Microsoft® Desktop Optimization Pack for Software Assurance

MBAM Client Timers

Enterprise System Timers and Timing for Microsoft BitLocker Administration and Monitoring

Technical White Paper

Published: August 2011

By William Lees and Nathan Barnett

Microsoft

CONTENTS

Situation

MDOP MBAM is a loosely coupled enterprise system that is distributed and communicates asynchronously and periodically between components. It is sometimes difficult to tell how long to wait for an expected event.

Solution

A conceptual model for understanding work activities, timing and communication latencies in MBAM system. This helps administrators and troubleshooters predict the best deployment and operations for the MBAM components.

Benefits

- Understand enterprise-wide view of MBAM behavior.
- Set expectations around normal system latencies (i.e. How quickly events happen).
- Provide starting points for troubleshooting when expected behaviors do not occur.

Products & Technologies

- Microsoft Windows Server 2008 R2
- SQL Server 2008 R2
- Microsoft Windows 7 Enterprise
- Microsoft Windows 7 Ultimate
- Microsoft BitLocker Drive Encryption
- Microsoft BitLocker-2-Go

EXECUTIVE SUMMARY

Microsoft Desktop Optimization Pack (MDOP) product Microsoft BitLocker Administration and Monitoring (MBAM) uses a loosely coupled asynchronous design to span enterprises with segmented secure network management infrastructures of arbitrary complexity and scope. MBAM, as a self-contained security management solution, "fits over" existing enterprises by leveraging existing, well-understood technologies of secure repository, reporting, and helpdesk assistance. MBAM provides a BitLocker Drive Encryption safety net for your organization. Being a self-adjusting system, the final end-user concrete timing of value delivery is not known in advance. Fortunately, the MBAM enterprise system derives from a simple set of atomic activities and events that, when understood, allow a conceptual model of timing for MBAM operations. For more information, see MBAM product documentation (http://go.microsoft.com/fwlink/?LinkId=218349).

The purpose of this whitepaper is to:

- Describe rationale for resolving design issues and altering deployment plans
- Provide details to support planning for infrastructure scalability and sizing Save time diagnosing problems
- Arrive at alternate solutions with less trial and error

Use this information to understand system-wide latencies, estimate timing for a given operation, set expectations for when tasks will complete, and decide when to begin troubleshooting, if necessary.

Use this document to estimate Service Level Agreements (SLA) for the timing of MBAM business operations.

INTRODUCTION

This document provides a model for timing in the MBAM enterprise system.

The MBAM system is loosely coupled and asynchronous: system processes and agents are independent and operate in their own times.

MBAM's timing can be described as “wait-less.” No one has to wait because the system just runs itself.

MBAM system is architected as a “system of cycles” to allow:

- The system to expand or “scale” from small to large businesses
- Reduction of time “waiting”, because no part of the system, include its users, have to “wait” for something to happen
- Users to come to the system on their own schedules. MBAM is driven by a participant entering the branch
- The system to perform as a “safety net” that “covers” a business of any size. The MBAM system is designed to be resilient, reliable, dependable, and scalable
- A timing expectation within “reasonable bounds” for MBAM tasks
- Minimized additional work or support cost. As a further benefit, the MBAM system will not impose a significant “degradation” on the pre-existing environment. You need not employ staff to supervise MBAM. The only additional monitoring is to watch for violations of the SLA or excessive delays.

This document helps the enterprise system analyst answer the following questions:

- What are the “meaningful work transactions” that can have an SLA?
- What are the triggers that start a timing period of an SLA?
- What are the “receipt signatures” that mark the delivery or end of a “meaningful work transaction?”
- What are the adjustable timing parameters for MBAM?
- Which underlying IT infrastructures must be operational for MBAM to meet its SLA?
- What are the hand-off points and end-to-end delivery chains required for a “meaningful work transaction” from “start” to “receipt signature? What are the hand-off flow charts for the meaningful work within that flow?

MBAM Enterprise System Diagrams

The following diagrams depict the MBAM System operating at the Enterprise level of scale.

Enterprise System Diagram

MBAM components communicate one-step at a time. Any component may contact related components at any time, as triggered by the sending component. The trigger for initiating contact may be a user request or a timer. Multiple communications between various components occur in parallel, independent of one another.

