LabLock Product Manual

1. Product Manual

LabLock
Version 1.1.0
JAKO-Solutions, Inc.
support@jako-solutions.com
sales@jako-solutions.com
info@jako-solutions.com
https://jako-solutions.com/

2. Scope

LabLock 1.0.0 is a 32-bit application but is also 64-bit aware. LabLock 1.0.0 has been tested in Windows 10 Professional. If you are using Windows 10 in a mission-critical setting, please consider using the Windows 10 Enterprise LTSB Edition. LabLock 1.0.0 is not in the Windows Store and therefore will not run in Windows 10 S.

3. Requirements

The requirements below list the minimal configuration. Any better hardware or newer software may be used. If you experience problems, nonetheless, please do not hesitate to contact us.

Software

- Windows 10
- .NET 4.7 or higher

Architecture

- 32-bit
- 64-bit

Hardware

- 1 gigahertz (GHz) or faster processor
- At least 2 gigabytes (GB) for 32-bit or 4 GB for 64-bit
- 1GB available disk space

Web Browser

- Firefox
- Chrome
- Microsoft Edge
- Internet Explorer 11

4. Installation

Open installation folder, right click on **"LabLockInstall.exe"** file from the installation folder and click on "**Run as administrator"** to start the installation
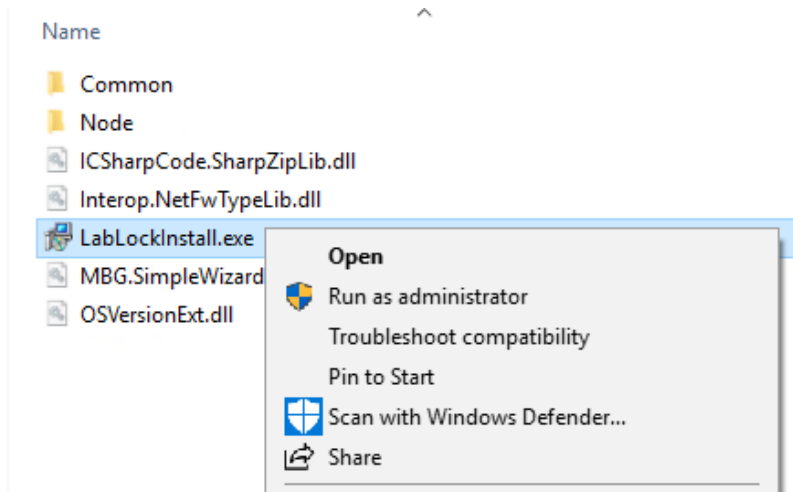
This will open the installation wizard. Click **"Start"** to begin the installation.
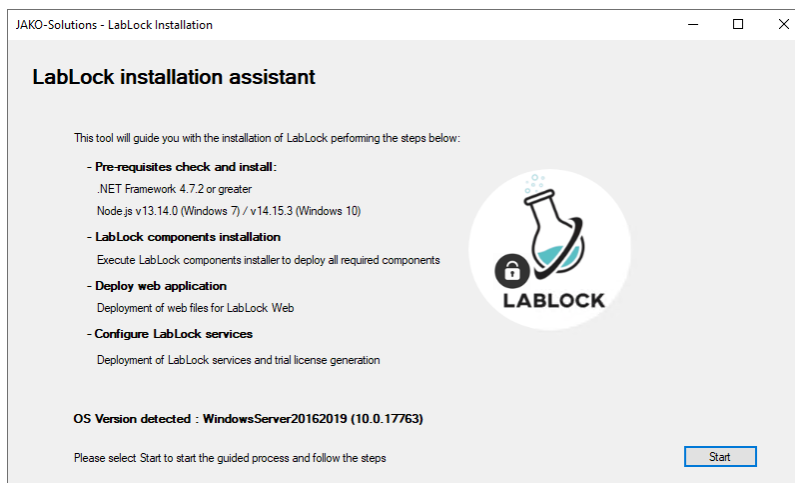
Read the EULA (End User License Agreement), click the checkbox to accept the license terms, and click on **"Next"**
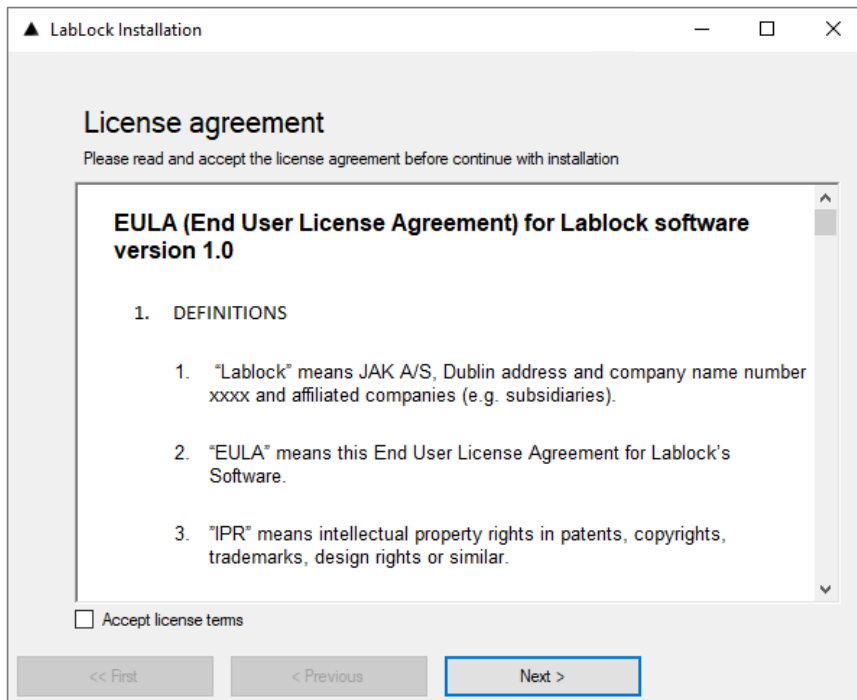
Click on **"Install .NET 4.7.2"** to install .NET on the PC.

Click **"Next"** to continue with the installation.
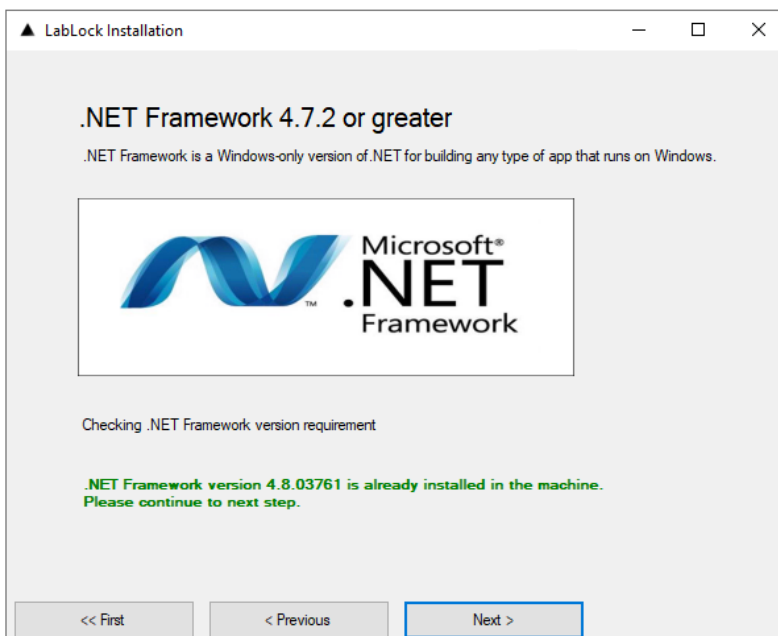
Click on **"NodeJS"** to install NodeJS on the PC.
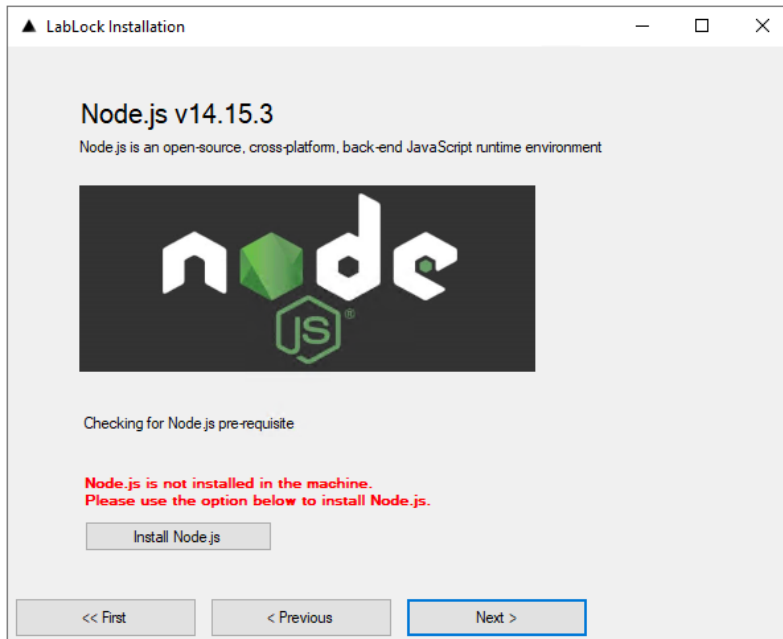
Once the installation is completed a pop up will be displayed. Click **"ok"** to confirm NodeJS is installed.

Click **"Next"** to continue with the installation.
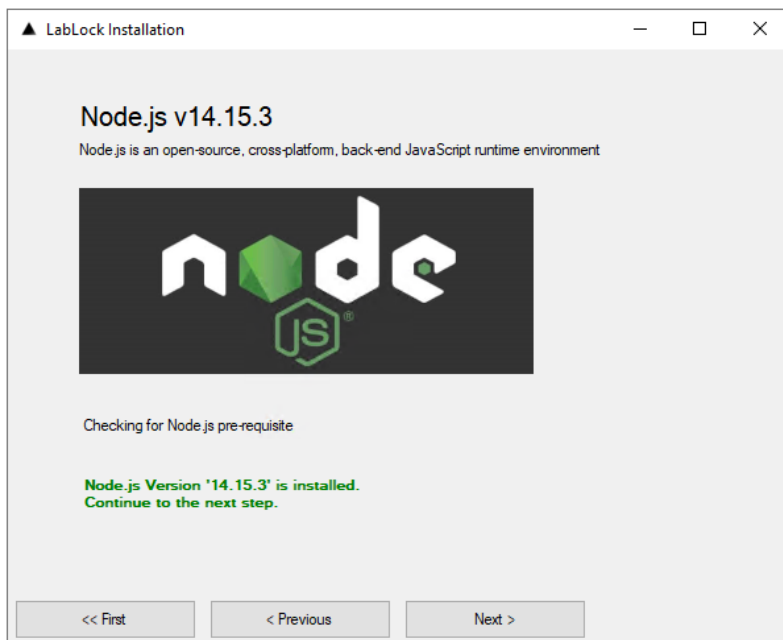
Click **"Install LabLock components"** to start the installation process of LabLock Service.
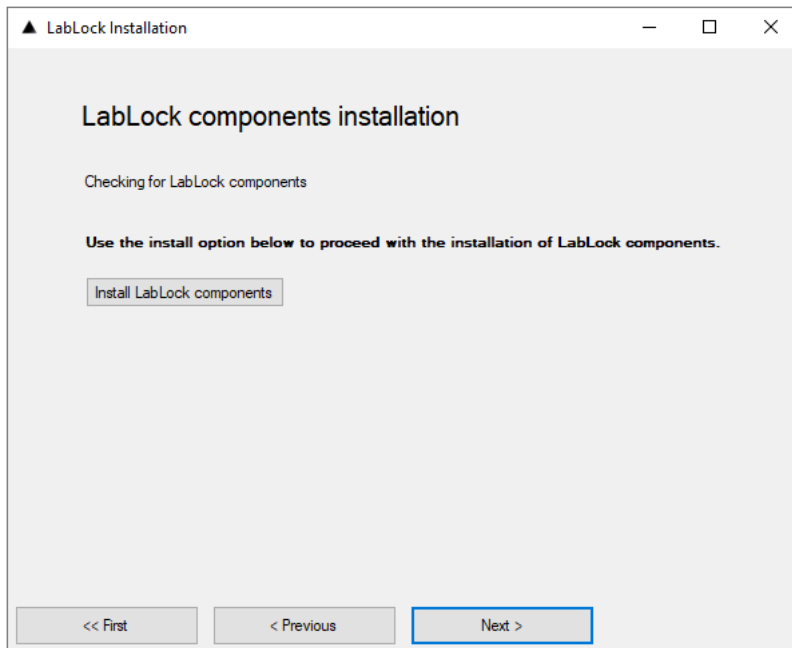
Click **"Next"** to continue the installation of LabLock Service.
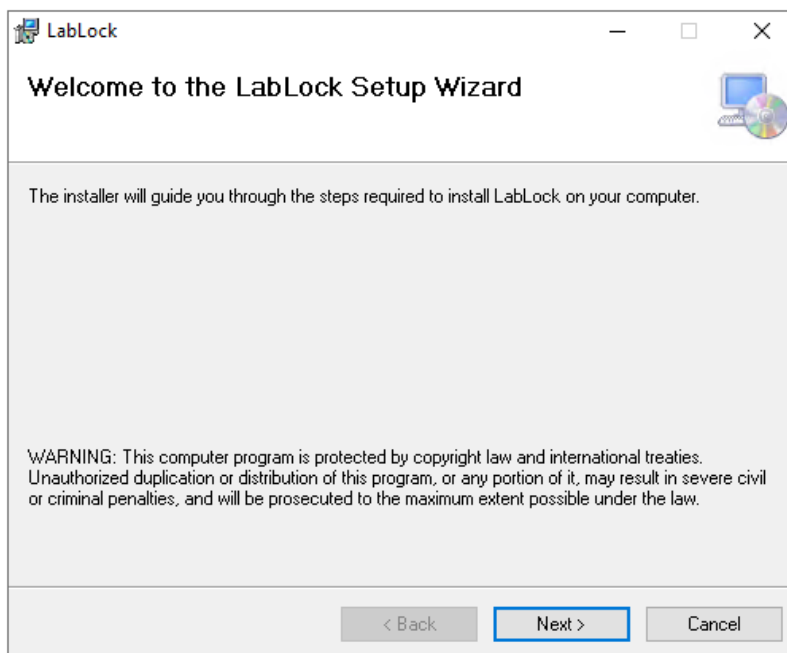
Select LabLock service port and click **"Next".**

