

How Xerox® Products Provide Data Storage Security

Protection beyond Image Overwrite

© 2021 Xerox Corporation. All rights reserved. Xerox®, AltaLink®, ColorQube®, ConnectKey®, Phaser®, PrimeLink®, VersaLink® and WorkCentre® are trademarks of Xerox Corporation in the United States and/or other countries. BR32939

Document Version: 2.0 (June 2021).

Contents

1. Introduction.....	ii
2. Encryption.....	2-1
Hard Disk Drive (HDD) and Solid-State Drive (SSD).....	2-1
TPM Private Key Storage	2-1
3. Image Overwrite	3-2
Image Overwrite Methods and Algorithm (HDDs Only)	3-2
Immediate Image Overwrite (IIO) and On Demand image Overwrite (ODIO).....	3-2
Detailed Image Overwrite Process	3-3
4. Things to Remember.....	4-4
Hard drive/solid state drive retention offering	4-4
Image overwrite considerations	4-4
Other important information	4-4
5. Model Breakdown	5-1
Monochrome Hardware Products	5-1
Color Hardware Products	5-5
Production Products (Color and Monochrome)	5-8
6. Resources	5-9

1. Introduction

Xerox® Copiers, printers and multifunction products are devices that contain a computer and the necessary software that allow them to accomplish the many productivity-enhancing tasks that have become so valuable to today's workplaces. These internal computers may have a disk drive or other non-volatile storage where image data may be temporarily written during processing. Additionally, image data may be stored for later reprint on some models. From the introduction of the first digital products, Xerox has recognized the risk of retained data being inappropriately recovered from non-volatile storage and have built in features and countermeasures in its products to help customers safeguard their image data.

This whitepaper will cover the encryption method used by Xerox® Products for data storage at rest in hard disk drives (HDDs) and solid-state drives (SSDs). It will also explain the image overwrite options available for HDDs and the associated algorithms used. A table is provided which details available data storage methods and product support of image overwrite and encryption. References to supporting documents and information are provided to further your understanding of how Xerox® Products protect customer image data.

Note: This information is most specific to AltaLink® and ConnectKey® and details of the implementation in other Xerox® Products may differ. Please consult your device Security Guide, Statement of Volatility (SOV) and/or Information Assurance Disclosure (IAD) for more information on what your specific model supports. Please be sure to review all footnote mentions for important details.

.

2. Encryption

Hard Disk Drive (HDD) and Solid-State Drive (SSD)

Overwrite functionality was developed to ensure security of image data on HDDs prior to the widespread use of encryption. Today, strong encryption methods are extremely effective in protecting image data from unauthorized disclosure. Its use with Image Overwrite functionality, however, is complimentary additional security for customers who have come to depend on Image Overwrite and consider it a required feature.

Xerox® Products use Advanced Encryption Standard (AES) 256-bit encryption for HDD and SSD storage. In some Xerox® Products, encryption is always enabled and cannot be disabled. Please refer to your product's Security Guide¹ for more information. In case there is a question about how secure AES encryption is consider the following:

AES is the strongest encryption commercially available and is the standard used by many government agencies including the military and NSA to name a few. Using a 256-bit key, offers 2^{256} possible key combinations. There are no known methods to break AES encryption or a computer which exists today which have the computational power to break it. The fastest computer in the world currently uses a brute force² attack to try all possible combinations, would take millions of years to crack AES encryption. It is therefore considered unbreakable and this is likely to be the case for many years to come.

What this means for customers is that even without the use of image overwrite, image data stored on an AES encrypted HDD or SSD is extremely secure. If image data on the drive is somehow accessed it is undecipherable and it will remain in that state unless it is decrypted with the corresponding encryption key.

TPM PRIVATE KEY STORAGE

All Xerox® Products use a secure encryption key storage method. It should also be noted that encryption key storage protection is an extremely important aspect of encryption. This section highlights the use of the Trusted Platform Module (TPM) for key storage specifically. AltaLink® products use a TPM module for private key storage on the system which is managed in compliance with NIST Special Publication 800-57 Recommendation for Key Management. This includes keying material in transition and at rest. An onboard TPM module (v2.0) compliant with ISO/IEC 11889 is used in support of private key management. Please consult the Security Guide for your specific model for more information on the use of a TPM or encryption key storage. Xerox Product Security Guides can be found at: <https://security.business.xerox.com/en-us/>.

