

Ultimate Recycle Bin User Guide



Table of contents

Introduction	3
Welcome!	3
What is the Ultimate Recycle Bin?	3
Some Basic Facts about the Ultimate Recycle Bin	4
Installation.....	4
Hardware and Software Requirements.....	4
64 bit or 32 bit?	5
Running the Setup	5
Failover Clustering File Server Support	5
Registration or Evaluation?	6
Self Service Recovery	6
Getting Help	7
Initial Configuration	
Enabling / Disabling	8
Set the Bin Location	9
Set the Bin Size.....	9
Configure the File Retention Rules.....	9
Including and Excluding Folders	9
Excluded File Types (global and local)	11
File Versioning	12
Email Settings.....	13
Connecting / Disconnecting a Remote URB	15
Using the Ultimate Recycle Bin	16
Launching the URB.....	16
CryptoShield / Blocked Users	16
CryptoShield / Honeypot Detection Management.....	17
CryptoShield / File Screening Management	18
CryptoShield / Excluded Users.....	19
CryptoShield / Excluded Folders	20
Ultimate Recycle Bins Tree	20
Recoverable Files List	22
Previous Versions List.....	23
Searching for Recoverable Files.....	24
Search Criteria	24
Saving and Loading Search Criteria	25
Viewing Search Results.....	25
Restoring Recoverable Files	26
Saving Recoverable Files (without restoring)	27
Maintaining an Ultimate Recycle Bin	27
Using Search to Clean up the Bin	28

Introduction

© 2017 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
Suite 720
Orlando, FL 32801

Ultimate Recycle Bin 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!

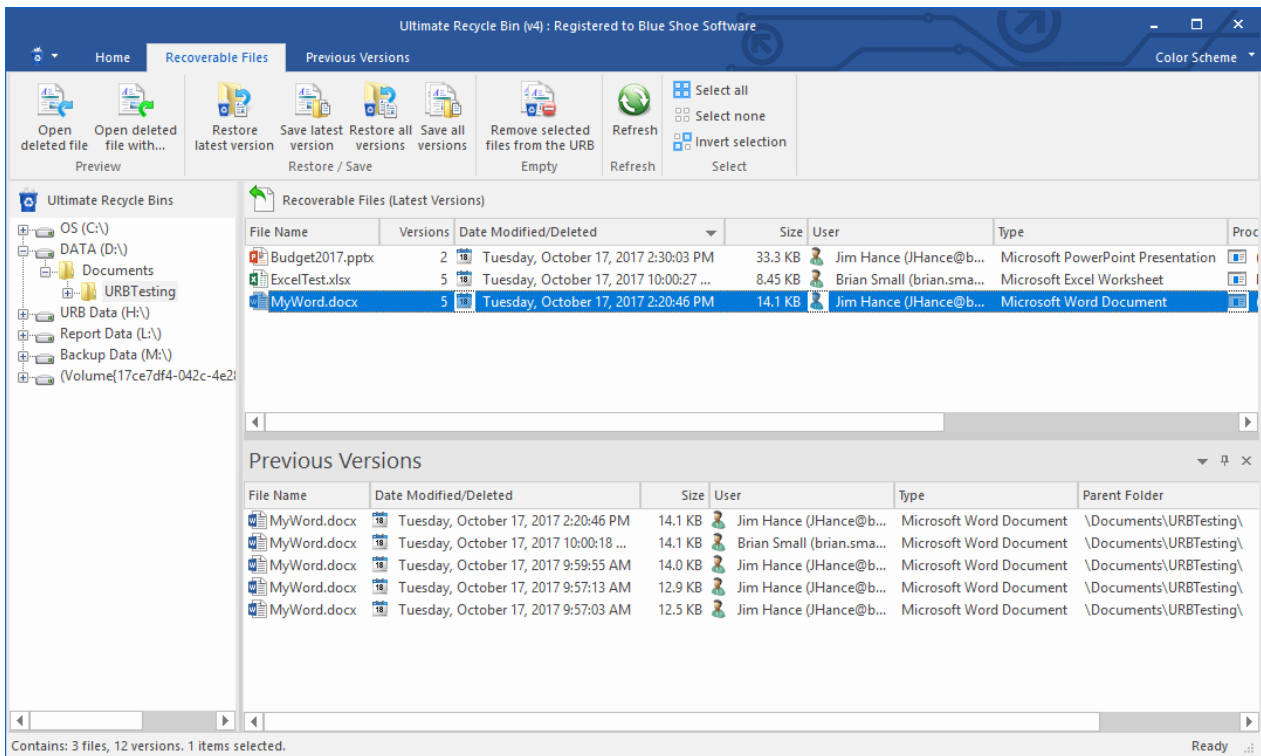
Thank you for purchasing or evaluating the Ultimate Recycle Bin. We would love to hear from you regarding your experience or any issues you have with the product.

What is the Ultimate Recycle Bin?

The Ultimate Recycle Bin can be compared to the Windows Recycle Bin. When files are deleted in Windows Explorer, they aren't actually deleted, but moved into the Windows Recycle Bin. This allows you to recover files after they are "deleted". However, the Windows Recycle Bin will NOT capture files that have been deleted from a network drive, or from a command prompt or malware, such as Ransomware. This is where the Ultimate Recycle Bin outperforms the Windows Recycle Bin in many ways:

- It captures files that have been deleted over the network - just install the Ultimate Recycle Bin on your Windows file server, and capture deletes from clients - without having to install any client software.
- It captures "file saves" from products such as Microsoft Office. This capability allows users to go back to previous versions of Word and Excel documents, for example, right from their desktop.
- It protects you from Ransomware such as CryptoWall and CryptoLocker – if files are encrypted, URB will **block the user from modifying any more files on the server**. If any files were encrypted prior to our CryptoShield technology kicking in, the URB will create a copy of the unencrypted version *before* it is encrypted by the bad guys and protect it from being modified while inside the Ultimate Recycle Bin. Once you feel you have the affected workstation off the network, you can unblock the user using the Ultimate Recycle Bin client.
- You can have an Ultimate Recycle Bin for every volume on the server, or just one specific folder on one volume (the D:\SharedData) folder, for example. Filtering options are endless.
- The Ultimate Recycle Bin displays files in the same folder as when they were deleted, making it so much easier to find deleted files than in the Windows Recycle Bin.
- It has tremendous search capabilities - search by date deleted, file name (with wildcards), user who deleted the file, size, and more.

Continuous data protection (CDP), also known as continuous backup, can now be achieved without constant snapshots. Simply install the Ultimate Recycle Bin on your Windows file server and be protected. We watch for files that are being deleted or modified and move them to the Ultimate Recycle Bin instantly with very little overhead.



Some Basic Facts about the Ultimate Recycle Bin

- It allows you to restore files deleted from clients across the network. It is a network recycle bin for Windows File Servers.
- It allows you to restore files deleted from any program on the server, Windows Explorer, command prompt, virus, etc...
- It will help to protect you from Ransomware that runs on user's workstations and targets mapped drives to your file server. CryptoShield will detect Ransomware file extensions as well as Honeypot file manipulation to protect your file server data. The user will be blocked and you can unblock him/her once you clean the workstation.
- Files that are deleted are stored in the Ultimate Recycle Bin using their original folder path, unlike Windows Explorer's Recycle Bin. This makes it easy to drill down and find recoverable files.
- Security is in the forefront. The Ultimate Recycle Bin adheres to the rules of NTFS security when files are deleted on NTFS volumes. Administrators have the ability to access/recover/permanently delete any file in the Ultimate Recycle Bin.
- No existing file on your volumes will ever be *replaced* by the Ultimate Recycle Bin. If you are recovering a file, and a version of the file exists in the folder where you are recovering it, the file is recovered to a new name. We use the following naming convention: "(Original filename)[Date (YYYY-MM-DD HH-MM-SS-mmm).(Original file extension)]" So for example file "US_Contract0303.docx" exists and a previous version of it is restored, the filename would end up something like this: "US_Contract0303[2014-02-23 17-20-22-320].docx". Now, if that file already exists, it increments a number following the date. For example: "US_Contract0303[2014-02-23 17-20-22-320]-001.docx".

Installation

Hardware and Software Requirements

Supported Windows Platforms

- Windows Server 2016 (Including Failover Clustering File Server support)
- Windows Server 2012 R2 (Including Failover Clustering File Server support)
- Windows Server 2012 (Including Failover Clustering File Server support)
- 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)

64 bit or 32 bit?

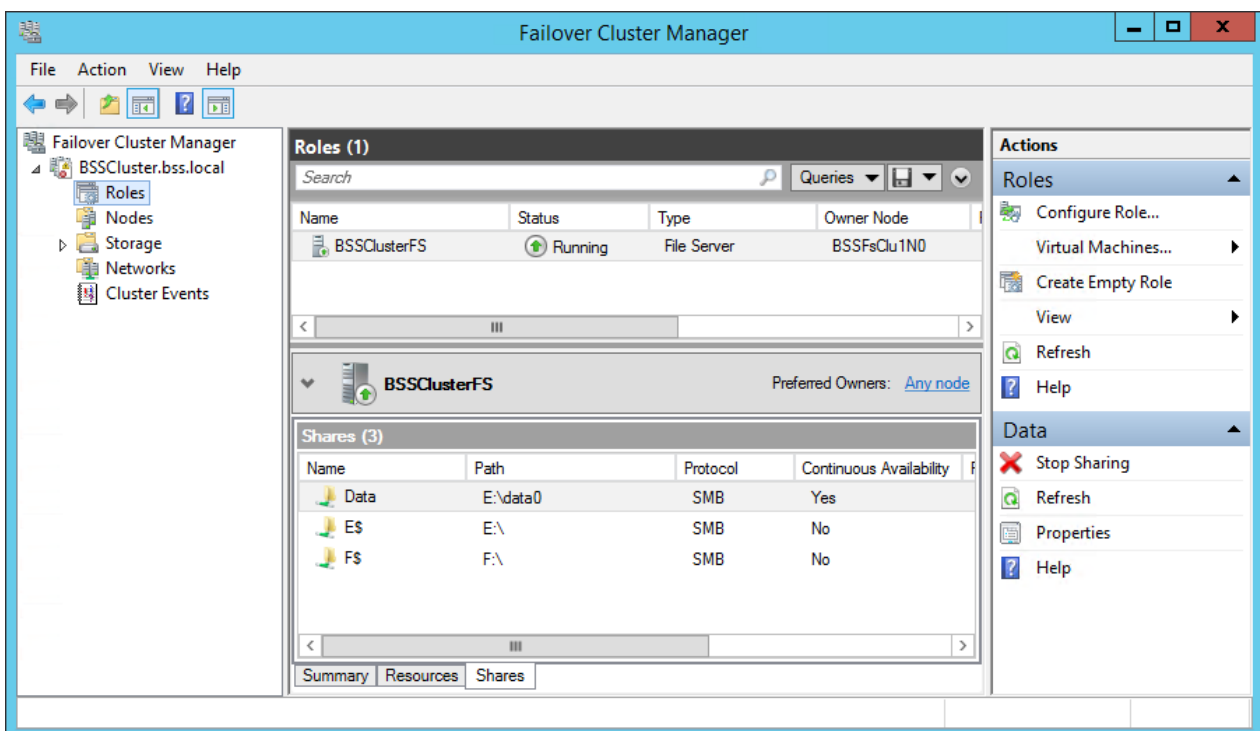
Windows Vista, 7, 8.x, and 10 all come in 32 and 64 bit versions. We support both versions for each version.

