

— REDiSAFE™ NEWSLETTER —



REDiSAFE™

Support for Microsoft Outlook

A new feature

“With REDiSAFE, you are able to backup your mails, contacts and appointments automatically.”

REDiSAFE will be able to backup PST files(protected by Microsoft) for Microsoft Outlook 2003 and onwards soon. The Personal Folder file (.pst / PST) is the place where Outlook stores its data (when you're using Outlook without Microsoft® Exchange Server).

REDiSAFE now provides incremental email backup, resulting in a much faster process and a smaller backup file size. Restoring those data will also be faster and you do not need to restore such a huge PST file with REDiSAFE. Files that are backed up in REDiSAFE will also be encrypted and compressed.

Each Personal Folder file contains all of your Outlook folders, including the Inbox, Calendar, and Contacts. You may have a single .pst file or you may also have an additional .pst file that you use to archive messages (named "Archive Folders"). By backing up these PST files you will be backing up most of your Outlook information.

With REDiSAFE, you are able to backup your mails, contacts and appointments automatically. You can simply schedule your backup and the REDiSAFE client will help you back up those mails automatically. REDiSAFE with its' near zero daily administration is highly preferred by many IT departments. Thanks to its highly automated self contained administration and web-based client application, Recovery can be as easy as a click of a button.



The usual way to backup the Microsoft Outlook is to backup the entire PST files. The PST file has a upper limit of 2GB and in average ranges from 300 to 500 MB. This results in a huge amount of data to be backed up daily.

Target date of release Mid - Q2'06

Text Justin Foo

REDiSAFE SECURITY

The ultimate data protection system

“Maximum security to your data in the servers”

REDiSAFE places important emphasis on security of data that is backed up and stored in the REDiSAFE server appliances.

From the moment a user's data leaves the client's machines, a SSL connection can be enabled to securely transfer the data from the client to the REDiSAFE servers.

The data will be compressed and encrypted at the server before being stored within the designated storage space provided to the individual user. As REDiSAFE does not execute any files during the backup, it is resilient to any virus-infected files or malicious form of files. These files could have broken through the virus-protection strategy of the corporate network.

When a company deploys the remote REDiSAFE server, for business continuity and disaster recovery planning, the same set of data in the local REDiSAFE server will be transmitted by a secured protocol, rsync over SSH, to the remote REDiSAFE server. This also ensures that data are kept secured and integrated.

REDiSAFE's two token security system ensures that security of data stored are not compromised. For normal functioning of the REDiSAFE server, ie. for backup and recovery, an authorised administrative token inserted upon every cold start of the system. This provides maximum security to your data has to be in the servers and you will not need to worry even if your server are stolen. To prevent unauthorized access to recover particular user's data onto alternative machine, REDiSAFE server will require an emergency token which is usually held by an authorized officer or director of the company.

With REDiSAFE you can be assured that all your data is well protected.



Text Meng Piow