PrimeLink® and VersaLink® also use a TPM. Please consult the product Security Guide for more information on TPM function for your specific model.

¹ Older products may not have a Security Guide which encompasses the IAD and SOV information.

² Brute Force attacks try all possible combinations of letters, numbers and special characters to “guess” a password.

3. Image Overwrite

Image Overwrite³ Methods and Algorithm (HDDs Only)

Image data may be written to nonvolatile memory (e.g. to a hard drive) during processing. Image overwrite is effective at eliminating the encrypted image data from the hard drive once the image data is no longer needed. For customers that want the additional peace of mind (or have regulatory requirements that mandate) even though image data on an encrypted drive is not recoverable, another level of security can be applied by using Image Overwrite.

IMMEDIATE IMAGE OVERWRITE (IIO) AND ON DEMAND IMAGE OVERWRITE (ODIO).

When enabled, IIO will overwrite any temporary files that were created on the magnetic hard disk that may contain user data. This process may be performed at the end of a job, where it will overwrite the files used for that job. When enabled IIO will overwrite and remove any remnants and temporary files of all print, copy, scan, and fax jobs from the image disk as soon as the job finishes processing.

Complementing IIO is ODIO. While IIO overwrites individual files, ODIO overwrites entire partitions. The ODIO feature can be invoked at any time and optionally may be scheduled to run automatically. Please consult your product System Administrator Guide for your specific product to see what Image Overwrite features are available. Following are more details on both overwrite methods.

1. The process used for IIO to overwrite data in AltaLink®, ConnectKey®, PrimeLink®, and VersaLink® products complies with NIST SP.800-88-r1 Purge option 1a⁴. This process meets or exceeds the requirements of the Clear function. For AltaLink® and WorkCentre® products specifically, the process also complies with DOD NISPOM 5220.22-M section 8-301⁵.

2. ODIO may also be referred to as a Full or Standard Image Overwrite and goes beyond an IIO. Xerox recommends that customers enable IIO which occurs after each job and schedule an ODIO at low usage hours to remove Image data such as Secure Print jobs that may not have been retrieved by users on a daily basis. This is a very secure option that requires no additional effort and is easily implemented. Please refer to the System Administrator Guide (SAG) and the Security Guide of your Xerox® Product for more information.

Note: For security of SSD drives “Job Data Removal” is being introduced starting with AltaLink® C81xx/B81xx. Xerox now provides customers with SSD data storage products with the ability to clean up the disk by purging image data (not an overwrite) using the same interface as ODIO available with HDD configuration.

⁴ NIST Special Publication 800-88r1:

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>

⁵ DOD NISPOM 5220-22-M: <http://www.dss.mil/documents/odaa/nispom2006-5220.pdf>

Please see our whitepaper titled “Data Protection: Solid State Drives and Data at Rest” available at:

<https://security.business.xerox.com/en-us/documents/white-papers/> as well as consulting your model’s Security Guide.

Detailed Image Overwrite Process⁶

1. When the overwrite operation is started, a start indication is recorded in the audit log.
2. This process is executed on multiple partitions, depending on the type of overwrite enabled.
3. A single pattern is written to the entire partition.
4. The inverse of the pattern above (ones-complement) is written to the entire partition.
5. A unique new pattern is then written to the entire partition.
6. Starting at a random starting position, 10% of the partition is sampled for the occurrence of the last pattern. The 10% block is continuous.
7. If the sample check fails, then the operation terminates, and indicates a failed condition via a persistent message on the device user interface. When the device restarts, this message persists until an overwrite procedure is repeated⁷. A failed indication will be recorded in the audit log.
8. If the sample succeeds, then the next partition in the list is used, and the process repeats at step 3.
9. When all the partitions in the list have completed, a “success” is recorded, and the device is rebooted.
10. After the reboot, the device may print a confirmation sheet, if it was enabled.
11. The success or failure of the process is recorded in the audit log.

⁶ Compliant to NIST SP.800-88r1

⁷ For VersaLink® models Image Overwrite will automatically resume when the device restarts.