Beginning with Windows Server 2008 R2, only 64 bit versions are available. We provide a single setup installation for the Ultimate Recycle Bin. The setup will detect which OS you are running and install the appropriate files automatically. 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 exe from launching and our drivers from installing properly.

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! Towards the end of the installation, the installer will run a command that will add and enable a firewall rule to allow the Ultimate Recycle Bin to be communicated through a port in the firewall (32801). On uninstall, it will run a similar command to remove the rule from the firewall. This is to allow the Ultimate Recycle Bin to be accessed and configured by remote clients.

Failover Clustering File Server Support



Failover Clustering is a feature found in Windows Server 2012 and Windows Server 2012 R2. Ultimate

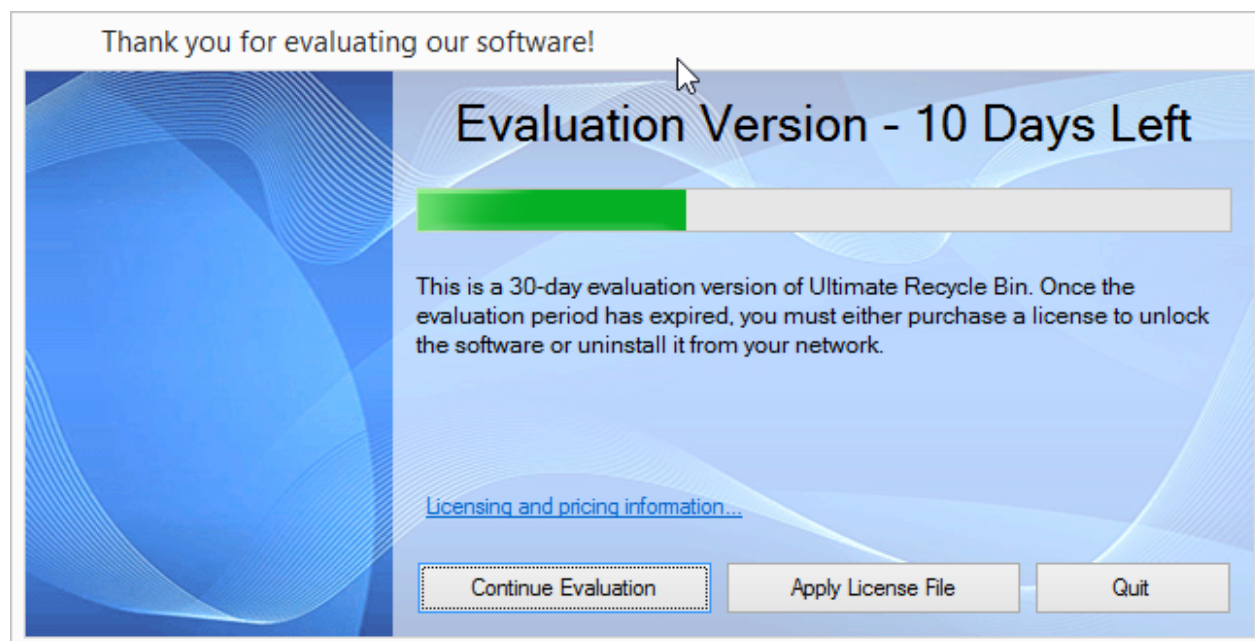
Recycle Bin can quickly and easily be set up to protect Cluster Shares in a File Server role as shown above. In order to fully protect the data, Ultimate Recycle Bin will eventually need to be installed on *ALL* nodes of the File Server Cluster. Ultimate Recycle Bin will automatically detect when a failover occurs and begin protecting the data on the new owner node. Note: An Ultimate Recycle Bin Server Edition license is required for *each* node in the cluster.

Follow these steps when installing Ultimate Recycle Bin on a Windows Server 2012 (R2) File Server Cluster.

1. **Determine the current owner node:** Begin by installing Ultimate Recycle Bin on the current "Owner node" of the File Server Cluster. The owner node can be determined by opening the Failover Cluster Manager and viewing the "Owner Node" column of the File Server role. If you have more than one File Server role, move them to the same owner node for ease of installation.
2. **Install URB:** Log in to the owner node (BSSFsClu1N0) in the example above and run the installation of Ultimate Recycle Bin (64 bit version). This will create the necessary folder structures and initialize URB on the Storage Resources associated with the File Server roles automatically.
3. **Configure URB:** By default, all drives will be protected with the exclusion of temporary files and folders. Refer to the [Initial Configuration](#) section below for more advance configuration of Ultimate Recycle Bin. When adding "Excluded File Types" for a File Server Cluster volume, you must add them to the "Excluded Files" section, not the "Excluded Files (Global)" section. If at any time you would like to configure the settings for File Server cluster storage drives, you will again need to determine the current owner node and run Ultimate Recycle Bin client on that node. You do **NOT** have to configure each node in the cluster.
4. **Install URB on additional nodes:** Once you have configured the File Server Cluster volume settings, the final step is to install URB on each additional node in the cluster. The URB services should be running on all nodes at all times in order to ensure that the shared volumes are protected after a failover.

Registration or Evaluation?

The first time you run the Ultimate Recycle Bin, you will see a screen similar to this:



If you have purchased the Ultimate Recycle Bin, you should have received a license file via email. Save that license file to your desktop (or anywhere on your computer), click the "Apply License File" button, browse for the license file, and click OK.

Self Service Recovery

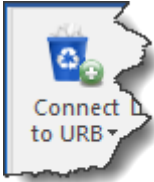
Once you have Ultimate Recycle Bin installed on your server, you may want to deploy the client software to

user's workstations so they can view and recover their own files right from their own desktop.

The client software has been conveniently packaged into its own MSI and is located in the installation folder on the URB server.

Typically, this is C:\Program Files\Blue Shoe Software\Ultimate Recycle Bin
The name of the MSI is 'URBDesktopClientSetupx86.msi'

Simply run this MSI on a user's workstation and any mapped drives that are mapped to shares on a Ultimate Recycle Bin server will show up automatically when they run the URB Client. If there are other URB servers in your environment, they can be added by clicking on "Connect to URB" in the ribbon bar.



Ultimate Recycle Bin will only display files that the logged on user has access to - you don't have to worry about an end user gaining access to deleted files through Ultimate Recycle Bin.

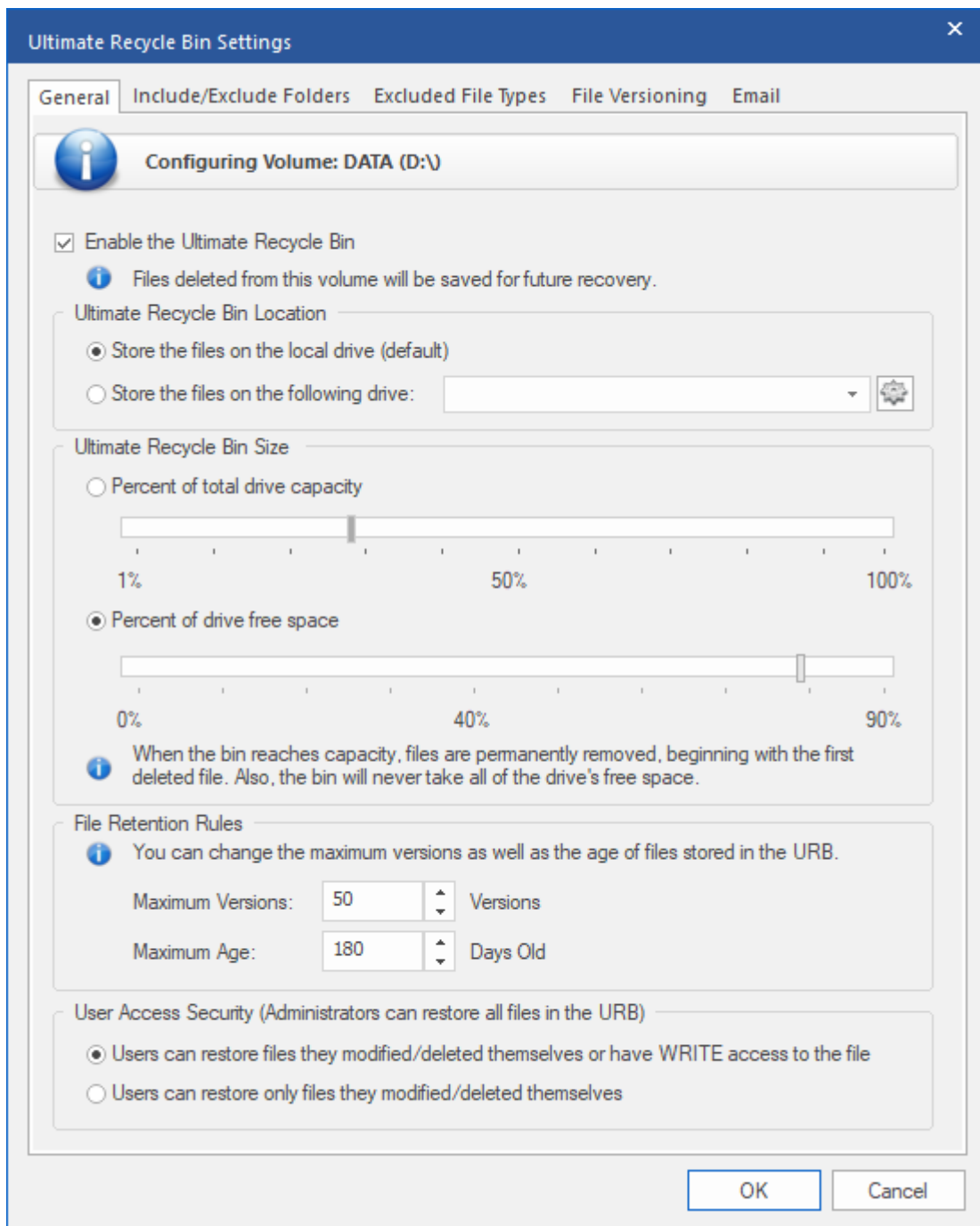
Getting Help

If you run into any problems during installation, or your evaluation, 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: <https://www.BlueShoeSoftware.com>

Initial Configuration

In order to configure the Ultimate Recycle Bin for a given volume, first select the volume, then right click and choose "Configure URB Settings...", or use corresponding ribbon icon.




Enabling / Disabling

Each volume on the machine can have the Ultimate Recycle Bin either enabled or disabled. To enable, simply check the box at the top of the General tab. When you disable the URB on a volume, the recoverable files in the bin are still available for restoration. Disabling a volume simply means no more files will be saved when deleted or overwritten.

