



RDX Manager Product Manual



©2019 Overland-Tandberg™. All rights reserved.

Overland®, Overland Storage®, DynamicRAID®, NEO®, NEO Series®, PowerLoader®, RAINcloud®, RapidRebuild®, REO 4000®, REO Series®, VR2®, and XchangeNOW® are registered trademarks of Overland Storage, Inc.

Tandberg®, Tandberg Data®, AccuGuard®, AccuVault®, BizNAS®, QuadPak®, QuikStation®, QuikStor®, RDX®, RDXPRESS®, RDXPRO®, StorageLoader®, SupportSuite®, Tandberg SecureService®, and Tandberg StorageLibrary® are registered trademarks of Tandberg Data Holdings S.A.R.L.

Overland-Tandberg™ is a trademark of Overland Storage, Inc.

All other brand names or trademarks are the property of their respective owners.

The names of companies and individuals used in examples are fictitious and intended to illustrate the use of the software. Any resemblance to actual companies or individuals, whether past or present, is coincidental.

PROPRIETARY NOTICE

The information contained in this document is subject to change without notice.

All information contained in or disclosed by this document is considered proprietary by Overland-Tandberg. By accepting this material the recipient agrees that this material and the information contained therein are held in confidence and in trust and will not be used, reproduced in whole or in part, nor its contents revealed to others, except to meet the purpose for which it was delivered. It is understood that no right is conveyed to reproduce or have reproduced any item herein disclosed without express permission from Overland-Tandberg.

Overland-Tandberg provides this manual as is, without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Overland-Tandberg may make improvements or changes in the product(s) or programs described in this manual at any time. These changes will be incorporated in new editions of this publication.

Overland-Tandberg assumes no responsibility for the accuracy, completeness, sufficiency, or usefulness of this manual, nor for any problem that might arise from the use of the information in this manual.

FW 0.1.0.33

REVISION HISTORY

Revision	Date	Description
Rev A	April 2018	Initial release
Rev B	July 2018	Minor content changes and updates
Rev C	February 2018	Added features command line options & silent install
Rev D	October 2019	How to switch GUI language & password protection updates

Overland-Tandberg
4542 Ruffner Street, Suite 250
San Diego, CA 92111 USA

TEL 1.800.729.8725 (toll free)
1.858.571.5555
FAX 1.858.571.3664

Tandberg Data
Feldstraße 81
44141 Dortmund, Germany

TEL +49 231 5436 0
FAX +49 231 5436 111



www.overlandtandberg.com



Preface

Audience and Purpose

This guide describes how to install and use the RDX Manager software as intended in a network environment. Familiarity with system and network configuration is highly recommended.

The information in this guide applies to both the SATA III and USB 3.0 versions of RDX QuikStor.

Organization

The following chapters are included in this guide:

- [Chapter 1, “Product Information,”](#) provides an overview of the features of the RDX Manager.
- [Chapter 2, “Installation,”](#) describes information on how to install and initially configure RDX Manager.
- [Chapter 3, “RDX Manager Drive List,”](#) describes how to access RDX drives and their settings.
- [Chapter 4, “Management Pop-up Window,”](#) describes using the Management Pop-up Window for configuration tasks, such as encryption and user account management.
- [Appendix A, “Troubleshooting,”](#) provides basic troubleshooting information.

Product Documentation & Updates

Product documentation and additional information are available online at our Knowledge Base website:

<https://www.overlandtandberg.com/knowledgebase/>

Select:

- **Product Type = RDX Solutions**
- **Product Family = RDX Software**
- **Model = All**

Use **Document Type** to select the document for which you are specifically looking. For additional information about the RDX Manager, refer to the following publications:




- *RDX Manager Product Manual*
- Various other RDX QuikStation Knowledge Base articles such as regulatory documents and technical bulletins.

To download drivers and software updates, see the [Drivers and Downloads](#) page.

Conventions

This document exercises several alerts and typographical conventions.

Alerts

Convention	Description & Usage
NOTE: Text	A Note indicates neutral or positive information that emphasizes or supplements important points of the main text. A note supplies information that may apply only in special cases, for example, memory limitations or details that apply to specific program versions.
 IMPORTANT	An Important note is a type of note that provides information essential to the completion of a task or that can impact the product and its function.
 CAUTION	A Caution contains information that the user needs to know to avoid damaging or permanently deleting data or causing physical damage to the hardware or system.
 WARNING	A Warning contains information concerning personal safety. Failure to follow directions in the warning could result in bodily harm or death.
WARNUNG	Eine <i>Warnung</i> enthält Informationen zur persönlichen Sicherheit. Das Nichtbeachten der Anweisungen in der Warnung kann zu Verletzungen oder zum Tod führen.
AVERTISSEMENT	Un Canadien avertissement comme celui-ci contient des informations relatives à la sécurité personnelle. Ignorer les instructions dans l'avertissement peut entraîner des lésions corporelles ou la mort.

Typographical Conventions

Convention	Description & Usage
Button_name	Words in this special boldface font indicate command buttons found in the Remote Management Interface (RMI) or Operator Control Panel (OCP).
Ctrl-Alt-R	Denotes the keys that you press simultaneously. In this example, hold down the Ctrl and Alt keys and press the R key.
Menu Flow Indicator (>)	Words with a greater than sign between them indicate the flow of actions to accomplish a task. For example, Setup > Passwords > User indicates that you should press the Setup button, then the Password button, and finally the User button to accomplish a task.
<i>Courier Italic</i>	Used to exemplify a variable for which you must substitute a value.
Courier Bold	Represents commands or text in a command-line interface (CLI).

Information contained in this guide has been reviewed for accuracy, but not for product warranty because of the various environments, operating systems, or settings involved. Information and specifications may change without notice.

Technical Support

You can get additional technical support information on the [Contact Us](#) web page at:

<https://www.overlandstorage.com/company/contact-us/index.aspx>

For a complete list of support types, levels, and times, visit our website at:

http://support.overlandstorage.com/support/overland_care.html



Contents

Preface

Organization	3
Conventions	4
Technical Support	5

Chapter 1: Product Information

Overview	8
RDX Manager Drive List	8
Management Pop-up Window	9
Key Features	9

Chapter 2: Installation

RDX Manager Software Download	10
Install RDX Manager	10
Launch RDX Manager	11
Uninstall RDX Manager	11

Chapter 3: RDX Manager Drive List

Overview	12
RDX Manager Drive List Window	13
Menu Options	13
Exit	13
Auto Scan	13
Help Options	13
Management Pop-up Window Access	13
RDX Manager Drive List Update	14

Chapter 4: Management Pop-up Window

Status Tab	15
Status Drive Data	16
Status Cartridge Data	16
Encryption Tab	17
Enable Cartridge Encryption or Password Protection	17
How to Choose a Strong Password	20
Disable/Enable Cartridge Access	20
Disable Access	21
Enable Access	21
Change Protection Password	22
Remove Encryption or Password Protection	24
Remove AES 256 XTS Encryption	24
Remove Basic Password Protection	25

Advanced Options	25
Add a Password	26
View/Modify/Delete Existing Passwords	27
Add an Automatic Drive Media Authentication Password	28
Delete Automatic Drive Media Authentication from RDX Drive	30
Test Tab	31
Self Test	31
Self Test Recommendations	32
LED Test	32
Write/Read Test	32
Utility Tab	32
Update Firmware	33
Update Procedure	33
Partition and Format Cartridge	34
Windows 7 or Higher	34
Apple OSX	34
Change Drive Mode	34
Change SATA III Mode	35
Eject Cartridge	35

Appendix A: Troubleshooting

Basic Troubleshooting	36
Check for Firmware Updates	36
Cannot Write to a Cartridge	36
Read-Only RDX Cartridge Not Readable on SATA I and SATA III Drives	36
Recommended Way to Change/Upgrade SATA Driver	36
Command Line Eject Feature (rdxcmdline.exe)	37
Command Line Language Selection	37
Optional Shortcut	38
Technical Support	38

Index

1

Product Information

RDX Manager is a utility from Overland-Tandberg that allows easy management and configuration of RDX drives and cartridges. RDX Manager provides options to optimize RDX for specific storage requirements and incorporates compatibility with your operating system. RDX Manager also provides easy cartridge encryption and password protection to safeguard your data.

Supported OS versions include Windows 7, Windows 8, Windows 10, Server 2008, Server 2012, Server 2012R2, and Server 2016.