4. Things to Remember

HARD DRIVE/SOLID STATE DRIVE RETENTION OFFERING

Hard Drive Retention Offering is a service that can be requested by a customer who wants to retain their HDD or SSD for security reasons. A Xerox technician will remove the drive and leave it with the customer. Contact Xerox Customer Support for information on fees and availability in your geography. Please see the link for whitepapers on hard drive retention in the US and Europe: <https://security.business.xerox.com/en-us/documents/white-papers/>

IMAGE OVEWRITE CONSIDERATIONS

- Not all products have HDDs.
- Some products have HDDs, but do not use the hard disk drive to save image data
- Image overwrite features are available for hard drive equipped products only and are not applicable to Solid-State nonvolatile memory (SSD), SD (Secure Digital), IC (Integrated Chip) or eMMC (embedded Multi-Media Card) storage methods. Please be sure to reference the Security Guide, or if an older product, the Information Assurance Disclosure (IAD) or Statement of Volatility (SOV) document of your product for information on data security.
- Image overwrite features may be available as Full or Standard. Consult your product Security Guide or System Administrator Guide for the specific available overwrite features of your Xerox Product.

Note: Xerox does not offer sanitization or cleansing services for returned disk drives. Please see the whitepaper “ Hard Drive Retention Offering and Equipment Returns for Products in the US” at: <https://security.business.xerox.com/en-us/documents/white-papers/> for information on equipment returned to Xerox.

OTHER IMPORTANT INFORMATION

Security related information, including Security Bulletins⁸, patch information, US-CERT advisory updates and white papers which focus on security and the mitigation of security risks can be found on the Product Security website www.xerox.com/security.

Xerox also provides detailed information about internal product workflows and key security features now contained in product Security Guides (formerly Information Assurance Disclosure documents and Statements of Volatility) which are available for many products at the website. Security Guides have expanded information on the various product security features and are a combination of IADs and SOVs. We suggest you consult these publications for more complete information on how your specific Xerox® Product secures your information.

For Production equipment data storage security information for the associated Digital Front End (DFE) should be referenced.

⁸ Please be sure to sign up for RSS feeds on the Product Security page www.xerox.com/security

5. Model Breakdown

Monochrome Hardware Products

Xerox® Products (Alphabetical Order)	HDD	SSD/ SSM	IC, SD Card or Other	Immediate Image Overwrite	On Demand Image Overwrite (Y/N) Or Process to Clear	Encryption
Xerox® AltaLink® B8100 Series	Optional	SSD	N/A	SSD: N/A Optional HDD: Yes	SSD: Data Purge Optional HDD: On Demand Image Overwrite	Yes
Xerox® AltaLink® B8045/B8055/B8065/B8075/B8090 Series Multifunction Printer	Yes	N/A	SD Card	SD: N/A HDD: Yes	HDD: On Demand Image Overwrite SD: N/A	Yes
Xerox® Phaser® 3052 Printer	No	N/A	N/A	N/A	N/A	N/A
Xerox® Phaser® 3260 Printer	No	N/A	N/A	N/A	N/A	N/A
Xerox® WorkCentre® 3325 Printer	Yes	N/A	N/A	No ⁹	Yes	Yes
Xerox® WorkCentre® 3315 Printer	No	N/A	N/A	N/A	N/A	N/A
Xerox® Phaser® 3320 Printer	No	N/A	N/A	N/A	N/A	N/A
Xerox® Phaser® 3330 Printer	No	No	N/A	N/A	N/A	N/A
Xerox® Phaser® 3610 Printer	No	No	Optional SD Card	N/A	Invoke Clear Storage	No
Xerox® Phaser® 3635 MFP	Yes	N/A	N/A	Yes	Yes	Yes

