GRAU DATA

YOUR DATA. YOUR CONTROL

Blocky4Backup Administration Guide

GRAU DATA GmbH

Version 2.7.0.56 - Release, 2023-03-16 10:37:28

Table of Contents

1. Product Information

1.1. Overview

Blocky4Backup 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 an unique fingerprint calculated from several binary checksums and other hashes from dependent components. Therefore unwanted modifications on a trusted application can also be detected and reported to the user. Unauthorized attempts are logged and notifications can be sent to security administrators.

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:

Blocky4Backup 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 Blocky GUI is running, the write access is set on hold first and request will be displayed on the Request Table, so you can choose to allow or deny acccess. Blocky4Backup 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 status is displayed in the “Monitoring” window in the tab „Status“. To check for notifications select the tab “Notifications” from the “Monitoring” window.

Notification:

Blocky4Backup can send alert notifications to the Windows application event log, to email recipients and to the Status Area of the Blocky4Backup 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 responsible for the graphical user interface and can configurate a Core. The Core is the engine and 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. 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.

1.3. Platform support and restrictions

1. Supported platforms (with restrictions):
    - MS Windows Server 2012 R2 Standard & Enterprise Edition
    - MS Windows Server 2016
    - MS Windows Server 2019
    - MS Windows Server 2022
    - Full GUI aka Desktop Experience required.
2. Blocky4Backup supports local disks, e.g. block storage only.
3. Running on Microsoft fail-over cluster or Active Directory Domain Controllers is not supported.
4. NTFS and ReFS file systems are supported.
5. Basic support for build-in deduplication on NTFS file systems.
   On ReFS dedup is not supported. Use block cloning feature instead.
6. System volumes can not be protected
7. Only simple volumes on MBR and GPT disks are supported.
   Dynamic disks (e.g. striped, mirrored or RAID-5) are not supported.
8. 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.
9. Restrictions apply for volumes mounted in folders of parent volumes. AccessControl for folder-mounted volumes and their parent volumes are mutually exclusive.
10. Running the Blocky GUI requires certain security privileges which are granted by default to admin users. See chapter Diagnostics for details.
11. 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 Blocky4Backup.
12. Some Windows System Services may perform raw volume access on Blocky protected volumes which may cause unauthorized access events. See chapter Monitoring for details.

1.4. Deduplication

Blocky4Backup has basic support for build-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.

1.5. Announcement of discontinuation

With the upcoming version 3.0 of Blocky4Backup, platform support for MS Windows Server 2012 R2 will be discontinued.

2. Password protection

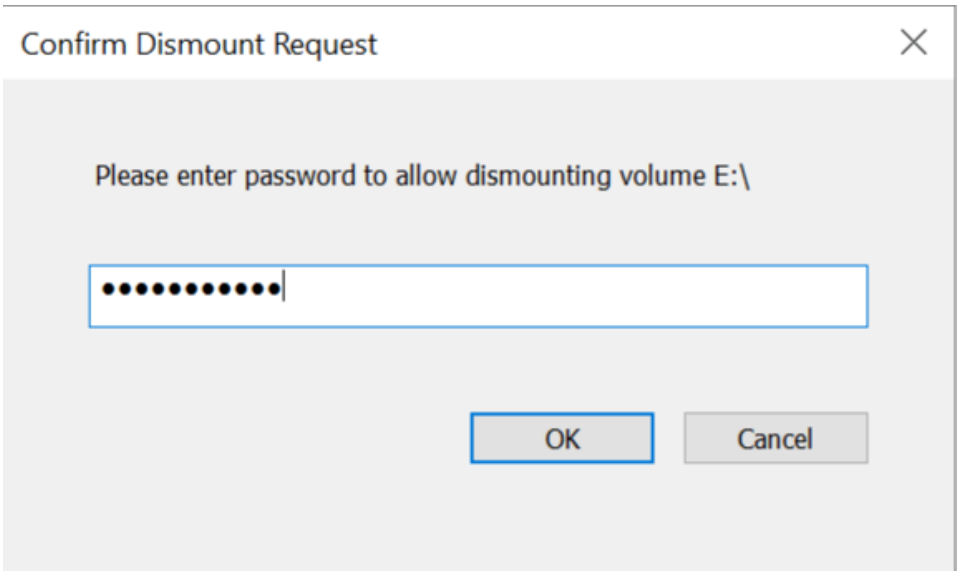
To protect the software against unauthorized configuration changes, an additional password must be defined for starting the GUI. When the GUI is started for the first time, this self-defined password is requested. See Set initial password.

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

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 Blocky4Backup
- Uninstallation of Blocky4Backup
- Ejection and detachment 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 Blocky4Backup a password is only requested if the core is installed.

3. Installation

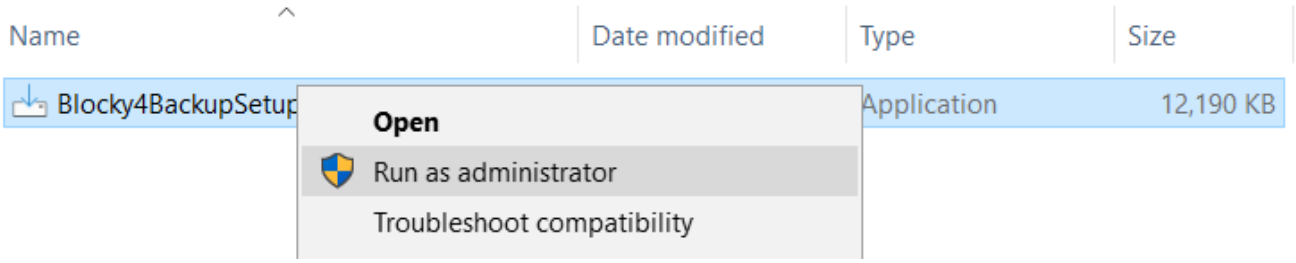
3.1. Installing

3.1.1. Launch the Installation

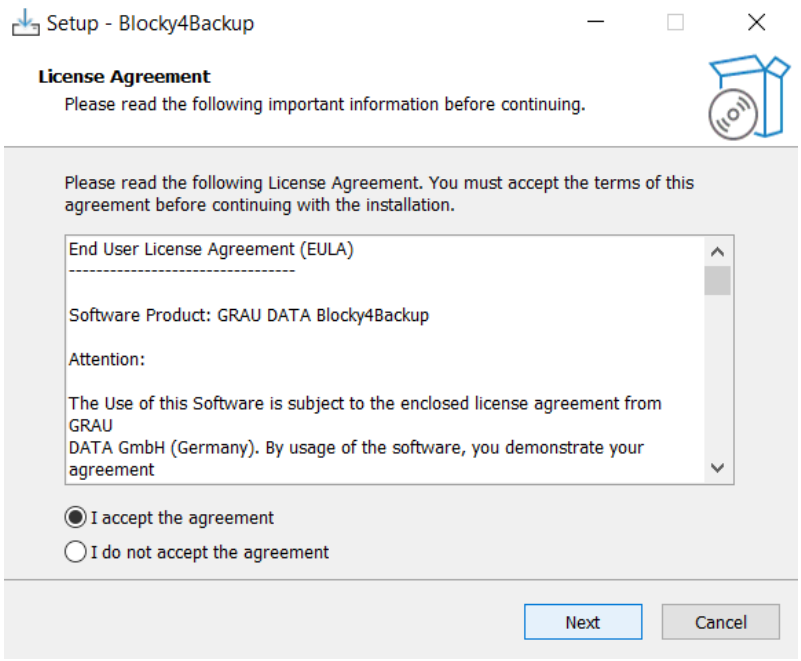
- Close all applications running on the system.
- Run the setup program `Blocky4BackupSetup_2_7_0_56.exe` to start the installation wizard.

Administrative rights are required to install, configure, license or update Blocky4Backup. 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 Blocky4Backup setup file).

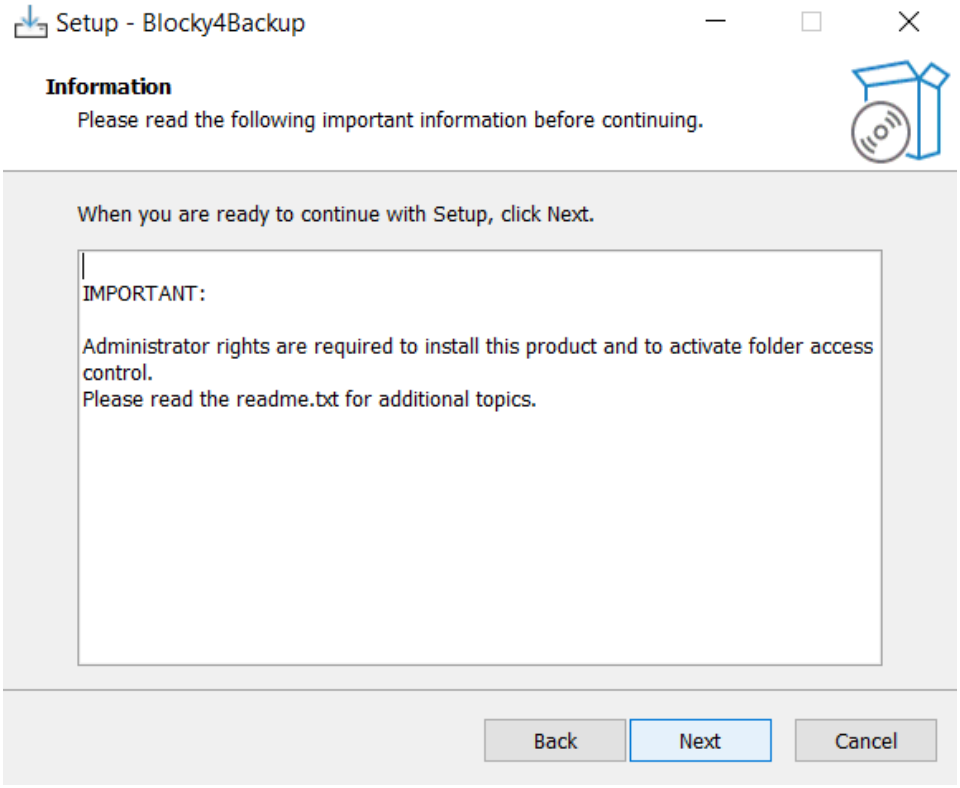
Check Controlled folder feature and turn off if activated. See Restrictions.



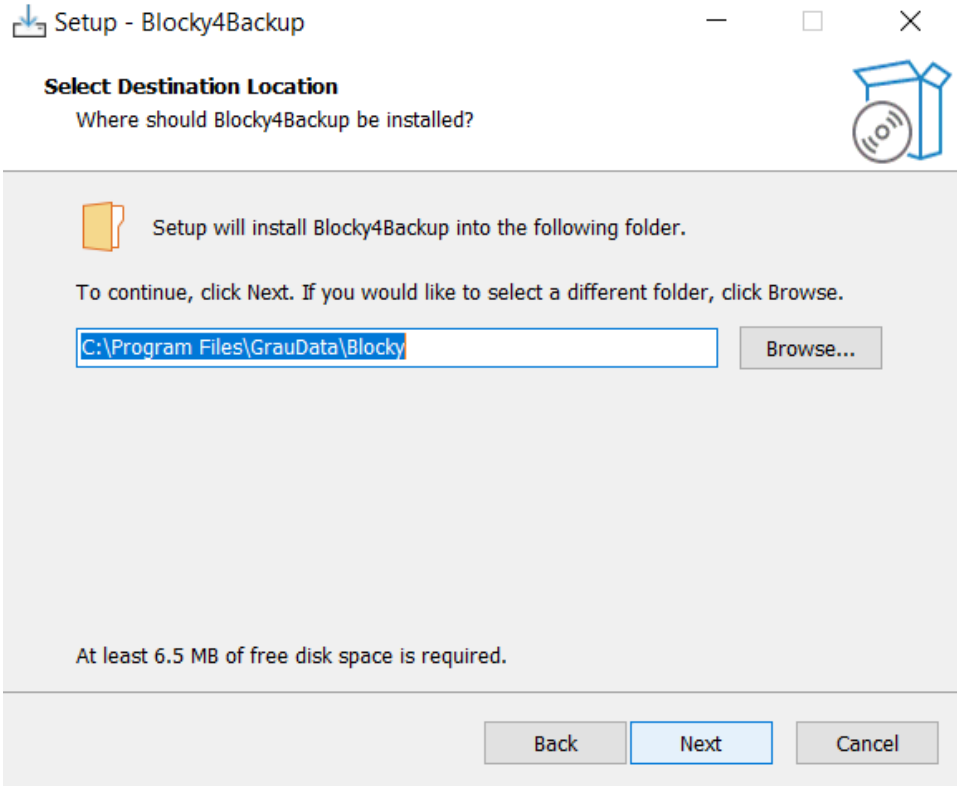
3.1.2. License Agreement



You have to accept the „License Agreement“ in order to continue with the Blocky4Backup installation procedure.



3.1.3. Select the installation path and additional tasks

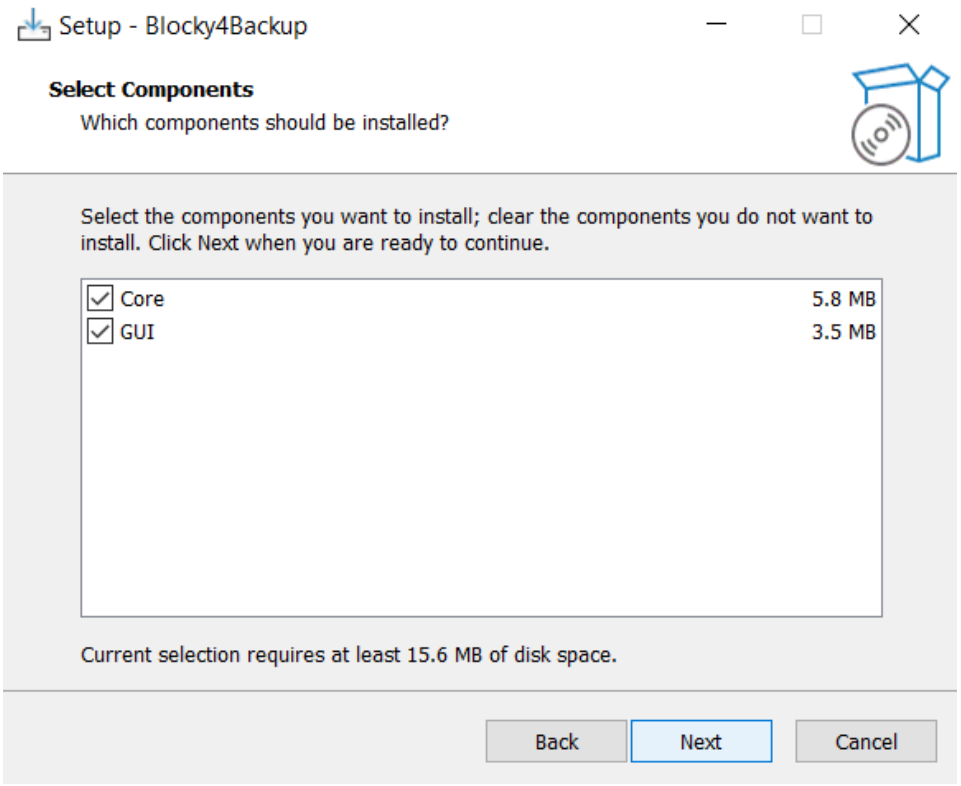


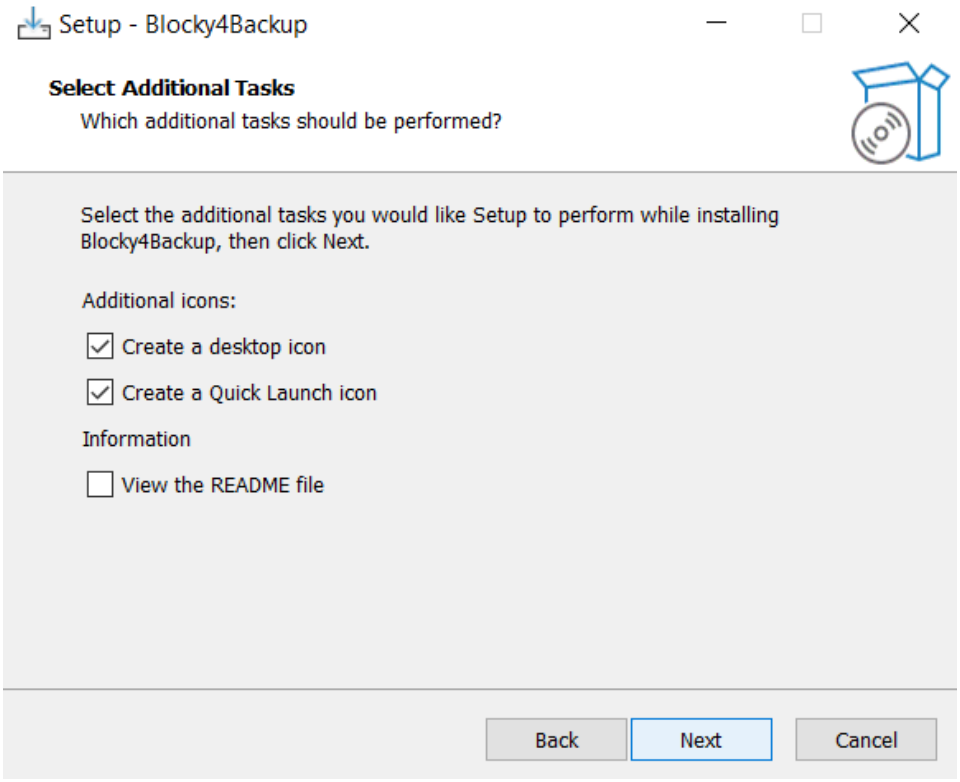
3.1.4. Select Components

Please select the components you want to install.