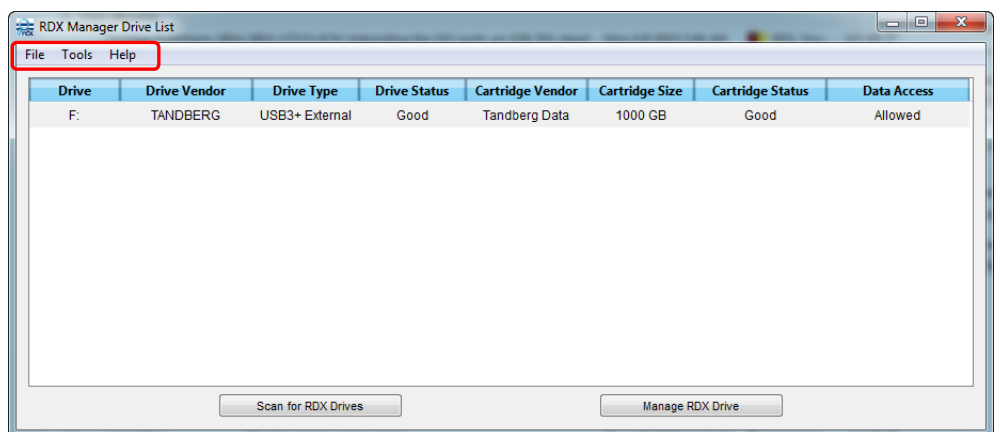
Topics in Product Information:

- [Overview](#)
- [Key Features](#)

Overview

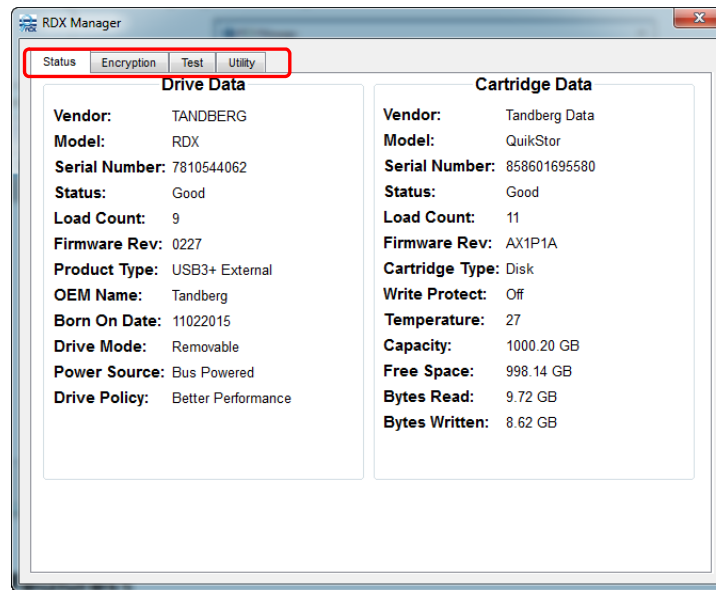
The RDX Manager utility consists of two parts: an RDX Manager Drive List to access all connected RDX devices and a Management Pop-up Window with options for configuration and management of individual devices.

RDX Manager Drive List



This window displays a table listing all RDX devices found on this system. A menu provides access to additional options. For a complete list of options, see [Chapter 3, “RDX Manager Drive List,”](#) on page 12.

Management Pop-up Window



This pop-up window provides all the management tools for your RDX devices with each tool on a different tab. For a complete list of options, see [Chapter 4, “Management Pop-up Window,” on page 15.](#)

Key Features

- Free and simple download and installation from the Overland-Tandberg website: <http://www.tandbergdata.com/us/index.cfm/products/data-protection-software/>
- For Windows users, it works with Windows 7, Windows 8, Windows 10, Server 2008, Server 2012, Server 2012R2, or Server 2016.
- For Apple users, it works with OS X 10.11 through OS X 10.13.
- Compatibility with all RDX cartridge generations and capacities.
- Both full disk AES 256 XTS encryption and basic password protection available.
- Multiple diagnostic test and service features.
- Flexible RDX media partition and format options.
- Remote RDX media eject option.

2

Installation

This section covers the installation of the RDX Manager software.

NOTE: Administrative rights are required to install, configure, license, and update RDX Manager. When installing RDX Manager on Windows 7 or Windows 2008 Server (or higher), you need to be logged in as Administrator or to run the installation program using the **Run as administrator** context menu option.

Topics in Installation:

- [RDX Manager Software Download](#)
- [Install RDX Manager](#)
- [Launch RDX Manager](#)
- [Uninstall RDX Manager](#)

RDX Manager Software Download

The RDX Manager software and release notes can be downloaded from the Overland-Tandberg FTP website:

1. Go to the FTP website (<ftp://ftp1.overlandtandberg.com/rdx>).
The link can also be accessed from the regular website:
<http://www.tandbergdata.com/us/index.cfm/products/removable-disk/rdx-quickstor/>
In the right column, click **Downloads** and then click the “Click here” link shown.
2. At the FTP site, click **RDX Manager**.
3. Depending on your OS, click either **Mac** or **Windows**.
4. To automatically download the files, click the **release notes PDF link** and then the **installer ZIP link**.

Make a note of the location of where you downloaded the files.

Install RDX Manager

NOTE: To install the RDX Manager in “silent mode,” use an Admin command shell and run the command “RDXManagerInstaller_0.1.0.30.exe isSilent=true” making sure to use the exact case and spacing shown. No user interaction is required when running a silent mode install.

To install RDX Manager onto your RDX dock:

1. Open the ZIP file and double-click the **EXE file** to launch the installation wizard.
2. At Welcome screen, click **Next**.

3. Accept the default installation folder by clicking **Next**.
4. Accept the RDX Manager component for installation by clicking **Next**.
5. Accept the license by clicking the button and then clicking **Next**.
6. Accept the Start Menu shortcut by clicking **Next**.
7. At the installation confirmation screen, click **Install**.
8. Click **Finish**.

Launch RDX Manager

The RDX Manager EXE file (RDXManager.exe) is located at:

C:\Program Files (x86)\Overland-Tandberg\RDXManager\Manager\

For easy access, a quick access icon was created during installation on the bottom task bar:



Click the RDX Manager icon to launch the software and open the RDX Manager Drive List screen.

Uninstall RDX Manager

NOTE: You must exit RDX Manager before it can be uninstalled.

You can uninstall RDX Manager using the Windows Programs and Features:

1. Click **Start > Control Panel > Programs and Features**.
2. From the list of programs, select the RDX Manager product and click **Uninstall (or Remove)**.
3. At the first confirmation screen, click **Yes**.
4. At the second confirmation screen, click **Yes** again.
During uninstall, a status screen shows the progress.

3

RDX Manager Drive List

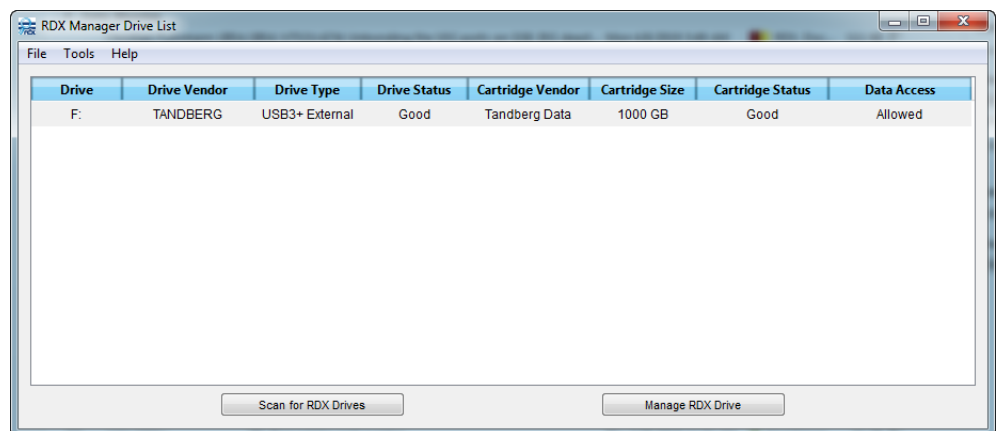
The RDX Manager Drive List displays a table of all RDX devices connected to your computer.

Topics in RDX Manager Drive List:

- [Overview](#)
- [RDX Manager Drive List Window](#)
- [Management Pop-up Window Access](#)
- [RDX Manager Drive List Update](#)

Overview

RDX Manager Drive List allows for the management of your RDX devices in a single place. It shows a window with a table listing all discoverable RDX devices.



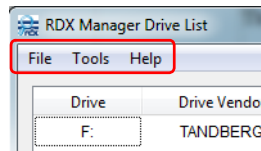
The RDX Manager Drive List consists of:

- Three menu options (**Files**, **Tools**, and **Help**) located at the top of the window.
- A table with rows showing information about the installed RDX drives and any inserted cartridges.
 - **Drive** – The drive letter used by the RDX
 - **Drive Vendor** – Maker of the drive
 - **Drive Type** – Product type of drive
 - **Drive Status** – Current status of the drive
 - **Cartridge Vendor** – Capacity of a cartridge (if in the drive)
 - **Cartridge Size** – Type of cartridge (if in the drive)
 - **Cartridge Status** – Current status of the cartridge (if in the drive).

- **Data Access** – Indicates if data access is allowed.
- Two buttons at the bottom (**Scan for RDX Drives** and **Manage RDX Drive**).

RDX Manager Drive List Window

Menu Options



There are three main menu options for the RDX Manager Drive List window:

- **File** – Provides the Exit option.
- **Tools** – Provides the Auto Scan feature.
- **Help** – Provides options for Help (F1), About, Check for Updates, and (Technical) Support.

Exit

Clicking **File > Exit** results in the closing of RDX Manager Drive List.

Auto Scan

Clicking **Tools > Auto Scan** scans the network for RDX drives the same as the **Scan for RDX Drives** button. This scan occurs once per second.

Help Options

There are four submenu items under the **Help** menu:

- **Help (F1)** – Clicking this option is the same as pressing the **F1** function button. The RDX Manager online help opens in a new window.
- **About** – Opens an About dialog that shows the current version number and copyright date.
- **Check for Updates** – Checks the Overland-Tandberg website to determine if a newer version of RDX Manager or the drive firmware exists.
- **Support** – Opens the RDX Manager Support dialog with a **Generate RDX System Summary** button. See [Appendix A, “Technical Support,”](#) on page 38.

Management Pop-up Window Access

Click either the **Manage RDX Drive** button or a table row to open the Management Pop-up Window to do any of the following:

- See a detailed status of the drive/cartridge.
- Encrypt or password protect a cartridge.
- Run drive tests.
- Run drive utility functions.

For more information, see [Chapter 4, “Management Pop-up Window,”](#) on page 15.

RDX Manager Drive List Update

Click **Scan for RDX Drives** to scan for RDX drives or update current drive information in the table.

4

Management Pop-up Window

At the RDX Manager Drive List, clicking either the **Manage RDX Drive** button or a row in the table opens the Management Pop-up Window. The window has four tabs for managing your RDX devices—**Status**, **Encryption**, **Test**, and **Utility**. The default view is the **Status** tab.