Set the Bin Location

When disk space is an issue on a drive you want to protect, you can select an alternate drive to store its deleted and modified files.

For example, in the example shown above, the Data drive (D:\) is running low on disk space. I want to protect the files on that volume, so I created another volume on my SAN and named it URBin (U:\). Then I can configure that when a file is deleted or modified on the D:\ drive, the file is moved to the Ultimate Recycle Bin on the U:\ drive (which has plenty of space).

Keep in mind that the Ultimate Recycle Bin Size shown (90% of total drive capacity) only applies to files stored on the D:\ drive - at this point, either locally, or another volume sets D:\ as its alternate volume. Therefore, we added a shortcut to configure the alternate drive location (U:\ in this case) by simply clicking on the settings gear to the right of the selected alternate drive. 

Set the Bin Size

You can set the maximum size of the recycle bin in two ways:

1. **Percent of total drive capacity** - this sets the maximum size of files in the bin by taking the percent shown from the total size of the volume.
2. **Percent of drive free space** - this sets the maximum size of files in the bin by taking the percent shown from the total free space available on the volume.

Note: When the Ultimate Recycle Bin reaches capacity, files in the bin are permanently removed, beginning with the first deleted or modified file (oldest files first).

Configure the File Retention Rules

In addition to the maximum size of the Ultimate Recycle Bin, you can configure file retention rules on each volume. You can manage the number of versions as well as the age of each file in the Ultimate Recycle Bin.

1. **Maximum Versions:** A file version is defined as a file with the same name in the same folder. For example, you can create a file "myfile.docx" in your documents folder, then delete it, create the same file again, and delete it, and you will have two versions of the same file in the Ultimate Recycle Bin. Some programs, such as Microsoft Office products (Word, Excel, PowerPoint, etc...) will overwrite files each time you save a document. The Ultimate Recycle Bin service watches for this and will save each version of the file in the bin. This allows a user to be able to go back to previous versions of a document and view changes between the two. You can set the maximum number of versions for each file - if the number of versions exceeds the maximum, the URB service will permanently delete the oldest version from the bin.
2. **Maximum Age:** You may have a file retention policy of 90 days, for example, so that you should never keep files longer than this time. The URB service can be set up to automatically remove files in the bin that are older than a certain number of days. The default number of days is 365 days.

Including and Excluding Folders

In order to keep a clean and orderly Ultimate Recycle Bin, you have the ability to include and exclude specific folders for each volume. By default, we include all folders (a wildcard asterisk) and exclude many Windows operating system folders.

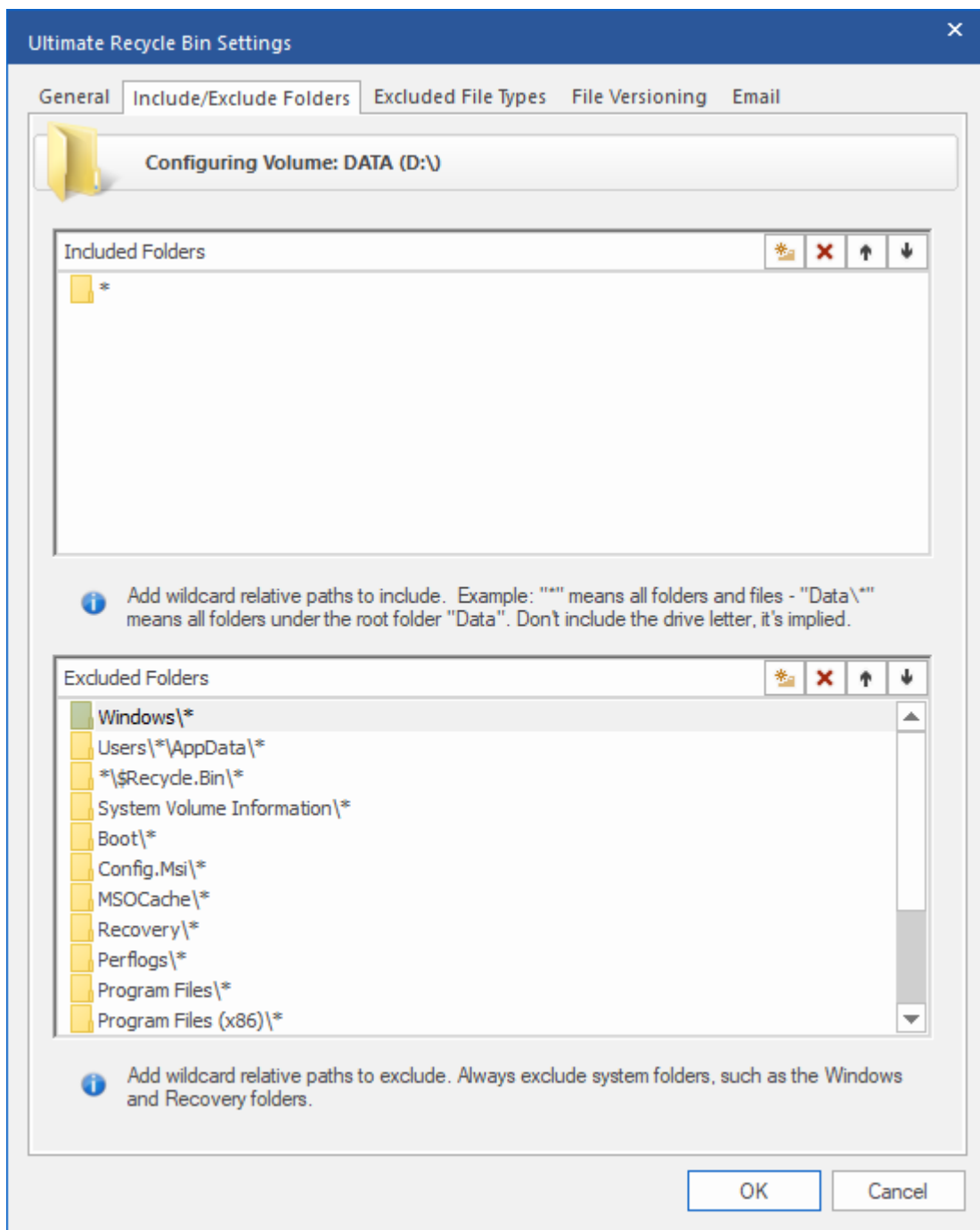
When adding include/exclude folders do NOT specify the drive letter. Drive letters can change so we use Volume GUIDs to identify the volumes. Wildcards are perfectly acceptable as seen in some of the examples below. In fact, you will likely end all of your entries in a wildcard asterisk to denote any folder or file under the path.

Note: Please do NOT remove the default Exclusion folders from a System Drive. This can cause the URB to grow in size very quickly. The Ultimate Recycle Bin is NOT meant to replace system level

backups and should not be expected to do so.

Default Excluded Folders

- Windows*
- Users*\AppData*
- *\$Recycle.Bin*
- System Volume Information*
- Boot*
- Config.Msi*
- MSOCache*
- Recovery*
- Perflogs*
- Program Files*
- Program Files (x86)*
- ProgramData*
- *\Temporary Internet Files*



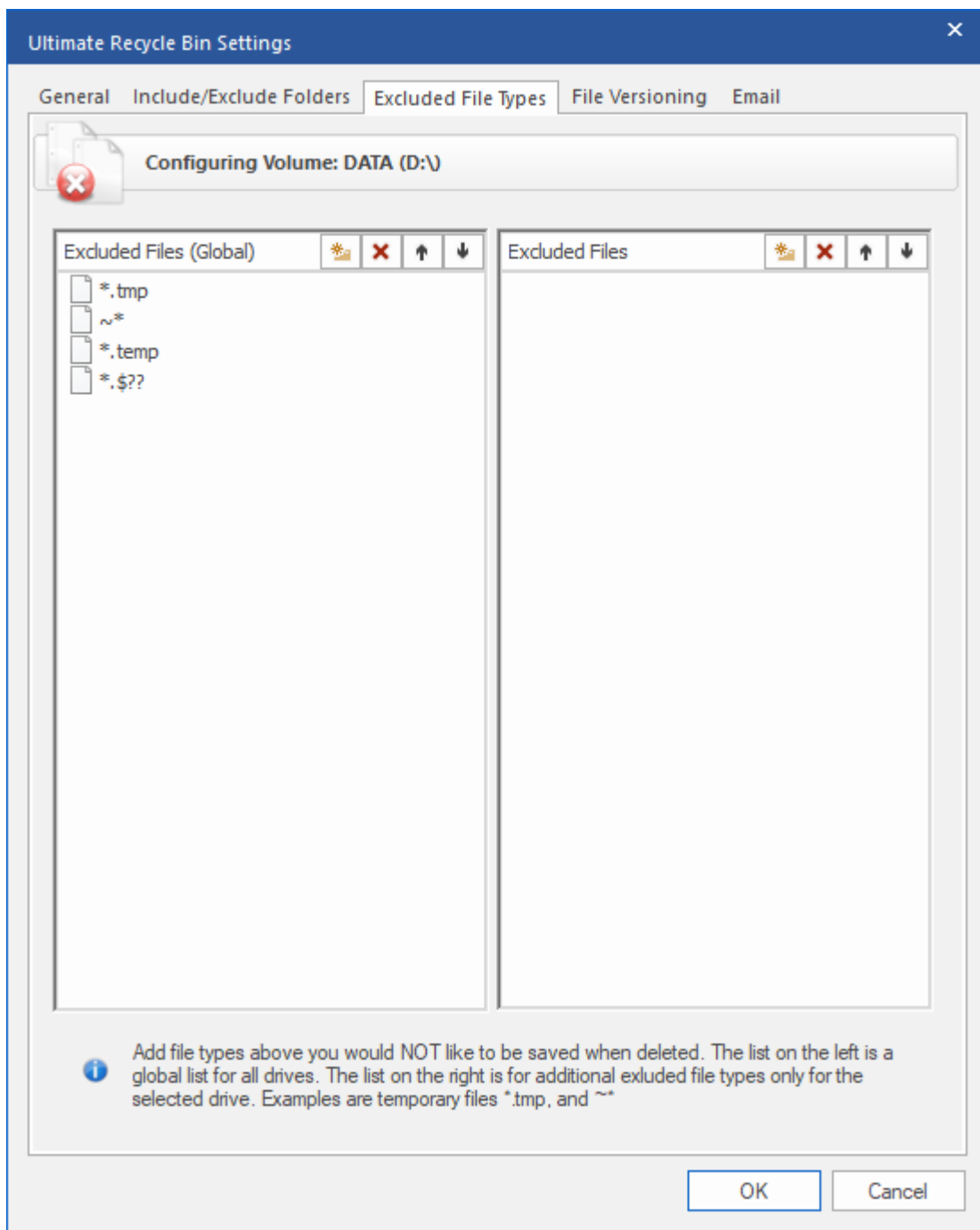
Excluded File Types (global and local)

In order to keep an orderly Ultimate Recycle Bin, you may want to exclude certain file types. You can specify global (server wide) exclusions or volume specific exclusions.

