WHITE PAPER

RDX® PowerEncrypt

RDX PowerEncrypt data encryption provides security of data stored on RDX media during transportation or off-site archiving by protecting against unauthorized access.

Introducing RDX PowerEncrypt

RDX PowerEncrypt data encryption can be added to any RDX media. It encrypts the data written to the RDX media using AES-256 XTS standards and access to the data is secured by a password key deployed with the RDX Manager software. Without the password key, the data that resides on the RDX media cannot be accessed by an unauthorized user making both the media and data useless. With RDX PowerEncrypt, you can be confident your data is protected.

Access to the encrypted RDX media requires that RDX Manager be installed on the system. RDX Manager facilitates access to both the media and data as well as the erasure, partitioning and formatting tools. Additionally, when using RDX Manager to remove encryption, a secure media erase is performed automatically.

The latest RDX Manager software, which includes RDX PowerEncrypt functionality, is available for download from the RDX QuikStor product web page. It is highly recommended that RDX Manager be installed whenever RDX is used, as it provides easy access for all RDX capabilities including media eject safety, mode changes, media preparation, diagnostics, firmware upgrades and now RDX PowerEncrypt functions.

PowerEncrypt value

RDX PowerEncrypt is a complementary value built into RDX QuikStor SATA III drives using version 0253 and later firmware and will be available soon for other RDX products as part of our extensive product development roadmap.

RDX PowerEncrypt is powered by the FIPS 140-2 validated RDX SATA III drive. Now data on RDX media can be encrypted with confidence in any use case requiring data security. Customers who need to operate the RDX SATA III drive in FIPS 140-2 mode can order a tamper-evident seal kit from Overland-Tandberg.

Operational modes and options

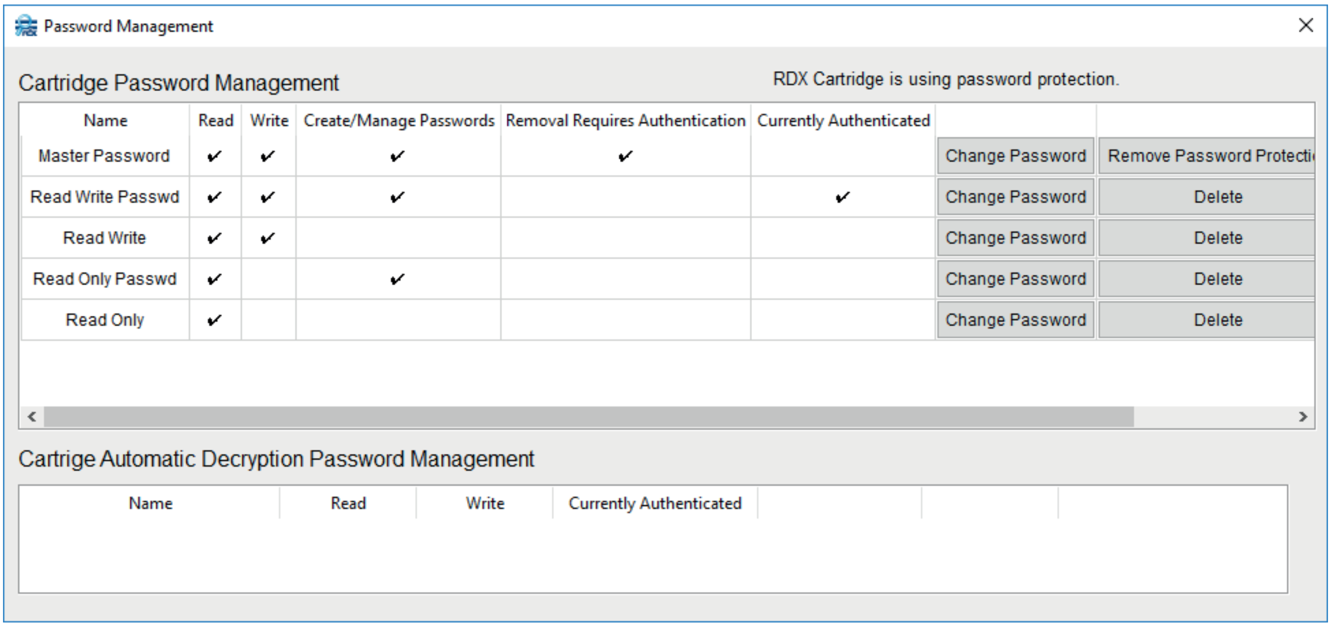
RDX PowerEncrypt provides two modes of data security – password-only protection and password protection with encryption.