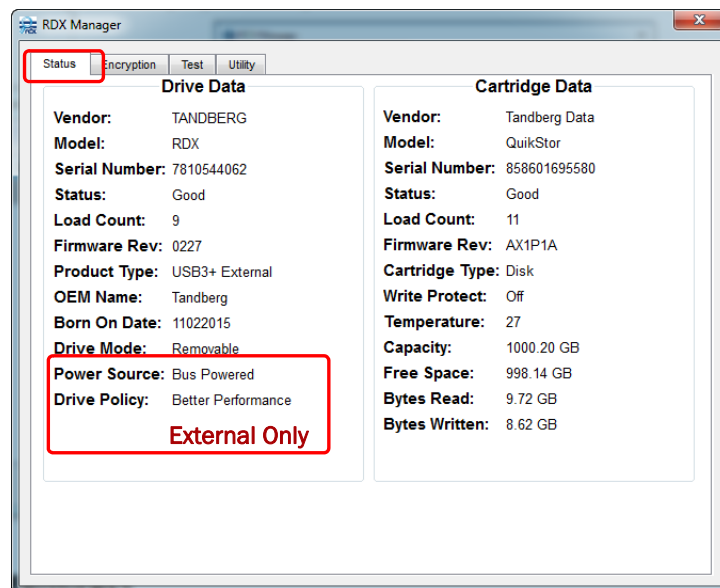
NOTE: As long as this window is open, the RDX Device Window cannot be accessed.

Topics in Management Pop-up Window:

- [Status Tab](#)
- [Encryption Tab](#)
- [Test Tab](#)
- [Utility Tab](#)

Status Tab

The **Status** tab is the default view in the Management Pop-up Window.



It shows two data sets:

- **Drive Data** – On the left, the basic information for the RDX drive that was selected from the RDX Manager Drive List table.
- **Cartridge Data** – On the right, the basic information for the RDX media currently in the selected drive. If no media is in the drive, the Cartridge Data side only shows a Status of **No Media**. The other items are blank.

Status Drive Data

The Drive Data area of the **Status** tab lists the following information:

Field	Content
Vendor:	The drive vendor name (for example, TANDBERG)
Model:	The drive model (RDX)
Serial Number:	The drive serial number
Status:	The drive status (Good or Drive Error)
Load Count:	The total number of times media was loaded in this drive
Firmware Rev:	The current drive firmware revision
Product Type:	The type of product (for example, USB3, USB3+, or SATA-III)
OEM Name:	Indicates if the firmware is specific to an OEM (for example: Tandberg)
Born On Date:	The date the drive was manufactured (may be blank on older models)
Drive Mode:	The drive's operation mode (Removable or Fixed)
Power Source (External Only)	USB 3.0 external drive power source (Adapter Powered or Bus Powered)
Drive Policy (External Only)	The policy governing the drive's performance.

Status Cartridge Data

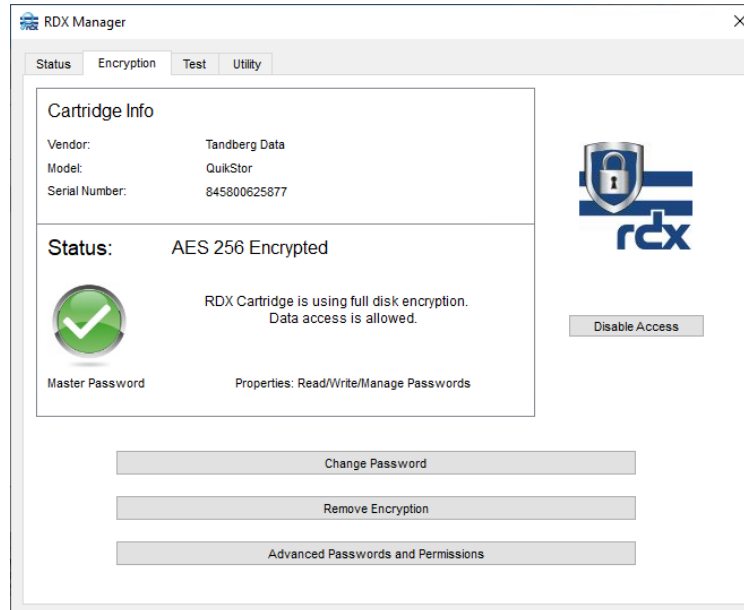
The Cartridge Data area of the **Status** tab lists the following information:

Field	Content
Vendor:	The cartridge vendor name (for example, Tandberg Data)
Model:	The cartridge model (for example, QuikStor)
Serial Number:	The cartridge serial number
Status:	The cartridge status (Good or Cartridge Error)
Load Count:	The total number of times this cartridge was loaded
Firmware Rev:	The firmware revision of the HDD inside the cartridge
Cartridge Type:	Type of cartridge (Disk)
Write Protect:	The Write Protect state of the cartridge (OFF = writing enabled, ON = writing disabled)
Temperature:	The cartridge temperature reported in degrees centigrade (C)
Capacity:	The total cartridge user data space (available space and space in-use)
Free Space:	The amount of unused, available cartridge user data space
Bytes Read:	The total number of bytes read from the cartridge
Bytes Written:	The total number of bytes written to the cartridge

Encryption Tab

The **Encryption** tab in the Management Pop-up Window shows two information fields:

- **Cartridge Info** – The cartridge primary information (**Vendor**, **Model**, and **Serial Number**).
- **Status** – The protection status (such as, **AES 256 Encrypted** or **Not Encrypted**).



NOTE: If the RDX drive had previously been enabled for automatic drive media authentication, the **Advanced Passwords and Permissions** button will also be visible.

There are two types of cartridge data protection available:

- **Full Disk AES 256 XTS Encryption** – All data stored on the cartridge is encrypted using the XTS-AES 256 encryption standard (recommended).
- **Basic Password Protection** – Access to the cartridge and its data is protected by a single password.



IMPORTANT: When using the **Basic Password Protection** option, data on the cartridge is **NOT** encrypted and is only protected by a password.

Topics in Encryption Tab:

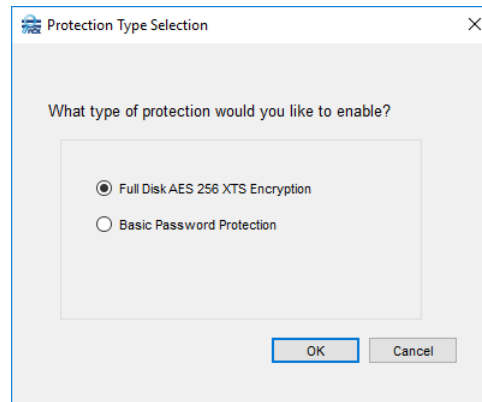
- [Enable Cartridge Encryption or Password Protection](#)
- [Disable/Enable Cartridge Access](#)
- [Change Protection Password](#)
- [Remove Encryption or Password Protection](#)
- [Advanced Options](#)

Enable Cartridge Encryption or Password Protection

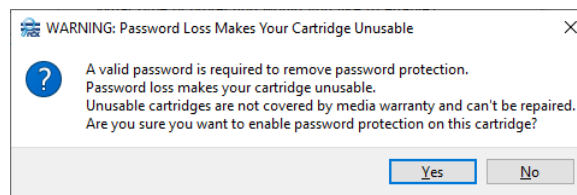
To apply a protection type:

1. At the default **Encryption** tab, click **Enable Cartridge Encryption/Password Protection**.

- At the **Protection Type Selection** dialog box, select your protection **type**.



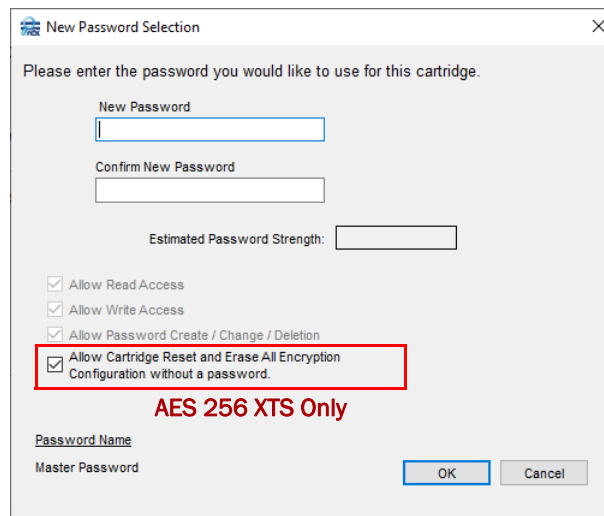
- If **Basic Password Protection** is selected, at the pop-up warning about losing your password, select **Yes** to continue.



Clicking **Yes** accepts the Basic Password Protection selection while clicking **No** clears the Basic Password Protection selection and returns you to the Protection Type Selection dialog box.

CAUTION: If you lose your password, the media becomes unusable and a media reset is not possible. Forgetting your password is not covered under our product warranty.

- Click **OK** to continue.
- At the **New Password Selection dialog** that opens (AES 256 XTS screen shown here), perform the following steps.



- a. **Enter and confirm** a password for the protection type.
As the new password is entered, its estimated strength is shown (**Poor, Weak, Better, Good, or Very Good**). See [“How to Choose a Strong Password”](#) on page 20.

- b. For the AES 256 XTS encryption option, to make sure the cartridge can be erased, **uncheck** the **Allow Cartridge Reset and Erase All Encryption Configuration Without a Password** box.