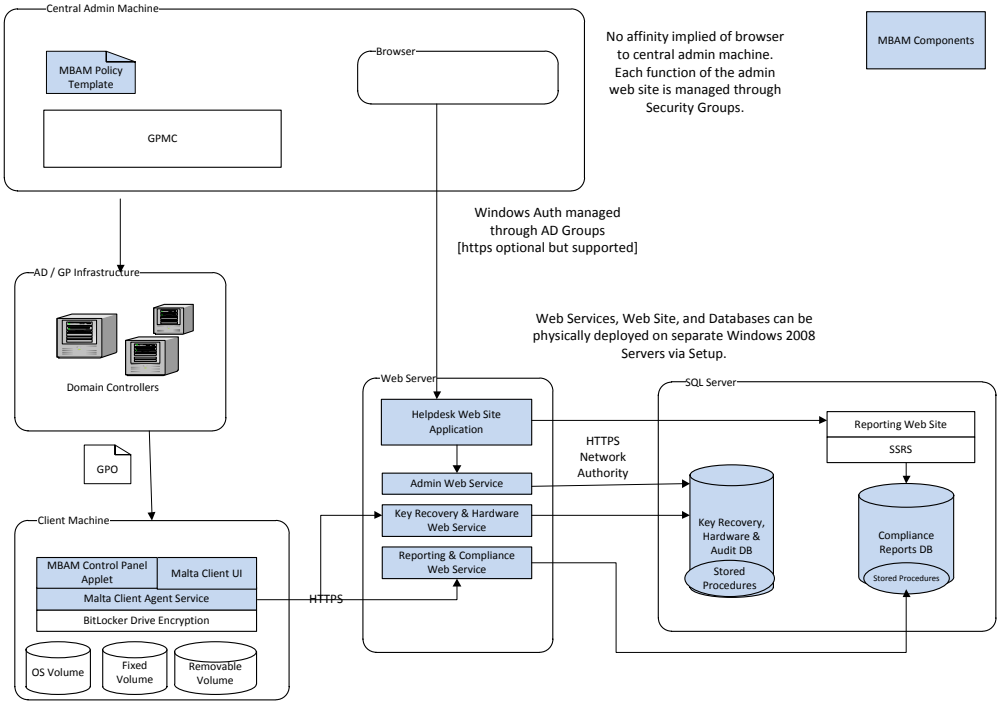


Figure 1. Architecture Diagram

MBAM System Enterprise Component Stack Diagram

The flow of information and the completion of activity happen in this order.

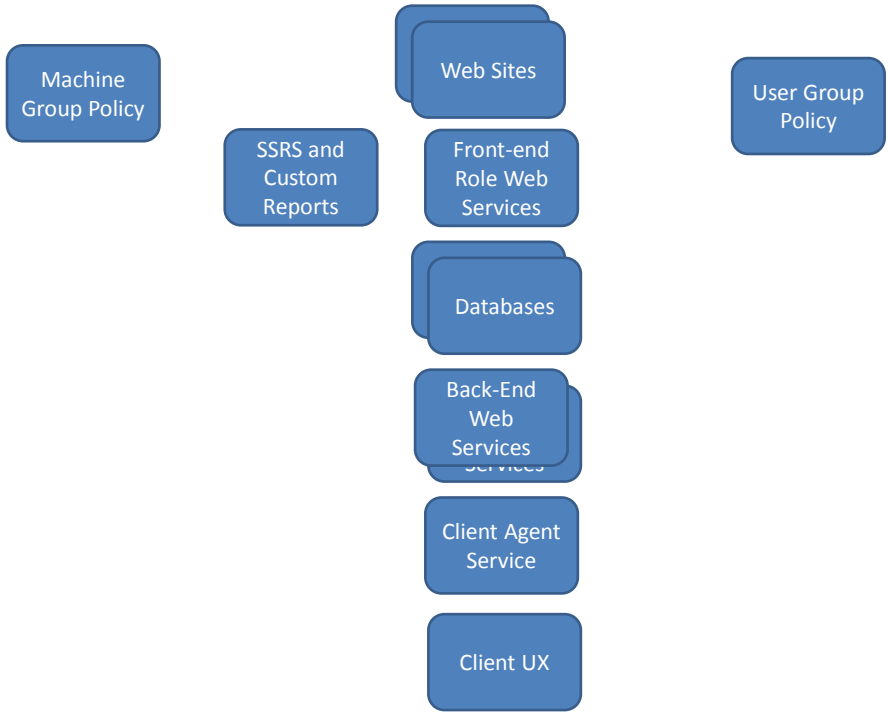
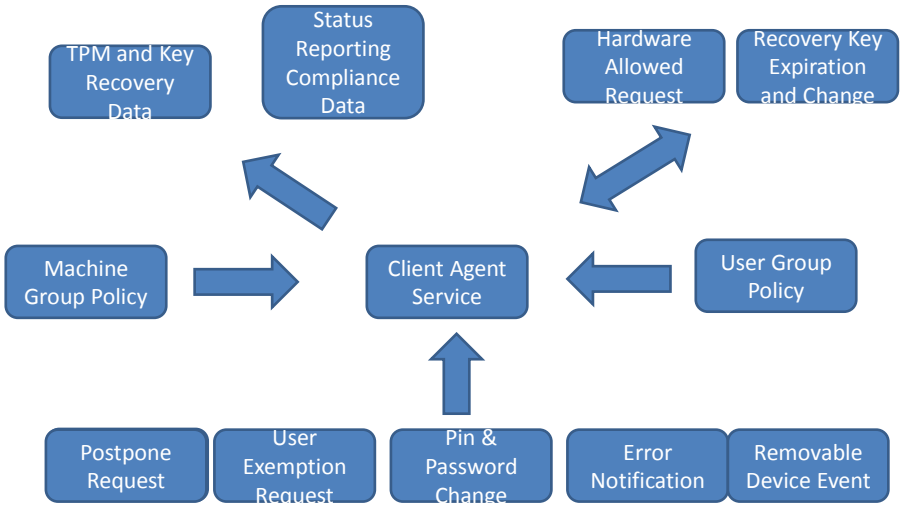


Figure 2. Component Stack Diagram

MBAM Agent Enterprise Services Diagrams

All functions and services provided by MBAM are driven by knowledge obtained by each computer's MBAM client agent. The MBAM client agent is the logical hub for all MBAM activity in relation to a given computer's volumes.



MBAM Enterprise Fault Model

Errors in MBAM are detected at the web service layer, when a web service is unable to complete a request. If an error occurs at the web service layer, then one reason might that the database in question was unable to complete the sub-operation.