⁹ Overwrite consists of a single pass using the F Character

Xerox® Products	HDD	SSD/ SSM	IC, SD Card or Other	Immediate Image Overwrite	On Demand Image Overwrite (Y/N) Or Process to Clear	Encryption
Phaser® 4510 network printer	Optional	No	N/A	No	Optional HDD: Yes	No
Xerox® Phaser® 4600/4620 Printer	Yes	No	N/A	Yes	Yes	Yes ¹⁰
Xerox® Phaser® 4622	Yes	No	N/A	Yes	Yes	Yes
Phaser® 5335 Printer	Yes	No	N/A	Yes	Yes	Yes
Xerox® Phaser® 5550 Printer	Optional	N/A	N/A	No	Optional HDD: Yes	No
Xerox® WorkCentre® 3025 Multifunction Printer	No	No	N/A	N/A	N/A	N/A
Xerox® WorkCentre® 3210/3220 Multifunction Printer	No	No	N/A	N/A	N/A	N/A
Xerox® WorkCentre® 3215/3225 Multifunction Printer	No	No	N/A	N/A	N/A	N/A
Xerox® WorkCentre® 3315 Multifunction Printer	No	No	N/A	N/A	N/A	N/A
Xerox® WorkCentre® 3325 Multifunction Printer	Yes	No	N/A	No	Yes (Single Pass using the F character)	Yes

¹⁰ Contingent on the Hard Drive option installed

Xerox® Products	HDD	SSD/ SSM	IC, SD Card or Other	Immediate Image Overwrite	On Demand Image Overwrite (Y/N) Or Process to Clear	Encryption
Xerox® WorkCentre® 3335/3345 Multifunction Printer	No	No	SD Card	N/A	Clear via Diagnostic Procedure	No
Xerox® WorkCentre® 3550 Multifunction Printer	No	No	N/A	N/A	N/A	N/A
Xerox® WorkCentre® 3615 Multifunction Printer	No	No	SD Card	N/A	Clear Storage option on LUI	N/A
Xerox® WorkCentre® 3655 Multifunction Printer	Yes	No	N/A	Yes	Yes	Yes
WorkCentre® 4250 MFP	Yes	No	N/A	No	Yes	Yes
Xerox® WorkCentre® 4265 Multifunction Printer	Yes	No	N/A	No	Yes	Yes
Xerox® WorkCentre® 5135/5150 Multifunction Printer	Yes	No	Flash NVRAM	No	HDD and NVRAM: On Demand clears	No
Xerox® WorkCentre® 5325/5330/5335 Series Multifunction Printer	Yes	N/A	N/A	Yes	Yes	Yes
Xerox® WorkCentre® 5740/5745/5755/5765/5775/5790 Series	Yes	N/A	N/A	Yes	Yes	Yes
Xerox® WorkCentre® 5845/5855/5865/5875/5890 Series Multifunction Printer	Yes	N/A	N/A	Yes	Yes	Yes
Xerox® WorkCentre® 5945/5955 Multifunction Printer	Yes	N/A	N/A	Yes	Yes	Yes
Xerox® VersaLink® B400 Printer	No	Optional	IC	No	Clear via Diagnostic Procedure	Yes
Xerox® VersaLink® B405 Multifunction Printer	No	Optional	IC	No	Clear via Diagnostic Procedure	Yes

Xerox® Products	HDD	SSD/ SSM	IC, SD Card or Other	Immediate Image Overwrite	On Demand Image Overwrite (Y/N) Or Process to Clear	Encryption
Xerox® VersaLink® B600/B610 Printer	Optional	No	IC	Optional HDD: Overwrite after job Completion	Optional HDD: Yes IC: Clear via Diagnostic Procedure	Yes
Xerox® VersaLink® B605/B615 MFP	Optional	No	IC	Optional HDD: Overwrite after job Completion	Optional HDD: Yes IC: Clear via Diagnostic Procedure	Yes
Xerox® VersaLink® B7025/B7030/B7035 Series Multifunction Printer	Optional	No	SD Card	Optional HDD: Overwrite after job Completion	Optional HDD: Yes SD Card: N/A	Yes
Xerox® B1022/B1025 Multifunction Printer	No	No	N/A	N/A	N/A	N/A