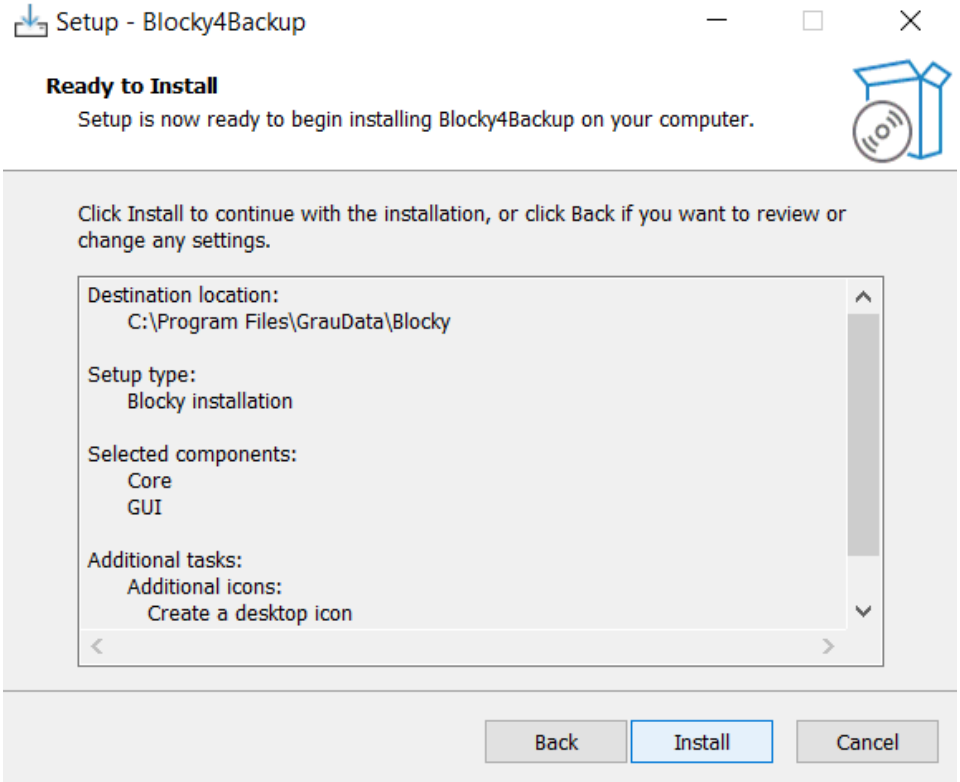
The components can only be selected for a new installation!

If you want to change the components after installation you have to uninstall Blocky4Backup and then install it again.



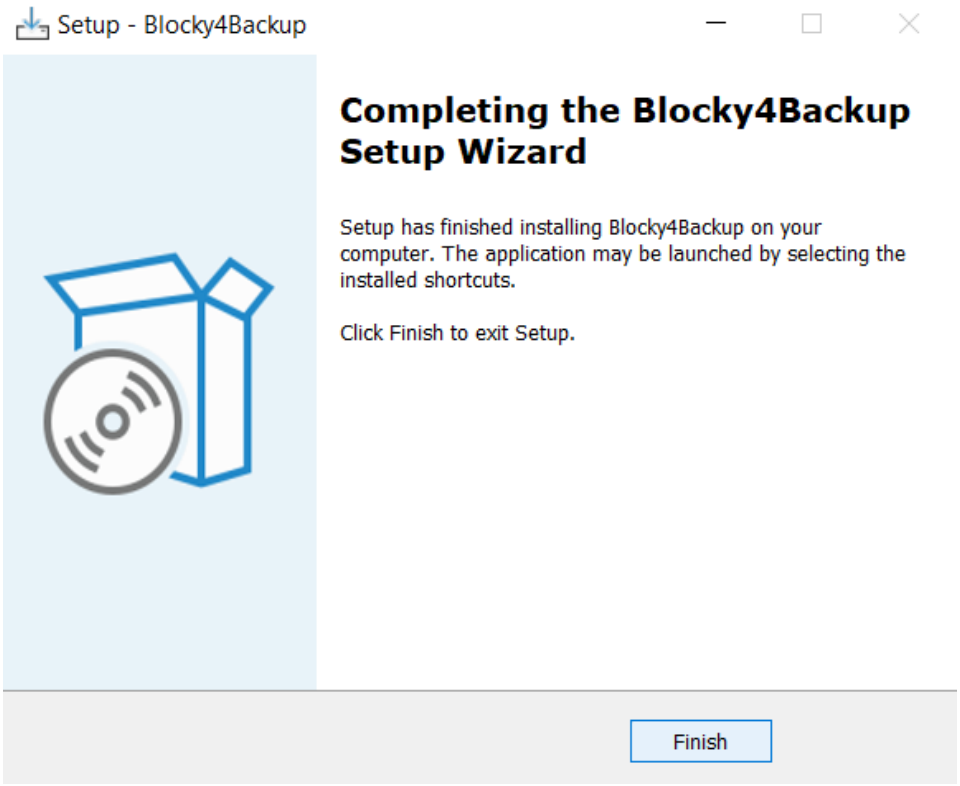


3.1.5. Start the Installation



After clicking the Install button, Blocky4Backup will be installed to the selected destination folder.

3.1.6. Completing the Installation



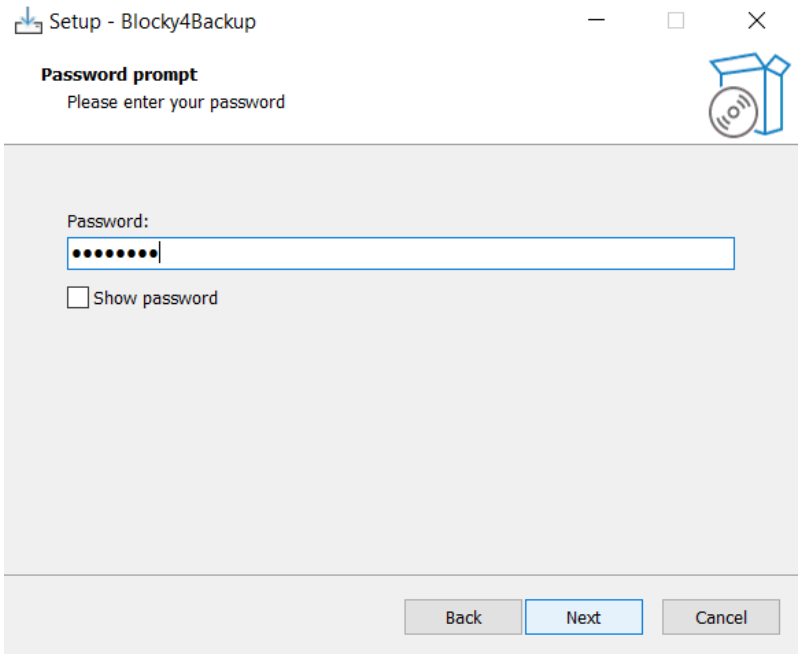
After clicking „Finish“ the installation is completed.

On Core-only installations, you have to set the initial password via BlockyCLI after installation or via Blocky4Backup setup parameter during installation. See chapters BlockyCLI and Setup command line parameters.

3.2. Updating

The update process from an earlier 2.6 and 2.7 versions is similiar to the installation described in chapter Installation.

When updating Blocky4Backup a password query is only requested if the core is installed.



When a Central GUI installation is updated to version 2.7, all remote managed Blocky4Backup servers must also be updated to version 2.7

3.3. Upgrading from Version 2.5 and earlier

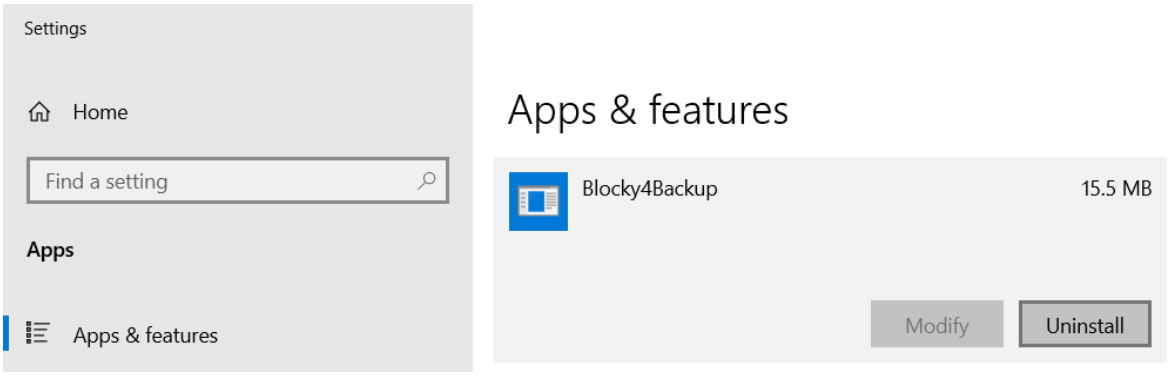
Versions 2.6 and 2.7 can be upgraded directly from version 2.5.

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.

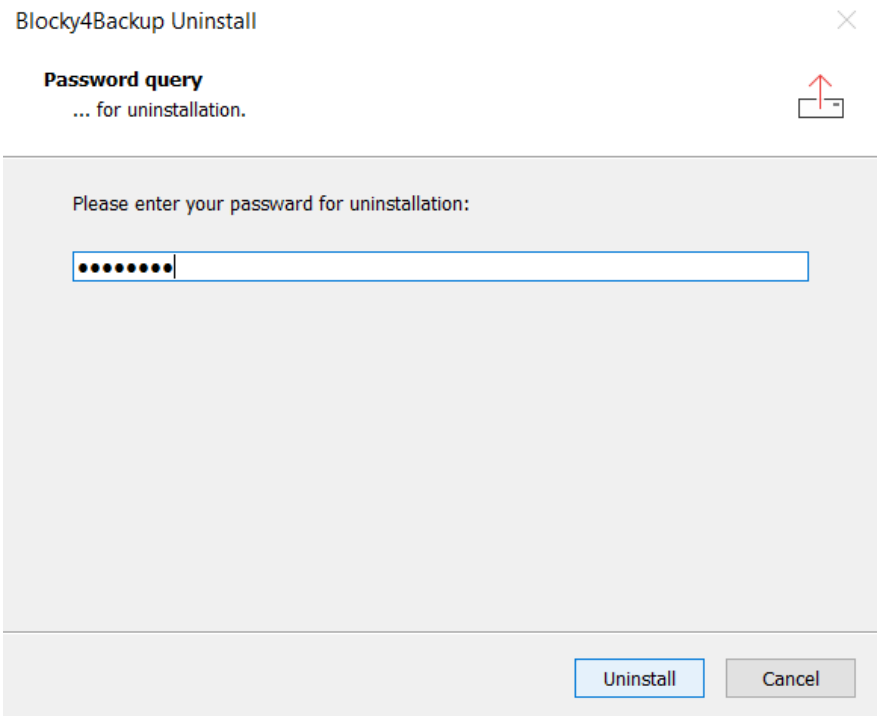
For further information or assistance please contact our GRAU DATA GmbH support (support@graudata.com).

3.4. Uninstallation



Blocky4Backup can be uninstalled by using the Windows Software Manager.
Click "Start >> Control Panel >> Add or Remove Programs"
Select the Blocky4Backup product and press the “Uninstall” button.

With core component installed:

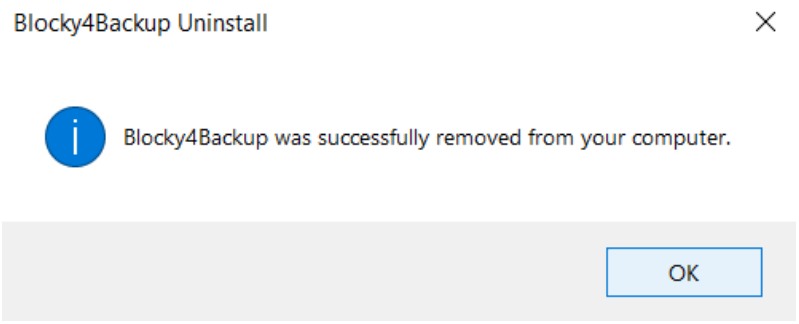


Confirm the Uninstallation of Blocky4Backup with your password.

To uninstall Blocky4Backup 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.

Continue by pressing “Uninstall” and Blocky4Backup will be removed.



A pop-up message informs if Blocky4Backup was successfully removed.

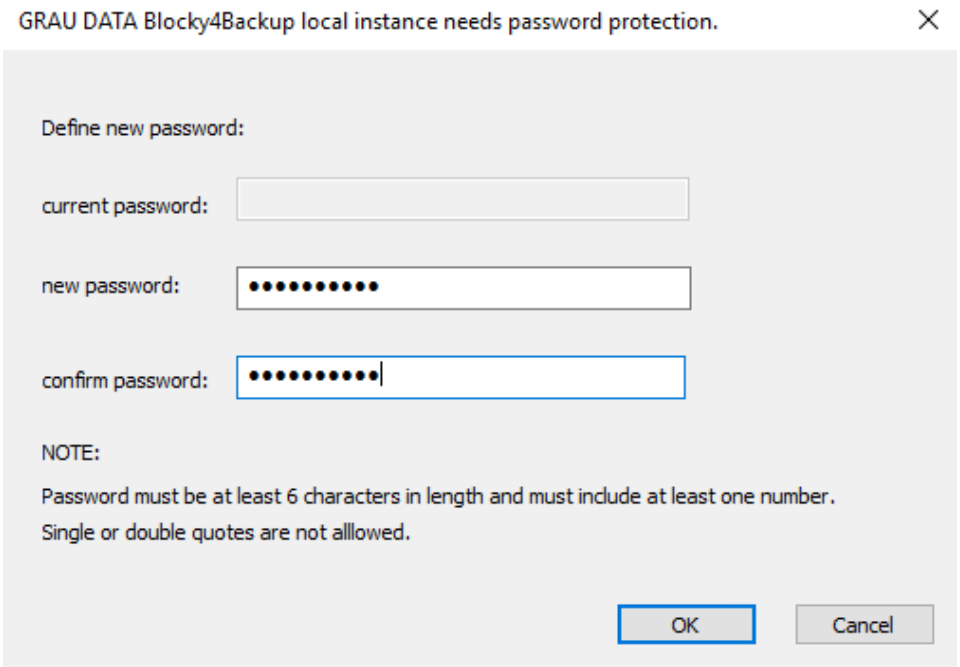
4. Configuration

4.1. Start of the GUI

In order to configure Blocky4Backup run the program `Blocky GUI.exe` by clicking on its desktop icon.

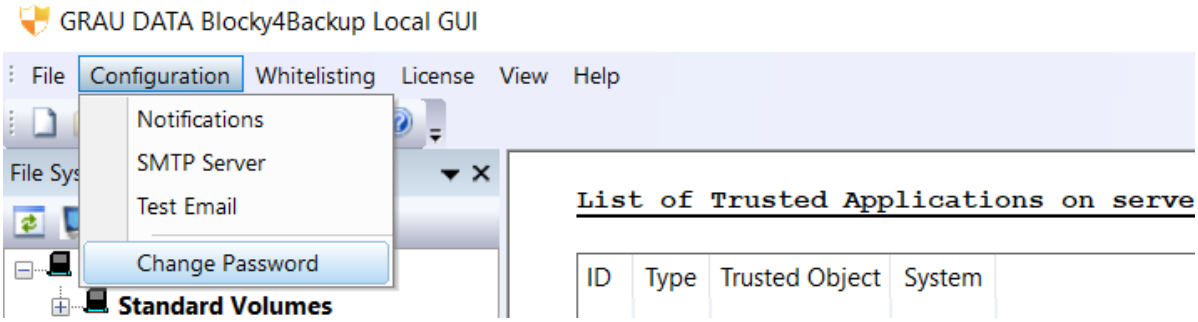
Administrative rights are required to run Blocky GUI. You need to be logged in as Administrator or you need to run the program using the context menu option “Run as administrator” (Right-click the Blocky4Backup icon). In case of missing privileges, see chapter Diagnostics for details.

