



# GRAU DATA

YOUR DATA. YOUR CONTROL

## Blocky Administration Guide

GRAU DATA GmbH

Version 3.5.2.984 - Release, 2025-05-20 13:56:04

# Table of Contents

1. Product Information .....	1
1.1. Overview .....	1
1.2. Key Features .....	1
1.3. Deduplication .....	2
1.4. Platform support and restrictions .....	3
1.5. Announcement of discontinuation .....	3
2. Password protection .....	4
3. Installation .....	5
3.1. Installing .....	5
3.2. Updating .....	10
3.3. Upgrading from Version 2.5 and earlier .....	10
3.4. Uninstallation .....	11
4. Configuration .....	14
4.1. Start of the GUI .....	14
4.2. Set initial password .....	14
4.3. Change password .....	15
4.4. Access Control .....	16
4.5. Disk protection .....	17
4.6. Whitelisted Applications .....	19
4.7. Notifications .....	23
4.8. SMTP Server Configuration .....	25
4.9. Save / Load Configuration .....	26
4.10. Central GUI Mode .....	27
4.11. Add server .....	29
4.12. Server selection .....	31
4.13. Define a new Group .....	33
4.14. Master Configuration .....	35
4.15. Licensing .....	40
4.16. Multi-factor authentication .....	48
5. Monitoring .....	53
5.1. Request Table .....	53
5.2. Status Informationen .....	53
5.3. Access Log .....	54
5.4. License Information .....	54
5.5. Alert Notifications .....	55
5.6. Windows event logs .....	55
5.7. Raw volume access .....	55
6. Diagnostics .....	56

6.1. Service Report .....	56
6.2. Access denied. ....	56
6.3. Missing privileges. ....	56
6.4. System clock tampering .....	57
6.5. Self-protection .....	57
6.6. Reset GUI Layout .....	58
Appx A: Setup command line parameters .....	59
Appx B: BlockyCLI parameters .....	61
Appx C: Blocky Change Log .....	76
C.1. Version 3.5.2.984 - Release .....	76
C.2. Version 3.5.1.896 - Release .....	76
C.3. Version 3.5.0.848 - Release .....	77
C.4. Version 3.1.1.450 - Release .....	77
C.5. Version 3.1.0.362 - Release .....	77
C.6. Version 2.7.1.186 - Release .....	78
C.7. Version 2.7.0.56 - Release .....	78
C.8. Version 2.6.2.217 - Release .....	79
C.9. Version 2.6.1.107 - Release .....	80
C.10. Version 2.5.0.52 - Fix-5 .....	80
C.11. Version 2.5.0.48 - Fix-4 .....	81
C.12. Version 2.5.0.41 - Fix-3 .....	81
C.13. Version 2.5.0.36 - Fix-2 .....	81
C.14. Version 2.5.0.32 - Fix-1 .....	82
C.15. Version 2.5.0.30 - Release .....	82
Appx D: Open Source Licenses .....	83
Index .....	84

# Chapter 1. Product Information

## 1.1. Overview

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

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 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 a unique fingerprint calculated from several binary checksums and other hashes from dependent components. Therefore unwanted manipulations 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.

Beginning with version 3.5 Blocky also [protects physical disks](#) to prevent manipulation or deletion of volumes and partitions which contain Blocky volumes.

## 1.2. Key Features

### Access Control:

Access control modes can be enabled on a complete NTFS or ReFS volume or independently on folders on the 1st directory level of such a volume.

### Whitelist:

Blocky allows unrestricted file access to trusted whitelisted applications.

### Monitoring:

If an untrusted, non-whitelisted application tries to modify a file on a protected folder or volume, this write access is denied by default. However, if the BlockyGUI is running, the write access is set on hold first and a request will be displayed on the [Request Table](#), so you can choose to allow or deny access. Blocky writes all access requests and responses to the log file `C:\ProgramData\GrauData\Blocky\AccessControl.log`. The content is also displayed in the “Monitoring” window in the tab “Logging”. The current system status is displayed in the “Monitoring” window in the tab „Status“. To check for notifications select the tab “Notifications” from the “Monitoring” window.

### Notification:

Blocky can send alert notifications to the Windows application event log, to email recipients and to the Status Area of the Blocky GUI depending on certain rules.

## GUI and Core:

In the case of a new installation, two components, the GUI and the Core can be selected whether both or just one of them should be installed. The GUI is the graphical user interface to configure a Core. The Core is the engine and is responsible for protection and whitelisting.

## Local and central GUI:

The GUI can operate in two different modes. After the installation the GUI is in the local mode. Only when a server is added the GUI mode changes into a central GUI for managing local and remote Blocky systems. As long as the GUI is in the local mode, GUI and Core share a common password. By changing into central GUI mode a separate password must be assigned for the central GUI. See [Central GUI Mode](#).

# 1.3. Deduplication

Blocky has basic support for the built-in deduplication on NTFS file systems. Deduplication on ReFS file systems is not supported.

Deduplication is performed by the Windows components `fsdmhost.exe` and `svchost.exe`. To allow deduplication on Blocky protected Volumes you must add both binaries to the list of trusted applications. Please whitelist both components either manually or during automatic whitelisting.



The Windows component `svchost.exe` is responsible for various internal tasks. However only the deduplication task is allowed when this component is added to the whitelist.

## 1.4. Platform support and restrictions

Restrictions apply with regard to supported platforms and specific functionalities.

1. Supported platforms (with restrictions, see below):
  - MS Windows Server 2012 R2
  - MS Windows Server 2016
  - MS Windows Server 2019
  - MS Windows Server 2022
  - MS Windows Server 2025
  - Full GUI aka Desktop Experience required.
2. Running on Microsoft fail-over cluster or Active Directory Domain Controllers is not supported.
3. Blocky supports local disks, e.g. block storage only. NTFS and ReFS file systems are supported.
4. Basic support for built-in deduplication on NTFS file systems.  
On ReFS dedup is not supported. Use block cloning feature instead.
5. System volumes can not be protected
6. Only simple volumes on MBR and GPT disks are supported.  
Dynamic disks (e.g. striped, mirrored or RAID-5) are not supported.
7. Each protected volume must have a single drive letter assigned or must be mounted in a folder of a parent volume (junctions) which is not under access control.
8. Restrictions apply for volumes mounted in folders of parent volumes. AccessControl for folder-mounted volumes and their parent volumes are mutually exclusive.
9. Running the BlockyGUI requires certain security privileges which are granted by default to admin users. See chapter [Diagnostics](#) for details.
10. The "Controlled folder access" feature from built-in Windows Defender or Microsoft Defender for endpoint is not supported. This feature must be turned off when installing and using Blocky.
11. Some Windows System Services may perform raw volume access on Blocky protected volumes which may cause unauthorized access events. See chapter [Monitoring](#) for details.
12. Blocky protects physical disks which contain Blocky volumes. In case of Windows Storage Spaces, Blocky protects the virtual disk. The underlying physical disks of the storage pool remain unprotected.
13. The new disk protection function requires that the protected Blocky volume is **not** located on the disk containing the system volume, but on a separate disk. However, if your protected Blocky volume is located on the system disk, do **not** update to Blocky version 3.5.x, but contact GRAU DATA GmbH support ([support@graudata.com](mailto:support@graudata.com)) instead.

## 1.5. Announcement of discontinuation

With a later version 3.x of Blocky, platform support for MS Windows Server 2012 R2 will be discontinued.

# Chapter 2. Password protection

To protect the software against unauthorized configuration changes, an password must be defined for starting the GUI. When starting the GUI for the first time, this self-defined password must be set. See [Set initial password](#). To enhance protection, [multi-factor authentication](#) can be activated at a later time.



The password defined in the local GUI also represents the password for the core components.



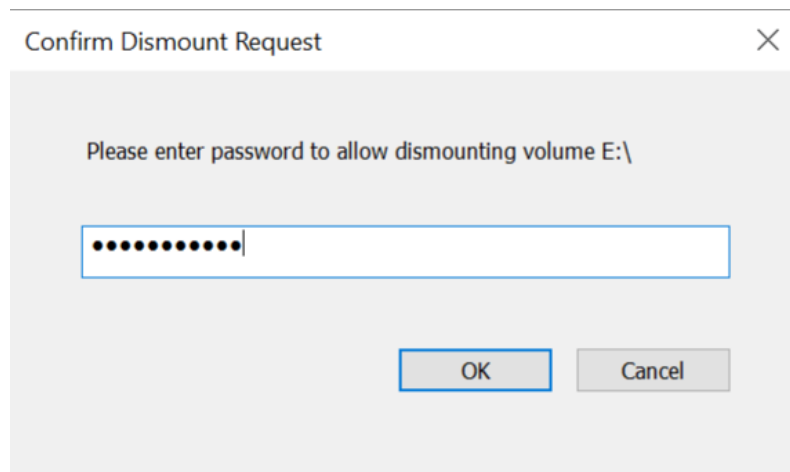
The password length is limited to 128 characters. It must be at least 6 characters in length and must contain at least one number. Single quote (') and double quote (") characters are not allowed.



To prevent brute force password attacks, a delay is used in GUI and CLI startup if too many incorrect passwords have been entered.

## A password is required for:

- [Start of the GUI](#)
- [Update of Blocky](#)
- [Uninstallation of Blocky](#)
- Eject and detach of a volume under access control



Any eject or detach request of a volume must be confirmed with the password while the GUI is running. After confirming the volume will be detached/ejected.



When updating or uninstalling Blocky a password is only requested if the core is installed.

# Chapter 3. Installation

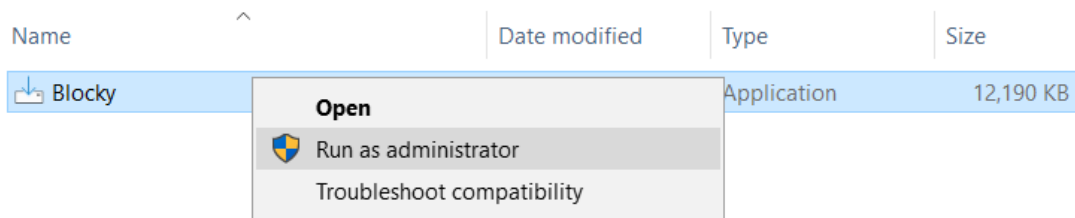
## 3.1. Installing

### 3.1.1. Launch the Installation

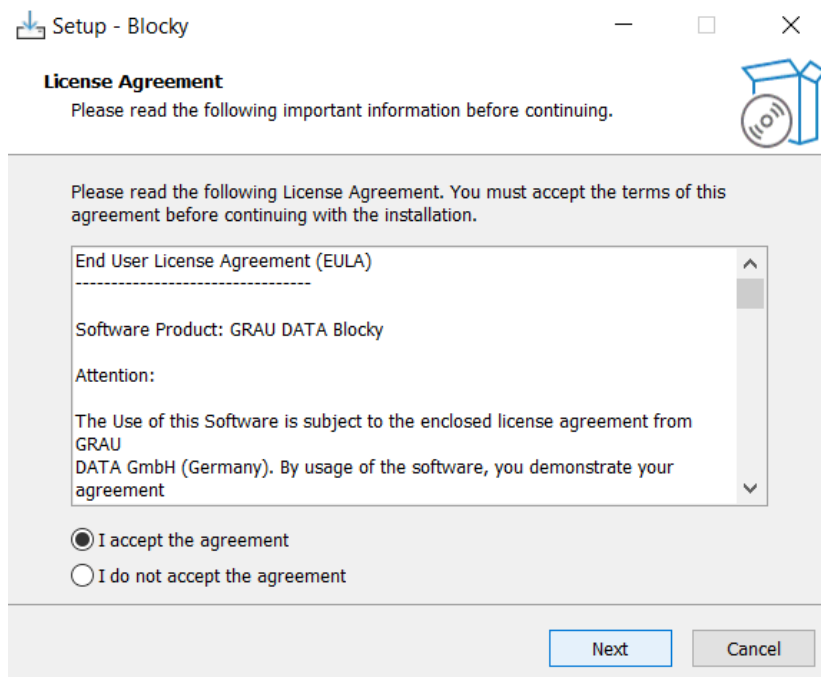
- Close all applications running on the system.
- Run the setup program **BlockySetup\_3\_5\_2\_984.exe** to start the installation wizard.



Administrative rights are required to install, configure, license or update Blocky. When installing, you need to be logged in as Administrator or you need to run the installation program using the context menu option “Run as administrator”. (Right-click the Blocky setup file). See [Restrictions](#) for further details.

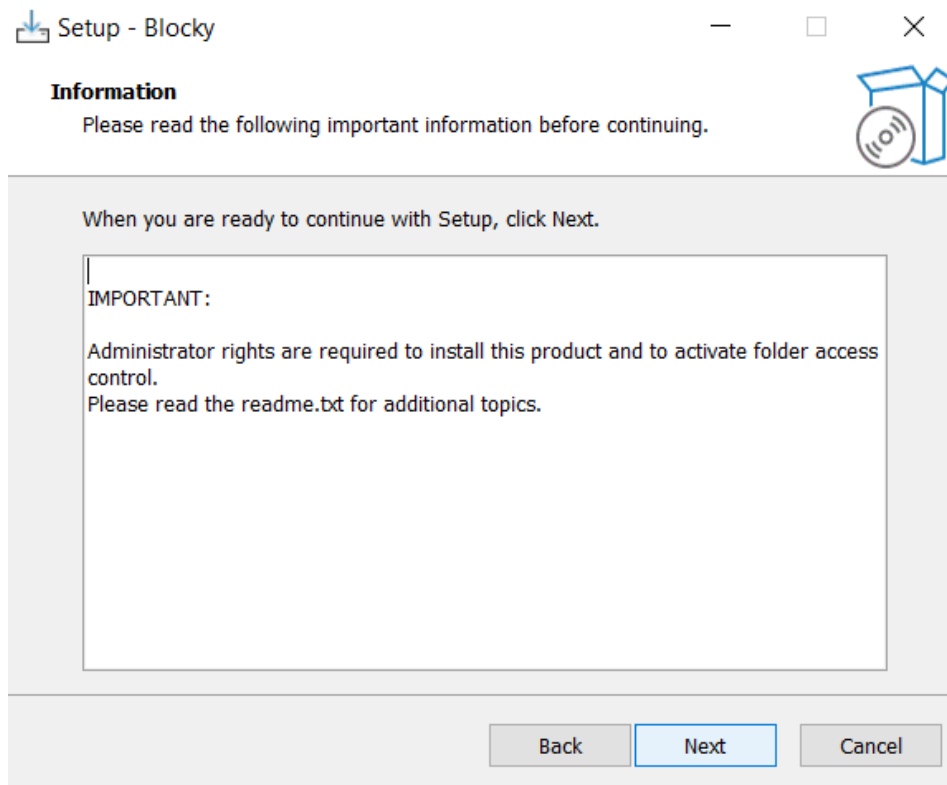


### 3.1.2. License Agreement

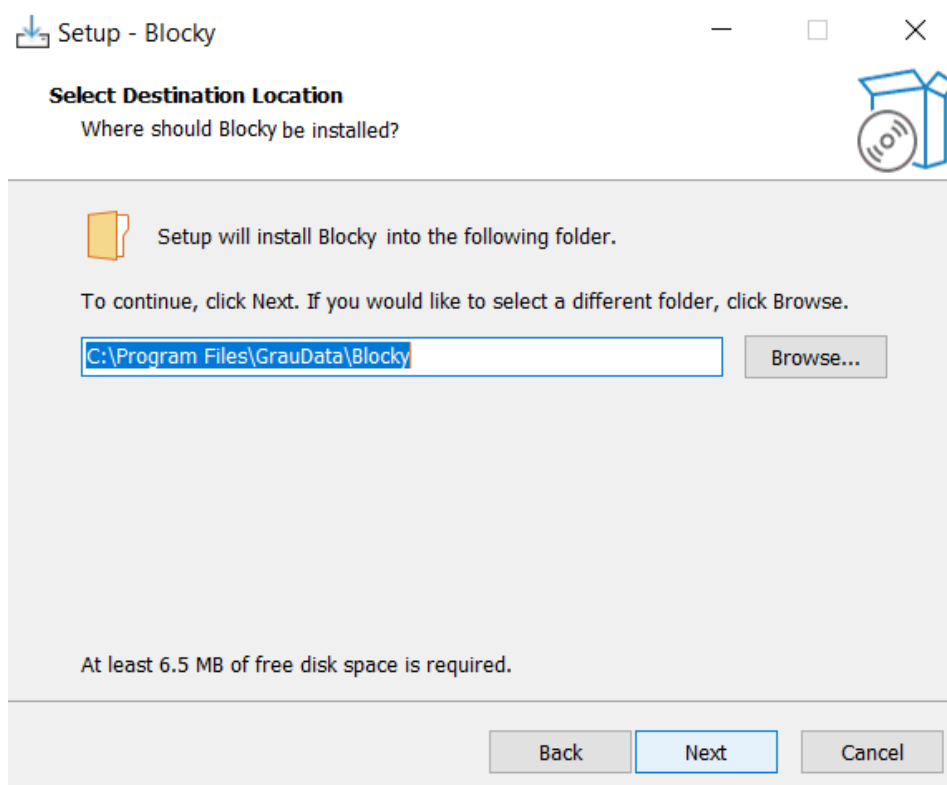


You have to accept the „License Agreement“ in order to continue with the Blocky installation procedure.





### 3.1.3. Select the installation path and additional tasks



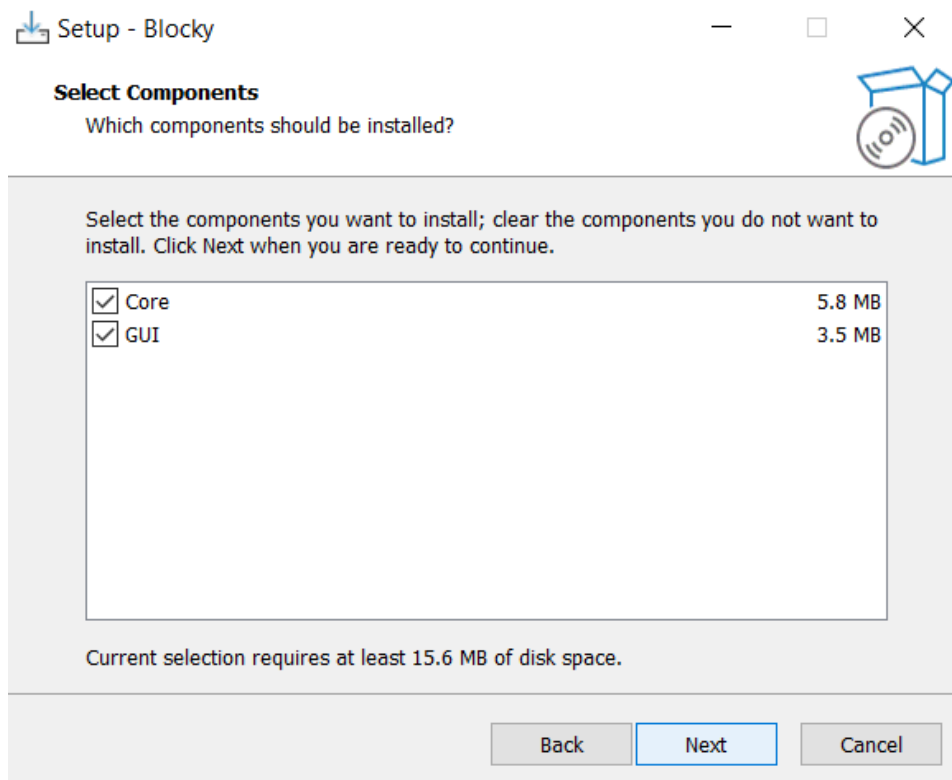
### 3.1.4. Select Components

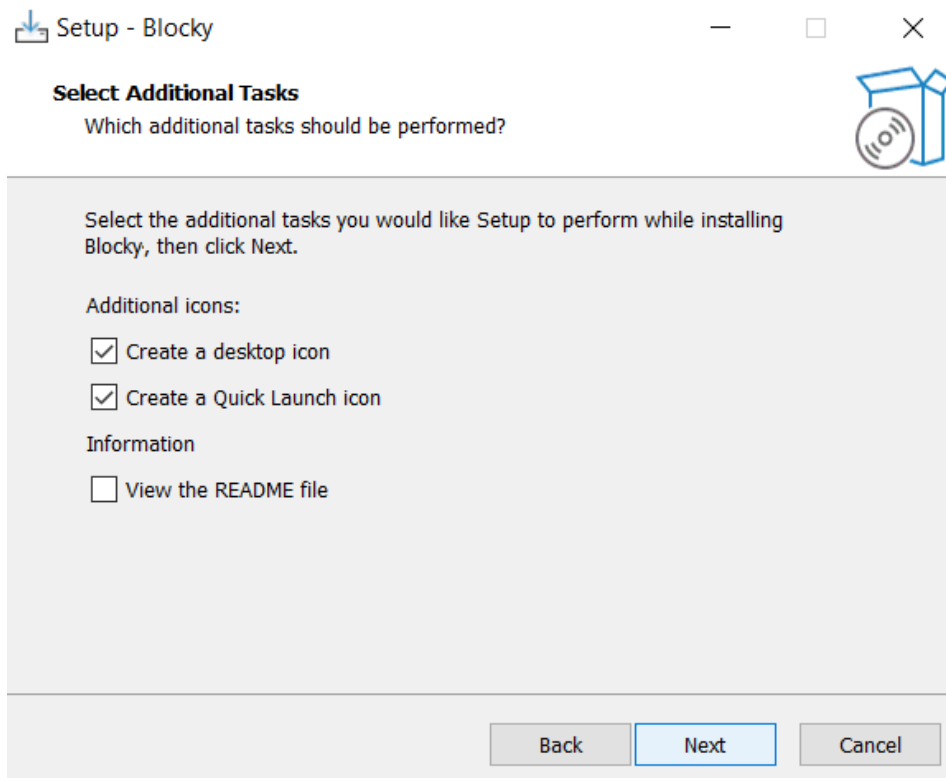
Please select the components you want to install.



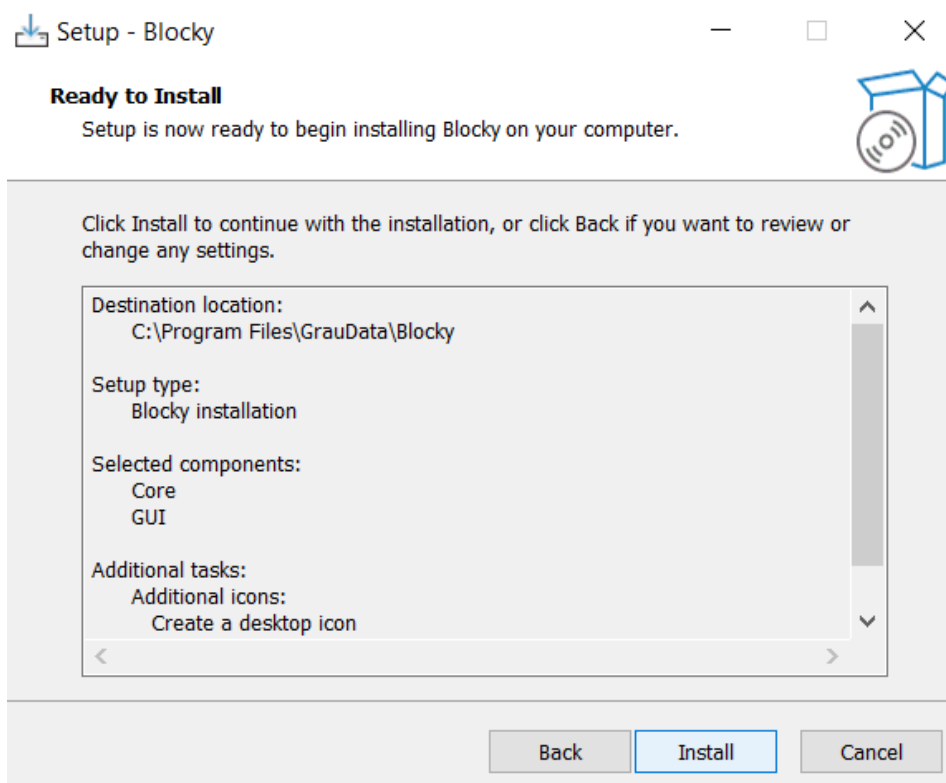
The components can only be selected for a new installation!