Color Hardware Products

Xerox® Products	HDD	SSD/ SSM	IC, SD Card or Other	Immediate Image Overwrite	On Demand Image Overwrite (Y/N) Or Process to Clear	Encryption
Xerox® AltaLink® C8100 Series	Optional	Yes	N/A	Yes (for HDD Only)	HDD: On Demand SSD: Job Data Removal (Scheduled and On Demand)	Yes
Xerox® AltaLink® C8030/C8035/C8045/C8055/C8070 Series Color Multifunction Printer	Yes	No	SD Card	SD Card: N/A HDD: Yes	HDD: Yes SD Card: N/A	Yes
Xerox® ColorQube™ 8580/8880 Printer	No	Yes	N/A	N/A	No	Yes
Xerox® Phaser® 6020 Printer	No	No	N/A	N/A	N/A	N/A
Xerox® Phaser® 6022 Printer	No	No	N/A	N/A	N/A	N/A
Xerox® Phaser® 6500 Printer	No	No	N/A	N/A	N/A	N/A
Xerox® Phaser® 6510 Color Printer	No	No	eMMC ¹¹	N/A	N/A	Yes
Xerox® Phaser® 6600 Printer	No	No	N/A	N/A	N/A	N/A
Xerox® Phaser® 6700 Printer	Yes	No	N/A	N/A	Optional Image Overwrite Kit	No
Xerox® Phaser® 7100 Printer	Optional	No	N/A	Optional HDD: Yes	Optional HDD Yes	No
Xerox® Phaser® 7500	Yes	No	N/A	Automatic Overwrite Removal Option	Select Overwrite Removals	No

¹¹ Embedded Multi-Media Controller consists of flash memory and a flash memory controller in one component.

Xerox® Products	HDD	SSD/ SSM	IC, SD Card or Other	Immediate Image Overwrite	On Demand Image Overwrite (Y/N) Or Process to Clear	Encryption
Xerox® Phaser® 7800 Printer	Yes	No	N/A	Yes (Optional Kit)	Yes (Optional Kit)	No
Xerox® WorkCentre® 6025 Multifunction Printer	No	No	N/A	N/A	N/A	N/A
Xerox® WorkCentre® 6027 Multifunction Printer	No	No	N/A	N/A	N/A	N/A
Xerox® WorkCentre® 6515 Color Multifunction Printer	No	No	eMMC	N/A	N/A	Yes
Xerox® WorkCentre® 6605 Multifunction Printer	Optional	No	N/A	No	Clear Storage Option on LUI	Yes
Xerox® WorkCentre® 6655 Color Multifunction Printer	Yes	No	N/A	Yes	Yes	Yes
Xerox® WorkCentre® 7120/7125/7132 Series Multifunction Printer	Yes	No	N/A	No	Yes	Yes
Xerox® WorkCentre® 7220/7225 Multifunction Printer	Yes	No	N/A	Yes	Yes	Yes
Xerox® WorkCentre® 7525/7530/7535/7545/7556 Series MFP	Yes	No	N/A	Yes	Yes	Yes
Xerox® WorkCentre® 7755/7765/7775 MFP	Yes	No	N/A	Yes	Yes	Yes
Xerox® WorkCentre® 7830/7835/7845/7855 Series Multifunction Printer	Yes	No	N/A	Yes	Yes	Yes
Xerox® WorkCentre® 7970 Color Multifunction Printer	Yes	No	N/A	Yes	Yes	Yes
Xerox® VersaLink® C400 Color Printer	Optional	No	IC	Optional HDD Yes	Optional HDD: Yes IC: Clear via Diagnostic Procedure	Yes
Xerox® VersaLink® C405 Color Multifunction Printer	Optional	No	IC	Optional HDD Yes	Optional HDD: Yes IC: Clear via Diagnostic Procedure	Yes

Xerox® Products	HDD	SSD/ SSM	IC, SD Card or Other	Immediate Image Overwrite	On Demand Image Overwrite (Y/N) Or Process to Clear	Encryption
Xerox® VersaLink® C500 Color Printer	Optional	No	IC	Optional HDD Yes	Optional HDD: Yes IC: Clear via Diagnostic Procedure	Yes
Xerox® VersaLink® C505 Color Multifunction Printer	Optional	No	IC	Optional HDD Yes	Optional HDD: Yes	Yes
Xerox® VersaLink® C600 Color Printer	Optional	No	IC	Optional HDD Yes	Optional HDD: Yes IC: Clear via Diagnostic Procedure	Yes
Xerox® VersaLink® C605 Color Multifunction Printer	Optional	No	IC	Optional HDD Yes	Optional HDD: Yes IC: Clear via Diagnostic Procedure	Yes
Xerox® VersaLink® C7000 Color Printer	Optional	No	SD Card	Optional HDD: Yes SD Card: No	Optional HDD: Yes SD: N/A	Yes
Xerox® VersaLink® C7020/C7025/C7030 Series Color Multifunction Printer	Optional	No	SD Card	Optional HDD: Yes SD Card: No	Optional HDD: Yes SD: N/A	Yes
Xerox® VersaLink® C8000/C9000 Color Printer	Optional	No	SD Card	Optional HDD: Yes SD Card: No	Optional HDD: Yes SD: N/A	Yes
Xerox® VersaLink® C8000W	Optional	No	SD Card	Optional HDD: Yes SD Card: No	Optional HDD: Yes SD: N/A	Yes