We have excluded a few common temporary file types to the list of global exclusions. You can use the [Search](#) capabilities in order to find large files and exclude those file types.

Default Excluded Files

- *.tmp
- ~*
- *.temp
- *.\$??



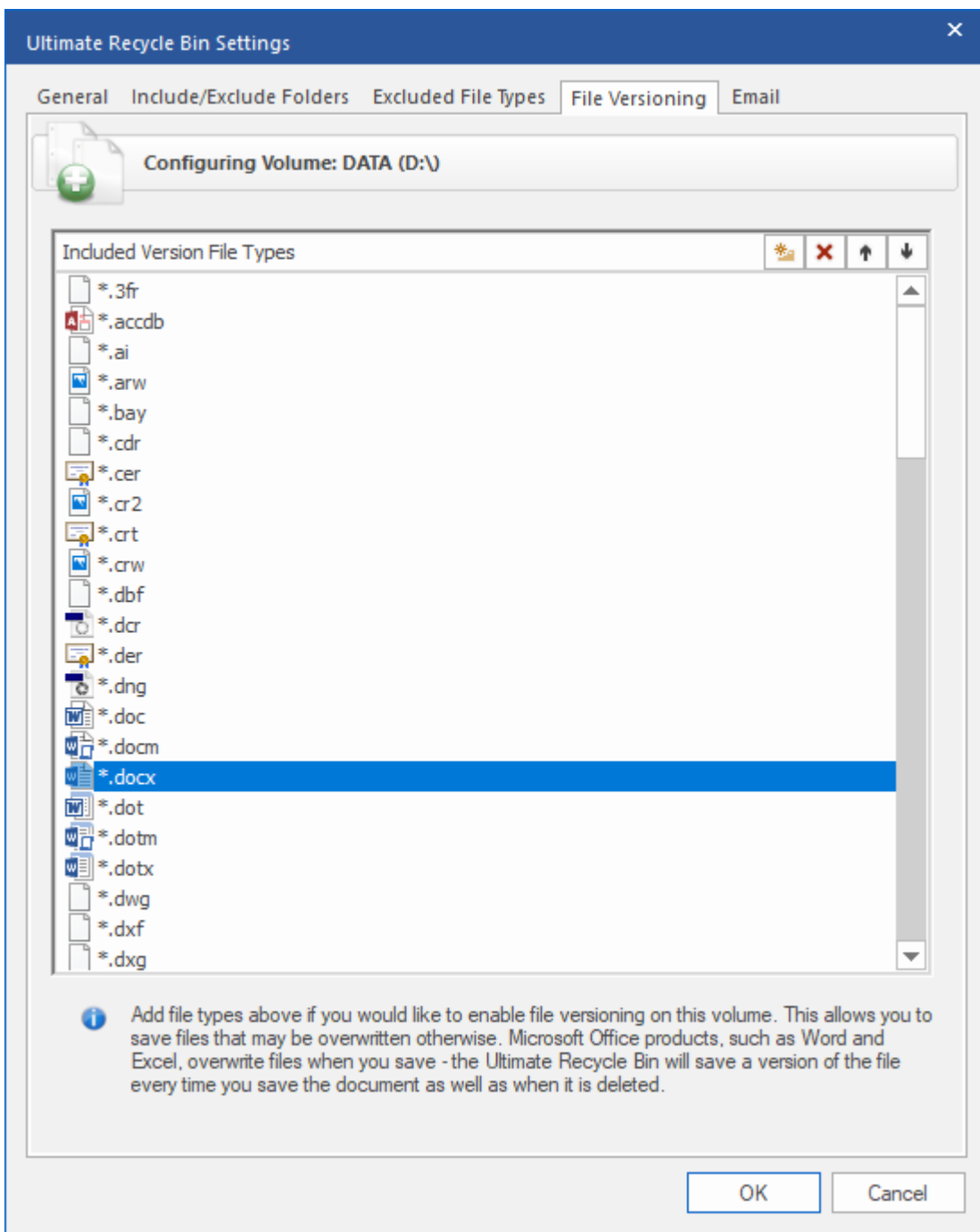
File Versioning

In addition to capturing and saving files as they are deleted by users, the Ultimate Recycle Bin can capture "file saves" and keep the version of the file that is about to be overwritten.

By default, we add all of the Microsoft Office file extensions - feel free to add more extensions as you see fit. Any file that is not only deleted, but saved multiple times (PDF, Photoshop Files (PSD), JPG, HTML, etc...)

Default File Versioning File Types

- *.txt, *.doc, *.xls, *.dot, *.docx, *.docm, *.dotx, *.dotm, *.xlt, *.xlm, *.xlsx, *.xlsm, *.xltx, *.xltm, *.xlsb, *.xla, *.xlam, *.xll, *.xlw, *.ppt, *.pot, *.pps, *.pptx, *.pptm, *.potx, *.potm, *.ppam, *.ppsm, *.sldx, *.sldm, *.rtf, *.xml



Email Settings

Ultimate Recycle Bin allows you to send an alert to one or more email addresses when a user is blocked by CryptoProhibit technology. This blocks users from modifying files on the server when the user has modified special witness files created by Ultimate Recycle Bin. These files are placed on the file shares to determine when a user has accidentally executed Ransomware on his or her workstation. Ransomware is a growing problem in corporations and this is an additional layer to save corporate data from being encrypted by this malicious software. Once the System Administrator is alerted that the user has been blocked, the System Administrator can take the workstation offline and unblock the user using the "Manage CryptoProhibit" dialog on the Ultimate Recycle Bin client.

- **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
- **Servename:** 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).

Ultimate Recycle Bin Settings

General Include/Exclude Folders Excluded File Types File Versioning **Email**

Configuring Volume: DATA (D:\)

Use the controls below to configure the outgoing email server connection settings that you would like any alerts that are generated through Ultimate Recycle Bin to be sent through. Be sure to test the connection to ensure a reliable configuration.

Email Address

Send Alerts To: ** Comma separate multiple addresses*

Mail Server Information

Servename:

TCP Port: 25 (None), 465 (SSL/TLS), 587

Security:

Login Information

Username:

Password:

From Information

Name:

Email:

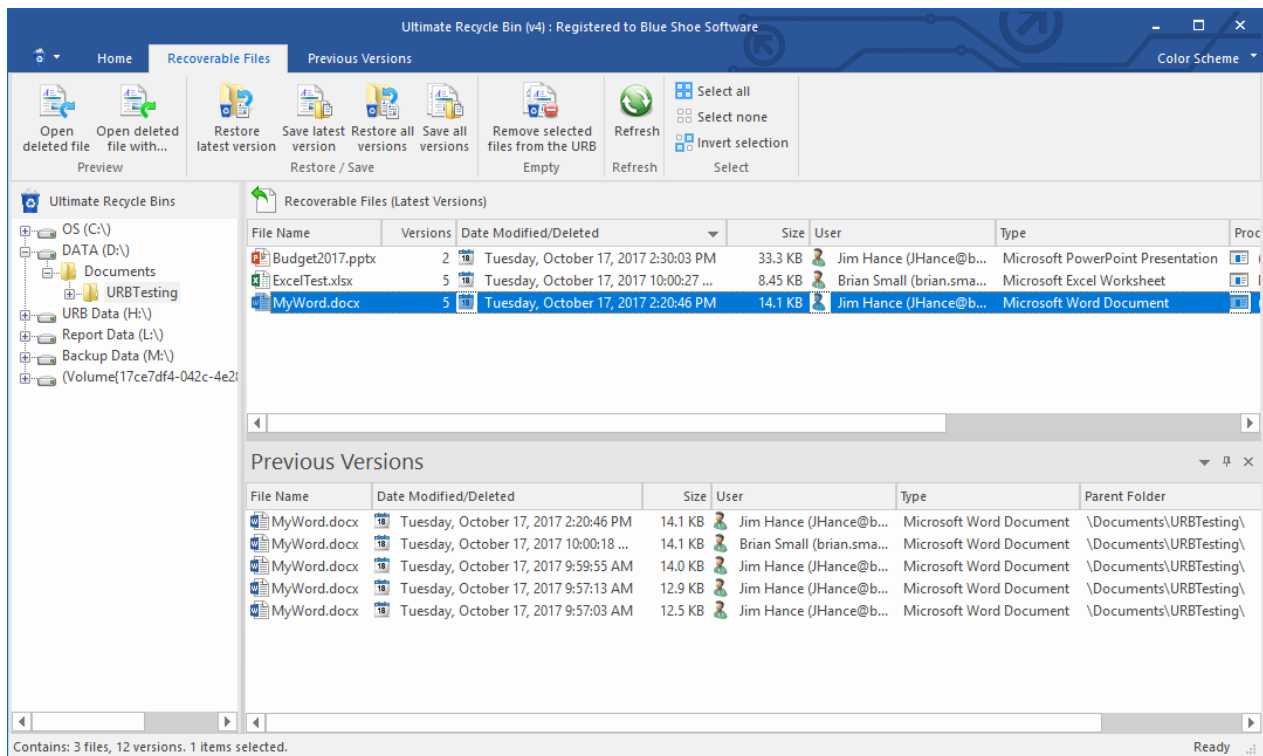
Connecting / Disconnecting a Remote URB

The Ultimate Recycle Bin allows you to fully connect to and manage a remote Ultimate Recycle Bin instance on a separate server. You have two options to connect:

1. **Connect by URB Server** - click this option and simply type the name of a server where the Ultimate Recycle Bin is installed
2. **Connect by URB Path** - click this option and browse by UNC Path to a volume where the Ultimate Recycle Bin is installed.

Note: If you have problems connecting make sure port 32801 is opened on the remote server.

