OVERLAND TANDBERG

RANSOM BLOCK

Administrator's Guide

December 2018
1022139 Rev. A

REVISION HISTORY

Revision	Date	Description
Rev A	December 2018	Initial release

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

www.overlandstorage.com

Tandberg Data
Feldstraße 81
44141 Dortmund, Germany

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

www.tandbergdata.com

Contents

Chapter 1: Product Information

Chapter 2: Installation

Chapter 3: Configuration

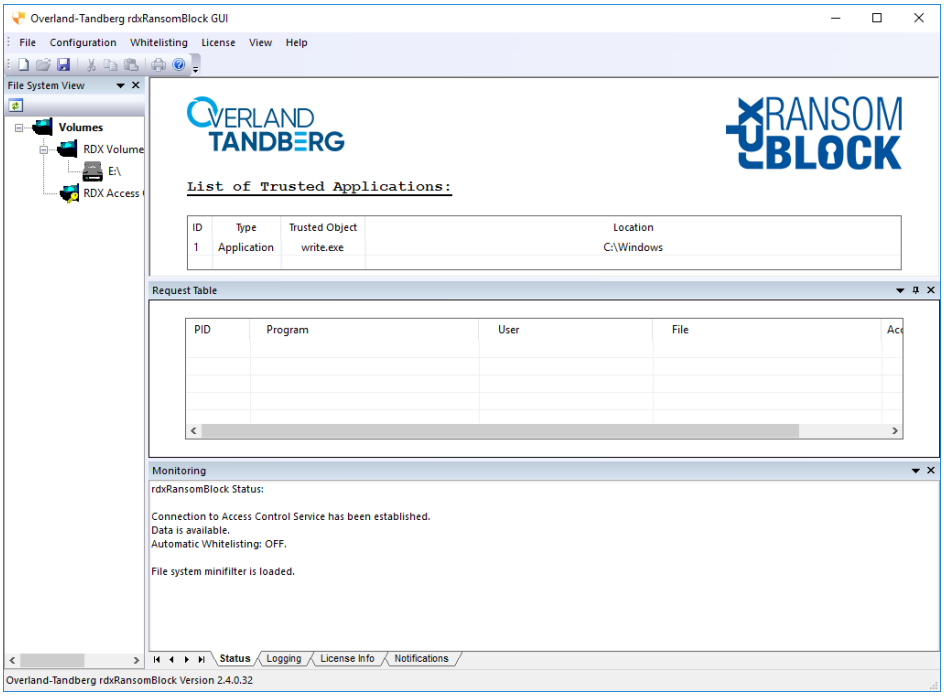
1 Product Information

The rdxRansomBlock software is designed to protect data on Windows NTFS volumes from unauthorized manipulation by viruses, ransomware, and other malicious software by continuously monitoring file operations in real-time on protected file system locations.

Topics in Product Information:

Overview

When rdxRansomBlock is running, any application can write new data to a protected file system. When a file is closed, no application (not even the creating application) is allowed to modify, rename, move, or overwrite the file except if the request is initiated by a trusted application. The feature works on a “block everything by default” approach. The integrity of a trusted, whitelisted application is ensured by its SHA1 hash value and other hashes from dependent components. Therefore, unwanted modifications on a trusted application can also be detected and reported to the user. Unauthorized attempts are logged and notifications can be sent to security administrators.



Key Features

- **Access Control** – Access control can be enabled on a complete NTFS volume or on folders on the first directory level of a NTFS volume.
- **Whitelisting** – rdxRansomBlock allows unrestricted file access to predefined applications.
- **Notifications** – Depending on certain rules, rdxRansomBlock can send alert notifications to the Windows application event log, to email recipients, and to the **Status Area** of the rdxRansomBlock GUI.
- **Monitoring** – If an application that is not whitelisted tries to modify or delete a file in a protected folder or volume, it is displayed in the Request Table so you can choose to allow or deny access.

  The rdxRansomBlock software writes all access requests and responses to a log file called AccessControl.log which is located in the directory `<install_path>\log`. The content is also displayed in the **Monitoring** window in the **Logging** tab.

  The current status is displayed in the **Monitoring** window in the tab **Status**. To check for notifications select the **Notifications** tab from the **Monitoring** window.

Restrictions

- The rdxRansomBlock software supports all RDX removable media.
- Only NTFS file systems are supported; however, ReFS can be used for testing.
- System volumes cannot be protected.

GUI Screen

When started, rdxRansomBlock displays a GUI that lets you configure and control the software.

Menu Layout

The menu options of the rdxRansomBlock GUI are organized as follows:

- **File**
  - **Generate Service Report**
  - **Save Configuration**
  - **Load Configuration**
  - **Exit**
- **Configuration**
  - **Notifications**
  - **SMTP Server**
  - **Test Email**
- **Whitelisting**
  - **Whitelist Programs**
  - **Automatic Whitelisting**
- **License**
  - **Show Licenses**

- Manage Licenses
- View
  - Refresh
  - Toolbars and Docking Window
    - Standard
    - File System View
    - Monitoring
    - Request Table
    - Customize
  - Status Bar
  - Application Look
    - Windows 2000
    - Office XP
    - Windows XP
    - Office 2003
    - Visual Studio 2005
    - Visual Studio 2008
    - Office 2007
      - Blue Style
      - Black Style
      - Silver Style
      - Aqua Style
- Help
  - About

2 Installation

This section covers the installation of the rdxRansomBlock software using the wizard.

Topics in Installation:

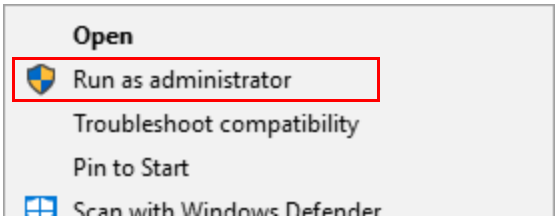
Download the rdxRansomBlock Software

The rdxRansomBlock software and release notes can be downloaded from the Overland-Tandberg FTP website.

1. Go to the FTP website (ftp://ftp1.overlandtandberg.com/rdx).
2. Click and save the rdxRansomBlock software **installer ZIP file**.
   Make a note of the location of where you downloaded the files.