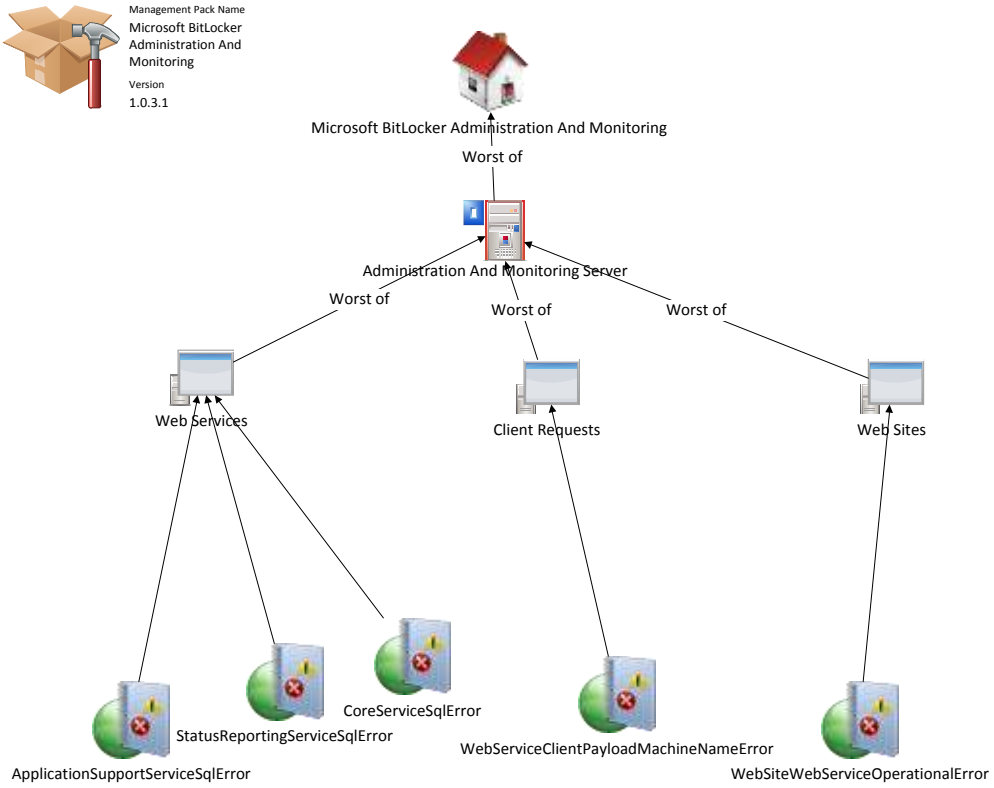


Figure 4. Enterprise Fault Model Diagram

CLIENT AGENT WORK THREADS

MBAM client agents populate and drive MBAM functionality. For more information, see Planning and Configuring Group Policy for MBAM (http://go.microsoft.com/fwlink/?LinkId=217225).

The MBAM client agent is a Windows Service running as System, independent of any users. The client agent schedules its work in activities that run when triggered.

Some client work requires an active user session, for example providing a PIN or initiating a "physical presence" operation that requires that a user is present. In cases where user interaction is required but no session is present, the agent will reschedule until it an active user session is available.

Note: Only a local user is considered an active user session. A non-interactive process or a Terminal Services session is ineligible for MBAM functionality. Lack of an active user is one common reason that the MBAM client agent cannot act.

All MBAM client functionality requires that communication with the MBAM server infrastructure (web services and databases) is working and responsive. The MBAM client agent uses a "heartbeat" operation at the start of tasks that require communication to ensure that the path from the client to the web service to database is responsive. If a client agent task cannot obtain a "heartbeat", then it will reschedule the task for the next interval.

Note: Lack of "heartbeat" causes the MBAM agent to appear nonfunctional. If an MBAM client agent appears nonfunctional, then a communication failure may be the cause.

If the MBAM client agent Windows service is stopped or paused, no MBAM-related processing will be performed. The agent will "catch up" when it starts again. When the MBAM agent schedules a task such as processing policy it reads and acts on the current physical state of the computer. If the MBAM agent "misses" a volume change while work is not scheduled, the task will "pick up" the change at the next interval.

Each MBAM client agent has several distinct worker threads that run on their own timer and event detection.

1. RPC listener thread
2. Volume listener thread
3. Timer Queue
    a. 'Enact Policy' scheduled thread
    b. 'Send Status Data' scheduled thread

RPC Listener Thread

This thread handles user-initiated requests from the active user session.

Any program running in local user context may request one of the MBAM client agent operations.

Note: As part of the MBAM client agent security threat model any active user session user can request these operations. In addition, any Windows program can call these local end-points and be extensions of the MBAM client user interface.

If a user can logon locally to the computer, that logon is sufficient claim to allow a restricted set of volume encryption operations. It is outside the scope of MBAM to determine which users are allowed to logon to the computer.

Note: A request to change a PIN or passphrase does not require the caller to supply the previous PIN or passphrase value. Any active user (locally logged on) may re-protect the volumes as they choose.

In the case of dueling users who consecutively change the PIN, the last writer wins. In a worst case scenario where one valid user “locks out” another valid user by changing the PIN, the denied user can appeal to helpdesk. Helpdesk can verify the user and provide the recovery key.

The following are user-requested BitLocker-related operations:

- Is TPM Ready
- Take Ownership of TPM
- Notify of Volume Error to Server
- Notify of Machine Error to Server
- Set TPM State (activation)
- Get Action To Set TPM State (activation)
- Get PhysicalPresenceResponse
- Get Encryption Percentage
- Get User Protector
- Protect Key With TPM
- Protect Key With TPM and Startup Key
- Protect Key With TPM and PIN and Startup Key
- Protect Key With TPM and PIN
- Protect Key With Passphrase
- Protect Key With External Key
- Change PIN
- Change Passphrase
- Notify of User Exemption
- Unlock with Passphrase
- Unlock with Numerical Password
- Get Numerical Password Protector Ids
- Get Lock Status

Any user program may attempt any of these requests at any time. In the case of the control panel applet, the user starts the control panel when they choose. In the case of the Client Wizard user interface, the client agent service starts itself in the user context when the service needs input.

Note: At present, the set of user programs that are started by the client agent cannot be extended or changed.

Volume Listener Thread

The volume listener thread performs work on behalf of removable devices.

The volume listener thread watches for removable devices being added or removed. The volume listener thread enumerates removable devices that are already inserted when it starts for the first time in order to catch any devices added since the last shutdown.