Note: By default, LabLock uses the port 8081 for the service API traffic.
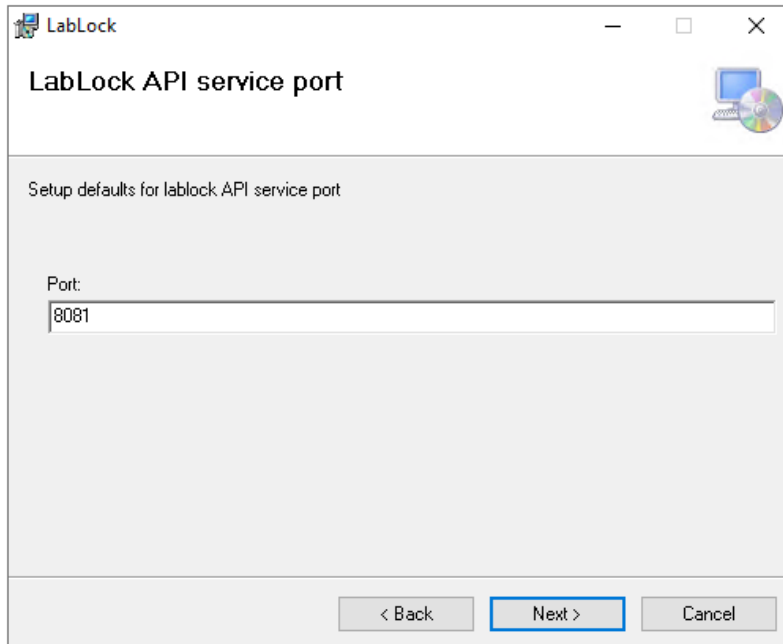
Select LabLock web portal port and click **"Next".**

Note: By default, LabLock uses the port 3000 for the Web traffic.
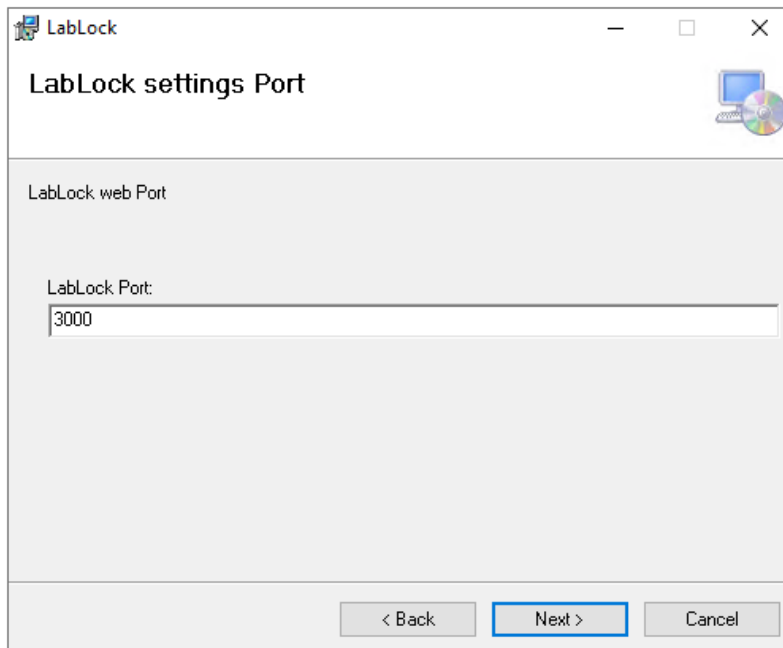
Select LabLock installation folder and click **"Next".**

Note: By default, LabLock folder is located on "C:\Program Files\JAKO-Solutions\LabLock\"
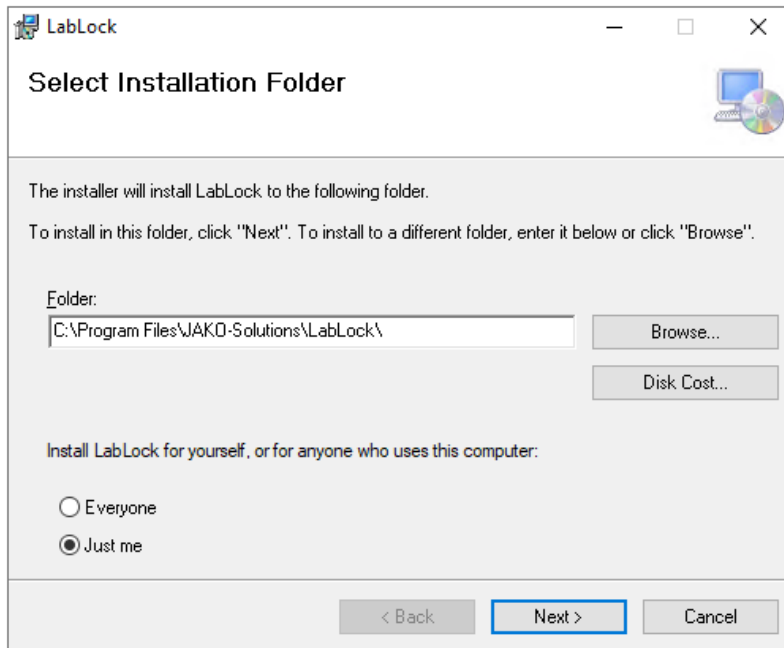
Click **"Next**" in "Confirm Installation" windows to start LabLock Service installation.
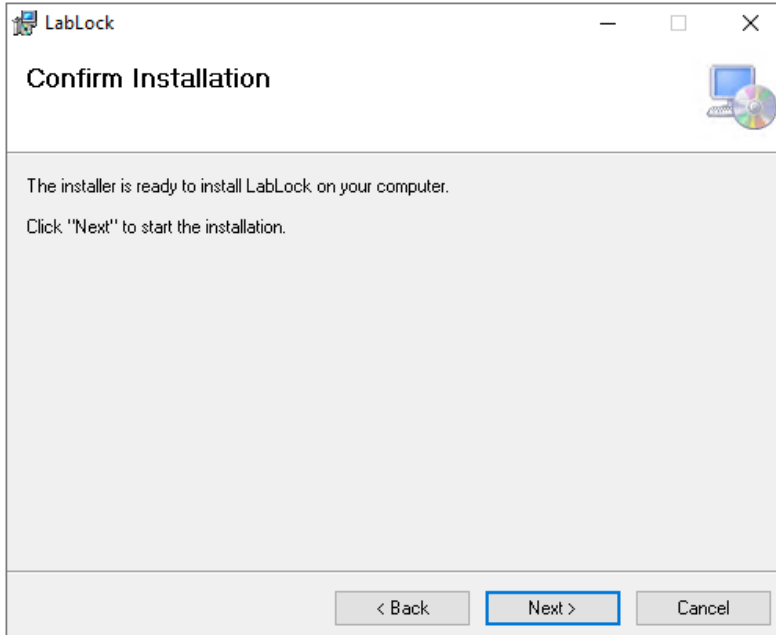
Once LabLock service is installed click **"Close"** to return to LabLock wizard.
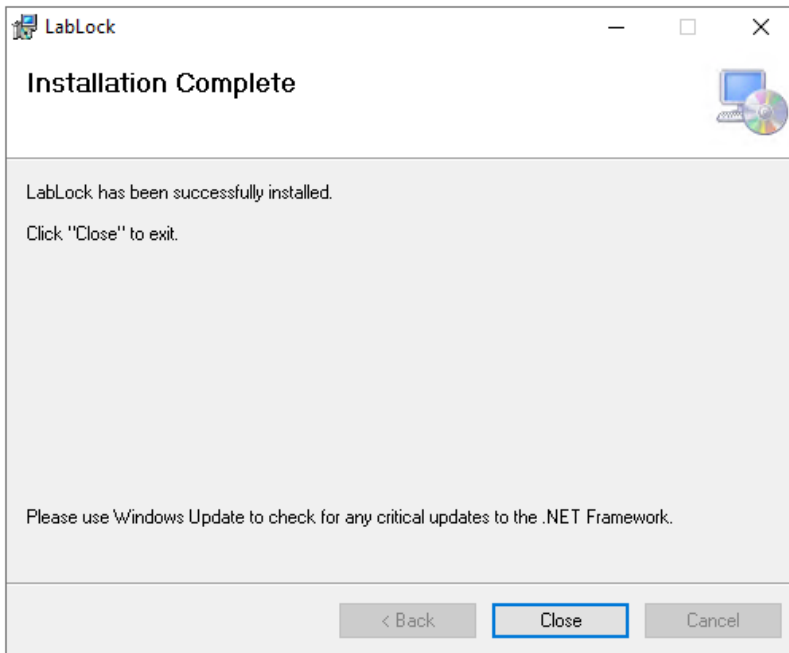
Click on **"Validate"** to validate LabLock service installation.
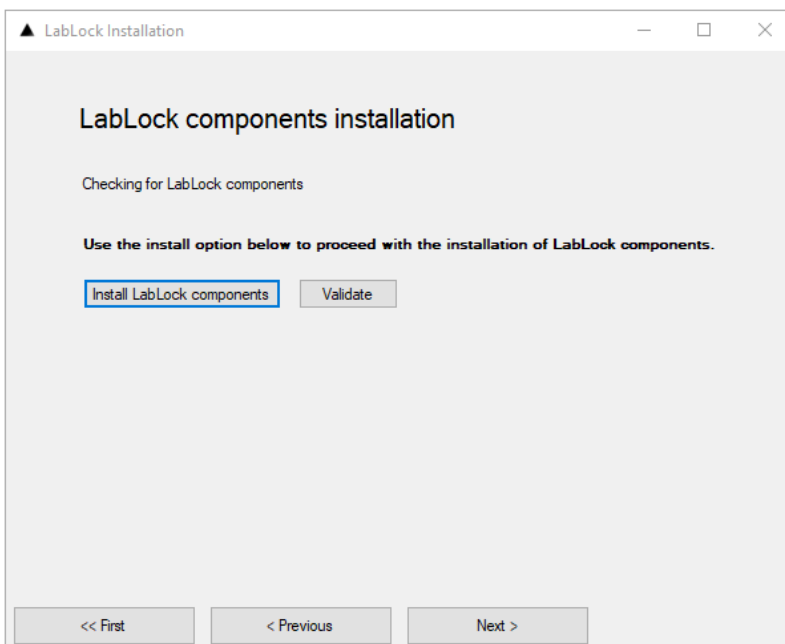
After clicking **"Validate"**, if the installation was successful the following message will appear: **"LabLock version 1.1.0 already installed in the machine".**