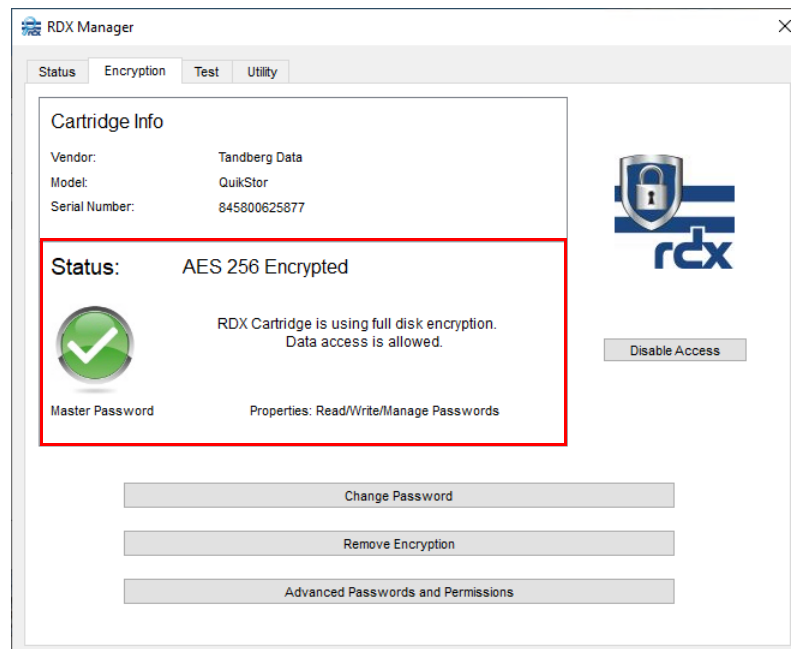
Otherwise, this prevents anyone with physical access to the cartridge from permanently deleting all encrypted contents and reusing the cartridge. When this box is checked, any password for the cartridge (including a read-only password) can be used to securely erase the cartridge.



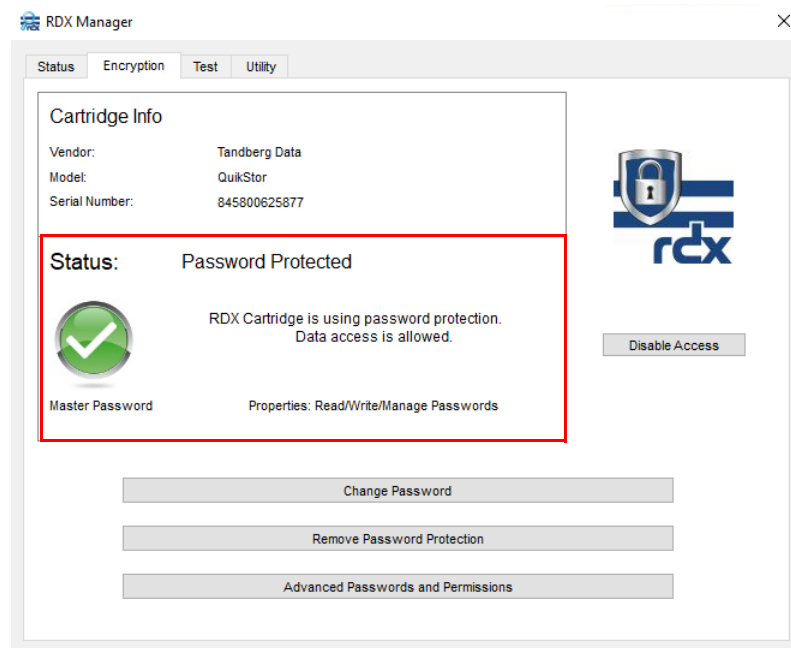
CAUTION: If you lose the passwords for your RDX cartridge, it cannot be erased and is no longer usable. Data recovery services are both excluded and impossible. Forgetting your password is not covered under our product warranty.

- c. Click **OK** to accept the changes.
6. For **AES 256 XTS encryption only**, at the Cartridge Format Selection dialog box, select either **NFTS** or **exFAT**, and click **OK**.
7. At the Confirmation dialog box, verify the **settings** are correct and click **OK**.
A progress bar for enabling protection on the cartridge is shown. When done, the cartridge is protected and you are returned to the **Encryption** tab which displays the type of protection selected.

AES 256 XTS Encryption Enabled:



Basic Password Protection Enabled:



How to Choose a Strong Password

When adding or changing a password in RDX Manager, an Estimated Password Strength is shown below and to the right of the password fields.

Traditionally, a password was considered to be strong if it met these four qualities:

- Had, at a minimum, 12 characters (longer is better).
- Includes uppercase letters, lowercase letters, numbers, and symbols.
- Did not include words or combinations of words found in the dictionary.
- Did not have obvious letter substitutions (such as “3” for “E”).

However, due to the advances in technology that makes password cracking easier, the latest trend is to have the following criteria:

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

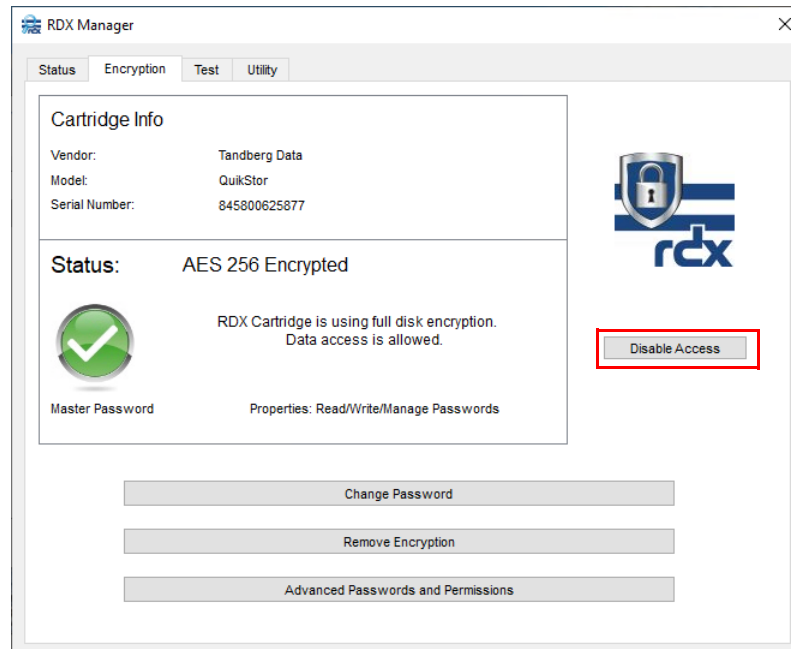
The password strength indicator built into RDX Manager uses text descriptors (**Poor**, **Weak**, **Better**, **Good**, or **Very Good**) to help you find a strong password.

Disable/Enable Cartridge Access

If encryption or password protection has been enabled, you can turn cartridge data access off and on. The access button is located on the right side of the **Encryption** tab.

Disable Access

Once encryption or password protection has been set, the access button shows **Disable Access**.



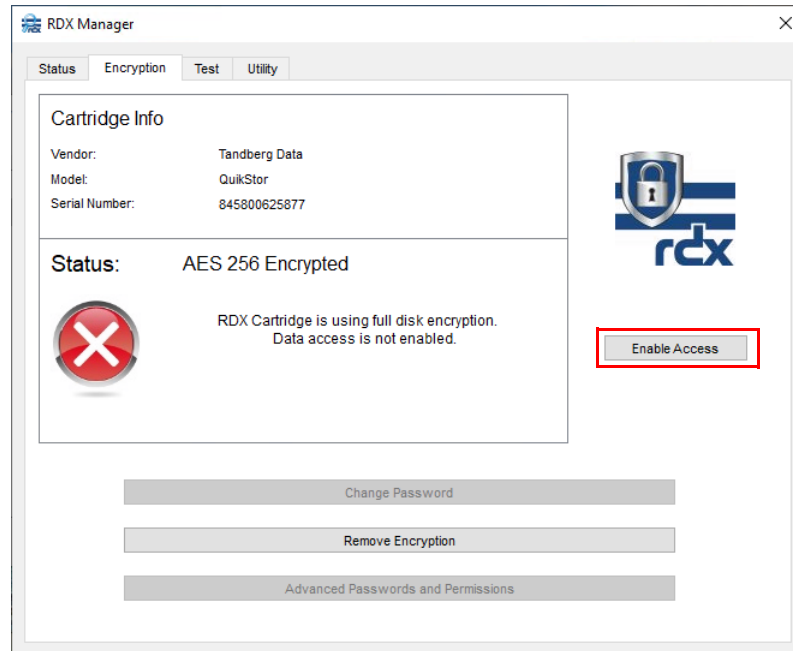
To disable access:

1. Click the **Disable Access** button.
2. At the Access Disabled pop-up message, click **OK**.

Access is now disabled, a large red icon with an "X" is shown in the Status information field, and the access button changes to **Enable Access**.

Enable Access

If access to the media has been disabled, the access button then shows **Enable Access**.



To enable access:

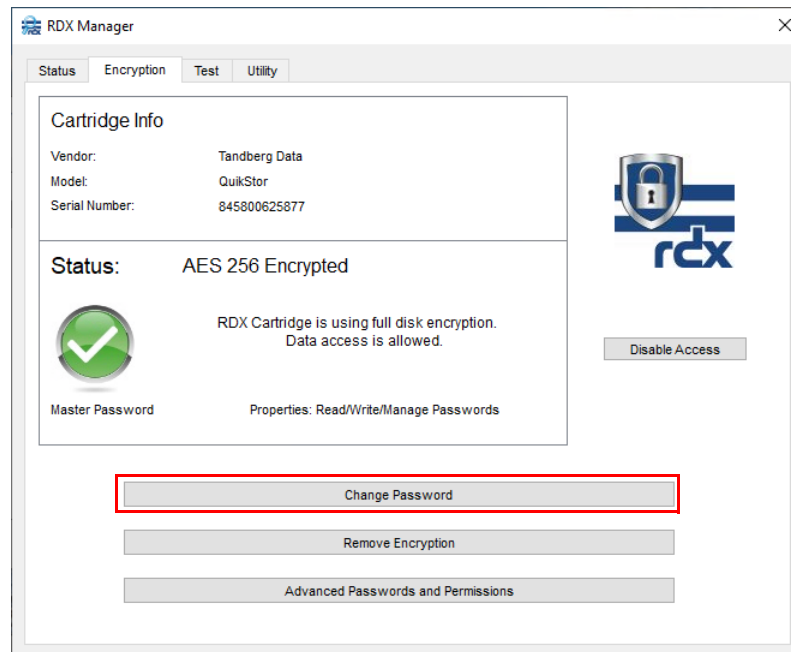
1. Click the **Enable Access** button.
2. At the Input Password dialog box, enter your **password** and click **OK**.

