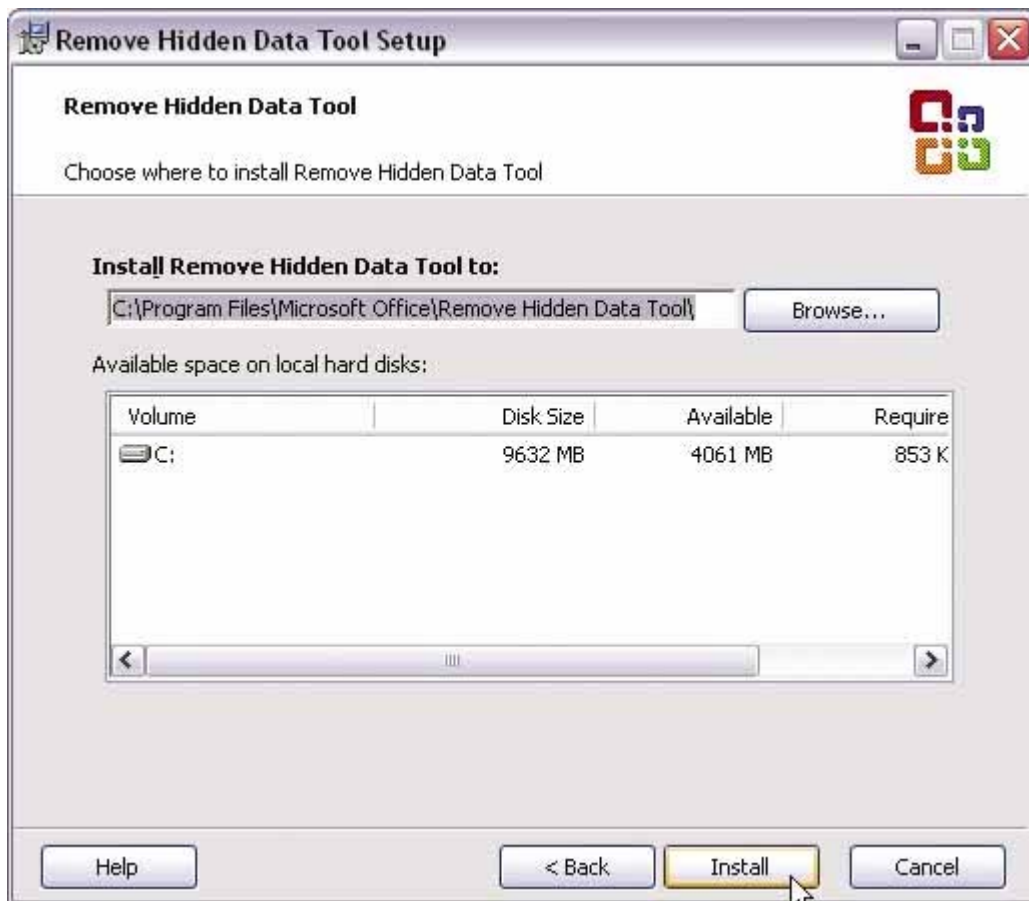


# Scrub Word Documents & Excel<sup>X</sup> Spreadsheets

## How To Remove Hidden Data That Lurks Inside

When you send a Microsoft Office document, such as an Excel spreadsheet or a Word document, outside your organization, you are also sending organizational secrets along with it and probably don't even think twice about it. You can make private corporate data available to the public via press releases you post on your Web site or in the form of a sensitive document you send to a client without even knowing about it.

What's Inside



**Remove Hidden Data Tool 1.1 requires 853KB of hard drive space and, unless you specify otherwise, creates and installs from the PROGRAM FILES\MICROSOFT OFFICE\REMOVE HIDDEN DATA TOOL\ directory.**

Remove Hidden Data Tool 1.1 requires 853KB of hard drive space and, unless you specify otherwise, creates and installs from the PROGRAM FILES\MICROSOFT OFFICE\REMOVE HIDDEN DATA TOOL\ directory.

Microsoft Word, Excel, and PowerPoint documents contain a lot of metadata that is not readily viewable in the document itself. Some of this data could be sensitive; it can include author names, computer names, file directory information, and collaborative information recorded using the Track Changes feature. Such information could shed unnecessary light on parts of your business that shouldn't be visible to external parties.