Using the Ultimate Recycle Bin



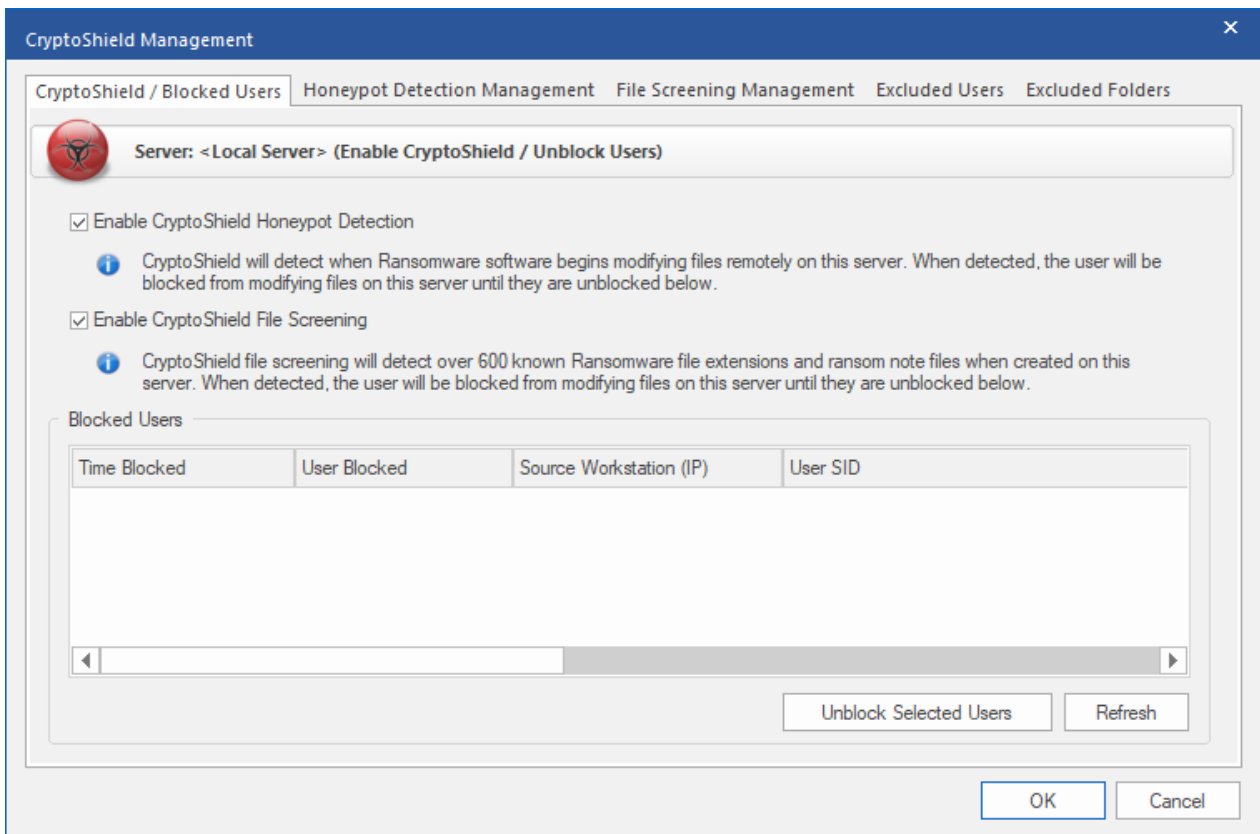
Launching the URB

Launch the Ultimate Recycle Bin from the Start menu or Start Screen.

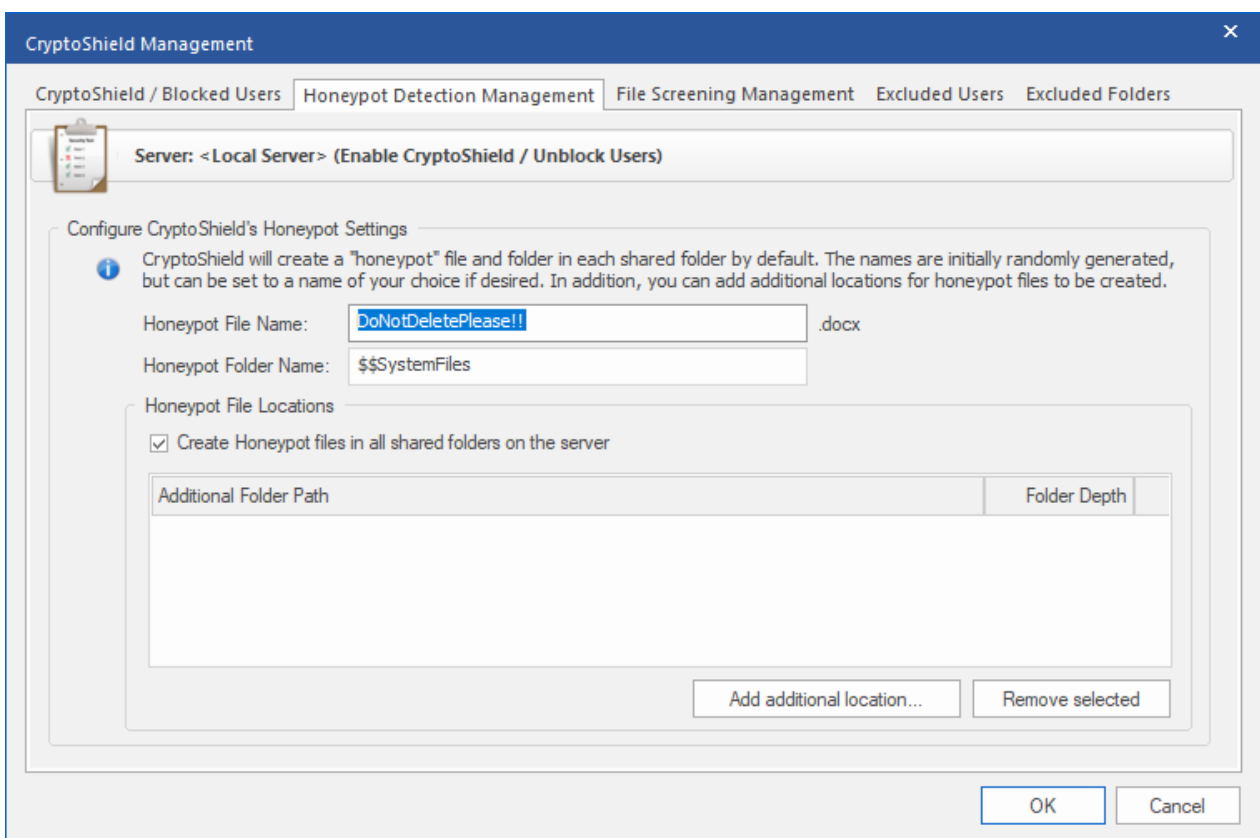
It will look similar to the screen above. The main areas are the Ultimate Recycle Bin Tree (the left pane), the Recoverable Files List, and the Previous Versions List.

CryptoShield / Blocked Users

Ultimate Recycle Bin v4 introduces a new and unique way of dealing with the ever growing Ransomware problem plaguing the corporate world. As antivirus software is struggling to prevent new Ransomware strains from infecting their customer's networks, we came up with solutions to the problem on the file server itself, HoneyPot Detection and File Screening, which are described in the following sections.



CryptoShield / Honeypot Detection Management



Ultimate Recycle Bin creates witness files, initially with a random filename, on your file shares. If a user modifies or deletes these witness files, the user will be blocked from modifying files on the file server until the System Administrator unblocks the user using this dialog. Any files that were encrypted prior to blocking

the user will be backed up to the Ultimate Recycle Bin and quickly and easily restored.

Ultimate Recycle Bin will alert the System Administrator via email when this occurs, giving the System Administrator the workstation name and IP address of the computer that is infected! Simply take that workstation offline, clean it up and unblock the user to get them back up and running.

Honeypot Detection can be enabled or disabled on the “CryptoShield / Blocked Users” screen. The Honeypot Detection Management screen, shown above, allows you to modify the name of the honeypot file name that will be created on your file server. The name is initially generated randomly, but you may change it at any time. Any already-existing honeypot files will be removed and replaced with new ones that have the name you have entered. The honeypot files are Microsoft Word documents, and will always have the .docx extension, which you do not need to include in the file name as it is automatically included.

You may also change the name of the folder that includes the honeypot files. Just like with the honeypot file names, once you have made and applied the change, existing honeypot folders will be removed and replaced with ones with the new name.

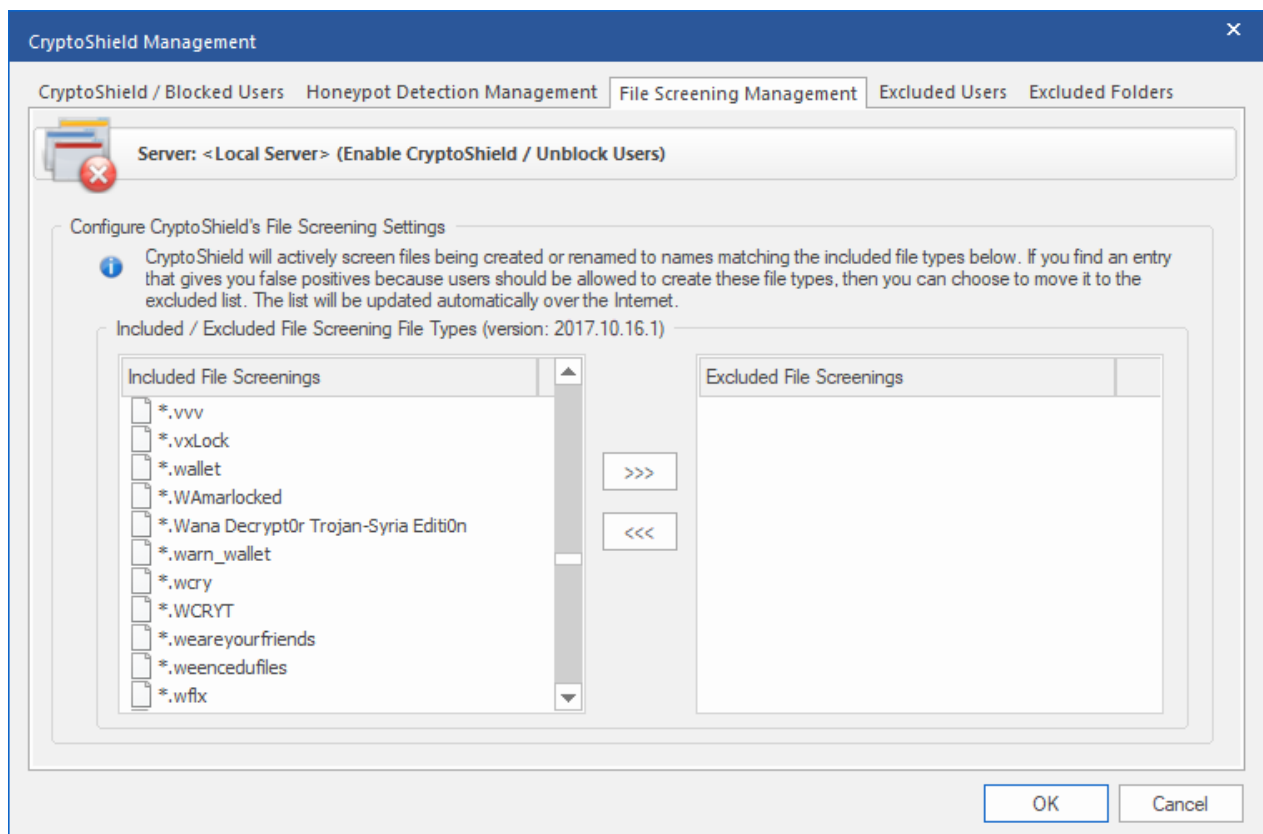
There is also a section on this screen that allows you to define additional folders on your file server where you will want to ensure that honeypot files and folders are created. You may add these folders by selecting the “Add additional location...” button, enter the folder location, and how deep within the subfolder structure you would like to have honeypot files and folders created.