Install rdxRansomBlock

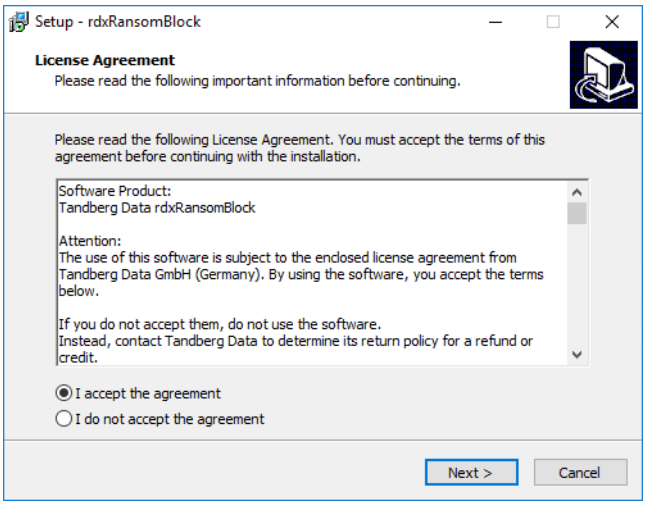
NOTE: Administrative rights are required to install, configure, license, and update rdxRansomBlock. When installing rdxRansomBlock on Windows 7 or Windows 2008 Server (or higher), you need to be logged in as an Administrator or to run the installation program using the **Run as administrator** option (right-click the setup file name).



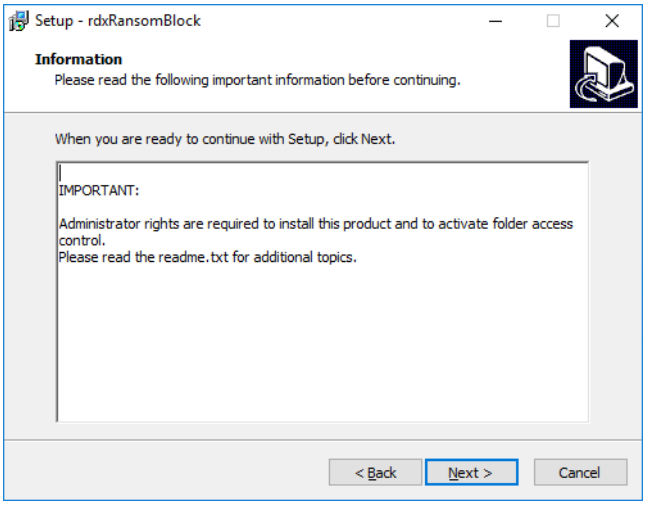
To install the rdxRansomBlock software onto your system:

1. Close **all applications** running on the system.
2. Open the **ZIP** file.
3. Double-click the **EXE file** to launch the installation wizard.

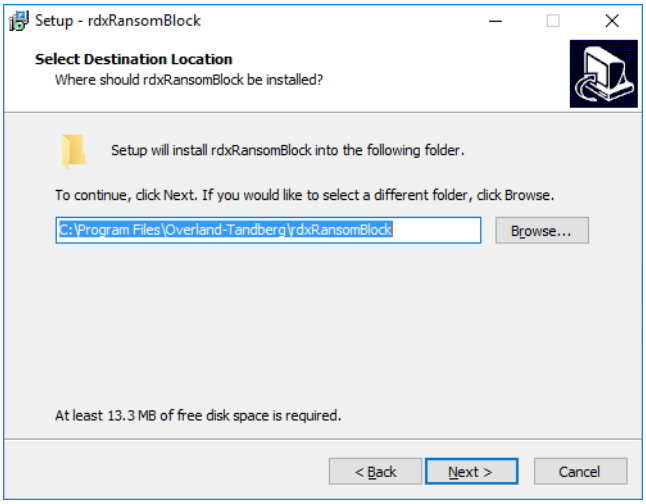
4. At the **License Agreement** dialog, click **Next** to agree to the license contract.



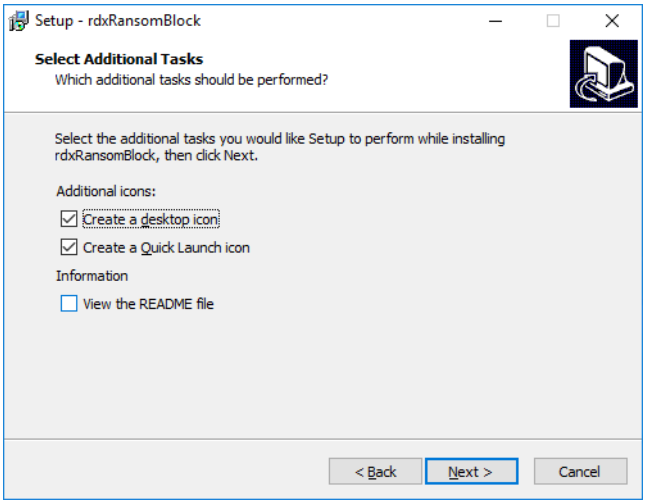
5. At the **Information** dialog, click **Next** to confirm Administration rights.



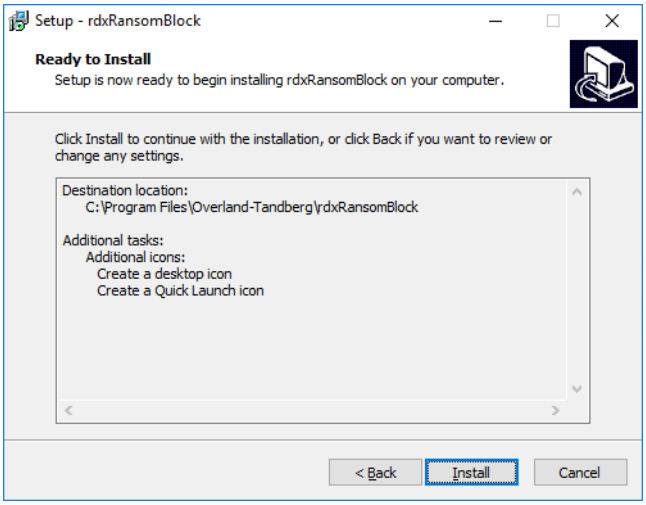
6. At the **Select Destination Location** dialog, click **Next** to accept the default installation folder.