Securing your Microsoft Office document metadata can save both embarrassment and the unintentional slippage of organizational secrets, and that's where the Remove Hidden Data add-in comes in.

### Get Microsoft's Remove Hidden Data Tool

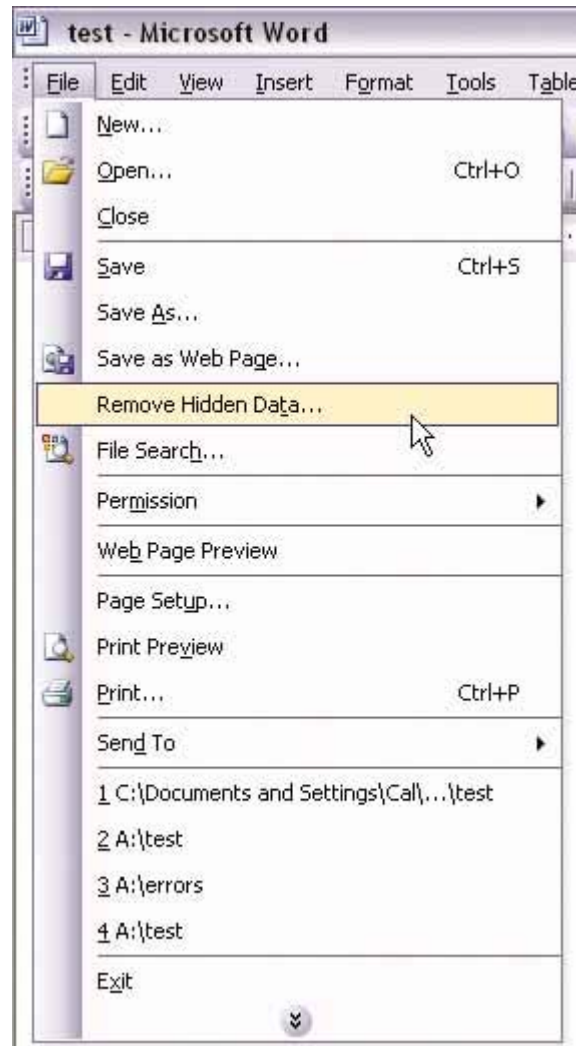
The Remove Hidden Data add-in (the actual program name is Remove Hidden Data Tool 1.1) works with Office XP and Office System 2003, although it runs only on Windows XP (Service Pack 1 or Service Pack 2) and Windows 2000 Service Pack 4. It's available at no charge from the Microsoft Office Online Home Page ([www.office.microsoft.com](http://www.office.microsoft.com)). When you visit the site, type remove hidden data in the Keywords box and click Go; then click the Office 2003/XP Add-In: Remove Hidden Data link that displays on the Search Results page. Follow the on-screen instructions to download, install, and run the rhdtool.exe file, which is 260KB in size and takes little time to download even with a dial-up Internet connection.

### Remove Hidden Data From A Single Document

You can access Remove Hidden Data Tool from the File menu in the 2002 (Office XP) and 2003 versions of Word, Excel, and PowerPoint. We suggest that you remove hidden document data as a final step after completing the document and before releasing the document externally.

Remove Hidden Data Tool only works if you save the document first, so save the file from which you want to remove hidden data. Click the File menu and select Remove Hidden Data; this displays the Remove Hidden Data dialog box. Click Browse to select a document from which you will remove hidden data. Then click Next. Enter a new file name for the file you are sanitizing with the Remove Hidden Data Tool. It's a best practice to save the document under a new file name and use the previous version of the file for archival purposes. Follow the prompts until you complete the process. The tool produces a read-only version of the file without any hidden data.

## Run Remove Hidden Data Tool On Multiple Documents



**To remove hidden data from a saved Word 2002/2003 document, start by selecting Remove Hidden Data from the File menu.**

You also have the option to use Remove Hidden Data Tool from a command line interface for sanitizing multiple Office documents of metadata. Some users consider working from a command line more expedient, but you will have to know some syntax in order to execute Remove Hidden Data Tool on multiple Office documents.

