PortBlocker User Guide

version 1.0.0

DataLocker Inc.

January 2019

PortBlocker

Contents

About PortBlocker USB Port Control

DataLocker PortBlocker is an endpoint protection agent that limits which USB Mass Storage Devices can be used on a workstation. Your SafeConsole administrator can define which devices are allowed to be used. PortBlocker is commonly used to allow only SafeConsoleReady devices to provide a full encrypted and managed solution for portable device usage.

Affected Devices

PortBlocker can filter USB mass storage MTP and PTP devices. Other devices, such as USB mice and keyboards, are always allowed.

Common USB-connected peripherals known to use the USB mass-storage device class:

- USB flash drives
- USB external hard drives
- MP3 players
- Digital cameras
- Media card readers
- Cellular devices

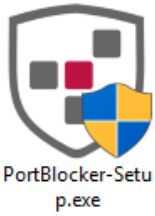
Note: It will still be possible to charge portable devices via USB.

Installation

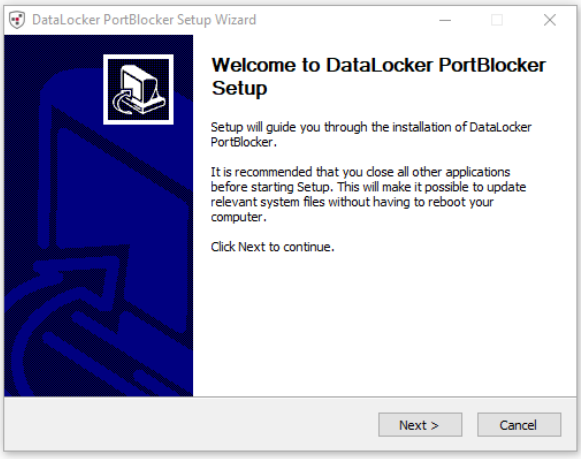
Note: Installation requires administrative permissions. Please contact your administrator to complete this process if PortBlocker is not already installed.

1. Double click the **PortBlocker-Setup.exe**. This will launch the install wizard.

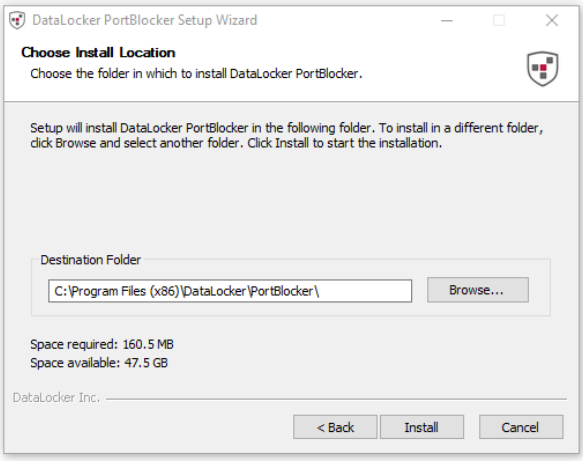
   Note: Installing PortBlocker requires administrative privileges.



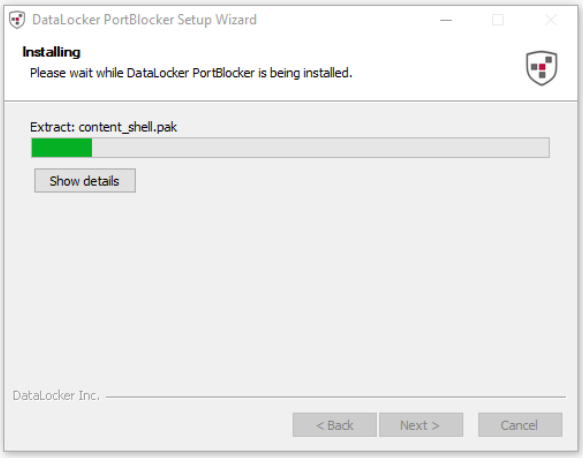
2. On the first page of the installer, click **Next**.



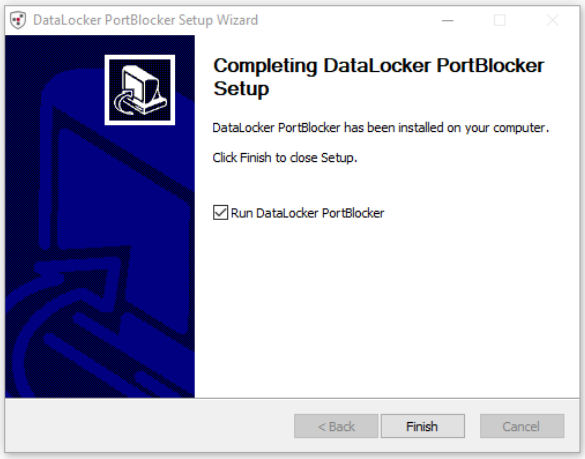
3. Choose an install location and click **Install**.