If you want to change the components after installation you have to uninstall Blocky and then install it again.



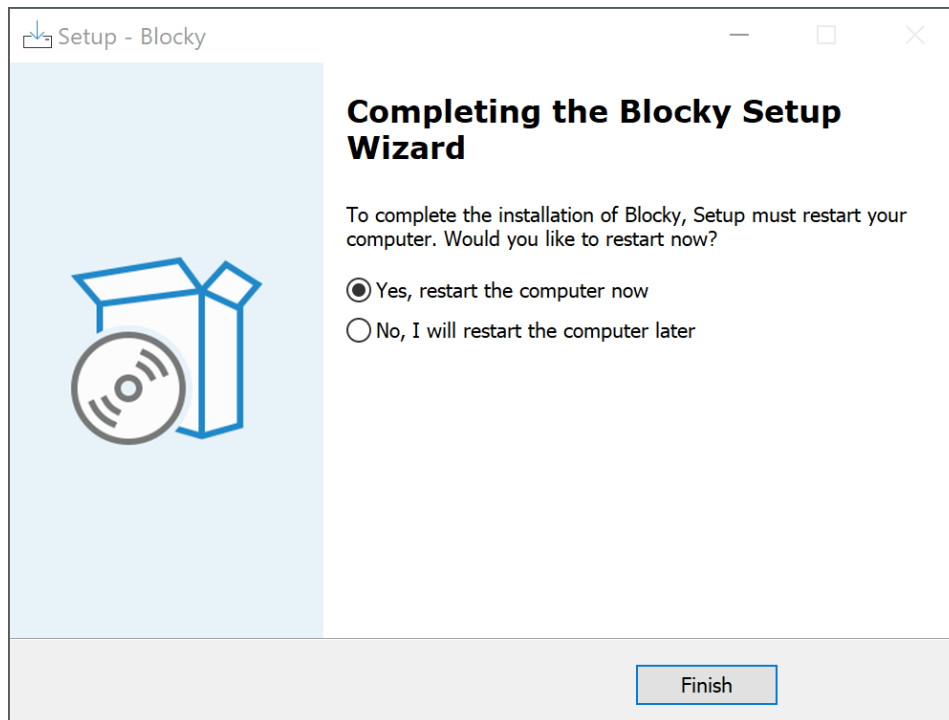


### 3.1.5. Start the Installation



After clicking the Install button, Blocky will be installed to the selected destination folder.

### 3.1.6. Completing the Installation



After clicking on „Finish“, the installation is complete and the system is rebooted, if selected.



From Blocky version 3.5 on, an additional device driver is installed to protect the physical disks. This driver is activated at system startup. If you decide not to restart the system after installation, you will have to restart it manually later for Blocky to work properly.



On Core-only installations, you have to set the initial password via BlockyCLI after installation or with a Blocky setup parameter during installation. See chapters [BlockyCLI](#) and [Setup command line parameters](#).

## 3.2. Updating

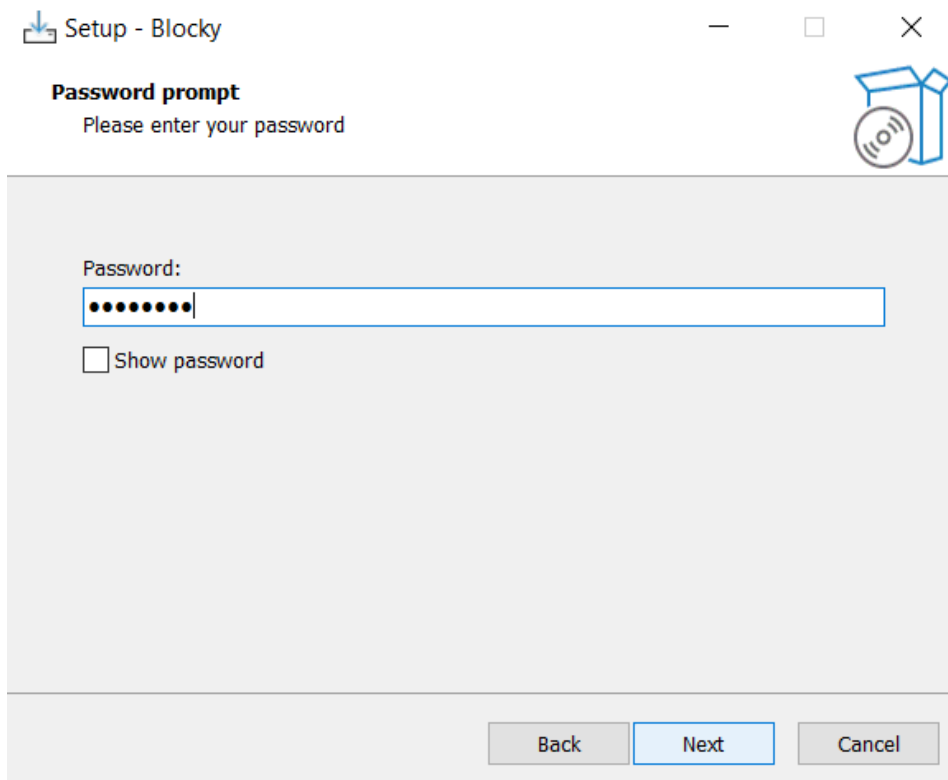
The update process from an earlier 2.6, 2.7 and 3.1 versions is similar to the installation described in chapter [Installation](#).



When updating Blocky a password query is only requested if the core is installed.



If there is a manually added service dependency to the Blocky service, you have to stop the dependent service before updating.



Setup - Blocky

**Password prompt**  
Please enter your password

Password:  
[Masked Password Field]

☐ Show password

Back Next Cancel



When a Central GUI installation is updated, all remote managed Blocky servers must also be updated and vice versa. Central GUI and remote managed Blocky servers must run the same major version, e.g. 2.7 or 3.1.

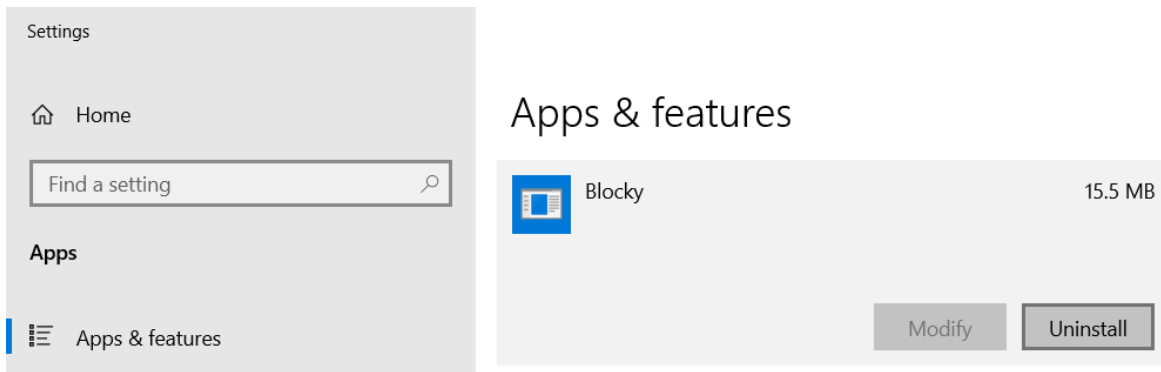
## 3.3. Upgrading from Version 2.5 and earlier

Versions 2.6, 2.7 and 3.x can be upgraded directly from version 2.5. An upgrade from a Blocky version older than 2.5 can only be done with an intermediate upgrade to Blocky 2.5.

The password is entered in the same way as for an update, see [Updating](#).

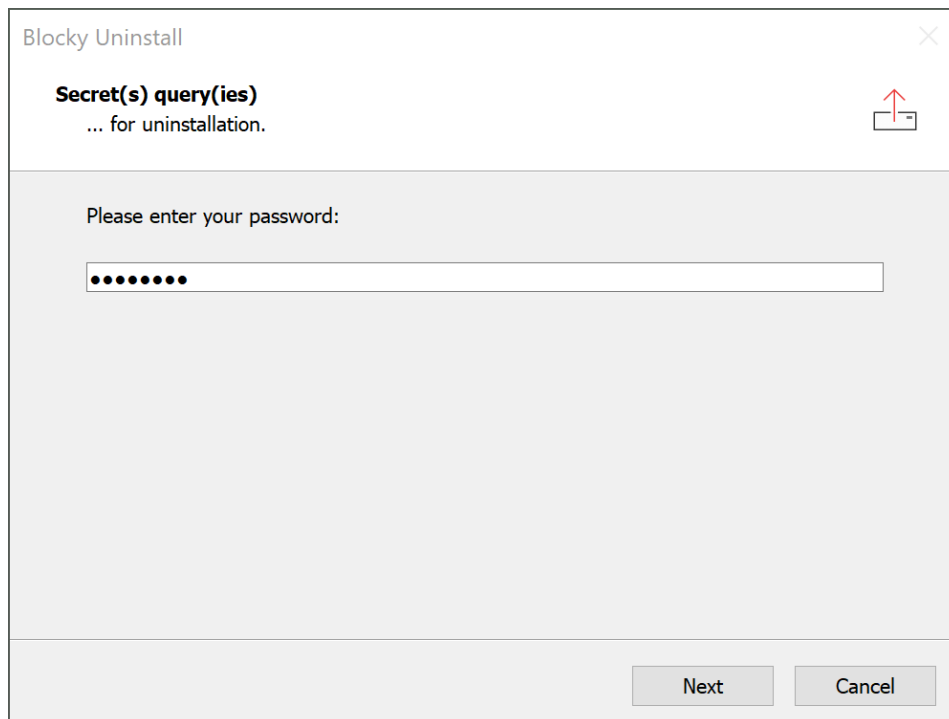
For further information or assistance please contact our GRAU DATA GmbH support ([support@graudata.com](mailto:support@graudata.com)).

## 3.4. Uninstallation



Blocky can be uninstalled by using the Windows Software Manager.  
Click "Start >> Control Panel >> Add or Remove Programs"  
Select the Blocky product and press the "Uninstall" button.

### With core component installed:



Confirm the Uninstallation of Blocky with your password.



To uninstall Blocky the self-defined password must have been set. The uninstallation will fail if the self defined password has not been set. See [Set initial password](#) for setting the password. On GUI-only installations the uninstall password is not required.



If there is a manually added service dependency to the Blocky service, you must stop the dependent service before uninstalling.

### With optional MFA activated:

Blocky Uninstall

**Secret(s) query(ies)**  
... for uninstallation.

Please enter your TOTP:

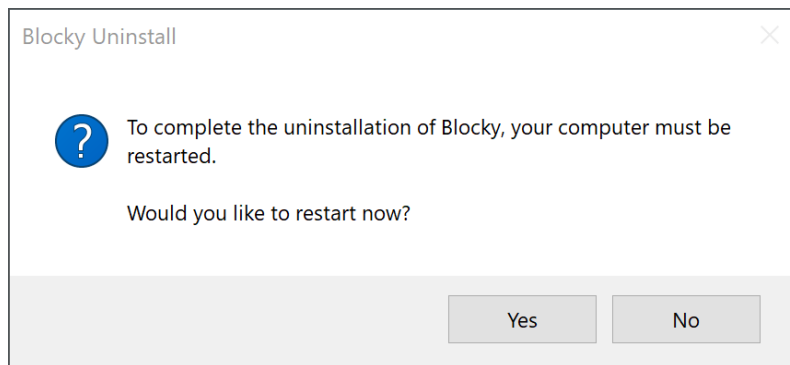
641980

Back Next Cancel

If MFA is activated for this Blocky instance, you must also supply the current one-time token. Continue by pressing “Next”.

## **Complete uninstalled:**

Next click "Uninstall" and Blocky will be removed.



A pop-up message informs if Blocky was successfully removed and a system restart is required.



If you do not restart at this point, you will have to restart at a later time to be able to reinstall Blocky.



# Chapter 4. Configuration

## 4.1. Start of the GUI

In order to configure Blocky run the program **BlockyGUI.exe** by clicking on its desktop icon.



Administrative rights are required to run BlockyGUI. 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 Blocky icon). In case of missing privileges, see chapter [Diagnostics](#) for details.



On Core-only installations the configuration has to be done from a Central GUI or via CLI.

## 4.2. Set initial password

GRAU DATA Blocky instance needs password protection. ×

Define new password:

current password:

new password:

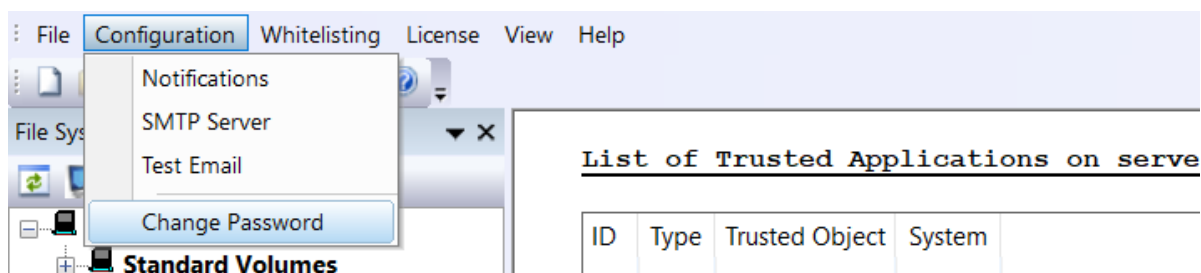
confirm password:

NOTE:  
Password must be at least 6 characters in length and must include at least one number.  
Single or double quotes are not allowed.

To protect the software against unauthorized configuration changes a password has to be supplied for the GUI to launch. When starting the GUI for the first time, you need to set this password. Please note that single quote (') and double quote (") characters are not allowed. This local GUI password also represents the password for the local core components.

To enhance protection, [multi-factor authentication](#) can be activated at a later time.

## 4.3. Change password



The password can be changed via the menu item "Configuration >> Change password".

A screenshot of a dialog box titled 'Change password for GRAU DATA Blocky'. The dialog box has a close button (X) in the top right corner. It contains three password input fields, each preceded by a label: 'current password:', 'new password:', and 'confirm password:'. Each field contains a series of dots representing masked characters. Below the input fields, there is a 'NOTE:' section with the text: 'Password must be at least 6 characters in length and must include at least one number. Single or double quotes are not allowed.' At the bottom right of the dialog box, there are two buttons: 'OK' and 'Cancel'.

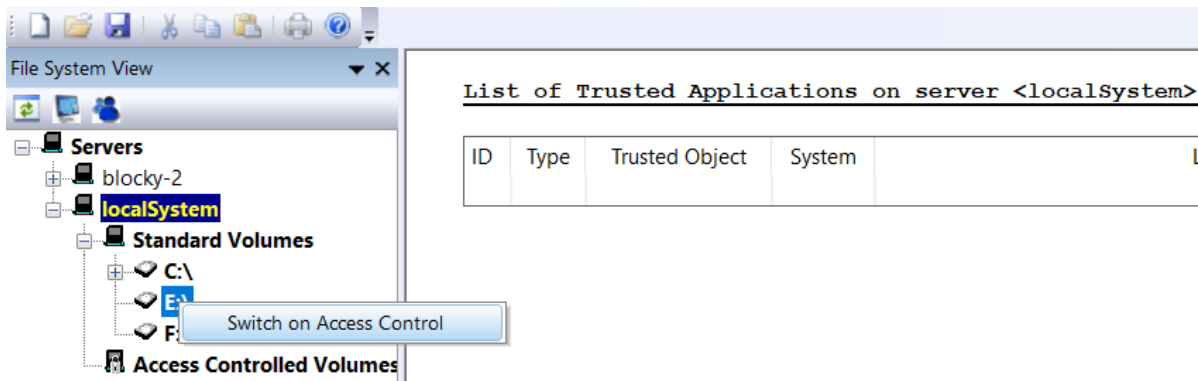
To define the new password, the current password must be provided and the new password needs to be confirmed. The changing process will be finished after clicking "OK".

If you have forgotten the password or if the password has been compromised, you can reset the password. See chapter [BlockyCLI](#).

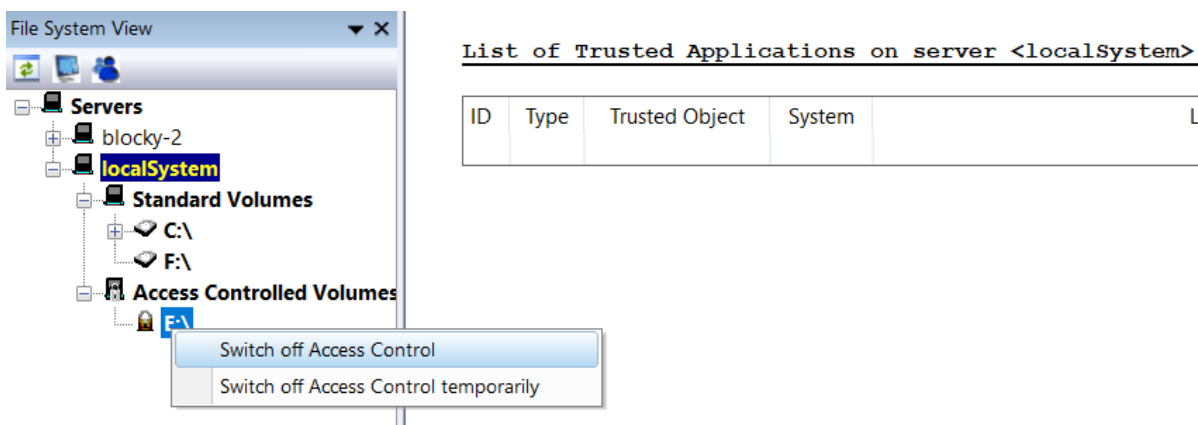
## 4.4. Access Control

Access control can be enabled on a complete volume or on folders on the 1st directory level of a volume. Volumes are shown with their assigned drive letter. Volumes mounted in folders of a parent volume are shown as separate entries in the volume tree.

On access controlled volumes and folders only whitelisted applications have unrestricted file access. Untrusted programs are not allowed to change or modify any existing files.



To enable access control right-click on the root or 1st level folder of the volume in the left pane and select “Switch on Access Control”.



To deactivate access control right-click on the controlled folder and select “Switch off Access Control”.



AccessControl for folder-mounted volumes and their parent volumes are mutually exclusive. Once AccessControl is enabled on a folder-mounted volume, you cannot enable AccessControl on any folder of the parent volume, and vice versa.



It is not recommended to assign both, a driveletter and a folder-mount to a volume. Enabling AccessControl via driveletter while the volume is also mounted in a folder may lead to unsupported configurations and unexpected behaviour.

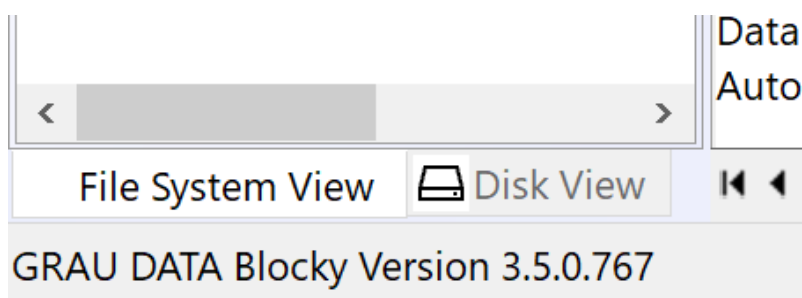


Since Blocky 3.5 it is not possible to enable access control on volumes which are located on the same physical disk as the system volume. See [Restrictions](#).

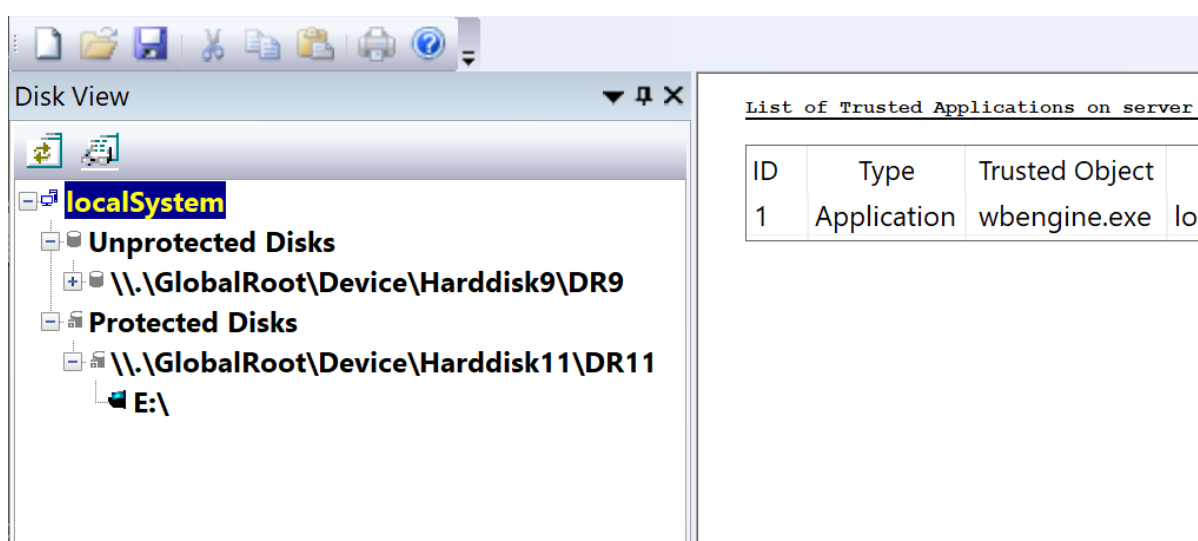
## 4.5. Disk protection


Once [access control](#) has been switched on for a specific volume, Blocky protects the underlying physical disk which contains that Blocky volume. Blocky then prevents any creation or deletion of volumes and partitions performed by standard Windows mechanism on that physical disk. However resizing existing volumes or partitions is still possible.

The tree view on the left-hand side shows the protection status of each physical disk in a separate panel. In the bottom line, you can switch between the view of the file systems (e.g. access-controlled volumes) and the view of the physical disks.



The disk view then shows the protection status of each physical disk, grouped by protected and unprotected disks.