For example, let's assume you have a folder structure like this:

- C:\Folder\
- C:\Folder\SubFolder1
- C:\Folder\SubFolder1\SubFolder2
- C:\Folder\SubFolder1\SubFolder2\SubFolder3

If you select add a honeypot file to C:\Folder\SubFolder1, and set a folder depth of 0 (zero) that is the folder that will receive the honeypot file. If you select a folder depth of 1, a honeypot file will also be created in C:\Folder\Subfolder1\SubFolder2

CryptoShield / File Screening Management



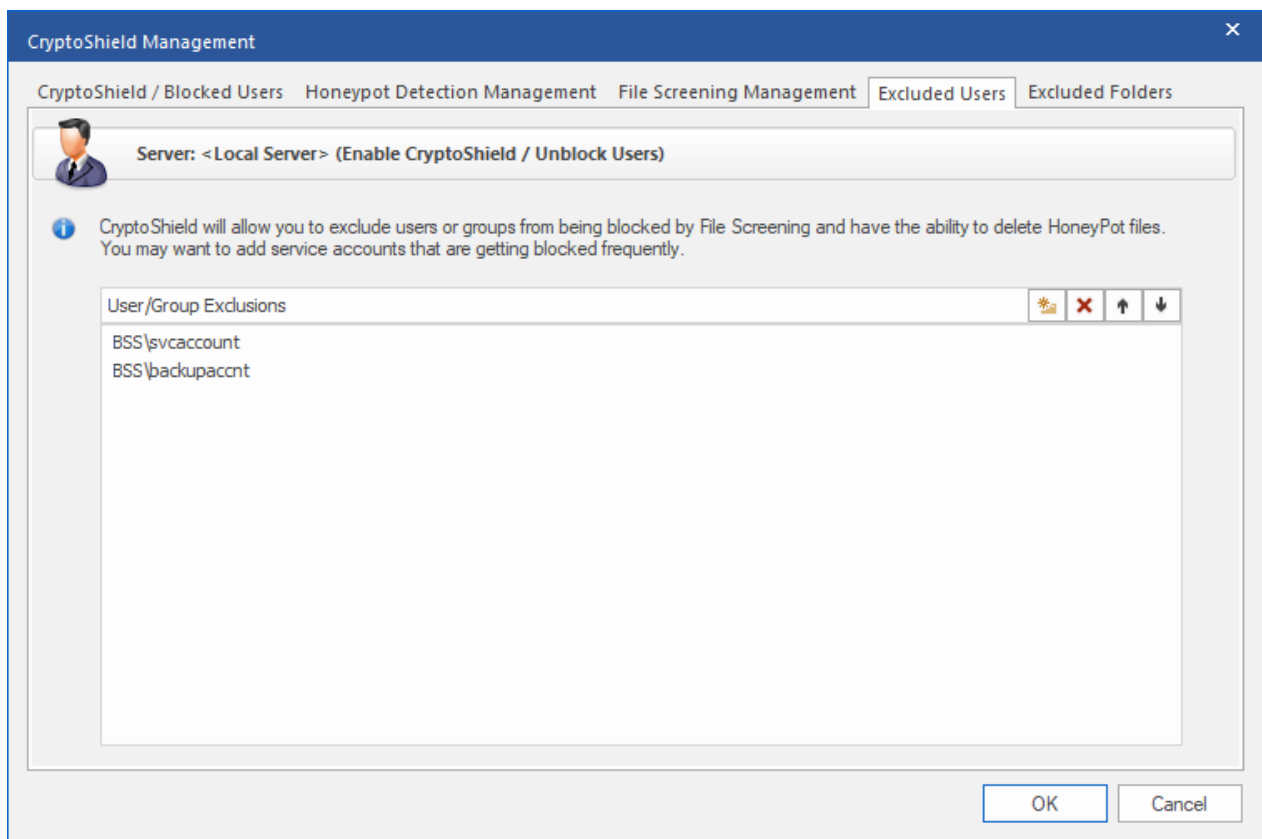
Ultimate Recycle Bin uses its File Screening feature to actively screen newly-created or renamed files. If the filename matches any of the masks contained in the “Included File Screenings” list, the activity will be prevented and the user will be blocked from creating, modifying, or deleting files on the file server until the System Administrator unblocks the user. Any files that were encrypted prior to blocking the user will already have been backed up to the Ultimate Recycle Bin and can be quickly and easily restored.

Ultimate Recycle Bin will alert the System Administrator via email when this occurs, giving the System Administrator the workstation name and IP address of the computer that is infected! Simply take that workstation offline, clean it up and unblock the user to get them back up and running.

The File Screening Management screen allows you to select which file screening masks will be used whenever File Screening is enabled (it can be enabled or disabled on the “CryptoShield / Blocked Users” screen). If there are any masks that you do not wish for CryptoShield to screen, you may move them into the “Excluded File Screenings” list and they will be ignored.

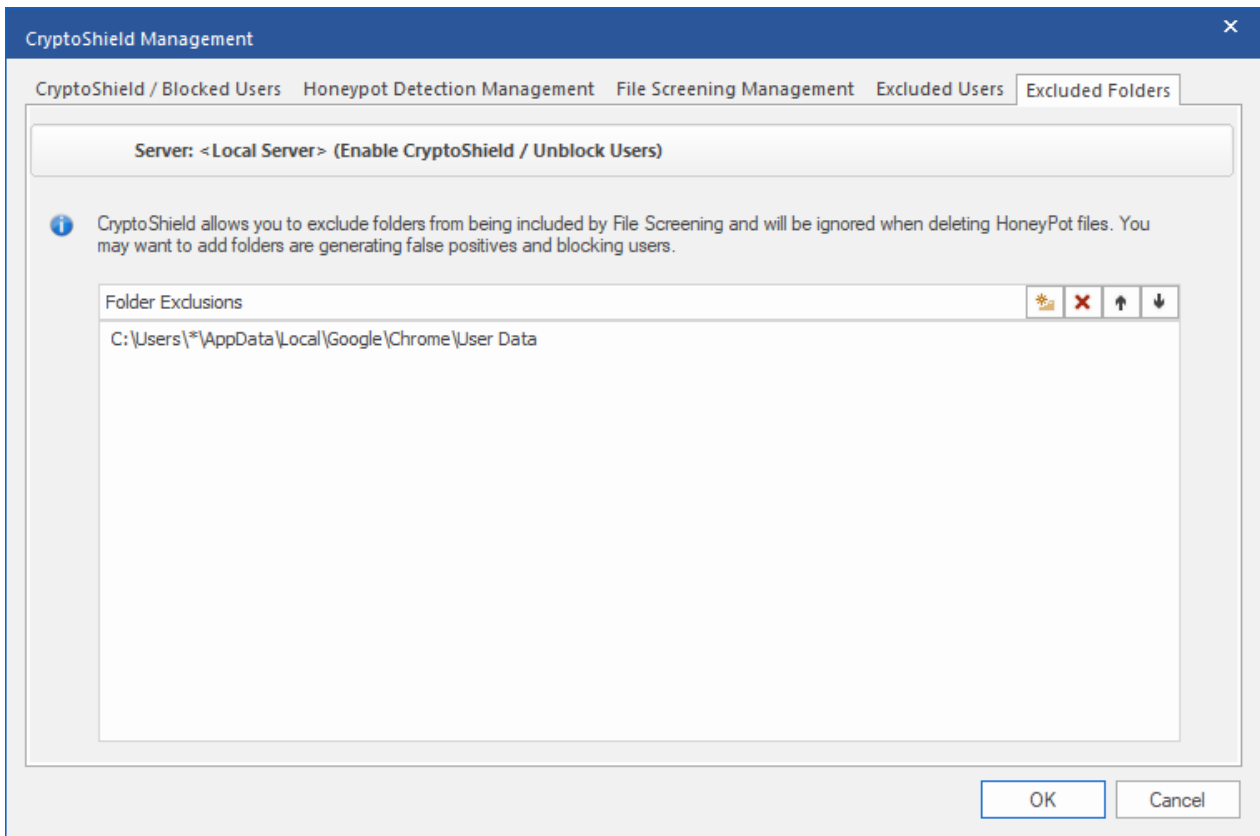
Blue Shoe Software maintains this list of Ransomware extensions and ransom files and will periodically check for updates to it.

CryptoShield / Excluded Users



Ultimate Recycle Bin allows you to exclude certain users or groups of users from being blocked by CryptoShield. Use this only in cases where you know the accounts are not used on workstations where Ransomware may be contracted. This is mainly used for service accounts such as for your backups. Sometimes backup software will delete old files, etc... or create a file listed in File Screening Management causing the software to be blocked from working properly. This is when you should either allow the user to be excluded, or as you will see below, you can exclude specific folders as well.

CryptoShield / Excluded Folders



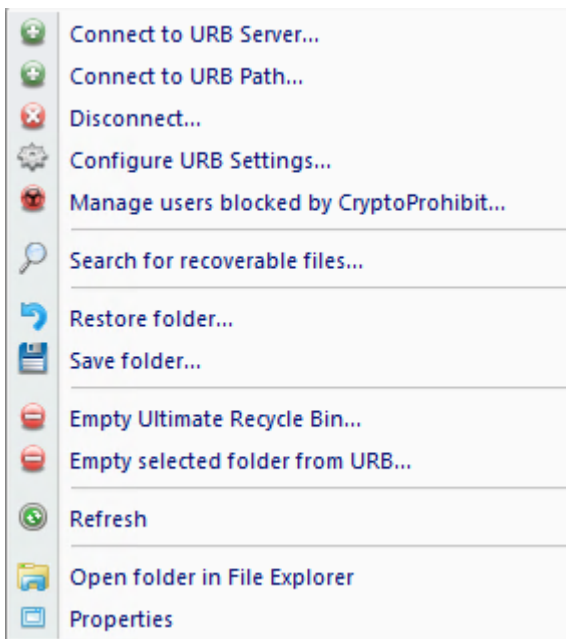
Ultimate Recycle Bin allows you to exclude specific folders from being used in CryptoShield technology. For example, if you know you have a specific folder in which someone needs to create files that are listed on the File Screening management list, then simply add that folder to the Folder Exclusions list. Asterisks are able to be used as wildcards.

Example: D:\CitrixProfiles*\AppData\Roaming\Mozilla\Firefox\Profiles*

Sometime Firefox will save files with *.news extensions, the above exclusion will prevent users from being blocked in these cases where users log on to the server remotely.

Ultimate Recycle Bins Tree

This area contains the connected Ultimate Recycle Bins (one for each volume on each server connected). Here you can drill down into the subfolders which include recoverable files for that URB. You can right-click on a node to get the context menu shown below, or you can simply choose an action from the Ribbon Bar.