The volume listener thread is only interested in removable-class devices that are already encrypted. Unencrypted devices are not tracked by this operation.

The set of "in progress" removable devices is tracked in the "Active Device List". Entries are added and removed as devices are inserted or ejected. The active device list serves as a "retry queue" for devices discovered but not reported to the MBAM server.

Discovered devices are added to the active device list and become subject to "retry behavior." The retry-until-unlocked task attempts to read the device and send its recovery key to the server according to these parameters:

Initial Delay = 30 seconds

Periodic Retry = 15 seconds

Retry may be necessary because the device is not accessible until it the user supplies the passphrase to unlock it.

The retry attempts continue until a clear success or error state is received. There is no retry limit. The retry behavior stops if a serious error occurs or the device is removed.

Note: Lack of "heartbeat" is not a "retry" condition. If the server infrastructure is unavailable when the device is inserted and unlocked, the attempt stops. Ejecting and inserting the device will cause another round of attempts to save the recovery key.

Note: Removable device may be encrypted without guaranteeing that its recovery key is escrowed in the database. MBAM does not enforce recovery-key-saving at encryption-time for removable devices. A removable device may have been encrypted prior to MBAM installation. MBAM makes a best effort to "uncover" the recovery key of a removable device afterwards.

Enact Policy Thread

The "enact policy" scheduled thread includes the following steps:

1. Processing for the operating system drive:
    a. Only occurs if the "Should Encrypt operating system drive" policy is enabled
    b. Checks that a "system volume" is present. A system volume is a dedicated partition on the drive that contains the boot files. This configuration is standard in Windows 7 but may not be in place for computers installed with earlier editions of Windows.
    c. The policy for the operating system drive protector determines the kind of protector applied.
    d. If the protector applied requires the TPM, then the TPM must be present.

2. If the current user is subject to a “user exemption” policy, then no further work is performed.
3. If the current computer type is subject to a “hardware exemption”, then no further work is performed
4. Pre-processing for the operating system drive occurs.
    a. Determine whether the work requires a user interaction
    b. If the work does not require user interaction, perform the “non-interactive” work
        i. If Drive is to be encrypted
            1. Reset the recovery key if needed
            2. Add numeric password protector
            3. Send recovery data
        ii. If Drive is to be decrypted
            1. Clear all auto unlock keys
            2. Decrypt the drive
5. Pre-processing for the fixed drive occurs
    a. Determine whether the work requires a user interaction
    b. If the work does not require user interaction, then perform the “non-interactive” work
        i. The policies for “should encrypt fixed data drive” and “use passphrase for fixed data drive” must be true; if not, the no work is performed
        ii. For each fixed drive
        iii. If drive should be encrypted (policy enabled)
            1. If policy “should auto unlock fixed data drive” is enabled, then set auto unlock, else “unset” auto unlock
            2. Reset recovery key if needed
        iv. If drive should be decrypted (policy disabled)
            1. “unset” auto unlock
            2. decrypt
6. If there is work remaining which requires user interaction
    a. Obtain the “heartbeat” to the key recovery web service and key recovery database
    b. If there is no heartbeat, then no further work is performed
    c. Determine whether an active user session is present
    d. If an active user session is not present, no further work is performed

e. If an active user session is present, then the service starts the “Client UI Wizard” program in user-context.

7. At this point, the scheduled part of this task’s work is complete and the activity concludes until the next interval.
    a. However, the user-program that was started will interact with the user and “call back” into the client agent service to drive the subsequent user-based activities.
    b. Common RPC requests called by the Client UI Wizard are the “TPM series” and the “Protect Key” series.

Send Status Data Thread

The following steps occur when the “send status data” scheduled thread runs.

1. If the “use reporting service” policy is disabled, then processing stops
2. Create (collect) compliance data
    a. Collect data for operating system drive
    b. Collect data for fixed drives
3. Generate data payload
4. Send status data
    a. Determine the reporting service endpoint from policy
    b. Determine whether secure communication is required by policy
        i. Either send by HTTP
        ii. Or Send by HTTPS

Note: it is by design that compliance data for removable drives is not reported to the server infrastructure by this task. This is because all removable drives are not always inserted consistently; having no results for this class of drive was deemed better than having incomplete results. Inferences about the currency of some removable drives could theoretically be made by examining the time of last key escrow in the key recovery database.

ENTERPRISE SYSTEM END-TO-END PATH ANALYSIS

Understanding Key Recovery Escrow, Path of Agent to Database

This section explains the steps that are followed in a recovery key escrow situation.

Recovery key related activities only occur after the trigger of an active user session.

The agent policy 'ClientWakeupFrequency' controls how frequently the MBAM agent service will perform its periodic tasks.

After system boot, the MBAM System Agent delays for a random period before beginning its first work period. The policy setting 'NoStartupDelay', when present, indicates that the MBAM system agent should begin its work immediately and not be subject to the random delay.

The MBAM system agent can only save the recovery key when the volume is accessible. Each encrypted volume must be in the unlocked state in order for MBAM system agent to be able to read the current recovery key and send it to the MBAM server database.

Removable drive volumes are only processed in the context of an active user session.

