

ABSOLUTE AND MICROSOFT BITLOCKER

MAINTAINING ENCRYPTION HEALTH WITH ABSOLUTE

TECHNOTE

THE CHALLENGES WITH MANAGING ENCRYPTION SOFTWARE

Encryption is a critical security control measure for organizations to protect against unauthorized access to sensitive data. Many industry-specific and country/continent regulations require organizations to encrypt data, and more importantly prove that data encryption is healthy and functioning at the time of a security incident. This ability to prove encryption, and that data was not accessed post-incident, can save organizations from having to issue a data breach notification, mitigating both reputational and financial damage.

While there are many variations of encryption solutions available, ranging from full-disk, to file and folder based and even self-encrypting drives, one of the more widely deployed solutions is Microsoft® BitLocker, a full-disk encryption product available with Windows.

WHAT IS BITLOCKER?

BitLocker Drive Encryption allows a user or administrator to encrypt all data stored on the Windows operating system volume and configured data volumes. BitLocker is supported on the following versions of Windows:

- Ultimate and Enterprise editions of Windows 7
- Pro and Enterprise editions of Windows 8 and 8.1
- Pro, Enterprise and Education versions of Windows 10
- Windows Server 2008 and later

BitLocker provides the most protection when used with a Trusted Platform Module (TPM). The TPM is a hardware component installed in devices by manufacturers. The TPM works with BitLocker to help protect user data by ensuring that the system components have not been tampered with and that the encrypted drive is located in the original computer.

MAINTAINING BITLOCKER HEALTH

While Encryption is a good data security practice and an important component of a defense-in-depth strategy, encryption can only protect data when the solution is properly configured and functional. However, there are many variables and circumstances that can cause BitLocker to be misconfigured, preventing the data from being encrypted and, as a result, creating security vulnerabilities. This ranges from Windows Management Instrumentation (WMI) files not functioning, system partitions being tampered with or absent, BitLocker Management Client Services inactive, or service URLs misconfigured or removed. These events could simply be the result of degradation over the lifetime of the device, or a malicious user attempting to bypass security measures to access sensitive data.

Regardless of the circumstances, Absolute viewed this as an opportunity to leverage the patented self-healing capabilities Absolute Persistence® provides, and to extend Absolute's Application Persistence functionality to automatically remediate critical Microsoft BitLocker components, and as a result of these self-healing capabilities, ensure encryption is active and data is protected.

MAINTAINING BITLOCKER COMPLIANCE

The August 2017 release of Absolute 7 introduced the capability to report on the status of BitLocker, and when necessary automatically remediate non-compliant configurations. Absolute does not encrypt or re-encrypt any files. However, by remediating critical BitLocker components, this can help ensure data is protected. Additionally, users can also configure

the reinstall of the Microsoft BitLocker Administration and Monitoring (or MBAM) client on endpoints where the client is not compliant.

To report on the status of BitLocker, repair when necessary and reinstall the MBAM client, a device policy needs to be configured and activated from within the Absolute console. A policy can then be applied to a group of devices, or all devices. This flexibility allows you to target specific devices in your population that may be compatible or require BitLocker encryption. If this policy is applied to a Global Policy Group, it will be activated across all devices.

