

Secure Microsoft Exchange Backups with SecureZIP

Messages and attachments in Microsoft® Exchange Server email databases contain valuable and often sensitive information. For regulatory compliance and to ensure business continuity in the event of a calamity, an email administrator needs to make routine backup of company email a critical part of his organization's recovery procedures.

This guide describes how to use SecureZIP to apply strong encryption to Exchange backups done with the standard Microsoft backup utility programs. Adding encryption to the backup process secures the backups and ensures their confidentiality both when stored and when in transit to a storage facility.

What You Need

This guide assumes that you have an Exchange 2000/2003 environment and are using one of the native backup utilities provided with Exchange, namely:

- NTBackup
- ExMerge, the graphical Microsoft Exchange Mailbox Merge wizard

You can run these utilities to do backups on the Exchange server itself, if you have sufficient disk space, or on a remote server that has the Exchange Management Tools installed.

Backup and Encryption of the Information Store

Various backup solutions are available for Exchange, including third-party applications such as ARCserve® and Backup Exec™. Determining which is most suitable in your case depends on such factors as the size of your organization and your requirements for advanced scheduling and media library devices. Microsoft recommends using NTBackup to back up your Exchange databases, so this guide focuses on using that approach. SecureZIP easily integrates with any pre-existing NTBackup schedule to provide the compression and encryption you need to securely store your data.

Integrate with Pre-Existing NTBackup Scheduled Task (GUI)

If you manage your Exchange database backups with the aid of the NTBackup GUI, the best way to use SecureZIP to encrypt your information store is to simply create a separate, second scheduled task that runs after your database backups. The second task can be responsible for compressing and encrypting your data.

Such a task can simply run the SecureZIP **pkzipc** command-line utility to instruct SecureZIP to archive any .bak files your backup job has created. The following sample code provides a template. (Some line breaks are adjusted for readability in this and other code samples in this guide.)

```
@echo off
REM Misc pre-job operations

REM You can use certificate- or password-based encryption to secure
REM your Archives

REM Example using password based encryption
pkzipc -add -password="<secret>" d:\backups\exch\store.zip
d:\backups\exch\store.bak

REM Encrypt backups using the backup_admin certificate.
REM Certificate is pulled through LDAP from a local domain controller
pkzipc -add -ldap=pknet\backup_admin:secret@domain_controller:389/ou=
organization_inc,dc=domain,dc=com -recipient=backup_admin@domain.com
d:\backups\exch\store.zip d:\backups\exch\store.bak

REM misc post-job operations
:end
Exit
```

As you can see, this approach also enables you to use scripts to do your NTBackup jobs in batches. Depending on your security requirements, you can use either password-based or certificate-based encryption methods for securing backup files. The example script above provides command lines for both cases. Comment out the method you do not need.

Integrate with a Batched NTBackup Job (Command Line)

If you customarily manage your Exchange database backups with scripts and batch files, you can incorporate calls to the SecureZIP command-line interface to add compression and certificate-based encryption to your backups. For example:

```

@echo off
SET servername=exch-server

REM misc pre-job operations

IF EXIST d:\backups\exch-server.bks GOTO run

ECHO JET %SERVERNAME%\Microsoft Information Store\First Storage Group\
>d:\backups\exch-server.bks

ECHO JET %SERVERNAME%\Microsoft Site Replication Service\SRS Storage\
>>d:\backups\exch-server.bks

ECHO SystemState >>d:\backups\exch-server.bks

GOTO run

REM Create Backup job that will backup the system state, mail store,
REM and srs storage on the mail server: exch-server

:run

C:\WINNT\system32\NTBACKUP.EXE backup "@D:\backups\exch-server.bks" /n
"Media created mm/dd/yyyy at hh:mm PM" /d "SystemState-MailStore-SRS"
/v:yes /r:no /rs:no /hc:off /m copy /j "SystemStage-MailStore-SRS"
/l:s /f "D:\backups\mailbox_store.bkf"

REM Call SecureZIP Command Line to compress and certificate encrypt
REM for the backup-admin certificate found in the LDAP directory

pkzipc -add -ldap=
pknet\backup_admin:secret@domain_controller:389/ou=
organization_inc,dc=domain,dc=com -recipient=backup_admin@pkware.com
d:\backups\exch\store.zip d:\backups\exch\store.bak

REM misc post-job operations

:end
exit

```

Brick-Level Backup and Encryption with ExMerge

Brick-level backup jobs (that is, jobs that back up at the level of individual mailboxes) log into selected mailboxes within the store using a MAPI client. They then export all of the messages in the mailbox to a location on the file system where they can be backed up to your media library of choice. Folder structure is maintained during the export.