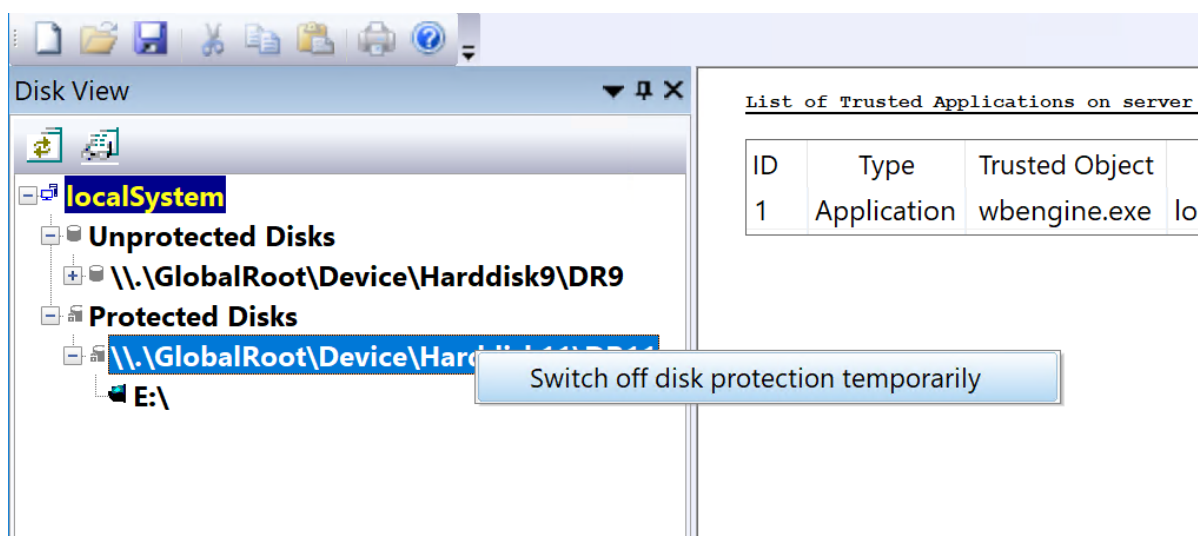


By default, BlockyGUI shows all connected physical disks. When using Windows Storage Spaces, physical disks which belong to a storage pool are hidden by the OS. However BlockyGUI would still show such disks in the disk view. To toggle the visibility of such disks, click on the corresponding icon  in the top of the disk view pane.

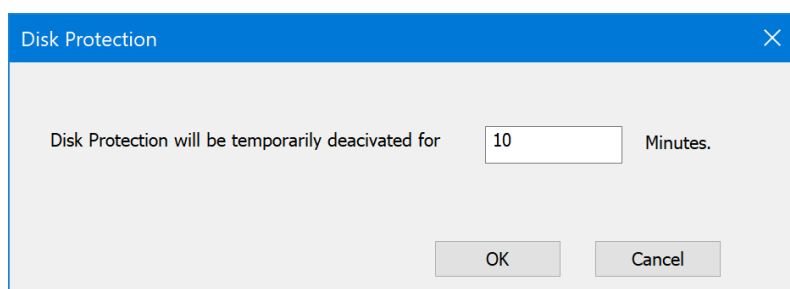


A physical disk is automatically set to protected status if it contains at least one access controlled volume, and is automatically set to unprotected status if it does not contain any access controlled volume or when the last access controlled volume has been switched off.

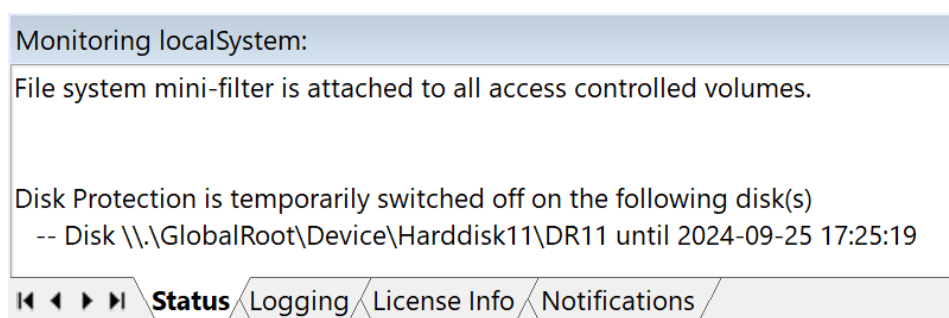
To perform tasks such as creating or deleting volumes and partitions for legitimate reasons, you must temporarily disable physical disk protection.



To disable protection, right click on the desired disk and select “Switch off disk protection temporarily”.



Then select the duration for which the protection is to be disabled.



You can monitor the protection status in the status windows of the BlockyGUI. As soon as the timer has expired, the protection is automatically switched on again.

Managing protection status is also possible via [BlockyCLI](#).

When working with volumes and partitions, please see also notes about [Raw volume access](#).

## 4.6. Whitelisted Applications

Each application that should be able to modify existing data must be included in the whitelist. To do this, a fingerprint of the application is taken and stored as a reference. In regular operation, each write access is then checked to see whether it comes from a trusted application. For this purpose, a runtime fingerprint is created and compared with the reference.

There are several ways to whitelist trusted applications.

### 4.6.1. Automatically whitelist applications



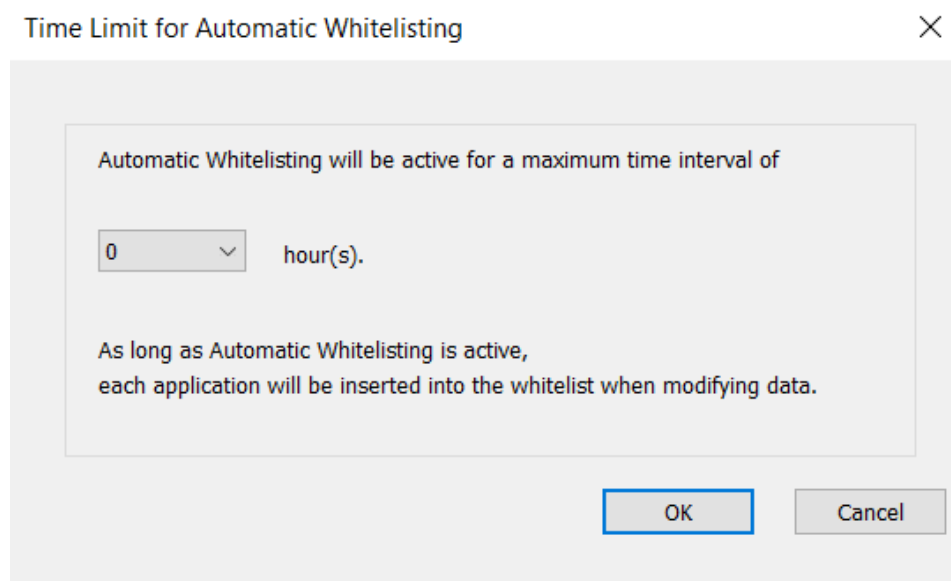
**Caution:**

When using Automatic Whitelisting, ALL access requests are granted and the applications 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 temporarily to configure systems which can be rated as clean and “secure”.

The Automatic Whitelisting feature can be accessed by selecting the menu item “Whitelisting >> Automatic Whitelisting”. At the Automatic Whitelisting Time Limit dialog, use the drop-down list and choose between 1 and 24 hours. After the countdown has ended, automatic whitelisting is turned off automatically.

To manually turn off automatic whitelisting, select menu item “WhiteListing >> Automatic WhiteListing” again.

Please check the list of trusted applications after automatic whitelisting has been turned off and remove any unwanted applications from the list. It is recommended to keep only absolutely required applications!





Do not close the GUI while automatic whitelisting is running. Closing the GUI as well as connecting from another GUI will terminate automatic whitelisting in the background.

## 4.6.2. Manually whitelist applications

Select the menu item “WhiteListing >> Whitelist Programs” from the BlockyGUI main menu and pick the application you want to allow unrestricted file access in the FileBrowserDialog. If the whitelisting process was successful the application is displayed in the table “List of Trusted Applications”.



## 4.6.3. Whitelist via request table

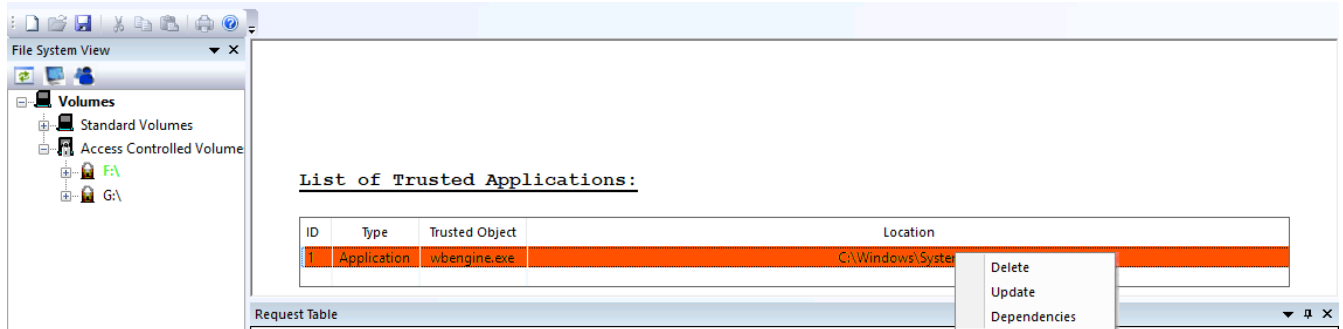
It is also possible to whitelist an application via the request table that pops up in the GUI if a non-whitelisted application tries to modify a file under Access control. See [Request Table](#).

## 4.6.4. Invalid whitelist entry

When a whitelisted application has been modified, e.g. by updating the application or its loaded DLL's, or via malicious manipulation, the fingerprint will change and the corresponding whitelist entry is getting invalid. BlockyGUI will show this whitelist entry marked in red color.

If the modification of the application is known as harmless, the whitelist entry may be updated to re-calculate the fingerprint. To update, right-click on the invalid entry and select "Update".

Updating a whitelist entry is also possible via BlockyCLI. See chapter [BlockyCLI](#).



Detailed information about the modified components of the invalid entry, e.g. the executable itself or one of the loaded DLL's, will be shown in the [dependencies](#) and are also reported in the notification message. See chapter [Notifications](#).



When a whitelist entry is invalid, all write access attempts of that application will be denied. You have to update this entry to grant access.



Do not update an invalid whitelist entry if you are not aware of any expected changes to the system as the system may be compromised.



## 4.6.5. Check module dependencies

If you want to check which dependencies are taken into account when calculating the fingerprint, right-click on an entry in the list of trusted applications and select “Dependencies”. A pop-up window shows all relevant modules. If an entry in the whitelist is invalid, the affected modules are displayed in red.

List of Trusted Applications on server <localSystem>:

ID	Type	Trusted Object	System	Location
1	Application	wbengine.exe	localSystem	C:\Windows\System32
2	Application	svchost.exe (volume access only)	localSystem	C:\Windows\System32

**Program Dependencies**

No	Checksum	Module Name
17	valid	c:\windows\system32\SXSHARED.dll
18	valid	c:\windows\system32\FLTLIB.DLL
19	invalid	C:\Windows\SYSTEM32\WLDAP.DLL
20	invalid	C:\Windows\System32\CRYPT32.dll
21	invalid	C:\Windows\System32\MSASN1.dll
22	invalid	C:\Windows\System32\WINTRUST.dll
23	valid	C:\Windows\System32\kernel.appcore.dll
24	valid	C:\Windows\SYSTEM32\ntmarta.dll
25	invalid	C:\Windows\System32\user32.dll
26	invalid	C:\Windows\System32\win32u.dll
27	invalid	C:\Windows\System32\GDI32.dll
28	invalid	C:\Windows\System32\gdi32full.dll
29	invalid	C:\Windows\System32\clbcatq.dll
30	valid	C:\Windows\System32\cfgmgr32.dll
31	valid	C:\Windows\system32\defragproxy.dll

OK

## 4.7. Notifications

Blocky can send alert notifications to the Windows application event log, to configured email recipients and to the Status Area of the BlockyGUI depending on certain rules. When sending email notifications, multiple recipients can be specified separated by semicolons. To configure notification delivery select the menu item “[Configuration](#) >> [Notifications](#)” from the main menu.

Notification Setup

No	Event	Target	Threshold Count	Threshold Time Interval [min]	Status
1	License Expires soon	Email Notification -> add recipient	n/a	24	Disabled
2	No Valid License	Application Event Log	n/a	1	Enabled
3	No Valid License	Email Notification -> add recipient	n/a	1	Disabled
4	Unauthorized Access	Email Notification -> add recipient	1	0	Disabled
5	Unauthorized Access	Application Event Log	1	0	Enabled
6	WhiteListEntry Invalid	Email Notification -> add recipient	n/a	0	Enabled

Note:  
Right-click to launch context menu in order to insert or delete a row.  
Select "Append" to append a new row or "Delete" to remove a selected row.  
Click on the cell to invoke the inplace drop down list or edit control.

SAVECancel



The preconfigured entries in the notification list only serve as a template. You must configure the desired notifications to suit your requirements.

### The following stateful event types are available:

- no license valid
- license will expire soon
- licensed capacity exceeded
- invalid whitelist entry
- filter unloaded

### The following stateless event types are available:

- unauthorized access (m)
- internal error (m)
- service started (o)
- service stopped (o)

Note: Stateless events may occur only once (o) or multiple (m) times.



The check for invalid whitelist entries is performed on:

- file access from a whitelisted application
- start of Blocky service

The whitelist check investigates whether the entries in the whitelist are still valid or whether the fingerprint of the binary on disk or it's dependent DLL's has changed.

## Notification Rules:

Threshold Count	ThresHold Time Interval [min]	Action
<n>	0	Stateless event: notification is sent after <n> occurrences.
<n>	<m>	Stateless event: notification is sent when the event has occurred <n> times within <m> minutes.
n/a	n/a	Stateless event: event occurs only once and notification is sent once the event has occurred.
n/a	<i>	Stateful event: notification is sent every <i> minutes when the event has occurred. When <i> is set to 0 the notification is sent only once.

### Example: (email notification)

**<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,**

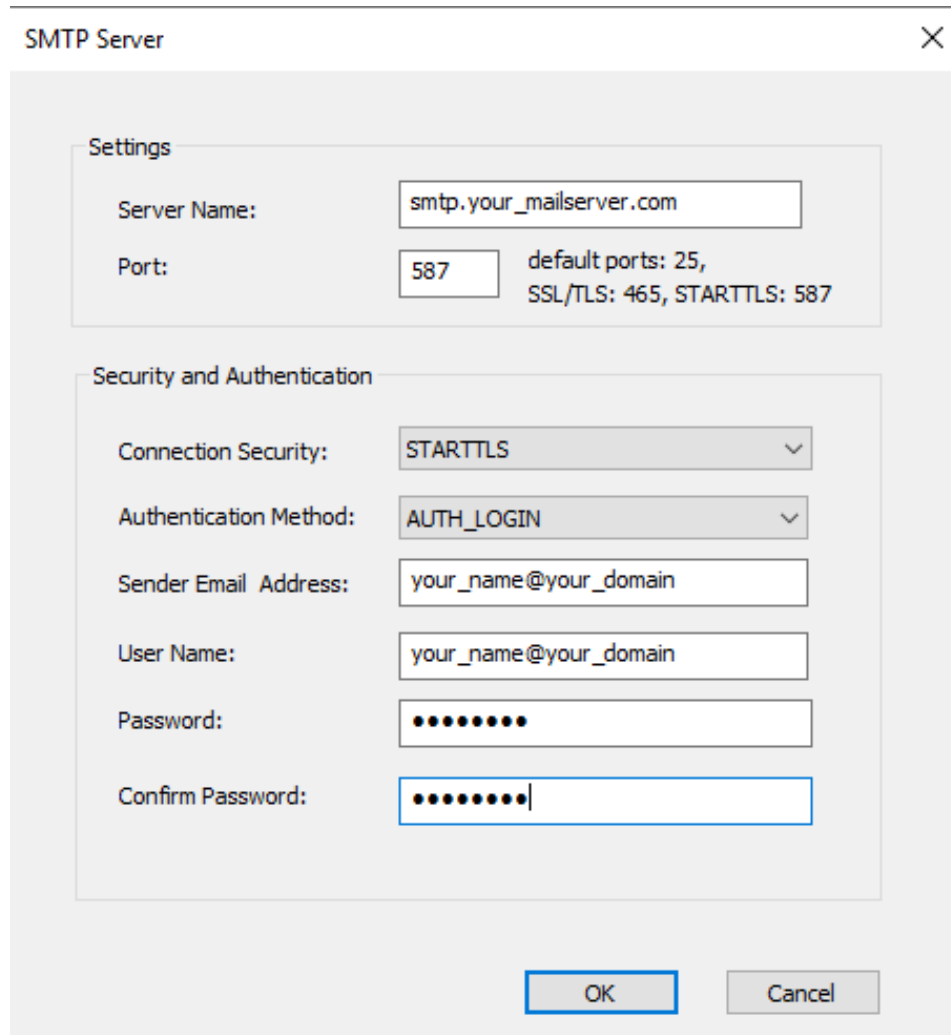
**File: \\?\E:\t1\230\_49\_e.log, User: WIN-DC65PAE604F\Administrator**

### Example: (GUI status area)



## 4.8. SMTP Server Configuration

In order to send notifications to email recipients an outgoing SMTP mail server must be configured. Several connection security options and authentication methods are available. Supply SMTP authentication data if required. Select “Configuration >> SMTP Server” to open the following configuration dialog:



The image shows a dialog box titled "SMTP Server" with a close button (X) in the top right corner. The dialog is divided into two main sections: "Settings" and "Security and Authentication".

**Settings:**

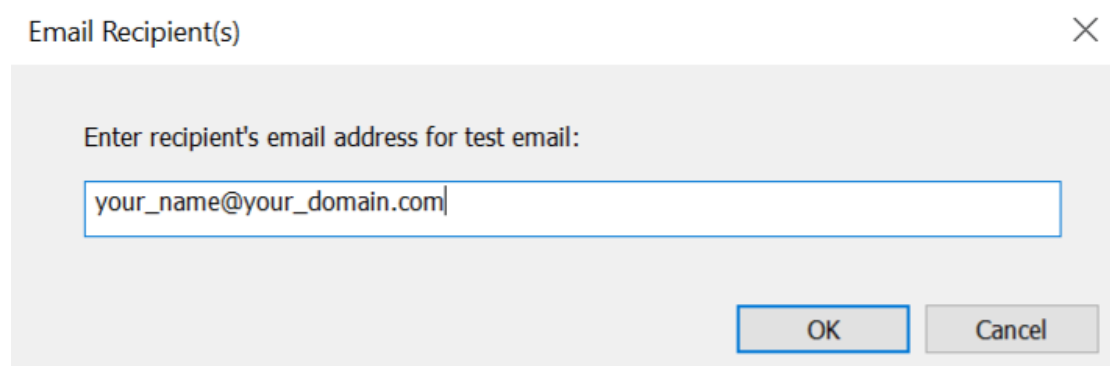
- Server Name:** A text field containing "smtp.your\_mailserver.com".
- Port:** A text field containing "587". To the right of this field, it says "default ports: 25, SSL/TLS: 465, STARTTLS: 587".

**Security and Authentication:**

- Connection Security:** A dropdown menu with "STARTTLS" selected.
- Authentication Method:** A dropdown menu with "AUTH\_LOGIN" selected.
- Sender Email Address:** A text field containing "your\_name@your\_domain".
- User Name:** A text field containing "your\_name@your\_domain".
- Password:** A text field with 10 dots, indicating a masked password.
- Confirm Password:** A text field with 10 dots and a cursor at the end, indicating a masked password.

At the bottom right of the dialog are two buttons: "OK" and "Cancel".

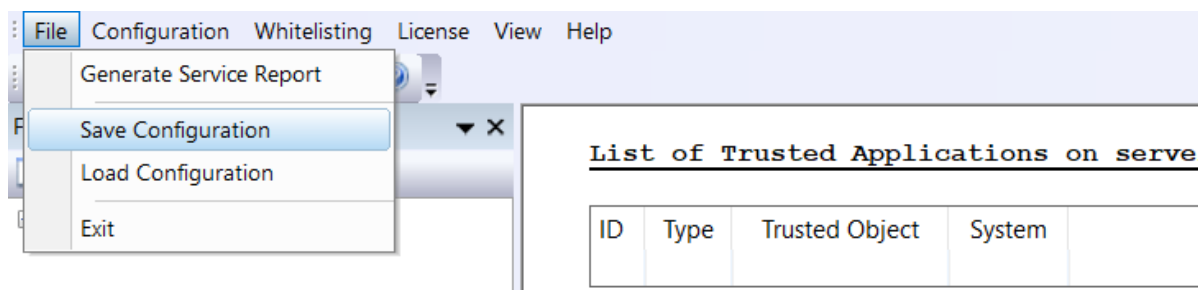
Your settings can be tested by sending a test email to your user account. "Configuration >> Test Email"



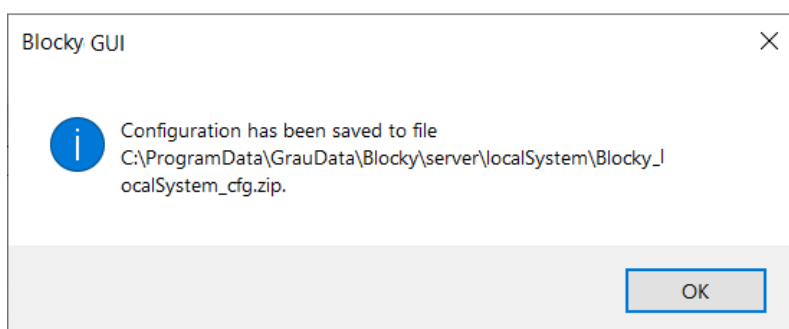
The image shows a dialog box titled "Email Recipient(s)" with a close button (X) in the top right corner. The dialog contains a single text field with the label "Enter recipient's email address for test email:" above it. The text field contains the placeholder text "your\_name@your\_domain.com". At the bottom right of the dialog are two buttons: "OK" and "Cancel".

## 4.9. Save / Load Configuration

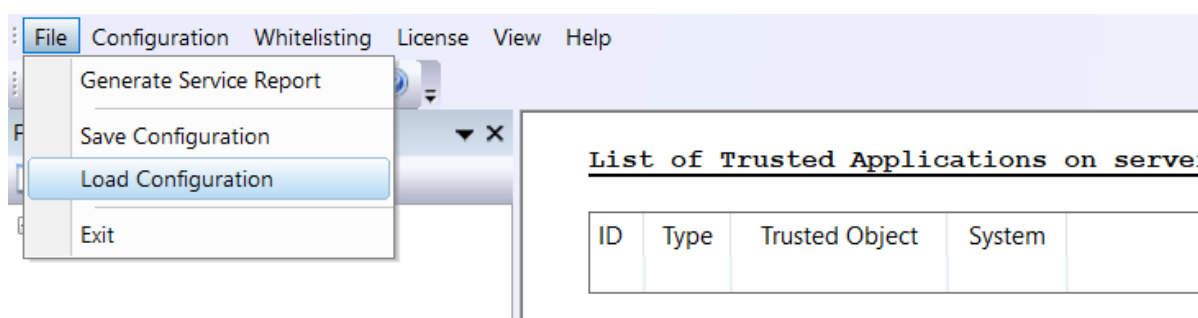
The current configuration can be stored for a later restore. This will store the SMTP Server configuration and other settings for notification and whitelist in the file `C:\ProgramData\GrauData\Blocky\server\localSystem\Blocky_localSystem_cfg.zip`.



To save all configuration settings select the menu item “File >> Save Configuration”.



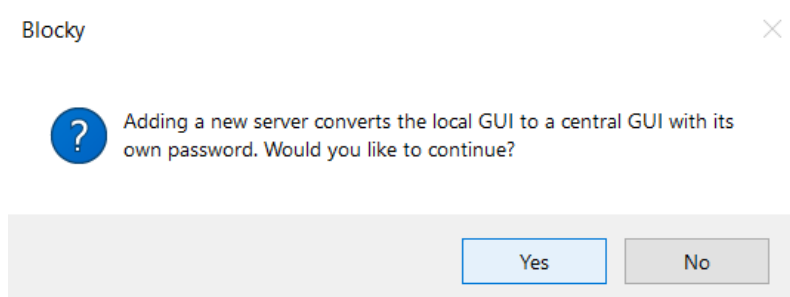
To restore configuration settings use “File >> Load Configuration” and navigate to a previously saved configuration file.