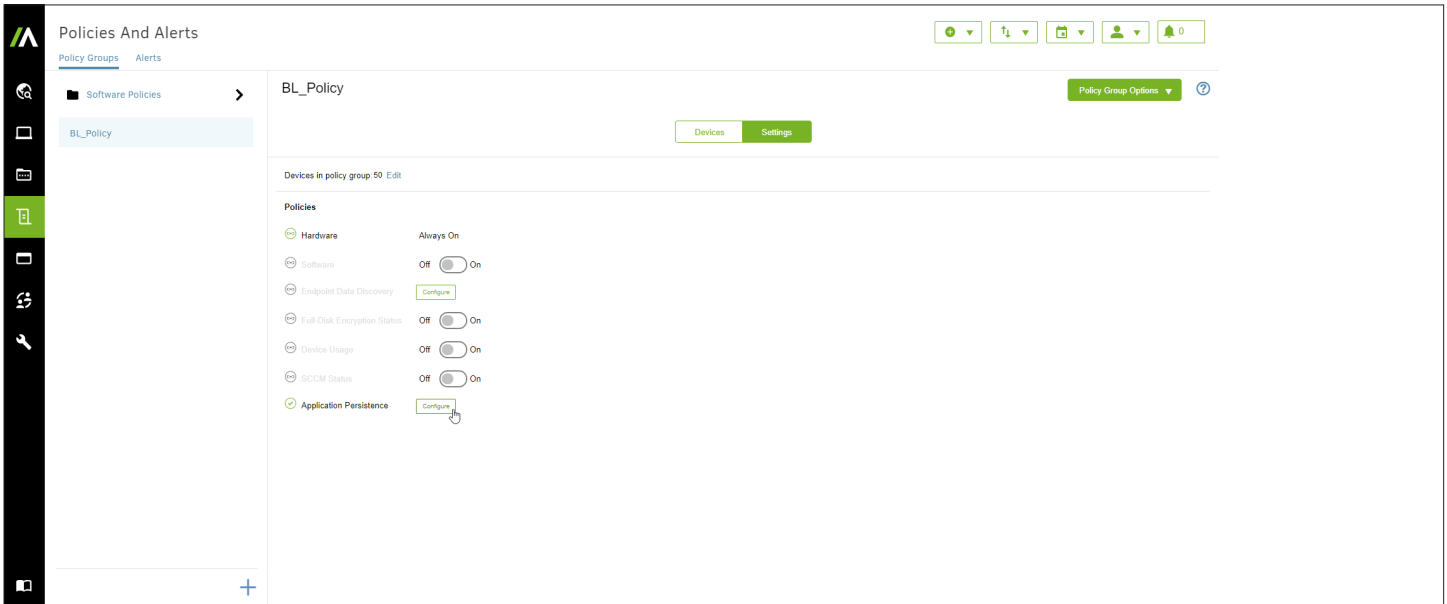


Figure 1: Configuring a Policy Group

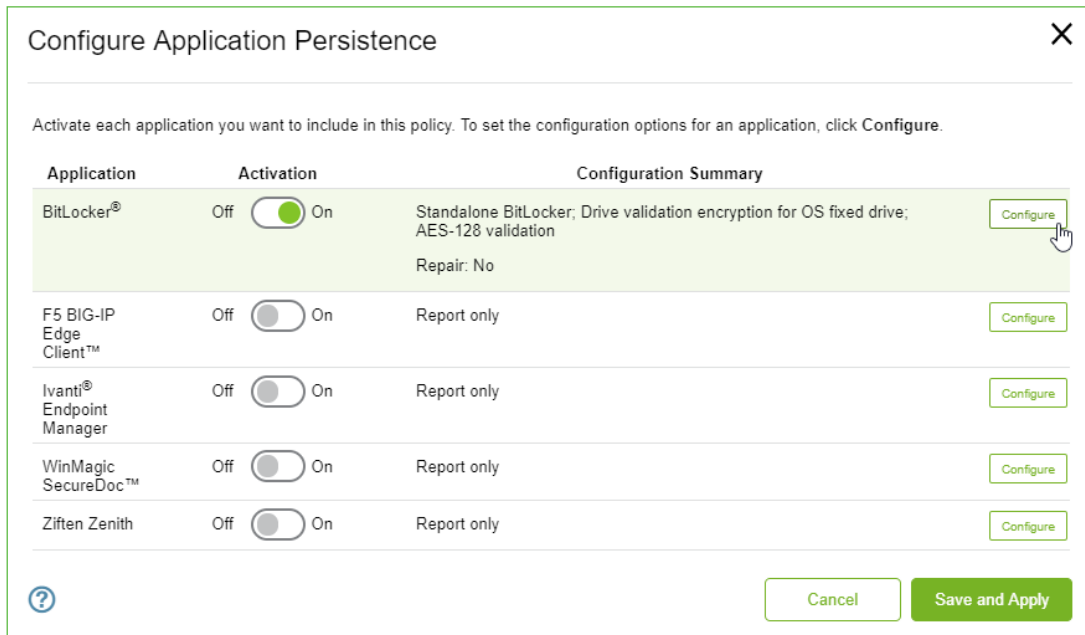


Figure 2: Activating BitLocker application repair

Reporting capabilities will identify compliance if BitLocker is installed, functional and configured as expected. The option to specify what 'compliant' is in your environment is based on the following configuration settings.