Start by closing all Microsoft Office applications running on the PC. Then click Start and Run to open the Run dialog box. Type cmd in the Open field. Click OK or press ENTER

to bring up a command line prompt. Next, change to the directory where you installed Remove Hidden Data Tool 1.1; this directory houses the Offrhd.exe file (the tool's application file). The syntax for running Remove Hidden Data Tool 1.1 from the Windows command line is as follows:

```
OFFRHD [/?] source [destination] [/O] [/R] [/F:filetype] [/L:logfile] [/A]
```

To remove hidden data from a saved Word 2002/2003 document, start by selecting Remove Hidden Data from the File menu.

For source, specify the file location for the document you want to sanitize. The source can be a drive, directory, or file. For example, you could create a directory in which to place the documents you want to sanitize with the Remove Hidden Data Tool and then use that directory as your source.

You don't have to use the Destination parameter; how you decide to use it is ultimately a question of file management. This parameter specifies the target destination for the sanitized files. Although it makes sense to create a new destination directory for these files, it is not a requirement. To use it, replace destination with the directory location. If you don't use this option, the output files will be saved in the same directory with today's date as a prefix to the file name.

Overwriting a file is usually not a good practice when dealing with sensitive documents, but you can use the /O parameter to govern whether a prompt appears when you try to overwrite an existing file with a scanned file. Include the /O parameter in the syntax if you don't want Remove Hidden Data Tool to ask whether you want to overwrite the existing file.

Remove Hidden Data Tool scans files in the specified directory. If you also want the tool to scan files in the subdirectories, include the /R parameter.

The /F parameter specifies the output format of the destination files generated after the Remove Hidden Data Tool finishes sanitizing a document of metadata. You can specify the following options for the filetype portion within the /F parameter:

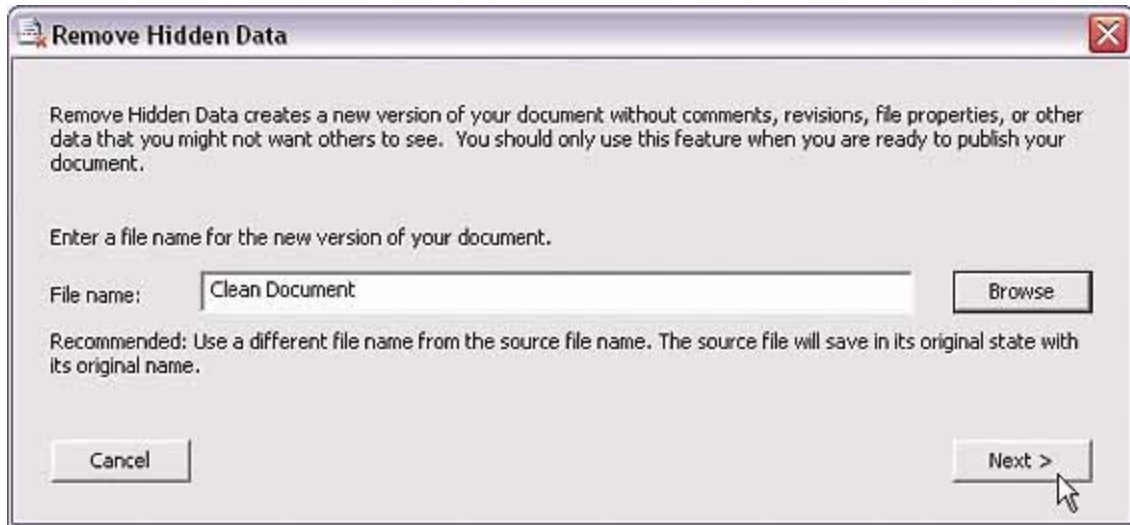
- H (as in /F:H) to specify standard HTML as the destination file's output format.
- B (as in /F:B) to specify a binary file as the destination file's output format. The default for this parameter is to save the sanitized file in the same format as the source file.
- M (as in /F:M) to specify MHTML (Mime Encapsulation of Aggregate HTML; an Internet standard for sending HTML-based files) as the destination file's output format.

Log files are useful in the Remove Hidden Data Tool process to help troubleshoot any issues that occur during the process. The /L parameter governs the location of the log file, where you can replace logfile with a specific directory path.