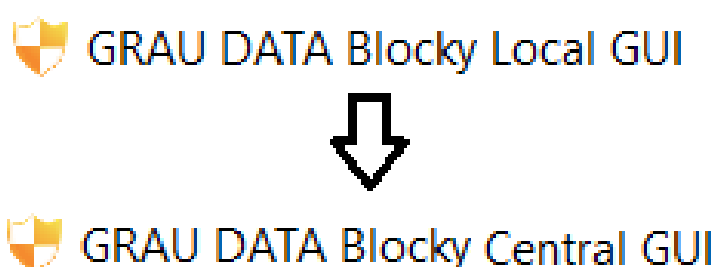
In Central GUI Mode, save configuration will store the configuration from the active connected server on the system running the Central GUI in a corresponding subfolder in path `C:\ProgramData\GrauData\Blocky\server\`. Load configuration will restore the configuration then from this location.

## 4.10. Central GUI Mode

After installing Blocky with Core and GUI components, the GUI is in the local mode. On GUI only installations (without local Core components), the GUI is already in central mode. The operation mode of the GUI is shown in the heading of the GUI. By adding a server to a local GUI, the GUI has to change its mode from local mode to central mode. Accept the warning with "Yes" to continue.



The heading of the GUI changes.



When first adding a new server a new password for the central GUI has to be set. On GUI only installations, the initially defined password is already set for central GUI mode.

A dialog box titled "GRAU DATA Blocky Central GUI needs password protection." with a close button (X) in the top right corner. The dialog contains the following fields and text:

- "Define new password:" label.
- "current password:" label followed by an empty text input field.
- "new password:" label followed by a text input field filled with 10 dots.
- "confirm password:" label followed by a text input field filled with 10 dots.
- "NOTE:" label.
- A note text: "Password must be at least 6 characters in length and must include at least one number. Single or double quotes are not allowed."
- At the bottom right, there are two buttons: "OK" (highlighted with a blue border) and "Cancel" (disabled, greyed out).



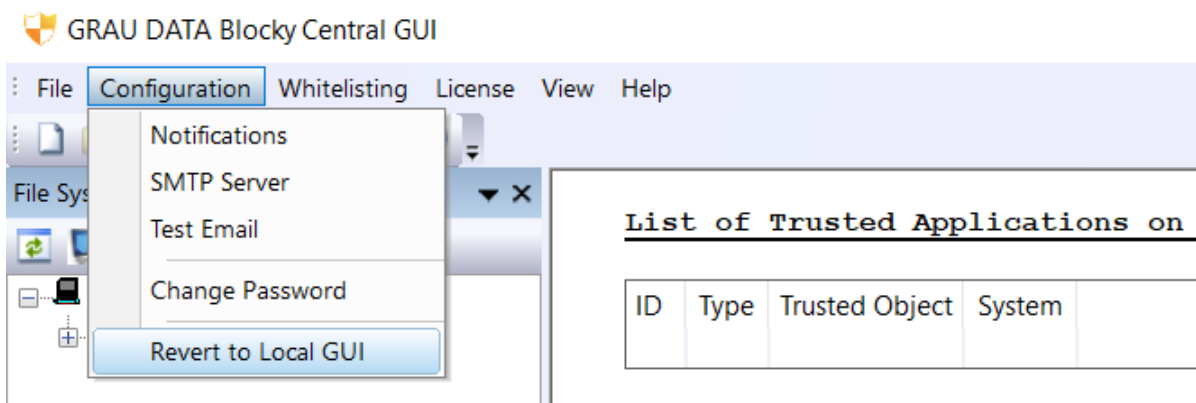
By changing the operation mode from local GUI mode to central GUI mode, the newly defined password is valid for the central GUI only. The previously used password from local GUI mode is still valid for the local core components.



In central GUI mode you always have to select a server for managing and configuring. Any configuration changes (e.g. whitelisting, notifications, licensing etc.) will be applied to the selected server only, except for LicenseHub configuration which will be applied globally.

## Revert to Local GUI:

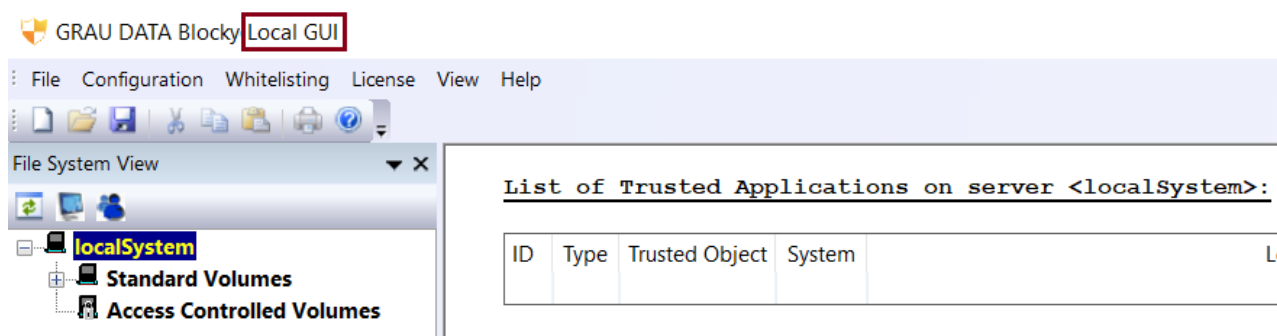
To revert from a central GUI to a local one you first have to remove all configured servers and groups. Then a new menu item will show up. Select the menu item “**Configuration** >> **Revert to Local GUI**”. The Item is only visible when the GUI is in central mode with empty server list.



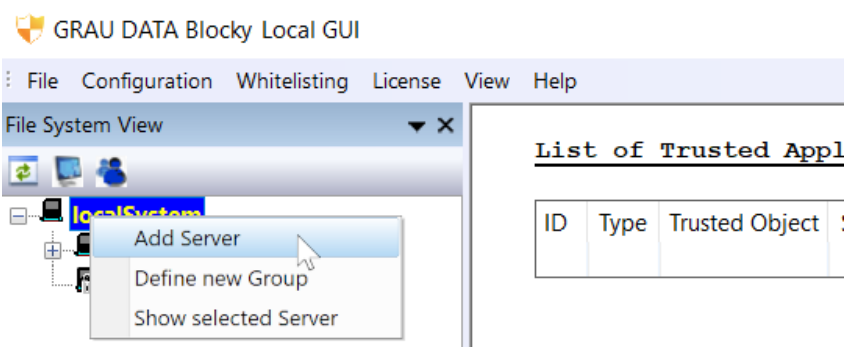
To recreate the entry for the localSystem the GUI needs to be restarted.

## 4.11. Add server

Change the operation mode from local GUI to central GUI by adding a server to the GUI.



To add a server right-click on "localSystem" under the "File System View" and select "Add Server". Once the GUI has changed to central GUI mode, right-click on "Servers" to add another server.



For successful connections from the central GUI to remote servers, the system running the central GUI must be able to ping the remote server (i.e. send ICMP echo requests) and the remote server must allow incoming connections on the Blocky service port (default port **7880/tcp**). Please adjust firewall settings accordingly. When using built-in Windows firewall, you have to enable existing inbound rule **File and Printer Sharing (Echo Request)** and also add a new inbound rule for default port **7880/tcp**. Furthermore the central GUI and the remote systems must run the same major version. See chapter [Updating](#).



Please make sure the initial password on the remote server has been set. Either via local GUI if installed, via BlockyCLI or via Blocky setup parameter. See chapters [BlockyCLI](#) and [Setup command line parameters](#).



Please make sure the system clock of the remote server is in sync with the system running the central GUI. If the service authentication fails please check system clock.



Fill in the following dialog with the data of your server. Use the “Check connection” button to check whether your server is available. You can only add the server if the check was successful.

Add Server

✕

Server Name:

blocky-2

Hostname/Ip-Address:

192.168.252.68

Port:

7880

Permanent Connection

☒

Description

testblocky

Group:

no group assignment ▾

Password:

●●●●●●●●

CHECK Connection

OK

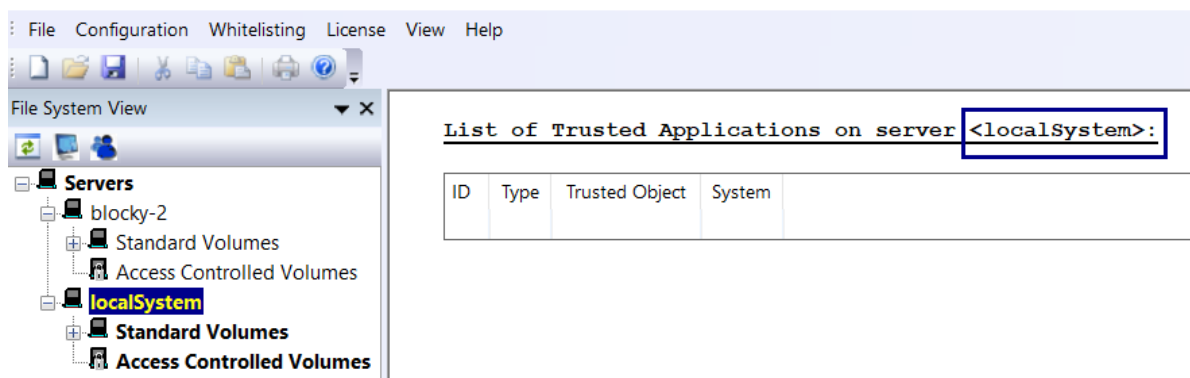
Cancel



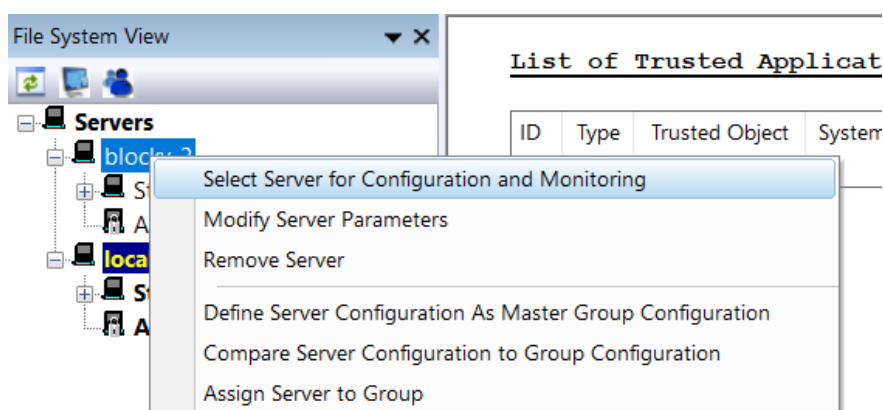
If the Server to add has MFA activated, you also have to supply the one-time token for the Central GUI to connect successfully. See chapter [MFA for Central GUI](#)

## 4.12. Server selection

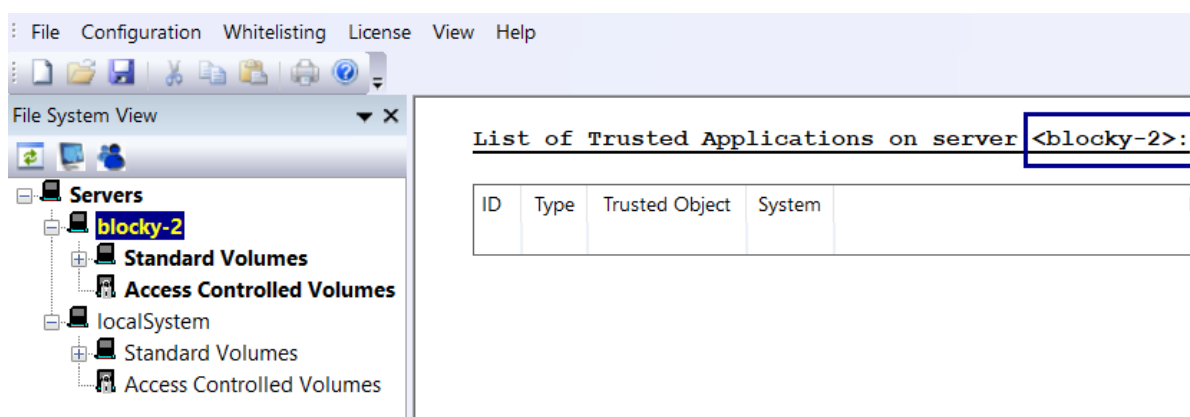
Per default the **localSystem** is selected for configuration and monitoring. The selected server is displayed in a yellow color with dark blue background, it can be configured and its List of trusted Applications, Request Table and other Informations are shown in the GUI.



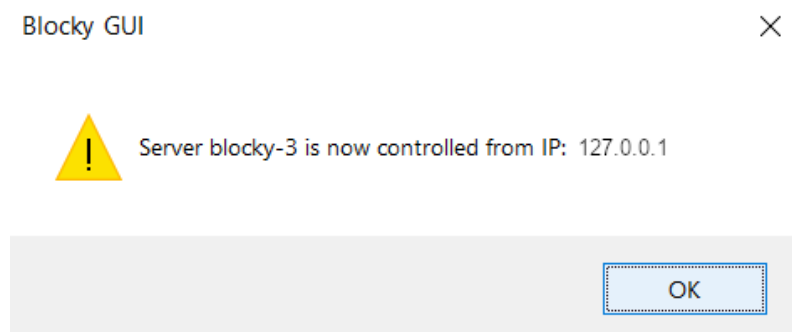
To change the server context right-click on the server you want to configure and select "Select Server for Configuration and Monitoring". This will change the context within the GUI for configuration and monitoring to the selected server.



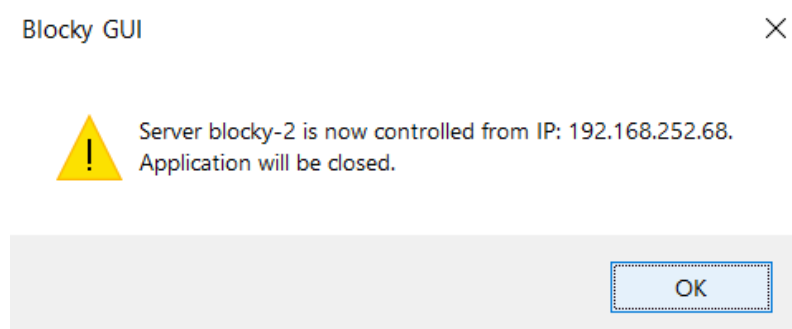
When the connection is established the highlight color changes and your selected server appears in yellow color with dark blue background and the list shows the Trusted Applications on the server.



When a server has an active connection from the central GUI and the local GUI is started and connected on that server, the connection from the central GUI will detach.

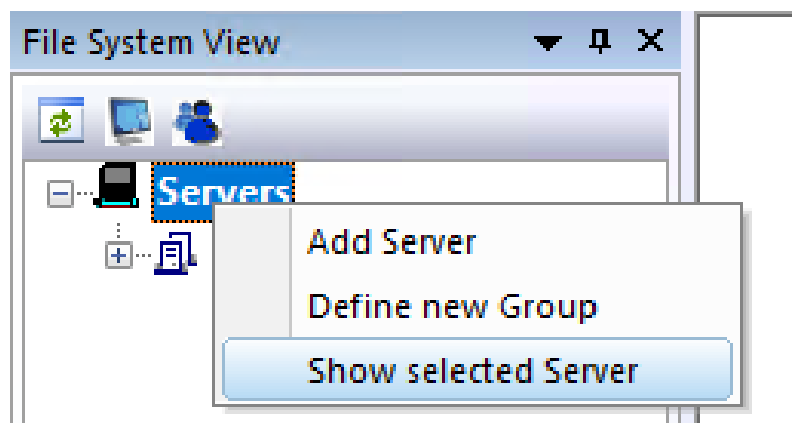


When a server has an active connection from the local GUI and the central GUI does open a connection to that server, the connection from the local GUI will detach and the local GUI is closed.



Each server can handle only one active connection at a given time, either from the local or a central GUI.

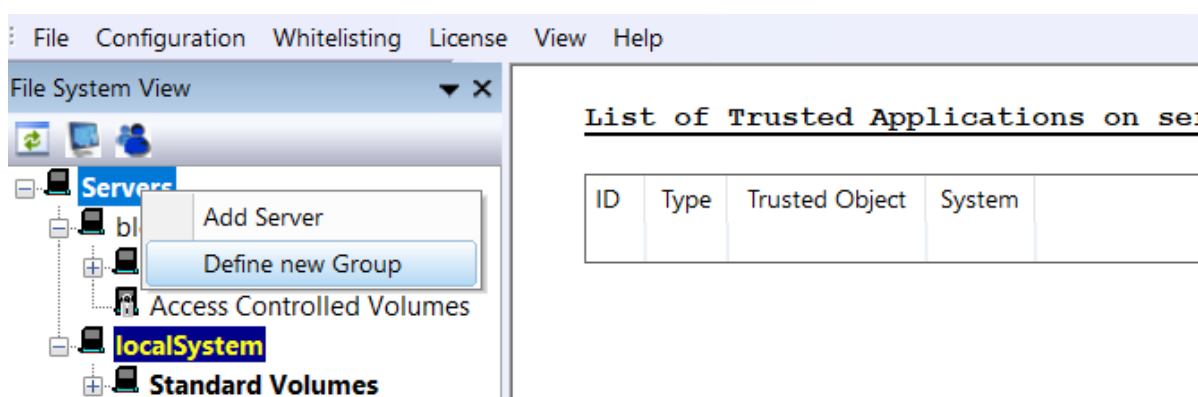
If you have configured many servers and groups in a central GUI, you can quickly navigate to the currently selected server by right-clicking on "Servers" and selecting "Show selected server".



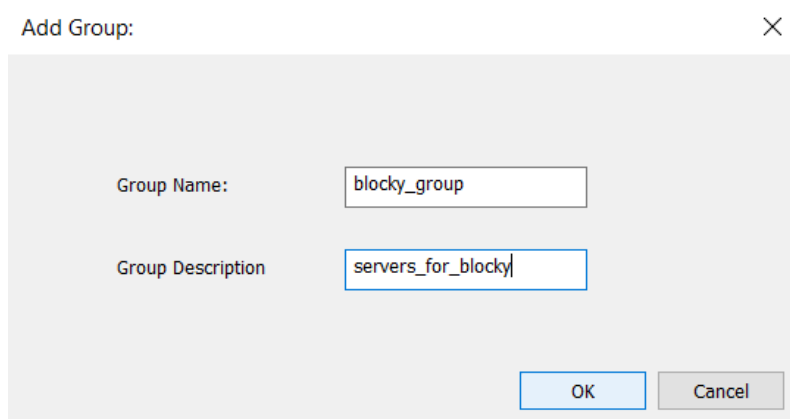
## 4.13. Define a new Group

If you have multiple servers that share a common configurations of Trusted Applications, Notification and Mail settings or Controlled Folders you can collect those servers in groups and define a master config of these parameters that can be applied to all group members.

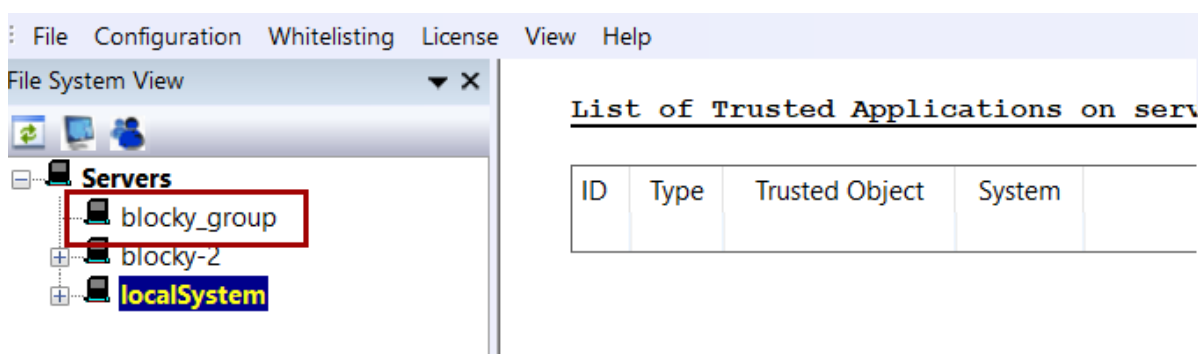
To define a new group right-click on "Servers" under the "File System View" and select "Define new Group".



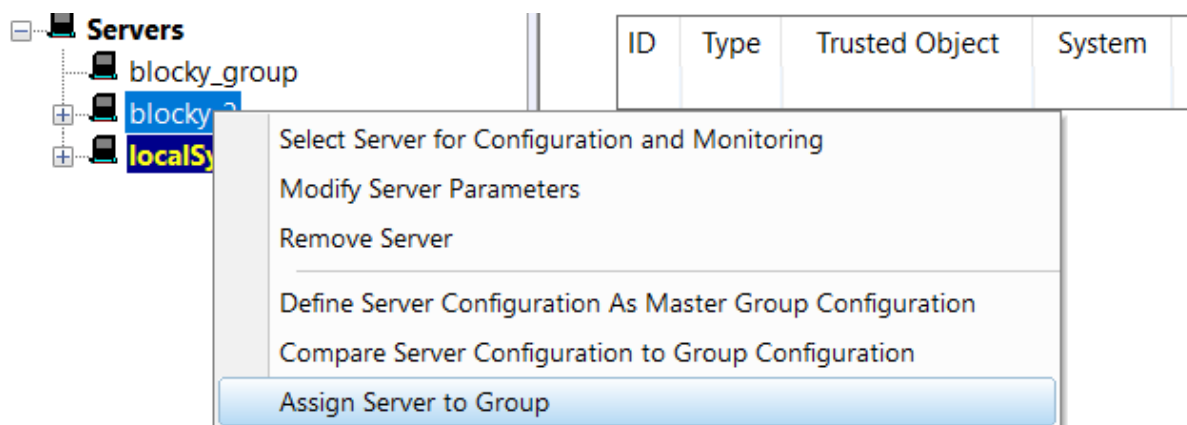
Name your group and fill out the description box. After clicking "OK" your group will be added.



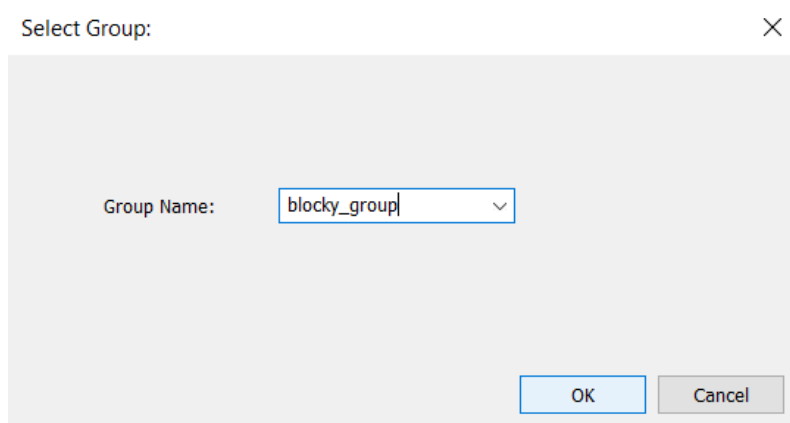
The group will be listed under "Servers" in the "File System View".