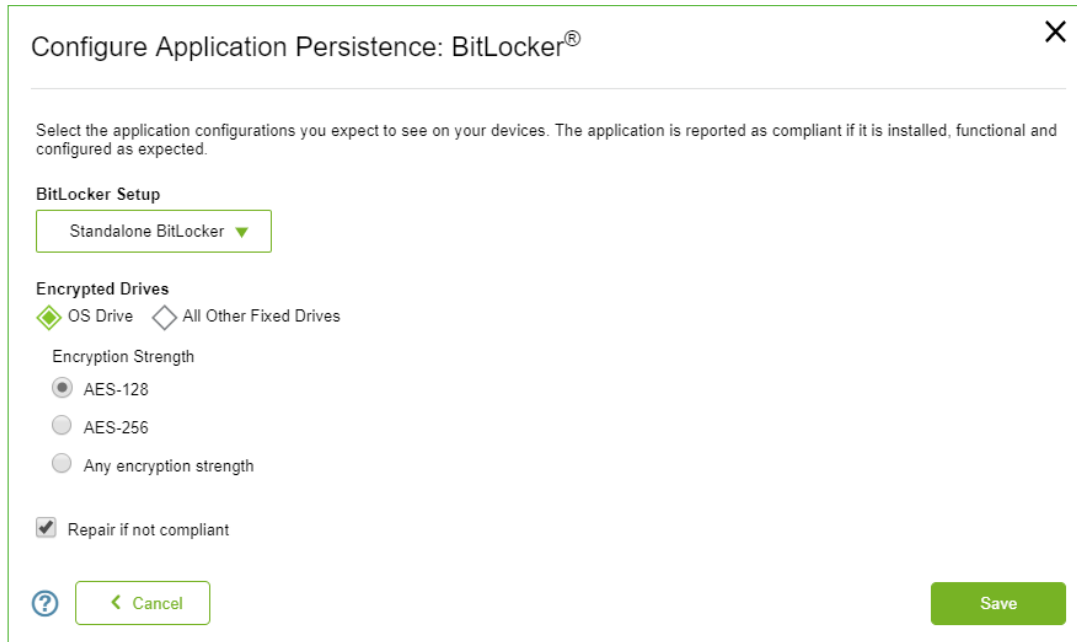


Figure 3: Defining BitLocker compliance based on configuration settings

BITLOCKER DEPLOYMENT MODELS

Most organizations will manage their BitLocker deployment using one of the three following methods.

1. **BitLocker 'Standalone'**: Does not rely on an application to manage BitLocker encryption of drives. Before BitLocker encrypts a drive, it generates a 48-digit recovery key that must be stored or printed. The recovery key is required if a system lockout occurs. Absolute's application repair functionality does not encrypt unencrypted drives, it simply reports on the status of BitLocker in this deployment model, and when necessary will initiate the repair workflow. Enterprises do not usually use BitLocker in a standalone mode.
2. **Microsoft BitLocker Administration and Monitoring (MBAM)**: MBAM provides enterprise management capabilities for BitLocker, including BitLocker deployment and key recovery, and centralized policy configuration. An MBAM client runs on the designated endpoint and communicates with an MBAM server. Absolute's BitLocker application repair capabilities acts on maintaining the 'health' of the MBAM client only and does not interfere with the policies managed by MBAM.
3. **System Center Configuration Manager (SCCM) maintained MBAM**: in this category the SCCM agent maintains the MBAM agent, which in turn enforces the enterprise's BitLocker policies. Absolute addresses this scenario through our SCCM application repair capabilities, which would repair the SCCM agent, which then reconfigures BitLocker.

NOTE: BitLocker To Go is a removable drive encryption solution, used for encrypting removable media USB drives. BitLocker To Go is not supported by Absolute's BitLocker application repair solution.

ENCRYPTED DRIVE REPORTING

As an enterprise may have thousands of Windows PCs with many different drive configurations, MBAM assists by categorizing drives into two categories:

- Operating System drive: the drive containing the Windows operating system and user data.
- Fixed drives: the other hard drives in the PC

With Absolute's BitLocker reporting capabilities, organizations can choose to report on the status of only the Operating System Drive, Fixed Drives, or both.

REPORTING ON REQUIRED ENCRYPTION STRENGTH

BitLocker support two levels of cipher strength: 128-bit and 256-bit. Both use the Advanced Encryption Standard (AES) to perform encryption. Longer encryption keys provide an enhanced level of security. Absolute's BitLocker Reporting functionality allows the administrator to report on the status of both AES-128 or AES-256 encryption, critical to understand if devices meet the necessary compliance requirements, which may vary by organization or regulatory bodies.