Brick-level backups deal only with individual mailboxes. They cannot be used to restore an entire mail server. Only use brick-level backups in conjunction with a full information store backup.

The Exchange utility ExMerge can do brick-level backups of individual Exchange mailboxes. The utility is included in the Exchange 2000 Resource

Kit. Before using, it must first be extracted to %Program Files%\Exchsrvr\bin. ExMerge must run as a user with full mailbox access rights to the mailboxes from which you want to export messages.

ExMerge is a graphical utility with batch options. It is useful for quickly backing up one or more selected mailboxes. A batch or scheduled brick-level job with ExMerge requires the following files:

- A script to run the job and secure the backups
- An `exmerge.ini` file that tells ExMerge what settings to use when performing the backup
- A `mailboxes.txt` file that tells ExMerge which mailboxes to backup

When you do a backup from the ExMerge GUI, ExMerge itself creates the `exmerge.ini` and `mailboxes.txt` files if they do not already exist.

To create a scheduled ExMerge backup, first do a one-time backup to create the `exmerge.ini` and `mailboxes.txt` files. Then supply a script referencing these files to run as a scheduled backup. You can incorporate in the script calls to SecureZIP to encrypt the backup.

Note that ExMerge does *not* password-protect or encrypt the `.pst` files it creates. To add this security, you must use SecureZIP to encrypt the files.

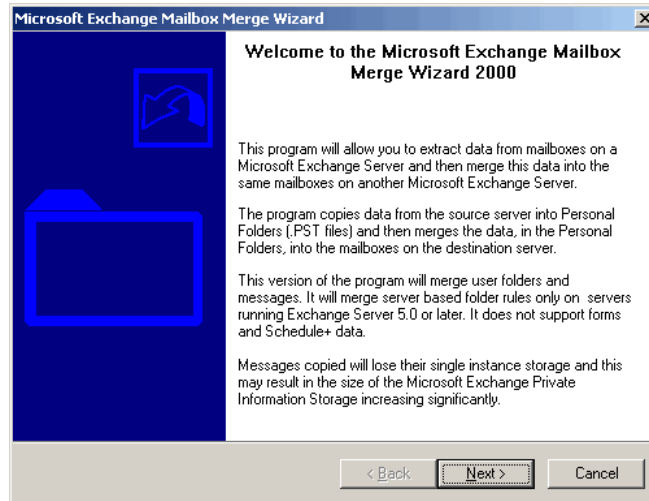
Steps to run a one-time ExMerge backup, and a sample script for a scheduled backup, are given in the following sections.

Perform a One-Time ExMerge Backup

To perform a one-time backup with ExMerge and create `.pst` files from selected mailboxes, follow the steps below.

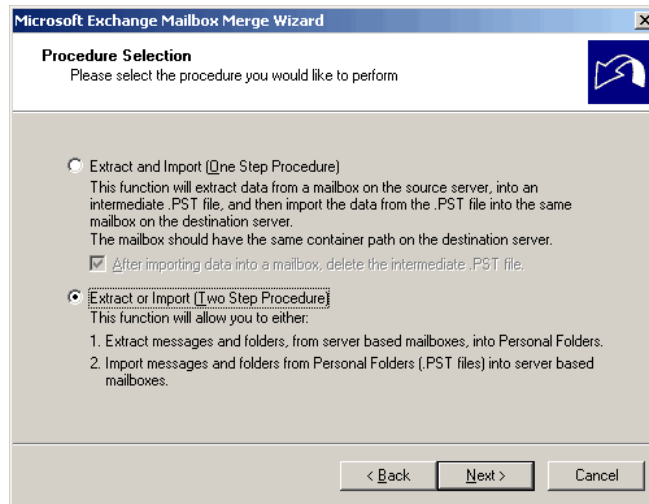
1. Run ExMerge.

Double-click `exmerge.exe` in the `exchsrvr\bin` directory (assuming you extracted it there) to display the Welcome screen shown below.

