Microsoft® Desktop Optimization Pack
for Software Assurance

MBAM Data Retention and Consistency Strategies

Technical White Paper

Published: September 2011

William Lees, James Hedrick, and Nathan Barnett

Microsoft®

CONTENTS

Situation

Encrypted volumes may outlast their original use. Recovery Keys for these volumes must be retained for an extended period to meet data retention requirements.

Solution

Adhere to best practices for backup, restore and archival of MBAM databases can assure consistently complete key retention over time.

Benefits

- Reduce windows where Keys may be lost
- Assure recovery keys are available to meet data retention requirements
- Ensure that backups are high fidelity and complete and consistent
- Ensure that Enterprise is in a clean, predictable state moving forward after an MBAM database restoration

Products & Technologies

- Microsoft Windows Server 2008 (and R2)
- Microsoft SQL Server 2008 (and R2)
- Backup feature in Windows Server 2008 (and R2)
- Microsoft Data Protection Manager

EXECUTIVE SUMMARY

Encrypted Disk Volumes outlast their original use, original computer, original owner, and original purpose or role. MBAM centralizes and applies uniform policy over such volumes when they are in active use, but how are the keys retained after the original utilization of the volume is complete, but the volume lingers on? Volume disk encryption ensures peace-of-mind if a laptop goes missing. Laptop location tools are increasing the odds that a stolen laptop could eventually be recovered. If a stolen or lost laptop returns to the corporation after an extended absence, how can an MBAM enterprise ensure that its recovery keys be found?

The purpose of the whitepaper is to:

- Capture unexpected discoveries or observations that the deployment team makes
- Save time diagnosing anticipated problems
- Concisely enumerate the lessons learned and best practices

Executive Summary:

This paper shares observations, lessons and best practices that can improve data consistency and retention for BitLocker recovery keys. For more information about Microsoft BitLocker Administration and Monitoring (MBAM), see the MBAM product documentation at (http://go.microsoft.com/fwlink/?LinkId=218349).

INTRODUCTION

Are you prepared to handle the following scenarios?

After reading this paper, you can be!

- Laptops are off the corporate network for extended periods after encryption, and potentially never reconnect with the MBAM server infrastructure.
- An employee leaves or changes groups, and leaves their computers behind in an encrypted state. Those computers sit idle in storage for a period. The employee is later involved in an incident where their device must be searched.
- A laptop is lost while an employee is traveling. The laptop is reported stolen and the employee is issued a new laptop. Years later, when the lost laptop is returned to the company no one is able to start it because they do not know the PIN.
- Your company's computers carry extremely sensitive data, and your company pledges to exercise "high recovery key discipline". In this scenario, recovery keys are never written down, never stored persistently anywhere but the 'Recovery Key' database. Your company assures that there are never any active copies of a recovery key outside of the database and in the volume's protector structure. Your company relies on MBAM 'Single Use Recovery Key' feature to assure that a key is changed promptly after a recovery event. Each day, the help desk receives a number of calls to release recovery keys to their proper users. Your company practices regular daily backups. One day, the database fails irrecoverably and must be restored from backup. Recovery keys released, since backup, prior to the failure may, on recovery, no longer be marked for reset. What can be done to minimize the possibility of these unchanged keys?
- MBAM stores its data across two databases. Audit records in the 'Status & Compliance' database cover or account for accesses (helpdesk-based retrievals of keys through the portal) to keys in the 'Recovery Key' database. How can we assure high consistency and referential integrity between these two databases in the event of a failure of one database but not the other?
- Suppose an unscrupulous help desk operator released recovery keys for unauthorized use without valid claim. Suppose then, that they sabotaged the 'Status & Compliance' database so that recent audit records would be destroyed. What is to be done?

GUIDELINES FOR CONSISTENT DATABASE RETENTION

As a legally bound entity, your organization is subject to data retention policies for the kinds of data you collect, generate and store. Often this concept applies to on-line or near-line storage, data sets that the company has "on the books". For the data you know about, you legally comply with the requirements around it.

Disk Volume Encryption introduces a high-order accountability/liability, "Retainable Data Recoverability Retention," that applies to the data you may have "written off the books". Your ability to show or accomplish future compliance on past data depends on your policy now around your generations of recovery keys. Your organization must consider the implications that data, once thought lost or destroyed, may reappear long after the fact.

> *BEST PRACTICE: Your organization should have an intentional stance around the longevity and guardianship of BitLocker recovery keys that will outlast the present administration. Your policies around the MBAM 'Recovery Key' database and 'Status & Compliance' database SQL Transparent Data Encryption (TDE) Keys will determine your future administration of past data.*

RULE: An MBAM Key Recovery database must be preserved and archived when an MBAM enterprise deployment or database role is retired or uninstalled.