Errors can occur when using the Remove Hidden Data Tool due to a variety of circumstances. Tracking the issues helps troubleshooting. The /A parameter, should you decide to use it, specifies that the tool will output a report of any issues encountered while running on multiple documents.

If you forget what the parameters are, you can use the /:? parameter to display a list.

### Use Remove Hidden Data Tool On Protected Documents



**When scrubbing a document of its metadata, Remove Hidden Data Tool saves the scrubbed document under a new name that you specify.**

When scrubbing a document of its metadata, Remove Hidden Data Tool saves the scrubbed document under a new name that you specify.

Office 2003 includes support for IRM (Information Rights Management), an additional layer of security that guards corporate information and intellectual property created in Microsoft Office 2003 Professional with special access policies. You can use Remove Hidden Data Tool on IRM-protected documents, but you must first adjust document permissions. You must either be the document owner, or the owner must grant you Change permission to run the tool.

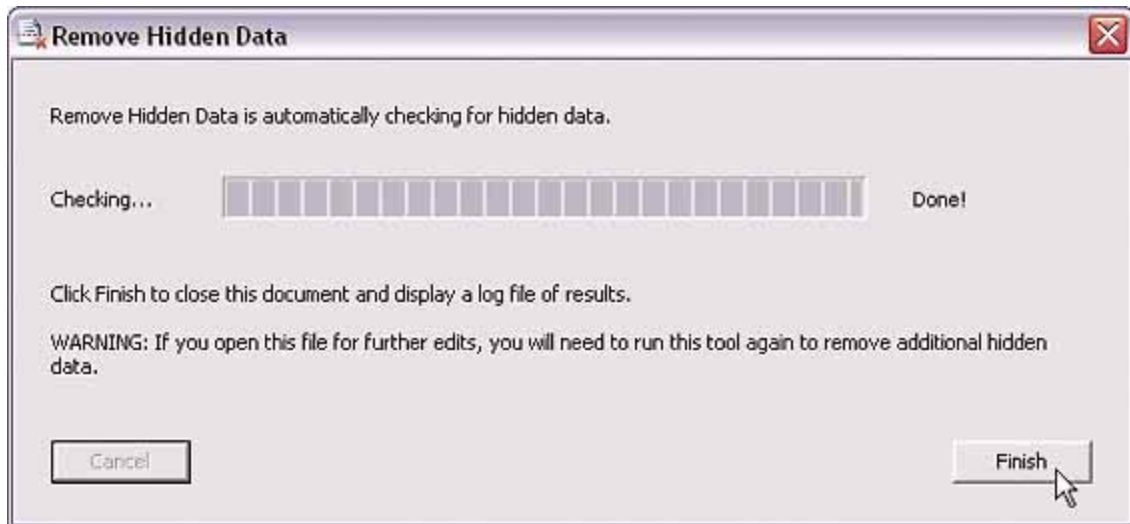
Open the IRM-protected document, go to the File menu, and select Permission to open the Permissions drop-down menu. Click More Options. Select the user account for the person running the Remove Hidden Data Tool on the document. Remember, Change permission is required to run the Remove Hidden Data Tool. Select Access Content to enable Remove Hidden Data Tool access to the document, and click OK to confirm the choice.

### Other Security Measures For Your Documents

Using the Remove Hidden Data Tool should be one element of your overall document metadata security strategy. Making tracked changes permanent and setting privacy options should become standard practice along with use of the Remove Hidden Data Tool 1.1 prior to sending documents out of your organization.

Office's Track Changes and Comments features are standard methods for revising and adding feedback to Office documents. The Reviewing toolbar includes options for accepting changes and rejecting changes. Always use these options as opposed to just setting the document view to Final. The Track Changes marks are still in your document, and all a reader needs to do is to change the view to Original Showing Markup or Final Showing Markup to view the tracked changes.

A progress bar indicates the status of the data removal process.