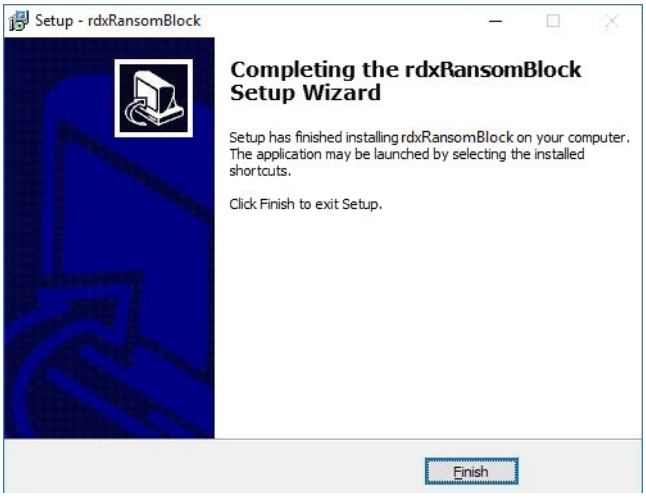
7. At the **Select Additional Tasks** dialog, click **Next** to accept the additional tasks (desktop icon, Quick Launch icon, and viewing the README file).



8. At the **Ready To Install** dialog, click **Install**.



9. At the completion dialog, click **Finish**.



Launch rdxRansomBlock

The rdxRansomBlock EXE file (rdxRansomBlock.exe) is located at:

C:\Program Files (x86)\Overland-Tandberg\rdxRansomBlock

For easy access, a Quick Access icon was created during installation on the bottom task bar. Click the rdxRansomBlock icon to launch the software.

Uninstall rdxRansomBlock

NOTE: You must exit rdxRansomBlock before it can be uninstalled.

The rdxRansomBlock software can be uninstalled using the Windows Software Manager.

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

When uninstalled, a confirmation screen is shown:

3 Configuration

Administrative rights are required to run the rdxRansomBlock user interface. You need to be logged in as Administrator or you need to run the program using the context menu option **Run as administrator** (right-click the rdxRansomBlock icon).

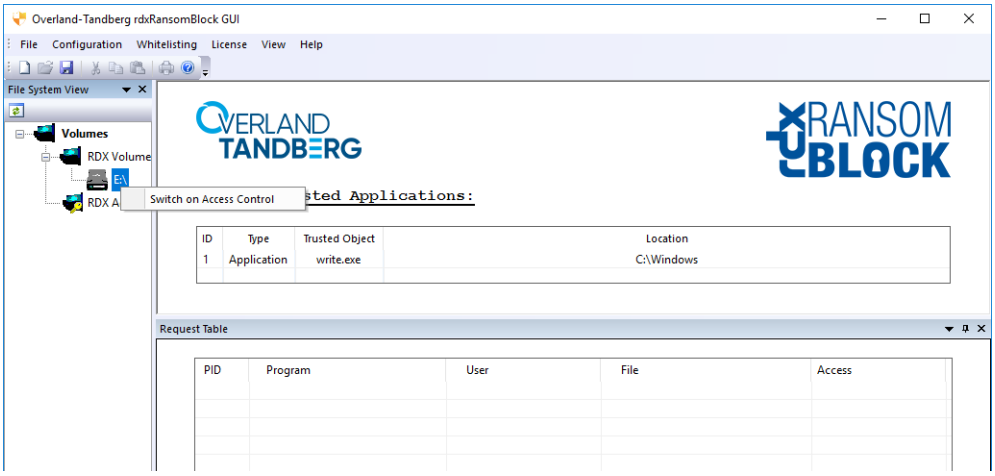
Topics in Configuration:

Access Control Configuration

Access control can be enabled on either an NTFS volume or a folder on the first-level directory of an NTFS volume.

To Enable Access Control

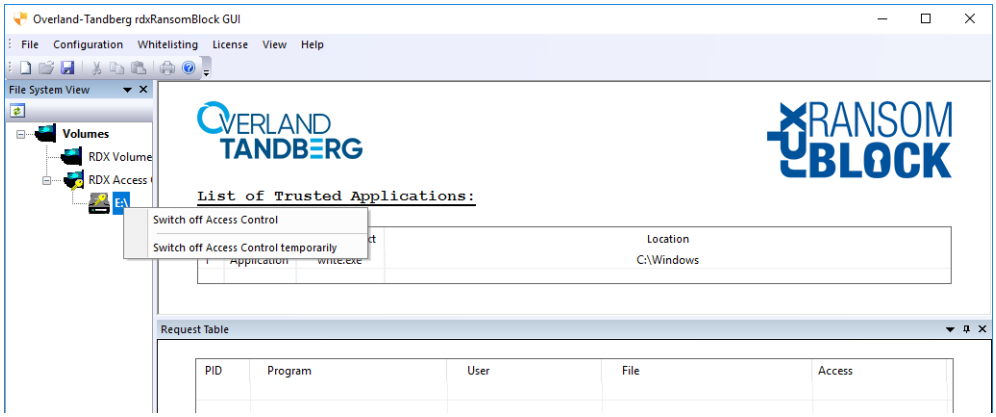
1. Expand the left-pane **RDX Volumes** folder by clicking the plus (+) symbol.
2. At the NTFS volume you want to configure with access control, right-click the **root volume or first-level folder** and select **Switch on Access Control**.



When Access Control is activated, the folder moves to the **RDX Access Controlled Volumes** folder and is shown in a green font indicating Access Control is active.

To Deactivate Access Control

1. Expand the left-pane **RDX Access Controlled Volumes** folder by clicking the plus (+) symbol.
2. Right-click the **volume or folder** you want to switch off and select **Switch off Access Control**.

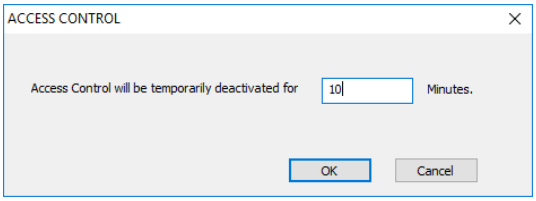


The folder moves to the **RDX Volumes** folder and is shown in a black font indicating Access Control is inactive.

To Deactivate Access Control Temporarily

1. Expand the left-pane **RDX Access Controlled Volumes** folder by clicking the plus (+) symbol.
2. Right-click the access-controlled folder you want to switch off temporarily and select **Switch off Access Control temporarily**.

   The ACCESS CONTROL **dialog box** is shown.



3. Click **OK** to switch off Access Control temporarily for the time selected.

   If you don't want to use the default of 10 minutes, enter a **number** up to 1440 minutes (24 hours).