Access is now enabled, a large **green** icon with a check mark symbol is shown in the Status information field, and the access button changes to **Disable Access**.

Change Protection Password

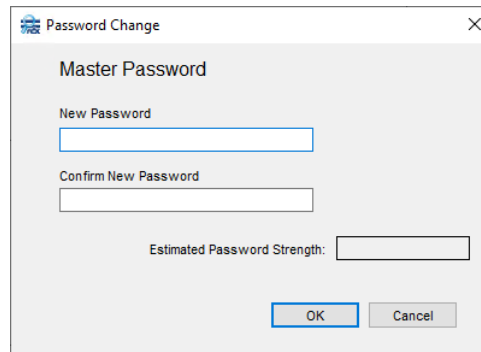
NOTE: If access is disabled, to activate the buttons at the bottom of the **Encryption** tab, click **Enable Access** and use the current password to access the cartridge.

The protection password can be changed for both AES 256 XTS encryption and basic password protection.



1. Click **Change Password**.

The **Password Change** dialog box is displayed.



2. Enter and confirm a new **Master Password**.

As the new password is entered, its estimated strength is shown (**Poor**, **Weak**, **Better**, **Good**, or **Very Good**). See [“How to Choose a Strong Password”](#) on page 20.

3. Click **OK**.

4. At the Confirmation dialog box, click **OK**.

A progress bar for changing the password is shown. When done, the new password is in effect.

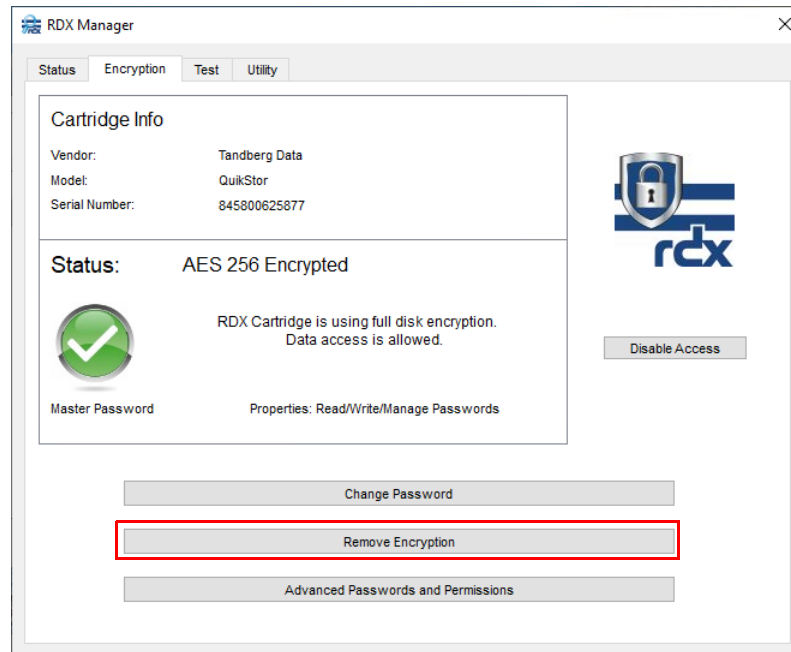


CAUTION: If you lose your password, the media becomes unusable and a media reset is not possible. Forgetting your password is not covered under our product warranty.

Remove Encryption or Password Protection

NOTE: If access is disabled, to activate the buttons at the bottom of the **Encryption** tab, click **Enable Access** and use the current password to access the cartridge.

Cartridge data protection (AES 256 XTS encryption or basic password protection) can be removed.

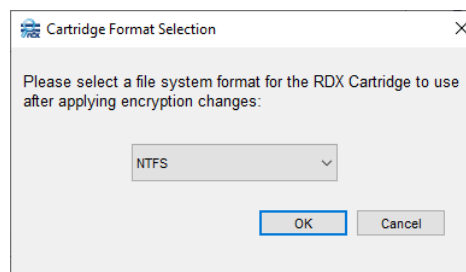


The two different procedures [Remove AES 256 XTS Encryption](#) (page 24) and [Remove Basic Password Protection](#) (page 25) follow.


Remove AES 256 XTS Encryption

1. Click the **Remove Encryption** button.

The **Cartridge Format Selection** dialog box is displayed.




2. At the dialog box, select either **NTFS** or **exFAT**, and click **OK**.
3. For AES 256 XTS, to permanently delete all data and reformat the cartridge, at the removal Confirmation dialog box, click **OK**.

 **CAUTION:** As soon as you confirm the removal of the encryption, this option completely deletes all the passwords and all the data, and then repartitions and reformats the RDX cartridge. **There is no undo option.** Any data on the cartridge is **permanently lost** and is not recoverable as the data was only readable with passwords that were initially used to generate the unique encryption key.

A progress bar for removing encryption on the cartridge is shown. When done, the cartridge is no longer protected and you are returned to the **Encryption** tab.

Remove Basic Password Protection

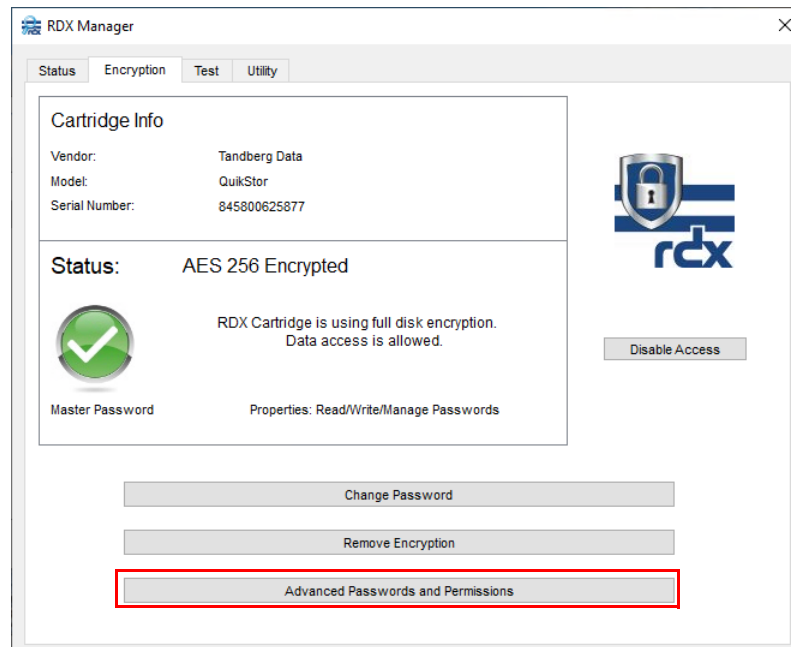
1. Click the **Remove Password Protection** button.
2. At the password protection removal Confirmation dialog box, click **OK**.

 **IMPORTANT:** This operation doesn't delete any data and, after the password is removed, the data can be accessed normally.

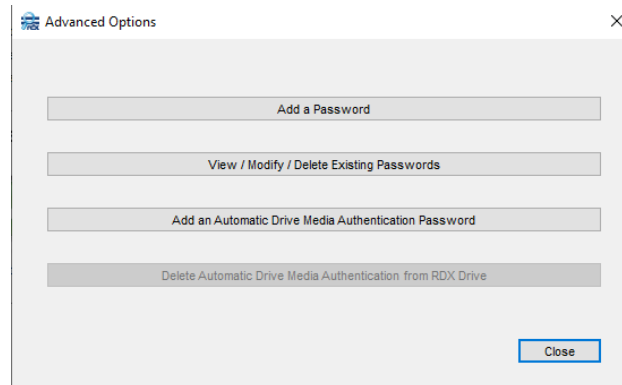
A progress bar for removing password protection is shown. When done, the cartridge is no longer protected and you are returned to the **Encryption** tab.

Advanced Options

NOTE: If access is currently disabled, to activate the buttons at the bottom of the **Encryption** tab, click **Enable Access** and use the current password to access the cartridge and the **Advanced Passwords and Permissions** button.



Clicking the **Advanced Passwords and Permissions** button displays a dialog box with four advanced configurable options:



- [Add a Password](#)
- [View/Modify/Delete Existing Passwords](#)
- [Add an Automatic Drive Media Authentication Password](#)
- [Delete Automatic Drive Media Authentication from RDX Drive](#)

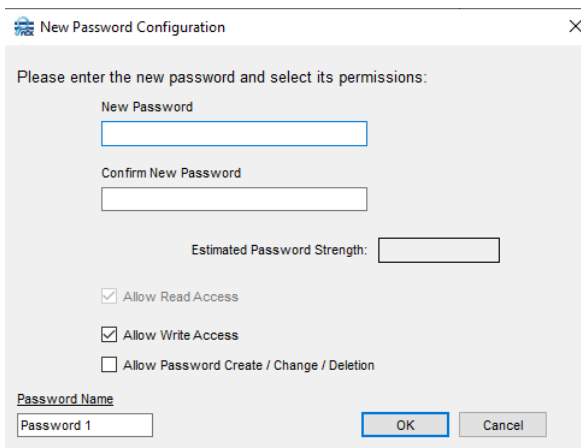
When done, click **Close** to return to the **Encryption** tab.

The procedures for configuring these advanced options follow.

Add a Password

Use this option to configure additional passwords for cartridge access with different permissions. Up to eight passwords can be configured per cartridge (one Master Password and up to seven additional or automatic authentication passwords).