**A progress bar indicates the status of the data removal process.**

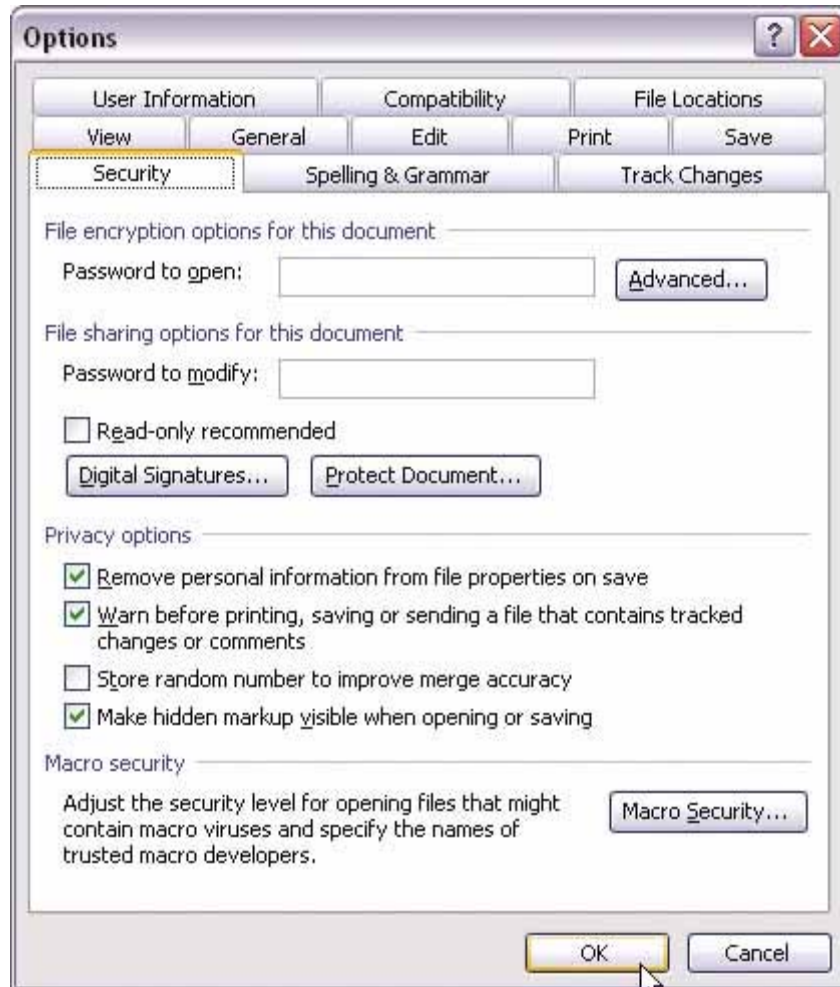
There are also privacy options included in Word 2003, Excel 2003, and PowerPoint 2003 which can help secure your document's metadata. In any of these programs, go to the Tools menu and select Options. Select the Security tab, and under Privacy Options make sure the following checkboxes are checked:

- Remove Personal Information From File Properties On Save
- Warn Before Printing, Saving Or Sending A File That Contains Tracked Changes Or Comments
- Make Hidden Markup Visible When Opening Or Saving

Secure Documents With Non-Microsoft Products

Lastly, if you are seeking a non-Microsoft solution for securing your document's metadata from prying eyes, then two ready options are Adobe Acrobat 6.0 (\$299 for Standard version, \$449 for Professional version; [www.adobe.com](http://www.adobe.com)) and Macromedia FlashPaper 2 (\$79; [www.macromedia.com](http://www.macromedia.com)).

In addition to using Remove Hidden Data Tool, use the Security tab in your document's Options dialog box to specify what privacy options to apply.



**In addition to using Remove Hidden Data Tool, use the Security tab in your document's Options dialog box to specify what privacy options to apply.**

Although Adobe's PDF (Portable Document Format) is already an industry standard, FlashPaper 2 files are beginning to gain traction as an alternative for posting documents online. FlashPaper 2 renders documents in Macromedia Flash format. Choosing PDF as a document output format still requires you to set the privacy options described earlier in

this article because some document properties do transfer over in the Acrobat distillation process. FlashPaper 2 has no such requirements.

### A Complete Security Policy

Putting the measures described in this article into practice can help ensure another level of security over your organization's documents. You protect the integrity and security of your organization by secure document metadata before the documents leave your organization.

Use of the Remove Hidden Data Tool 1.1 should be worked into your current document creation and dissemination process. Keep in mind that you should run the tool as the last step before sending a document out the door.

by Will Kelly