MICROSOFT BITLOCKER ADMINISTRATION AND MONITORING (MBAM) SERVICE URLS:

MBAM requires both a Key Recovery Service Endpoint URL and a Status Reporting Service URL. These are locations the BitLocker client reports to, with <servername> and <port> configured based on your own environment.

By default, the URL for **KEYRECOVERYSERVICEENDPOINT** (MBAM Recovery and Hardware service endpoint) is in the following format, <http://<servername>:<port>/MBAMRecoveryAndHardwareService/CoreService.svc>. This URL is used to maintain communications with the MBAM server, storing recovery keys.

By default, the URL for **STATUSREPORTINGSERVICEENDPOINT** (MBAM Status reporting service endpoint) is in the following format: <http://<servername>:<port>/MBAMComplianceStatusService/StatusReportingService.svc>. This URL is used to maintain communications with the MBAM server, reporting the status of the BitLocker encryption client.

Administrators can validate the URL as part of the configuration process to ensure they are communicating correctly. These URLs are important for MBAM reporting and management purposes, and are used to ensure successful communications to the MBAM server, which include transmitting its status and recovery keys as needed.

These URLs are configured in the BitLocker application repair policy in Absolute. If a URL is changed either unintentionally or maliciously on a device, Absolute's BitLocker Application Persistence capabilities will repair these to the correct URLs as specified in the configuration settings.

Configure Application Persistence: BitLocker®

Select the application configurations you expect to see on your devices. The application is reported as compliant if it is installed, functional and configured as expected.

BitLocker Setup

BitLocker with standalone MBAM ▼

Encrypted Drives

OS Drive All Other Fixed Drives

Encryption Strength

AES-128

AES-256

Any encryption strength

Location of the MBAM Recovery and Hardware service endpoint

URL

Required

Validate URL

Format: <protocol>://<hostname>:<port>/MBAMRecoveryAndHardwareService/CoreService.svc

Location of the MBAM Status reporting service endpoint

URL

Required

Validate URL

Format: <protocol>://<hostname>:<port>/MBAMComplianceStatusService/StatusReportingService.svc

Repair if not compliant

? < Cancel Save

Figure 4: Configuring BitLocker compliance when setup with MBAM

ACTIVATING BITLOCKER REPORTING

COMPATIBILITY:

BitLocker status reporting is applicable for customers with the following Operating Systems:

- Windows Vista and Windows 7, Ultimate and Enterprise editions
- Windows 8 and 8.1, Pro and Enterprise editions
- Windows 10, Pro, Enterprise and Education versions
- Windows Server 2008 and later

AVAILABILITY:

BitLocker Reporting is available with Absolute Resilience. Legacy Absolute Computrace and DDS Premium customers with Computrace Data Protect, Computrace Plus, Computrace Complete or Computrace One licenses will also receive BitLocker reporting functionality. Absolute Visibility and Control customers can also purchase the Application Persistence for Microsoft Applications add-on module.

ACTIVATION:

Existing Absolute customers can activate this feature within the cloud-based Absolute console, based on policies. This feature can be turned on for specified groups of devices, or for all devices.

Administrators can specify their compliance requirements in the 'Configuration Application Persistence: BitLocker' screen, as shown in Figure 3.

IMPLEMENTATION:

When the BitLocker status reporting feature is configured and activated via Policy Groups, the Absolute agent detects the status of the BitLocker client by running a script on the device. This script performs a series of health checks to determine if the required services are present and functioning correctly. The script runs on a schedule outside of regular Absolute agent communication. The scheduled period for BitLocker status checks is every 6 hours. If the BitLocker options are changed on the server (e.g. configuration changed), the BitLocker reporting script is run immediately when it is received by the agent. No user input or changes to an organization's existing BitLocker environment are required.

