Absolute Device Wipe FAQ

This document addresses a few commonly asked questions about Absolute Device Wipe, its use cases, how it functions and the data erasure standards it complies with.

What is Absolute Device Wipe?

Device Wipe is a device action available through the Absolute Control and Absolute Resilience service tiers of the Secure Endpoint product line. The action allows you to securely and remotely sanitize the drive of a Windows or Mac device that is either lost, stolen or has been compromised. Only Absolute can ensure that you can wipe sensitive data in the riskiest situations. Device Wipe can also be used as part of an organization's device decommissioning process to protect sensitive data from falling in the wrong hands.

Why is data sanitization important?

In today's anywhere work environment where remote and hybrid work policies are the norm, it has become common for endpoints to accumulate a variety of sensitive files over time. Devices hold a treasure-trove of sensitive data such as personally identifiable information (PII), health records (PHI), credit cards details, corporate intellectual property (IP) or customer information. Considering the endpoint is the primary source of most global security breaches (68% of breaches today originate at the endpoint[1]), it is of paramount importance for organizations to implement robust data sanitization practices to limit the risk of sensitive data being leaked and falling into the wrong hands. This ultimately boosts customer confidence and avoids the possibility of the organization incurring large fines for data breaches and reputational damage.

What use cases does Device Wipe cater to?

Device Wipe is typically executed in response to a device being lost, stolen or compromised in order to protect sensitive data residing on the device. As the action is executed remotely, it enables IT and Security teams to secure sensitive files on endpoints even in the riskiest or most vulnerable situations.

Device Wipe can also be incorporated as part of an organization's Device Lifecycle Management process. Examples of this include:

- Executing a wipe as part of the decommission process for devices at the end of their life.
- Executing a wipe prior to transferring them to a refurbishment facility.
- Executing a wipe as part of a school district's end-of-year reclamation of 1:1 devices (i.e. for K-12 Education).

What data sanitization methods are available with Device Wipe and how do they function?

Device Wipe offers two data sanitization methods, Delete All Files and Cryptographic Wipe. They can be described as follows:

Delete All Files:

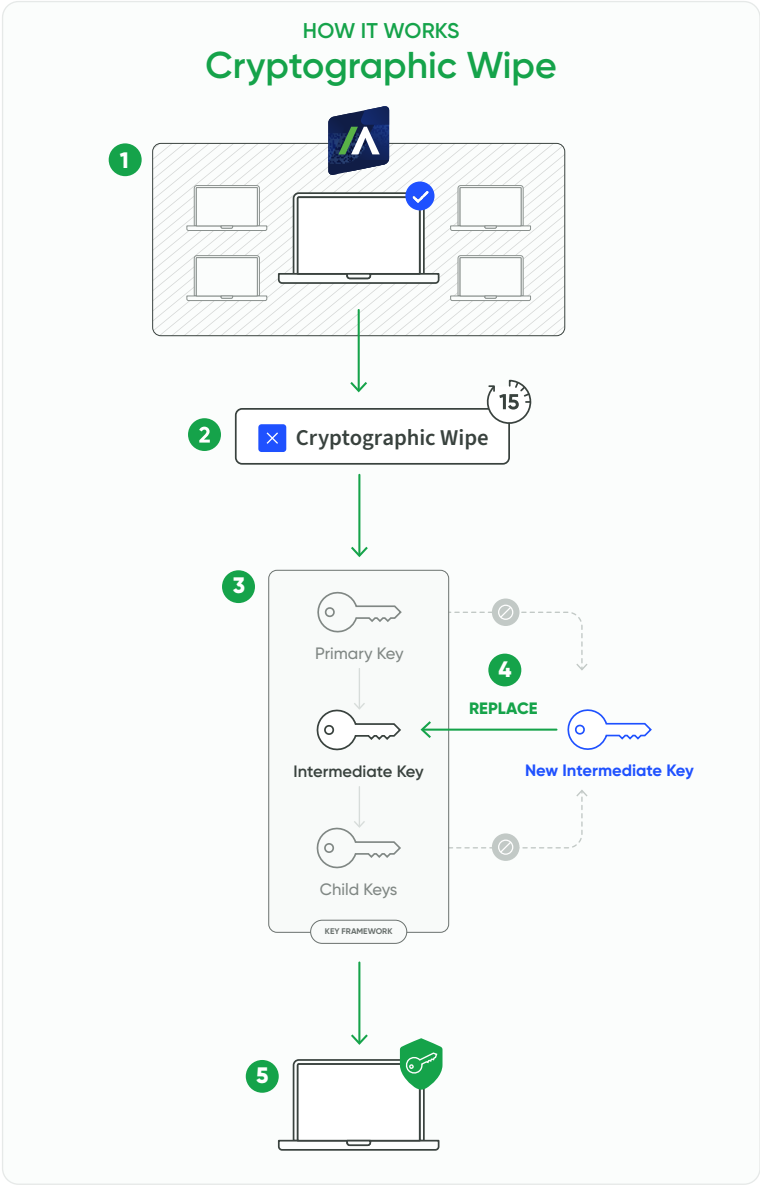
- The Delete All Files wipe option securely deletes files that are stored in directories where user data is typically found.
- Files are securely deleted by removing the file and overwriting the file's location with a fixed data pattern.
- Delete All Files relies on operating system commands to securely delete files, therefore special care is taken with operating system files and directories to prevent the operating system from crashing during the Delete All Files operation.