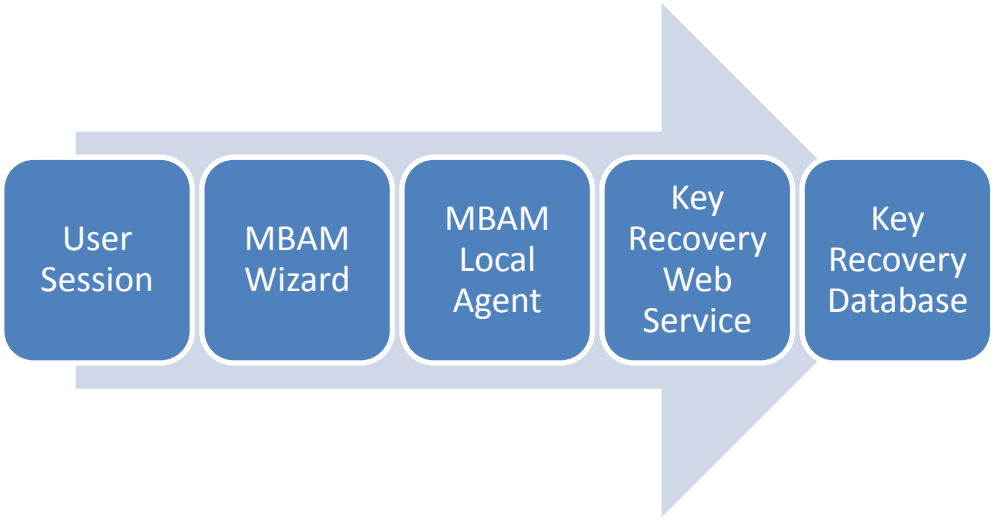


Figure 5. Volume Recovery Key Escrow Path Diagram

Understanding Compliance Status, Path of Agent to Database to Reports

This section explains the steps that are followed in a compliance status-reporting situation.

Status compliance data is reported periodically in the background of the MBAM service.

The agent policy 'StatusReportingFrequency' controls how frequently the MBAM agent service will perform its periodic compliance-status reporting tasks.

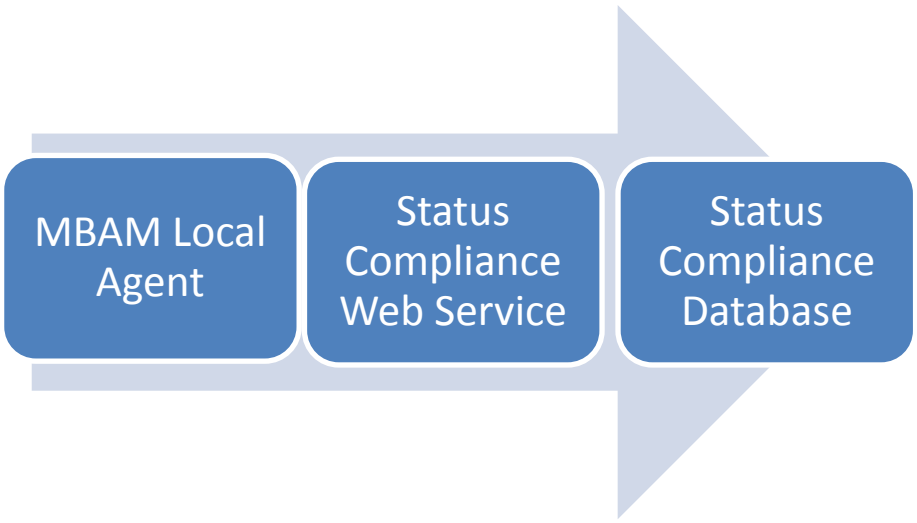


Figure 6. Status Compliance Reporting Data Path Diagram

Periodically, the report cache pulls data up from the status compliance database.

An active user at the report portal pulls up the report, with data coming either from the report cache, or from the live status-compliance database.

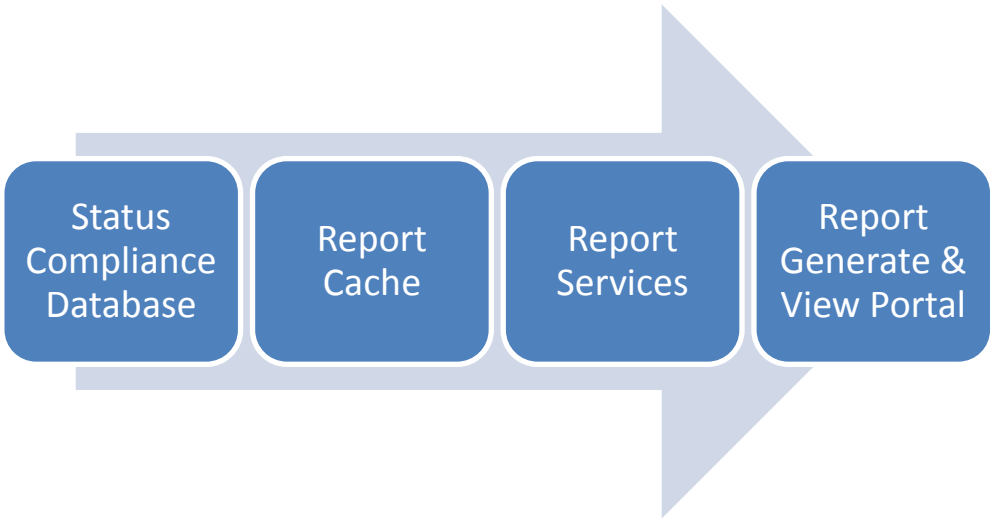


Figure 7. Report Content Generation Data Path Diagram

Understanding User Requests Helpdesk to Release Recovery Key

This section explains the steps that are followed in a helpdesk recovery key release situation.

In order for there to be a current recovery key in the recovery key database to be released, a recovery key escrow call sequence needs to have occurred recently. The recovery key database is populated in the service's background, independent of calls to the recovery portal to retrieve the keys.

Release of a recovery key is based on the current recovery key database's contents at the time that the recovery key portal attempts to retrieve the key.

It is permitted that a release of recovery key operation through the recovery key portal can occur while a single-user recovery key change 4-step transaction is in progress. The recovery key release mechanism is designed so that the recovery key(s) released at any given point are valid and useable at the user computer. Note that more than one recovery key may be released to a single user calling helpdesk in some cases.

Release of a recovery key is a situation that calls for a single-use recovery key change transition.