Click **"Next"** to move to the next window.
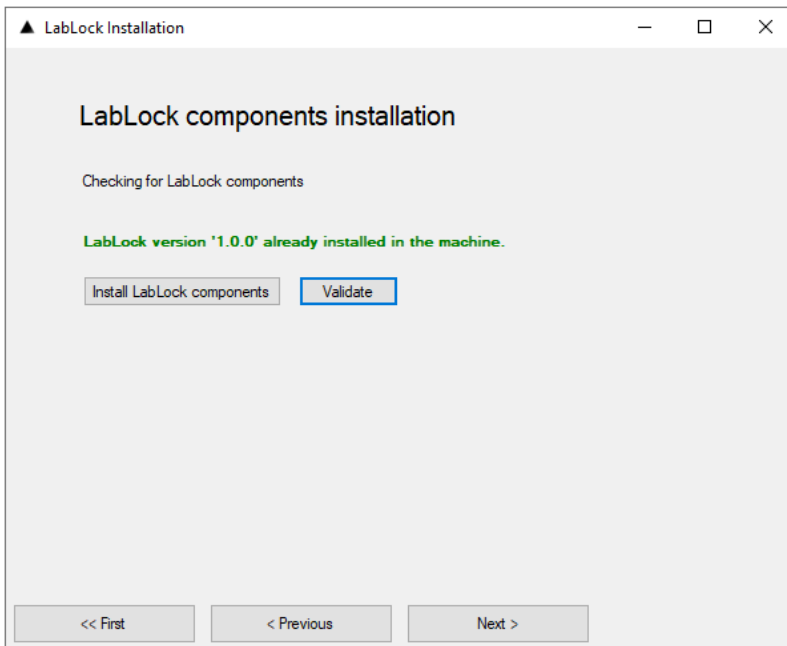
Click **"Deploy"** to bring the LabLock web interface into effect.
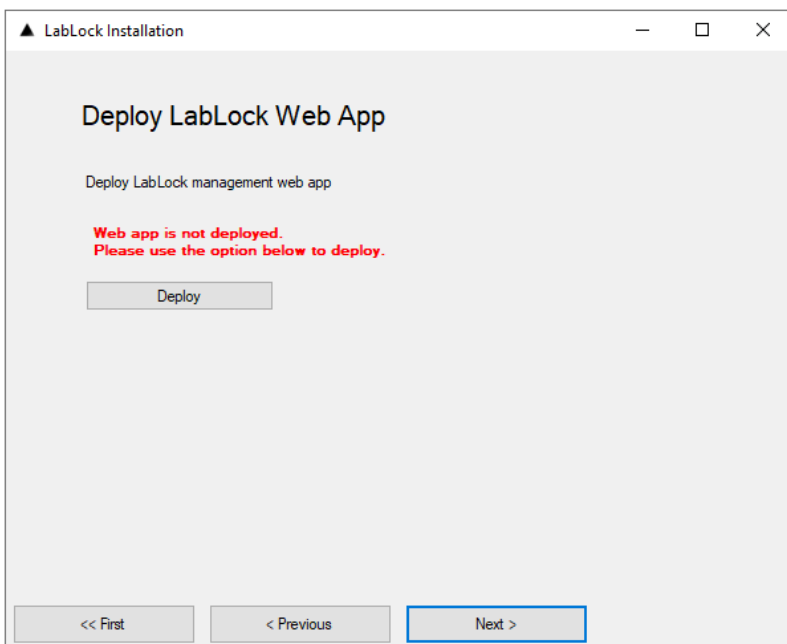
Once the Web interface is installed, it will show a message in green.

Click **"Next"** to continue.
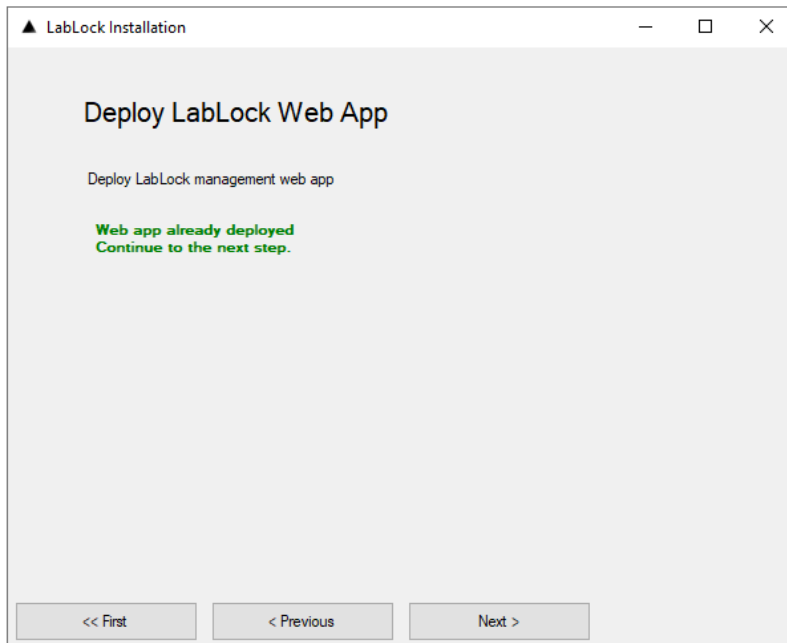
Click on **"Reboot"** to restart the PC or Finish to go back to Windows.

Note: The computer will need to be restarted to begin using LabLock.
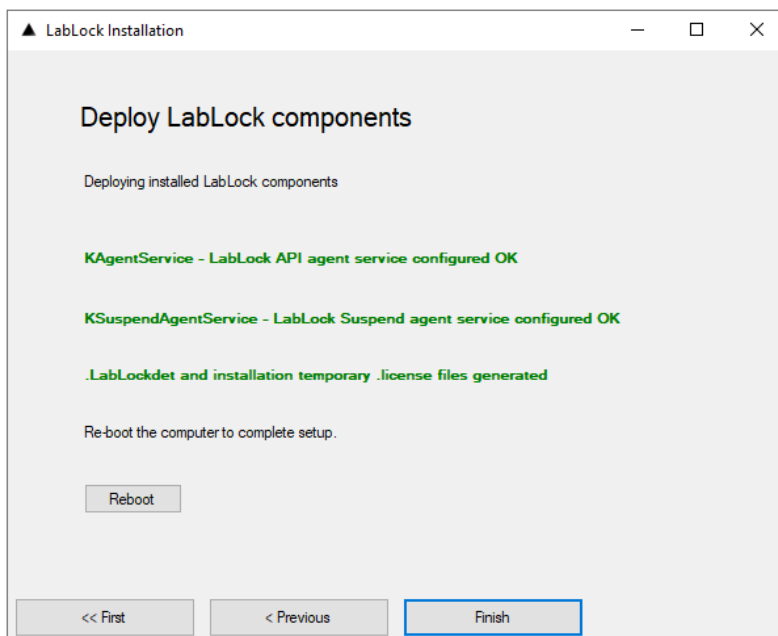
5. Getting Started

After the LabLock installation is complete, restart the PC to start using the product. LabLock portal can be accessed remotely or locally from different web browsers.

Open one of the supported web browsers (Edge, Chrome, Mozilla) and type in the following URLs:

For local access: http://localhost:port or http://127.0.0.1:port

For remote access: introduce computer name or IP followed by the port. Example: http://computername:port or http://ip:port Where the port is the port number configured during the installation. By default, LabLock uses port "3000"

The login page to introduce your username and password will appear.

If Active Directory is used, it is recommended to use "UserPrincipalName" for the user, however, SamAccountName can be used and accepted depending on your AD user configuration.

Once the credentials are accepted, you will be redirected to the LabLock landing page.

LabLock Top menu contains the main 5 sections of LabLock: Dashboard, Restrictions, Settings, Import/Export, and Activity.
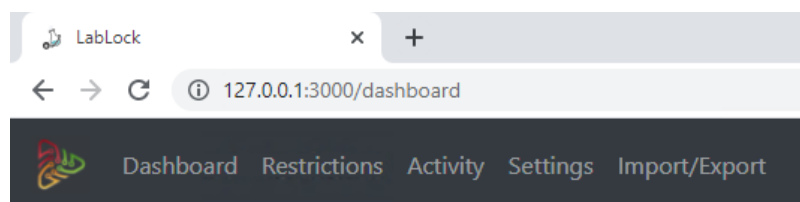
On the right side of the menu, there is a dropdown menu with the information of the user logged into the LabLock interface. The dropdown menu shows the full name of the logged in user. Click on the user's full name to open menu.
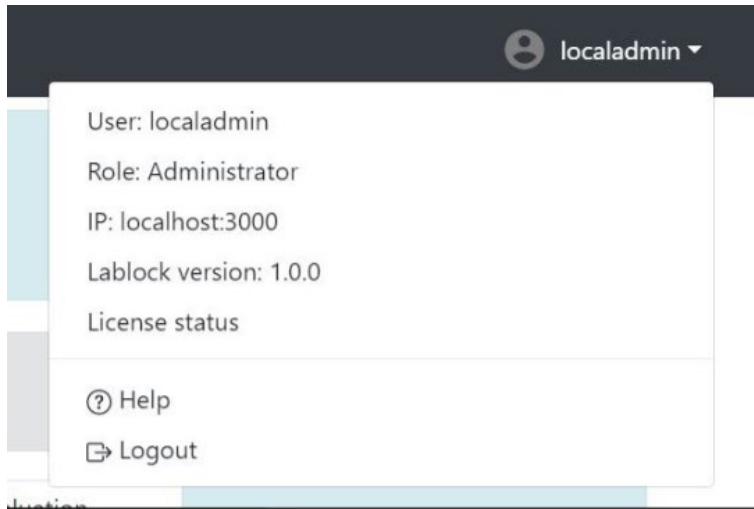
The menu contains the following information:

User: This is the local user for local authentication or the SAMaccountname for AD authentication of the logged user to the LabLock portal.

Role: This is the role that the user is part of.

IP: This is the IP from the computer that is logging into the LabLock portal.

LabLock Version: This is the version of LabLock installed on the PC.

License Status: This is a link to a Windows where the license status is displayed.

Help: This is a link to the documentation located on the LabLock website.

Logout: This is a button to log the user from the LabLock portal.

License Status Window gives an overview of the status of license where the following information can be found:

License: Maybe "Permanent" or "Temporary".

License ID: This is the ID of the license file.

Computer: This is the name of the computer where the license file is activated.

Customer name: The name of the company assigned by JAKO-Solutions when the license is generated.

Customer ID: This is the JAKO-Solutions customer ID.

6. Dashboard

The top version of the dashboard contains 3 parts: Desktop details, Restrictions Dashboard, and user details:

Desktop details: This section displays computer details. It will provide the computer name, operation system, and time when the PC was turned on.

There are 3 buttons where the PC can be logged off, restarted, and shut down.

Restrictions: This section details the restriction's status. In this section, you can suspend the LabLock restrictions temporarily by clicking suspend. Restrictions will be activated automatically if the suspension count down reaches 0. Restrictions can be activated by clicking the suspend button again.

Suspend button is disabled if no restrictions are set in the Restrictions section.

User Details: This section contains the user's details. If a user is logged on to the PC, it will show what users are logged in and when they logged into the PC.

You can screenshot the desktop by clicking on the "**camera**" icon.

You can also send a 100-character message to the PC where LabLock is installed by clicking on the "**message**" icon.

Note: Users that are part of the interactive group will not have screenshots and message icons. Those users aren't fully logged into Windows OS, they're just running a process or service. Therefore, message and screenshot options are disabled.

When Core restrictions are applied, it will activate a Core restriction summary. The graphics will give you overall information about the applied restrictions and total restrictions.