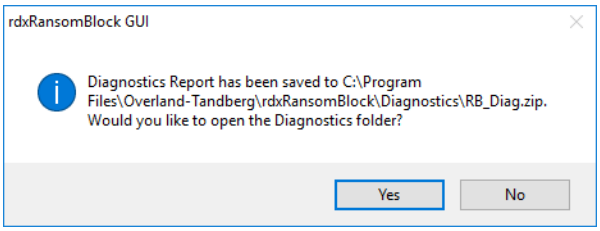
The volume or folder name color switches to black for the duration of the time selected, but remains in the **RDX Access Controlled Volumes** folder. When time expires, the volume or folder name switches back to a green font.

File Options

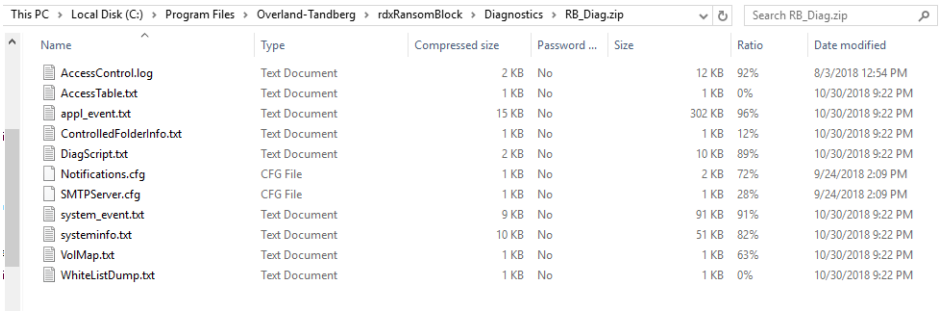
File is the first item on the menu bar. The options consist of:

- **Generate Service Report** – A report (RB_Diag.zip) is generated and save to C:\Program Files\Overland-Tandberg\rdxRansomBlock\Diagnostics folder. The ZIP file contains text and CFG files.

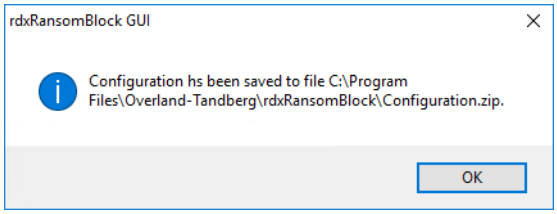
At the saved message, click **Yes** to open the Diagnostics folder to access the report



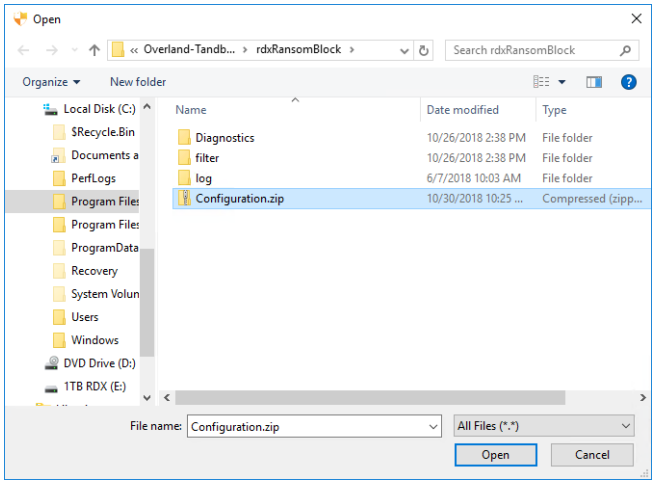
Open the **ZIP file** to review it.



- **Save Configuration** – Saves a copy of the rdxRansomBlock configuration (Configuration.zip) to C:\Program Files\Overland-Tandberg\rdxRansomBlock.



- **Load Configuration** – Loads a previously saved configuration ZIP file.



- **Exit** – Closes rdxRansomBlock.

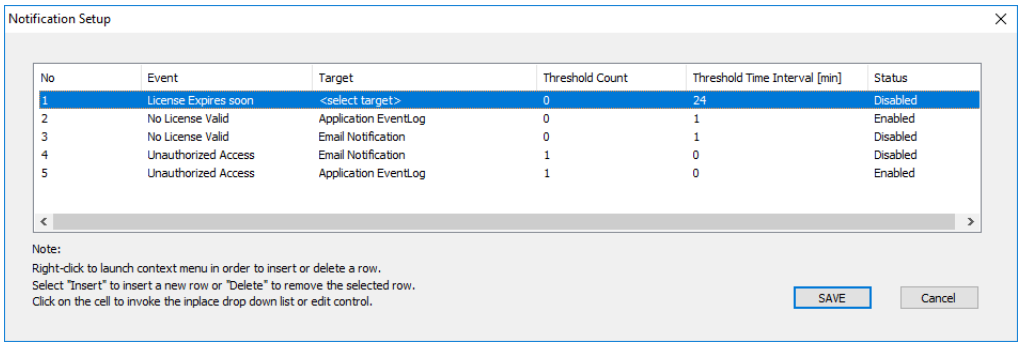
Basic Configuration

The Configuration menu option provides three configurable rdxRansomBlock options.

Notifications

Depending on how your notification rules are configured, rdxRansomBlock can send alerts to targets such as the Windows Application Event Log, email recipients, and the Monitoring Area of the rdxRansomBlock GUI.

To configure notification delivery, select **Configuration > Notifications** from the main menu.



Add a Notification

1. Right-click anywhere in the list to open the **context menu**.
2. Select **Insert** to create a new rule.
3. In each column, use the drop-down menus or editable fields to select your **options**.

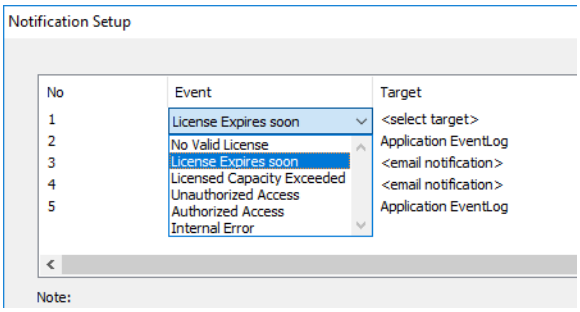
Delete a Notification

1. Right-click the **notification rule** you want to delete.
2. Select **Delete**.

Notification Settings

There are five settings that can be addressed for each notification in this pop-up.