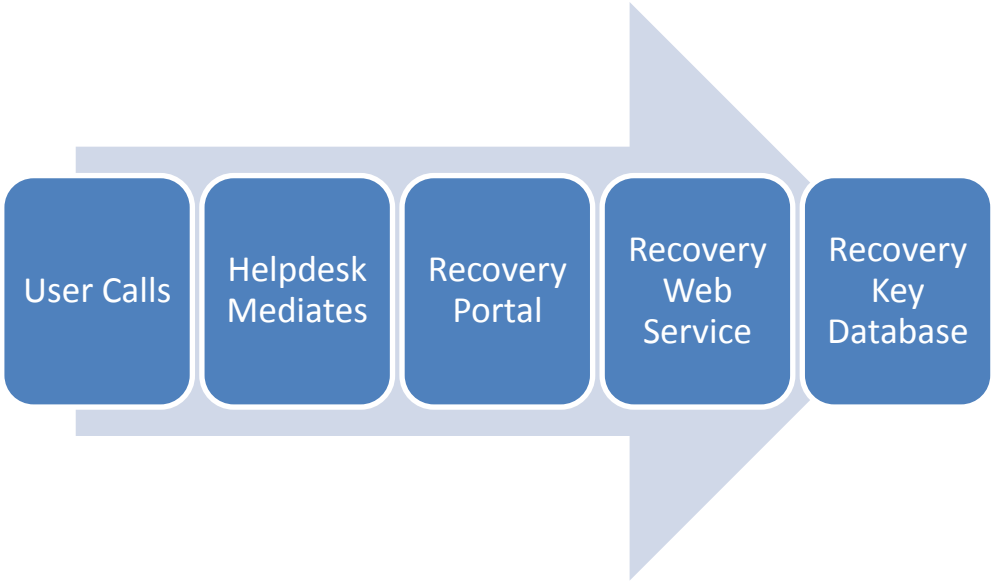


Figure 8. User-Helpdesk Recovery Key Retrieval Data Path Diagram

Understanding Single-Use Recovery Key Multi-Step Transaction, Path of Agent to Database

This section explains the steps that are followed in a single-user recovery key change situation.

The agent policy 'ClientWakeupFrequency' controls how frequently the MBAM agent service will perform its periodic tasks.

There are situations where the recovery key needs to be changed.

The presence of the active user session triggers the recovery key change logic, in the situations where the recovery key needs to be changed.

The volume for which the recovery key will be changed, that volume must be in the unlocked state in order for the MBAM system agent to be able to read and write the recovery key which is stored as one of the volume's protector entries.

Removable drive volumes are only processed in the context of an active user session.

The recovery key change is done and visible when the 4-step change transaction logic is complete. Any given agent may remain at one of the intermediate steps for a period of time if

it is blocked from completing that step due to intermittent failure. The agent remains at its current step across reboots and across user session changes.

If a recovery key change transaction is already in progress, the next attempt simply re-tries the whole transaction over again from step 1. Should this transaction also become blocked part way through the 4-step process, the agent remains at its current step until the next attempt.

If an agent is temporarily blocked in the middle of completing the 4-step transaction, one of the visible side effects is that there may temporarily be more than one recovery key actively associated with the volume. During this time, a user-helpdesk recovery procedure may include or involve more than one recovery key for a given user-volume at a time of request.

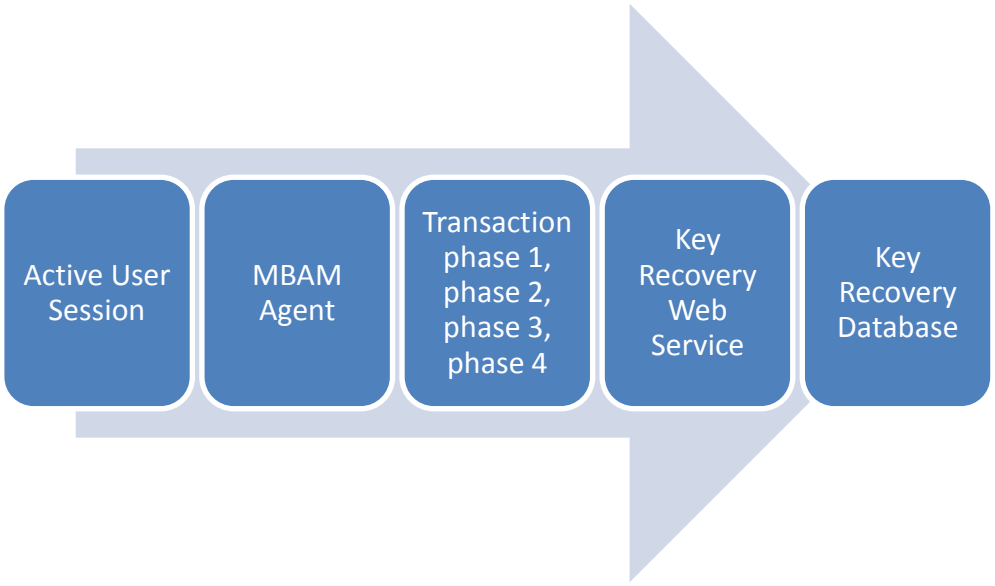


Figure 9. Agent Recovery Key Reset Data Path Diagram

Understanding MBAM System Hardware Exemption Exclusion

This section explains the steps that are followed in a client hardware exemption situation.

The MBAM agent contacts the server at each processing period to determine whether the current computer should be exempted from processing of MBAM policy due to hardware-based exclusion.

While the MBAM system agent is determined to be subject to hardware-based exclusion, it reschedules itself at a different rate than the customary 'ClientWakeupFrequency'.

The current accumulated amount of time that has accrued during the hardware exemption delay period is tracked by the MBAM system agent in the system registry using the 'HWExemptionTimer'.