Basic password protection (without encryption)

RDX PowerEncrypt supports up to eight passwords with four different access right options and management capabilities. These four access rights are:

- Read only access
- Read only access with password management
- Read/Write access
- Read/Write access with password management

In addition, a Master Password with read/write access and password management is automatically provided. This Master Password is used to manage the RDX media protection.



Cartridge Password Management

RDX Cartridge is using password protection.

Name	Read	Write	Create/Manage Passwords	Removal Requires Authentication	Currently Authenticated		
Master Password	✓	✓	✓	✓		Change Password	Remove Password Protecti
Read Write Passwd	✓	✓	✓		✓	Change Password	Delete
Read Write	✓	✓				Change Password	Delete
Read Only Passwd	✓		✓			Change Password	Delete
Read Only	✓					Change Password	Delete

Cartrige Automatic Decryption Password Management

Name	Read	Write	Currently Authenticated		

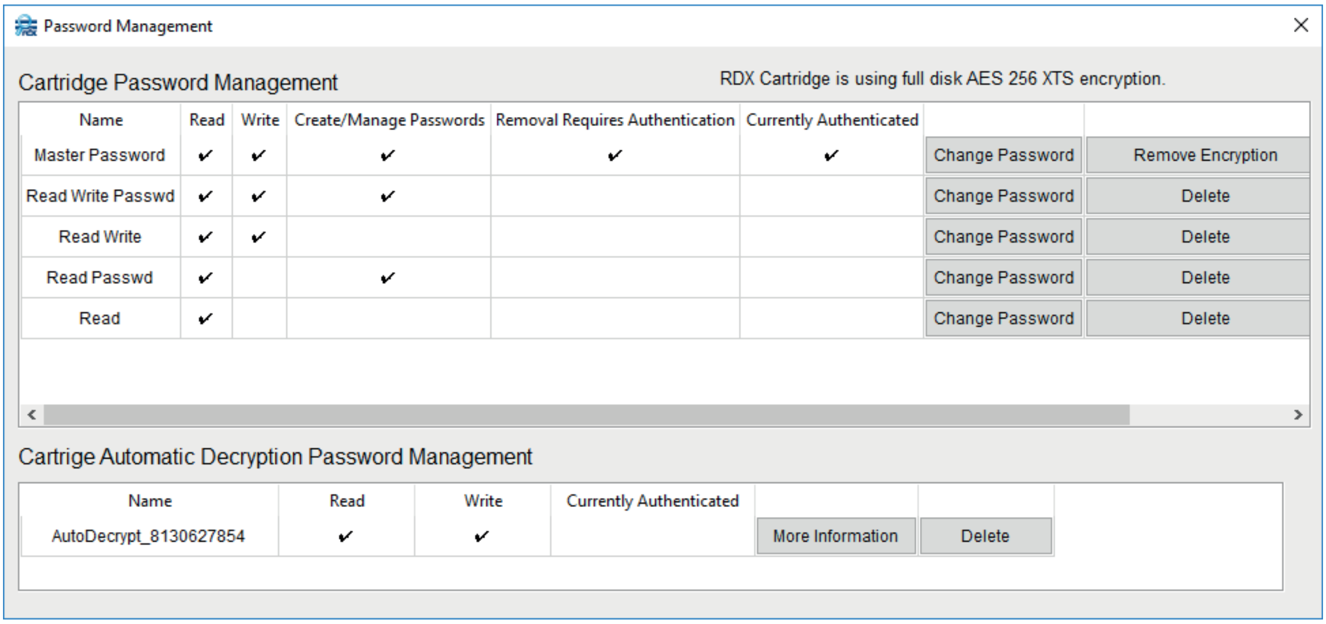
The picture shows password combinations for the basic password protection

RDX PowerEncrypt allows selectable features and functions to be deployed to different personnel in the company or to clients for secure data exchange. Based on the different authorization levels, features may be grayed out and not be selectable.