Core Restrictions Summary

Restriction	Description	Area
Disable Bin on Desktop	This option disable Bin from Desktop	Desktop
Hide Action Center on Taskbar	Hide Action Center from the taskbar on Windows 10	Taskbar
Add Folder default path to File Explorer	Add a default path to winodws file explorer, only this folder and subfolders ...	FileExplorer
Hide OneDrive on File Explorer	Hides OneDrive folder on File Explorer and open/save dialog boxes	FileExplorer
Hide switch user option on PC	Hide switch user option from start menu and lock screen	System

|< < Page 1 of 1 > >| Results per page 10 ▼ Showing 1 - 5 of 5

When System Keys restrictions are applied, it will activate a Core restriction summary. The graphics will give you an overview of applied restrictions and total restrictions.

System Keys Restrictions Summary

Total VS Applied
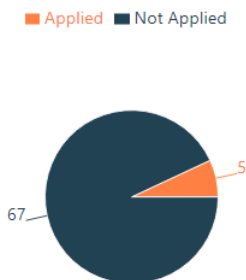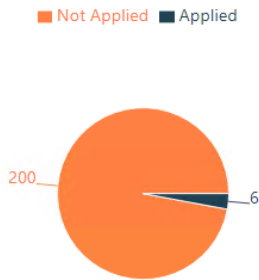
Applied by section
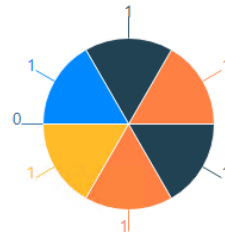
Total VS Applied by Section

Not Applied Applied
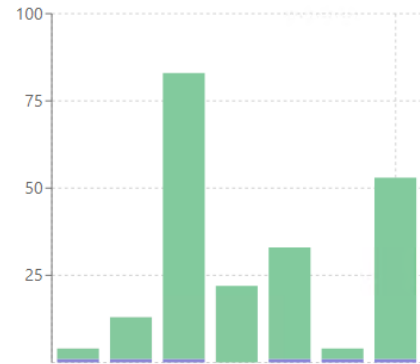
Restriction	Description	Area
Middle Button	Restrict Mouse Middle Button	Disable Mouse...
F5	Disable Refresh the instance of File Explorer and Refresh File Explorer's curr...	Disable functio...
NumPad3	Disable NumPad 3 key	Disable Keybo...
Ctrl+A	Disable Select all content.	Disable Contro...
Shift+F10	Disable Open context menu for selected item.	Disable Shift k...
Win+B	Disbale Set focus notification area in the taskbar.	Disable Windo...

|< < Page 1 of 1 > >| | Results per page 10 ▼ | Showing 1 - 6 of 6

7. Restrictions Menu

Restrictions are divided into 5 different sections: Core, System Keys, Apps, Startup, and Firewall.

7.1 Core

Core tab is a section where you can configure restrictions based on Desktop, Taskbar, FileExplorer and System.

7.1.1 Desktop

In this section, you can find restrictions related to Desktop.
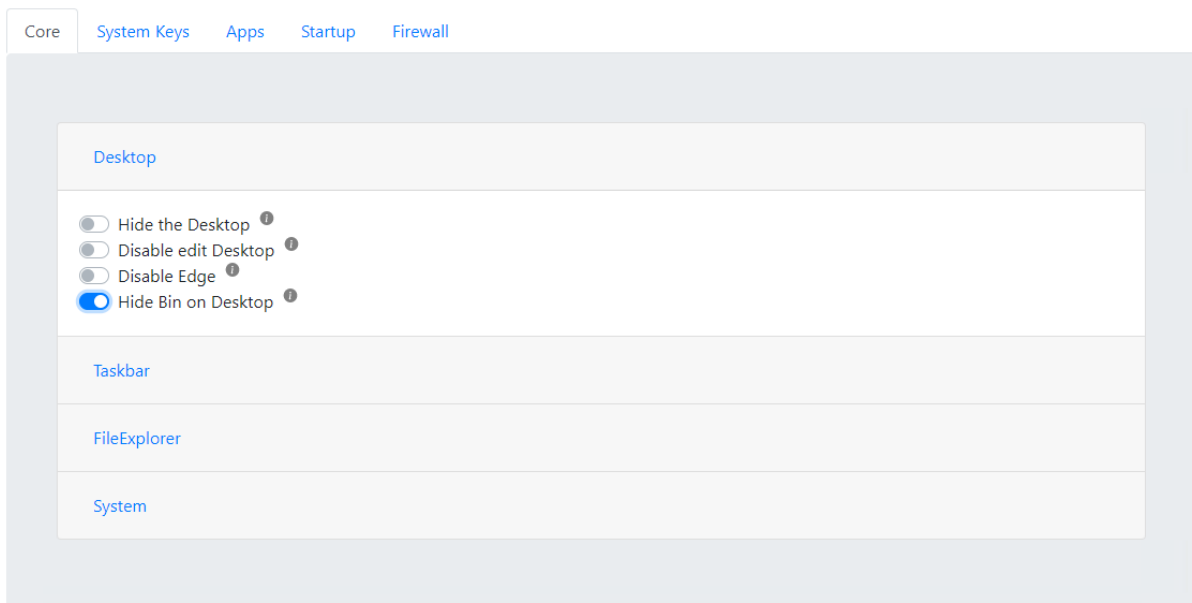
Hide the Desktop	Hides all desktop icons and disables desktop context menus
Disable edit Desktop	Protects desktop icons and desktop files/folders from tampering: they can be executed, but cannot be edited or deleted
Disable Edge	Disables the ability to swipe using touch from the edges of the screen
Hide Bin on Desktop	Hides the Bin from the Desktop

Table 1 : Desktop restrictions

7.1.2 **Taskbar**

In this section, you can find restrictions related to the Taskbar.
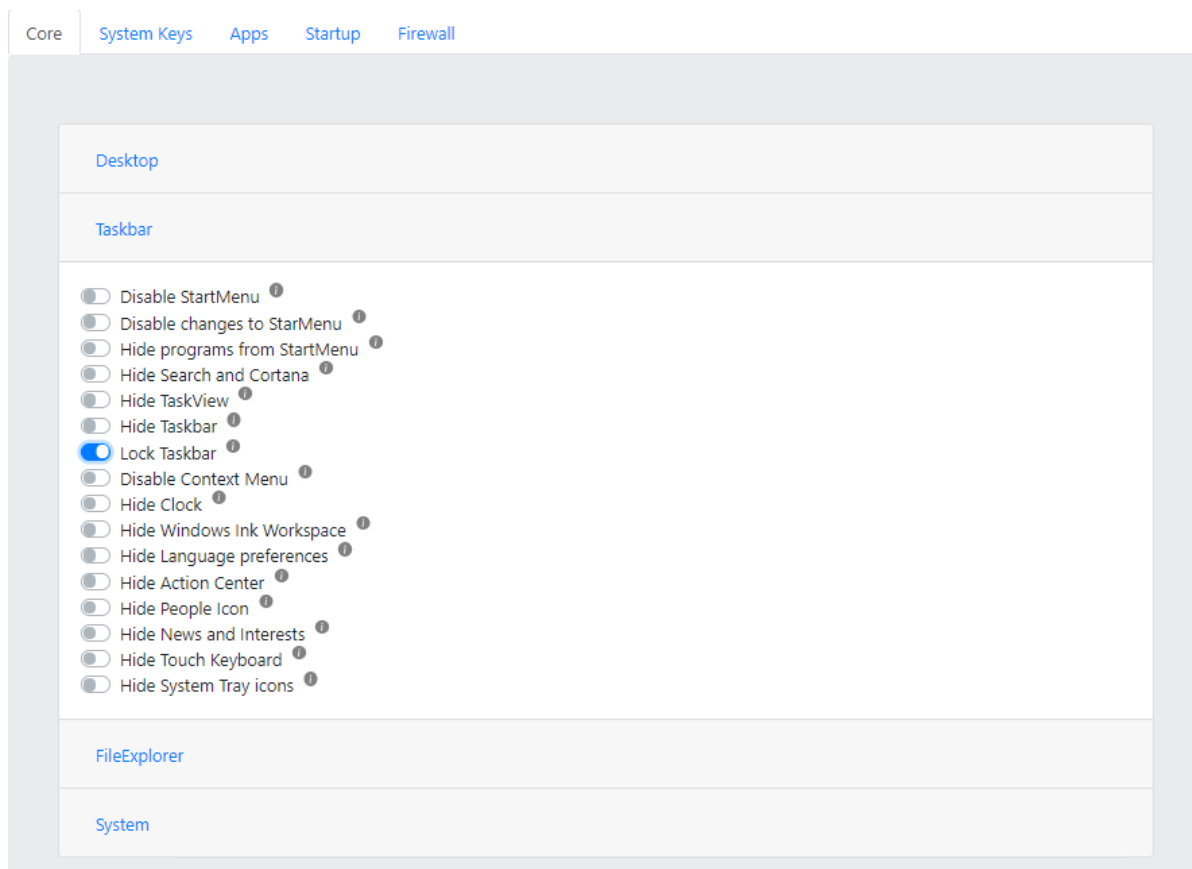
Disable StartMenu	Disables the StartMenu button
Disable changes to StartMenu	Blocks the users' ability to change StartMenu
Hide programs from StartMenu	Hides the programs list in the Start Menu
Hide Search and Cortana	Disables the ability to search and run local files from the Start Menu and Taskbar
Hide TaskView	Disables the TaskView functionality
Hide Taskbar	Hides the Taskbar completely
Lock Taskbar	Disables the ability to resize and move the Taskbar
Disable the right-click Menu	Disables the right-click settings menu in the Taskbar
Hide Clock	Hides the system Clock located on the right-side area of the Taskbar.

Hide Windows Ink Workspace	Hides the Ink Workspace icon from the right-side area of the Taskbar.
Hide Language preferences	Hides Language preference icon from the right side of the Taskbar.
Hide Action Centre	Hides the Action Centre from the right side of the Taskbar.
Hide People Icon	Hides the People icon from the right side of the Taskbar.
Hide News and Interests	Hides News and Interest icon from the Taskbar.
Hide Touch Keyboard	Hides the Touch keyboard icon from the Taskbar.
Hide System Tray icons	Hides the System Tray icons located on the right-side area of the Taskbar.