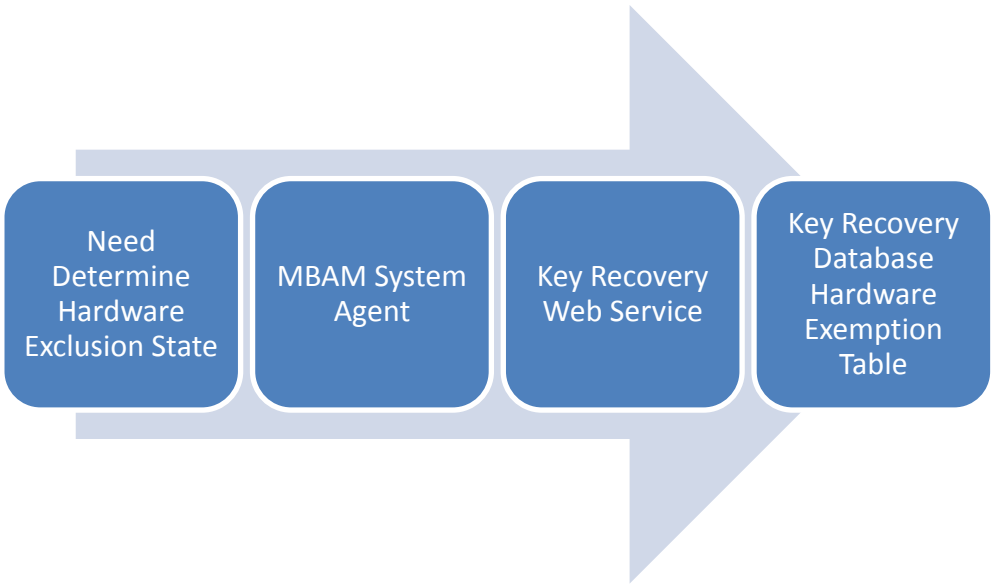


Figure 10. Agent Checks Local Hardware for Exclusion Data Path Diagram

Understanding MBAM System User Exemption Grace-Period

This section explains the steps that are followed in a user-exemption grace-period situation.

During an active user session, when the MBAM Wizard is presented on the screen for the first time, the user has the option of selecting the 'Request Exemption' operation. When this option is selected, the user is instructed on the means that their enterprise wants them to use to request the exemption.

It is outside the scope of MBAM how the user employs this means. The result, if successfully exempted, is that a user-based policy is set for this user.

When this option is selected, the MBAM system agent enters a timing period called the 'user exemption grace-period'. During this time interval, the MBAM System Agent will exclude itself from processing policy.

The policy setting 'AllowUserExemption' controls whether the MBAM Wizard offers the option of 'Request Exemption'.

The policy setting 'MaxTimeToGetUserExemption' controls the total allowed time interval for the 'grace-period'.

The 'grace-period' ends either when the total allowed elapsed time has occurred, or when a policy setting arrives (is present) that directs the agent explicitly to be included or excluded on this computer.

The current accumulated amount of time that has accrued during the grace period is tracked by the MBAM system agent in the system registry using the 'UserExemptionTimer'.

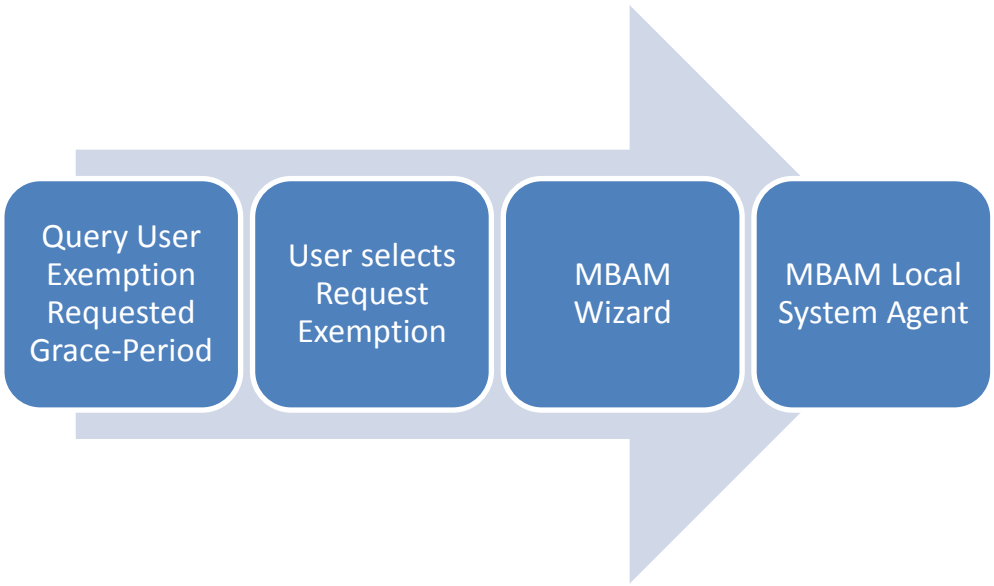


Figure 11. User Wizard Request Exclusion to Agent Data Path Diagram

Understanding MBAM System User Exemption Exclusion

This section explains the steps that are followed in a user exemption situation.

There is a dynamic per-user policy setting which explicitly indicates whether the user is subject to MBAM system agent policy processing on the given computer. When the MBAM system agent begins a work period, the agent is subject to a policy setting arrives (is present) that directs the agent explicitly to be included or excluded on this computer. When the MBAM system agent detects that it is explicitly excluded from processing policy, it defers execution of the current work.