Applying the read-only data access protects the data from both virus and ransomware attacks. Read-only mode means data cannot be modified, encrypted or deleted by anyone except with the appropriate password.

Full Disk AES 256 XTS encryption

In addition to RDX media basic password protection, RDX PowerEncrypt is able to encrypt the data using AES-256 XTS encryption. Using this encryption is highly recommended if the RDX media is to be stored off-site or transported to another location. Like the RDX basic password protection feature, up to eight different passwords with dedicated data access rights and a range of functions can be assigned for different levels of access.



Password Management

Cartridge Password Management

RDX Cartridge is using full disk AES 256 XTS encryption.

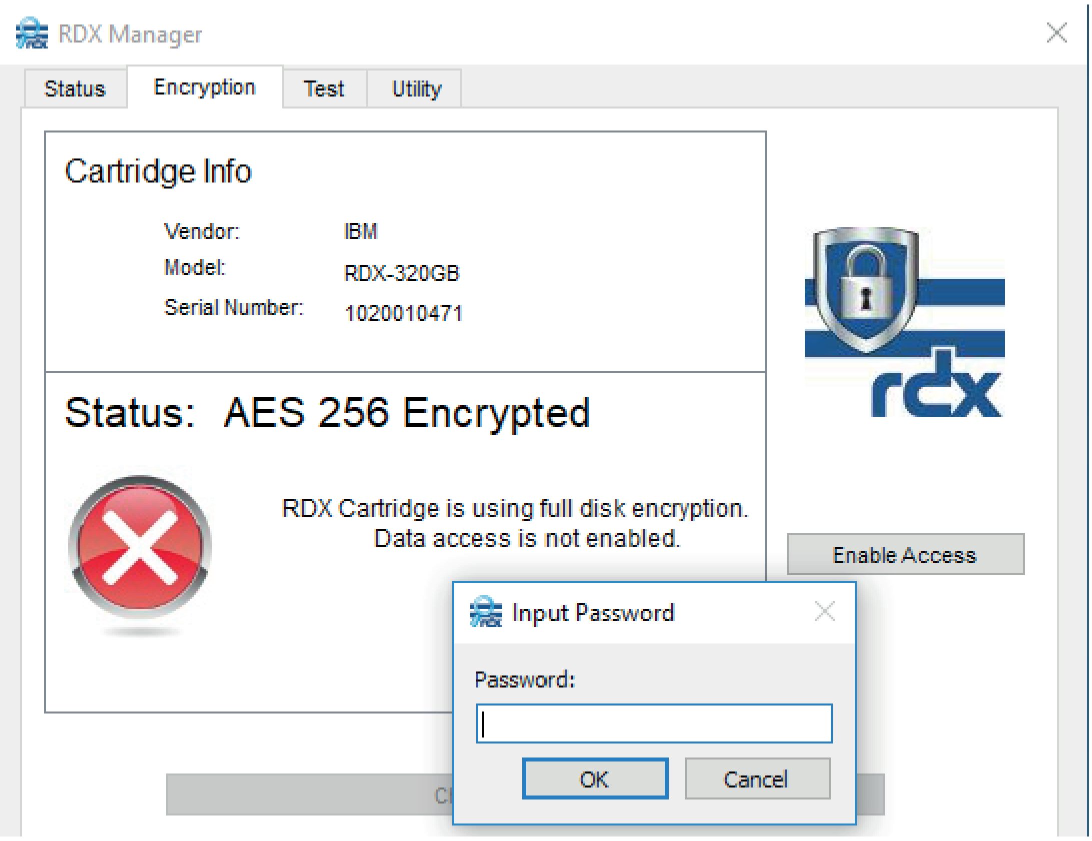
Name	Read	Write	Create/Manage Passwords	Removal Requires Authentication	Currently Authenticated		
Master Password	✔	✔	✔	✔	✔	Change Password	Remove Encryption
Read Write Passwd	✔	✔	✔			Change Password	Delete
Read Write	✔	✔				Change Password	Delete
Read Passwd	✔		✔			Change Password	Delete
Read	✔					Change Password	Delete