RULE: When a beta test or evaluation of MBAM completes, the MBAM 'Recovery Key' database for that trial installation must be archived for long term retention. The exception to the rule is when a beta database is updated to a production database through a conversion such that all keys are retained.

RULE: If it becomes necessary to remove or uninstall an MBAM client agent from a computer for any reason, all of its encrypted volumes should be decrypted. Such a computer is undefined for recovery.

An MBAM 'Recovery Key' database must be retained for as many years as the statute-of-limitations that applies to any data potentially on any encrypted volume covered by that deployment.

If an MBAM 'Recovery Key' database is not going to be archived, it is prudent to contact the users of all the computers listed in that database, informing them to decrypt their volumes, since they are no longer recoverable.

An MBAM 'Recovery Key' database must be retained when the deployment is complete if there are any computers that were encrypted under that database that are off-line and unreachable to decrypt them.

LAW OF PESSIMISM: If any computers still in operation, with volumes encrypted originally by MBAM, without their MBAM Agent and without their original MBAM 'Recovery Key' database in either official operation or in officially archived state, then the computers will eventually become unusable due to encryption.

GUIDELINES FOR CONSISTENT KEY DATA SECURITY

The SQL Transparent Data Encryption (TDE) encryption certificate for the MBAM 'Recovery Key' database is the highest-order bit in your hierarchy of enterprise data to be managed and retained. Protect it as you value all your organization's investments combined.

Regularly review and audit the audit history records stored in the MBAM 'Status & Compliance' database. Appoint someone outside of the helpdesk organization to audit the administrative transactions against the MBAM 'Recovery Key' database.

Keep your MBAM 'Recovery Key' database on a separate restricted network subnet.

Keep your MBAM 'Recovery Key' database on a physically separate computer with a restricted set of tenants.

Keep your MBAM 'Recovery Key' database in a physically secure location with restricted access.

Understand the rights and responsibilities of the MBAM data access roles; routinely manage and review access to these roles. Understand the distinction between the MBAM helpdesk portal operator roles of "Tier 1" and "Tier 2". Restrict access to the "Tier 2" role, to only appropriate supervisory personnel.

GUIDELINES FOR CONSISTENT DATABASE BACKUP

SQL TDE encryption certificates should be protected and persisted with the backups of their databases.

The MBAM 'Recovery Key' database must be backed up frequently.

The MBAM 'Status & Compliance' database should be backed up with the 'Recovery Key' database.

Best Practice: Backup images of MBAM databases should be stored as safely and persistently as your organization allows itself to exist. The MBAM 'Recovery Key' database is the most important, more so than your corporate users' data, because the recovery keys lock and unlock access to all of the other user hard drive volumes in your enterprise. If the corporate loses access to its hard drives, then it loses access to its institutional memory.

IMPORTANT: Enterprises using MBAM should use a backup solution that supports the VSS requestor/writer interfaces. Backed up in this fashion, MBAM can assure a higher fidelity coordinated snapshot of the enterprise system. One such product is Microsoft System Center Data Protection Manager.

Although not the preferred method, if a manual backup procedure must be used, it should include the following steps.

1. Stop the MBAM web services on the MBAM web sites and services role (administrative role).
2. Back up the 'Status & Compliance' database (to preserve the audit records)
3. Back up the 'Recovery Key' database
4. Restart the MBAM web services

NOTE: As part of the corporate data retention policy, you should understand the relationship between the TDE certificate protecting the live database, and the copy of the data that is preserved in the backup data image. You should assure that the backup software that you employ creates a backup image that is itself independent from the live database's TDE certificate.

The backup images generated by the back-up process should themselves be protected from theft and unauthorized access.

NOTE: The two MBAM databases should be backed up together. The 'Status & Compliance' database contains audit records that account for releases (accesses through the portal) of the keys in the 'Recovery Key' database.

It is possible though not as desirable, for the 'Recovery Key' database to be restored from backup while the 'Status & Compliance' database is allowed to regenerate from scratch. In this case, it is even more imperative that the recovery keys be 'bulk reset' through the 'Single Use Recovery Key' feature so that the new audit records can be trusted to be complete.

GUIDELINES FOR CONSISTENT DATABASE RESTORE

IMPORTANT: Enterprises using MBAM should restore from backup using a backup-restore-product that supports the VSS requestor/writer interfaces. When restored in this fashion, MBAM can assure a higher fidelity coordinated snapshot of the enterprise system. One such product is Microsoft Data Protection Manager.

Though not the preferred method, if a manual restore procedure must be used, we recommend it be done in the following steps.