Summary of Commands

- Connect to URB Server - choose this option and simply type the name of a server where the Ultimate Recycle Bin is installed.
- Connect to URB Path - choose this option and browse by UNC Path to a volume where the Ultimate Recycle Bin is installed.
- Disconnect - select a node in the tree and choose this option to disconnect from a remote URB.
- Configure URB Settings - choose this option to [manage the configuration](#) of the URB **for the selected volume**.
- Manage users blocked by CryptoProhibit... - choose this option to unblock users and allow the user to modify files once again on the server. Make sure their workstation is clean of Ransomware before unblocking a user.
- Search for recoverable files - choose this option to [search for recoverable files](#) from the selected folder and all subfolders.
- Restore folder - choosing this option will [restore all recoverable files](#) contained in the selected folder as well as all subfolders. After this option finishes, the files will be removed from the Ultimate Recycle Bin.
- Save folder - choose this option to save all recoverable files contained in the selected folder as well as all subfolders. After this option finishes the files will remain in the Ultimate Recycle Bin.
- Empty Ultimate Recycle Bin - choose this option to remove ALL recoverable files under the selected URB. This cannot be undone, but only files which the user has access to will be removed. Administrators have access to all recoverable files. If normal users choose this option, only files which they have access to will be removed from the URB.
- Empty selected folder from URB - exactly the same operation as above, except that it will only remove recoverable files under the selected folder.
- Refresh - reloads the tree from the selected node.
- Open folder in File Explorer - if the folder still exists in its original location, it will launch it in Windows File Explorer.
- Properties - displays summary information on the size and number of recoverable files under the selected node. Please note that the size and number is dependent on the user using this function. For example, user 'bob' in accounting may select a folder, choose Properties and he will see 1000 files (which he has access to); however, user 'betty' in marketing may select the same folder, choose Properties and she will see 500 files (which she has access to). This is based on the NTFS file permissions that the file had when it was deleted or modified. Local Administrators on the URB Server will have access to see all recoverable files.

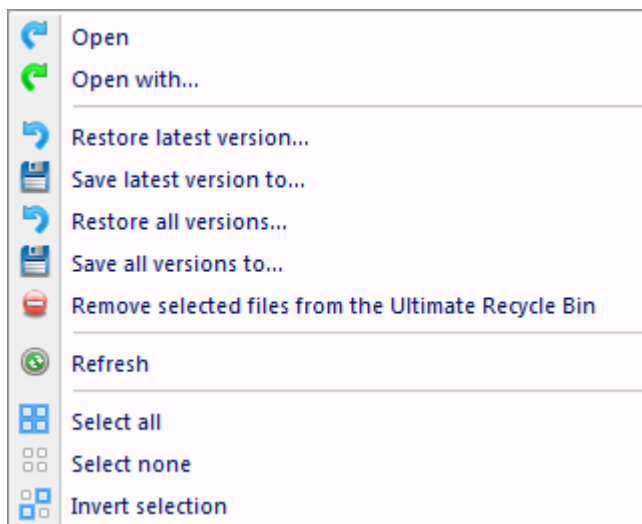
Recoverable Files List

Once you select a folder in the Ultimate Recycle Bins Tree on the left, this pane will be loaded with the list of recoverable files that were deleted or modified in the selected folder.

Columns Defined

1. File Name - the original name of the file when it was deleted or modified.
2. Versions - the number of versions of the File Name. See [File Versioning](#).
3. Date Deleted - the date and time (displayed in local time) that the file was deleted or a new version was created.
4. Size - the size of the file.
5. Deleted by User - the user who deleted or created a new version of the file. Since there can be more than one version of the file, this column displays the *last* person to delete or modify the file. Select the file to see all versions in the Previous Versions List (see below).
6. Type - the type of file as displayed in Windows Explorer.
7. Deleted By Process - the name of the process which was used to delete or modify the file. Unfortunately Windows does not allow you to capture this information when files are deleted across the network. In this case you will see (Remote machine) instead. Since there can be more than one version of the file, this column displays the *last* process to delete or modify the file. Select the file to see all versions in the Previous Versions List (see below).
8. Parent Folder - the full path to the file when it was deleted or a new version was created. This will come in handy when you [Search](#) for recoverable files - search will find files in multiple parent folders and you can sort by this column.

Right-click on a recoverable file or use the Ribbon Bar to choose an action.



Summary of Commands

- Open / Open with - this option will open the latest version of the file (if multiple versions) for preview. It first copies the file to temporary storage on your machine, then opens it from there. Those temporary files are removed when you exit the Ultimate Recycle Bin client. "Open" will open the file in the default application - just like Windows Explorer - "Open with..." will allow you to choose from a list of applications to preview the file.
- Restore latest version - restore the latest version to its original location on the server, or to an alternate location (selected on the confirmation screen).
- Save latest version to - this will copy the latest version of the recoverable file from the server to a place you specify on your local machine.
- Restore all versions - this will restore *all* versions of a file to its original location on the server, or to an alternate location (selected on the confirmation screen).
- Save all versions to - this will copy *all* versions of a file from the server to a place you specify on your local machine.
- Remove selected files from the URB - the selected files **and all versions of the selected file** will be permanently removed from the Ultimate Recycle Bin.

- Refresh - this will refresh the list
- Select all / none / Invert selection - pretty self explanatory :)

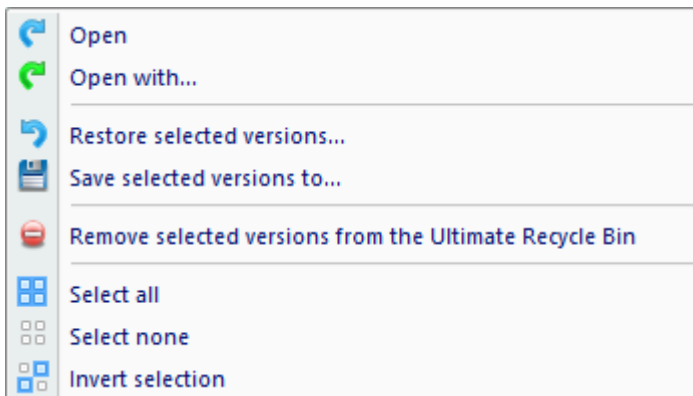
Previous Versions List

Once you select a folder in the Recoverable Files List on the top pane, this pane will be loaded with previous versions of the selected file(s). You can select multiple recoverable files and see all versions of each file in this list.

Columns Defined

1. File Name - the original name of the file when it was deleted or modified.
2. Date Deleted - the date and time (displayed in local time) that the file was deleted or a new version was created.
3. Size - the size of the file.
4. Deleted by User - the user who deleted or created a new version of the file. Since there can be more than one version of the file, this column displays the *last* person to delete or modify the file. Select the file to see all versions in the Previous Versions List (see below).
5. Type - the type of file as displayed in Windows Explorer.
6. Deleted By Process - the name of the process which was used to delete or modify the file. Unfortunately Windows does not allow you to capture this information when files are deleted across the network. In this case you will see (Remote machine) instead. Since there can be more than one version of the file, this column displays the *last* process to delete or modify the file. Select the file to see all versions in the Previous Versions List (see below).
7. Parent Folder - the full path to the file when it was deleted or a new version was created. This will come in handy when you [Search](#) for recoverable files - search will find files in multiple parent folders and you can sort by this column.

Right-click on a previous version file or use the Ribbon Bar to choose an action.



Summary of Commands

- Open / Open with - this option will open the selected version of the file for preview. It first copies the file to temporary storage on your machine, then opens it from there. Those temporary files are removed when you exit the Ultimate Recycle Bin client. "Open" will open the file in the default application - just like Windows Explorer - "Open with..." will allow you to choose from a list of applications to preview the file.
- Restore selected versions - restore the selected version to its original location on the server, or to an alternate location (selected on the confirmation screen).
- Save selected version to - this will copy the selected version of the recoverable file from the server to a place you specify on your local machine.
- Remove selected versions from the URB - the selected versions will be permanently removed from the Ultimate Recycle Bin.
- Select all / none / Invert selection - again, pretty self explanatory :)

Searching for Recoverable Files

Search for recoverable files...

Search Ultimate Recycle Bin

Find deleted and previous versions of files using the search criteria below.

Search path: D:\Documents\URBTesting\

Saved search: <Select a saved query or enter the information below>

File: Wildcard: *.docx
Enter file name wildcards above separated by semicolons. Eg: (*.docx;*.xlsx;*.salary*)

Date: ☐ Filter by date deleted:
☒ File was deleted between 0 days ago and 0 days ago.
☐ File was deleted between Oct /17/2017 and Oct /17/2017

Size: ☐ File was larger than 0 kilobytes
☐ File was smaller than 0 kilobytes

User: User contains:
Separate by semicolons. Eg. (Full Name; username; *@domain.local;)

Process: Process contains:
Separate by semicolons. Eg. (explorer.exe; cmd.exe;)

Search Cancel

Search Criteria

Searching by File Name

Type the name of the file you wish to search for - this supports wildcard selections such as *.docx - you can separate multiple filenames by semicolons to include multiple filenames in your search criteria.

Searching by Date

There are two ways to search by date. Both involve a start date and an end date. The difference is how you specify the dates.

1. The first method is by "days ago". The first digit represents the "start" days ago, the second is the

"ending" days ago. For example: The statement "The file was deleted between 3 days ago and 7 days ago." will find files that were deleted between 3 and 7 days ago. If you want to start from present time, use zero as the "start" days ago.

2. The second method is by specific dates. If you have specific dates in mind and don't want to figure out how many days ago those were, then enter them here. For example: If you wanted to search for recoverable files in January, 2013, enter "File was deleted between "1/1/2013" and "1/31/2013".

Searching by File Size

There are two ways to search by size. Larger than a specific number of kilobytes, or smaller than a specific number of kilobytes. Use the check boxes to specify which (if any) criteria you would like to specify.

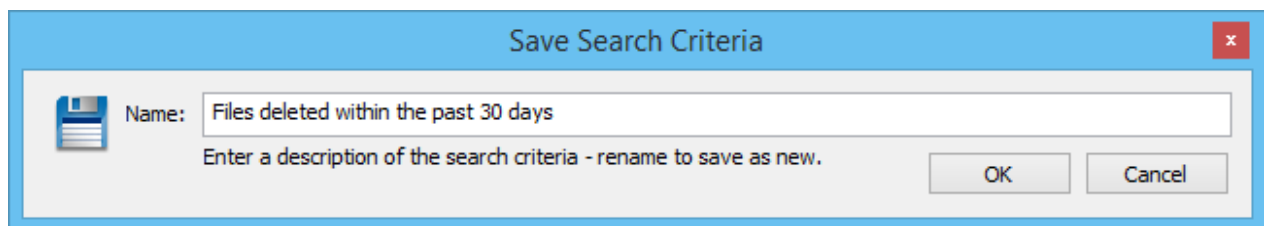
Searching by User

The account that was used to delete or modify the file will be captured by the Ultimate Recycle Bin and stored in its database. You can type any bit of information you know about the user. Any part of the user's display name (full, first, last), SAM account name (username), full SID, userPrincipalName, and yes, wildcards are acceptable.

Searching by Process

The process which was used to delete or modify the file will be captured by the Ultimate Recycle Bin **only** if the process is running on the Ultimate Recycle Bin Server. Otherwise it captures it as "(Remote machine)". If you would like to search for files which were delete by remote users only, then type "(Remote machine)". Sometimes this makes sense if you have had a rogue process on the machine delete a bunch of files (virus, etc...) and would like to restore them all in one step. You can type in the name of the process (as seen in the Recoverable Files List), do the search, then highlight all files and click "Restore all versions..." or right click on the Search Results node in the URB Tree and choose "Restore folder....". Wildcards are acceptable here as well.