Cartrige Automatic Decryption Password Management

Name	Read	Write	Currently Authenticated		
AutoDecrypt_8130627854	✔	✔		More Information	Delete

The picture shows password combinations for the AES 256 XTS encryption

Usability is enhanced with the automatic-password option for the RDX drive and media. This option allows data access the moment the cartridge is inserted into a drive configured with this option. This functionality is ideal for either backup scenarios involving media rotation or bare metal recovery purposes where RDX Manager is not available to provide the data password protection. The password is held in the drive and can be used with multiple pieces of RDX media enabling restores to be spanned across a number of RDX cartridges. If necessary, the password can be securely removed from the drive at any time.



Cartridge Info

Vendor: IBM

Model: RDX-320GB

Serial Number: 1020010471

Status: AES 256 Encrypted

RDX Cartridge is using full disk encryption.
Data access is not enabled.

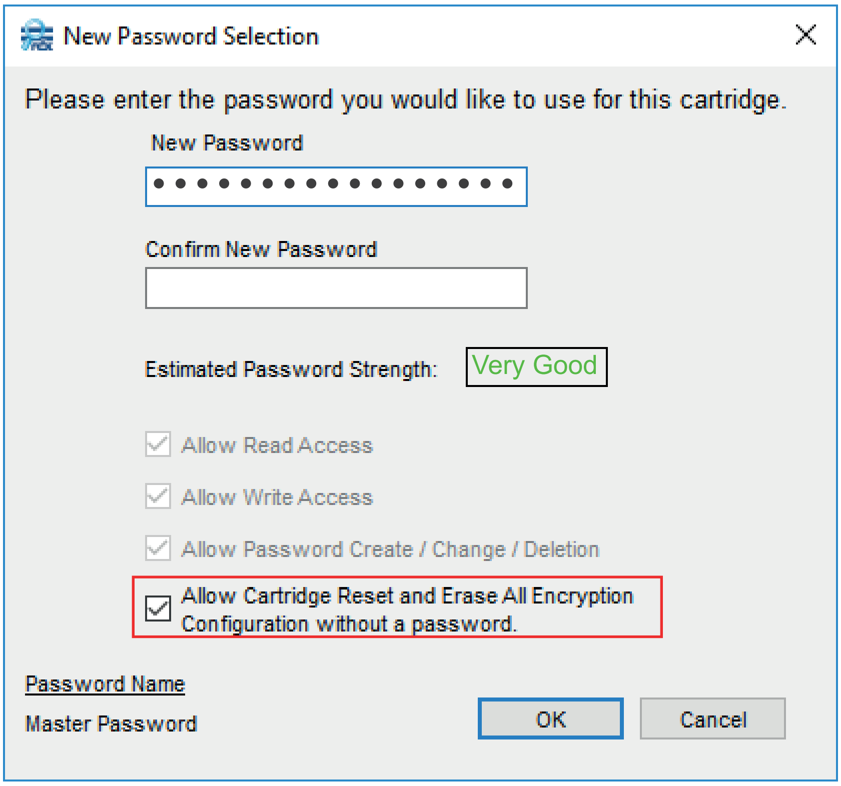
Password:

If automatoc decryption in not enabled, a password is required to access data on the RDX media

Alternatively, for data transfer between locations, there would be automatic access by the RDX drives where the password option was enabled and automatic rejection by any other RDX drives where the password option was not enabled. This keeps the data both secure and encrypted on your RDX media. Another convenient benefit is users do not have to enter a password when this option is enabled thus providing quick access to the data. If automatic decryption is not enabled, a password is required to access the data on the RDX Media.

Password considerations

As configured for security, a password is required to access the data stored on an RDX media. If the password is lost or forgotten for an encrypted RDX media, the data cannot be accessed by anyone.