4.2. Set initial password

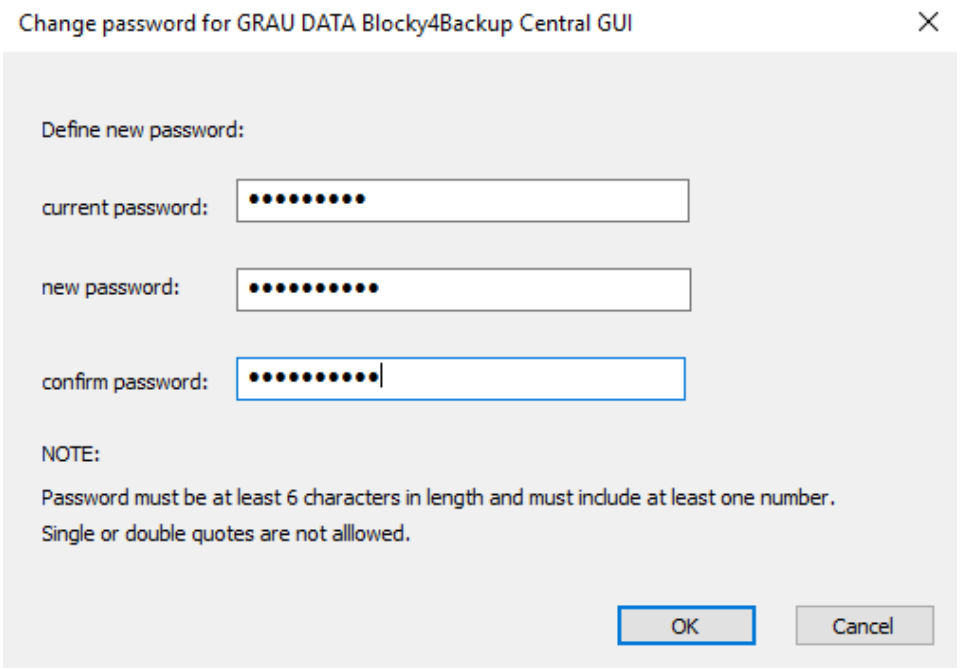


To protect the software against unauthorized configuration changes a password has to be supplied for the GUI to launch. When starting the GUI for the first time, you need to set this password. Please note that single quote (') and double quote (") characters are not allowed. This local GUI password also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

4.3. Change password



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

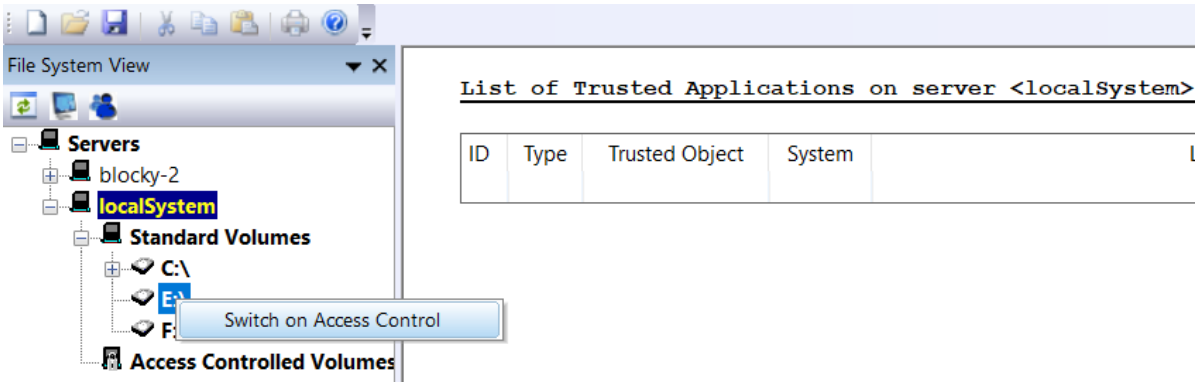


To define the new password, the current password must be provided and the new password needs to be confirmed. The changing process will be finished after clicking “OK”.

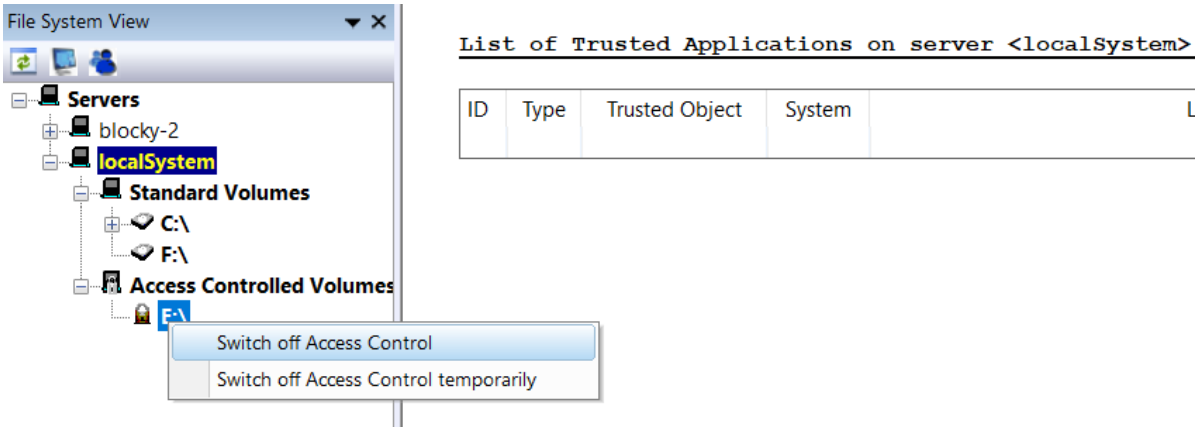
4.4. Access Control

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 controled 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.

4.5. Whitelisted Applications

There are several options to whitelist trusted applications.

4.5.1. Automatically whitelist applications

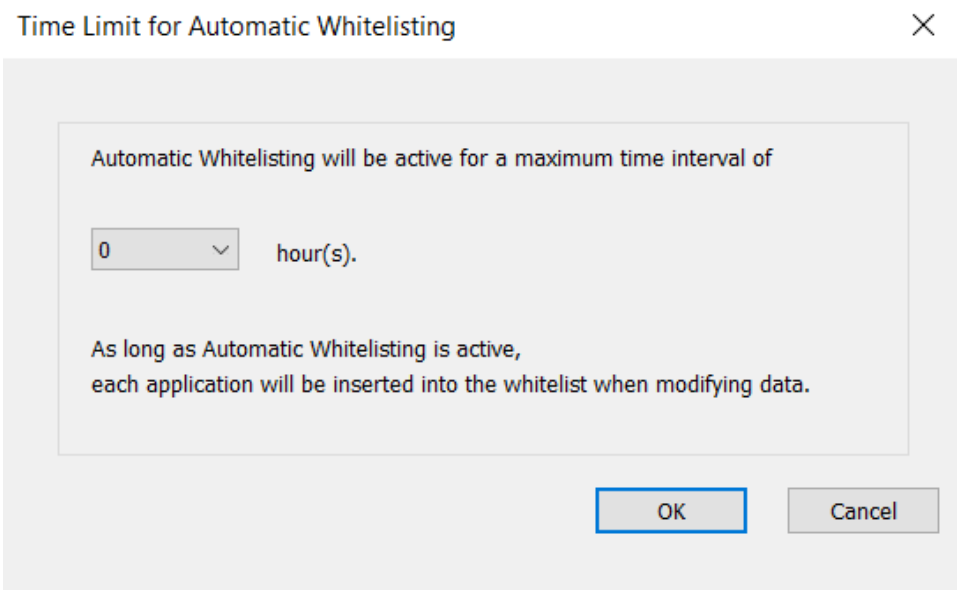
Caution:

When using Automatic Whitelisting, ALL program requests are granted and they 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 temporarily be used 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 connection from another GUI will terminate automatic whitelisting in the background.



4.5.2. Manually whitelist applications

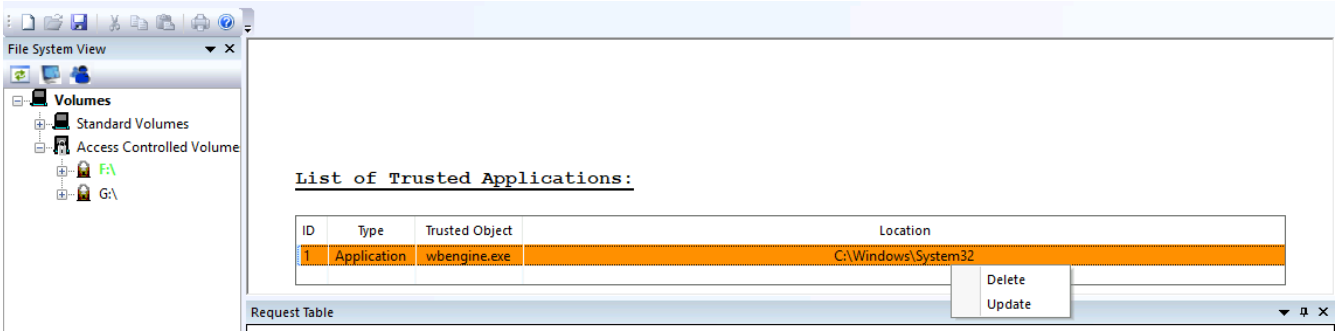
Select the menu item “WhiteListing >> Whitelist Programs” from the Blocky GUI main menu and pick the application you want to allow unrestricted file access in the FileBrowserDialog. If the whitelisting process was successful the application is displayed in the table “List of Trusted Applications”.

4.5.3. 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.

4.5.4. 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

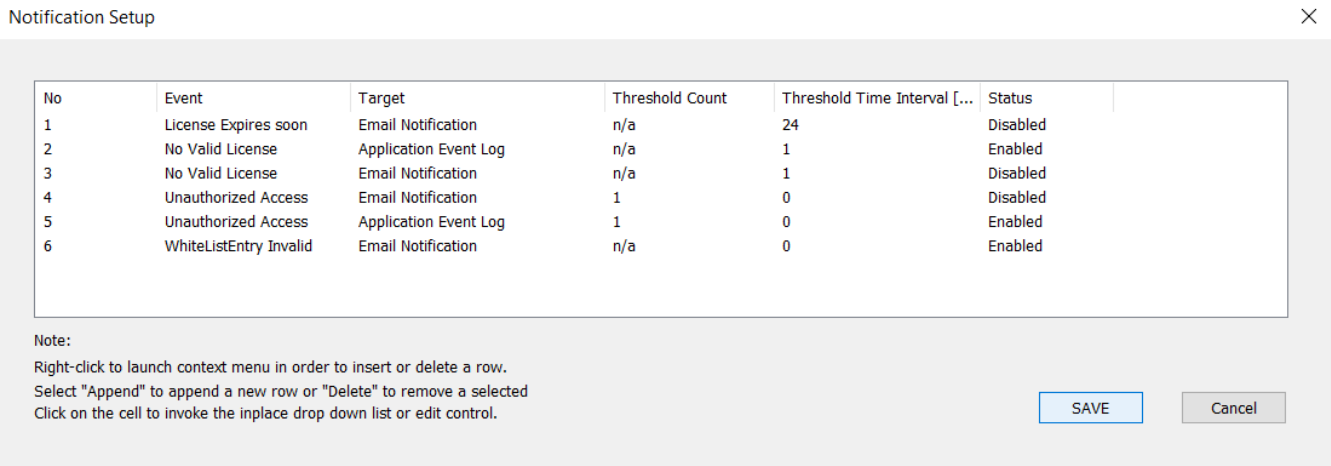


When a whitelist entry is invalid, all write access attempts of that application will be denied. You have to update this entry to grant access.

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. Notifications

Blocky4Backup can send alert notifications to the Windows application event log, to configured email recipients and to the Status Area of the Blocky GUI 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.



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 via whitelisted app
- 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.

Rules:

Threshold Count	ThresHold Time Interval [min]	Action
<n>	0	Stateless event: notification is sent after <n> occurences.
<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 occured.
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.

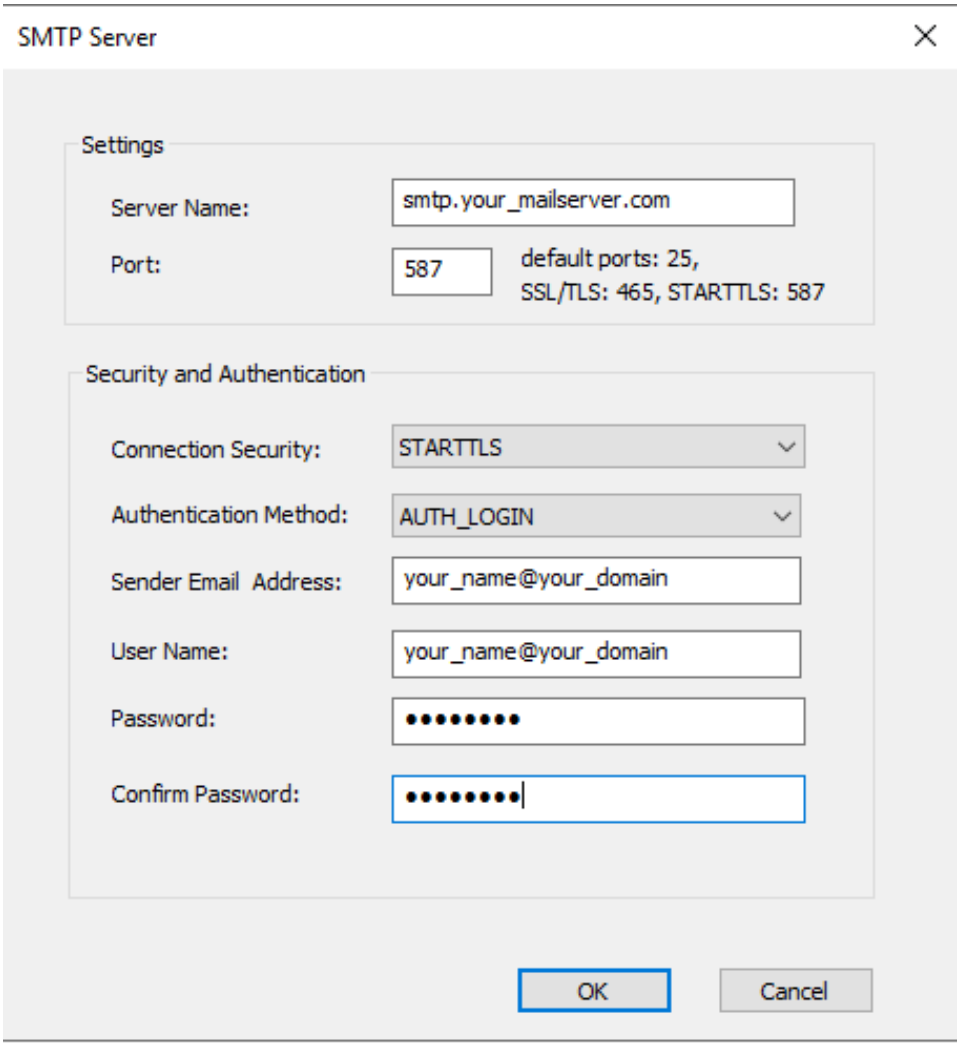
Example: (email notification)

<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

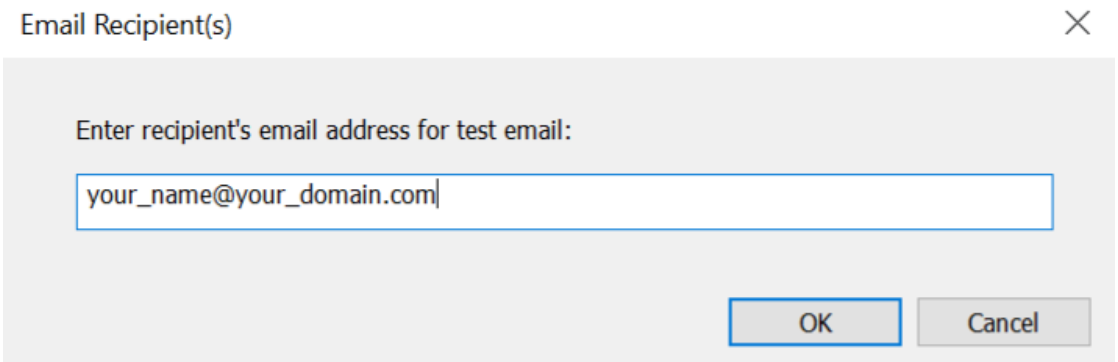
Example: (GUI status area)

4.7. 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:

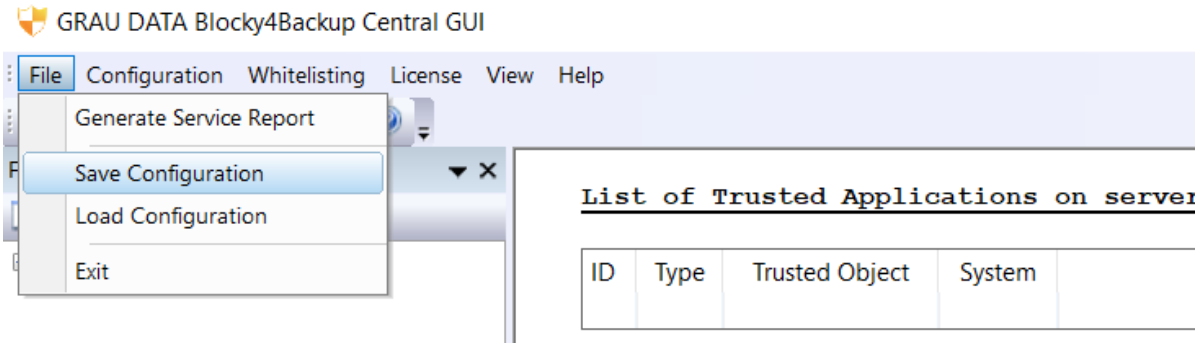


Your settings can be tested by sending a test email to your user account.
"Configuration >> Test Email"

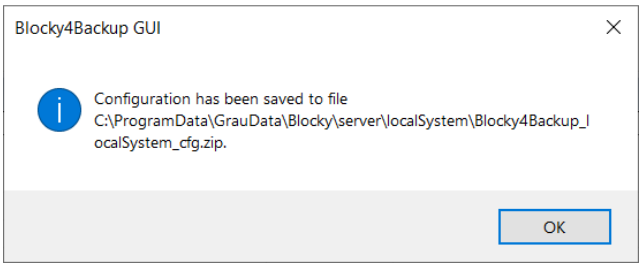


4.8. Save / Load Configuration

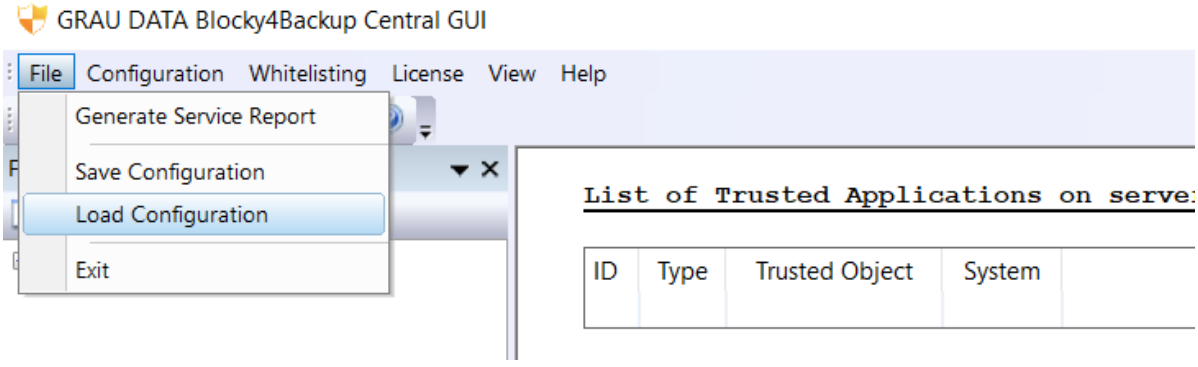
The current configuration can be stored for a later restore. This will store the SMTP Server configuration and other settings for notification and whitelist in the file `C:\ProgramData\GrauData\Blocky\server\localSystem\Blocky4Backup_localSystem_cfg.zip`.



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



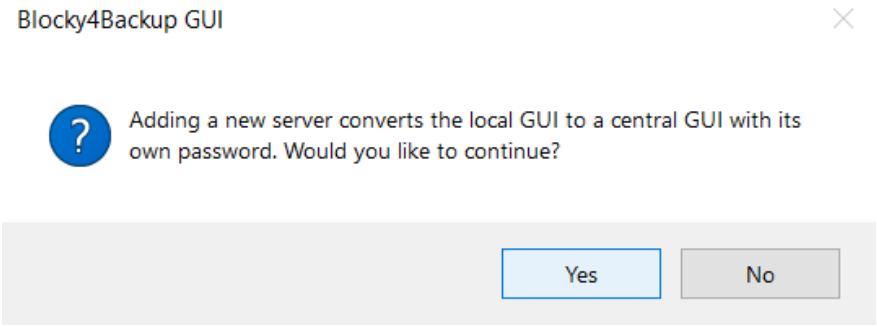
To restore configuration settings use “File >> Load Configuration” and navigate to a previousely saved configuration file.



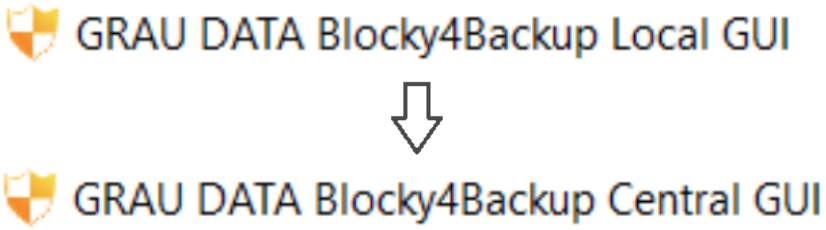
In Central GUI Mode, save configuration will store the configuration from the active connected server on the system running the Central GUI in a corresponding subfolder in path `C:\ProgramData\GrauData\Blocky\server\`
Load configuration will restore the configuration then from this location.

4.9. Central GUI Mode

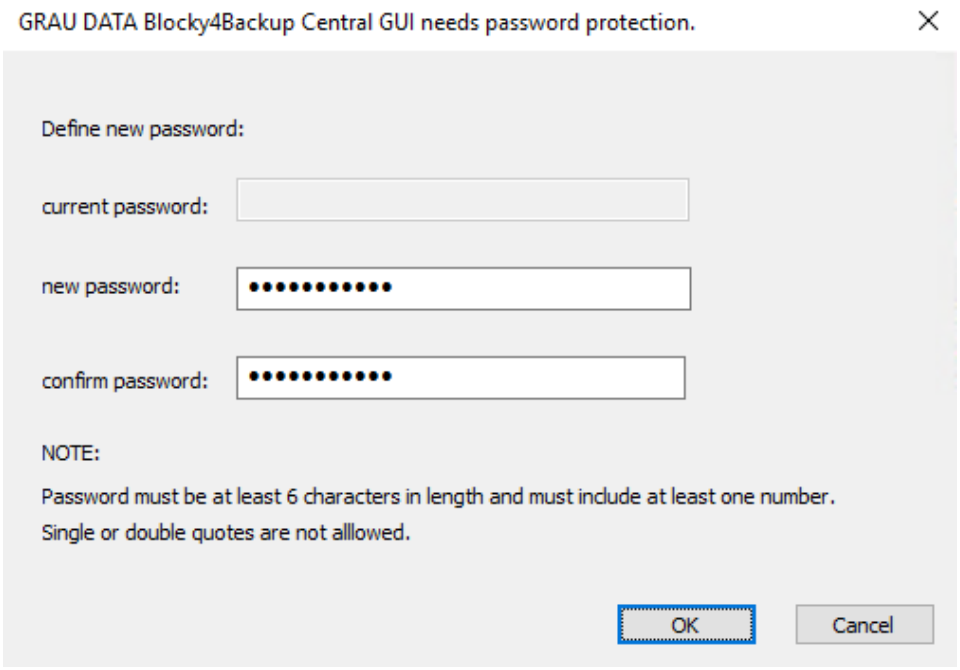
After installing Blocky with Core and GUI components, the GUI is in the local mode. On GUI only installations (without local Core components), the GUI is already in central mode. The operation mode of the GUI is shown in the heading of the GUI. By adding a server to a local GUI, the GUI has to change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

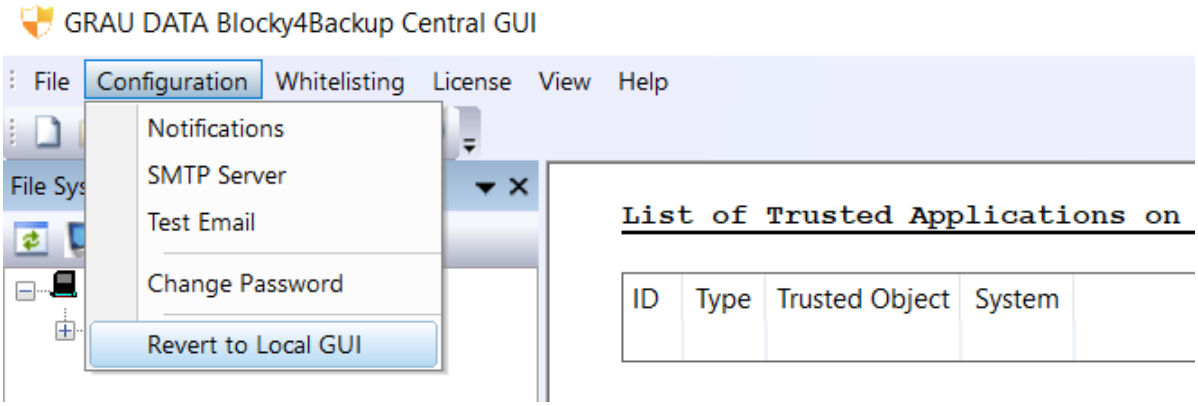


By changing the operation mode from local GUI mode to central GUI mode, the newly definied password is valid for the central GUI only. The previously used password from local GUI mode is still valid for the local core components.

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:

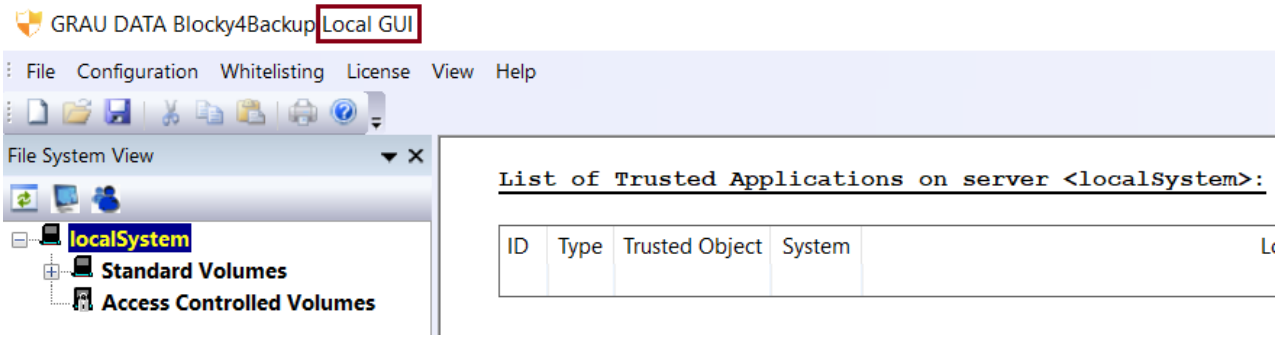
To revert from a central GUI to a local one you first have to remove all configured servers and groups. Then a new menu item will show up. Select the menu item “Configuration >> Revert to Local GUI”. The Item is only visible when the GUI is in central mode with empty server list.



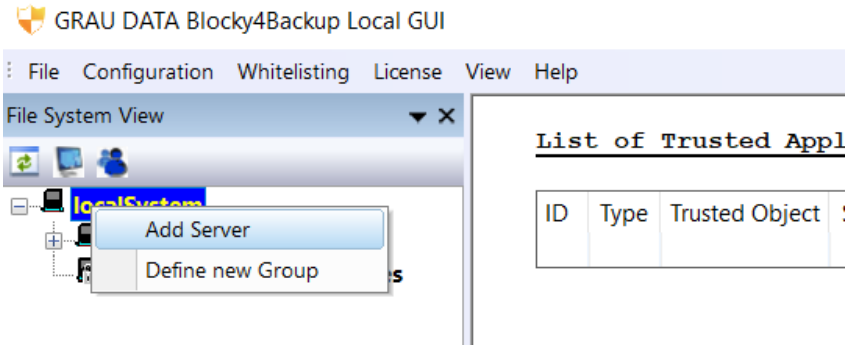
To recreate the entry for the localSystem the GUI needs to be restartet.

4.10. 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 "Servers" under the "File System View" and select "Add Server".

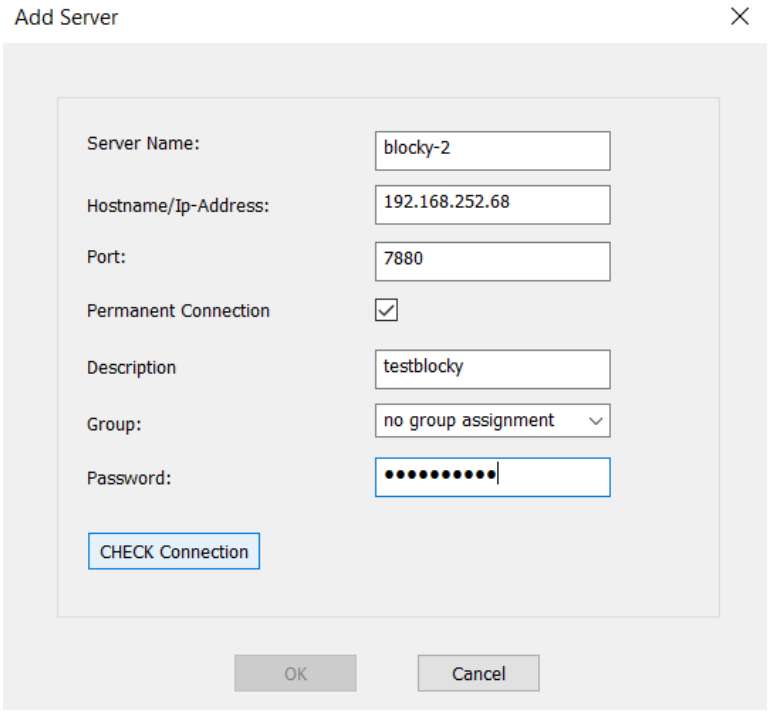


For successful connections from the central GUI to remote servers, the system running the central GUI must be able to ping the remote server (i.e. send ICMP echo requests) and the remote server must allow incoming connections on the Blocky service port (default port `7880/tcp`). Please adjust firewall 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`.

Please make sure the initial password on the remote server has been set. Either via local GUI if installed, via BlockyCLI or via Blocky4Backup setup parameter. See chapters BlockyCLI and Setup command line parameters.

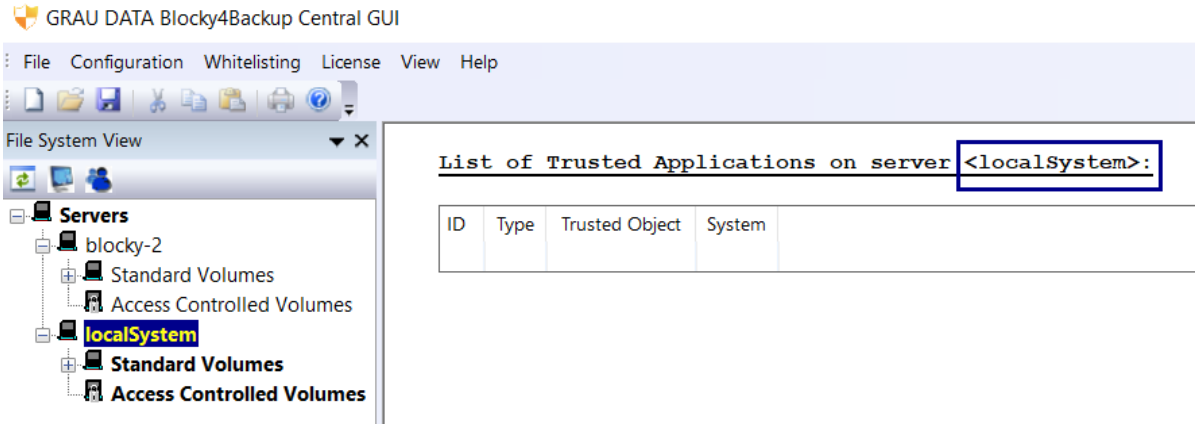
Please make sure the system clock of the remote server is in sync with the system running the central GUI. If the service authentication fails check system clock.

Fill out the following dialog with your servers data. Use the "Check Connection" button to check if your server is reachable. You can add the server only if the check was successful.