Event Options

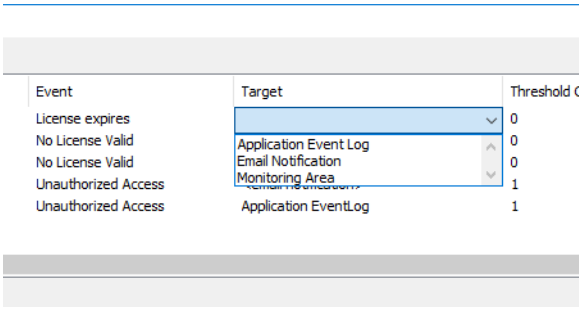


The following Event types are available:

- **No Valid License**

- **License Expires Soon**
- **Licensed Capacity Exceeded**
- **Unauthorized Access**
- **Authorized Access**
- **Internal Error**

Target Options



The following Target types are available:

- **Application Event Log**
- **Email Notification**
- **Monitoring Area**

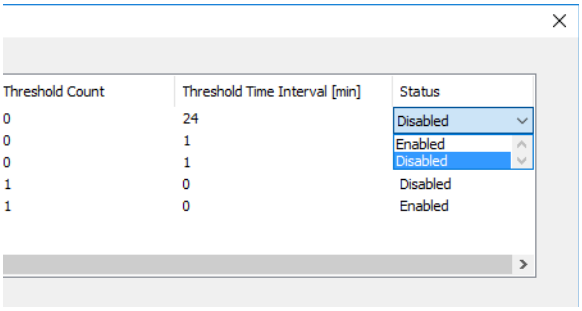
Threshold Count/Threshold Time Interval (min)

Highlight and enter a number in each field. The Count can be any whole number. The Time Interval is the number of minutes up to 1440 (24 hours).

The following table shows the possible actions depending on the settings used:

Threshold Count	Threshold Time Interval [min]	Action
<n>	0	Notification is sent after <n> occurrences.
<n>	<m>	Notification is sent when the event has occurred <n> times within <m> minutes.
0	<i>	Notification is sent every <i> minutes when the event has occurred at least once.

Status



Use this field to enable or disable a rule.

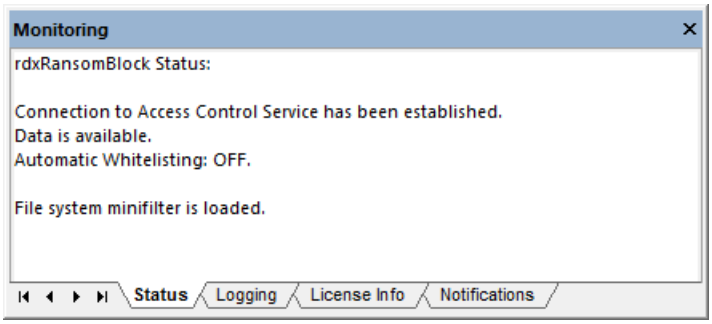
Example: Email Notification Message

The following is an example of the email text that is sent:

<Unauthorized Access> event occurred 1 times. (threshold settings: Count: 1 / TimeInterval:0 min) additional information: PID: 2188, App: C:\Program Files\Windows NT\Accessories\wordpad.exe, File: \\?\E:\t1\230_49_e.log

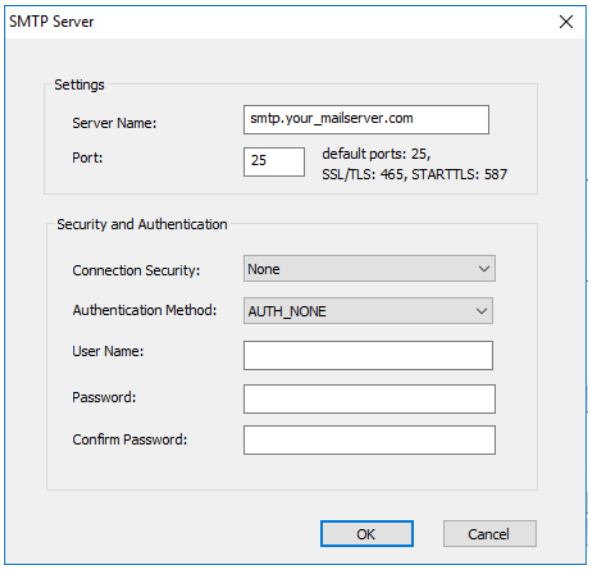
Example: GUI Monitoring Area

The following shows a sample notice in the **Monitoring Area** of the **Status** tab of the GUI.



SMTP Server

To send notifications to email recipients, an outgoing SMTP mail server must be configured. Select **Configuration > SMTP Server** to open the configuration dialog box:



Test Email

Your SMTP settings can be tested by sending an email to a user account by entering its email address and clicking **OK**.

Whitelisting Applications

There are two options to whitelist trusted applications—manually or automatically.

Manually Whitelist Applications

1. Select **Whitelisting > Whitelist Programs**.
2. Use the file browser to pick the application to which you want to allow unrestricted file access.
3. Click **Open**.

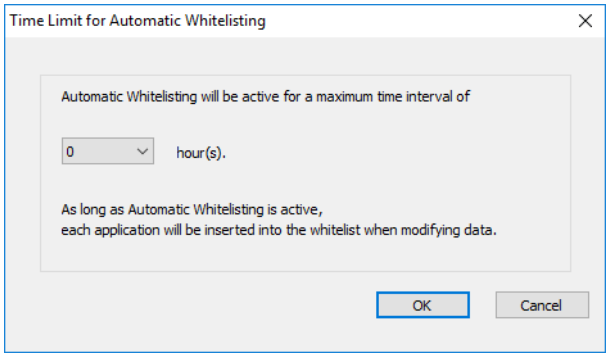
When the whitelisting process is successful, the application is displayed in the table **List of Trusted Applications**.

NOTE: If no applications are whitelisted, the table will be blank.

Automatically Whitelist Applications

CAUTION: When using Automatic Whitelisting, ALL program requests are granted and are added to the Whitelist. This can be dangerous as this does NOT protect against viruses, worms, ransomware, or human error. *This feature should only be used on systems which can be rated as clean and secure.*

1. Select **Whitelisting > Automatic Whitelisting**.
2. In the **Time Limit for Automatic Whitelisting**, use the drop-down menu to select the number of hours (1-24)



After the countdown has ended, automatic whitelisting is turned off automatically.