Please enter the password you would like to use for this cartridge.

New Password: ●●●●●●●●●●●●●●●●●

Confirm New Password:

Estimated Password Strength: Very Good

☑ Allow Read Access

☑ Allow Write Access

☑ Allow Password Create / Change / Deletion

☑ Allow Cartridge Reset and Erase All Encryption Configuration without a password.

Password Name

Master Password

If the marked checkbox is unchecked and the password forgotten, the media becomes useless.

If the **Allow Cartridge Reset and Erase All Encryption Configuration without a password** box is ***unchecked*** and you forget your password, not only is the data inaccessible but the RDX media cannot be reformatted so the media is no longer usable. Note that forgetting your password is not covered under the RDX Media warranty.

Password strength is the key to keeping data safe. If hackers try to crack the password, it is important to use a really strong password. To assist in creating a strong password, RDX PowerEncrypt analyses the given password and shows the estimated strength (Poor, Weak, Better, Good or Very Good).

RDX PowerEncrypt evaluates a password‘s entropy based on several algorithms including common words, repeated characters, date formats, number substitution (Leet) and keyboard layout.

To achieve a strong password for RDX PowerEncrypt we recommend using the following

- At least six unrelated words used together
- Random capital letters in the words (for example, the second letter of each word)
- Symbols and numbers as separators between the words

As best practice, use a sentence with 6 or more words.

Due to advances in technology (such as faster CPU speeds, brute force attacks and dictionary attacks), password cracking is getting easier. Todays fastest computers can send about 1014 keys per second and this will only increase in the future. To counter this, RDX PowerEncrypt allows just one try per second reducing all password cracking attempts to a slow 60 attempts per minute. This greatly reduces the chance of guessing a secure user password and makes the software so robust it can even resist hacker parallel cracking techniques used to reduce cracking time.

FIPS 140-2 validation

FIPS (Federal Information Processing Standard) 140 has been issued by NIST (National Institute of Standards and Technology) to coordinate the requirements and standards for cryptography modules that include both hardware and software components.

The RDX PowerEncrypt software uses the FIPS 140-2 validated RDX SATA III drive to fulfill the standards for cryptography modules. With this validation, the RDX SATA III drive and RDX PowerEncrypt meet the legal procurement requirement and maintains the confidentiality and integrity of the information protected by the module.

Validation to the FIPS 140-2 standard ensures that the RDX SATA III drive and RDX PowerEncrypt use solid security practices, such as approved, strong encryption algorithms and methods. It also specifies how individuals or other processes must be authorized to use the product, and how modules or components must be designed to interact securely with other systems. To be FIPS 140-2 Validated, the RDX SATA III drive and RDX PowerEncrypt had to adhere to the stated design and implementation requirements and be tested and approved by one of 13 independent labs that have been accredited by NIST.

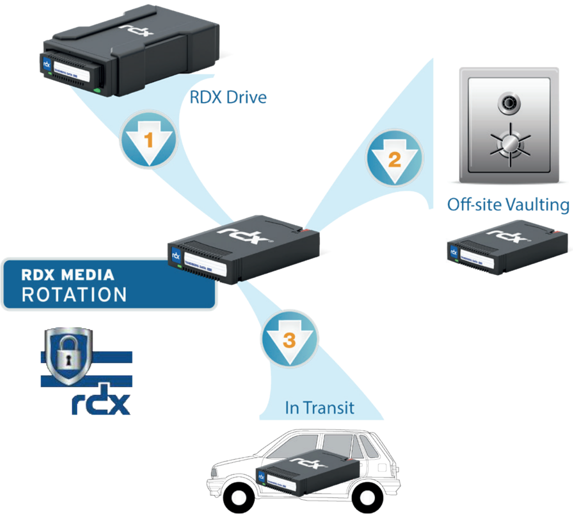
Use Cases

Backup and archive

RDX PowerEncrypt is a great fit for any backup and archiving applications. The removability of RDX media allows storing backups off-site for disaster recovery and archive purpose and can utilize a media-rotation scheme.