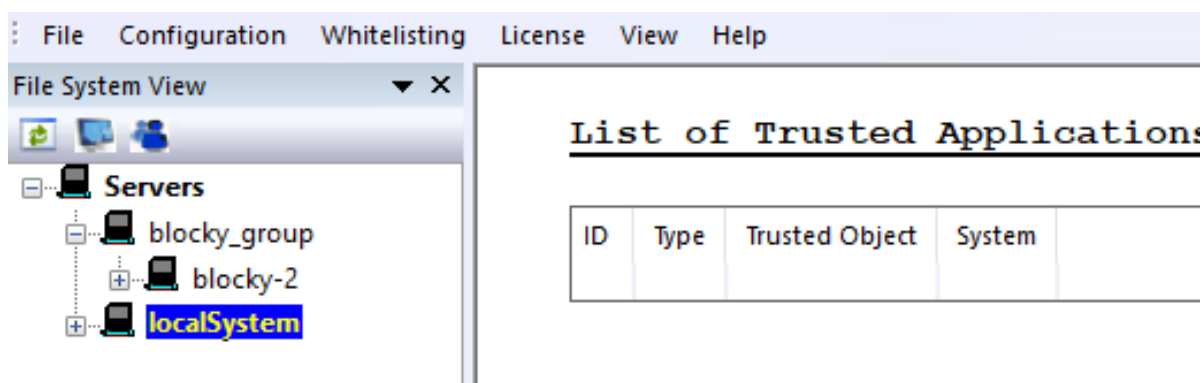
To assign a server to a Group right-click on the server you want to assign and select "Assign Server to Group".



Then select the group the server should be assigned to.



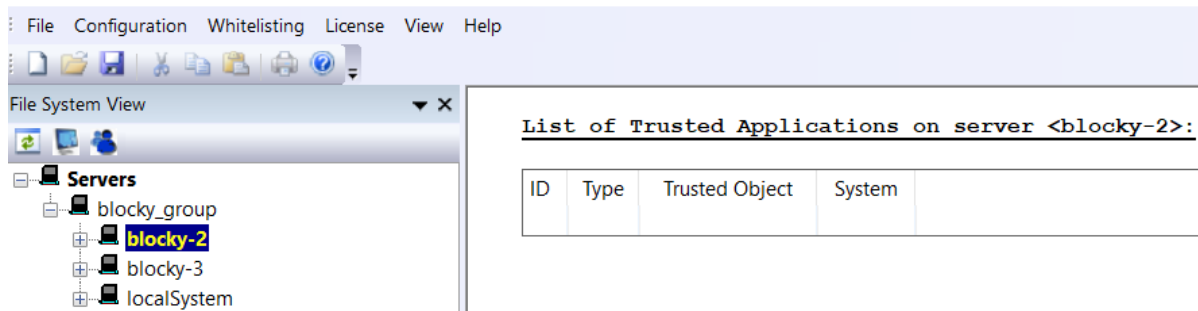
In the "File System View" this server is now listed under the selected group.



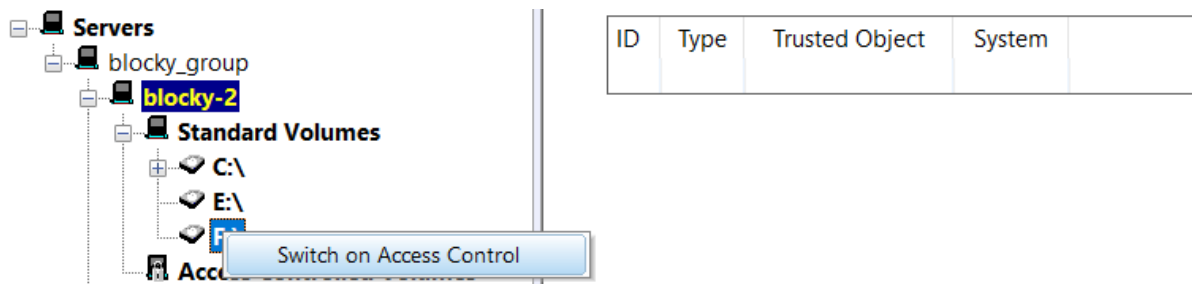
## 4.14. Master Configuration

By defining a master configuration for a group you can apply the configuration from a specific server to all servers in the defined group. Master configuration includes whitelist, controlled folders and notification/SMTP settings.

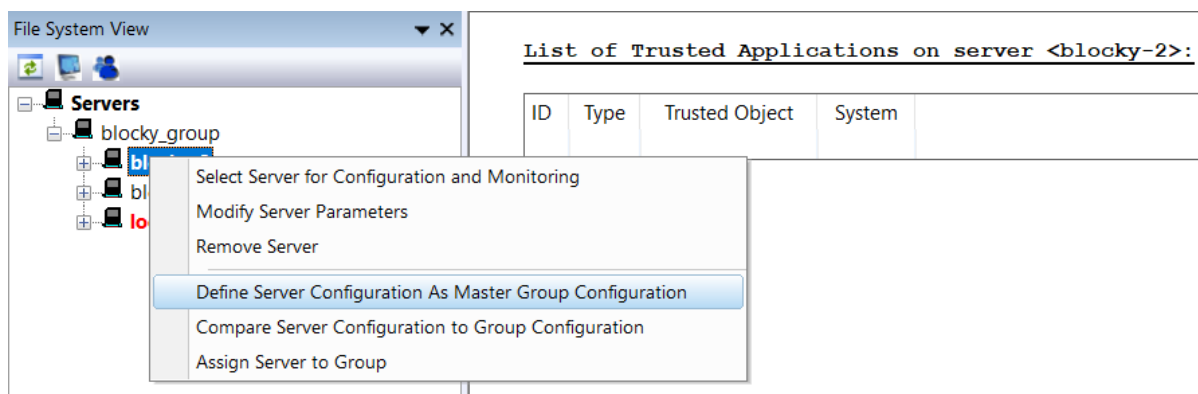
Select a server for Configuration and Monitoring.



Configure the desired settings on this server. For example, switch on access control on a volume.



Define the group master configuration by selecting "Define Server Configuration As Master Group Configuration".

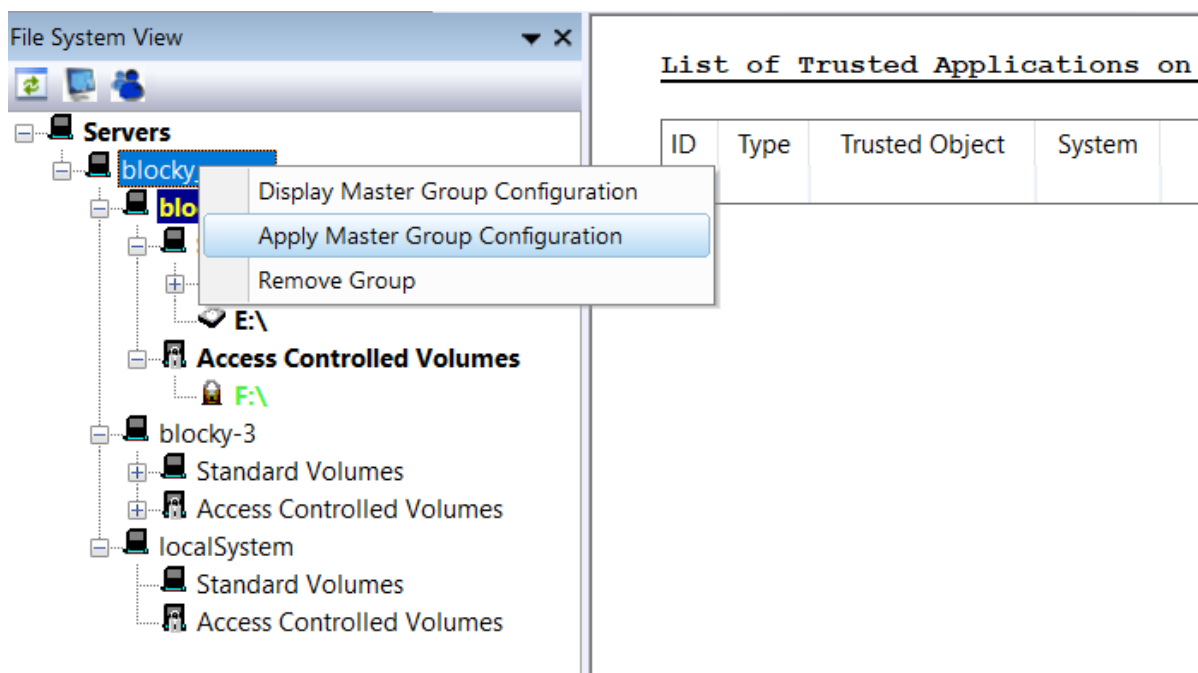




Current configuration of server <blocky-2> has been defined as group configuration of group <blocky\_group>.

OK

The configuration can now be published by right-clicking on the group and selecting "Apply Master Group Configuration".



Would you like to apply the Master Group Configuration of group <blocky\_group> to group members?

Yes

No

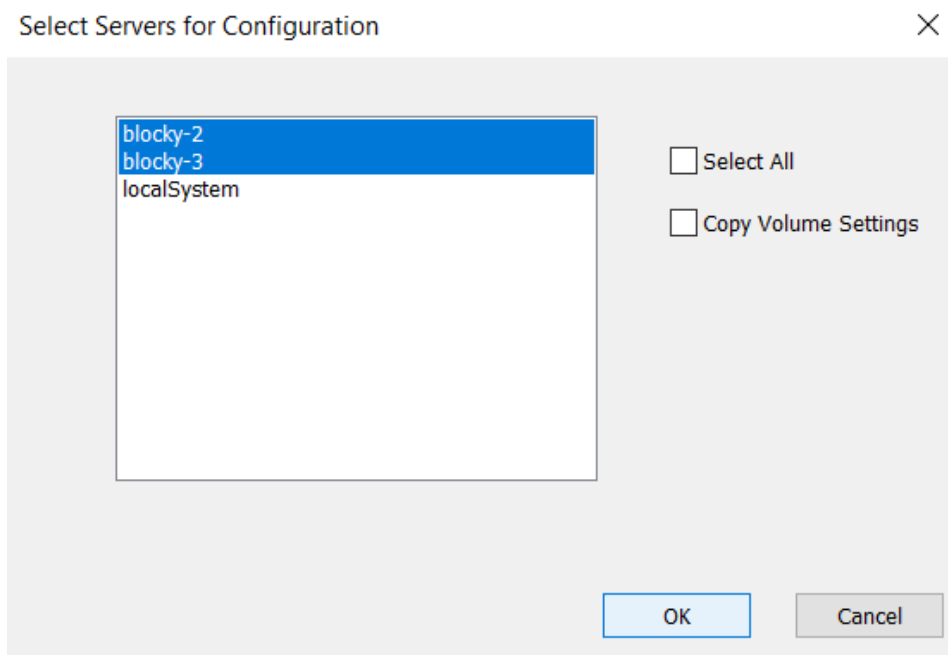
Select the servers where the Master Configuration shall be applied.

Select "Copy Volume Settings" to transfer the access control settings for the volumes from the Master Configuration too.



**Caution:**

On the target systems, the access control of other already access controlled volumes, which are not part of the Master Configuration, is switched off if "Copy Volume Settings" is enabled.



Blocky GUI



Successfully rolled-out configuration to selected group members.

OK



This configuration is now applied to the selected servers in the group.

File System View

Servers

blocky\_group

blocky-2

Standard Volumes

C:\

E:\

Access Controlled Volumes

F:\

blocky-3

Standard Volumes

E:\

Access Controlled Volumes

F:\

localSystem

Standard Volumes

Access Controlled Volumes

List of Trusted Applications

ID	Type	Trusted Object	System

Request Table



If some servers are not connected in Central GUI and the rollout of the configuration would fail, you have to choose to reconnect these servers or to rollout only to connected servers. If you choose to reconnect, any local connected GUI will terminate and the Central GUI will take over. You then have to initiate the configuration rollout again.

Blocky GUI



The following group member(s) are NOT connected: W2K22  
Would you like to apply the Master Group Configuration to the connected servers ONLY?  
<No> will cancel the rollout to all selected servers (connected or not).

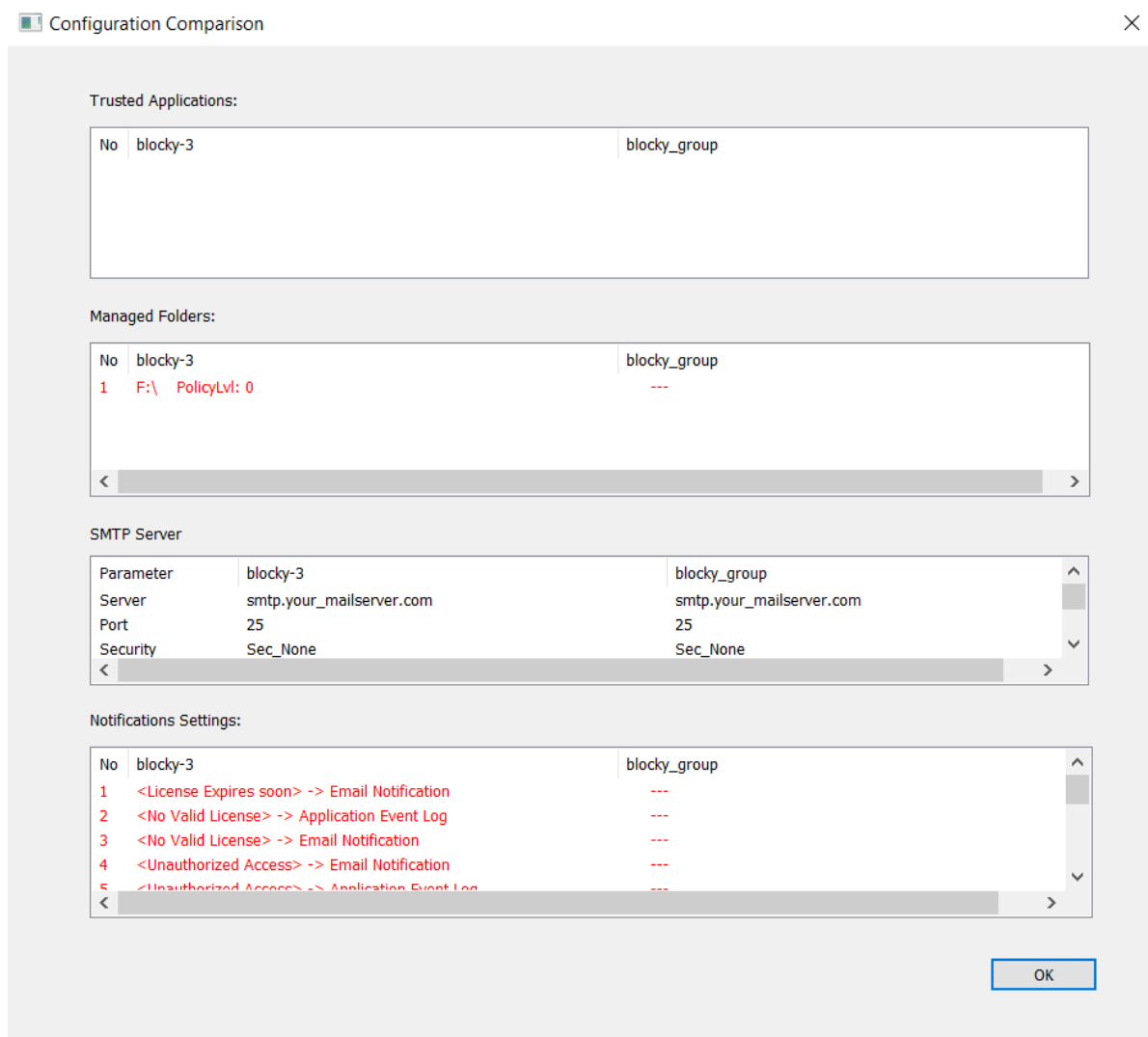
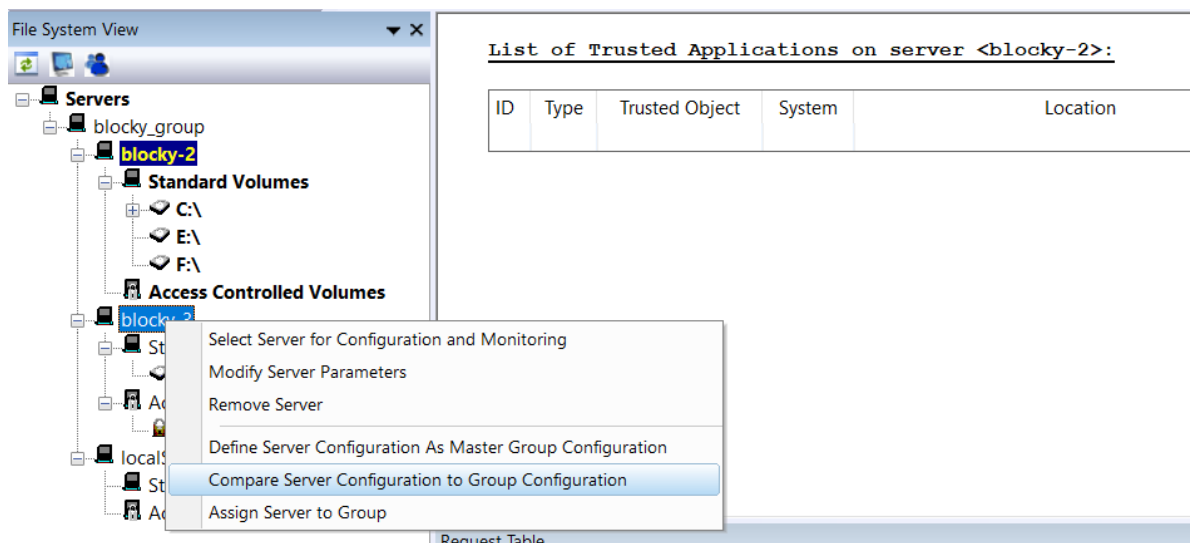
Yes

No

To apply/rollout all configurations all servers must be connected. If some servers are not connected you can apply the configuration to only the servers connected by clicking "Yes" or stop the process by clicking "No". Then try to reconnect the remaining servers and repeat the procedure.

## 4.14.1. Configuration Comparison

To compare a server configuration with the master group configuration, right-click on the server you want to compare and select "Compare Server Configuration to Group Configuration".



## 4.15. Licensing

Blocky allows the use of a fresh activated Blocky volume for 60 days. The trial license has neither a capacity limit nor a limit of the number of Blocky volumes. Every volume receives this trial license when the Access control is switched on for the first time. If you want to keep a Blocky volume past the trial period, you need to register the volume to obtain a key for a registered license.

When using the GUI in central mode, licensing is performed for the currently selected server.

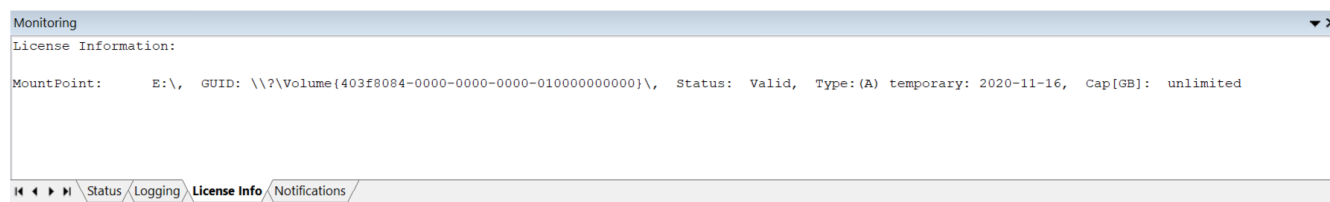
Licensing is also possible via BlockyCLI. See chapter [BlockyCLI](#) for available CLI commands.

The following section about [initial licensing](#) applies to standard licensing on a per-volume base. For large environments, licensing is also possible via a separate licensing service. See section [LicenseHub](#) then.

### 4.15.1. Initial Licensing

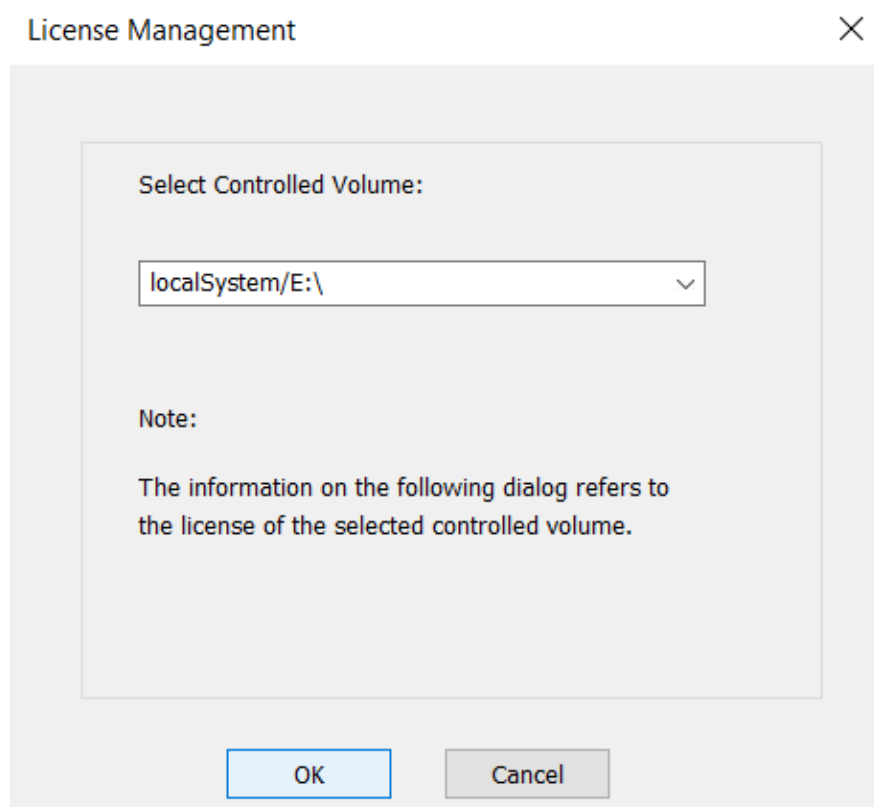
If the Access Control feature is activated on a volume, the temporary trial license for 60 days will be automatically installed on that volume. Licensing is always volume-based, which means that a license must be ordered for each volume which should be protected by Blocky.

You can see your current status in the "Monitoring" window.

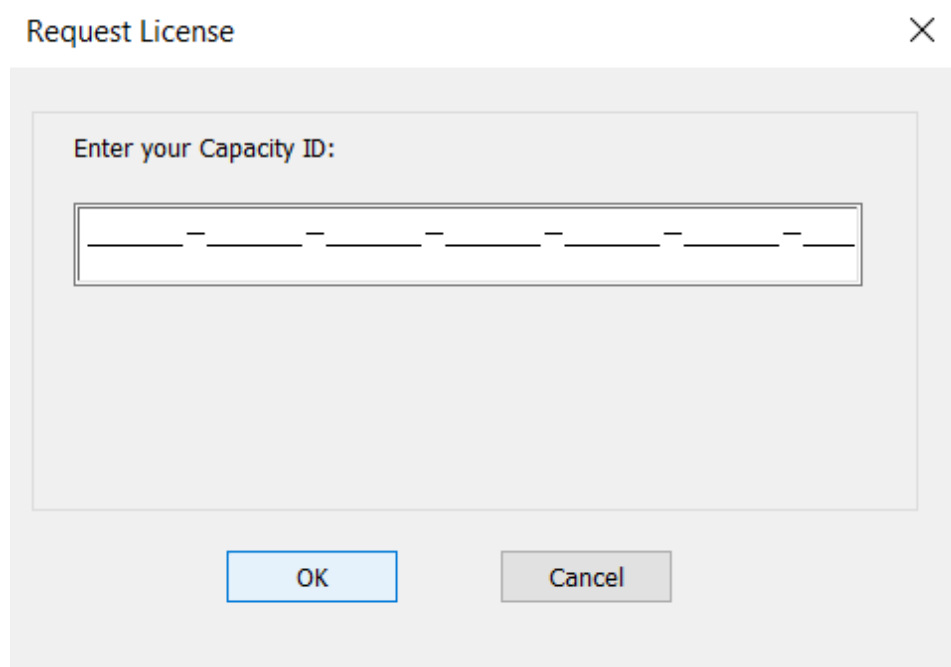


Each Blocky volume is registered separately and therefore has its own Blocky generated Capacity-ID, which is needed when requesting a registered license key for a Blocky volume.