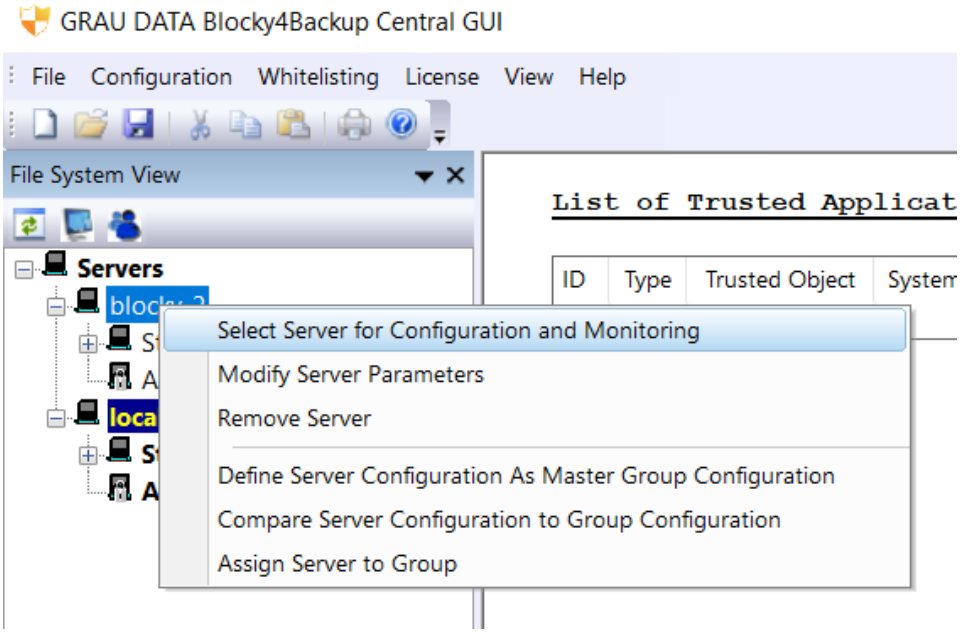


4.11. Server selection

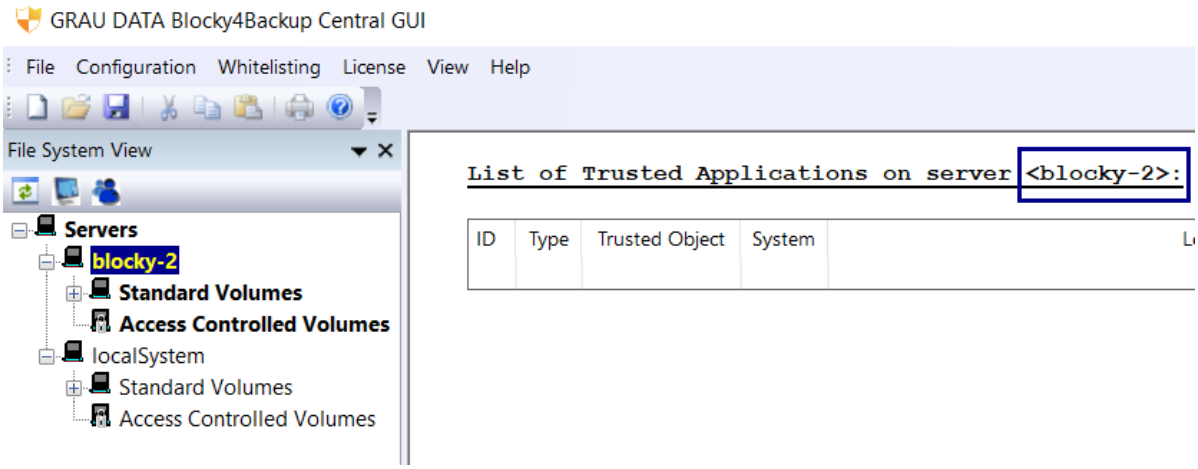
Per default the localSystem is selected for configuration and monitoring. The selected server is displayed in a yellow color with dark blue background, it can be configured and its List of trusted Applications, Request Table and other Informations are shown in the GUI.



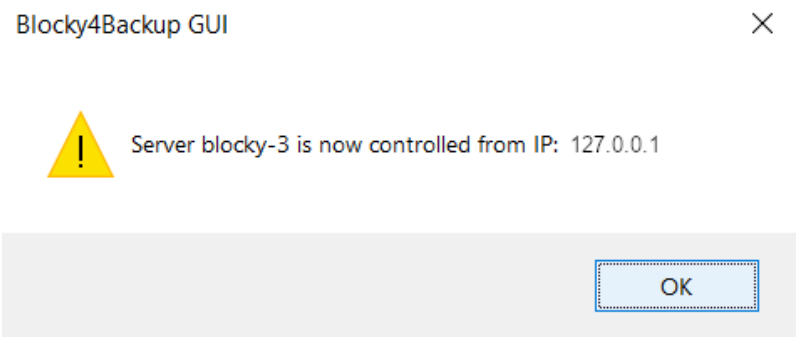
To change server right-click on the server you want to configurate and select "Select Server for Configuration and Monitoring". This will change the context within the GUI for configuration and monitoring to the selected server.



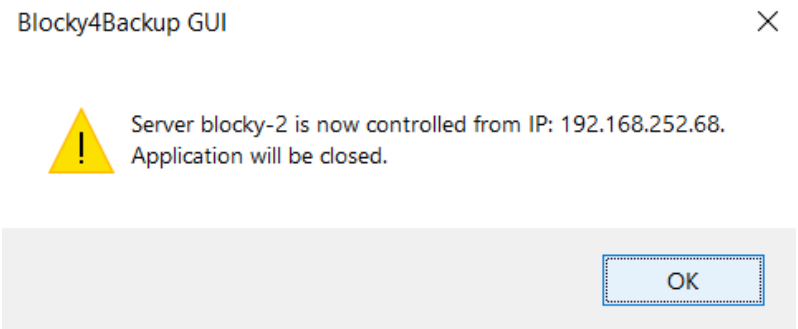
When the connection is established the highlight color changes and your selected server appears in yellow color with dark blue background and the list shows the Trusted Applications on the server.



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.

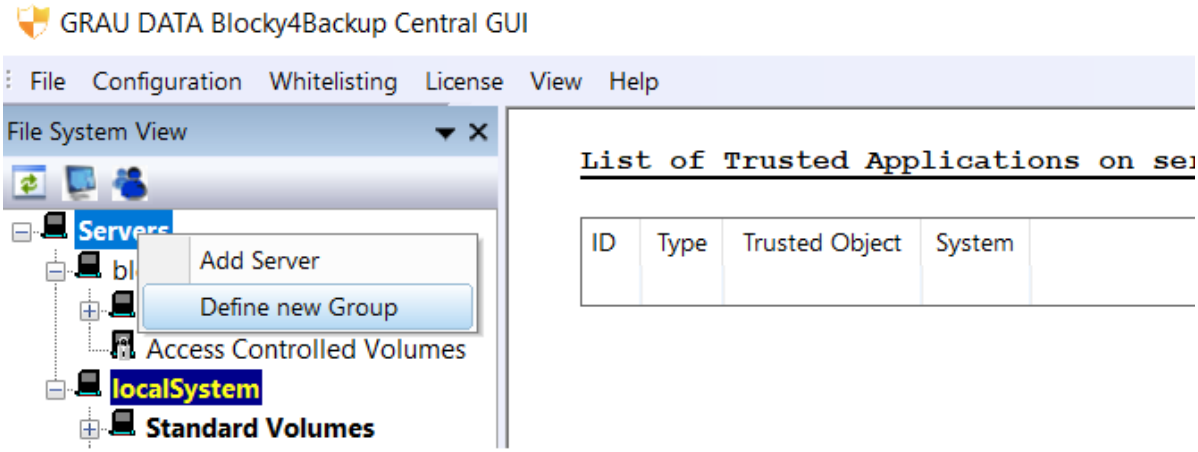


Each server can handle only one active connection at a given time, either from the local or a central GUI.

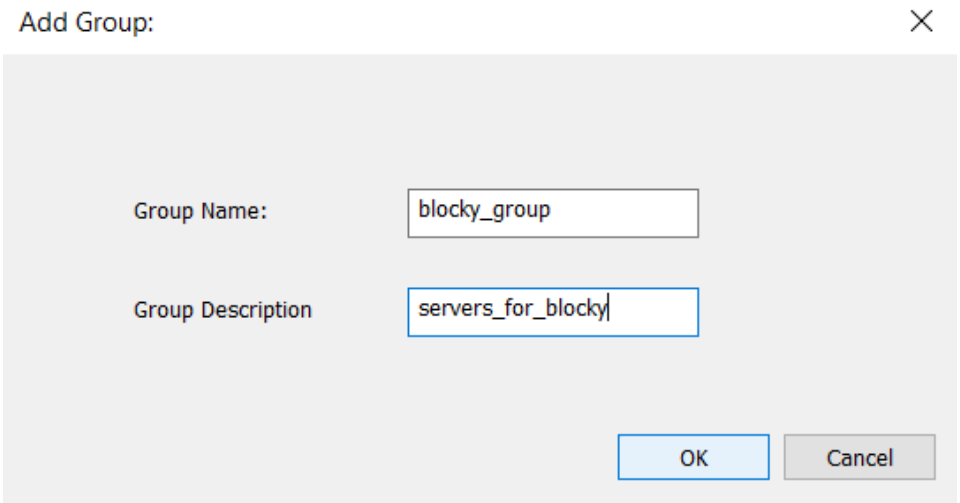
4.12. Define a new Group

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.

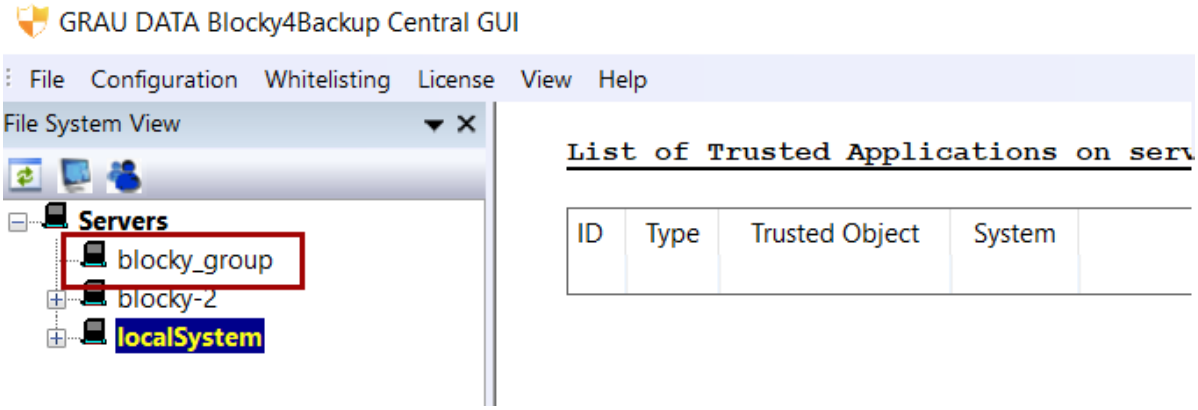
To define a new group right-click on "Servers" under the "File System View" and select "Define new Group".



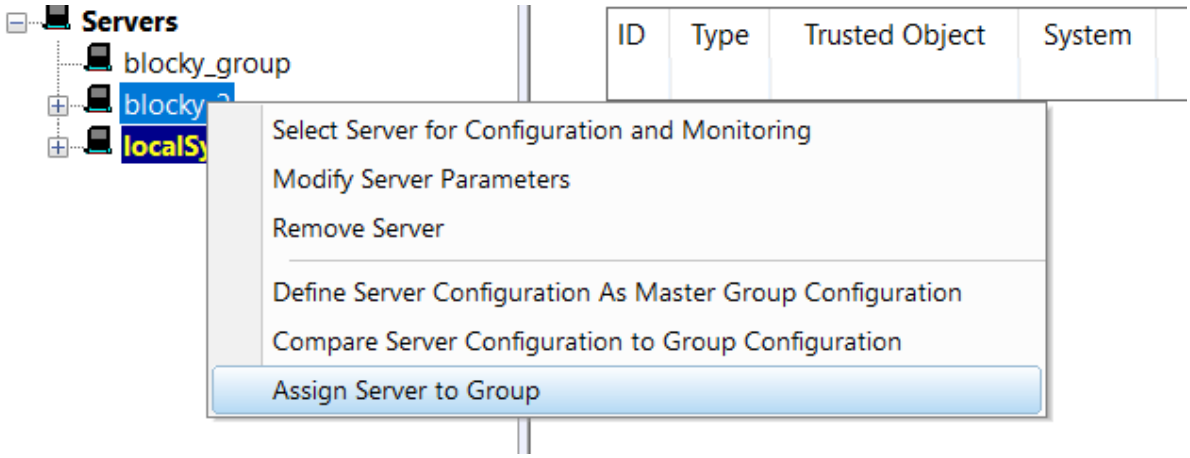
Name your group and fill out the description box. After clicking "OK" your group will be added.



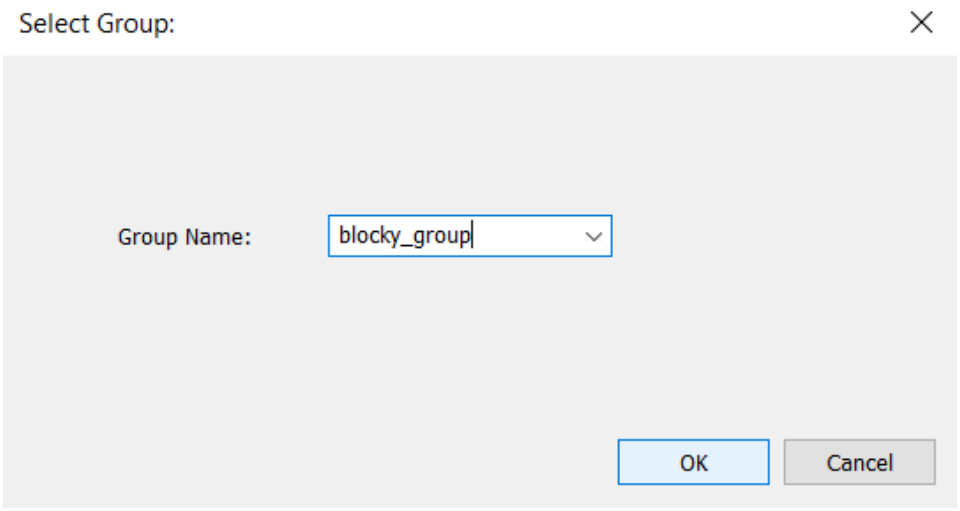
The group will be listed under "Servers" in the "File System View".



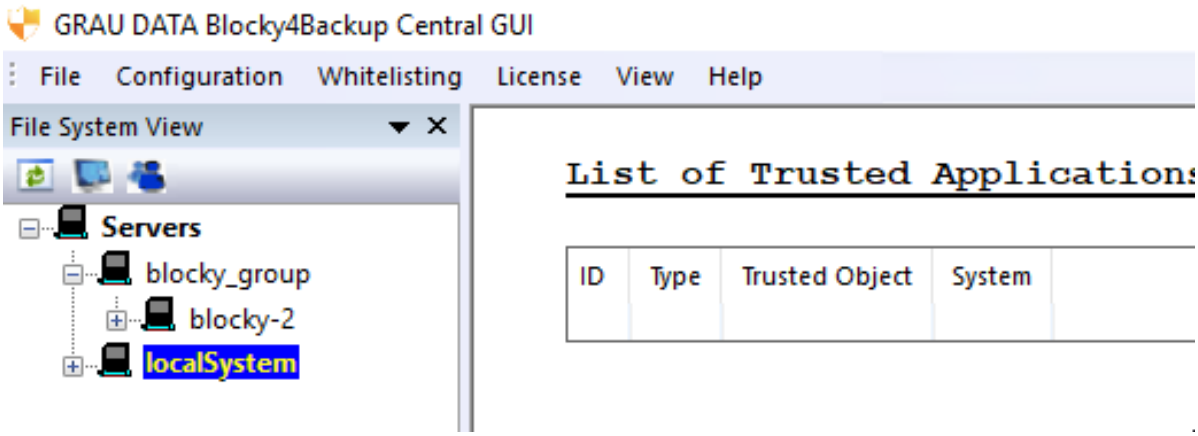
To assign a server to a Group right-click on the server you want to assign and select "Assign Server to Group".



Then select the group the server should be assigned to.



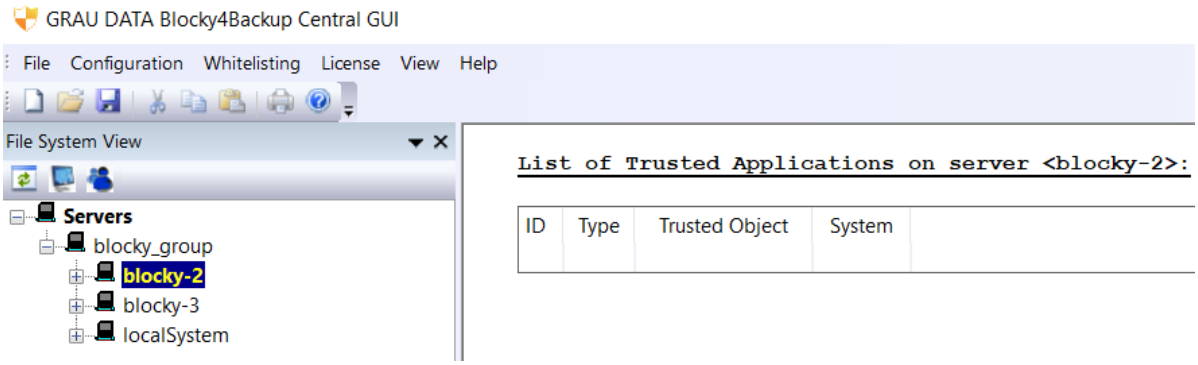
In the "File System View" this server is now listed under the selected group.