To protect the backups against unauthorized access while stored at another location, RDX PowerEncrypt provides the highest data protection and security of the backup set and archives. The automatic password access feature makes it easy to use the encrypted media in case of a bare metal restore is needed.

RDX media demonstrates long-term archival life of 10+ years and is an ideal solution for an archive meeting regulatory guidelines and compliance.



With RDX PowerEncrypt, data is safe and cannot be read, changed or deleted with unauthorized access.

New government regulations for Data Protection

There are new regulations being implemented like General Data Protection Regulation (GDPR). The GDPR regulates how the personal data of customers, suppliers and employees must be handled, processed and secured in our digitized world to ensure privacy.

GDPR Article 23 speaks about limiting the access to personal data to only the individuals supporting data processing, thus requiring that the data needs to be secured against unauthorized access.

GDPR Article 32, paragraph 1, describes the security of personal data by using encryption.

GDPR Article 34, paragraph 3, describes how data breaches must be communicated immediately, unless the data is encrypted. Using RDX encryption, no communication needs to take place.

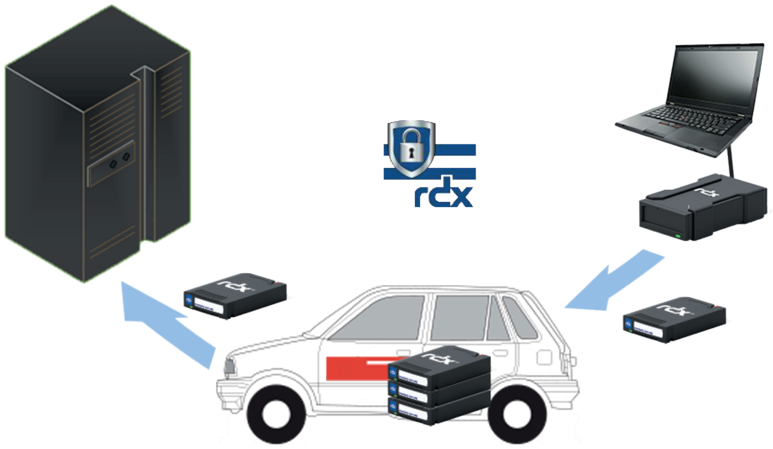
RDX PowerEncrypt provides all these functionalities. Access control is safeguarded by the different levels of access rights with password protection and data encryption ensures the highest data security.

Data transport and data exchange

The ruggedized design of RDX media facilitates transport. RDX withstands vibrations, harsh environments and drops of up to 1m on concrete floor. RDX media can be easily shipped with regular postal or transportation services. Heavy load data seeding to or from cloud resources using current network transfer rates is a challenge. An alternative to slow transfer rates over a local or wide network would be to use RDX connected to a local server for a much faster transfer.

Also, for consolidating large data from branches to a central data center, the large capacity of RDX media is a better solution than network transfers.

During transit, if RDX media is stolen, the unencrypted data written on this media could be breached. Sensitive data from companies or governments needs to be protected. RDX PowerEncrypt provides a powerful solution for protecting such data assets.



Conclusion

With its easy administration and full functionality, RDX PowerEncrypt can be can be Implemented in a wide range of personal, small business or corporate applications. This built-in password protection functionality for RDX QuikStor SATA III drives is an included value. RDX PowerEncrypt ensures the highest confidence for data protection with industry-leading and regulatory-compliant AES-256 XTS encryption along with access-control options.

Validated compliant to FIPS 140-2 standards for cryptography, RDX PowerEncrypt is an acceptable solution for international industry regulatory agencies in charge of data security. RDX PowerEncrypt is compatible with a broad range of applications like backup and recovery, archiving, data transportation and data exchange.

RDX PowerEncrypt is currently available for internal RDX QuikStor SATA III drives with firmware level 0253 or later along with the new RDX Manager software utility. Per our extensive product development roadmap, it will be available soon for other RDX products as well.

Sales and support for Overland-Tandberg products and solutions are available in over 90 countries.
Contact us today at sales@overlandstorage.com or sales@tandbergdata.com