

Realtime
publishers

The Essentials Series:
Operations Benefits of Email Archiving

Eradicating PST Files from Your Network

sponsored by



by Jim McBee

Eradicating PST Files from Your Network	1
Understanding the Disadvantages of PST Files.....	1
Incorporating PST Files into the Archive	3
Blocking PST File Usage.....	3
Archiving Solutions Overcome PST Limitations	5

Copyright Statement

© 2008 Realtime Publishers, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtime Publishers, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtime Publishers, Inc or its web site sponsors. In no event shall Realtime Publishers, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtime Publishers and the Realtime Publishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtime Publishers, please contact us via e-mail at info@realtimepublishers.com.

Eradicating PST Files from Your Network

Prior to the popularity of email archiving systems, Microsoft Personal Folders (PST) files were often used as a form of email archiving. In fact, Microsoft Outlook has a feature that will automatically move mail out of a user's mailbox and into a PST file.

For specific reasons, PST files may be of use for an Exchange administrator. One reason would be to provide a mechanism to move email data between two Exchange Server systems. Another reason would be to deliver requested email data to opposing counsel in the case of litigation. However, if you have or are implementing an email archiving system, there is no good reason to allow end users to employ PST files.

This article will explore the disadvantages of using PSTs, ways to incorporate existing PST files into an email archiving system, and methods for blocking future PST file usage.

Understanding the Disadvantages of PST Files

At first glance, PST files might seem like a useful feature, but PST-based archiving and storage can introduce potential legal issues as well as assorted headaches. The use of PST files often results in lost or misplaced data due to a variety of reasons:

- Outlook has an “auto-archive” feature that will automatically move mail to an archive. PST file located in the Local Settings folder, which is on the user's local hard drive. In many Outlook installations, this feature is enabled by default; thus, users often having PST files on their local hard drives without even realizing it.
- Users who move from one computer to another frequently end up with multiple PST files or archive PST files with content spread across those computers.
- Once email is moved to a PST file, it is no longer accessible via remote technologies such as Outlook Web Access (OWA) or Windows Mobile/iPhone devices.
- Outlook configured to be a POP3 client using an Exchange Server will pull all mail out of the mailbox and place it in a PST file.
- Outlook has a “local delivery” option available during the Outlook profile configuration that will enable Outlook to pull all mail off the Exchange Server and use a PST file as the primary storage location for email, calendar, and contacts. The shortcomings of this setting usually do not manifest until the user's local hard drive fails and the computer is rebuilt; then, of course, the user's email is gone.
- The default location for PST files is in the Local Settings portion of the user's Windows profile; this location is on the user's local computer. Local computer hard drives are not backed up in most organizations. In addition, the use of file shares (such as a user's home folder) to store and access PST files is neither supported nor recommended by Microsoft (for more information, see Microsoft Knowledge Base article 297019).

A fairly common issue that arises as a result of PST usage stems from the fact that users can password-protect a PST file; if they forget the password, a third-party utility or data recovery service will be required to retrieve the data. The password-protection feature often gives users a false sense of security because they don't realize that the feature can be disabled and sensitive data can be compromised.

In addition, the PST file was never intended for or designed to store large amounts of data; thus, data is not efficiently stored in PST files. Message bodies stored in PST files are stored twice; once in the ASCII text format and once in rich text. This duplication can result in PST files consuming a considerable amount of disk space. Also, Outlook 2002 and earlier PST files are limited to a maximum size of 2GB. Corruption will occur at 2GB, but the file's performance declines before that limit is reached. And Unicode PST files cannot be read by Outlook 2002 and earlier or the ExMerge program.

One of the biggest headaches for Exchange administrators is that email that is moved into a PST file is no longer centrally managed. Therefore, it is difficult and expensive to collect data for eDiscovery because the task of locating widely distributed PST files is challenging. PST files can be an easily hidden form of data leakage, as a disgruntled employee can quickly and easily transfer many gigabytes of mail data to PST files, transfer those files to a USB thumb drive, and walk out with the data.