Select the menu item “License >> Request License” from the main menu.



Use the drop-down list and choose the volume for which you want to request a license key.



Enter the Capacity-ID, which you have received from your Blocky sales representative. Characters are automatically converted to upper case when entered in lower case.

Request License ✕

Enter your Capacity ID:

HG-676H-GJ89-VVGH-09SD-FVHH-RNKM

OK Cancel

After pressing the “OK” button Blocky generates the license request key, which must be sent to the licensing service by using either the online WEB-PORTAL or sending the information via email.

Request License ✕

License Request Information

C847-CWY6-T5CC-5ER9-FV3Z-P5Z4-XRVV-9VA5-4UPX-4YT3-!

< >

Request License Key by ▾

- WEB-PORTAL -preferred-**
- MAIL...
- SAVE Request Key to file
- SEND Request Key to Clipboard

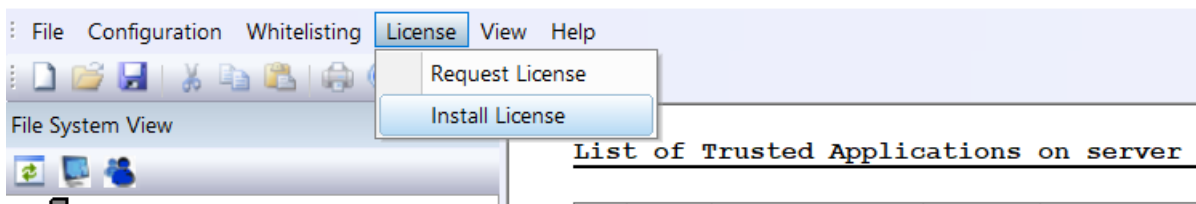
OK Cancel

Please ensure that your server is connected to the internet, when choosing the "WEB-PORTAL" for requesting the license key. To access the licensing service you have to log in to the WEB-PORTAL. If you do not yet have log-in credentials, please register and provide a valid email address, which is used by the licensing service to respond back to you.

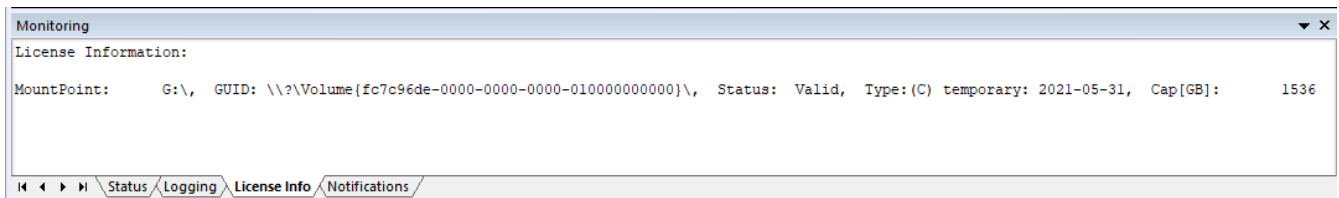
If you decide to send the license key request via email, you may either use the menu item "EMAIL...", which launches your email client and automatically generates an email with the necessary information or you may copy the license request key to a text file and send it as an email attachment to [support@graudata.com](mailto:support@graudata.com).

## 4.15.2. Install License

After receiving the registered license key file for the volume, select the menu item “License >> Install License” from the main menu.



Check the license status on the right-side pane of the BlockyGUI. It may take up to 4 minutes until the license status is updated.



When using the GUI in central mode you can concat several license files into a combined file, one license per line. The central GUI will install the licenses on all available servers with the corresponding volumes.

## 4.15.3. License update and renewal

After you have installed the registered license initially, you can still add additional capacity to a Blocky volume or extend the license time limit by an updated license key file. The updated license key file must be requested via “License >> Request License” and installed via the menu item “License >> Install License” as well. The previously entered Capacity-ID is not required anymore.

You may request a new license key file at any time, however the resulting license key file reflects your currently purchased license. To receive a license file with additional capacity or extended timeframe, you must purchase an additional license from GRAU DATA GmbH sales or your local distributor first before requesting an updated license.

Blocky monitors the overall physical capacity on each Blocky volume and the license time limit, and displays a warning message in the application event log when a Blocky volume exceeds the licensed capacity or time limit.

If either the capacity or time limit is exceeded, the license gets invalid and access protection also denies modification requests from whitelisted applications until an updated license key is installed for the volume to cover the overall capacity or extend the time limit.

As a workaround to gain write access on a Blocky volume with invalid license, an Administrator may disable access protection for that Blocky volume manually. Access protection must be enabled again before installing a valid license.

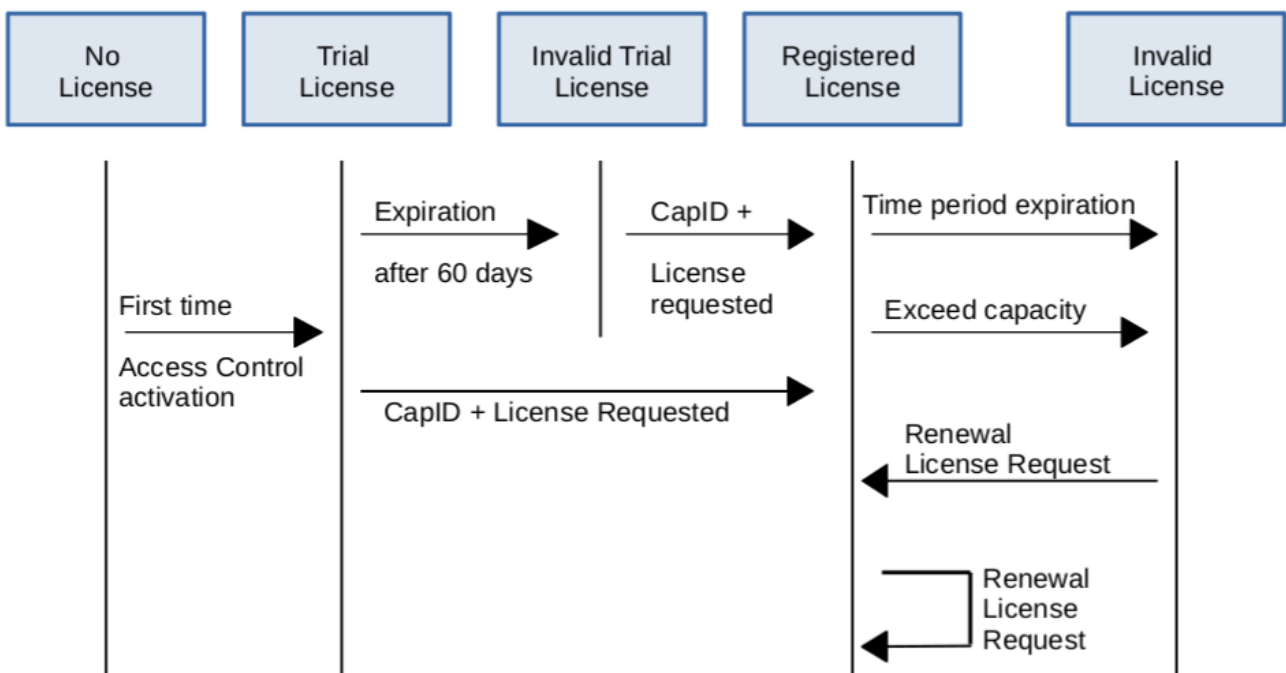
The Blocky user interface provides an overview of the installed license types, status and licensed capacity. It is recommended to request and install a new license before the installed license expires or the volume's physical capacity is extended.



During Upgrade from Blocky version 2.4 to version 2.5 or later, all valid licenses will be migrated automatically. To update or renew such migrated licenses at a later time, you must send a [Service Report](#) to GRAU DATA GmbH support ([support@graudata.com](mailto:support@graudata.com)) first before requesting an updated license key file. Invalid, e.g. expired licenses, are not migrated during upgrade. To obtain a valid license for such Blocky volumes you must follow the [initial licensing](#) workflow which requires a valid Capacity-ID.

## Summary:

- Each license is volume based.
- The trial license is valid for 60 days after activation.
- The trial license has no capacity limit.
- The registered license has a time and capacity limit (depending on the purchase).
- Capacity is the volume provisioned size not the used space.
- An invalid license denies any modification on existing files (on the affected volume).

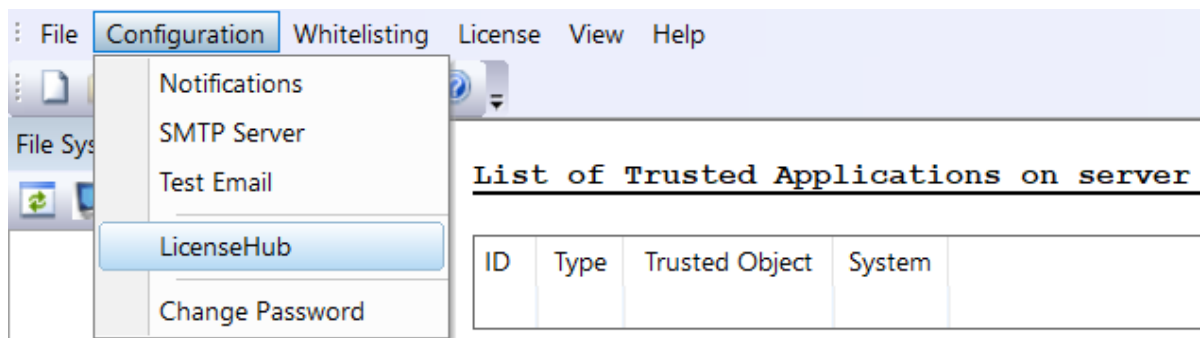




## 4.15.4. Using LicenseHub

In large environments with several Blocky servers and volumes, licensing is also possible with LicenseHub instead of stand-alone licensing on a per-volume base. Licenses for all Blocky volumes are requested from LicenseHub automatically and regularly refreshed.

For installation and configuration of LicenseHub, please refer to the LicenseHub admin guide. At least one Blocky license has to be installed on the license server of LicenseHub for use with Blocky servers.



Open the LicenseHub configuration via the menu item "Configuration >> LicenseHub".

LicenseHub ✕

Location

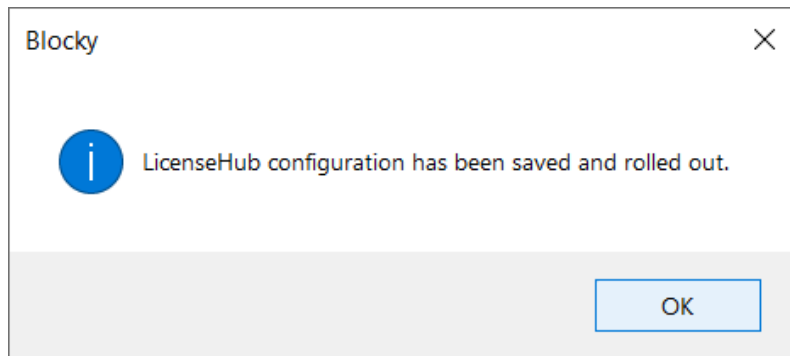
Hostname/IP-Address:

Port:

Password:

Confirm Password:

Enter the hostname/IP-address, port of the license server and set a password. Confirm by pressing the "Ok"-Button.



Blocky negotiates now all license requests with the license server of LicenseHub.

To disable the usage of LicenseHub leave the hostname empty and press "OK".



- Central GUI can only configure the same LicenseHub for all Blocky servers assigned to it.
- A configured LicenseHub in Central GUI will be immediately activated on connected (or later reconnected) servers. The same applies to removing the LicenseHub from Central GUI configuration.
- For Blocky servers with configured LicenseHub usage, managed volumes will get more or less immediately the license lease from LicenseHub. They will not run in an evaluation mode.
- To enforce evaluation mode for Blocky volumes, the LicenseHub configuration of this Blocky server must be disabled before activating the volume for the first time. If the server is managed by a Central GUI with configured LicenseHub, the server must be removed from Central GUI and managed locally.
- LicenseHub assigned licenses for Blocky volumes will be valid for 30 days, but will be refreshed automatically.
- Unused volumes should be set to unmanaged by switching off the access control permanently in the Blocky configuration. Then the license lease is reverted back immediately and the license capacity is available in the LicenseHub capacity pool. Otherwise it's blocked for the rest of the expiration time frame (currently max 30 days).

## 4.16. Multi-factor authentication

Beginning with version 3.5.0 Blocky supports Multi-factor authentication to enhance protection of the GUI and CLI. Blocky has implemented time-based one-time passwords (TOTP) defined by OATH in RFC 6238. You can therefore use any authenticator application of your choice that supports such TOTP tokens and uses QR codes to set up accounts.

MFA is an optional feature that can be activated individually for each Blocky instance. After activation, you must always enter both the password and the one-time token for all actions that previously only required the password.

By default, each Blocky instance uses its own so-called shared secret. This means that if you have multiple Blocky instances, you will need to set up separate accounts for each instance in your authenticator app. If you want to have only a single account for all your instances, you have to activate MFA via [CLI](#) using the same self-defined shared secret. This secret has to be a string of 16 characters in the range 2-7A-Z.



Once MFA is activated, you must always supply the token in addition to the password also for the CLI. Follow the [CLI guide](#) on how to provide the password together with the token.



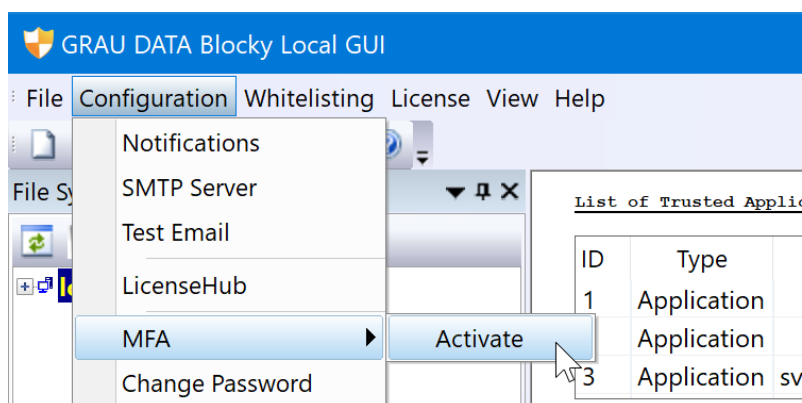
Due to the TOTP algorithm, the one-time token changes every 30 seconds. Make sure that you always enter the currently valid token.



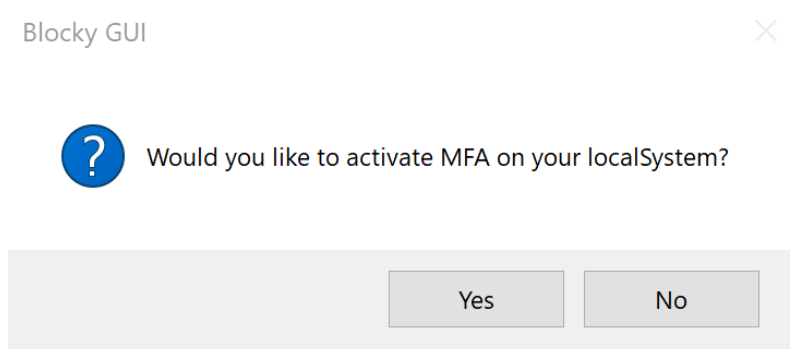
MFA relies on a synchronized time between the components involved, i.e. the Blocky systems and the Authenticator app. Make sure that all devices have a valid system clock. If you use Central GUI with MFA-enabled managed instances, these must also have a synchronized clock.

## 4.16.1. MFA for Single / Local Instance

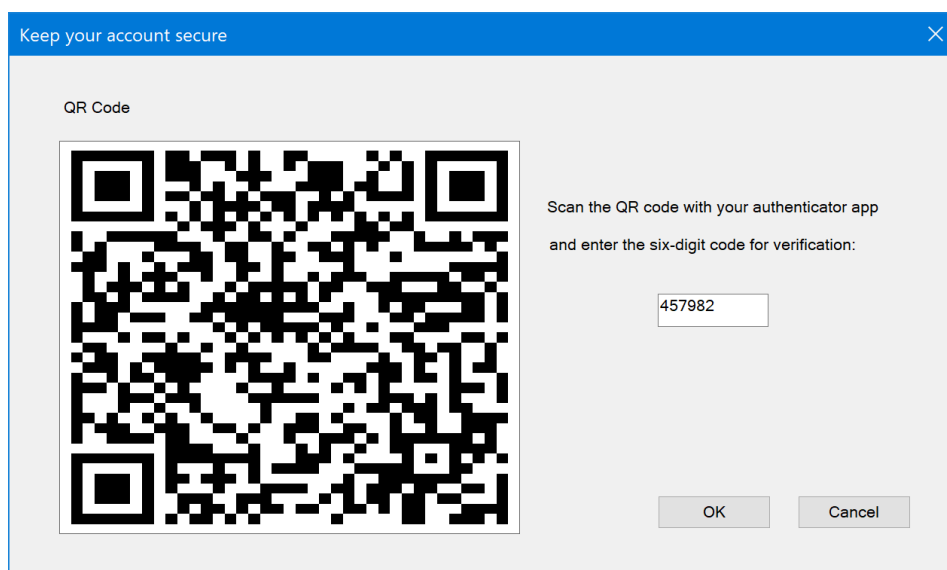
You can activate MFA for single respectively local instances via GUI and [CLI](#).



Activate MFA via the menu item "Configuration >> MFA >> Activate".



In the next popup window select "yes" if you want to activate MFA.



You will then be shown a QR code. Use this QR code to create an account in your authenticator App. Then enter the generated token from the newly created account for verification and click "OK".



MFA has been activated on your localSystem.

OK

The MFA is only activated if you enter a valid token.

If you want to set up another authenticator app at a later time you can get the required QR code via the menu item "Configuration >> MFA >> Show QR Code". To deactivate MFA and revert back to password only, select menu item "Configuration >> MFA >> Deactivate". To manage MFA via CLI, refer to the [corresponding chapter](#) in the appendix.



If you have lost your authenticator app and you are not able to generate valid tokens anymore, you must perform the password reset procedure via GUI or [CLI](#). This will reset the password and also an activated MFA.



For Blocky installations where the installed GUI serves as the Central GUI, all MFA-related actions of the GUI only affect the Central GUI. To activate MFA for the local core, you must use the [CLI](#).

## GUI Logon:

The image shows a dialog box titled "MFA OTP Input" with a close button (✕) in the top right corner. The main text inside the dialog says "Enter your 6-digit one-time code". Below this text, there are six input fields, each containing a digit: 6, 2, 8, 4, 6, and 6. At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

The next time you start the BlockyGUI, you must enter the currently generated token after you have entered the password.

## 4.16.2. MFA for Central GUI

The MFA activation of the Central GUI is separate from the MFA status of the managed Blocky instances, i.e. you must set up a separate account in your Authenticator app for this.

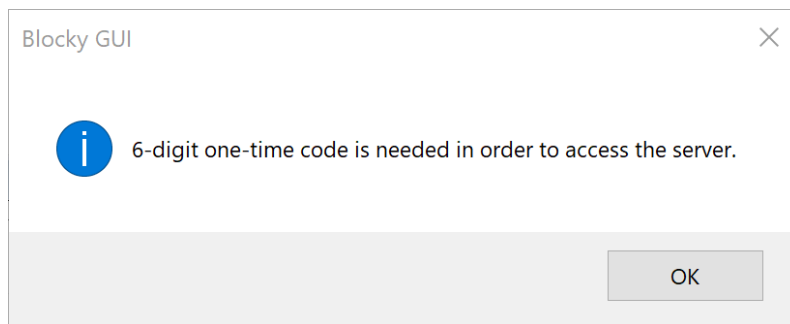


You can activate MFA in the Central GUI while the managed instances are still running without MFA and vice versa. However, if at least one of the managed instances has MFA enabled, we highly recommend to also enable MFA for the Central GUI.

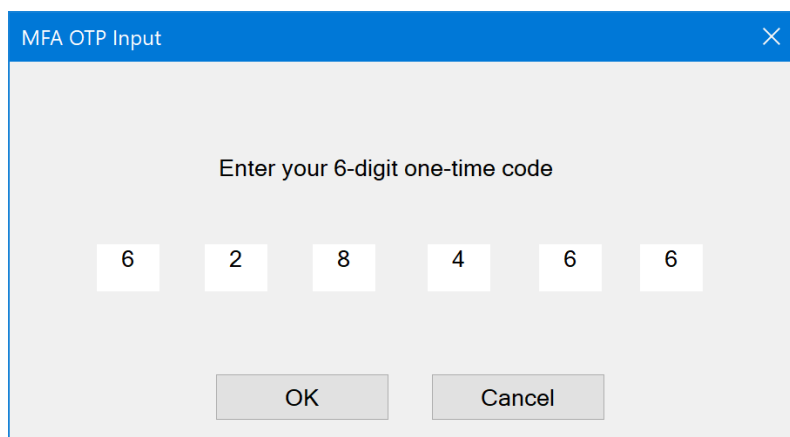
The activation of MFA for the Central GUI works in the same way as for a local instance via the GUI menu "[Configuration](#) >> [MFA](#) >> [Activate](#)". See the beginning of this [chapter](#). The same applies to displaying the QR code and deactivation. As soon as MFA is activated, you will be prompted to enter the one-time token each time you log in to the GUI.

### Adding a server with MFA:

If you add a server with activated MFA, you must also specify its one-time token for the connection to the Central GUI. You will find general instructions on adding servers in the [add server chapter](#). After you have clicked on “OK” and checked whether the connection was successful, the Central GUI determines whether MFA is activated on the managed server to add.



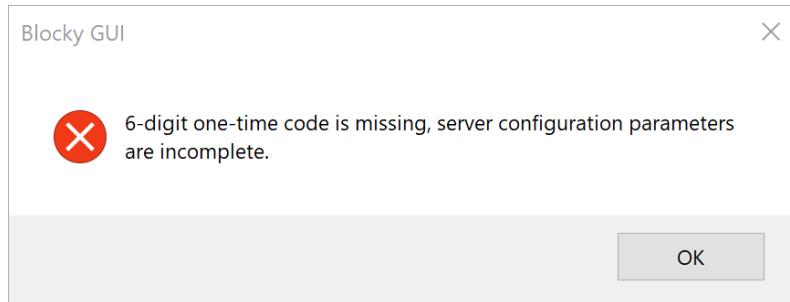
If MFA is enabled on the managed server, you will be prompted to enter the current one-time token for this server.



If the valid one-time token has been entered, the server is added and the corresponding shared

secret is cached in the Central GUI so that the one-time token does not have to be entered each time for further connections. However, we strongly recommend that you also activate the MFA for the Central GUI if you have not already done so.

If you skip entering the token, the server is added, but the Central GUI cannot connect to the server afterwards. In this case, you must modify the [server parameters](#) and check the connection again.