1. Click **Add a Password** to open the **New Password Configuration** dialog box for adding a password.

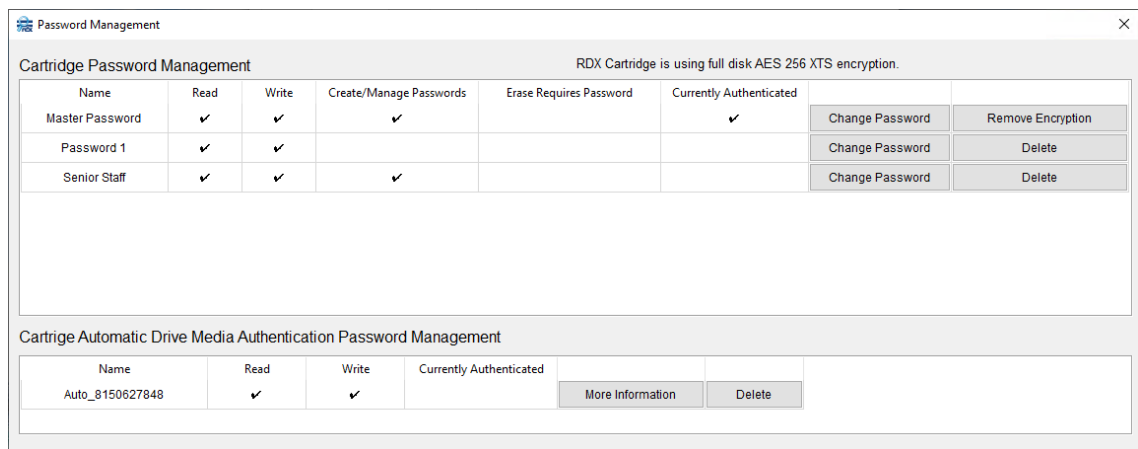


2. Enter and confirm a **new password** for Read Access.
As the new password is entered, its estimated strength is shown (**Poor, Weak, Better, Good, or Very Good**). See [“How to Choose a Strong Password”](#) on page 20.
3. If required, add **other options** by checking the appropriate boxes:
 - **Allow Write Access**
 - **Allow Password Create / Change / Deletion**

4. At the lower left, you can change the **default name** of the new password in the **Password Name** field.
5. Click **OK** to accept the settings.
6. At the Confirmation dialog box, click **OK**.
A progress bar for adding an additional password is shown. When done, the new password is immediately in effect and you are returned to the **Advanced Options** dialog box.

View/Modify/Delete Existing Passwords

Select this option to view and manage your cartridge password settings for both encryption and basic password protection. Click **View/Modify/Delete Existing Passwords** to open the **Password Management** window.



Use one of the following procedures:

- To **change** any password (including the Master Password):
 - a. On the right side of the password's table row, click **Change Password**.
 - b. Enter and confirm a **new password**.
 - c. Click **OK** to accept the new password.
 - d. At the Confirmation dialog box, click **OK**.
A progress bar is shown. When done, the new password is immediately in effect and you are returned to the **Password Management** window.
- To **delete** a regular (non-master) password:
 - a. On the right side of the password's table row, click **Delete**.
 - b. At the Confirmation dialog box, click **OK**.
The password is removed and the **Password Management** window is refreshed.
- To **remove** cartridge protection (by removing the Master Password):
 - a. On the right side of the password's table row, click the **Remove button**.
 - For AES 256 XTS encryption, click **Remove Encryption**.
 - For Basic Password Protection, click **Remove Password Protection**.
 - b. For **AES 256 XTS encryption only**, at the Cartridge Format Selection dialog box, select either **NFTS** or **exFAT**, and click **OK**.

- c. At the Confirmation dialog box, click **OK**.



CAUTION: As soon as you confirm the removal of **AES 256 XTS** encryption, this option completely deletes all the passwords and all the data, and then repartitions and reformats the RDX cartridge. **There is no undo option.** Any data on the cartridge is **permanently lost** and is not recoverable as the data was only readable with passwords that were initially used to generate the unique encryption key.

As the protection is removed:

- For **AES 256 XTS encryption**, a progress bar for removing encryption on the cartridge is shown followed by a dialog to repartition and format the cartridge. When done, the cartridge is no longer encrypted and is freshly reformatted.
- For **basic password protection**, a progress bar for removing password protection is shown. When done, the cartridge is no longer protected and the data is fully accessible.

You are returned to the **Encryption** tab.

When done, **close** the **Password Management** window by clicking the “X” in the upper right corner. To exit Advanced Options, click **Close**.

Add an Automatic Drive Media Authentication Password

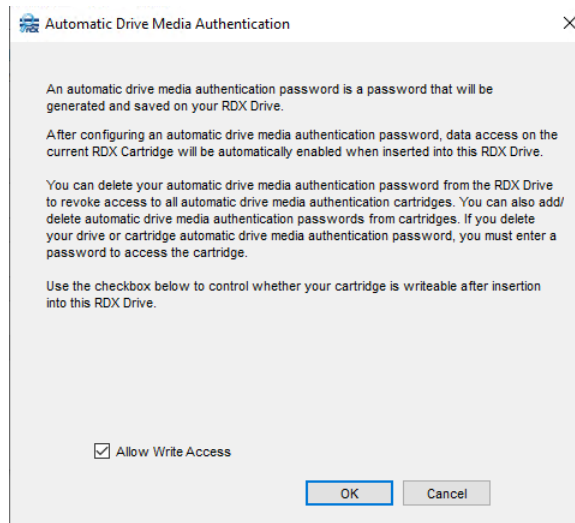
For both AES 256 XTS encryption and basic password protection, an RDX cartridge can be configured with an automatic authentication password that allows its data to be automatically accessible upon insertion into an associated RDX SATA III drive. RDX cartridges can be configured with this option for up to seven RDX SATA III drives.

An RDX SATA III drive creates the key internally and a user doesn't need to enter a password for data access when the cartridge is used in that RDX SATA III drive. The cartridge remains either fully AES 256 XTS encrypted or password protected when it is stored off-site or loaded into another RDX drive. If inserted into a different, unconfigured RDX drive, the user can still access the data normally using one of the assigned passwords for the RDX cartridge.

This option is ideally used for backup or data exchange without needing an operator to enter a password. It can also be used to perform a data or system recovery operation without RDX Manager running.

1. Under Advanced Options, click **Add Drive's Automatic Authentication Password to Cartridge**.

The Automatic Drive Media Authentication dialog box is shown.



2. If required, clear (uncheck) the **Allow Write Access** box.

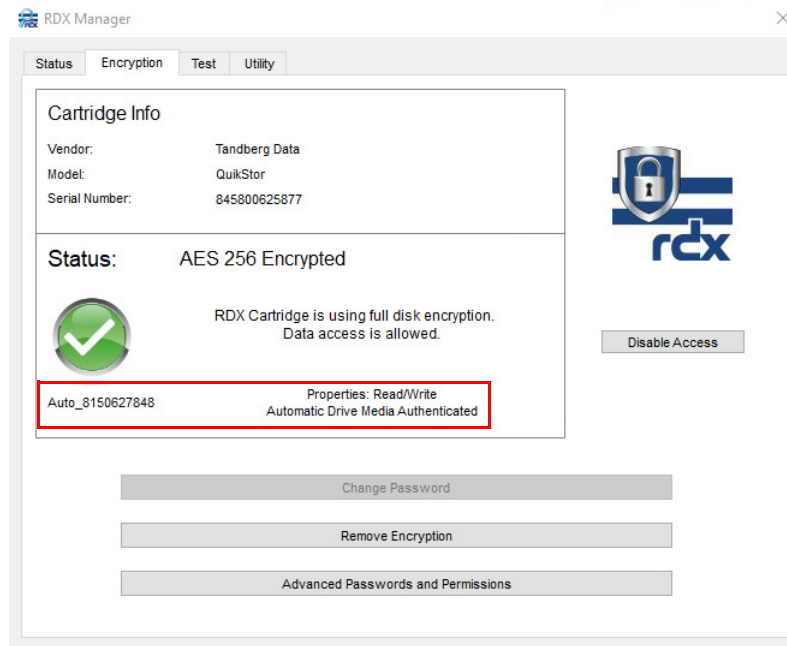
Clearing this option limits the cartridge to only read access when it is inserted and automatically authenticated. Any write operation would fail.

NOTE: To re-enable write access, return to this option, disable the current automatic authentication, and then re-enable it allowing write access.

3. Click **OK** to add the generated automatic authentication password.
4. At the Confirmation dialog box, click **OK**.

A progress bar for adding automatic authentication to the cartridge is shown. When done, access is given to the cartridge and you are returned to the **Advanced Options** dialog box. The **Add an Automatic Drive Media Authentication Password** button is now grayed-out and the **Delete Automatic Drive Media Authentication from RDX Drive** button is active.
5. Click **Close** to exit **Advanced Options**.
6. Eject and re-insert the **cartridge** to verify the change.

Once configured and ejected, whenever the RDX cartridge is re-inserted in that RDX drive, the encryption status shows it to be auto-decrypted.



Whenever an unencrypted RDX cartridge is inserted, you can either:

- Enable encryption/password protection.
- Use the advanced options to delete the automatic decryption on the RDX drive itself.

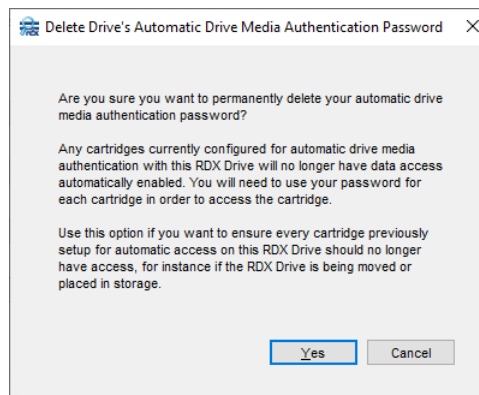
An RDX cartridge can be configured to be automatically authenticated with up to seven different RDX SATA III drives. Each RDX SATA III drive can be configured with automatic authentication for an unlimited number of cartridges.