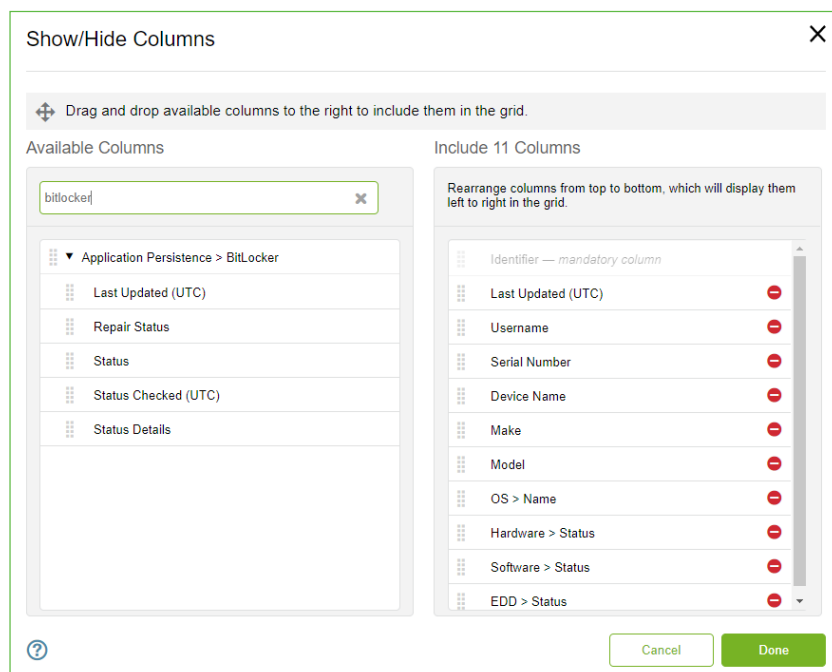


Figure 5: Adding BitLocker attributes to an Absolute report

Once activated, to add BitLocker attributes to a new or existing Absolute report, simply click on Show/Hide Columns, and search for BitLocker attributes as indicated in Figure 4. These can be added to any predefined or custom report, and then saved for future reference.

The following attributes are available to be reported on:

- **APPLICATION PERSISTENCE › BITLOCKER › LAST UPDATED (UTC):** The date and time the results of the BitLocker status check were made available in the Absolute console
- **APPLICATION PERSISTENCE › BITLOCKER › REPAIR STATUS:** The status of any attempted BitLocker repairs. Note Repair Status may not show if the account does not have the correct Absolute licenses. See BitLocker repair section below for more information. Possible values displayed in this reporting column include:
 - **No repairs:** the Repair option is not enabled in the application repair policy, or the device has a Status of Compliant so no repairs were attempted.
 - **All repairs succeeded:** the device has a Status of Not compliant and all attempted repairs were successful.
 - **All repairs failed:** the device has a Status of Not compliant and no attempted repairs were successful.
 - **Unknown:** unable to accurately detect the status of any BitLocker repairs
- **APPLICATION PERSISTENCE › BITLOCKER › STATUS:** The detected status of BitLocker on the device. Possible values are:
 - **Compliant:** BitLocker is functioning correctly and the BitLocker configurations detected on the device comply with the configurations set in the BitLocker policy
 - **Not compliant:** BitLocker is not functioning correctly, or the BitLocker configurations detected on the device do not comply with the configurations set in the BitLocker policy
 - **Error:** an unexpected error occurred while the BitLocker status check was running on the device. Status information was not uploaded.
 - **Unknown:** unable to accurately detect the status of BitLocker
- **APPLICATION PERSISTENCE › BITLOCKER › STATUS CHECKED (UTC):** The date and time the application repair: BitLocker status check was completed on the device.
- **APPLICATION PERSISTENCE › BITLOCKER › STATUS DETAILS:** Provides additional details about Not compliant statuses. If the Status is Compliant, no details are provided and two em dashes (– –) show in the column. The BitLocker status check consists of three key steps, as outlined in the table on the next page.