However, if you enter an invalid token, the connection fails, which means that the Central GUI cannot establish a connection either. You must then also modify the [server parameters](#). The same applies if MFA is only activated at a later point in time when the server has already been successfully set up in the Central GUI.

# Chapter 5. Monitoring

## 5.1. Request Table

If the GUI is running and a non-whitelisted program attempts a file modification, the request will be displayed in the request table and an administrator may control the file access. If there is no answer to a request within 1 minute, the access is automatically denied. Access can be manually set by clicking the <set access> drop-down list in the Access column and choosing an access option.

Request Table				
PID	Program	User	File	Access
1884	C:\Program Files\Windows NT\Accessories\wordpad.exe	Administrator	\\?\G:\t1\readme.txt	<set access>

The following options are available:

- GRANT – Allows the running process to modify the specified file object
- DENY – Denies the running 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 – The whitelisted program is permanently allowed to modify existing files.

Program	User	File	Access
C:\Program Files\Windows NT\Accessories\wordpad.exe	Administrator	\\?\G:\t1\readme.txt	<set access>
			<set access>
			GRANT
			DENY
			AUTHORIZE PID
			WHITELIST PROGRAM

## 5.2. Status Information

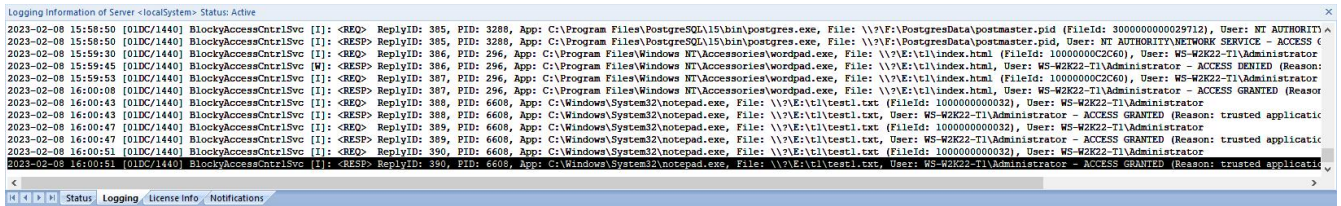
An overall status is shown in the “Monitoring” window in the tab “Status”.

Monitoring:	
Blocky Status of Server <ID: localSystem, Hostname: localhost, Software-Version: < Version >	
Connection to Access Control Service has been established.	
Data is available.	
Automatic Whitelisting: OFF.	
File system mini-filter is loaded.	
Status   Logging   License Info   Notifications	



## 5.3. Access Log

Blocky writes all modification requests on protected files and responses to the log file `C:\ProgramData\GrauData\Blocky\AccessControl.log`. The content of the log file is also displayed in the “Monitoring” window in the tab “Logging”.



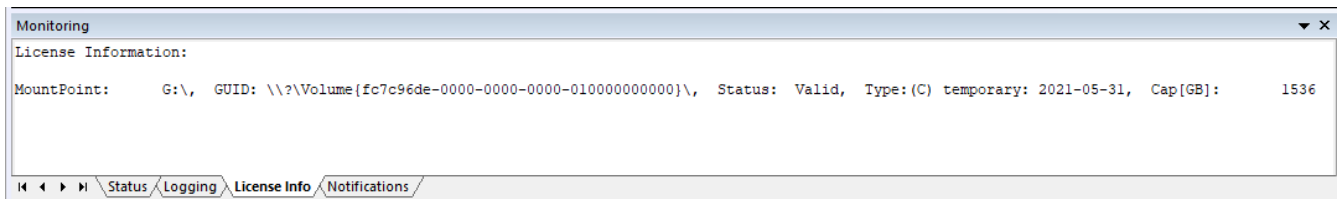
Beginning with Blocky version 2.7 the log file is rotated by timestamp extension instead of simple numeric extension. When upgrading from previous versions, older log files must be cleaned manually.



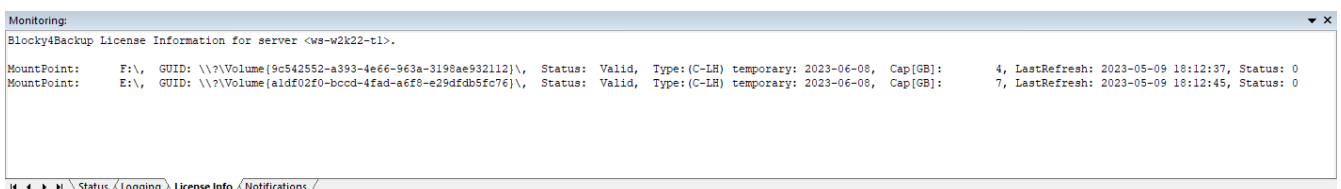
In previous versions of Blocky, each file modification access was checked by calculating the application’s runtime fingerprint each time. All accesses were logged. Starting with version 3.x the running applications are cached as long as the application runs with the same process ID, but for a maximum of 5 min. Only when a new process ID is started or the application cache expires, the runtime fingerprint is calculated and the access is logged.

## 5.4. License Information

To show the license status with license expiration and capacity select the tab "License Info" from the “Monitoring” window.

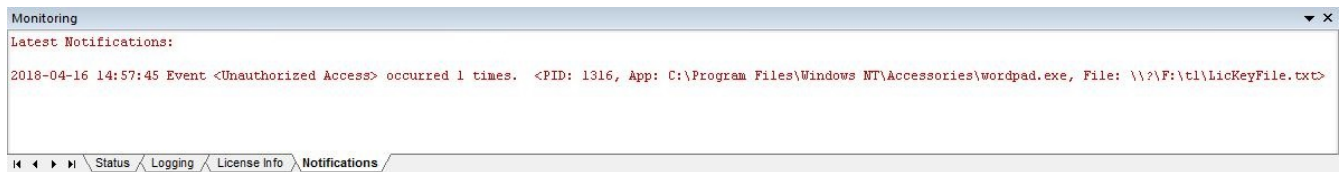


If you use [LicenseHub](#) for automatic licensing, the installed license is always valid for 30 days only, but is updated and renewed daily. The last refresh timestamp and refresh status is additionally displayed in this case. If a daily refresh has failed the license information is displayed in orange color.



## 5.5. Alert Notifications

To check for notifications select the tab “Notifications” from the “Monitoring” window.



## 5.6. Windows event logs

Further status informations are available in the Windows application and system event logs.

## 5.7. Raw volume access

Some Windows System Services may perform raw volume access on certain volumes, for example Windows components `svchost.exe`, `vssvc.exe` or `vds.exe`. On Blocky protected volumes, some of these raw volume accesses are handled by Blocky and will be denied as these components are usually not whitelisted. This results in unauthorized access events or, if the GUI is running, the raw volume access is displayed in the request table. See below for a notification example.

When using NTFS Deduplication you have to whitelist the components `svchost.exe` and `fsdmhost.exe`. When using Shadow Copies, manually or via scheduling, you have to whitelist the components `svchost.exe` and `vssvc.exe`.

If you do neither Shadow Copies nor Deduplication, there is currently no known impact when such raw volume access is denied. However, if you want to intentionally make changes to volumes and partitions with the Disk Manager, diskpart CLI or Server Manager, you should grant at least temporary access from `vds.exe`. When making changes to Blocky protected disks, you must also temporarily disable disk protection. See chapter [Disk protection](#).

In normal operation, however, we advise against whitelisting the `vds.exe`.

Example: (email notification)

***Event <Unauthorized Access> event occurred 2 times. (threshold settings: Count: 1 / TimeInterval:0 min)***

***additional information:***

**PID: 1724, App: C:\Windows\System32\vds.exe, File: \Device\HarddiskVolume3, User: NT AUTHORITY\SYSTEM**

**PID: 1724, App: C:\Windows\System32\vds.exe, File: \Device\HarddiskVolume3, User: NT AUTHORITY\SYSTEM**

# Chapter 6. Diagnostics

## 6.1. Service Report

To help our service to analyze unexpected behaviour of our software you can generate a Service Report by selecting the menu item “File >> [Generate Service Report](#)”. All service information is stored to the file [C:\ProgramData\GrauData\Blocky\Blocky\\_Diag.zip](#). Generating a service report is also available via the [BlockyCli](#).



When using the Central GUI, the Service Report is generated on the active connected target server and must be collected from there once finished. If the service is not running, a reduced report is created.

## 6.2. Access denied

There are several reasons why an application is denied write access to a file:

- Application is not whitelisted at all
- Application has been modified, e.g. [whitelist entry invalid](#)
- [Invalid license](#)
- Blocky service not running
- [System clock tampering](#)



When a file write access is denied for an application, this may result in unexpected behavior. Please ensure that all applications can perform required write accesses.

## 6.3. Missing privileges

The BlockyGUI requires certain privileges to run properly, so you have to make sure, the user is able to gain such privileges.

The required privileges are:

- SE\_BACKUP (SeBackupPrivilege)
- SE\_RESTORE (SeRestorePrivilege)
- SE\_TAKE\_OWNERSHIP (SeTakeOwnershipPrivilege)
- SE\_LOAD\_DRIVER (SeLoadDriverPrivilege)
- SE\_SECURITY\_NAME (SeSecurityPrivilege)

In standard installations, any local or domain admin user is allowed to gain these privileges by default. However it is possible to restrict these privileges via local security policies or domain group policies. Please make sure to **not** restrict these policies for users who need to run the BlockyGUI.

## 6.4. System clock tampering

Blocky monitors the system clock and detects backward time manipulations. Once such a system clock tampering is detected, this will be reported in the Windows eventlog and access control will refuse any write access, even from whitelisted applications.

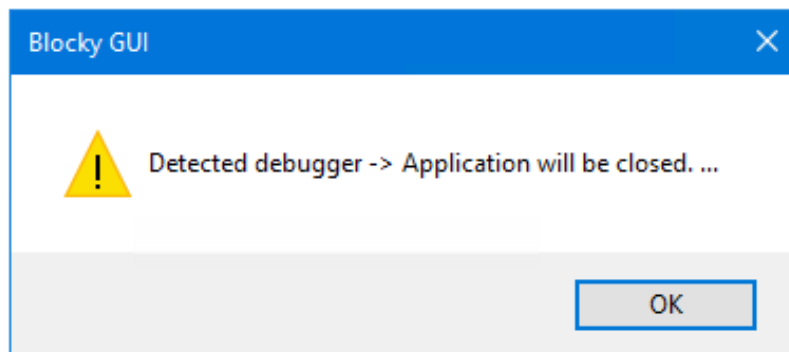
## 6.5. Self-protection

Blocky protects itself against various forms of manipulation by malicious attacks. This improves the integrity of the services. If such manipulations are detected, the Blocky components terminate themselves or do not start at all.

### 6.5.1. Process interception

Blocky detects interception by other processes or applications, e.g. when a debugger is attached to one of the running Blocky processes or when a Blocky process is started under the supervision of another process. This protects the internals of Blocky and prevents spying on sensitive data.

When the BlockyGUI detects debugging, the GUI will terminate or does not start at all:



The Same applies to the Blocky service. You will find appropriate messages in the [Windows event log](#):

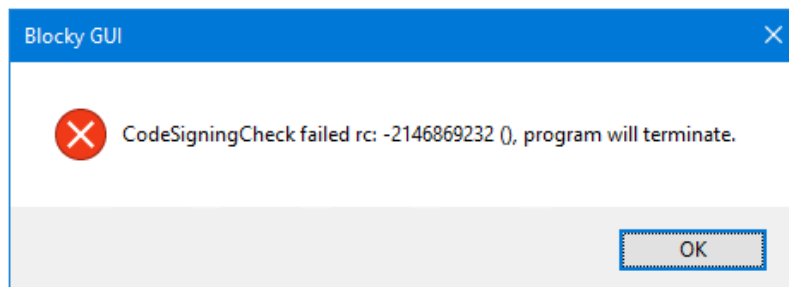
```
Detected debugger - > Application will be closed ..  
GRAU DATA Blocky Service is terminating ..  
GRAU DATA Blocky AccessControl Service Version 3.5.2.984 - Release has been terminated.
```



Do not attempt to attach debuggers on Blocky processes.

## 6.5.2. Code signing check

Blocky binaries will check their integrity via code signing to ensure proper functionality. If that check fails due to tampered binaries, these will refuse to start, e.g. for the BlockyGUI:



If code signing check fails for the Blocky service, you will find an appropriate message in the [Windows event log](#):

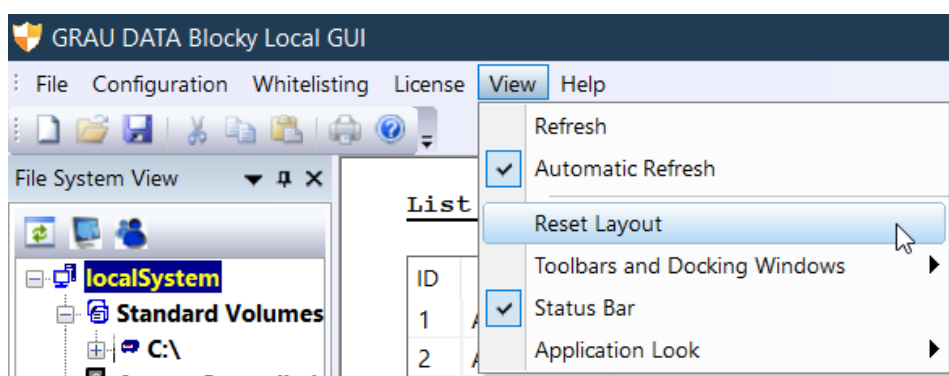
GRAU DATA Blocky AccessControl Service Version 3.5.2.984 - Release - CodeSigningCheck failed rc: -2146869232 (), process will terminate.



Please contact our GRAU DATA GmbH support ([support@graudata.com](mailto:support@graudata.com)) if you encounter permanent malfunction of the Blocky software.

## 6.6. Reset GUI Layout

In the event that you have messed up the GUI, e.g. by accidentally changing the window positions or closing some elements, you can reset the GUI layout to its original state.



Select item "View >> Reset Layout". You must restart the graphical user interface immediately afterwards for the changes to take effect by selecting "Yes" in the next dialog. Otherwise the reset will not be carried out, even if you restart the GUI later manually.

Layout reset is also possible via [BlockyCli](#), but only while the GUI is not running.

# Appx A: Setup command line parameters

The Blocky setup accepts optional command line parameters. These are intended for system administrators or scripted installations.

The same goes for the uninstallation which can be invoked by the uninstallation program `unins000.exe` in the Blocky installation path.



Administrative rights are required to install, update or uninstall Blocky.



Setup requires basic graphical environment (e.g. local or RDP session), except when using the parameter **/VERYSILENT**

Installation via remote SSH session is not supported.

As Blocky setup is based on Inno Setup, please check for the general command line parameter description on their [website](#).

## Setup command line

### Syntax:

```
BlockySetup_3_5_2_984.exe [optional parameters]
```

```
unins000.exe [optional parameters]
```

### Optional parameters:

#### **/COMPONENTS="core,gui"**

- Only selectable for a new installation
- If not specified both gui and core will be installed.

#### **/Secret=<self-defined-password>**

- On new installation: This sets the initial self defined password.
- On update: This supplies the self defined password required for updates.
- On deinstallation: This supplies the self defined password required for deinstallation.



Silent mode (**/silent** or **/verysilent**) requires the above secret parameter.  
When using **/verysilent** a required restart of the system is performed immediately without further notice.



Don't confuse it with the parameter **/Password** provided by Inno Setup.  
This is not used.

### Example:

#### *Installation/Uninstallation*

```
BlockySetup_3_5_2_984.exe /silent /COMPONENTS="core" /secret=MyPassword2020
```

```
BlockySetup_3_5_2_984.exe /silent /secret=MyPassword2020
```

```
unins000.exe /silent /secret=MyPassword2020
```

# Appx B: BlockyCLI parameters

BlockyCli.exe is a command-line utility for Blocky to manage the access control, licenses and password. It is located in the Blocky installation path.



Membership in the local **Administrators** group, or equivalent, is recommended to run the **BlockyCli**. For non-Admin users, several privileges must be assigned. See chapter [Missing privileges](#) for details. An elevated command prompt is required to gain these privileges.



When using an input file to supply the password, the file must only contain the password as ASCII in a single line. No CR/LF at the end and no empty lines. An input file cannot be used when MFA is active. See [MFA commands](#) for details.

## Access control commands:

### Syntax:

```
BlockyCli { <password> | -p | -i <pwdfile> } <command> <parameter>
```

The self defined password is required for all access control commands.

### Parameters:

Password parameter	Description
<password>	supply password on command line
-p	let CLI prompt for password.
-i <pwdfile>	supply password via given input file.

Management command	Parameters	Description
set_accesscontrol	<path>	Activate access control on provided path.
reset_accesscontrol	<path>	Deactivate access control on provided path.
reset_accesscontrol	<path> <n>	Deactivate access control on path temporarily for <n> minutes [1..60]
show_controlledfolders	<path>	Display if access control is active in path.
show_contolledfolders	ALL	Display all controlled folders.
add_whitelist	<program>	Add program to the whitelist.
del_whitelist	<program>	Remove program from the whitelist.
update_whitelist	<program>	Update program in the whitelist.
show_whitelist		Show all whitelisted objects.



## Examples:

### *Access control*

```
.\BlockyCli.exe password20 show_controlledfolders ALL
Controlled Folders: (0)
rc:0

.\BlockyCli.exe password20 set_accesscontrol E:\privat
rc:0

.\BlockyCli.exe password20 show_controlledfolders ALL
Controlled Folders: (1)
E:\privat
rc:0

.\BlockyCli.exe password20 show_controlledfolders E:\privat
Access Control is active on E:\privat.
rc:0

.\BlockyCli.exe password20 show_controlledfolders E:\protect
Access Control is not active on E:\protect.
rc:0

.\BlockyCli.exe password20 reset_accesscontrol E:\privat 10
rc:0

.\BlockyCli.exe password20 show_controlledfolders ALL
Controlled Folders: (1)
E:\privat (temporarily disabled for 10 min)
rc:0

.\BlockyCli.exe password20 show_controlledfolders E:\privat
Access Control on E:\privat is temporarily disabled for 10 min.
rc:0
```

### *Whitelist*

```
.\BlockyCli.exe password20 add_whitelist C:\Windows\System32\wbengine.exe
rc:0

.\BlockyCli.exe password20 show_whitelist
WhiteListed Applications:
  1. Checksum: valid, Access: File, Directory, Volume, Name: C:\Windows\System32\wbengine.exe
rc:0

.\BlockyCli.exe password20 update_whitelist C:\Windows\System32\wbengine.exe
rc:0

.\BlockyCli.exe password20 del_whitelist C:\Windows\System32\wbengine.exe
rc:0
```

## Disk protection commands:

### Syntax:

```
BlockyCli { <password> | -p | -i <pwdfile> } <command> <parameter>
```

The self defined password is required for all disk protection commands.

### Parameters:

Password parameter	Description
<password>	supply password on command line
-p	let CLI prompt for password.
-i <pwdfile>	supply password via given input file.

Management command	Parameters	Description
show_disk	<path>	display disk status for associated volume path.
show_disk	ALL	display status of all disks with associated volumes.
reset_diskprotection	<diskno> <n>	deactivate disk protection on <diskno> temporarily for <n> minutes [1..60]

### Examples:

#### *Show disk protection*

```
. \BlockyCli.exe password20 show_disk E:
DiskNo: 11, DiskDeviceName: \\.\GlobalRoot\Device\Harddisk11\DR11, Protection: ON , Boot: 0
--- GUID: \\?\Volume{e34f04e1-e941-4f70-8399-a9b7f9b22d20}\, Status: managed ,
Mountpoint: E:\
rc:0

. \BlockyCli.exe password20 show_disk ALL
DiskNo: 11, DiskDeviceName: \\.\GlobalRoot\Device\Harddisk11\DR11, Protection: ON , Boot: 0
--- GUID: \\?\Volume{e34f04e1-e941-4f70-8399-a9b7f9b22d20}\, Status: managed ,
Mountpoint: E:\

DiskNo: 9, DiskDeviceName: \\.\GlobalRoot\Device\Harddisk9\DR9, Protection: OFF , Boot: 0
--- GUID: \\?\Volume{048c65d8-78dd-412e-a1a5-d3f1b3f6d1a5}\, Status: unmanaged ,
Mountpoint: ---
--- GUID: \\?\Volume{0da9af9e-43a3-4a1e-bcb1-8507bf7dd7f7}\, Status: unmanaged ,
Mountpoint: C:\
--- GUID: \\?\Volume{1f3edd74-dc3e-4b5e-b784-c197395899f2}\, Status: unmanaged ,
Mountpoint: ---
rc:0
```

### Switch off protection

```
.\BlockyCli.exe password20 reset_diskprotection 11 5
rc:0

.\BlockyCli.exe password20 show_disk E:
DiskNo: 11, DiskDeviceName: \\.\GlobalRoot\Device\Harddisk11\DR11, Protection: off until 2024-
09-26 13:49:16, Boot: 0
--- GUID: \\?\Volume{e34f04e1-e941-4f70-8399-a9b7f9b22d20}\, Status:    managed ,
Mountpoint: E:\
rc:0
```

Protection of physical disk number 11, which contains access controlled volume E:, is switched off for 5 minutes.

## Diagnostic commands:

### Syntax:

```
BlockyCli { <password> | -p | -i <pwdfile> } <command> <parameter>
```

The self defined password is required for all diagnostic commands.

### Parameters:

Password parameter	Description
<password>	supply password on command line
-p	let CLI prompt for password.
-i <pwdfile>	supply password via given input file.

Management command	Parameters	Description
diagnostics		generate diagnostics report.
dump		dumps program whitelist and access table.
reset_gui_layout		set default gui layout.
restore_gui_layout		restores gui layout from versions below 3.1.

### Examples:

#### *Diagnostics*

```
.\BlockyCli.exe password20 diagnostics
Generating Diagnostics Report .....
rc:0
```

This creates the service report file **C:\ProgramData\GrauData\Blocky\Blocky\_Diag.zip**.

#### *Dump*

```
.\BlockyCli.exe password20 dump
rc:0
```

This creates the following files in the folder **C:\ProgramData\GrauData\Blocky\**:

- AccessTable.txt
- WhiteListDump.txt

### *Reset GUI Layout*

```
.\BlockyCli.exe password20 reset_gui_layout  
rc:0
```

This will reset the GUI layout to its original state. The command does not change the layout if the GUI is running when it is executed.

### *Restore GUI Layout*

```
.\BlockyCli.exe password20 restore_gui_layout  
rc:0
```

When upgrading from version 2.x to version 3.x, the GUI layout is set to a default state. This command restores the user-defined GUI layout from version 2.x. The command is silently ignored if the GUI is running. An error occurs if no pre 3.x layout is found.

## License handling commands:

### Syntax:

```
BlockyCli { <password> | -p | -i <pwdfile> } <command> <parameter>
```

The self defined password is required for all license handling commands.

### Parameters:

Password parameter	Description
<password>	supply password on command line
-p	let CLI prompt for password.
-i <pwdfile>	supply password via given input file.

Management command	Parameters	Description
request_license	<vol_path>   <vol_guid> [ -f license-file.txt ] [ -c CapID ]	get license request for volume.
install_license	{ -f license-file.txt   -k license-key-string }	install license key.
show_license	[-f output-file.csv]	show licenses of all controlled volumes.



If the system is configured for [LicenseHub](#) usage, the commands `request_license` and `install_license` are not supported. To set the LicenseHub configuration see the separate [LicenseHub CLI commands](#).