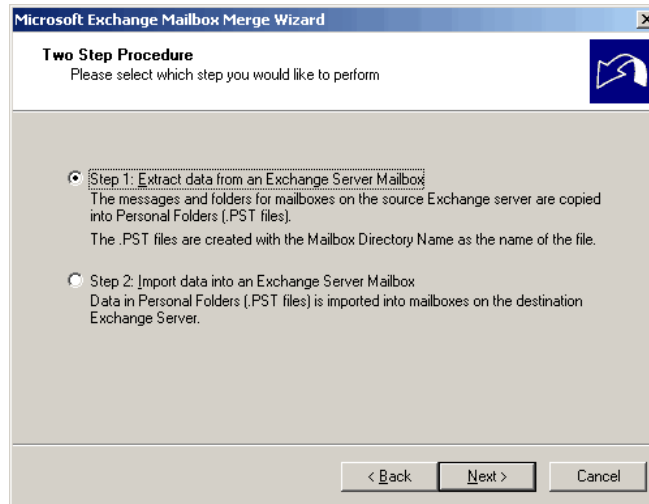


2. Choose **Next**.

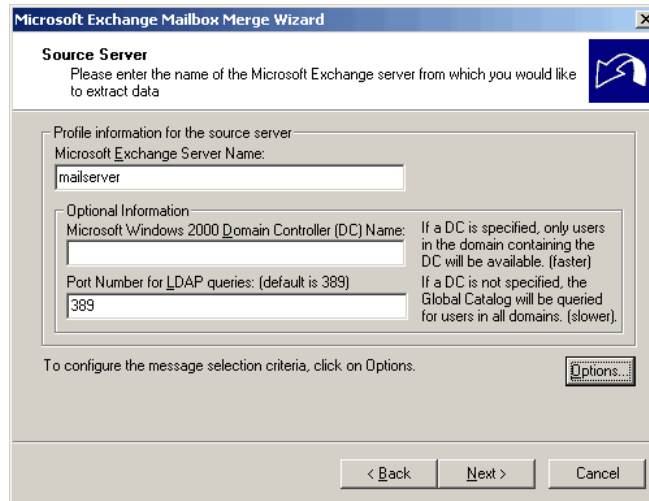
You are asked to select a procedure to perform.



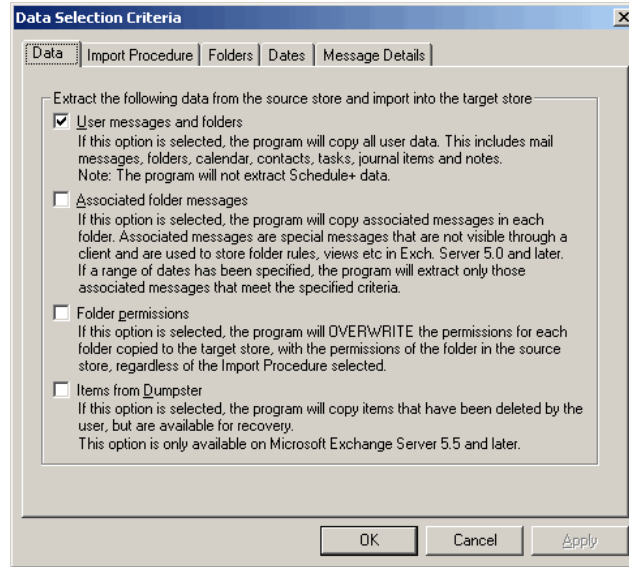
3. Select the *Two-Step Procedure* option and choose **Next** to open the dialog shown below.



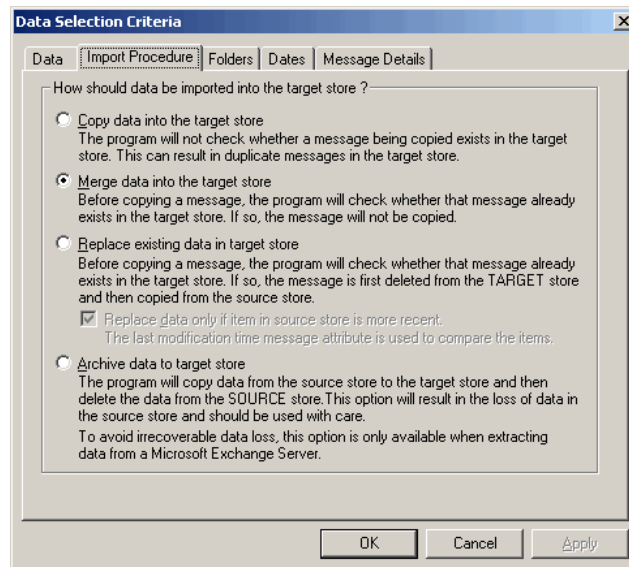
4. Select the option to *Extract data from an Exchange Server Mailbox* and choose **Next** to open the dialog shown below.