1 Ponemon Institute, 2020 State of Endpoint Security Risk

- As of the Absolute Secure Endpoint 9.0 release (available in April 2024), Delete All Files will take the additional step of deleting common document file types that are found within operating system directories on Windows 10 and higher.
- Delete All Files can also optionally disable the operating system as the final step.
- Delete All Files can take significant time to complete because of the time it takes to overwrite file data.
- Delete All Files wipe is supported on Windows and Mac devices that are encrypted or unencrypted.

Cryptographic Wipe:

- A Cryptographic Wipe employs the cryptographic erase data sanitization process, which removes all encryption keys, effectively making all data on encrypted partitions irretrievable, including the operating system. The drive can be formatted for reuse once the wipe is complete.
- Cryptographic Wipe is supported on devices that are encrypted with BitLocker on Windows or FileVault on macOS.
- Cryptographic Wipe completes very quickly because the procedure is implemented with cryptographic key operations rather than data overwrites.
- The steps involved in a Cryptographic Wipe are as follows:



1. An authorized administrator selects specific devices to be wiped through the Absolute Console.
2. The administrator then selects the Device Wipe action and opts to execute a Cryptographic Wipe
   a. The command percolates down to the endpoint at the next call-in (occurs every 15 minutes).
3. The device's drive is encrypted through a three-layered hierarchical key framework as described below.
   a. Primary key which protects the drive
   b. Intermediate key which protects the primary key
   c. Child keys which provide access to the intermediate key. These child keys are protected by a Trusted Platform Module (TPM), PIN/password or a recovery key.
4. Absolute's Cryptographic Wipe breaks this encryption key framework by replacing and discarding the intermediate key, which then renders the child keys to be invalid.
5. This then results in the drive still being encrypted without any keys in existence that can unlock it. The destruction of data on the drive then satisfies media sanitization standards listed in NIST SP 800-88r1.

When should you choose Cryptographic Wipe over Delete All Files?

Cryptographic Wipe is the preferred device wipe option when a drive is encrypted because the option completely sanitizes any encrypted data and because the operation executes very quickly. If, however, the drive is not encrypted or if you need to preserve the operating system, Delete All Files may be an appropriate secondary choice. Review this FAQ carefully to ensure that Delete All Files meets your data security requirements.

Does Device Wipe conform with data erasure guidelines as stated in NIST Special Publication 800-88 Revision 1 Guidelines for Media Sanitization (i.e. NIST SP 800-88r1) or other frameworks?

Delete All Files wipe conforms to the **Clear** standard defined in NIST SP 800-88r1. NIST SP 800-88r1 states that the **Clear** standard *"applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques."* The **Clear** standard is intended for device drives that will stay in the organization and that contain files with low or moderate security and confidentiality levels. Note that Delete All Files is often used in scenarios like loss or theft when the device is no longer within organizational control. This exceeds the applicability of the **Clear** standard. Nevertheless, in situations like these where there are few other options that can be executed remotely, Delete All Files provides a very good result.

Cryptographic Wipe conforms to the **Purge** standard defined in NIST SP 800-88r1. In NIST SP 800-88r1, the **Purge** standard is defined as one that *"applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques."* The **Purge** standard is intended for drives that 1) leave the organization and with information of low or moderate security and confidentiality or 2) remain in the organization with information of high security and confidentiality. Although the cryptographic erase operation performed by Cryptographic Wipe does not perform any data overwrites, it is recognized by the standard as an effective and quick method of data sanitization.

Both Delete All Files and Cryptographic Erase are HIPAA compliant.

What constraints must be understood to make best use of Delete All Files?

Delete All Files is designed to sanitize user data subject to the following constraints:

- It deletes files where user data is normally stored. It uses operating system commands, so it is limited to what the operating system can do and to what the operating system has access to. It cannot delete data that the operating system cannot address (e.g. bad sectors or unmounted partitions).
- It is not hardened against malicious users that store data in non-standard locations.
- It is not hardened against forensic tools.
- It must preserve the integrity of the operating system so that the delete operation completes successfully.
- As of the Absolute Secure Endpoint 9.0 release (available in April 2024), it can also delete standard document file types in the operating system directories.