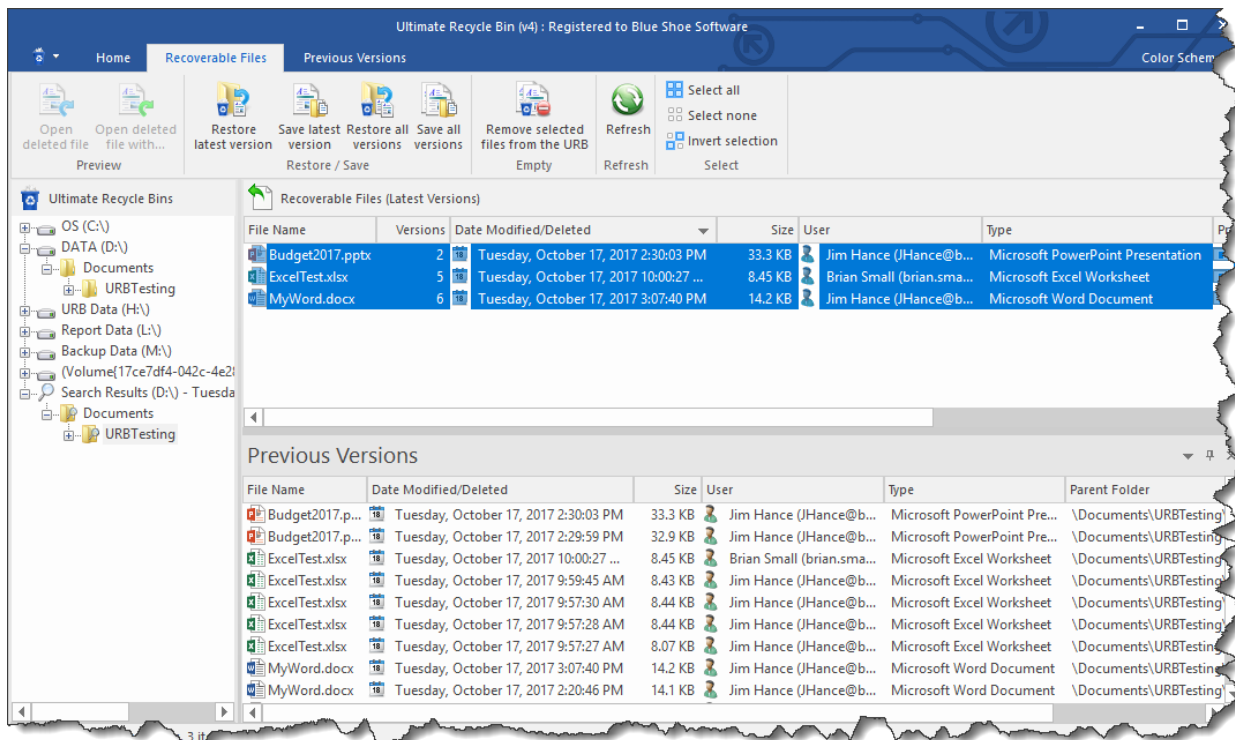
Saving and Loading Search Criteria



Once you set your search criteria, you may wish to save the search to access it quickly later. If you keep the same name shown above, it will overwrite the search criteria. If you modify the name, it will save as new. Click OK to save and Cancel to cancel the operation.

Viewing Search Results

Once you select your search criteria and click "Search", your results will be placed in a node in the URB Tree as shown below. It will show the root that the search was started from as well as the date and time the search was created. You can modify the search at any time by selecting any node under the search results and clicking "Search for recoverable files". This will bring up the currently selected criteria and allow you to modify or save the search criteria. If you click Search again, it will replace the search results. If you start from an entirely new URB folder, new Search Results will be shown in the tree.

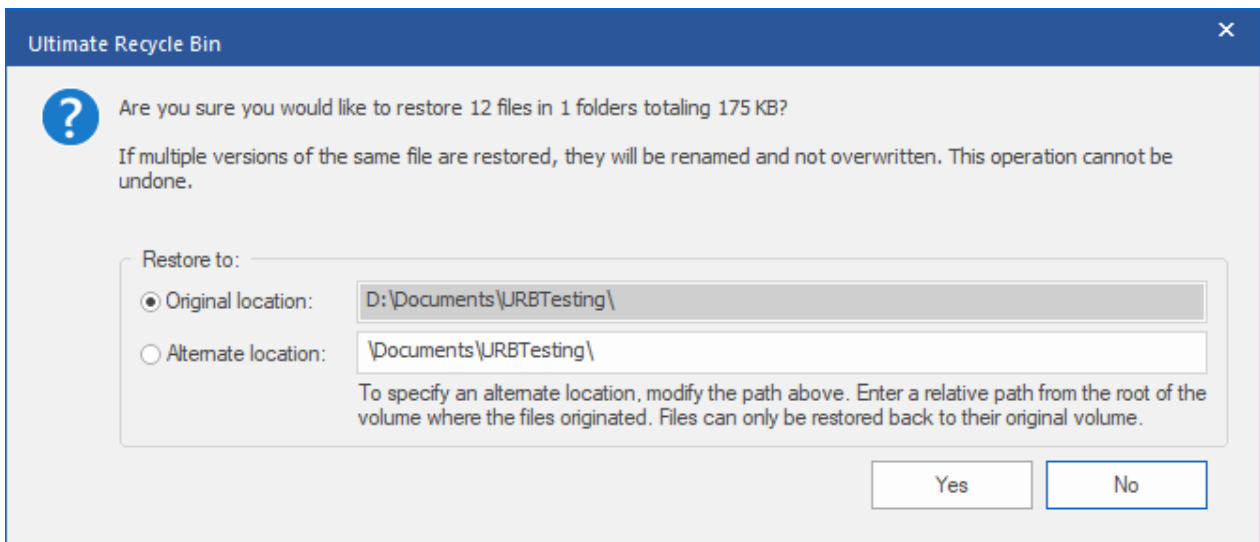


When you select the Search Results node itself, **all** recoverable files (including subfolders) will be shown in the Recoverable Files List. If you expand the Search Results node, only subfolders which contain recoverable files that are relevant to the search criteria will be shown. If you select one of these subfolders, the Recoverable Files List will show only files directly in that folder, not including recoverable files in subfolders. This gives you the ability to drill down into search results.

Restoring Recoverable Files

Use the "Restore deleted folder" option from the Ultimate Recycle Bins Tree to restore an entire folder, or choose recoverable files in the Recoverable Files List or Previous Versions List and use the Ribbon Bar or context menus to choose restoring options for multiple selected files. From the Recoverable Files List, you can choose to either restore *all versions*, or *just the latest version* of the selected files. When restoring multiple versions, the Ultimate Recycle Bin uses a naming convention that will append the date the file was deleted on to the end of the filename (before the file extension). See [here](#) for more details.

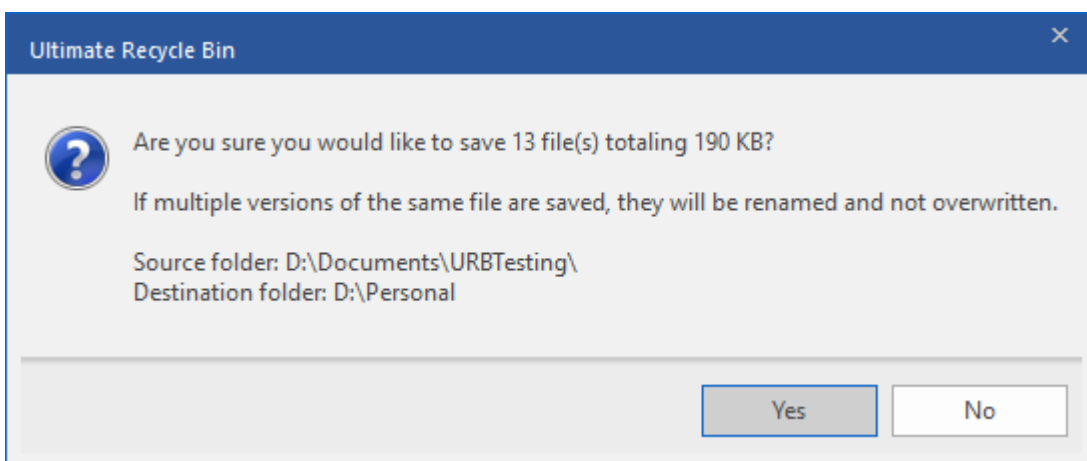
When you restore files, you will see a dialog similar to the one here. You can simply press OK to restore the files to their original location. If the original location no longer exists, the folder path will be recreated automatically. You can choose to restore the files to an alternate location as well. Simply modify the alternate location given, but do NOT add any drive letter or UNC paths, just a relative folder path from the root of the volume where the files were stored originally. Files can only be restored back to their original volume. Once they are restored, you can move them to another volume if you have the proper user rights.



Saving Recoverable Files (without restoring)

Use the "Save deleted folder" option from the Ultimate Recycle Bins Tree to save an entire folder's recoverable files, or choose recoverable files in the Recoverable Files List or Previous Versions List and use the Ribbon Bar or context menus to choose saving options for multiple selected files. From the Recoverable Files List, you can choose to either save *all versions*, or *just the latest version* of the selected files. When saving multiple versions, the Ultimate Recycle Bin uses a naming convention that will append the date the file was deleted on to the end of the filename (before the file extension). See [here](#) for more details.

When you save files, you will first be prompted to select a folder on your local machine in which to save the selected files. Next, you will see a dialog similar to the one below. You can simply press OK to save the files to the destination folder. If you are saving an entire folder of recoverable files, the folder structure will be recreated below the destination folder.



Maintaining an Ultimate Recycle Bin

Much of the maintenance of an Ultimate Recycle Bin is done automatically. You can choose a maximum size for the bin, automatically remove files from the bin based on maximum age as well as the maximum number of versions of a file.

However, there may be times where you would like to go into the bin and clean up some files that are taking up too much space or similar problem. You can easily accomplish this using the powerful Search

capabilities of the Ultimate Recycle Bin.

Using Search to Clean up the Bin

Let's take the scenario that you would like to free up some space on the volume. You can easily search for all files in the bin that are very large and permanently remove them from the bin, freeing up space on the volume. This can be accomplished in a few simple steps.

1. First, select the root of the volume that you would like to clean up.
2. Second, right click on it and choose "Search for recoverable files..." or click the same from the Ribbon Bar.
3. Third, drop down the "Saved searches" and choose "Huge Files (16 - 128 MB)". Feel free to tweak the numbers under the size criteria to your specific needs. Then click "Search".
4. Fourth, click the "Size" column header in the "Recoverable Files List" to sort by size. Now you can quickly see a few files that are really large and may not be necessary to save in the bin.
5. Finally, select the files you would like to remove and choose "Remove selected files from the URB" from the Ribbon Bar or the right-click context menu. Verify, and click OK.