Given these downsides to PST files, mail administrators are looking for ways to eliminate PST-related support calls. This article focuses on the additional benefits realized by eliminating the need for PST files. Your email archival system can allow nearly limitless email storage for a user's historical data while keeping the amount of email on the production mail server at a minimum.

PST File Internal Political Considerations

Don't discount the importance of end-user education regarding the elimination of PST files. Recently, I was working on a customer site that was both upgrading to Exchange Server 2007 and deploying an email archive system. The customer was implementing the archive system in order to reduce the total amount of mail storage required to make the actual migration run much faster.

This organization had always enforced mailbox limits for their users, and expected users to "self police" based on mailbox limitations. Users were routinely instructed on how to create PST files when their mailboxes were full.

During the upgrade and deployment process, one of the organization's email archive system operators discovered a user's home folder that contained a PST file for each quarter of each year since 1997. These files ranged from 350MB to 1.5GB in size. When this user first learned that her PST data would be moved out of her home folder and into the new email archive system, she was panicked about losing the PST files. However, once she understood that the new interface would allow her to have a full-text index of all her imported PST files and current data, she gladly gave up her PST files.

Incorporating PST Files into the Archive

Most email archive solutions provide a console program or tool that allows either an operator or end user to import PST files into the archive. As soon as your archive system is functional, begin the process of importing all PST files for all active employees. Doing so serves multiple purposes:

- Importing the users' PST files into the archive will immediately make users' historical information available to the end users. In addition, the data will be available for authorized users to perform eDiscovery searches.
- If PSTs are located in users' home folders or on file server storage, moving the PST data into the archive can allow for the recovery of file server disk space of as little as a few hundred megabytes to dozens of gigabytes.
- The more quickly an email archive system is put in place and a plan is established to import the PST files on the network, the less likely there will be any data loss.
- When PST files are no longer necessary, policies can be established that prevent end users from creating PST files.

 Beware of email archiving systems that require PST file data to be first imported back to users' mailboxes before being moved into the archive. This task adds considerable extra work and will dramatically increase the size of the Exchange Server databases.

Blocking PST File Usage

Once you have an email archiving system in production, the next step is to prevent users from creating or moving content into PST files. There are a few ways to ensure that you harvest all PST files, prevent users from creating new files, and completely eliminate PST-based mail storage:

- Use Active Directory (AD) Group Policy Objects (GPOs) to prevent future use of PSTs.
- Use the Microsoft Office deployment tools to ensure that future deployments of Outlook do not include the option to create or use PSTs.
- Write a script to scan users' home folders and move PSTs to a central location for importing; make sure your script can properly identify the owner of the PST when it is copied.
- Write a script (such as a logon script) that will scan a user's local profile for PST files during logon and copy them to a shared location.

The simplest and most effective of these approaches is to use Group Policy to restrict PST use. To do so, you need the Group Policy Administrative (ADM or ADMX) templates for the versions of Office that you support. You can download these from the Microsoft Office Web site (to find them, simply search the site for the text “ADM”). Once you have the ADM templates, create or edit an existing GPO, and add the appropriate templates to the Group Policy. Figure 1 shows a sample of the PST settings available in a GPO.