Note that hidden or corrupted files or files inaccessible by the operating system fall outside the execution of erasure methods that follow the **Clear** standard such as Delete All Files.

What constraints must be understood to make best use of Cryptographic Wipe?

Cryptographic Wipe is designed to sanitize user data subject to the following constraints:

- Requires all sensitive data to reside on a BitLocker or FileVault encrypted partition.
- The drive must be encrypted before any sensitive data is stored. Drives that are encrypted part way into their lifecycle may contain remnants of sensitive data that could not be encrypted. These remnants are not encrypted and therefore cannot be sanitized by Cryptographic Wipe.
- BitLocker's Full Drive Encryption option is recommended. While the "Used Space Only" option is supported, this configuration should only be used on drives that have not been previously used.

Does Delete All Files and Cryptographic Wipe perform a verification of the overwrite after the process has been completed and is this a requirement of the NIST SP 800-88r1 standard?

Verification is an important part of the NIST SP 800-88r1 standard, which includes verification that the equipment is capable of successfully performing the wipe, verification that staff are sufficiently trained, and verification that the wipe was successful. Verification should be built into your sanitization process.

Delete All Files and Cryptographic Wipe do not perform verification once the process is complete. It is not possible for a remote tool that runs at the application level to adequately perform a full verification. In cases like these where there is an operational impediment which prevents verification of every sanitization operation, NIST recommends representative sampling using a secondary tool from another developer. This verification step is distinct from and not mandated by the

NIST SP 800-88r1 **Clear** and **Purge** standards, which acknowledge that it isn't always possible for a sanitization tool to perform a verification step. Hence, the standards highlight the importance of security practitioners to assess risk against the sensitivity of the data and to treat sanitization as a process rather than a function performed by a single tool.

From which specific locations on a drive does the Delete All Files process deletes information from?

Windows

The following system directories are *not* deleted by the Delete All Files security action:

- C:\boot.ini
- C:\bootmgr
- C:\ntldr
- C:\bootsect
- C:\NTDETECT.COM
- C:\pagefile.sys
- C:\swapfile.sys
- C:\boot\
- C:\System Volume Information\
- C:\Internet Explorer\
- C:\Windows\
- **\\WWANSVC**
- **\\WLANSVC**
- *.PAC

Note that if you select the Disable the Windows OS option in the Wipe request, the following files *are* deleted:

- C:\boot.ini
- C:\bootmgr
- C:\ntldr
- C:\NTDETECT.COM
- C:\boot\

In addition to the files listed above, the Delete All Files security action *can't* delete files/folders that are:

- Encrypted or locked by a third party tool.
- Stored in a volume that is encrypted or locked by a third party tool.
- Stored in a hidden partition.
- Inaccessible because inherited permissions have been disabled.
- Created by a user after the area has already been scanned.
- Recreated automatically by the Windows operating system.

Mac

The following system directories are not deleted by the Delete All Files security action:

- /Library
- /Library/*
- /System
- /System/*
- /sbin
- /sbin/*
- /usr
- /usr/*
- /bin
- /bin/*

- /private
- /private/*
- /dev
- /dev/*
- /etc
- /etc/*
- /var
- /var/*
- /tmp
- /tmp/*
- /mach_kernel
- /Developer
- /Developer/*
- /home
- /home/*
- /net
- /net/*
- *.fseventsd
- *AftIICopyfiles.sh
- *AftIIInstall.sh
- *ARAT.tar.gz
- *ARAT.tar.gz.MD5
- *stopAndRemoveAFRAT.sh
- *.DocumentRevisions-V*
- *.Spotlight-V*

In addition to the files listed above, the Delete All Files security action *can't* delete files/folders that are:

- Encrypted or locked by a third-party tool.
- Stored in a volume that is encrypted or locked by a third-party tool.
- Stored in a hidden partition.
- Inaccessible because inherited permissions have been disabled.
- Created by a user after the area has already been scanned.

Also note that if a file's size is very large (> 1GB) and it exceeds the device's free space, the file can't be deleted.

Can you obtain a certificate of sanitization to prove that devices were indeed wiped?

Yes, you can obtain a Certificate of Sanitization through the Absolute Console once a Device Wipe (i.e. Cryptographic Wipe or Delete All Files) has been successfully executed on a device. This is particularly useful to demonstrate that a device's data was successfully sanitized in compliance with NIST SP 800-88r1.

For more information about Device Wipe and how to execute it through the Absolute Console, check out the **Absolute Help**.