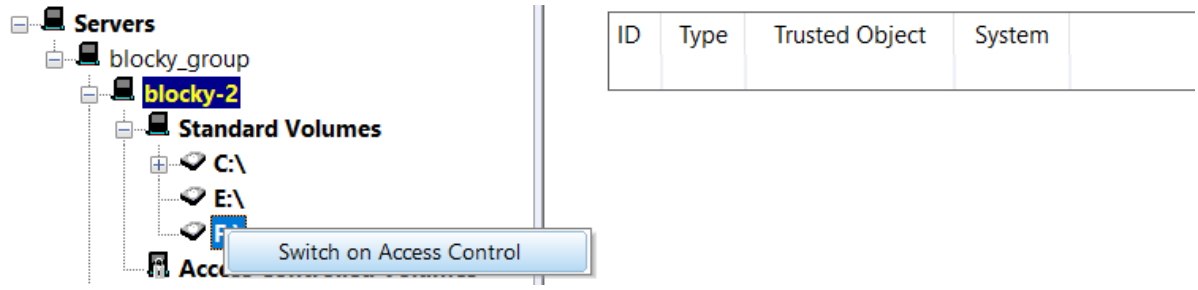
4.13. Master Configuration

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 configuraton includes whitelist, controlled folders and notification/SMTP settings.

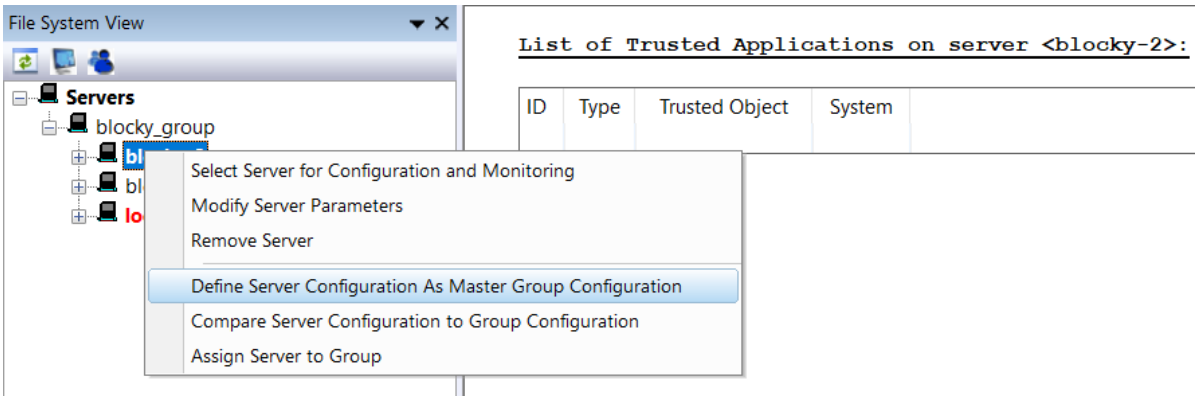
Select a server for Configuration and Monitoring.

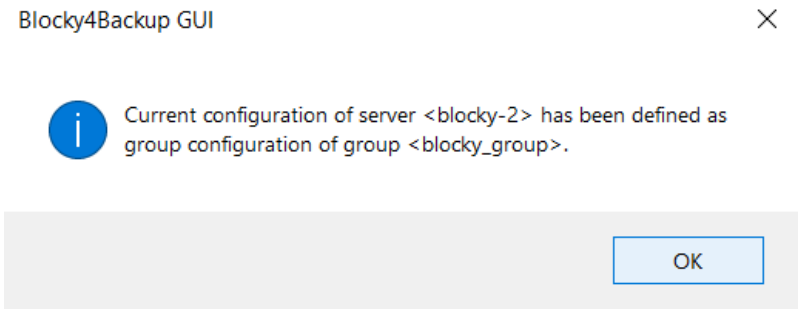


Configure the desired settings on this server. For example, switch on access control on a volume.

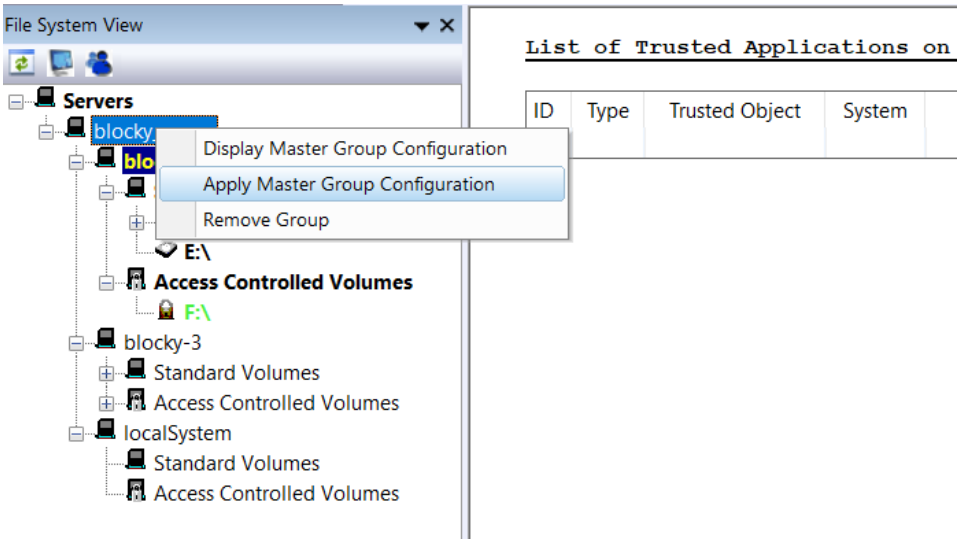


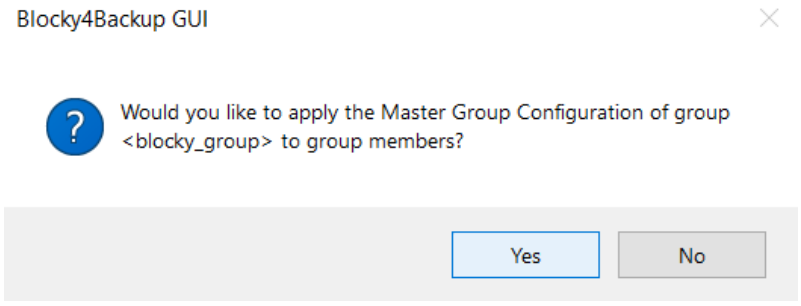
Define the group master configuration by selecting "Define Server Configuration As Master Group Configuration".





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



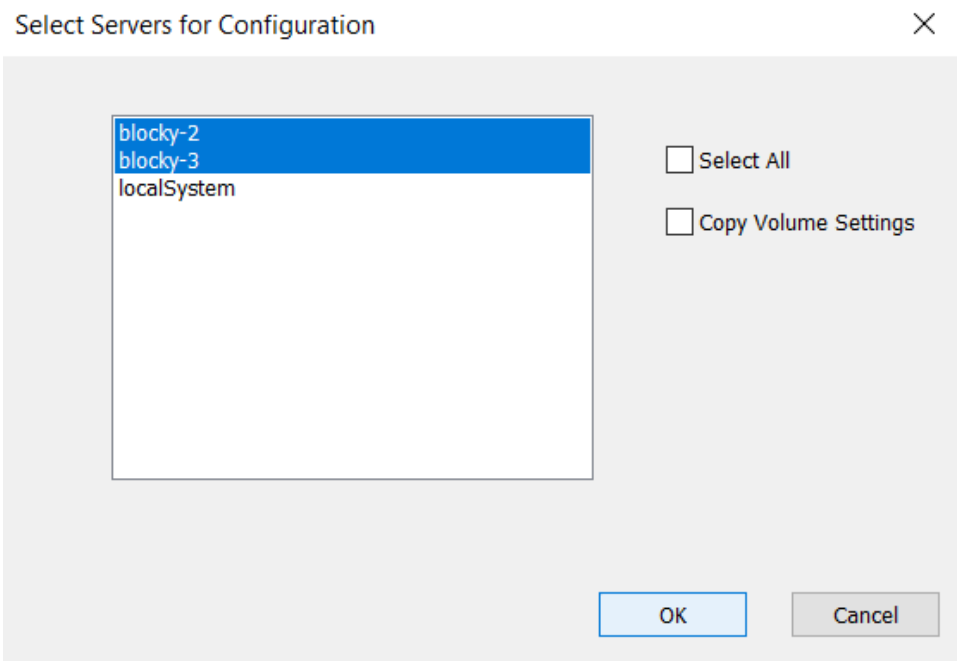


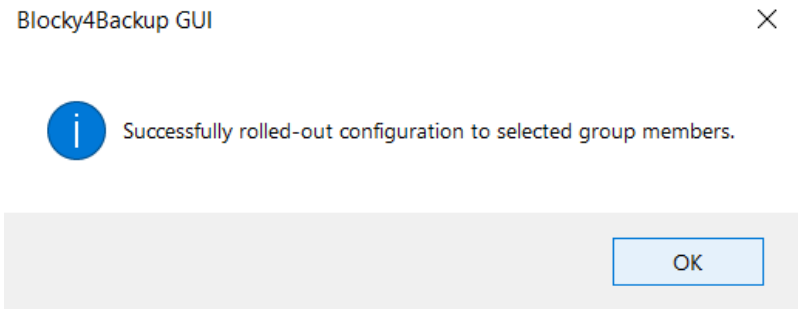
Select the servers where the Master Configuration shall be applied.

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

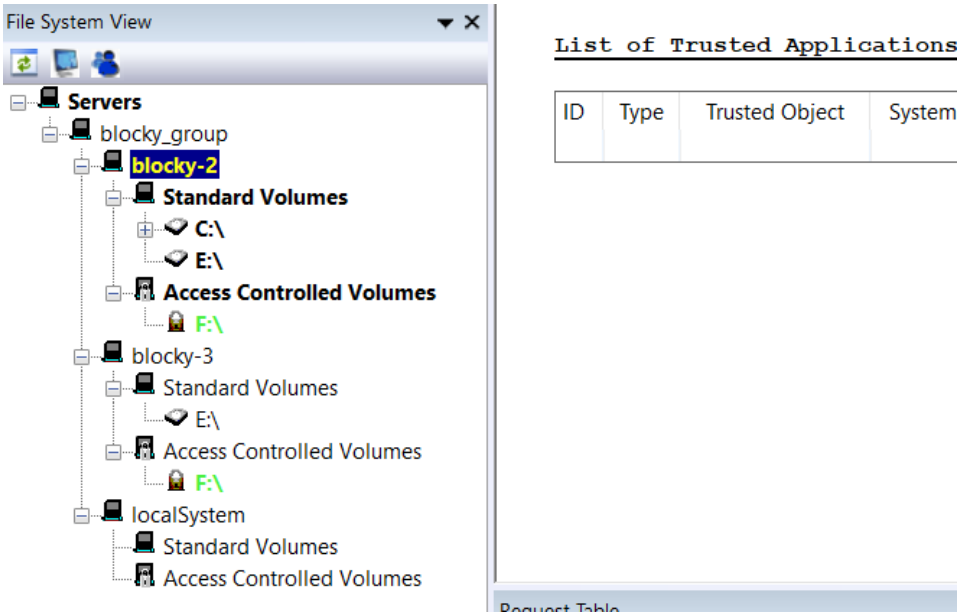
Caution:

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 Setings" is enabled.

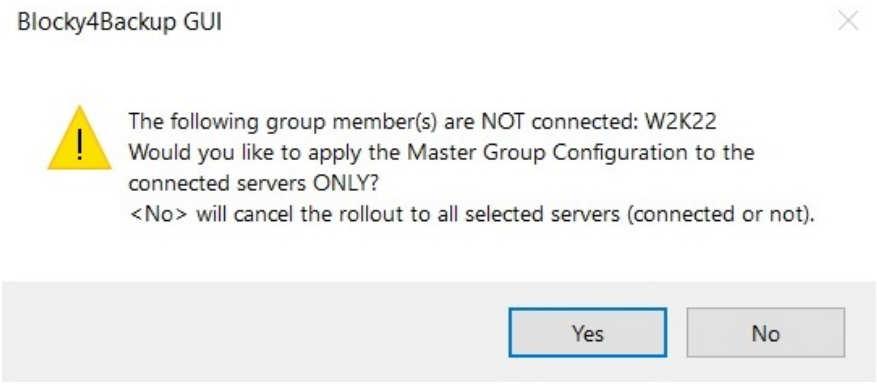




This configuration is now applied to the selected servers in the group.



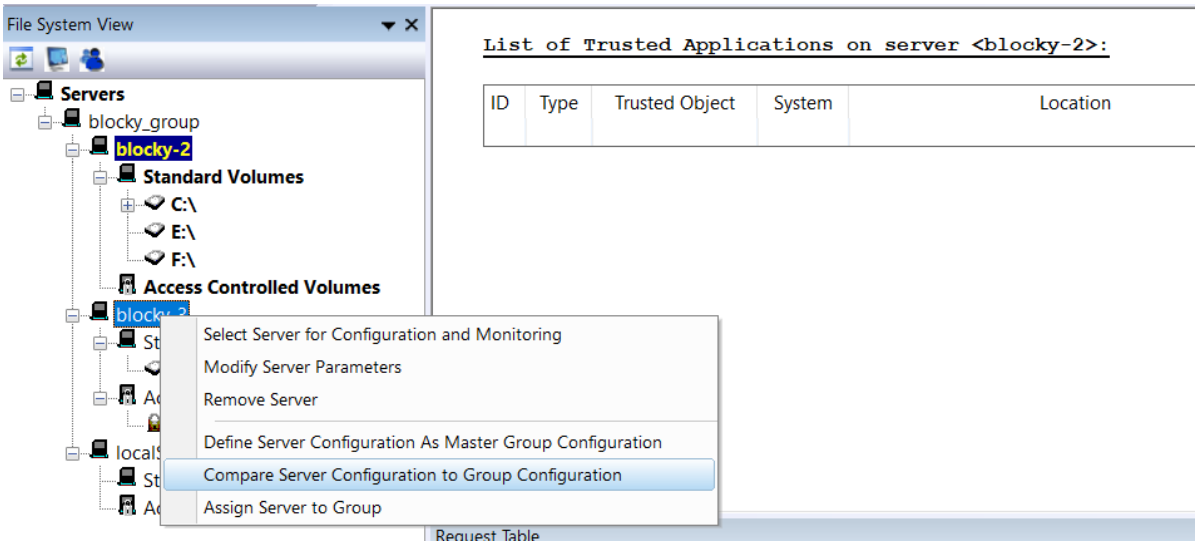
If some servers are not connected in Central GUI and the rollout of the configuration would fail, you have to choose to reconnect these servers or to rollout only to connected servers. If you choose to reconnect, any local connected GUI will terminate and the Central GUI will take over. You then have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

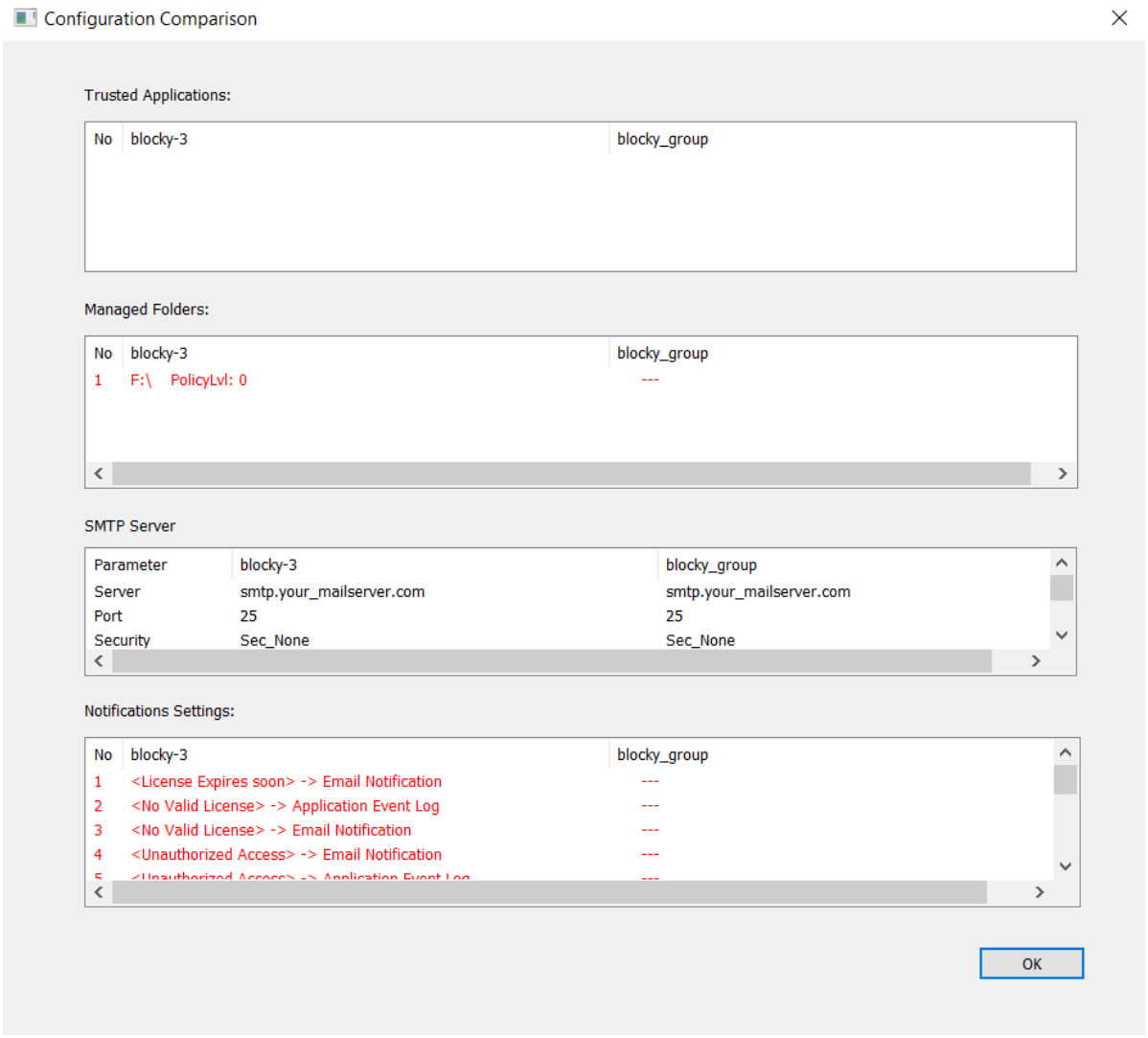


To apply/rollout all configurations all servers must be connected. If some servers are not connected you can apply the configuration to only the servers connected by clicking "Yes" or stop the process by clicking "No". Then try to reconnect the remaining servers and repeat the procedure.