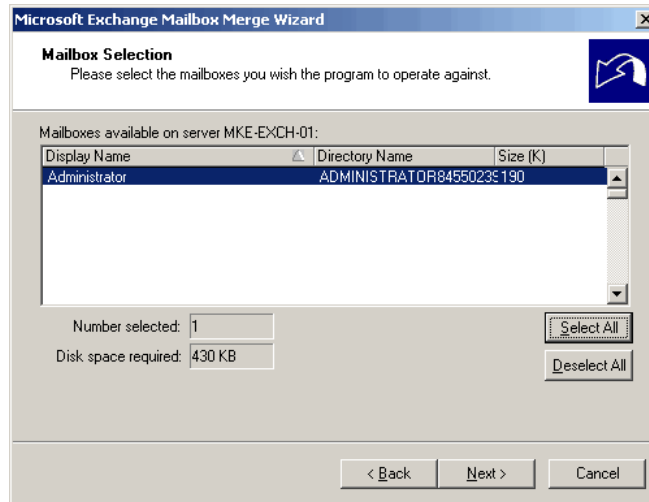
5. Specify the mail server name. Optionally, you may also enter the name of a domain controller. Then choose **Options** to open the dialog shown below.



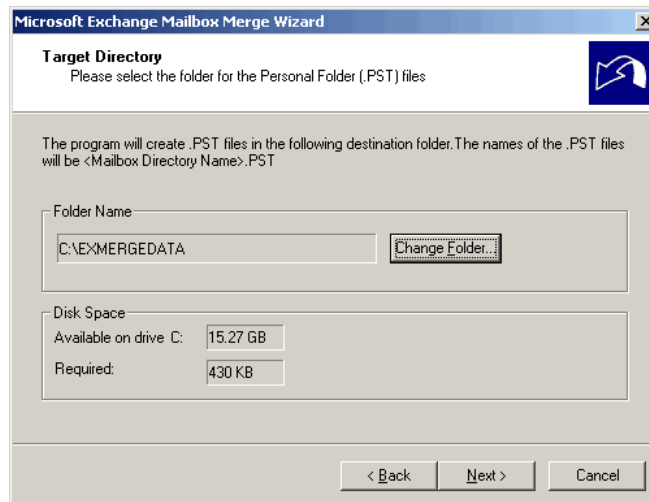
6. On the Data tab, select *User messages and folders*. Then select the Import Procedures tab.



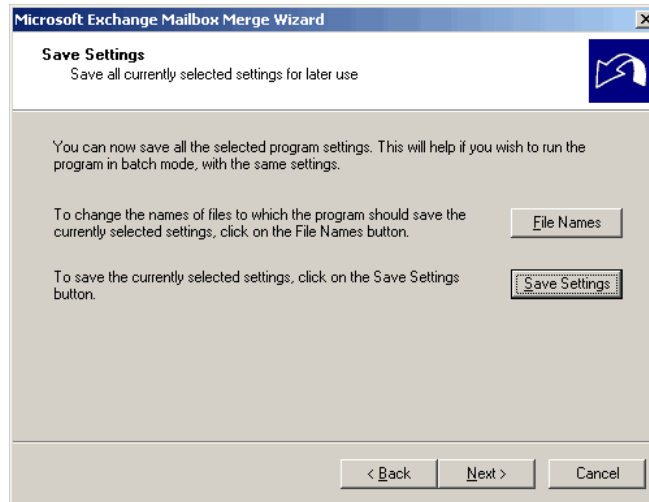
7. On the *Import Procedures Tab*, select *Merge data into the target store* and choose **OK** to open the dialog shown below.



8. Select the mailboxes you want to back up and choose **Next**. A dialog opens in which to select a target directory.



9. Select a location where you want to save the exported contents of the mailboxes. Choose **Next** to open the Save Settings dialog.



10. Choose **Save Settings**. Then choose **Next** if you plan to test or run your settings immediately. Otherwise, you can press **Cancel** if you plan to run a batch process.