Table 2: Taskbar restrictions

7.1.3 **File explorer**

In this section, you can find restrictions related to the File Explorer.
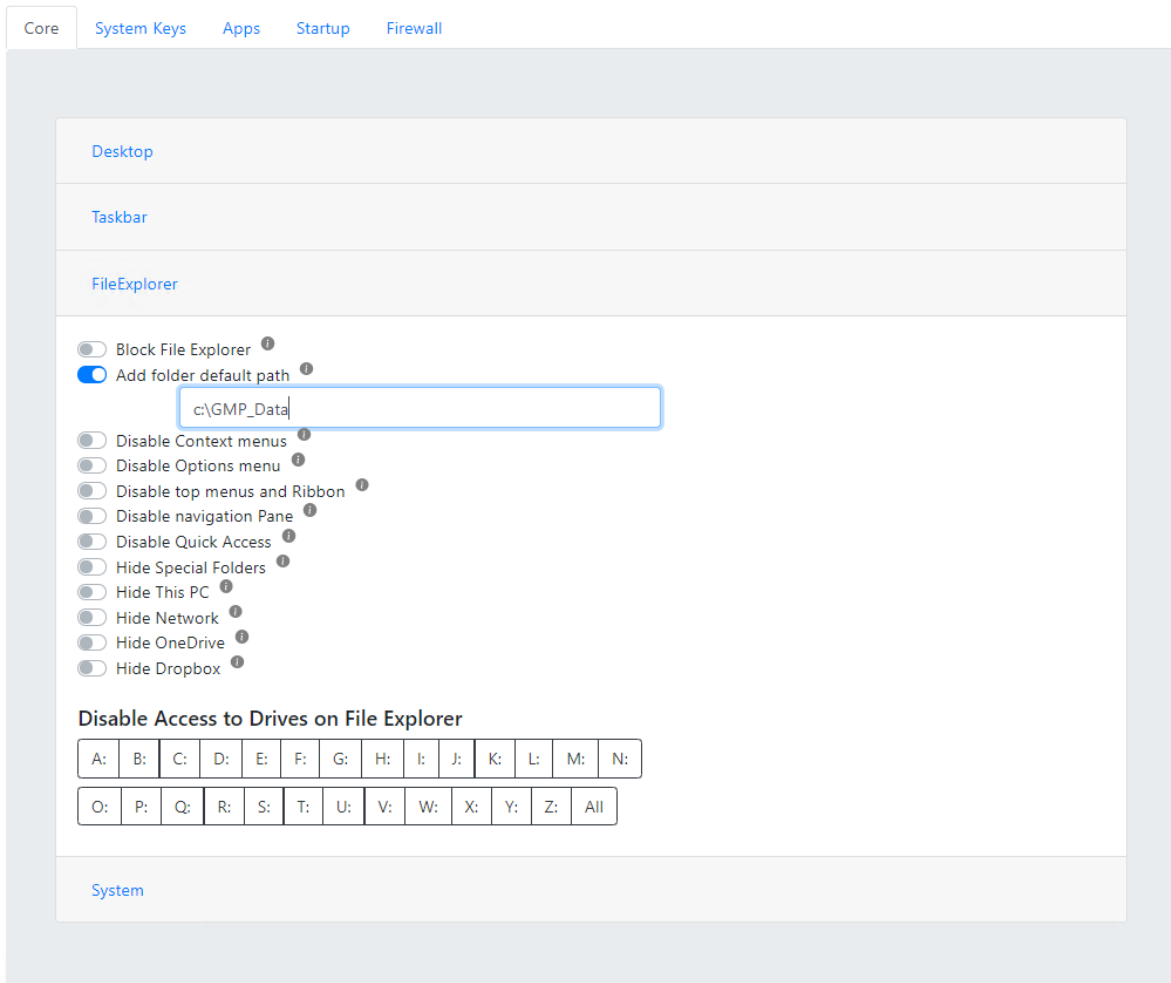
Block File Explorer	Blocks access to File Explorer. When selected, any File explorer window open will be automatically closed.
Add Folder default path	The File Explorer and the "Open" and "Save As" dialog boxes are redirected to the selected folder path. Other parts of these components are also disabled such as the navigation bar and buttons. The navigation menus will also be disabled for the dialog boxes.
Disable Context menus	Disables context menus on the File Explorer.
Disable Options menu	Disables access to the Folder Options menu on the File Explorer.
Disable top menus and ribbon	Disables top menus, ribbon, and bars in the File Explorer and the "Open" and "Save As" dialog boxes.
Disable navigation Pane	Disables the navigation pane (left column of file explorer).
Disable Quick Access	Disables the Quick Access from the navigation pane on File Explorer and in the "Open" and "Save As" dialog boxes.
Hide Special Folders	Removes special folders (3D Objects, Desktop, Documents, Downloads, Music, Pictures, and Videos) from This PC on File Explorer and "Open" and "Save As" dialog boxes.
Hide this PC	Hide the "This PC" folder in File Explorer and the "Open" and "Save As" dialog boxes.
Hide Network	Hides the "Network folder in File Explorer and the "Open" and "Save As" dialog boxes.
Hide OneDrive	Hides the OneDrive folder in File Explorer and the "Open" and "Save As" dialog boxes.
Hide Dropbox	Hides the Dropbox folder in File Explorer and the "Open" and "Save As" dialog boxes.
Disable access to Drives	Disables access to selected drives in File Explorer and the "Open" and "Save As" dialog boxes.

Table 3: File Explorer restrictions

7.1.4 **System**

In this section you can find restrictions related to the System.
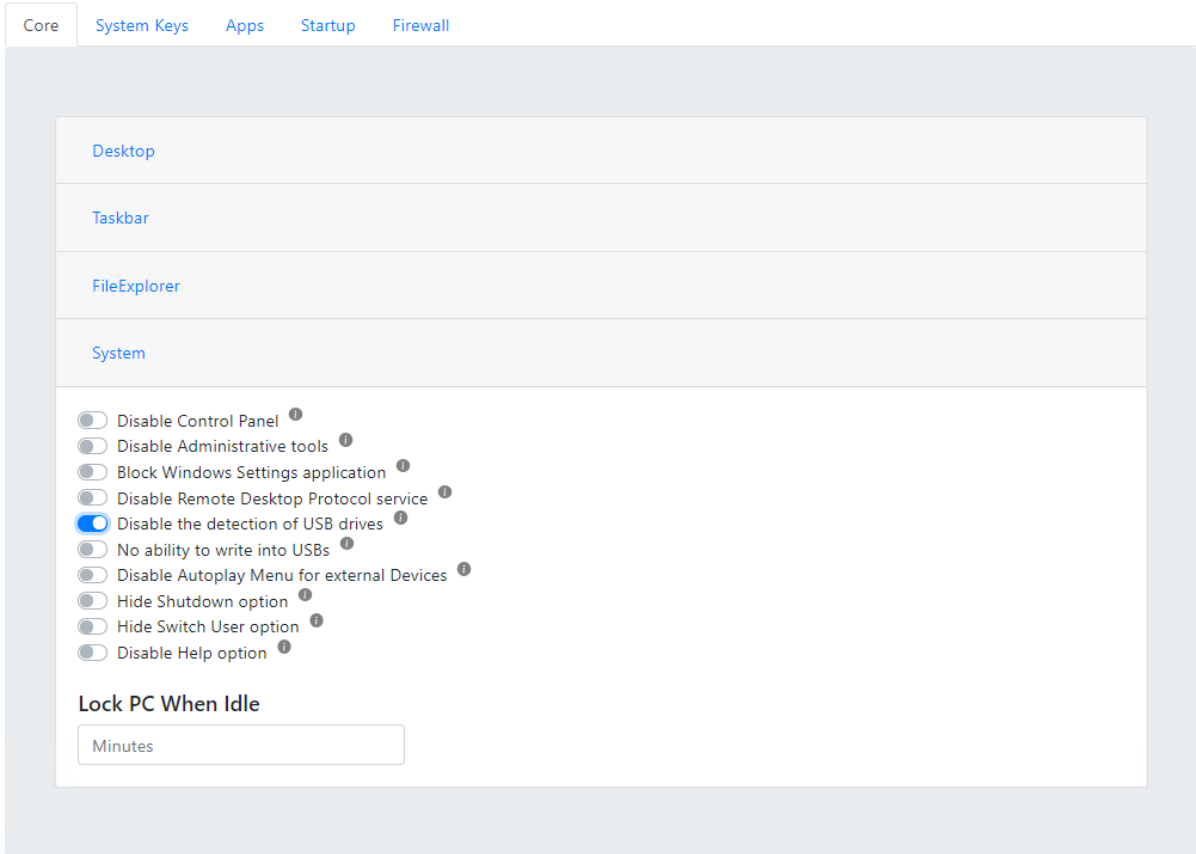
Disable Control Panel	Disables the Control Panel and the options displayed within the control panel section.
Disable Administrative tools	Blocks access to common administrative tools, including Windows Task Manager, Regedit, Cygwin, Process Explorer, and Microsoft Management Console.
Block Windows Settings application	Blocks Windows Settings application.
Disable Remote Desktop Protocol service	Disables the Remote Desktop Protocol service from the PC.
Disable the detection of USB drives	Disable the detection of USB drives.
No ability to write into USBs	Disables the ability to write to USB drives.

Disable Autoplay Menu for external Devices	Disables the Autoplay menu that is displayed when a new external drive is detected (DVD, USB, External hard drive...)
Hide Shutdown option on PC	Hides the shutdown option from the Start menu and the Lock screen.
Hide switch user option on PC	Hides the switch user option from the Start menu and the Lock screen.
Disable Help option	This option disables the help.
Lock PC when idle	The PC is automatically locked when there is no activity (value is in minutes).

Table 4: System restrictions

Click **"Undo"** to remove restrictions that were selected but not applied along with different restrictions tabs.

Click **"Clear all"** to remove all applied restrictions from the LabLock.

7.2 System Keys

The system keys tab allows you to block keyboard keys, keys combinations, and Mouse buttons. It is divided into subsections to represent different groups of keys:

7.2.1 Disable mouse buttons

Left Button	Disable the left mouse button.
Middle Button	Disable the middle mouse button.
Right button	Disable the right mouse button.

Table 5: Mouse key restrictions

7.2.2 Disable function keys

F1	Disable Help
F2	Disable Rename selected item
F3	Disable Search for a file or folder
F4	Disable Switch focus to address bar
F5	Disable Refresh the instance of File Explorer and Refresh File Explorer's current view
F6	Disable Cycle through elements on the screen
F7	Disable F7
F8	Disable F8
F9	Disable F9
F10	Disable Enable app menu bar
F11	Disable Switch active window full-screen mode
F12	Disable F12

Table 6: Functions key restrictions

7.2.3 Disable keyboard system keys

Esc	Close current task
PrintScreen	Take a screenshot and stores in the clipboard
Pause	Disable Pause key
`	Disable ` key
1	Disable number 1 key

2	Disable number 2 key
3	Disable number 3 key
4	Disable number 4 key
5	Disable number 5 key
6	Disable number 6 key
7	Disable number 7 key
8	Disable number 8 key
9	Disable number 9 key
0	Disable number 0 key
-	Disable – key
+	Disable + key
Backspace	Disable Backspace key
Tab	Disable Move forward through options
Q	Disable Q key
W	Disable W key
E	Disable E key
R	Disable R key
T	Disable T key
Y	Disable Y key
U	Disable U key
I	Disable I key
O	Disable O key
P	Disable P key
(	Disable (key
_	Disable _ key
Return	Disable Return key

A	Disable A key
S	Disable S key
D	Disable D key
F	Disable F key
G	Disable G key
H	Disable H key
J	Disable J key
K	Disable K key
L	Disable L key
;	Disable ; key
'	Disable ' key
|	Disable | key
\	Disable \ key
Z	Disable Z key
X	Disable X key
C	Disable C key
V	Disable V key
B	Disable B key
N	Disable N key
M	Disable M key
Comma	Disable Comma key
Period	Disable Period key
Question	Disable Question key
Spacebar	Disable Spacebar key
Left	Disable Left key
Up	Disable Up key

Down	Disable Down key
Right	Disable Right key
Insert	Disable Insert key
Del	Disable Delete key
Home	Disable Home key
End	Disable End key
PageUp	Disable PageUp key
PageDown	Disable PageDown key
NumPad1	Disable NumPad 1 key
NumPad2	Disable NumPad 2 key
NumPad3	Disable NumPad 3 key
NumPad4	Disable NumPad 4 key
NumPad5	Disable NumPad 5 key
NumPad6	Disable NumPad 6 key
NumPad7	Disable NumPad 7 key
NumPad8	Disable NumPad 8 key
NumPad9	Disable NumPad 9 key
NumPad0	Disable NumPad 0 key
Next	Disable Next key
Divide	Disable Divide key
Multiply	Disable Multiple key
Subtract	Disable Subtract key
Enter	Disable Enter key
Add	Disable Add key
Decimal	Disable Decimal key

Table 7: General system keys restrictions

7.2.4 **Disable Alt key combination system keys**

Alt	Disable Alt key and Disable Bar menu
Alt+A	Disable the Select Favourite tab from the bar menu
Alt+E	Disable the Select Edit tab from the bar menu
Alt+I	Disable open the Insert file menu
Alt+F	Disable Search the current topic
Alt+H	Disable Select Help from the bar menu
Alt+L	Disable open the Developer tab in the Ribbon
Alt+N	Disable Display the Connection Settings menu
Alt+D	Disable Select address bar
Alt+P	Disable Display preview panel on File explorer
Alt+Enter	Disable Open Properties settings for the selected item
AltGR	Disable AltGR key
Alt+Tab	Disable Switch between open apps while pressing Tab multiple times
Alt+F4	Disable Close active window. (If no active window is present, then shutdown box appears)
Alt+F8	Disable Reveals typed password in Sign-in screen
Alt+Left	Disable Go back
Alt+Right	Disable Go Forward
Alt+PageUp	Disable Move up one screen
Alt+PageDown	Disable Move down one screen
Alt+Esc	Disable Cycle through open windows
Alt+Spacebar	Disable Open context menu for the active window
Alt+UnderlinedLetter	Disable Runs command for the underlined letter in apps