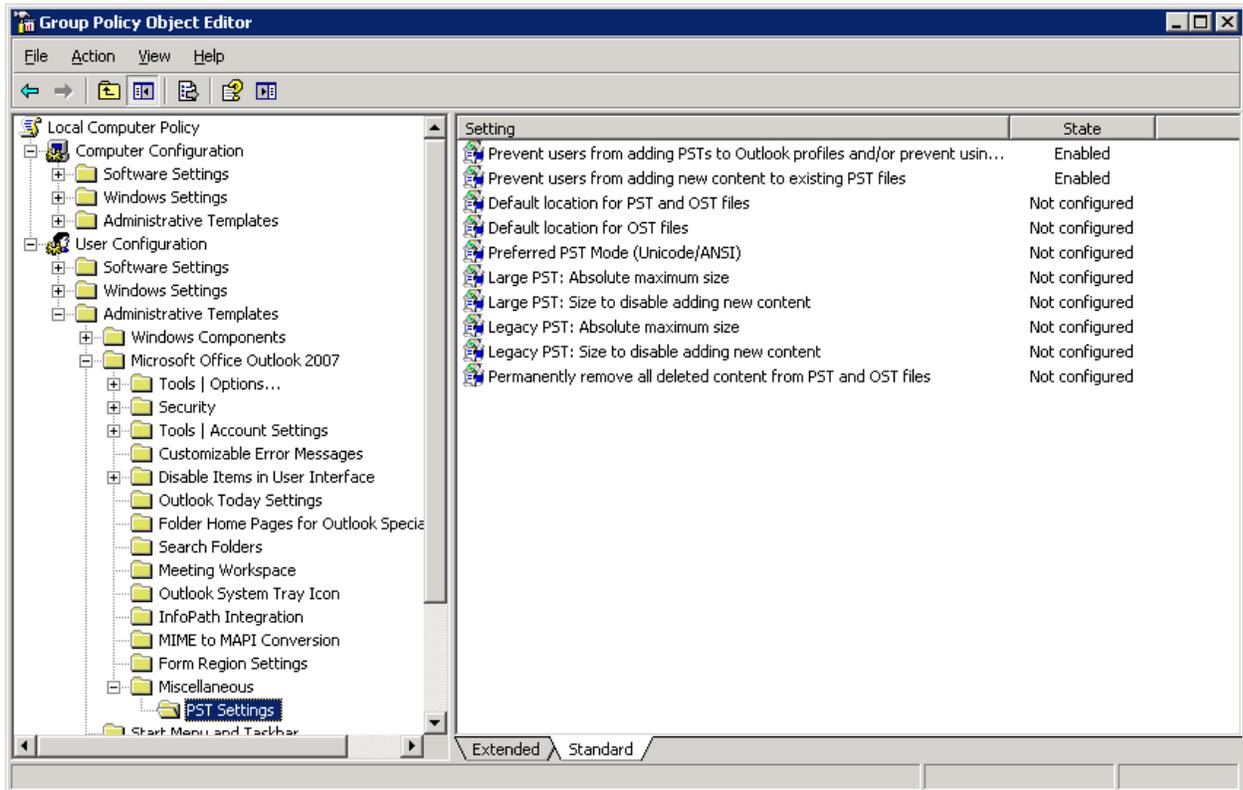


Figure 1: PST settings in a GPO.

The two settings that are enabled in the figure—*Prevent users from adding PSTs to Outlook profiles* and *Prevent users from adding new content to existing PST files*—are the ones you need to enable to prevent users from adding PSTs to Outlook and to prohibit users from adding new content to existing files. Keep in mind that not all PST restrictions will be available in older versions of Office/Outlook.

Archiving Solutions Overcome PST Limitations

PST files are often the result of mailbox storage limitations placed on users: Users require more email data storage than they are allowed, so they create PST files to move data off the Exchange Server. As discussed earlier, the spread of PST files across local hard drives and home folders, the lost data (or at the very least, misplaced data) that ends up in these PST files, corrupted PST files, and data that may now escape a mandatory legal eDiscovery are all good reasons to eliminate PSTs. Doing so will not only reduce Help desk calls but also aid with an organization's compliance and discovery requirements, simplify users' access to older email, and reduce the storage burden on home folders or local hard disk drives. With an email archive system, users no longer need to create PST files.

Before the deployment of an email archiving system, begin planning your PST eradication strategy. Important steps that you should consider immediately include:

- Develop a plan that covers how you will locate all PST files on your network, including users' local hard disks.
- Plan the best approach to import each user's PST data in the archive without moving the data from the PST files back into the Exchange Server databases. If users will be required to import the PST files into the archive themselves, develop a training plan that will teach users how to do so.
- Determine how you will prevent the creation and use of PST files in the future—for example, by blocking their use via AD GPOs.

The implementation of an email archive system is the best way to ensure the eradication of PST files because it will inhibit users from ever needing to move data to PSTs while still allowing users the capacity necessary to store virtually unlimited historical email.