	Status Detail	Description
Step 1: Check system	OS BitLocker Capable	An indication of whether the operating system supports BitLocker Possible values are true or false .
	TPM BitLocker Capable	An indication of whether the Trusted Platform Module (TPM) is enabled and its version is 1.2 or higher Possible values are true or false .
		NOTE: Trusted Platform Module works with BitLocker to help protect user data on the device. It also helps to ensure that a computer has not been tampered with while the system was offline.
	WMI Functional	An indication of whether the Windows Management Instrumentation (WMI) is functioning correctly Possible values are true or false .
	System Partition Valid	An indication of whether the hard disk is partitioned into at least two drives Possible values are true or false .
NOTE: If all of the above values are true , the status check proceeds to step 2 (or to step 3 if BitLocker is not integrated with MBAM). If any values are false , the status check terminates and a status of Not compliant is reported.		
Step 2: Check MBAM (if applicable)	MBAM Agent Running	An indication of whether the Microsoft BitLocker Administration and Monitoring (MBAM) agent is functioning correctly on the device Possible values are true or false .
	Management URL Valid	An indication of whether the MBAM service URLs in the device's registry are correct Possible values are true or false .
	Group Policy Compliant	An indication of whether the MBAM Group Policy settings are applied on the device Possible values are true or false .
	User Exempted	An indication of whether the user is exempt from drive encryption Possible values are true or false .
	NOTE: If all of the above values are true , the status check proceeds to step 3. If any values are false , the status check terminates and a status of Not compliant is reported.	
Step 3: Check drives	For each drive that is non-compliant, the following information shows:	
	Volume: <volume letter>	The drive letter of the detected drive
	Encryption strength found	The detected encryption strength used to encrypt this drive Possible values are AES-128 , AES-256 or NONE . A value of NONE indicates that the drive is not encrypted.
	Encryption strength expected	The encryption strength configured in the BitLocker policy Possible values are AES-128 , AES-256 , or Any .

Table 1: BitLocker Status Reporting Details

BITLOCKER REPAIR WITH ABSOLUTE

Along with the popular BitLocker status reporting, the Absolute platform also includes the ability to repair BitLocker components and services on a device, both on and off the network. BitLocker components that are identified as requiring attention within the BitLocker Status report are repaired with healthy components. This is performed by scripts deployed on the endpoint to perform specific tasks.

COMPATIBILITY:

BitLocker Repair is applicable for customers with the following versions of Windows:

- Windows Vista and Windows 7, Ultimate and Enterprise editions
- Windows 8 and 8.1, Pro and Enterprise editions
- Windows 10, Pro, Enterprise, and Education versions
- Windows Server 2008 and later.

AVAILABILITY:

BitLocker Repair is available to customers with Absolute Resilience, along with legacy Computrace Complete/One and DDS Premium editions. Absolute Visibility and Control customers can also purchase the Application Persistence for Microsoft Applications add-on module.

ACTIVATION:

Existing customers can activate this feature within the Absolute console, by selecting the checkbox 'Repair if not compliant', as shown in in Figure 4.

IMPLEMENTATION:

When the BitLocker repair feature is turned on, the Absolute agent detects the status of BitLocker components by running scripts on the device. This script performs a series of health check tests to determine if BitLocker and MBAM components are present and functioning correctly. The script runs every 6 hours. If one of the tests indicate that the BitLocker or MBAM components are non-compliant, it then automatically initiates an additional script to repair the components that require attention or are missing.

No user input or changes to an organization's existing BitLocker environment are required for BitLocker reporting or repair. However, for the BitLocker repair process to be initiated, BitLocker and/or MBAM is required to have been previously installed and functioning on the device.

Dependent on the BitLocker component that is missing or has become corrupt, the Absolute agent will then perform an action on the device to remediate. This ranges from restarting or reregistering processes, restarting services, to testing the availability of required components. The results of these tests are shown within BitLocker status reports, as outlined in the BitLocker reporting section of this document.

The following issues can be automatically repaired:

- Windows Management Instrumentation (WMI) is not functioning correctly
- A valid system partition is not found

If an organization is using Microsoft BitLocker Administration and Monitoring (MBAM) to manage BitLocker, the following services can also be repaired:

- The BitLocker Management Client Service is not running
- The MBAM service URLs in the device's registry are incorrect or not found

Based on the elements specified in the reporting configuration if detected as non-compliant, the repair workflow below is initiated.

REPAIR WORKFLOW

If a device is discovered as non-compliant against the BitLocker reporting rules as defined in the Configuration policies (Figure 4 and 5), a repair workflow is initiated. The repair workflow waits 10 minutes before running any of its rules, in order to allow processes and applications to start up. The scheduled period for BitLocker reporting checks is every 6 hours. If the BitLocker options are changed on the server (e.g. configuration changes), the BitLocker repair workflow rule is run immediately when the request is received by the Absolute agent.

If setup with BitLocker Standalone, the following repair workflow is initiated.

BITLOCKER STANDALONE:

1. WMI services are checked, and required services are started and stopped.
2. The presence of the SYSTEM partition is checked; with a minimum size of 300 MB. If not a repair process is run, initiating the BitLocker Preparation Tool.