Table 8: Alt combinations key restrictions

7.2.5 Disable Control key combination system keys

Ctrl	Disable Control key
Ctrl+A	Disable Select all content
Ctrl+C	Disable Copy selected items to the clipboard
Ctrl+D	Disable Delete selected item to the Recycle Bin
Ctrl+E	Disable Select search box
Ctrl+F	Disable Open search
Ctrl+L	Disable Focus on the address bar
Ctrl+M	Disable Starts mark mode
Ctrl+N	Disable Open new window
Ctrl+V	Paste content from the clipboard
Ctrl+W	Disable Close active window
Ctrl+X	Disable Cut selected items to the clipboard
Ctrl+Y	Disable Redo an action
Ctrl+Z	Disable Undo an action, including undelete files (limited)
Ctrl+F3	Disable Open search
Ctrl+DEL	Disable Delete selected item to the Recycle Bin
Ctrl+Left	Disable Change Start menu size
Ctrl+Right	Disable Change Start menu size
Ctrl+Up	Disable Change Start menu size
Ctrl+Down	Disable Change Start menu size
Ctrl+Shift+N	Disable Create a new folder on desktop or File Explorer
Ctrl+Shift+Esc	Disable Open Task Manager
Ctrl+Shift	Disable Switch keyboard layout
Ctrl+F5	Disable Refresh current window
Ctrl+Alt+Tab	Disable View open apps

Ctrl+Left+Spacebar	Disable Select multiple items on desktop or File Explorer
Ctrl+Right+Spacebar	Disable Select multiple items on desktop or File Explorer
Ctrl+Up+Spacebar	Disable Select multiple items on desktop or File Explorer
Ctrl+Down+Spacebar	Disable Select multiple items on desktop or File Explorer
Ctrl+Home	Disable Scroll to top of the console
Ctrl+End	Disable Scroll to the bottom of the console
Ctrl+Esc	Disable Open Start menu

Table 9: Control combinations key restrictions

7.2.6 Disable Shift key combination system keys

Shift	Disable Shift key
Shift+Delete	Disable Delete selected item permanently skipping RecycleBin
Shift+F10	Disable Open context menu for selected item
Shift + Ctrl + F10	Disable Open context menu for selected item

Table 10: Shift combinations key restrictions

7.2.7 Disable Windows key combination system keys

Win	Disable Open Start menu
Win+A	Disable Open Action center
Win+B	Disable Set focus notification area in the taskbar
Win+C	Disable Launch Cortana app
Win+D	Disable Display and hide the desktop
Win+E	Disable Open File Explorer
Win+F	Disable Launch Feedback Hub app
Win+G	Disable Launch Game bar app
Win+H	Disable Open dictation feature
Win+I	Disable Open Settings app
Win+J	Disable Set focus on a tip for Windows 10 when applicable

Win+K	Disable Open Connect settings
Win+M	Disable Minimize all windows
Win+N	Disable Open OneNote
Win+O	Disable Lock device orientation
Win+P	Disable Open Project settings
Win+Q	Disable Open Search
Win+R	Disable Open Run command
Win+S	Disable Open Search
Win+T	Disable Cycle through apps in the taskbar
Win+U	Disable Open Ease of Access settings
Win+V	Disable Open Clipboard bin
Win+W	Disable Open the Windows Ink Workspace
Win+X	Disable Open Quick Link menu
Win+Y	Disable Change input between desktop and Mixed Reality
Win+Z	Disable Switch input between the desktop experience and Windows Mixed Reality
Win+Left	Disable Snap app or window left
Win+Right	Disable Snap app or window Right
Win+Pause	Disable Show System Properties dialog box
Win+Tab	Disable Open Task View
Win+Alt+D	Disable Open date and time in the taskbar
Win+Ctrl+Enter	Disable Open Narrator
Win+Ctrl+D	Disable Create new virtual desktop
Win+Ctrl+F4	Disable Close active virtual desktop
Win+Ctrl+Right	Disable Switch to the virtual desktop on the right
Win+Ctrl+Left	Disable Switch to the virtual desktop on the left
Win+Ctrl+F	Disable Open search for the device on a domain network
Win+Ctrl+Q	Disable Open Quick Assist
Win+Ctrl+Shift+B	Wake up the device when black or a blank screen

Win+Shift+S	Disable Create part of the screen screenshot
Win+Shift+V	Disable Cycle through notifications
Win+PrintScreen	Disable Capture full screenshot in the Screenshots folder
Win+Alt+1	Open Jump List of the app in number 1 position from the taskbar
Win+Alt+2	Open Jump List of the app in number 2 position from the taskbar
Win+Alt+3	Open Jump List of the app in number 3 position from the taskbar
Win+Alt+4	Open Jump List of the app in number 4 position from the taskbar
Win+Alt+5	Open Jump List of the app in number 5 position from the taskbar
Win+Alt+6	Open Jump List of the app in number 6 position from the taskbar
Win+Alt+7	Open Jump List of the app in number 7 position from the taskbar
Win+Alt+8	Open Jump List of the app in number 8 position from the taskbar
Win+Alt+9	Open Jump List of the app in number 9 position from the taskbar
Win+Alt+0	Open Jump List of the app in number 10 position from the taskbar

Table 11: Win combinations key restrictions

7.3   Apps

The Apps tab is a white list of applications allowed to run on the PC.

Applications can be configured by adding the path of the executable file ".exe" or adding a folder where all executable files ".exe" within it and its subfolders will be allowed to run.

By default, the list is empty. The module won't block any applications until at least one application is added.

Note: The Task Manager is never blocked from the Apps Tab for security reasons. If you want to block Task Manager, it can be blocked from the **"Core -> Systems"** section.
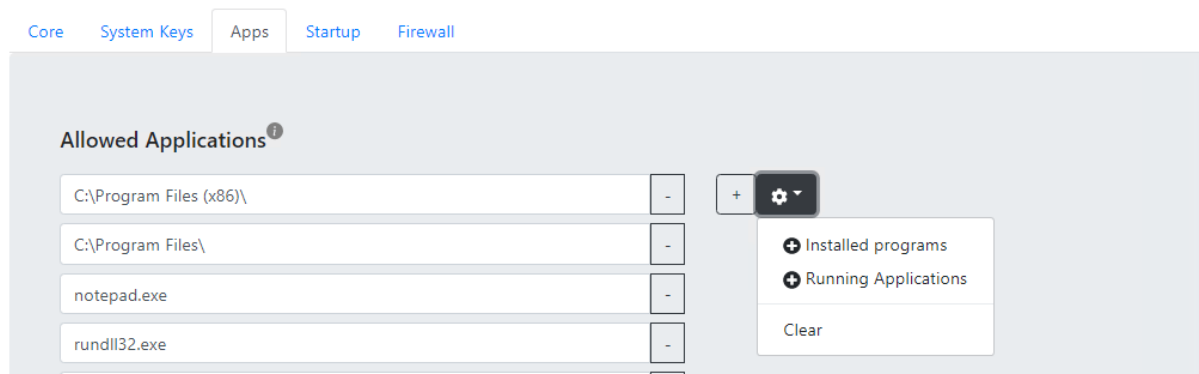
This section lists applications that are whitelisted by LabLock. Therefore, applications not listed on the Apps table will be blocked by LabLock.

Windows folder paths can also be added to the table. All .exe files in subfolders of added folder paths will be allowed to run.

On the right-hand side of the screen there is a **"Settings"** button where you have 3 predefined options:

- **Installed programs:** This option will add "C:\Program Files\" and "C:\Program Files (x86)\" folder paths to the list of allowed applications.

- **Running applications:** This option will add currently running apps to the list of allowed applications.

- **Clear:** This option will remove all the applications from the list.

In addition, you can add executables or paths by clicking on the **"+"** sign located on top of the table.

Individual entries can be deleted by clicking on the **"-"** sign located in each line of the table.

7.4 Startup

The Startup tab allows you to add paths to executables and scripts that will be executed by Windows at Start-up.
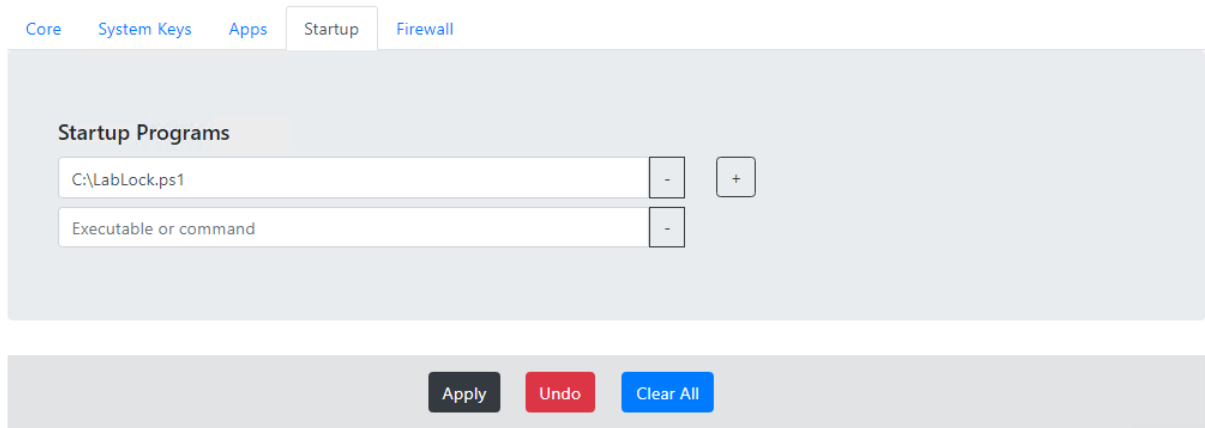
By clicking the **"+"** sign located at the top of the table, you will be able to add new lines to the list of Startup programs.

Each line will also have a **"-"** sign to delete the script or executable previously added.

7.5 Firewall

The firewall tab allows configuring local Firewall rules on the PC where LabLock is located. The screen is divided into two tables: LabLock firewall rules and Windows firewall rules.
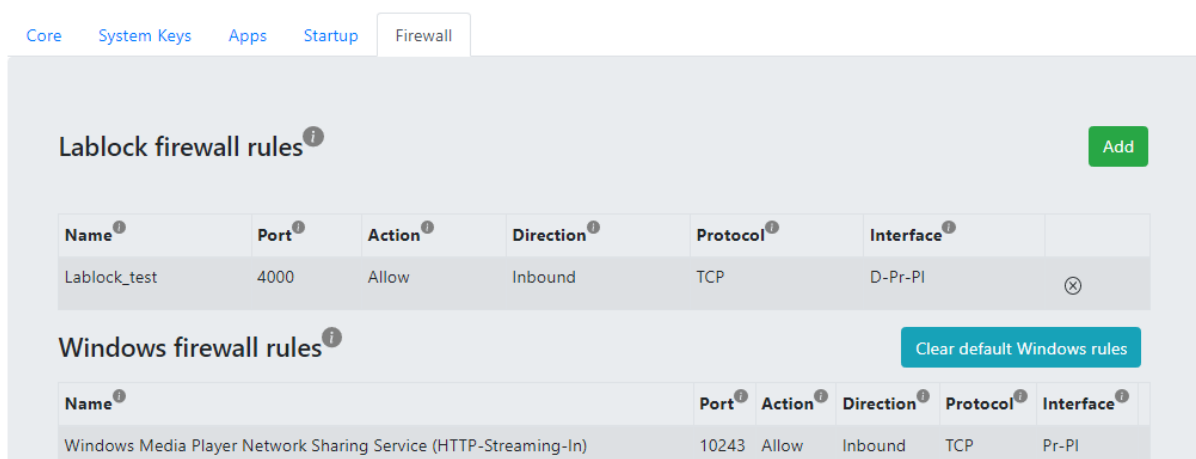
LabLock firewall rules: This table will display any rules created from this functionality. The rules added can also be deleted by clicking the remove button on the right-hand side of each rule.

.

To add new rules, you will need to click the "Add" button. A popup window will be displayed with the following:

Add new firewall rule ✕

Name [_____]

Port [_____]

Direction ○ Inbound ○ Outbound

Protocol ○ TCP ○ UDP

Action ○ Allow ○ Block

Profile ☑ Public ☑ Private ☑ Domain

[Save] [Close]

Name: Name for the firewall rule.

Port: Port number of the firewall rule. The numbers allowed are between 1 and 65535

Allow/Block: Determines if the port for the rule should be allowed or blocked.

Inbound/Outbound: Implements the rule as inbound or outbound.

TCP/UDP: This shows the protocol of the rule. It can be TCP or UDP.

Profile: Contains 3 options, Domain, Public, and Private. The table will show "D-PR-PL" depending on the option selected. Multiple options are allowed.