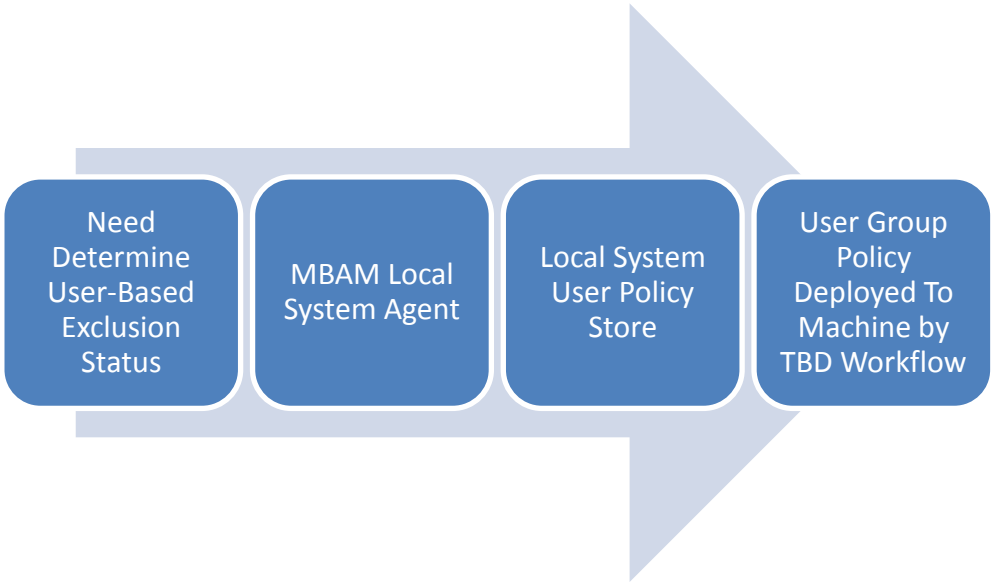


Figure 12. Determine User Exclusion Data Path Diagram

Understanding What Appears On MBAM Wizard Initial Screen

This section explains the logic that used to determine the initial screen in a MBAM Wizard situation.

The MBAM Wizard appears under the following conditions:

1. There is an active user session present
2. The MBAM system agent work period arises, that is the MBAM system agent periodic run happens to coincide with the user session.
3. The MBAM system agent policy processing logic determines that there is configuration change work that is needed. This is done by differencing the present policy settings that the computer is subject to, and the present encryption states of all the volumes presently visible (inserted, attached) to the computer.
4. That configuration change work is of the kind that requires a live, present user to interact to provide the needed live user data. Such data includes the providing the PIN and Passphrase for volumes.

The initial screen shown by the MBAM Wizard, in the presence of an active user session, depends on the state of the computer.

The state 'TpmInitializationState' is a record of whether this computer has under-gone a TPM Initialization Sequence operation, and if so, the subsequent success or failure of the attempt.

The state 'UserStartedProcess' is a record of whether this is the first time any user has interacted with the MBAM Wizard at all, or whether this is a subsequent showing of the MBAM Wizard to any user.

Understanding MBAM System Agent Removable Drive Processing

This section explains the steps that are followed in order to process a removable drive volume.

Removable drives are only processed in the context of the active user session.

The MBAM system agent regards all removable drives equally, regardless of which computer they were first encrypted.

Removable drives are not subject to the enforcement of policy. MBAM system agent does not cause the encryption of removable devices itself. Rather it simply depends on the existing Windows BitLocker policies present to perform that enforcement.

When the MBAM system agent runs for the first time, it enumerates any removable drives attached to the system, and attempts to escrow their recovery keys to the server.

At the time of removable drive insertion, the MBAM system agent watches the drive and waits for the drive to become available in an unlocked state. When a recently inserted removable drive becomes unlocked, the MBAM system agent will attempt to escrow its recovery key.

During the periodic interval when compliance status data is collected and reported, the state of removable drive policy is reported.

Understanding the Significance of the Active User Session

This section explains how the MBAM system agent behaves differently when there is an active user session and when there is not an active user session.

Note: An active user session is present when a user is logged on at the local, physical keyboard and screen. Non-interactive jobs and Terminal Server sessions do not apply.

Removable drives are only processed in the context of an active user session.

An active user session is needed in order to collect the “current user” when saving a removable drive recovery key.

An active user session is needed in situations when the MBAM Wizard must be displayed. When the computer’s policy is established initially or subsequently changed, if the policy requires interacting with the current user to gather information, then the MBAM Wizard must appear. If the MBAM system agent’s work period occurs at a time when there is no active user session, then if there is policy work requiring user interaction, then that work is deferred until the next work period.

User exemption policy is only processed in the context of the active user session.

SERVER REPORTING CACHING BEHAVIOR

There are two stories for the reports timings.

There is the case (1) for reports other than the enterprise compliance report, and there is the case (2) for the enterprise compliance report itself.

Most of the other reports are run directly off the database, so as soon as the information is in there they are up to date.

The enterprise compliance report is the only report that has a special set of timings. The enterprise report is run off a cached table for performance reasons, which is by default updated at 1am, 7am, 1pm and 7pm. The cache is populated by a SQL job, so if this timing is too often or not often enough it can be changed.

To change how often the job is run, open the SQL job named “CreateCache” and edit the schedule to your liking. If you need to do a one-time update you can also directly run the job from SQL management studio and that will update the cache.

Please note that this is not the standard caching that SQL server reporting services offers. If you would like to use the caching and snapshotting mechanisms provided by SQL server reporting services you are free to do so, it will not affect the caching that MBAM does. However if you do proceed with this make sure you keep the external cache in mind.

CONCLUSION

MDOP MBAM is a turnkey secure volume key management solution that is designed for extensibility and flexibility over a wide variety of real-world enterprise configurations. MDOP MBAM is designed to be simple and modular and self-contained so that it may be completely understood and verified based on physical facts and properties of the existing environment that it over-sees.

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.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

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.

© 2011 Microsoft Corporation. All rights reserved.

BitLocker, Microsoft, SQL Database Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.