to authenticate to the SMPT Host. Put the username here.
- **Login Password:** Put your password here - the password is encrypted when stored.
- **From Name:** This is the name of the sender (Blue Shoe Software Support is shown in this example).
- **From Email:** This is the email address of the sender.

Be sure to click the "Test Email Connection" button - this will save your settings and attempt to send a test email to the "Send Alerts To" email address(es).





Viewing the Log




Directory Defender will keep a log of the Time Blocked, User Blocked, what the user Attempted To do (Move Folder, Move File, Rename Folder, Rename File, Delete Folder, Delete File), Source and Target Folder. It keeps this in a file located in C:\ProgramData\Blue Shoe Software\Directory Defender\DDLog3.txt

This gives the Directory Defender Administrator an easy way to view the log file.


Example of an Email Alert

 Reply
  Reply All
  Forward
  IM

 Support - Blue Shoe Software | Support - Blue Shoe Software 3:16 PM

Directory Defender Alert - User blocked from moving folder




A user has been blocked from moving a folder.



The specified user below was blocked from moving a folder from one location to another by Directory Defender on machine **MALDC01**. If this user needs to move this folder, a System Administrator can add the user or a group of users into the exclusion list using the Directory Defender Client on the host machine.

Time Blocked:	Tuesday, May 3, 2016 3:16:03 PM
User Display:	Brad Pitt (bpitt@bsslslab.local)
User Account:	BSSLAB\bpitt
User Sid:	S-1-5-21-2329024067-2907235557-1574961883-1105
Source Folder (dragged):	F:\Data\Documents\URBSaveTesting\AutoCAD
Target Folder (dropped):	F:\Data\Documents\URBSaveTesting\Corel Draw\

This email was automatically generated by Directory Defender on Server: MALDC01

Once you have properly configured Email Alerts, you will receive an email every time a user has been blocked from moving a folder.

An example email is shown above (captured from Outlook 2016).

About Blue Shoe Software

Blue Shoe Software LLC, founded by software industry leaders with over 25 years of experience, is dedicated to developing and providing solutions for Windows networks. Our team is committed to designing state-of-the-art software solutions which enable our customers to improve network administration while lowering overall administrative costs. Known for innovativeness, performance, value, and reliability, we offer solutions for companies worldwide. Blue Shoe Software is committed to exceptional customer service. Founded on the desire to provide progressive products, for the best price, we support and recognize the importance of both our customers and employees and remain dedicated to providing superior products that empower our customers.

Be sure to download a free trial version of our other product, Ultimate Recycle Bin:

- Quickly and easily recover local and network files that were deleted or overwritten.
- No need to use snapshots to recover overwritten Word, Excel, and PowerPoint files.
- Network File Recovery. Enabling continuous data protection.
- Protect your file server from Ransomware.
- The network recycle bin for Windows Servers.
- Download free trial at: <http://www.blueshoesoftware.com/Products/UltimateRecycleBin>