Note that the rules can only be added by a specific port number using this functionality.

Windows firewall rules: This table will display any rules created in the computer outside LabLock. These rules can't be removed from the application but can be useful when creating rules that can't override the existing rules setup. To see the rules, click "Load Windows rules". Once the Windows rules are loaded, you can also hide them by clicking on "Clear default Windows rules".

Finally, click **"Apply"** to implement configured restrictions.

Click **"Undo"** to remove restrictions that were selected but not applied along with different restrictions tabs.
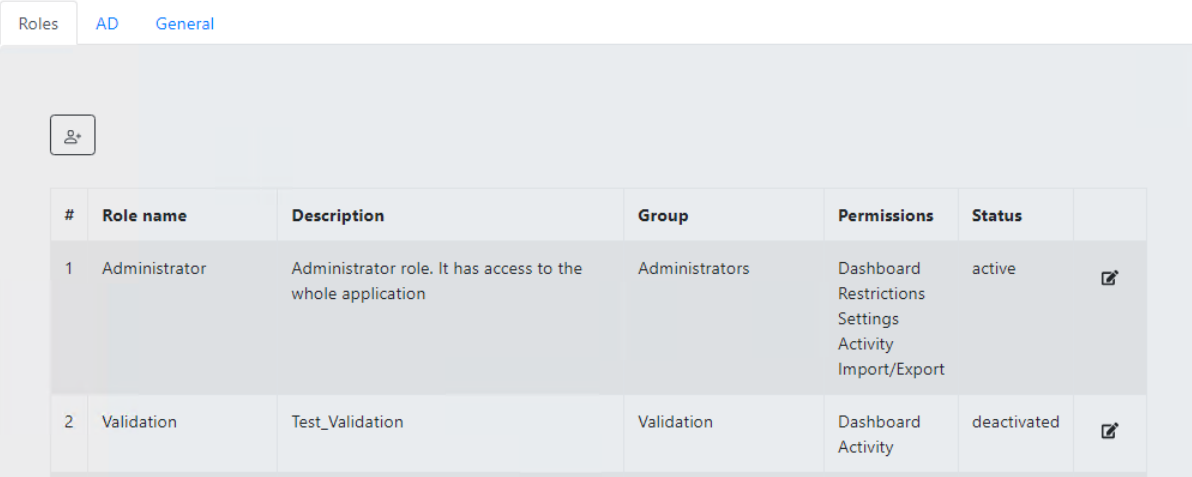
Click **"Clear all"** to remove all applied restrictions from the LabLock.

8. Settings Menu

Settings menu allows you to configure the different LabLock options. Settings are divided into 3 different sub-sections: Roles, AD, and General.

8.1 Roles

The Roles tab allows access to different profiles within LabLock. These roles must be attached to existing Local Windows groups or Active Directory security groups.

On the landing screen, there will be a list with all the roles created, a description, the group they belong to, the permissions granted for the role, and the status of the role. By default, there will be an Administrator role belonging to the Administrators local Windows group to access the application.

Note: To do the initial setup, only a user belonging to the Administrators windows group will be allowed to log in to LabLock.

You can also create new roles or edit existing ones:

- To create a new role, click on add role button
- To edit an existing role, click on the button

When pressing either button, a new screen will be displayed where we can set the following fields:

Role name: This is the name of the LabLock role

Description: This is a description of the LabLock Role

Group: This is the group used. The group can be a Windows local group or an Active Directory security group.

Permissions: This section is used to set the permissions of the group.

Status: The status of the role in LabLock, can be activated or deactivated.

Name: This is the name of the LabLock role**.**

Description: This is a description of the LabLock Role.

Windows group: Windows group can be **"Local"** or **"Active Directory"**. If **"Local"** is selected the user will be authenticated against a local user and group. However, if **"Active Directory"** is selected, the authentication will be done against an AD user and AD security group using LDAP.

Group name: This is the name of the local group or the name of the AD security group. For AD will be using the group DistinguishedName. For a user called "LabLock_User", the DN could be as follows: "CN=LabLock_users, OU=Groups, OU=LabLock, DC=LABLOCK, DC=local"

Health-check button: This button can be used to check the connectivity of AD groups. Click the button and if the AD group exists and the connection is configured correctly, the button will become green.

Active: Select active to make the group active or unchecked the option to disable the group
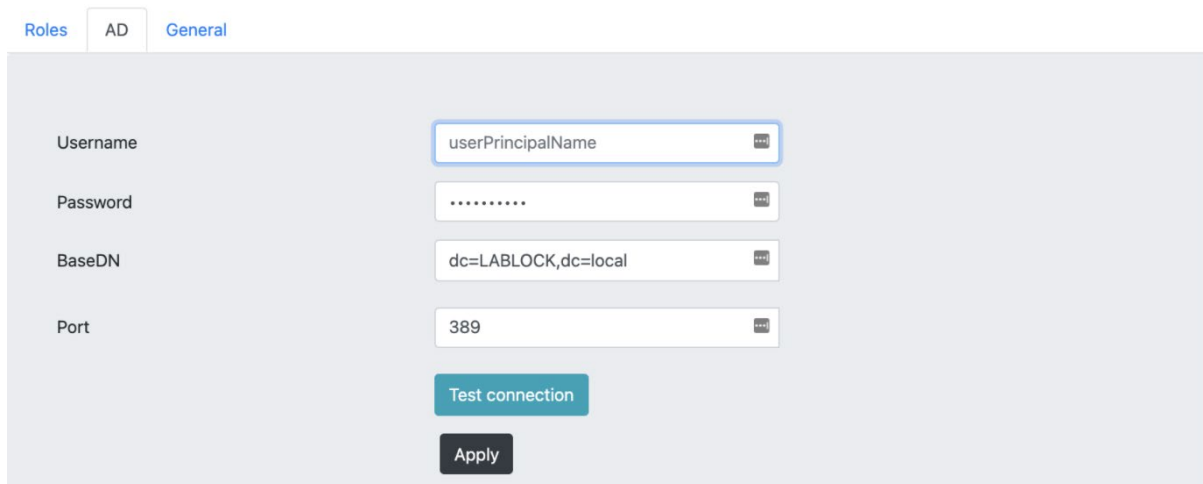
Permissions: Select the permissions to be granted to the role. You can choose from Dashboard, Restrictions, Activity, Settings, and Import/Export**.**

Cancel: Click **"Cancel"** to discard the changes and come back to the list Roles screen.

Save: Click **"Save"** to save the new group configuration.

8.2 AD

In this tab, you can configure the settings to connect to an Active Directory server. You will need a valid AD service account. Once you fill this section with a user, LDAP authentication will be activated.

NOTE: Filling this option allows to use LDAP authentication. LDAP and Local Authentication can be used simultaneously.

Username: User should add Active Directory account. Use "UserPrincipalName" account property for the Active Directory user.

Password: Password of the Active Directory service account.

BaseDN: stand for Base DistiguishedsName, this should be the domain controller name. For example "dc=domain,dc=com".

Port: This is the LDAP authentication port used by your domain. By default, the ports used can be 389 for LDAP and 636 for LDAPS.

Test Connection: the "**Test Connection**" button is used for checking the AD connectivity. If the authentication call is successful, it will display a box with a check icon with a green background. However, if the health check fails, it will show a box with an "X" inside with a red background.

Apply: Click Apply to save the changes.

8.3 General

General section contains general LabLock configuration settings:

Option	Explanation
LabLock port	The port will be used to connect to LabLock
Session Expiration	In the Session Expiration option, it can be created to automatically log out from a session in LabLock
Suspend restrictions time	In Suspend restrictions time can be configured a time (in minutes) to temporally disable LabLock windows restrictions
Suspend restrictions Hotkey combination	In Suspend Restrictions Hotkey combination can be configured as a hotkey combination to disable restrictions from locally in the computer. This hotkey can be executed without login to
Hotkey password	In Hotkey password, it can be configured a password to suspend windows restrictions temporally from the local computer
Hide user notifications	In Hide user notification, it can be enabled or disabled information notifications for Windows
Brand	In Brand, you can add the brand of your company to the notifications. This brand will only be shown if the Hide user notifications option is disabled

Choose Windows background image	In Choose Windows background image, it can be configured as a background image for Windows users.
Snapshot path	In the Snap-shot path option, it can be configured the folder path where the snapshot taken in the dashboard will be saved.
Backups retention period	In the Backups retention period, it can be configured the retention period for the backup's files. LabLock will delete the backup files older than the period selected automatically.
Backups path	In the Backups path option, it can be configured the folder path where the backups file will be saved. LabLock will generate a backup Zip file with the configuration and logs in a daily basis.

Table 12: General settings

9. Import / Export Tab

Import / Export menu is used to import and export LabLock configuration between different instances. There are two sections within this menu, one to Export configurations and another one to Import existing configurations.

9.1 Export
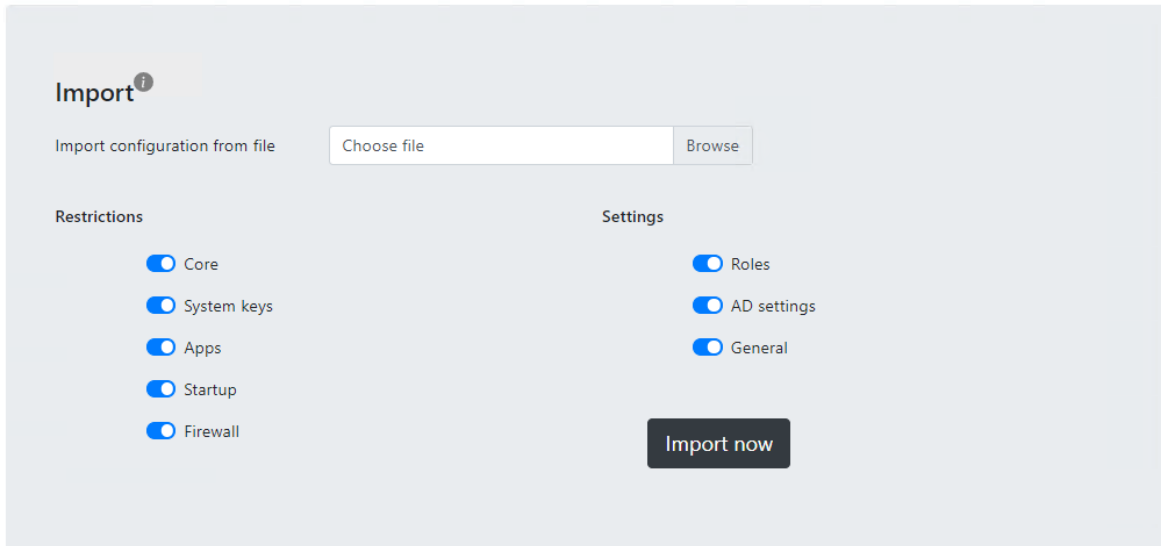
In the Export section, you will export the current LabLock restrictions and settings configurations into a file that can be shared with other computers.
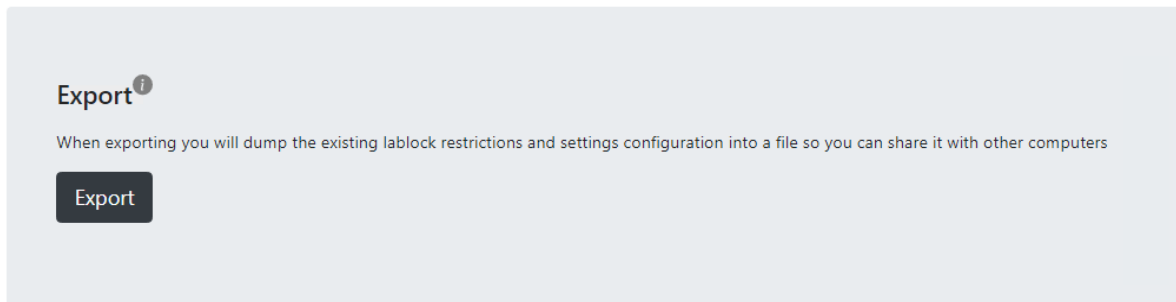
Click on the **"Export"** button to download the LabLock export configuration file. This file has a unique MD5 number that is created when the configuration file is requested. This MD5 number is recorded in the **"Activity"** menu.