Saving the settings creates new `exmerge.ini` and `mailboxes.txt` files in the folder that contains `exmerge.exe`. The files are text files. You can edit them to make changes instead of running ExMerge again.

For example, the following sample shows how mailboxes are specified in `mailboxes.txt`. To add more mailboxes, edit `mailboxes.txt` to add similar entries.

```
sample: mailboxes.txt

/O=FIRST ORGANIZATION/OU=FIRST ADMINISTRATIVE
GROUP/CN=RECIPIENTS/CN=user1

/O=FIRST ORGANIZATION/OU=FIRST ADMINISTRATIVE
GROUP/CN=RECIPIENTS/CN=user2

Etc...
```

Perform an ExMerge Backup from a Script

When you do a scripted ExMerge backup, you can incorporate calls to SecureZIP to encrypt the backup.

Below is a sample script that runs a job and calls SecureZIP to encrypt the resulting `.pst` files.

```

@echo off

REM sample brick_level.bat file.
REM misc pre-job operations

REM Call EXMERGE and run the backup job.
REM use -F to specify the setting's file: (exmerge.ini)
REM use -B for batch mode (required if running from a scheduled task)
REM use -D to display the GUI progress window while running

D:
cd progra~1\exchsrvr\bin
exmerge -F exmerge.ini -B -D

REM Encrypt backups using the backup_admin certificate.
REM Certificate is pulled through LDAP from a local domain controller

pkzipc -add -ldap=
pknet\backup_admin:secret@domain_controller:389/ou=
organization_inc,dc=domain,dc=com -recipient=backup_admin@domain.com
d:\exmergedata\ mailboxes.zip d:\exmergedata\*.pst

REM misc post-job operations

:end
Exit

```

You can run the script as a scheduled task. To add or remove user mailboxes from the job, just edit the `mailboxes.txt` file.

Notes

To learn how to configure an administrator account to use ExMerge, see the following Microsoft Article, ID 823143:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;823143>

To learn more about using the GUI and batch features of ExMerge, see the `exmerge.doc` file included with the utility.

Restoring and Decryption

The preceding backup examples used NTBackup or ExMerge to create a backup file in `.bak` or `.pst` format, respectively. SecureZIP was then used to compress and strongly encrypt the backup file into a standard ZIP file. To restore these encrypted backups when a recovery operation is required, you simply reverse the steps: First use SecureZIP to decrypt and extract the backup you want from the ZIP file that contains it. Then process the unencrypted backup file normally using either NTBackup or Exmerge.

Decrypting Password-Encrypted Files

When password-based encryption is used, you need only add the appropriate password on the SecureZIP command line to decrypt.

For example, the script below extracts and decrypts the password-encrypted file `joe_user.pst` from the ZIP archive

```
D:\backups\pst\bricklevels.zip
```

The password option is used to supply the password.

```
REM To extract a single PST file from a password encrypted archive
pkzipc -extract -password=p@$w0rD D:\backups\pst\bricklevels.zip
joe_user.pst
```

The following sample script decrypts files in `store.zip` that are encrypted with the supplied password and extracts them to `D:\backups\exch\`:

```
REM To extract an encrypted mail store backup made with NTBACKUP
pkzipc -extract -password="<secret>" d:\backups\exch\store.zip
d:\backups\exch\
```

Decrypting Certificate-Encrypted Files

Files that are encrypted with a public key are decrypted by applying the corresponding private key. SecureZIP applies the key for you automatically if SecureZIP can find it. Unlike with password-based encryption, no special option is needed on the command line to decrypt certificate-encrypted files.

To decrypt a certificate-encrypted file, SecureZIP looks for a suitable private key in the current user's Windows Personal Store. Unlike public keys, which can be publicly distributed or placed on Active Directory, private keys must be protected and kept under the sole control of the owner. For a restore operation, a private key for which the backups were encrypted must be in the Windows Personal Store of the administrator who will restore the data. If (and *only* if) such a key is found, SecureZIP transparently decrypts the files.

For example, the command line below extracts and decrypts the contents of `bricklevels.zip` if `bricklevels.zip` is encrypted for the user who runs the command, and the user's private key is on the system. The SecureZIP `extract` command is the only command or option required.

```
REM To extract the contents of a certificate encrypted archive that
REM contains a single PST file
pkzipc -extract d:\backups\pst\bricklevels.zip
```

Once extracted, the files can be used for a restore.