## Examples:

### Request License

```
.\BlockyCli.exe password20 request_license E: -c AAAA-BBBB-CCCC-3333-5555-ZZZZ-XXXY  
M8SU-MJZY-R94W-WZ9V-J4MF-YMX6-A9HS-2C4V-VZXW-NW4Z-EFDJ-6W57-FVIX-E5G6-69HV-BUDJ-FT7P-CEV5-RGDS-  
TUX7-4YJX-V6NS-KJR4-GVC2-P4HQ-G9CZ-8IET-S6XY-Q8KV-RJGE-UMU3-ATD2-G5J7-8VRN-S7XF-CINP-6T2G-6RTR-  
AN9C-MDJX-9AHK-QYGG-ZV5X-7CCM-FT8J-7PAH-AP54-4AJQ-W9WW-GX52-VFD4-PCDP-ASM3-S9HG-A8RA-8XFG-5Q6S-  
JAA  
rc:0  
  
.\BlockyCli.exe password20 request_license E: -f request-file.txt  
rc:0  
  
.\BlockyCli.exe password20 request_license "\\?\Volume{fc7c96de-0000-0000-0000-010000011000}\"  
M7SU-MJZY-R94W-WZ9V-J4MF-YMX6-A9HS-2C4V-VZXW-NW4Z-EFDJ-6W57-FVIX-E5G6-69HV-BUDJ-FT7P-CEV5-RGDS-  
TUX7-4YJX-V6NS-KJR4-GVC2-P4HQ-G9CZ-8IET-S6XY-Q8KV-RJGE-UMU3-ATD2-G5J7-8VRN-S7XF-CINP-6T2G-6RTR-  
AN9C-MDJX-9AHK-QYGG-ZV5X-7CCM-FT8J-7PAH-AP54-4AJQ-W9WW-GX52-VFD4-PCDP-ASM3-S9HG-A8RA-8XFG-5Q6S-  
JAA  
rc:0
```



The **request\_license** command only generates a license request key. Please proceed with the resulting license request by using our Web-Portal or via e-mail. See the chapter [Licensing](#).



For initial licensing request, a valid Cap-ID must be supplied with parameter "-c". For license renewal, this parameter should be omitted.



When a volume is supplied as volume GUID, this must be enclosed in single or double quotes.

### Install License

```
.\BlockyCli.exe password20 install_license -f LicKey-20210713-115523.txt  
rc:0  
  
.\BlockyCli.exe password20 install_license -k 4MXB-E8VU-Z9XS-6YCM-3ACK-QSBD-WCVH-QFE7-TPMM-  
SQUJ-7AZH-TAW9-FEBD-F3CN-CX7D-PAZA-C48Z-ZM6I-JUG4-YI4R-PKST-IIGW-BA5D-6MWB-RSHD-M7XG-YEWW-559C-  
DUR5-V7R5-3MNR-AZXT-JKFJ-7P3S-ATYN-BHNQ-6VDT-RMUK-PPR8-8ZWV-E43T-WB5R-7WMU-CHDW-M8ZS  
rc:0
```

## Show License

```
.\BlockyCli.exe password20 show_license
```

```
VolumeGUID,MountPoint,VolumeKey,LicenseType,ExpirationDate,LicensedCapacity,TotalCapacity,UsedCapacity
```

```
\\?\Volume{6e65ff6d-7d86-4f90-9eb1-f3b55087b321}\,F:\,01053782,C,2023-01-17,10240,10220,1024
```

```
\\?\Volume{fc7c96de-0600-0200-0300-010000000000}\,G:\,02021BCB,C,2022-01-02,20480,18384,2048
```

```
rc:0
```

```
.\BlockyCli.exe password20 show_license -f output-file.csv
```

```
rc:0
```



## LicenseHub management commands:

### Syntax:

```
BlockyCli { <password> | -p | -i <pwdfile> } <command> <parameter>
```

The self defined password is required for all LicenseHub management commands.

### Parameters:

Password parameter	Description
<password>	supply password on command line
-p	let CLI prompt for password.
-i <pwdfile>	supply password via given input file.

Management command	Parameters	Description
set_licensehub	<host> <port> <pwd>	configure LicenseHub access.
show_licensehub		show LicenseHub configuration.

### Examples:

#### *Set LicenseHub configuration*

```
.\BlockyCli.exe password20 set_licensehub 10.1.5.128 7887 MyLHPassw0rd  
rc:0
```

#### *Show LicenseHub configuration*

```
.\BlockyCli.exe password20 show_licensehub  
LicenseHub Location: hostname: 10.1.5.128, port: 7887  
rc:0
```

## Change password command:

### Syntax:

```
BlockyCli { <password> | -p | -i <pwdfile> } <command> <parameter>
```

The self defined password is required for the change password command.

### Parameters:

Password parameter	Description
<password>	supply password on command line
-p	let CLI prompt for current password.
-i <pwdfile>	supply current password via given input file.

Management command	Parameters	Description
change_password	[ <new_password>   -n <new_pwdfile> ]	change password.

### Examples:

#### *Change password*

```
.\BlockyCli.exe password20 change_password MyNewP4ssw0rd  
Password has been successfully changed.  
rc:0
```

```
.\BlockyCli.exe password20 change_password -n pwdfile.txt  
Password has been successfully changed.  
rc:0
```

## MFA commands:

### Syntax:

```
BlockyCli { <password> | -p | -i <pwdfile> } <command> <parameter>
```

The self defined password is required for all MFA commands.

### Parameters:

Password parameter	Description
<password>	supply password on command line
-p	let CLI prompt for current password.
-i <pwdfile>	supply current password via given input file.



As soon as MFA is activated, you must enter the password and the one-time token concatenated. For example, if your password is **password20** and the one-time token actually generated is **987654**, you must enter **password20987654**. This applies to all CLI commands that require a password.



Due to the TOTP algorithm, the one-time token changes every 30 seconds. Make sure that you always enter the currently valid token.

Management command	Parameters	Description
activate_mfa	[ secret ]	activate multi-factor authentication
deactivate_mfa		deactivate multi-factor authentication
show_mfa_qrcode		show QR Code of current MFA account
show_mfa_status		show MFA status

## Examples:

### *Activate MFA with random shared secret*

```
.\BlockyCli.exe password20 activate_mfa  
Enter 6-digit one-time code for verification: 914663  
MFA has been activated.  
rc:0
```

This CLI command will generate a QR code on the terminal which must be used to set up a new account in your preferred authenticator app. Once the authenticator app has been set up, enter the current one-time token generated for the new account to verify the MFA activation. See the next page for an example of the QR code.

### *Activate MFA with a self-defined shared secret*

```
.\BlockyCli.exe password20 activate_mfa ABCDEFGH234567XY  
Enter 6-digit one-time code for verification: 469975  
MFA has been activated.  
rc:0
```

This CLI command also generates a QR code on the terminal, which must be used to set up a new account in your preferred authentication app. Since the specified shared secret is used instead of a random secret you can use the same shared secret and the same account in your authenticator app for multiple Blocky installations. The secret has to consist of 16 characters in the range 2-7A-Z.

### *Deactivate MFA*

```
.\BlockyCli.exe password20987654 deactivate_mfa  
MFA has been deactivated.  
rc:0
```

### *Show the MFA status*

```
.\BlockyCli.exe password20 show_mfa_status  
MFA on local instance: ON.
```



`show_mfa_status` is the only command which always requires just the password, without the one-time token, even if MFA is activated.

## Show MFA QR Code

```
.\BlockyCli.exe password20987654 show_mfa_qrcode
```

This displays the QR code in the terminal, just like when activating MFA.



Please note: The QR code is displayed inside the console window if you run CMD or Powershell in the traditional console host (conhost.exe). When running in the modern Windows Terminal, especially on Windows Server 2025, the QR code is displayed outside the terminal window as an overlay directly on the desktop. You must then close the terminal window to clear the QR code.

## Initial password and password reset

Command	Description
BlockyCli <b>set_password</b> <password>	Sets the initial password.
BlockyCli <b>request_password_reset</b>	Creates a token for requesting a password reset key.
BlockyCli <b>reset_password</b> <reset_key>	Resets the password with the provided reset key.

### Examples:

#### *Set password*

```
.\BlockyCli.exe set_password password20  
rc:0
```

#### *Request password reset*

```
.\BlockyCli.exe request_password_reset
```

Send the following token to [support@graudata.com](mailto:support@graudata.com) in order receive a password reset key:

H9KC-CS2K-KSJR-L87T-N6ES-0X3T-U5TR-YWA4-BAN6-7ANG-26ZG-P2QD-3EX2-BB7H-J2RM-2VXT-7IE6-4NE8-6GY4-5K9Q-5ZZ4-QAMG-WDP9-AG87-2IVU-5K4V-X4CT-UID7-KT6E-8IXH-VTH4-48TS

#### *Reset password*

```
.\BlockyCli.exe reset_password OD9C-OUR5-KSFR-L80T-XKLS-0X3T-U5TR-YWA4-BAN6-7ANG-26ZG-P2QD-3EX2-BB7H-J2RM-2VXT-7IE6-4NE8-6GY4-5K9Q-5ZZ4-QAMG-WDP9-AG87-2JUS-5K4V-X4CT-UID7-KT6E-8IXH-VTH4-I00P  
rc:0
```

## Central GUI password reset

The above described BlockyCLI commands will reset the password of local Blocky instances only.

To reset the password of a central GUI, you must create the reset request from the login screen of the GUI. To apply the reset key, start the GUI executable via the Windows command line as follows:

```
.\BlockyGui.exe /reset_password JE3B-SH7Q-6PXN-DP2S-CCQ8-4XB9-IKFM-CT32-MGX6-PIDV-YS6I-KVNG-G2NK-UPW2-49U8-IF4S-D4S4-4QPJ-7XGD-DPEP-57HZ-BMBR-AMZC-3XK2-VHNW-HA8A-AQHD-3SGT-TIES-SUJT-2RGT-DRH8
```

# Appx C: Blocky Change Log

This appendix summarizes the changes between Blocky versions. The change log only contains relevant changes and fixes.

## C.1. Version 3.5.2.984 - Release

- Fix Release for 3.5.1
- (Feature) Support for Windows Server 2025
- (Feature) Password reset for Central GUI instances
- (Change) CLI shows temporarily deactivated access control
- (Change) Limited service report when service fails
- (Change) Allow copy/paste in MFA window
- (Change) Quickly navigate to the selected server in the GUI
- (Change) Validate e-mail address syntax for notifications
- (Change) Show module dependencies for whitelist entries
- (Bugfix) Fix GUI crash when certain window elements are floating
- (Bugfix) Fix notification settings
- (Bugfix) Fix CLI for MFA status check
- (Bugfix) Volumes located on the system disk will work as unsupported on upgrades

## C.2. Version 3.5.1.896 - Release

- Fix Release for 3.5.0
- (Bugfix) A protected file could be changed in rare cases when the AC service was stopped

## C.3. Version 3.5.0.848 - Release

- Initial Release 3.5.0
- (Feature) Protect physical disks against deletion of volumes
- (Feature) Optional MFA for GUI and CLI
- (Feature) Reset GUI layout to default
- (Change) Volumes located on the system disk are not supported anymore
- (Change) Import Code Signing CA Certificate
- (Change) Show invalid whitelist entries in CLI output
- (Change) Show missing email recipients in notification settings
- (Change) Enhance CLI output for whitelist
- (Bugfix) Prevent uninstall if service dependencies exist
- (Bugfix) Keep license on volume when AC is switched off and licenses are obtained from LH

## C.4. Version 3.1.1.450 - Release

- Fix Release for 3.1.0
- (Bugfix) Fix Bug in notification configuration
- (Bugfix) Fix Code Signing Check for isolated hosts

## C.5. Version 3.1.0.362 - Release

- Initial Release 3.1.0
- (Feature) Performance Optimization by AccessControl caching in filter
- (Change) Change product name from Blocky4Backup to Blocky
- (Change) Check of active dependencies to AC service during update or uninstall
- (Change) Protect Blocky binaries via code signing
- (Bugfix) Fix notificaton thresholds
- (Bugfix) Update hostname changes on License Hub
- (Bugfix) Protect internal data structures against interception



## C.6. Version 2.7.1.186 - Release

- Fix Release for 2.7.0
- (Change) Limit max password length to 128 characters
- (Change) Show refresh information for licenses issued by License Hub
- (Change) Include License Hub information in Service Report
- (Change) Remove unencrypted config files
- (Bugfix) Fix internal system name in config files
- (Bugfix) Fix file handle leak on invalid config files

## C.7. Version 2.7.0.56 - Release

- Initial Release 2.7.0
- (Feature) License Hub support
- (Change) Increased max password length up to 240 characters
- (Change) Enhanced error messages when fingerprint calculation fails
- (Change) Improved dialog when master config rollout would fail for some servers
- (Change) Improved visual group configuration compare
- (Change) Setup will install required VC runtime DLL's only if not yet available
- (Change) AC logging includes program and file information now also in response line
- (Change) Notification for invalid whitelist entry now contains modified component
- (Change) Whitelist update now takes care of all previous included DLL's
- (Bugfix) Improved enumeration of loaded DLL's on fingerprint calculation
- (Bugfix) Fix service crash on failed Service Report
- (Bugfix) Central GUI now allows change of remote server hostname and ip-address
- (Bugfix) Load config includes now all activated access-controlled folders
- (Bugfix) Setup checks for running instance of AC service

## C.8. Version 2.6.2.217 - Release

- Initial Release for 2.6.2
- (Feature) GUI shows installed Core product version
- (Feature) Possibility to revert Central GUI to Local GUI
- (Change) Save configuration also includes managed volumes
- (Change) Remove plain text configuration files
- (Change) Detect system clock mismatch when adding remote servers in Central GUI
- (Change) GUI shows error code on connection issues
- (Change) Remove GUI autostart on login
- (Bugfix) Better handling of volumes mounted in folders
- (Bugfix) Fix whitelist display in GUI with lots of entries
- (Bugfix) Fix testing of SMTP server settings
- (Bugfix) Fix master config rollout when local GUI is connected
- (Bugfix) Improve GUI connections to AC service
- (Bugfix) Fix CLI for switch on access control on additional volumes
- (Bugfix) Improve Installer on failed or interrupted upgrades
- (Bugfix) Fix fingerprint calculation for debug binaries

## C.9. Version 2.6.1.107 - Release

- Initial Release for 2.6.1
- (Feature) Central GUI to manage several Core Instances
- (Feature) Introduce separate components for Core und GUI
- (Feature) Extended disk/volume information in Service Report
- (Feature) Detect tampered Service Report Scripts
- (Feature) Added failsafe and debug mode for AC Service
- (Feature) BlockyCli prompt for password interactively or supply via input file
- (Change) Remove notifications for authorized access
- (Change) AC log now also contains internal requests
- (Change) Serveral raw volume accesses are now handeled by AC Service
- (Change) Changed path for saved configuration
- (Bugfix) Improved AC log message
- (Bugfix) Fix possible memory leak in AC Service
- (Bugfix) Fix wrong notification on volumes with short capacity

## C.10. Version 2.5.0.52 - Fix-5

- Fix Release for 2.5.0
- (Feature) Introduce SID cache for better performance
- (Bugfix) Performance enhancement for process lookup
- (Bugfix) Performance enhancement for file name lookup
- (Bugfix) Fix BlockyCli crash when called from service account
- (Bugfix) Add performance counters to trace timing issues
- (Bugfix) Fix license notifications for disabled volumes
- (Bugfix) Fix BlockyCli config for folder mounted volumes

## C.11. Version 2.5.0.48 - Fix-4

- Fix Release for 2.5.0
- (Feature) Support for multiple email recipients
- (Feature) Restricted support for volumes mounted in folders
- (Feature) Prevent brute force password attac
- (Feature) BlockyCli enhancement for license handling
- (Bugfix) Notifications in case of filter not loaded
- (Bugfix) Invalid characters in AccessControl.log cause GUI to hang
- (Bugfix) Fix service crash on runaway GUI connects
- (Bugfix) Particular folder names may cause service to terminate silently
- (Bugfix) Improve detection of system clock tampering
- (Bugfix) Fix for binaries with invalid internal checksums
- (Bugfix) BlockyCli fix for updating whitelist
- (Bugfix) Detect certain invalid volume configurations
- (Bugfix) Include rotated logfiles in service report

## C.12. Version 2.5.0.41 - Fix-3

- Fix Release for 2.5.0
- (Feature) Start/Stop service notification
- (Bugfix) Stateful notifications
- (Bugfix) Zero notification threshold count
- (Bugfix) Prevent stopping of filter
- (Bugfix) reject single quote (') and double quote (") in password

## C.13. Version 2.5.0.36 - Fix-2

- Fix Release for 2.5.0
- (Feature) Basic support for NTFS deduplication
- (Bugfix) AccessControl request for folder rename
- (Bugfix) Proper handling of internal ADS

## C.14. Version 2.5.0.32 - Fix-1

- Fix Release for 2.5.0
- (Bugfix) Stabilize installer for update/upgrade
- (Bugfix) Fix crash of service with duplicate license keys
- (Bugfix) Notification list entries
- (Bugfix) Missing file in service report

## C.15. Version 2.5.0.30 - Release

- Initial 2.5.0 Release
- (Feature) Introduce additional password for configuration
- (Feature) Uninstall/Upgrade now password protected
- (Feature) Changed 3rd party license handling to GRAU DATA Cap-ID based model
- (Feature) Adjusted SMTP configuration
- (Feature) Volume gets locked on expired license
- (Feature) Introduce notification on invalid whitelist entry
- (Feature) Remove account whitelisting
- (Feature) Introduce command-line tool
- (Bugfix) Rework internal timer actions

# Appx D: Open Source Licenses

GRAU DATA GmbH acknowledges the redistribution of open source components under the licenses shown below with Blocky.

## OpenSSL

Copyright © 1998-2019 The OpenSSL Project, OpenSSL License  
Copyright © 1995-1998 Eric Young ([eyay@cryptsoft.com](mailto:eyay@cryptsoft.com)), Original SSLeay License  
<https://www.openssl.org/source/license-openssl-ssleay.txt>

## POCO C++ Libraries

POCO C++ Libraries project, Boost Software License - Version 1.0 - August 17th, 2003  
<https://github.com/pocoproject/poco/blob/master/LICENSE>

## JsonCpp

Copyright © 2007-2010 Baptiste Lepilleur and The JsonCpp Authors, MIT License  
<https://github.com/open-source-parsers/jsoncpp/blob/master/LICENSE>

## Crypto++ Library

Compilation Copyright (c) 1995-2019 by Wei Dai,  
Boost Software License - Version 1.0 - August 17th, 2003  
<https://cryptopp.com/License.txt>

## ADVobfuscator

Written by Sebastien Andrivet - Copyright (c) 2010-2017 Sebastien Andrivet.  
<https://github.com/andrivet/ADVobfuscator/blob/master/README.md>

## QR Code generator library

Copyright © 2024 Project Nayuki. (MIT License)  
<https://www.nayuki.io/page/qr-code-generator-library>

# Index

## A

Access Control, [1](#), [16](#)  
Access denied, [53](#), [56](#)  
Access Log, [54](#)  
Access option, [53](#)  
AccessControl.log, [1](#), [54](#)  
Activate MFA, [49](#)  
Add Programs, [11](#)  
Add Server, [29](#)  
Additional tasks, [6](#)  
Alert Notifications, [55](#)  
Announcement of discontinuation, [3](#)  
AUTHORIZE PID, [53](#)  
Automatic Whitelisting, [19](#)

## B

Blocky\_Diag.zip, [56](#)  
BlockyCli, [61](#)  
BlockyGUI.exe, [14](#)

## C

Capacity limit, [40](#)  
Capacity-ID, [40](#), [41](#)  
Central GUI, [27](#)  
Change Log, [76](#)  
Change password, [15](#)  
CLI parameters, [61](#)  
Code signing check, [58](#)  
Command line parameters, [59](#)  
Complete Installation, [9](#)  
Configuration, [14](#), [15](#), [46](#), [49](#), [50](#), [50](#), [51](#)  
Configuration settings, [26](#)  
Control Panel, [11](#)  
Core, [7](#)

## D

Deactivate MFA, [50](#)  
Deduplication, [2](#), [55](#)  
Define new Group, [33](#)  
DENY, [53](#)  
Diagnostics, [56](#)  
Disk Protection, [1](#), [17](#), [77](#)  
Drop-down list, [53](#)  
Dynamic disks, [3](#)

## E

Eject and detach, [4](#)

## F

Fingerprint, [1](#), [19](#), [54](#)  
Firewall, [29](#)  
fsdmhost.exe, [2](#), [55](#)

## G

GPT, [3](#)  
GRANT, [53](#)  
GUI, [7](#)

## I

ICMP echo request, [29](#)  
Inno Setup, [59](#)  
Install license, [44](#)  
Installation, [5](#)  
Installation path, [6](#)  
Installation start, [8](#)  
Invalid license, [45](#), [56](#)  
Invalid whitelist, [21](#), [56](#)

## K

Key Features, [1](#)

## L

License Agreement, [5](#)  
License Information, [54](#)  
License renewal, [44](#)  
License status, [44](#)  
Licensehub, [46](#), [54](#), [70](#)  
Licensing, [40](#)  
Logging, [54](#)

## M

Manual Upgrade, [10](#)  
Manually whitelist applications, [20](#)  
Master Configuration, [35](#)  
MBR, [3](#)  
MFA, [48](#)  
MFA Central GUI, [51](#)  
MFA local instance, [49](#)  
Microsoft, [3](#)  
Missing privileges, [56](#)

Modification requests, [54](#)  
module dependencies, [22](#)  
Monitoring, [1](#), [53](#)  
Multi-factor authentication, [48](#)

## N

Non-whitelisted applications, [1](#)  
Notification, [1](#), [23](#)  
Notification Rules, [24](#)  
NTFS, [3](#)

## O

Open Source Licenses, [83](#)

## P

Password protection, [4](#)  
Password required, [4](#)  
Password reset, [15](#), [75](#)  
Platform support, [3](#)  
Process interception, [57](#)  
Product Information, [1](#)

## Q

QR Code, [49](#)

## R

raw volume access, [3](#), [55](#), [80](#)  
ReFS, [3](#)  
Remove Programs, [11](#)  
Request Table, [53](#)  
Requesting license key, [42](#)  
Reset GUI Layout, [58](#)  
Restore configuration settings, [26](#)  
Restrictions, [3](#)  
RFC 6238, [48](#)

## S

Save / Load Configuration, [26](#)  
Select Components, [7](#)  
Self-protection, [57](#)  
Server parameters, [30](#)  
Server selection, [31](#)  
Service Report, [56](#)  
Set initial password, [14](#)  
Setup command line parameters, [59](#)  
Shadow Copies, [55](#)  
Silent mode, [60](#)  
SMTP Server Configuration, [25](#)

Start of the GUI, [14](#)  
Status Information, [53](#)  
Support, [10](#)  
svchost.exe, [2](#), [55](#)  
Switch off Access Control, [16](#), [61](#)  
Switch off disk protection temporarily, [18](#)  
Switch on Access Control, [16](#), [61](#)  
System clock, [29](#), [57](#)

## T

Test Email, [25](#)  
TOTP, [48](#)  
Trial license, [40](#)  
Trial period, [40](#)

## U

Unauthorized configuration changes, [14](#)  
Uninstallation, [11](#)  
Untrusted applications, [1](#)  
Update license, [44](#)  
Updating, [10](#)  
Upgrading, [10](#)

## V

vds.exe, [55](#)  
VerySilent mode, [60](#)  
View, [58](#)  
vssvc.exe, [55](#)

## W

WEB-PORTAL, [42](#), [43](#)  
Whitelist, [1](#)  
WHITELIST PROGRAM, [53](#)  
Whitelist via request table, [20](#)  
Whitelisting, [19](#), [61](#)  
Windows event logs, [55](#), [57](#)