Production Products (Color and Monochrome)

Note: Production product functionality requires that a Digital Front End (DFE) be used for normal operation in many cases. This means that storage of customer image data as part of the reproduction process is managed by DFE data storage and not the device. Products that are capable of storing customer image data on the HDD are listed below. Security documentation for the DFE should still be referenced since even though a product may be able to use its HDD this may not be the case when connected to a DFE. This is encouraged

Please refer to the product's DFE Security Documentation: Statement of Volatility, Security Guide or System Administrator Guide for data security information regarding storage that will contain user data and or image data (print, scan, fax, copy – where applicable).

Xerox® Products	HDD	SSD/ SSM	IC, SD Card or Other	Immediate Image Overwrite	On Demand Image Overwrite (Y/N) Or Process to Clear	Encryption
Xerox® 4112/4127 CP & Enterprise Printing System	Optional (HDD not used to store image files during normal Operation)	No	N/A	No	Optional Security Kit w/On Demand/ Scheduled Image Overwrite	Yes
Xerox® 770 Digital Color Press	Optional	No	N/A	No	Optional Security Kit w/On Demand/ Scheduled Image Overwrite	Optional
Xerox® Color 550/560/570 Printer	Yes	No	N/A	No	Yes	Yes
Xerox® Color C60/C70 Printer	Yes	No	N/A	Yes	On Demand	Yes
Xerox® Color C75 Digital Press	Yes	No	N/A	No	On Demand w/Optional Kit	Yes (128 bit)
Xerox® Color J75 Digital Press	Yes	No	N/A	No	Yes	Yes
Xerox® D95/D110/D125/D136 Copier/Printer	Yes	No	N/A	No	Yes	Yes
Xerox® PrimeLink® B9100 Series	Yes	No	N/A	Yes	Yes	Yes

6. Resources

Resource	URL	How to access
Find your device Security Guide, IAD or SOV	www.xerox.com/security	Select your product family from the menu → Select your model → Select Information Assurance Disclosure/Statement of Volatility (if applicable)
Find your device System Administrator Guide (SAG)	https://www.support.xerox.com/	Either type in your model or choose the applicable category → Select your product family → Select your model → Select Documentation → Choose System Administrator Guide (SAG) or User Guide in a SAG is not available
Find the <u>Latest</u> Software Release for your product	www.xerox.com/security	Scroll down the right pane of the page and click on the link at Security Resources → Software Release Quick Lookup Table
Find Security Bulletins for your product	www.xerox.com/security	Select your product family from the menu → Select your model → Select the Security Bulletins for Xerox Products Menu
Sign Up for RSS Feeds (for notification of published Security Bulletins)	www.xerox.com/security	Sign up for RSS feeds to get notification of published security bulletins for your product. Scroll down the right pane of the page and click on the link at: Feed for new Security Bulletins
Have a question regarding a Security Function or want to report a vulnerability?	www.xerox.com/security	Scroll down the right pane of the page and click on the link at Contact us: Submit a question, report a vulnerability or request more information on product security
Articles and Whitepapers	https://security.business.xerox.com/en-us/documents/white-papers/	Access this link for Articles and Whitepapers focused on various security related topics for Xerox® Products, Services, Processes, etc.
What if: <ul style="list-style-type: none"> • My device is not functioning properly? • I have questions regarding supplies? • I don't know what my device password is? • I need sales assistance? 	https://www.xerox.com/en-us/about/contact-us	Numbers and websites for Technical Service, Sales and Supplies can be found on this page. For customers outside of the US please scroll down the page to Worldwide Contacts and select your applicable region.