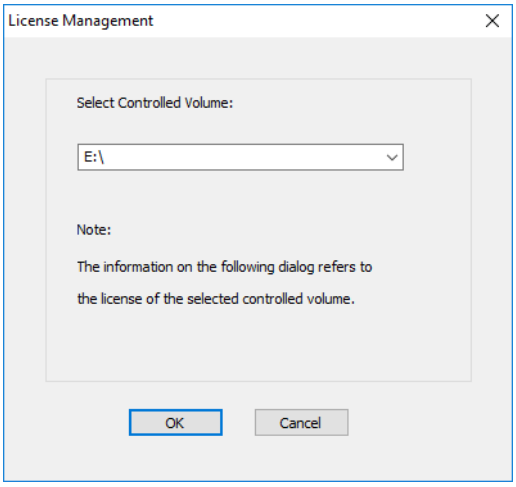
3. Click **OK** to activate.

Licensing

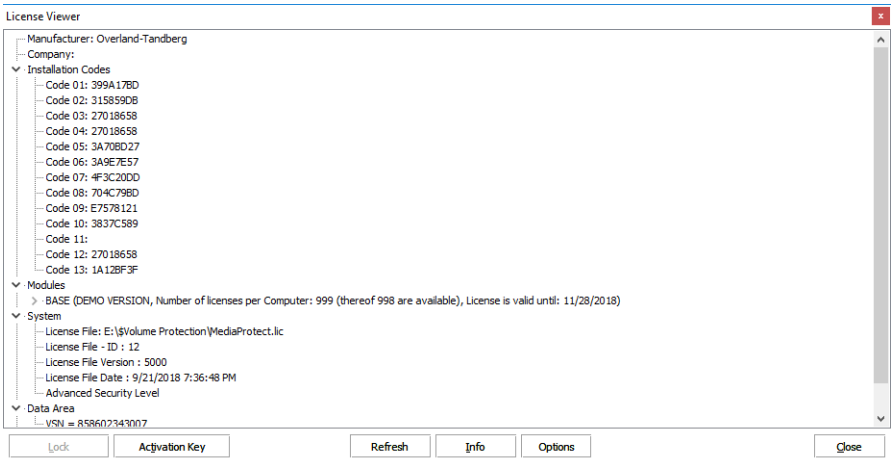
If the Access Control feature is activated on a volume, a temporary evaluation license for 30 days is automatically installed on that volume. Licensing is volume-based, which means that a license must be ordered for *each volume* protected by the product.

Show Licenses

Detailed license information can be requested by clicking the menu item **License > Show Licenses**.



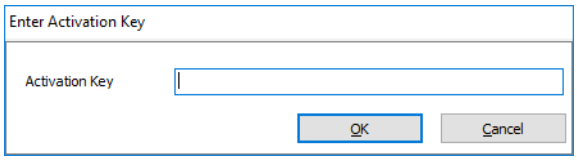
1. Use the drop-down list to select a **controlled volume**.
2. Click **OK**.
   The **License Viewer** opens.



The **License Viewer** is a complete administration interface with the following functions:

- Shows general license information (such as, Manufacturer, Company, copy protection, and system information).
- Shows license information per module (for example, number of licenses, time limitations, demo version, and activation status).
- Shows information on the protected volume (the VSN (Volume Serial Number) of the volume to which the license file is bound).
- Provides an option to install Activation Keys.
- Provides an option to transfer a license.
- Provides an option to deactivate a computer.
- Provides an option to enable license logging (the log file contains detailed debug information which can be used for error tracking).

Activation Key Option



To enter an Activation Key for a volume:

1. At the bottom of the **License Viewer**, click **Activation Key**.
2. In the field, enter the **key**.
3. Click **OK**.

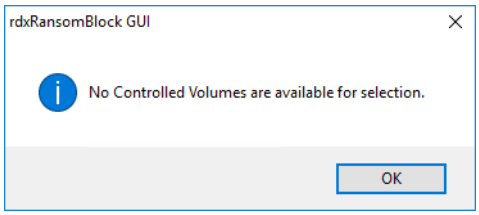
License Viewer Options

1. At the bottom of the **License Viewer**, click **Options**.
2. Click to select/deselect the options desired:
   - **Logging Enabled** – Turns logging on/off.
   - **Select path of log files** – Use the browser to select a folder for the log files.

Manage Licenses

After buying rdxRansomBlock for a volume, a Serial Number is provided and optionally an Activation Key for the Capacity Module depending on the licensing model.

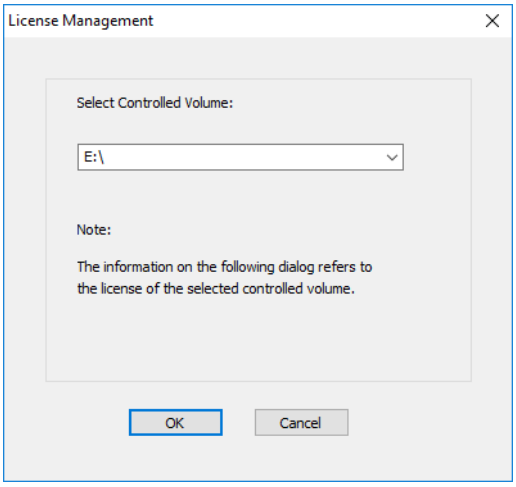
NOTE: If there are no access-controlled volumes, when you select the **Manage Licenses** option, the following screen is displayed:



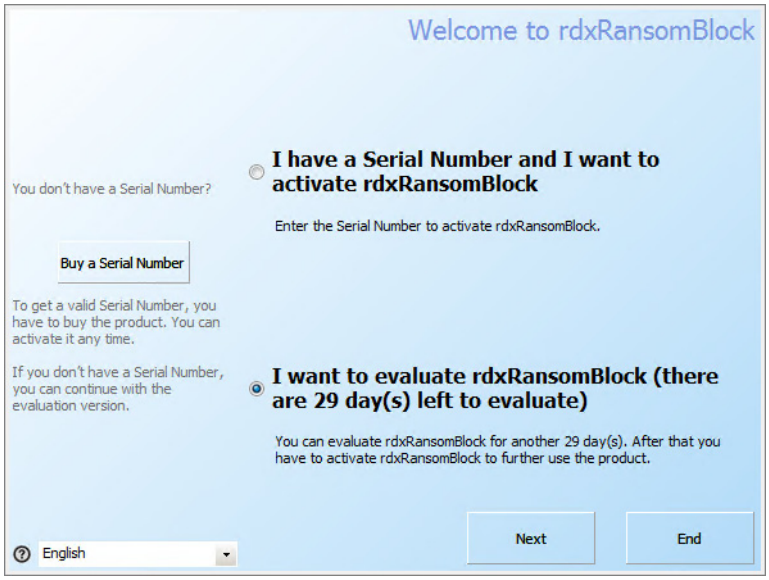
Activation Procedure

In order to activate rdxRansomBlock on an access-controlled volume:

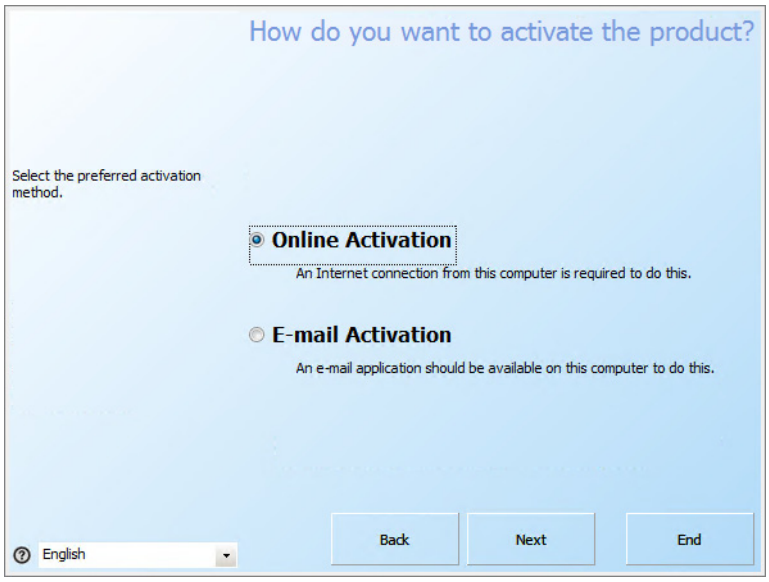
1. Select **License > Manage Licenses.**
   The volume selection screen is shown:



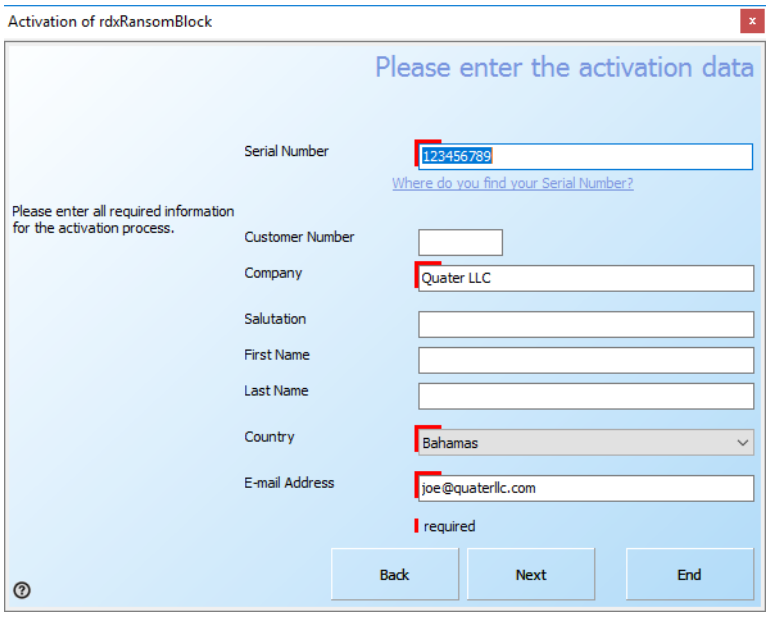
2. Use the drop-down list to select a **controlled volume**.
3. Click **OK**.
   The Welcome screen is displayed:



4. Select **I have a Serial Number and I want to activate rdxRansomBlock** and click **Next**.
   The screen for choosing an activation method is shown.



5. At the activation data entry screen, enter your **information** and then click **Next**.
   The fields with *red corner marks* are required. The serial number can be found in the rdxRansomBlock download confirmation message.



Continue with either Online Activation or Email Activation.

Online Activation

NOTE: For activation to be completed online, you need an internet connection.

1. At the online activation confirmation screen, click **Next**.
2. When the product activation succeeds, click **Next** to finish the process.

Email Activation

NOTE: If there is no email application available on the system where rdxRansomBlock is installed, the activation data is copied onto the clipboard for further processing.

The email address to the Activation Service Center and activation data is displayed in a dialog window. The activation request should contain the following information:

Please send this email to supportEMEA@tandbergdata.com

Activation-Request for rdxRansomBlock (27.07.2018 16:37:17) Please do not change the following information Name/Company: My_Company_Name, Inc.
Serial Number: xxxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
Email Address: john.doe@mycompany.com
Installation Codes:
01:xxxxxxxx
02:xxxxxxxx
03:xxxxxxxx
04:xxxxxxxx
05:xxxxxxxx
06:xxxxxxxx
07:xxxxxxxx
08:xxxxxxxx
09:xxxxxxxx
10:xxxxxxxx
11:
12:xxxxxxxx
13:xxxxxxxx

Your registration information is sent to our Activation Center. Please allow 1 to 2 business days to send an unlock key. Project:rdxRansomBlock - UVf001
User Info:
[*You can write any comments for the Activation Center in this space.*]

Registration Data: Customer Number: Company: MyCompany Salutation:
First Name: John
Last Name: Doe
Country: England
Newsletter:NO

The following block contains the information of this e-mail in an automatically processable form.
Please do not change the information, since otherwise the processing will not be possible or will be delayed.
- STARTBLOCK-
ab09b8S2WK6TbtTCROOQ8UP+A1qcZCjo2zw00whBmDnYEd5UVfpJE4H8p+P8AodhO
XF6fS1w2CyKTsmEtc9q2DeaHKrF6WAh2TbteLSBYN5WVD/W/dgCvMFvXf90011Lve
p06WIVCVqfdAyRfipoDXOocpTJ20551CI8JEBODqqfi2DnUwNgSbWUCXvCG7E7NO+
.
. [*actual data redacted*]
.
4rMSYbft8UAOF4mNpTbfgeG/GV+5u6hFt3VguReH5X9hxOTdaum7k+eAkpi2J7WCf
F6rn20TIlgnwHHYPiurW3gDeZ41motREINPLScZxFF10+eoDiAI4jm9eu5ECjIzWY
0qKy7370YuR+8VrhlgSXvpcsU+0DyR3WhZX4H/Y8EerPbOBPKyDjvVn82Pf6QZCLA MOp/UjZtI4hi=
-ENDBLOCK-

An Unlock Key is generated from the Installation Codes of the activation request and sent back within one to two days. It is used to unlock the license by activating the copy protection.