1. Stop the MBAM web services on the MBAM web sites and services role (administrative role).
2. Restore the 'Status & Compliance' database on the 'Compliance Database' role node.
3. Restore the 'Recovery Key' database on the 'Recovery Database' role node.
4. Restart the MBAM web services
5. Mitigate inconsistencies stemming from recovery keys affected between the time since the backup was taken and the time the backup was restored (see below).

NOTE: The two MBAM databases should be restored from backup together. The 'Status & Compliance' database contains audit records that account for releases of the keys in the 'Recovery Key' database. If this is not done, then the audit accuracy is suspect.

Closing the Window of Uncertainty

Theory

The period between when the backup was made and when the backup was restored, including all operations therein, is the "window of uncertainty."

To review the problem, a database that is restored will "forget" anything that happened to it (add, modify, delete) during the window of uncertainty. This phenomenon is called database "rollback". Client computers are unaware and unaffected by the "rollback". Because the MBAM 'Recovery Key' database should provide coverage of the encrypted volumes on client computers, there is a discrepancy between the client recovery keys and the database.

The MBAM enterprise consistency invariant is that are at-most two persistent copies of any given recovery key (48 digit unique number) in the universe: one in the 'Recovery Key' database and one in the "protector" of the encrypted volume. Notice we say "persistent", meaning saved on stable storage, since keys may be "in-flight" in memory as well, but that is expected to be transitory in the end.

This invariant is by definition violated by a key-release operation over the key recovery portal (mediated by helpdesk) since the user may not be utilizing the key immediately and must record it in some permanent fashion. The invariant is repaired through the 'Single Use Recovery Key' feature, which marks the key in the database as being "disclosed", thereby causing the client to trigger a key reset sequence at the next opportunity.

Malpractice

After restoration of the 'Recovery Key' database from backup, volume inconsistencies may result:

1. If a helpdesk operator releases keys to callers during the window of uncertainty, the audit records of key release operations will be missing.

- Impact: We cannot be certain that the help desk operator did not release more keys than appropriate.

2. If a help desk operator released a key to a caller during the window of uncertainty, and the given recovery key is used by the caller, the 'Single Use Recovery Key' feature will not reset that key because the flag in the database that marks the key as disclosed will have been "rolled back".

- Impact: We cannot be certain that the MBAM invariant is consistently true.

3. Consider the following sequence of events:

A. If a help desk operator released a key to a caller during the window of uncertainty, and

B. The recovery key is used by the caller, also during the window of uncertainty, and

C. The 'Single Use Recovery Key' feature kicks in to reset the key during the time window, then

D. The user's physical computer will be left unrecoverable (i.e. without a key) after restore, due to database "rollback", until

E. The time interval passes that the client can successfully resend the key, which it does periodically.

F. The MBAM client agent will resend its encrypted volume recovery keys periodically, at least once a day. This will resolve the uncoverage.

- Impact: If a laptop computer were to be taken off the corporate network during the period of uncoverage, it would not regain coverage until it returned to the corporate network.

Remediating Practice

Resynchronize with the Corporate Network

Mobile computers that are off the corporate network will miss opportunities to re-save their recovery keys, and miss directives from the database to activate the 'Single Use Recovery Key' feature (reset their key).

> *BEST PRACTICE: In the event of a database restoration, it would be a thorough practice to notify all computer owners that if they had recovered their computers recently they reconnect them to the corporate network to ensure their keys are resaved properly.*

Forced Disclosure

We recommend that all the keys in the 'Recovery Key' database be marked as "disclosed" after a restoration operation. This will allow the 'Single Use Recovery Key' feature logic to operate across the enterprise and move all the encrypted volumes to their new keys, which are consistently recorded in the database.

In SQL terms, the operation of mass-disclosing is accomplished using the following SQL statement:

```
UPDATE [RecoveryAndHardwareCore].Keys SET Disclosed = 1
```

There will be increased network traffic during this time as the client agents request a reset of their key. It is possible that web services will be unable to accommodate all requests for reset at that time and some fraction of the clients will be forced to retry at their next interval.

CONCLUSION

Your MBAM databases, from each and every MBAM deployment, trial or production, merger or acquisition, in health and in corruption, are part of your organization's institutional memory, and should be treated accordingly, for as long as your institution may exist. Please say, 'I will'.

FOR MORE INFORMATION

For more information about Microsoft products or services, call the Microsoft Sales Information Center at (800) 426-9400. In Canada, call the Microsoft Canada information Centre at (800) 563-9048. Outside the 50 United States and Canada, please contact your local Microsoft subsidiary. To access information through the World Wide Web, go to:

http://www.microsoft.com

http://www.microsoft.com/technet/itshowcase

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.