4.13.1. Configuration Comparison

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





4.14. Licensing

Blocky4Backup 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 while the trial license is still valid to obtain a key for a registered license.

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

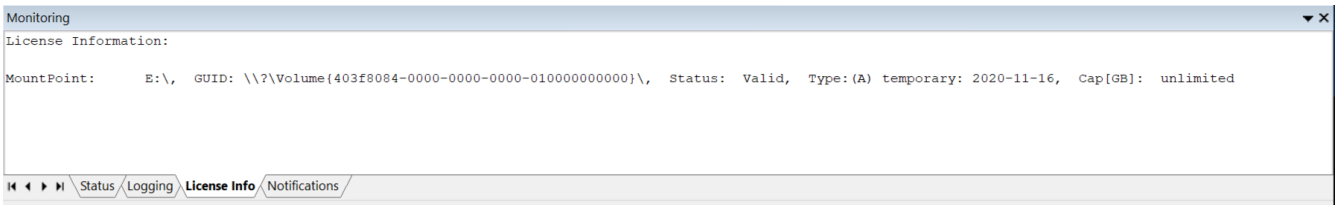
Licensing is also possible via BlockyCLI. See chapter BlockyCLI for available CLI commands.

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.

4.14.1. Initial Licensing

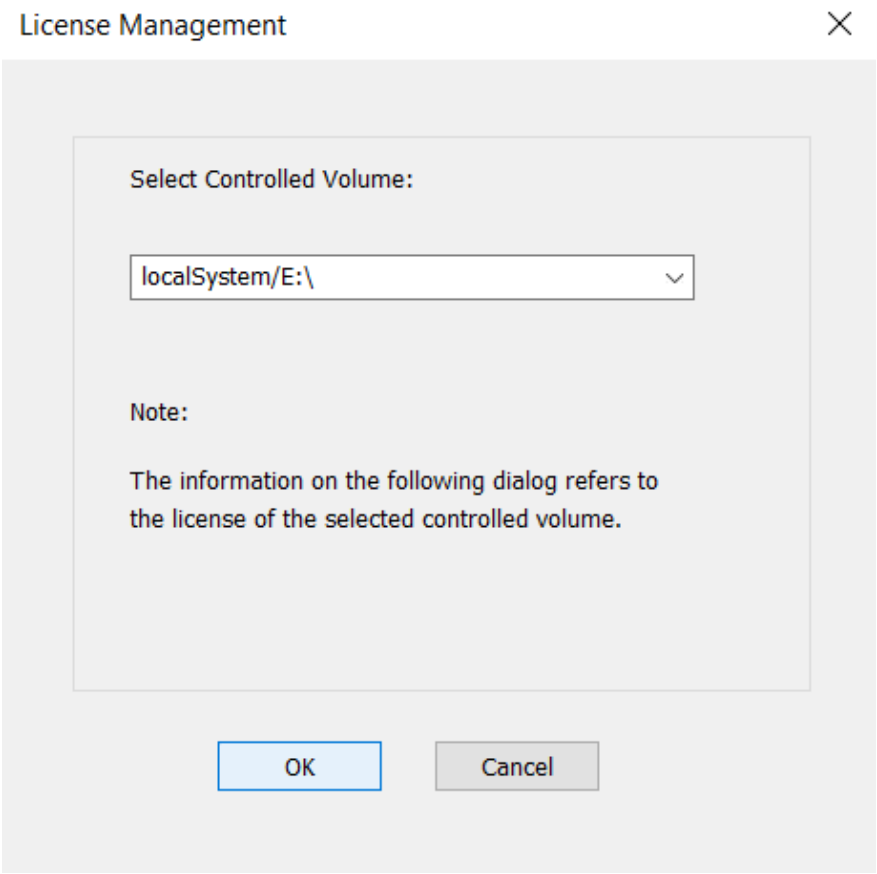
If the Access Control feature is activated on a volume, the temporary trial license for 60 days will be automatically installed on that volume. Licensing is always volume-based, which means that a license must be ordered for each volume which should be protected by Blocky4Backup.

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

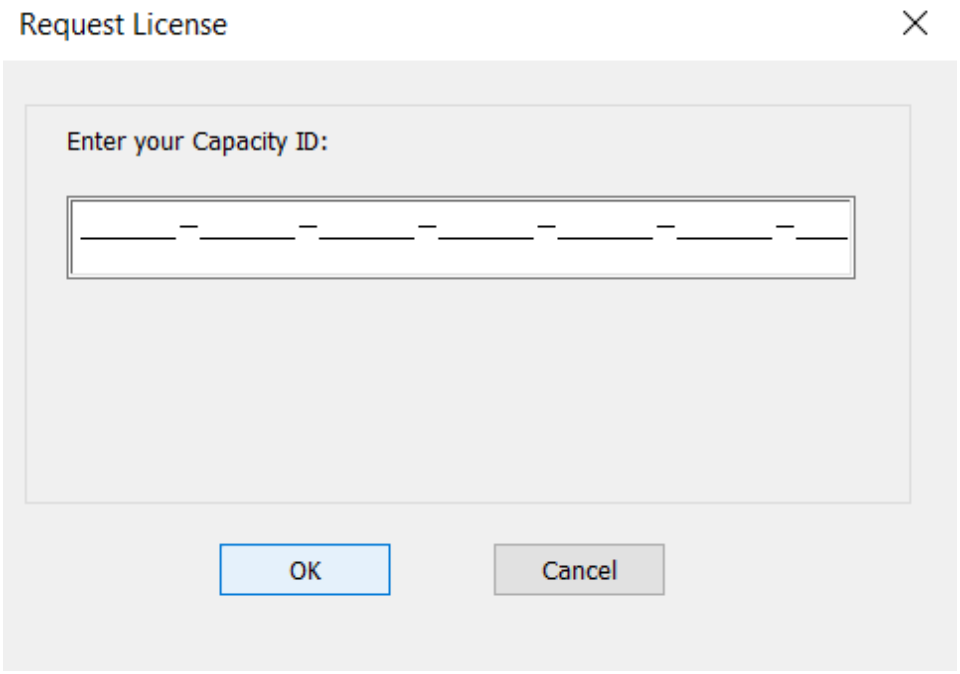


Each Blocky volume is registered separately and therefore has its own Blocky4Backup generated Capacity-ID, which is needed when requesting a registered license key for a Blocky volume.

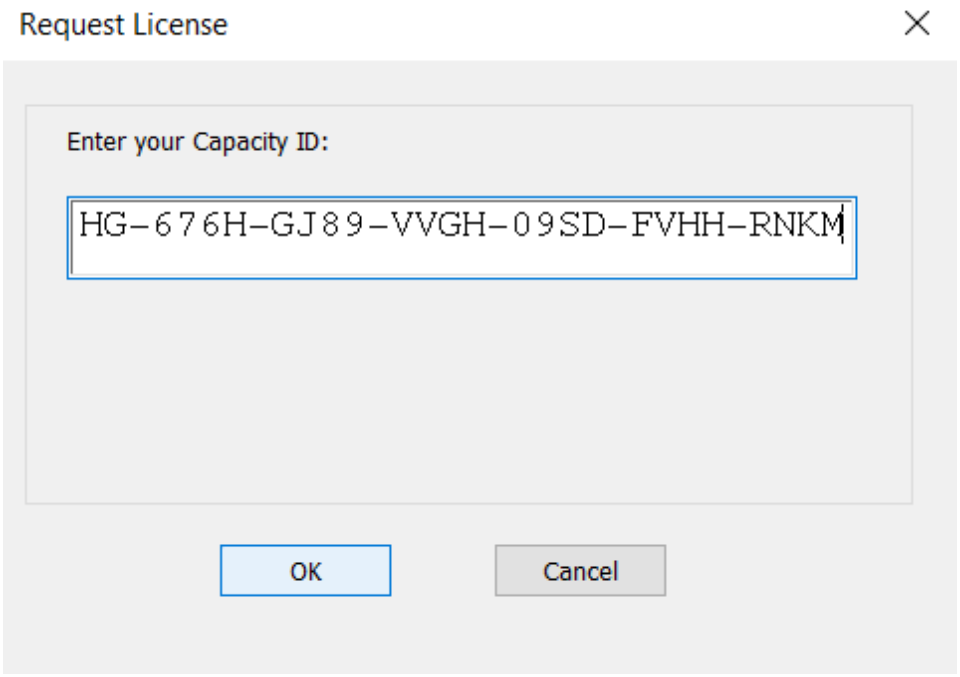
Select the menu item “License >> Request License” from the main menu.



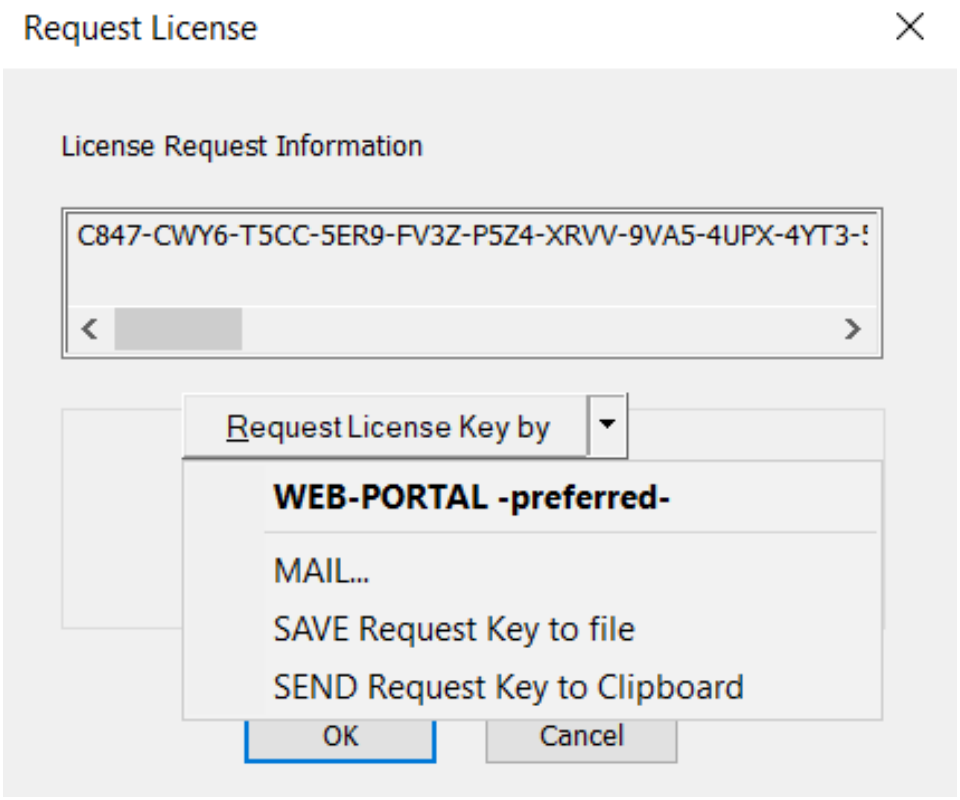
Use the drop-down list and choose the volume for which you want to request a license key.



Enter the Capacity-ID, which you have received from your Blocky4Backup sales representative. Characters are automatically converted to upper case when entering lower case.



After pressing the “OK” button Blocky4Backup generates the license request key, which must be sent to the licensing service by using either the on-line WEB-PORTAL or sending the information via email.

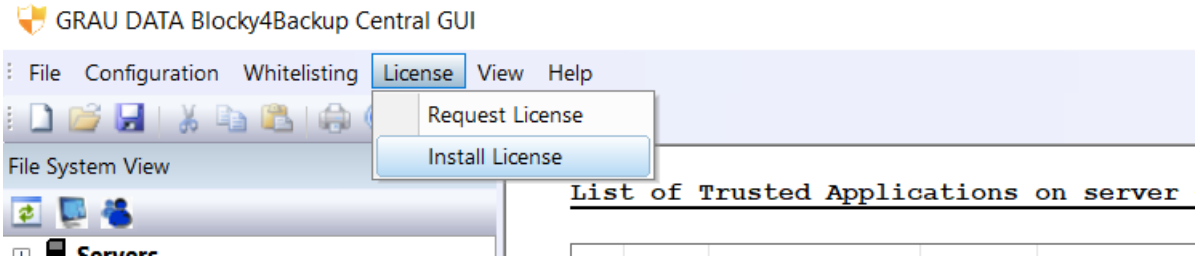


Please ensure that your server is connected to the internet, when choosing the "WEB-PORTAL" for requesting the license key. To access the licensing service you have to log in to the WEB-PORTAL. If you do not yet have log-in credentials, please register and provide a valid email address, which is used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

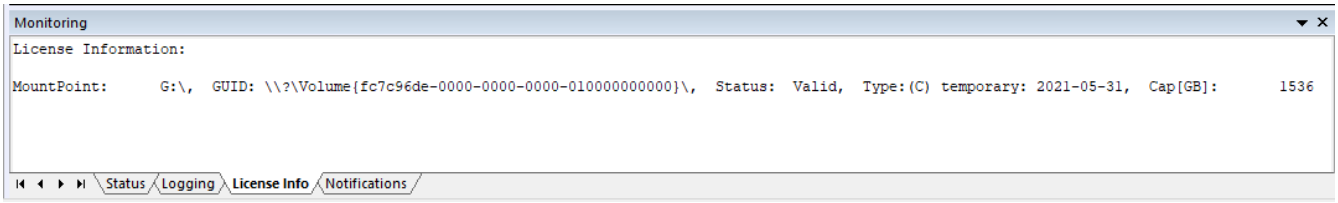
If you decide to send the license key request via email, you may either use the menu item “EMAIL…”, which launches your email client and automatically generates an email with the necessary information or you may copy the license request key to a text file and send it as an email attachment to support@graudata.com.

4.14.2. 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 Blocky GUI. 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.

4.14.3. 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 previousely 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.