Delete Automatic Drive Media Authentication from RDX Drive

When the RDX drive is configured for automatic authentication of cartridges, the feature can be removed so that any automatic authentication configured cartridges are no longer automatically authenticated or password confirmed upon insertion.

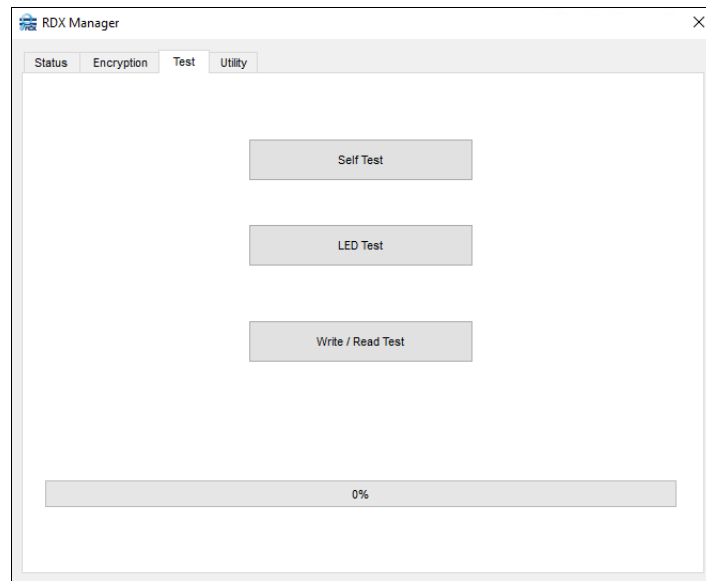
1. Click **Delete Automatic Drive Media Authentication from RDX Drive**.

The Delete Drive's Automatic Drive Media Authentication Password dialog box is shown.



2. Click **Yes** to delete the Auto Decrypt Password.
3. At the Confirmation dialog box, click **OK**.
RDX cartridges no longer automatically authenticate on this RDX drive. You are returned to the **Advanced Options** dialog box. The **Add an Automatic Drive Media Authentication Password** button is now active and the **Delete Automatic Drive Media Authentication from RDX Drive** button is grayed-out.
4. Click **Close** to exit **Advanced Options**.

Test Tab



The **Test** tab of the Management Pop-up Window has three different tests that you can run:

- **Self Test** – This test checks if the device is functioning properly.
- **LED Test** – This test checks the device LEDs.
- **Write/Read Test** – This test verifies that the drive can both write and read the RDX media in the device.

All tests run automatically when you click the button. A progress bar is located in the test message area at the bottom. While the test runs, the progress is shown in the bar.

Once the test is done:

- If the test completes successfully, the progress bar turns green and a success message is displayed.
- If the test fails, the progress bar remains blank (gray) and a failure message is displayed.

Self Test

Self Test performs a simple test of the drive and also the cartridge (if inserted).

Self Test is designed to determine if the host system can communicate with the drive and if the drive can communicate with the cartridge.

Self Test Recommendations

First, run Self Test without a cartridge inserted to determine if the drive is working properly. Next, after inserting a cartridge, run the test again to determine if the drive is communicating with the cartridge correctly.

LED Test

LED Test causes both the cartridge LED and drive LED to alternately flash first green then amber for several seconds.

NOTE: A cartridge needs to be inserted into the drive to see the cartridge LED flashing.

This test is designed to ensure that the both drive and cartridge LEDs work properly to give the user correct indications about drive and cartridge status.

Write/Read Test

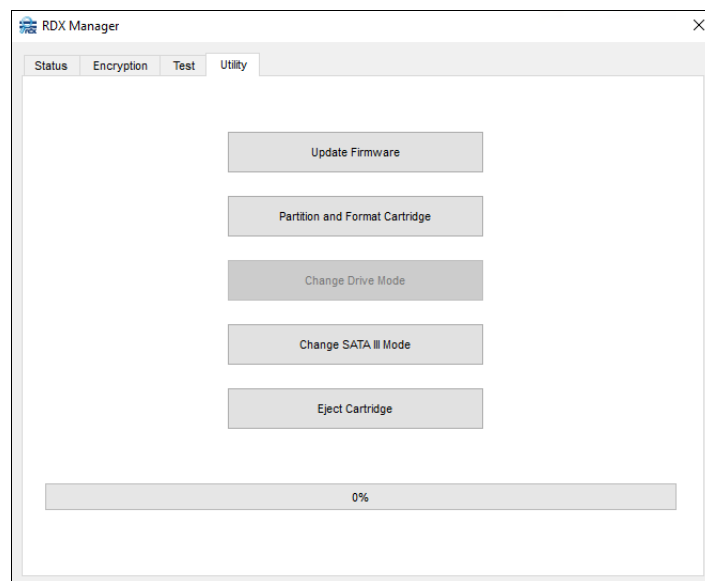
Write/Read Test is designed to ensure that the host system is capable of doing file writes to and file reads from a formatted cartridge.

The Write/Read test requires the following:

- A **properly formatted** cartridge is inserted into the drive.
- The cartridge must have some **free space** for the test to run.
- The cartridge write-protect switch is set to the **OFF** position.

This test writes a temporary file to the free space and then reads and compares the data in that file to the original file. When the test completes, the temporary file is deleted.

Utility Tab



The **Utility** tab of the Management Pop-up Window has the following utilities that you can run:

- **Update Firmware** – This utility enables you to update the device firmware by opening an update file and running it.

- **Partition and Format Cartridge** – This utility enables you to partition and format a cartridge in the drive. The formatting can be either NTFS or exFAT.
- **Change Drive Mode** – If the drive supports changing drive modes, this utility lets you change the mode (Fixed Disk or Removable Disk).
- **Change SATA III Mode** – This utility lets you switch between 3G/6G and 1.5G/3G SATA III modes.
- **Eject Cartridge** – Remotely ejects a loaded cartridge.

Utility functions run to completion. You are not allowed to run another utility function, switch tabs, or close the Management Pop-up Window while they run. A warning message appears when attempting to close the pop-up window before a function completes.

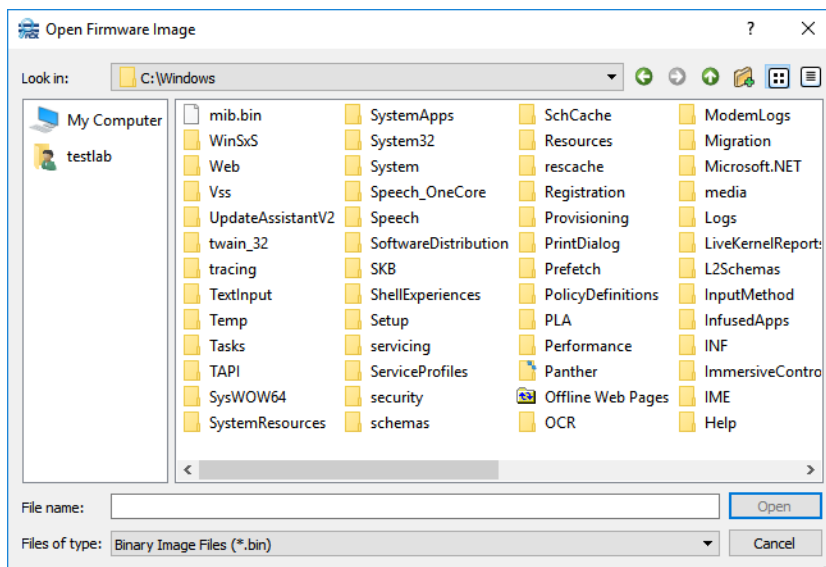
Update Firmware

CAUTION: DO NOT power OFF the system while updating drive firmware. If a cartridge is loaded, it must be ejected before continuing.

NOTE: To find the latest RDX drive firmware update, click **Help > Check For Updates**. A dialog box shows if there is an update and provides a link. You can also find updates listed on the Tandberg Data website:

<http://www.tandbergdata.com/us/index.cfm/products/data-protection-software/>

When you click **Update Firmware**, a dialog box appears for you to select the firmware image file. The file extension is drive dependent: “.BIP” for USB2 or SATA1 drives and “.BIN” for USB3 or SATA3 drives.



During the update process, RDX Manager checks to verify you have a good firmware image file and that it is the correct file for your RDX product.

Update Procedure

NOTE: Updating firmware can not be done with media in place even if the drive is in “Fixed Disk” mode. If media is in place, a message pops up to inform the user to eject the media. Click **OK** and then eject the cartridge from the drive.

1. From the RDX drive manufacturer's website, download the **latest firmware** image. Make a note of the location where you saved the file.
2. Click the **Update Firmware** button to display the search box.
3. Select the image file you downloaded and click **Open**.

The firmware update process starts. The update only takes a few seconds. When the update process is complete, the user is notified via the progress bar (green) and a success message in the message area.

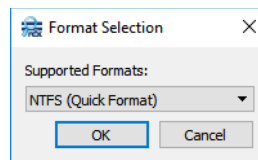
NOTE: If the firmware update process fails, immediately rerun the update process.

Partition and Format Cartridge

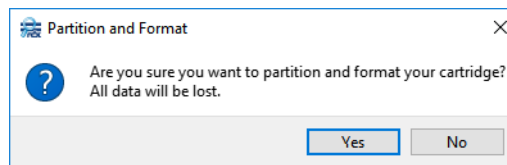
New RDX Cartridges are formatted using the NTFS filesystem. You can partition and format your cartridge based on your operating system (Windows or Apple).