If setup with BitLocker MBAM, the following repair workflow is initiated following the BitLocker Standalone process as outlined above.

BITLOCKER MBAM:

1. Check if the MBAM client is running
 - **Check:** check for a service running named "BitLocker Management Client Service" and ensure it is set for run automatically.
 - **Repair:** start the service and configure it to run automatically.
2. Verify the values of the management URLs, **KeyRecoveryServiceEndPoint** and **StatusReportingServiceEndPoint** as outlined above in the 'Maintaining BitLocker Compliance' section and demonstrated in Figure 4.

BITLOCKER MBAM REINSTALL WITH ABSOLUTE

In addition to report on the compliance of BitLocker and repair non-compliant components, users can also choose to reinstall the MBAM client on endpoint devices where it is not compliant. In cases where the repair function is unable to remediate the health of the client, a customer administrator can choose to configure the download of the BitLocker MBAM client from an external URI and subsequently reinstall the client on the endpoint.

COMPATIBILITY:

BitLocker MBAM reinstall is applicable for customers with the following versions of Windows:

- Windows Vista and Windows 7, Ultimate and Enterprise editions
- Windows 8 and 8.1, Pro and Enterprise editions
- Windows 10, Pro, Enterprise, and Education versions

AVAILABILITY:

BitLocker MBAM reinstall is available to customers with Absolute Resilience, along with legacy Computrace Complete/One and DDS Premium editions. Absolute Visibility and Control customers can also purchase the Application Persistence for Microsoft Applications add-on module.

ACTIVATION:

Existing customers can activate this feature within the Absolute console, by selecting "BitLocker with standalone MBAM" under BitLocker Setup and then selecting the "Report, repair and reinstall" configuration, as shown in Figure 6.

Select the policy configuration option you want to apply to this application. The application is reported as compliant if it is installed, functional, and configured as expected.

Report only
 Report and repair
 Report, repair, and reinstall

To configure a path to the BitLocker MBAM installer, enter the URI, username and password information.

Location of the BitLocker MBAM installer

URI

URI Format: <https://example.com/path/example.msi>

Username and password (if required)
 Enter a username and password to access the installer in the specified location.

Username

Password

 Show Password

SHA-256 Hash
 The SHA-256 hash is used to verify the integrity of the binary contents of the BitLocker MBAM installer that is referenced by the URI. Use a hash generation tool, such as the Certutil command-line utility, to generate the SHA-256 hash for the binary file.

SHA-256 Hash

Ensure the hash code doesn't contain any whitespace characters, including leading and trailing whitespace.

I certify that I have sufficient licenses to install BitLocker MBAM on the devices in this policy group, and agree to the Application Persistence Terms and Conditions.

Figure 6: Configuring reinstall for the MBAM client.

BITLOCKER MBAM REINSTALL WORKFLOW

The administrator will be required to provide a URI to either a customer-hosted server or share/sync service (such as DropBox or Box) from where the Application Persistence engine will download the MBAM installer. They have the option of providing basic authentication credentials to access and download from the URI. Lastly, the administrator will have to provide the SHA-256 hash code associated with the MBAM installer to verify the downloaded installer's binary contents before running it on the endpoint device. Once the administrator agrees to the Application Persistence Terms and Conditions, clicks "Save" and "Activate" on the subsequent window, the "Report, repair and reinstall" configuration will be enabled for the associated policy group.

Once activated, in cases where the BitLocker MBAM Repair workflow fails to remediate non-compliant components of the MBAM client, the Application Persistence engine downloads the client's installer from the URI and verifies its binary contents using the SHA-256 Hash. Once verified, the installer will run and the MBAM client will automatically be reinstalled on the endpoint.

NOTE: Absolute and the BitLocker Application Persistence functionality does not setup, install, re-install or configure BitLocker encryption if it has never been setup initially on the device. As the name suggests, this feature is designed to report on BitLocker component health, including MBAM, and make an attempt to repair components when required. Additionally, if configured by the user, the feature will reinstall the MBAM client specifically as a final remediation step to maintain its health on the endpoint. Absolute does not Encrypt or Decrypt any files or folders, nor store any Encryption recovery keys. If Recovery key storage is a challenge, please contact [Absolute's Professional Services team](#).

For more information on Absolute and Microsoft BitLocker application repair functionality, please contact your Absolute sales representative, absolute.com/contact