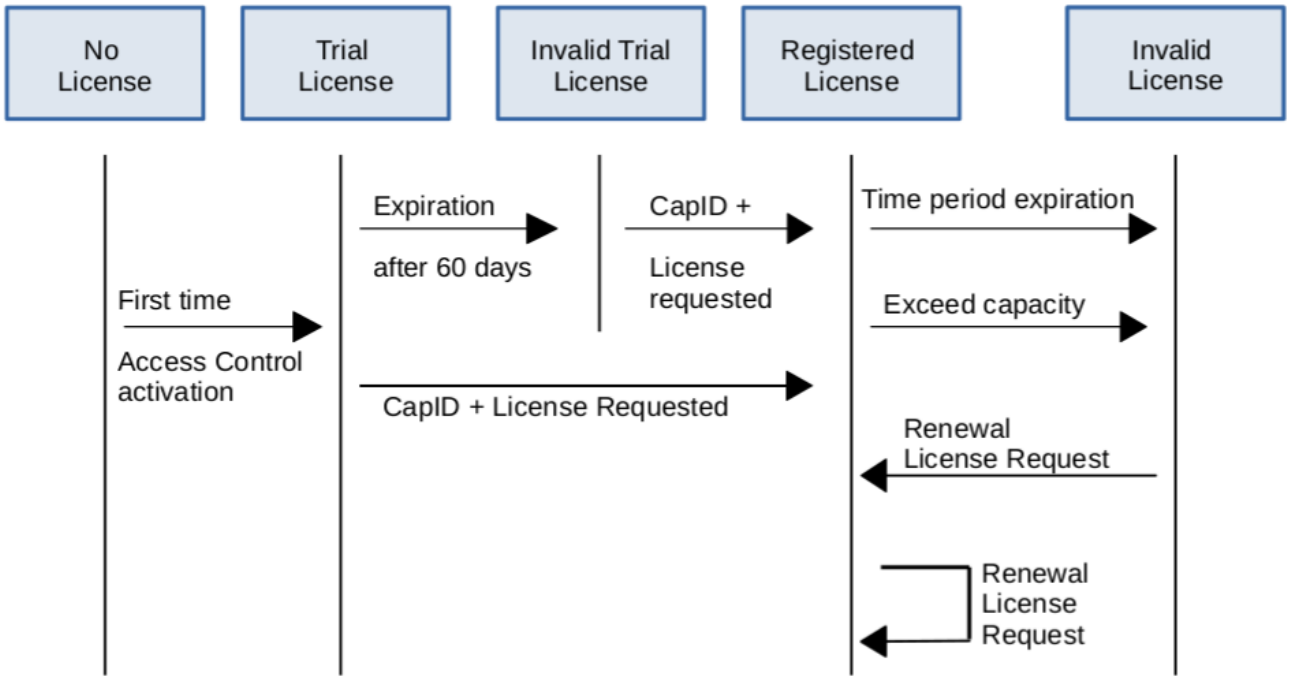
Blocky4Backup monitors the overall physical capacity on each Blocky volume and the license time limit, and displays a warning message in the application event log when a Blocky volume exceeds the licensed capacity or time limit. If either the capacity or time limit is exceeded, the license gets invalid 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 Blocky4Backup 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 Blocky4Backup 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) 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:

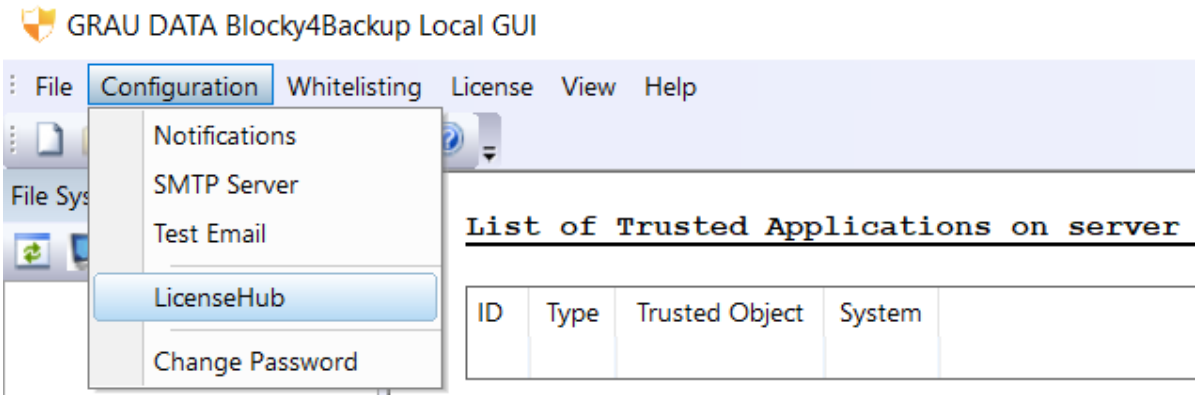
- Each license is volume based.
- The trial license is valid for 60 days after activation.
- The trial license has no capacity limit.
- The registered license has a time and capacity limit (depending on the purchase).
- Capacity is the volume provisioned size not the used space.
- An invalid license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



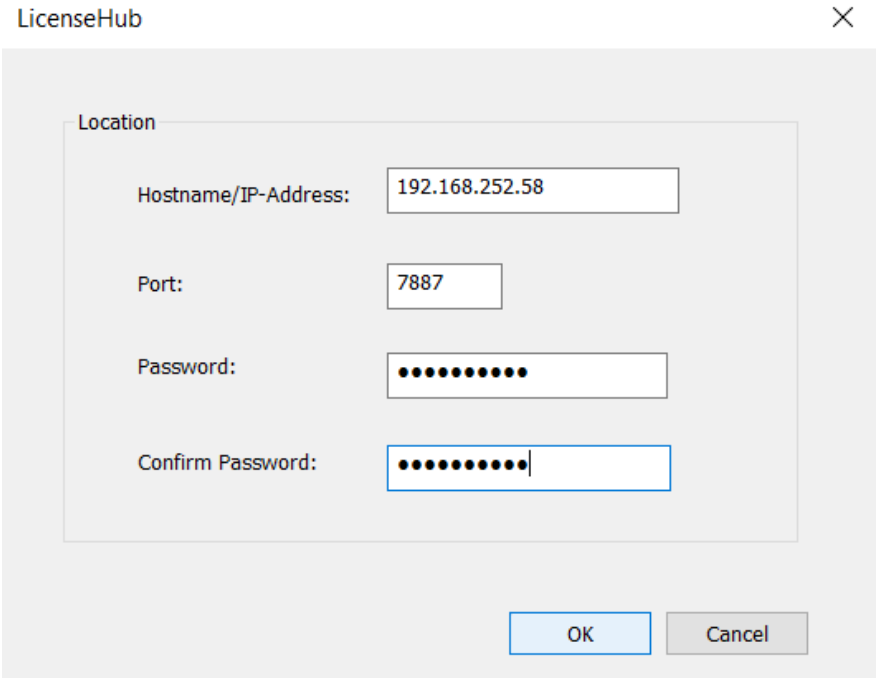
4.14.4. Using LicenseHub

In large environments with serveral Blocky4Backup servers and volumes, licensing is also possible with LicenseHub instead of stand-alone licensing on a per-volume base. Licenses for all Blocky volume are requested from LicenseHub automatically and regularly refreshed.

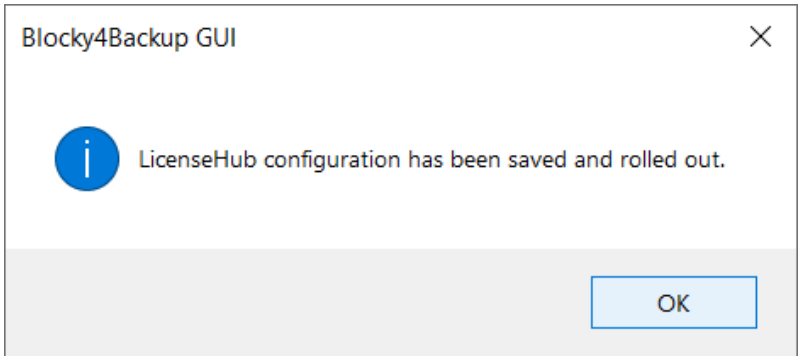
For installation and configuration of LicenseHub, please refer to the LicenseHub admin guide. At least one Blocky4Backup license has to be installed on the license server of LicenseHub for use with Blocky servers.



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



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



Blocky4Backup negotiates now all license requests with the license server of LicenseHub.

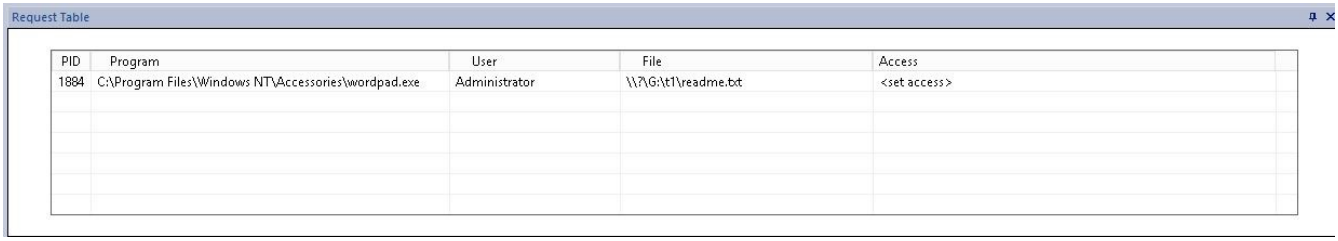
To disable the usage of LicenseHub leave the hostname empty and press "OK".

- Central GUI can only configure the same LicenseHub for all Blocky4Backup servers assigned to it.
- Configured LicenseHub in Central GUI will be immedeately activated on conntected (or later reconnected) servers. Same applies by removing the LicenseHub from Central GUI configuration.
- Volumes managed by Blocky4Backup with configured LicenseHub usage, will get more or less immediately the license lease from LicenseHub. They will not run in an evaluation mode.
- LicenseHub assigned licenses for Blocky volumes will be valid for 30 days, but will be refreshed automatically.
- To enforce evaluation mode for Blocky volumes, the LicenseHub configuration of this Blocky4Backup server must be disabled before activating the volume for the first time. Same applies with Central GUI.
- Unused volumes should be set to unmanaged, e.g. access control switched off permanently, in the Blocky4Backup configuration. By this 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).

5. Monitoring

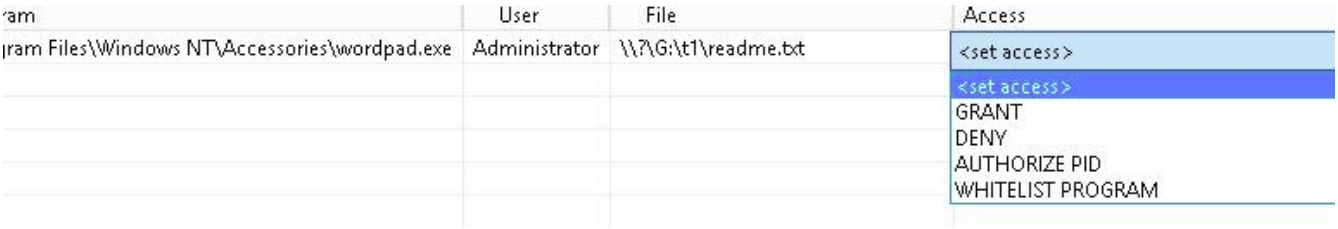
5.1. Request Table

If the GUI is running and a non-whitelisted program attempts a file modification, the request will be displayed in the request table and a 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.



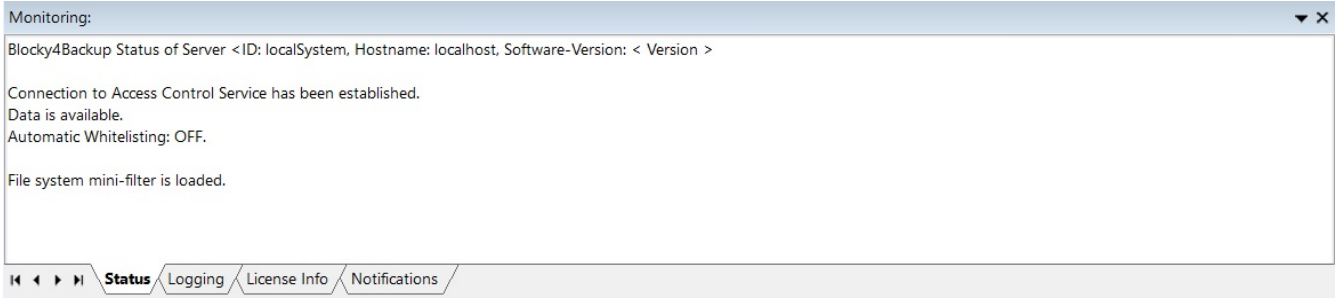
The following options are available:

- 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.



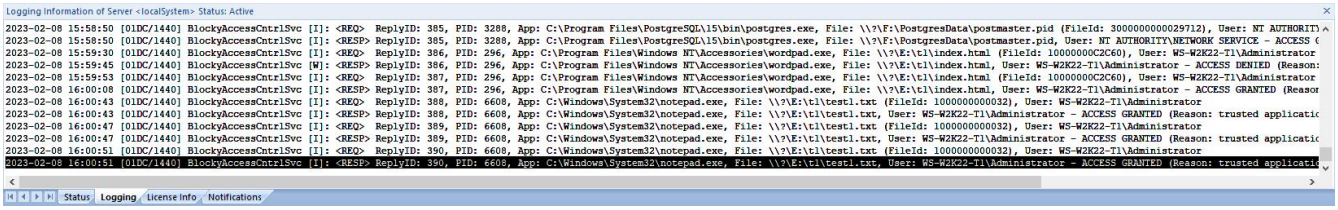
5.2. Status Informationen

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



5.3. Access Log

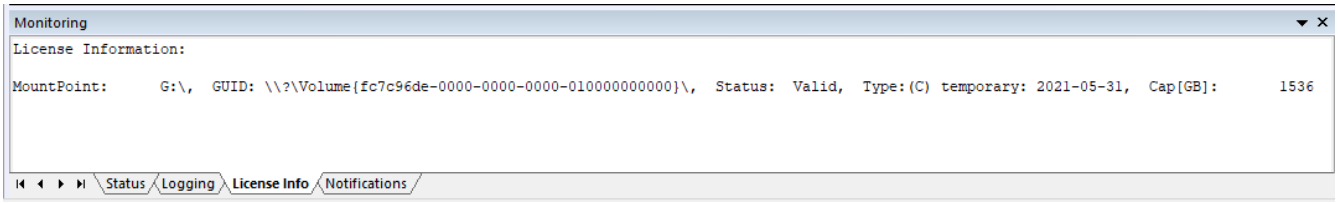
Blocky4Backup writes all modification requests on protected files and responses to the log file `C:\ProgramData\GrauData\Blocky\AccessControl.log`. The content of the log file is also displayed in the “Monitoring” window in the tab “Logging”.



Beginning with Blocky4Backup 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.

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.

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 handeled by Blocky and will be denied as these components are usually not whitelisted. This results in unauthorizes 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.

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

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\Blocky4Backup_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.

6.2. Missing privileges

The Blocky GUI 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 Blocky GUI.

6.3. System clock tampering

Blocky4Backup 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.

Appx A: Setup command line parameters

The Blocky4Backup 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 unistallation program `unins000.exe` in the Blocky4Backup installation path.

Administrative rights are required to install, update or uninstall Blocky4Backup.

As Blocky4Backup setup is based on Inno Setup, please check for the general command line parameter description on their website.

Setup command line

Syntax:

```
Blocky4BackupSetup_2_7_0_56.exe [optional parameters]

unins000.exe [optional parameters]
```

Optional parameters:

/COMPONENTS="core,gui"

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

/Secret=<self-defined-password>

- On new installation: This sets the inital 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.

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

Example:

Installation/Uninstallation

```
Blocky4BackupSetup_2_7_0_56.exe /silent /COMPONENTS="core" /secret=MyPassword2020

Blocky4BackupSetup_2_7_0_56.exe /silent /secret=MyPassword2020

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

Appx B: BlockyCLI parameters

BlockyCli.exe is a command-line utility for Blocky4Backup to manage the access control, licenses and password. It is located in the Blocky4Backup 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.

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 in path active.
show_contolledfolders	**ALL**	Display all controlled folders.
add_whitelist	**<program>**	Add program to whitelist.
del_whitelist	**<program>**	Remove program from whitelist.
update_whitelist	**<program>**	Update program in whitelist.
show_whitelist		Show whitelisted objects.
diagnostics		generate diagnostics report.
dump		Dumps program whitelist and access table.

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

Whitelist

.\BlockyCli.exe password20 **add_whitelist** C:\Windows\System32\notepad.exe
rc:0

.\BlockyCli.exe password20 **show_whitelist**
WhiteListed Applications:
C:\Windows\System32\notepad.exe
rc:0

.\BlockyCli.exe password20 **del_whitelist** C:\Windows\System32\notepad.exe
rc:0

.\BlockyCli.exe password20 **update_whitelist** C:\Windows\System32\notepad.exe
,+rc:0

Diagnostics

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

This creates the service report file `C:\ProgramData\GrauData\Blocky\Blocky4Backup_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

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, do not attempt to request or install licenses manually. Manually installed licenses will be discarded and replaced automatically. To set LicenseHub configuration see 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 resulting license request by using Web-Portal or e-mail. See 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 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 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

Initial password and password reset

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

Examples:

Set password

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

Request password

.\BlockyCli.exe **request_password_reset**

Send the following token to support@graudata.com in order receive a password reset key:

H9KC-CS2K-KSJR-L87T-N6ES-OX3T-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-L8OT-XKLS-OX3T-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-IO0P
rc:0

Appx C: Blocky4Backup Change Log

This appendix summarizes the changes between Blocky4Backup versions. The change log only contains relevant changes and fixes.

C.1. 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) Notifcation 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.2. 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 interupted upgrades
- (Bugfix) Fix fingerprint calculation for debug binaries

C.3. 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.4. 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.5. 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.6. 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.7. 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.8. 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.9. 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 Blocky4Backup.

OpenSSL

Copyright © 1998-2019 The OpenSSL Project, OpenSSL License
Copyright © 1995-1998 Eric Young (eay@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

Index