Windows 7 or Higher

When you click the **Partition and Format Cartridge** button on a Windows computer, a Format Selection dialog opens.



Select either **NTFS** (default) or **exFAT** option and click **OK**. A confirmation message regarding the deletion of any existing data on the cartridge is displayed.



Click **Yes** to start the format. Progress and the result is shown in the bottom message area.

Apple OSX

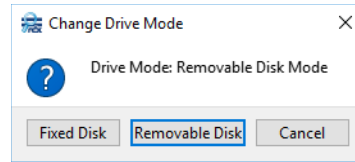
New RDX cartridges are formatted using the NTFS filesystem which may limit their ability to be written from an Apple computer. To erase and format drives to an OSX writable format, use the Apple Disk Utility. To manage your RDX drives from the Apple OSX, use the RDX Manager for Mac software.

Change Drive Mode

If supported, this utility enables changing between Fixed Disk and Removable Disk.

NOTE: The **Change Drive Mode** button is only enabled if the drive supports changing modes. Changing modes can not be done with media in place. If media is in place, a dialog informs the user to eject the media first. Click **OK** and then eject the cartridge from the drive.

When you click **Change Drive Mode**, a dialog box appears showing the current drive mode (with that mode button highlighted in blue). Selecting either the current mode or **Cancel** closes the function without making any changes.



Click the new mode to activate it. The change completes quickly with the progress showing in the message area bar.

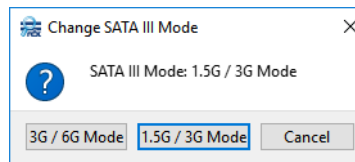
Change SATA III Mode

NOTE: It is recommended to keep the default setting of **1.5G/3G Mode** as the performance improvements from using 3G/6G Mode are only seen when using RDX SSD media.

For SATA III drives, this utility enables changing between 3G/6G mode and 1.5G/3G mode. For USB drives, the option is grayed-out.

NOTE: Changing modes can not be done with media in place. If media is in place, a dialog informs the user to eject the media first. Click **Yes** to eject the cartridge from the drive before changing the mode.

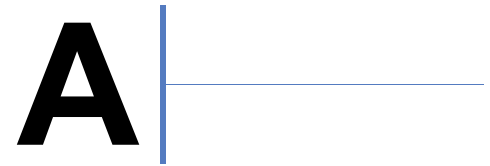
When you click Change SATA III Mode, a dialog box appears showing the current SATA III mode (with that mode button highlighted in blue). Selecting either the current mode or **Cancel** closes the function without making any changes.



Click the new mode to activate it. The change completes quickly with the progress showing in the message area bar.

Eject Cartridge

Use this feature to remotely eject a cartridge that is in the drive. This is necessary when updating the firmware.



Troubleshooting

This appendix provides information on some basic troubleshooting questions and solutions. It also covers how to contact Overland-Tandberg Technical Support.

Topics in Troubleshooting:

- [Basic Troubleshooting](#)
- [Technical Support](#)

Basic Troubleshooting

Check for Firmware Updates

Before any other troubleshooting, always check that you have the latest RDX Manager firmware installed. Click **Help > Check For Updates**. See [Chapter 4, “Update Firmware,”](#) for details.

Cannot Write to a Cartridge

Verify that the write protect tab is not set or that a read-only encryption password is not being used.

Read-Only RDX Cartridge Not Readable on SATA I and SATA III Drives

Some motherboard chipsets running the Windows operating system with Microsoft SATA drivers are unable to read an RDX cartridge on an RDX SATA I or SATA III drive that is in read-only mode.

Symptoms. Cartridges with read and write permissions work normally. Cartridges become unreadable while the write protect tab is set or while a read-only encryption password is used.

Solution. Updating SATA drivers available from the motherboard manufacturer or chipset vendor may resolve this issue. The latest tested version is Intel Enterprise driver 4.3 13.1.0.1058.



CAUTION: Installing incorrect SATA drivers may make your system fail to boot. It is recommended that you back up your data beforehand and proceed carefully when updating SATA drivers.

Recommended Way to Change/Upgrade SATA Driver

1. Open Windows **Device Manager**.
2. Select **IDE ATA/ATAPI controllers (non-enterprise)**.

3. Select **Storage controller (enterprise)**.
4. Double-click your specific **controller**.
5. Select **Update Driver**.
6. Select **Browse my computer for driver software**.
7. Do **one** of the following:
 - **Upgrade** (a new driver has never been loaded on your system).
Select **Search for driver software in this location** and supply a location that only has one driver choice. If the driver is not correct or incompatible, you get a message that your driver software is up to date. Repeat the search until you find a compatible driver (never force driver load).
 - **Change** (switch between Microsoft and Intel drivers that were previously loaded).
Select **Let me pick from a list of drivers on my computer**. Pick the **driver** (usually only two selections are shown). **Standard SATA AHCI Controller** is the default Microsoft driver.

Command Line Eject Feature (rdxcmdline.exe)

As many backup applications lack an eject option, the command “rdxcmdline.exe” can be run to force a media eject.

NOTE: Administrator privileges are needed to run this feature.

To access this file, go to:

C:\Program Files (x86)\Overland-Tandberg\RDXManager\Manager

Options for this command are:

Command Option	Description
-?, -h, --help	Displays this help.
-v, --version	Displays version information.
-s, --scan	Scan RDX drives.
-e, --eject <drive letter>	Eject RDX cartridge.
-f, --force	Force eject - requires eject option.

Command Line Language Selection

Languages can now be selected from the command line. It involves two steps:

1. At the command line, type:
cd C:\Program Files (x86)\Overland-Tandberg\RDXManager\Manager
2. Then type the executable name, dash L (-l), the language two-letter code, and **Enter**.
RDXManager.exe -l xx
 - English language code is “en”.
 - Chinese language code is “zh”.

- German language code is “de”.
- French language code is “fr”.
- Italian language code is “it”.
- Portuguese language code is “pt”.
- Spanish language code is “es”.

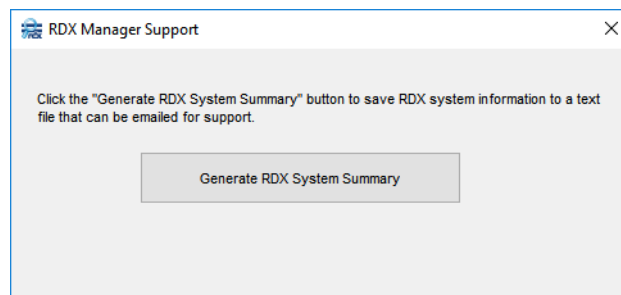
Optional Shortcut

Create a shortcut to RDXManager.exe and add the desired language extension to the target file path (English example shown):

```
C:\Program Files (x86)\Overland-Tandberg\RDXManager\Manager\  
RDXManager.exe -l en
```

Technical Support

When you click **Help > Support**, a RDX Manager Support window opens.



1. Click the **Generate RDX System Summary** button to create a text file containing the RDX system information.
2. At the Explorer window that opens, select where to save the **RdxSystemSummary.txt** file that is created.
It is recommended to save it to the desktop.
After the file is saved, the dialog box shows the path to the file.
3. Email the RDX System Summary report to Overland-Tandberg technical support: supportEMEA@tandbergdata.com
Include the following information about the issue in your email:
 - Provide symptoms of the issue.
 - When did the issue occur?
 - Which activities have caused the issue?
 - Which file objects are affected by the issue?
 - Provide a list of third-party-applications installed on your system, including antivirus scanners and backup management applications.

Symbols

> (menu flow indicator) 4

A

Add a Password 26

Add Drive's Automatic Authentication Password to Cartridge 28

Advanced Options

Add a Password 26

Add Drive's Automatic Authentication Password to Cartridge 28

Delete Automatic Drive Media Authentication from RDX Drive 30

overview 25

View/Modify/Delete Existing Passwords 27

AES 256 XTS Encryption

enable 17

removal 24

alert definitions 4

auto decrypted 30

B

Basic Password Protection 17

enable 17

removal 25

C

cartridge access 20

Change Drive Mode 33, 34

Change SATA III Mode 33, 35

changing protection password 23

command line options

language selection code 37

media eject code 37

conventions, typographical 4

customer support 5

D

data access 20

data protection removal 24

Delete Automatic Drive Media Authentication from RDX Drive 30

Disable Access 21

E

Eject Cartridge 33

Enable Access 21

F

Full Disk AES 256 XTS Encryption 17

G

GUI language 37

I

install RDX Manager 10

K

key features 9

L

language selection with CLI 37

launch RDX Manager 11

LED Test 32

M

Manage RDX Drive button 13

Management Pop-up Window

accessing 13

Encryption tab 17

Status tab **15**
Test tab **31**
Utility tab **32**
menu flow indicator **4**

O

Overland Technical Support **5**

P

Partition and Format Cartridge **33, 34**
product documentation **3**
protection password, changing **23**
protection type selection **17**

R

RDX Manager

- icon **11**
- installation **10**
- overview **8**
- software download **10**
- uninstall **11**

RDX Manager Drive List

- Manage RDX Drive button **13**
- menu options **13**
- overview **12**
- Scan for RDX Drives button **14**

RDX Manager Support dialog **13**

removing AES 256 XTS encryption **24**
removing Basic Password Protection **25**
removing encryption or password protection **24**
Revision History **2**

S

Scan for RDX Drives button **14**

Self Test **31**

silent mode installation **10**

software download **10**

Status tab

- Cartridge Data **16**
- Drive Data **16**

support, technical **38**

T

- technical support **5, 38**
- Test tab **31**
 - LED Test **32**
 - Self Test **31**
 - Write/Read Test **32**
- troubleshooting **36**
- typographical conventions **4**

U

- uninstall RDX Manager **11**
- Update Firmware **32, 33**
- Utility tab **32**

V

- View/Modify/Delete Existing Passwords **27**

W

- Write/Read Test **32**