9.2   Import

In the Import section, you will import the existing LabLock restrictions and settings configurations from other LabLock instances.

Click **"Browse"** to upload a LabLock configuration file.

Once loaded, you have different checkboxes for the different **"Restrictions"** and **"Settings"** available in LabLock. By default, all the sections will be imported.

Checked the sub-sections that you want to import to the system

Then click the **"Import now"** button to upload them and apply the configuration.

In the **"Activity"** section can be checked the MD5 number of the configuration file is imported for traceability.

10. Activity Tab

The activity menu can be used to view, search and trace the different activities and changes to the restrictions in the LabLock web portal, such as applied restrictions, warnings, user login information, and more. Use the search box to find specific entries.

On the top menu, you can filter the different entries based on the username, the IP accessing LabLock, the start and end dates, and even the different menu(s) within the LabLock application: Login, Dashboard, Restrictions, Settings, and Import/Export.

Applied restrictions can be inspected by locating the appropriate entry and then clicking the more info button

By default, the activity log has a limit of 50 explorable entries, which can be expanded to 200 or 1000 entries, at the bottom, while the total number of log entries can be exported.

Log entries can be exported by clicking export, located at the upper right corner. Logs can be exported in CSV format.

Following logs can be registered in the LabLock Activity section:

Filter	Message
Login	User or password is incorrect
Login	is locked
Login	is part of two or more groups
Login	doesn't have permissions to login to LabLock from
Login	login to LabLock from
Dashboard	took a screenshot from
Dashboard	Suspended restrictions from
Dashboard	Log off the PC from
Dashboard	Restarted the PC from

Dashboard	Shutdown the PC from
Import/export	import the configuration file with the identification number MD5 {the MD5 number}
Import/export	export the configuration file with the identification number MD5 {the MD5 number}
Activity	export activity log file in pdf format from
Activity	export activity log file in csv format from
Settings	Changed LabLock port from {Old port} to {New port} from
Settings	Modify Session Expiration time from {Old time} minutes to {New time} minutes from
Settings	Disable Single sign on from
Settings	Changed Suspend Restrictions time from {old value} to {new value) from
Settings	Changed hotkey combination from
Settings	Changed hotkey password from
Settings	Activate hide user notifications from
Settings	Disable hide user notifications from
Settings	Added {name of brand} brand from
Settings	Disable {when bran is empty} from
Settings	Change Background image path from {Old path} to {New Path} from
Settings	Disable background image path {When the path is empty}
Settings	Change Snapshot path from {Old Path} to {New Path} from
Settings	Changed backup retention period from {Old day} days to {New day} days from
Settings	Change backup path from {Old Path} to {New Path} from
Settings	Create the role {Name of the role} based on {Local PC/AD} from
Settings	Modify the role {Name of the role} based on {Local PC/AD} from
Settings	Enable the role {Name of the role} based on {Local PC/AD} from
Settings	Disable the role {Name of the role} based on {Local PC/AD} from
Settings	Added Active directory settings from
Settings	Modified Active Directory settings from
Restrictions	applied new restrictions from
Restrictions	removed all restrictions from

Table 13: Activity logs details

11. EULA (End User License Agreement) for LabLock software

11.1 DEFINITIONS

11.1.1 "LabLock" means JAKO-Solutions A/S

11.1.2 "EULA" means this End User License Agreement for LabLock's Software.

11.1.3 "IPR" means intellectual property rights in patents, copyrights, trademarks, design rights or similar.

11.1.4 "License" means the license to use the Software, as further specified in Section 2.

11.1.5 "Licensee" means the legal entity or individual that installs the Software.

11.1.6 "Software" means the software provided to the Customer by LabLock.

11.2 LICENSE

11.2.1 License: Subject to this EULA, LabLock hereby grants the Licensee a non-exclusive, non-transferable, non-sublicensable, revocable and limited right to install and use the Software. If the Software is paid for and provided as a package together with LabLock products, the Software may be used on two computers. If the Licensee wishes to use the Software for an additional computer, a license for one additional computer shall be purchased from LabLock through a separate agreement. The Licensee may not otherwise install, use, or copy the Software, and any rights not explicitly granted to the Licensee shall be considered reserved to LabLock.

11.2.2 Acceptance: By downloading, installing, copying, or otherwise using the Software, the Licensee shall be bound by this EULA.

11.3 IPR

11.3.1 IPR: LabLock retains all ownership and IPR to the Software and anything else delivered under this EULA. To the extent that the Software is changed, developed or adapted as a result of input, feedback or ideas from the Licensee, LabLock acquires all IPR to any such changes, developments or adaptations as well as to any such input, feedback or ideas.

11.3.2 No modifications: The Licensee may not copy or modify the Software in any way not authorized by LabLock. This prohibition includes adapting, translating, decompiling, reverse engineering, disassembling, or attempting to derive the source code from the Software.

11.3.3 Right to grant License: The software is owned and copyrighted by JAKO-Solutions. Your license confers no title or ownership in the software and should not be construed as a sale of any right in the software.

11.3.4 Limited Warranty: License grant. JAKO-Solutions grants you a license to use one copy of this software on any one system for as many licenses as Licensee purchase. "Use" means storing, loading, installing, executing, or displaying the software. You may not modify the software or disable any licensing or control features of the software except as an intended part of the software's programming features. When you first obtain a copy of the software, you are granted an evaluation period negotiated with JAKO-Solutions, after which time you must pay for the software according to the terms discussed in the software's documentation, or you must remove the software from your system. This license is not transferable to any other system, or to another organization or individual. You are expected to use the software on your system and to thoroughly evaluate its usefulness and functionality before making a purchase. This "try before you buy" approach is the ultimate guarantee that the software will perform to your satisfaction; therefore, you understand and agree that there is no refund policy for any purchase of the software.

11.3.5 Malicious code: JAKO-Solutions warrants that it has used reasonable efforts to ensure that the Software does not contain any malicious code such as worms, viruses, Trojan horses, protect codes, data destruct keys or similar codes intended to access, modify, delete, damage, deactivate or disable the Software or the Licensee's other systems. The Licensee's sole remedy for LabLock's breach of this warranty is that JAKO-Solutions shall take action to investigate, identify and remove such malicious code from the Software.

11.3.6 No other warranties. JAKO-Solutions does not warrant that the software is error free. JAKO-Solutions disclaims all other warranties with respect to the software, either express or implied, including but not limited to implied warranties of merchantability, fitness for a particular purpose and noninfringement of third-party rights. Some jurisdictions do not allow the exclusion of implied warranties or limitations on how long an implied warranty may last, or the exclusion or limitation of incidental or consequential damages, so the above limitations or exclusions may not apply to you. This warranty gives you specific legal rights and you may also have other rights which vary from jurisdiction to jurisdiction.

11.3.7 Disclaimer of warranties: The limited warranties in this section are the only warranties granted by JAKO-Solutions to the Licensee. LabLock MAKES NO OTHER WARRANTIES WHATSOEVER, EXPRESS OR IMPLIED, WITH REGARD TO THE SOFTWARE, NEITHER UNDER THIS EULA NOR IN SEPARATE AGREEMENTS. LabLock EXPLICITLY DISCLAIMS ALL WARRANTIES OF SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE. LabLock DOES NOT WARRANT THAT THE SOFTWARE – IN WHOLE OR IN PART – WILL BE ERROR FREE, OPERATE WITHOUT INTERRUPTION OR MEET THE LICENSEE'S REQUIREMENTS.

11.4 TERM AND TERMINATION

11.4.1 Term: The License is unlimited in time. However, LabLock may terminate the License with immediate effect if the Licensee violates this EULA.

11.4.2 Termination effect: Upon termination, the Licensee shall immediately stop using the Software and destroy all copies.

11.5 SUPPORT

11.5.1   Updates: LabLock may from time to time provide updates, bug fixes and patches to the Software, but LabLock shall be under no obligation to provide specific updates or to provide updates at specific intervals. LabLock shall not be obliged to provide other support services, except as agreed between LabLock and the Licensee.

11.5.2   Right to grant License: The software is owned and copyrighted by JAKO-Solutions. Your license confers no title or ownership in the software and should not be construed as a sale of any right in the software.

11.5.3   Limited Warranty: License grant. JAKO-Solutions grants you a license to use one copy of this software on any one system for as many licenses as Licensee purchase. "Use" means storing, loading, installing, executing, or displaying the software. You may not modify the software or disable any licensing or control features of the software except as an intended part of the software's programming features. When you first obtain a copy of the software, you are granted an evaluation period negotiated with JAKO-Solutions, after which time you must pay for the software according to the terms discussed in the software's documentation, or you must remove the software from your system. This license is not transferable to any other system, or to another organization or individual. You are expected to use the software on your system and to thoroughly evaluate its usefulness and functionality before making a purchase. This "try before you buy" approach is the ultimate guarantee that the software will perform to your satisfaction; therefore, you understand and agree that there is no refund policy for any purchase of the software.

11.5.4   Malicious code: JAKO-Solutions warrants that it has used reasonable efforts to ensure that the Software does not contain any malicious code such as worms, viruses, Trojan horses, protect codes, data destruct keys or similar codes intended to access, modify, delete, damage, deactivate or disable the Software or the Licensee's other systems. The Licensee's sole remedy for LabLock's breach of this warranty is that JAKO-Solutions shall take action to investigate, identify and remove such malicious code from the Software.

11.5.5   No other warranties. JAKO-Solutions does not warrant that the software is error free. JAKO-Solutions disclaims all other warranties with respect to the software, either express or implied, including but not limited to implied warranties of merchantability, fitness for a particular purpose and noninfringement of third-party rights. Some jurisdictions do not allow the exclusion of implied warranties or limitations on how long an implied warranty may last, or the exclusion or limitation of incidental or consequential damages, so the above limitations or exclusions may not apply to you. This warranty gives you specific legal rights and you may also have other rights which vary from jurisdiction to jurisdiction.

11.5.6   Disclaimer of warranties: The limited warranties in this section are the only warranties granted by JAKO-Solutions to the Licensee. LabLock MAKES NO OTHER WARRANTIES WHATSOEVER, EXPRESS OR IMPLIED, WITH REGARD TO THE SOFTWARE, NEITHER UNDER THIS EULA NOR IN SEPARATE AGREEMENTS. LabLock EXPLICITLY DISCLAIMS ALL WARRANTIES OF SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE. LabLock DOES NOT WARRANT THAT THE SOFTWARE – IN WHOLE OR IN PART – WILL BE ERROR FREE, OPERATE WITHOUT INTERRUPTION OR MEET THE LICENSEE'S REQUIREMENTS.

11.5.7 Term: The License is unlimited in time. However, LabLock may terminate the License with immediate effect if the Licensee violates this EULA.

11.5.8 Termination effect: Upon termination, the Licensee shall immediately stop using the Software and destroy all copies.

11.6 LIABILITY

11.6.1 Indirect losses: LabLock is not liable for any indirect or consequential damages, including damages for lost profits, loss of data, or business interruptions.

11.6.2 Software misuse. This software should never be installed, or used, without the PC administrator's consent. This software is designed for use when any required consents have been obtained. JAKO-Solution declines all responsibility concerning any illicit usage.

11.6.3 Liability cap: No liability for consequential damages. In no event shall JAKO-Solutions be liable to you for any consequential, special, incidental or indirect damages of any kind arising out of the delivery, performance or use of the software, even if JAKO-Solutions has been advised of the possibility of such damages. In no event will JAKO-Solutions liability for any claim, whether in contract, tort, or any other theory of liability, exceed the license fee paid by you, if any.

11.7 PREVAILING AGREEMENT AND SEVERABILITY

11.7.1 Terms & Conditions: To the extent that this EULA conflicts with JAKO-Solutions's general terms and conditions, JAKO-Solutions's general terms and conditions shall prevail.

11.7.2 Severability: If a court or other competent authority finds any provision of this EULA, or a portion thereof, to be unenforceable, the remainder of this EULA shall continue in full force and effect.

11.8 GOVERNING LAW AND DISPUTES

11.8.1 Governing law: This EULA, and all rights and obligations between JAKO-Solutions and the Licensee, shall be governed by the European law. The United Nations convention on contracts for the international sale of goods is specifically disclaimed.

11.8.2 Disputes: Any dispute between JAKO-Solutions and the Licensee which the parties cannot solve through negotiation shall be handled by the Commercial Court in Dublin, Ireland.