After a successful activation, the license status should be as follows:

- **Installation Codes** – Should show "Copy protection activated (*number_of_licenses*)".
- **Modules > BASE** – Should show "License is valid until: *dd.mm.yyyy*, Activation (done)".

All serial number keys are time limited. Once the license expires, a new serial number with a new expiration date must be requested and installed to continue the subscription.

To ensure continuous work, the new key should be installed via the **License Viewer > Activation Key** before the expiration date. The licensed time period of the new key is added to the remaining days of the previous key.

If the license has already expired, when you select **License > Manage Licenses**, an expiration screen is displayed.

IMPORTANT: Until a new license is installed, the rdxRansomBlock protection is no longer active on this volume.

View Options

The View menu provides options regarding the way the GUI is seen.

Refresh

This option updates the GUI to show the current status. You can also click the refresh button ( ) located at the top of the **File System View** pane on the left.

NOTE: Depending on the option selected from the File System View drop-down menu, the pane may be floating or hidden.

Toolbars and Docking Windows

Use this option to choose the toolbars and GUI window panes:

- **Standard** – Turns the toolbar icons on/off.
- **File System View** – Hides/displays the **File System View** pane.
- **Monitoring** – Hides/displays the **Monitoring** pane.
- **Request Table** – Hides/displays the **Request Table** pane.
- **Customize** – This lets you customize the menus and windows.

Status Bar

Click this option to turn the Status Bar at the bottom of the GUI on/off.

Application Look

Use this option to choose the way the GUI is displayed matching different Microsoft looks.

Help

Click **About** to see the version and copyright information for rdxRansomBlock.

Click **Overland-Tandberg** to access our website for more information about licensing.

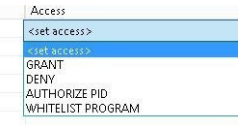
4 Monitoring

The Monitoring pane in the GUI provides details regarding numerous operations.

Topics in Monitoring:

Request Table

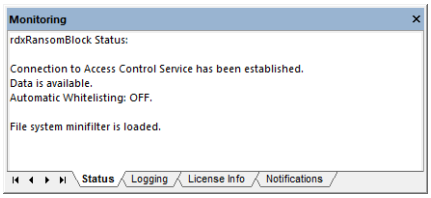
If a file modification attempt cannot be assigned to a whitelisted program, the request is displayed in the request table and an administrator can control the file access. If there is no answer to a request within one minute, the access is automatically denied. Access can be manually set by clicking the **<set access>** drop-down menu that is shown in the **Access** column and choosing an access option.



- **GRANT** – Allows the process to modify the specified file object.
- **DENY** – Denies the process from modifying the specified file object.
- **AUTHORIZE PID** – Write access is granted to all files for the specified process until its termination (NT kernel and system processes are excluded).
- **WHITELIST PROGRAM** – General write access on files is granted (whitelisted) for the specified program.

Status Information

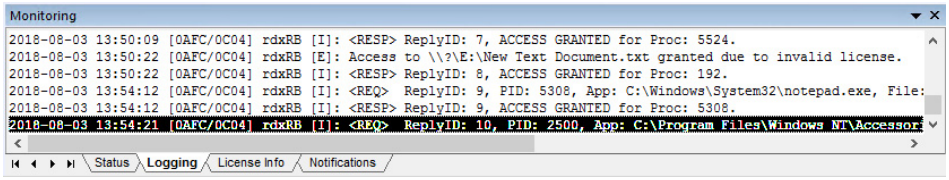
The current overall status is shown in the **Monitoring** pane in the **Status** tab.



Access Log

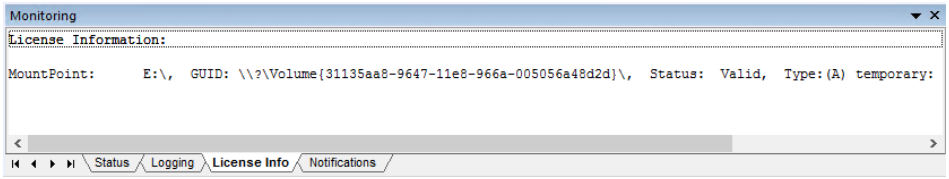
The rdxRansomBlock software writes all modification requests on protected files and responses to a log file called AccessControl.log which is located in the directory <*install_path*>\log.

The content of the log file is also displayed in the **Monitoring** pane in the **Logging** tab.



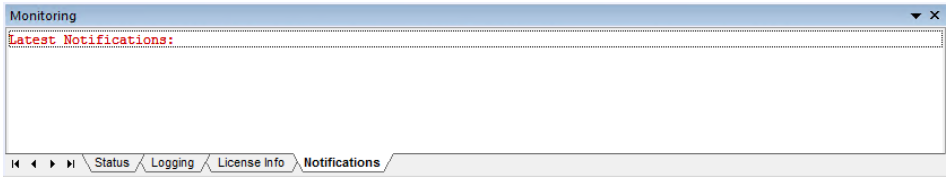
License Info

To check the licensing, select the **License Info** tab from the **Monitoring** pane.



Alert Notifications

To check for notifications, select the **Notifications** tab from the **Monitoring** pane. For details on licensing, see Licensing on page 18.



Windows Event Logs

Further status information is available in the Windows Application and System Event Logs.

A Troubleshooting

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

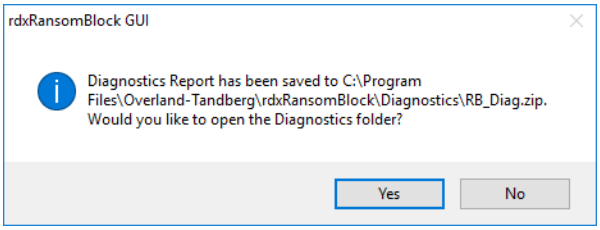
Topics in Troubleshooting:

Diagnostics

The rdxRansomBlock GUI automatically generates a Service Report by selecting the menu item **File > Generate Service Report**. All service information is stored to the file RB_Diag.zip, which is located in the directory:

<*installation_directory*>\Diagnostics

To access the RB_Diag.zip file, at the confirmation message, click **Yes**.



See Chapter 3, "File Options," for details.

Technical Support

For help configuring and using your RDX appliance, email our technical support staff at:

supportEMEA@tandbergdata.com

For additional assistance, search at http://www.tandbergdata.com/us/index.cfm/support/.

To help our technical support team analyze unexpected behavior of the software, you can manually generate a diagnostics report and emailing it to the support address.

Index