4. The installer will show the progress bar as it installs drivers signed by DataLocker.



5. Once the installer is finished, check the **Run DataLocker PortBlocker** checkbox if it's not already selected, and click **Finish**.



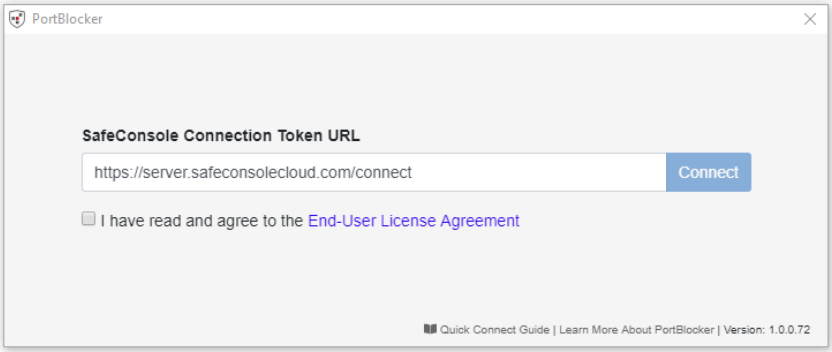
Registration

Upon first launch, registration will be the only option available. **All affected devices will be blocked until registration is completed.** See the Affected Devices section for more details.

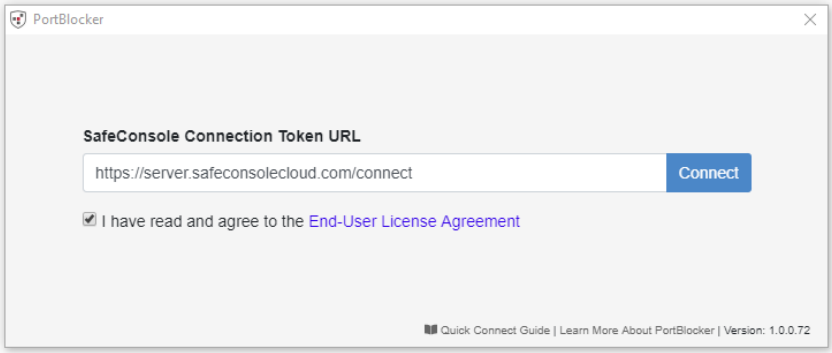
To register your PortBlocker client:

1. Type in the **SafeConsole Connection Token** provided by your administrator.

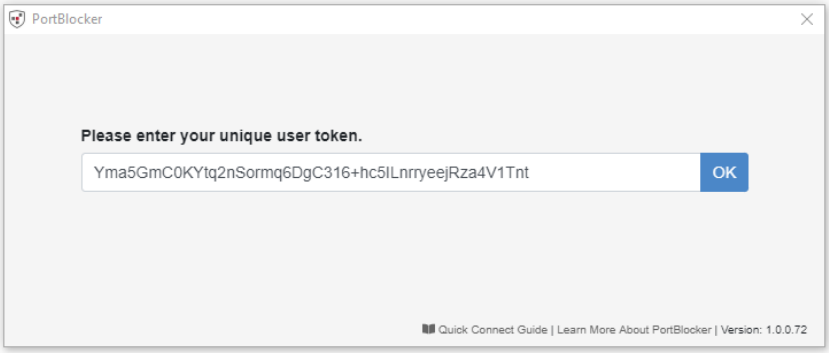
   Note: This box may be pre-filled with your Connection Token by your administrator.



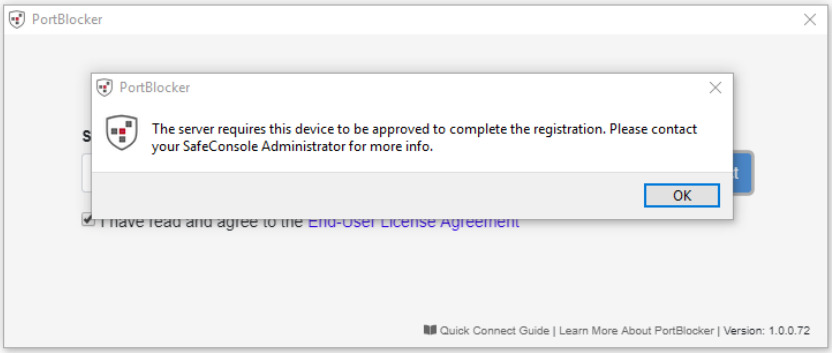
2. Check the **EULA** checkbox and click **Connect**.



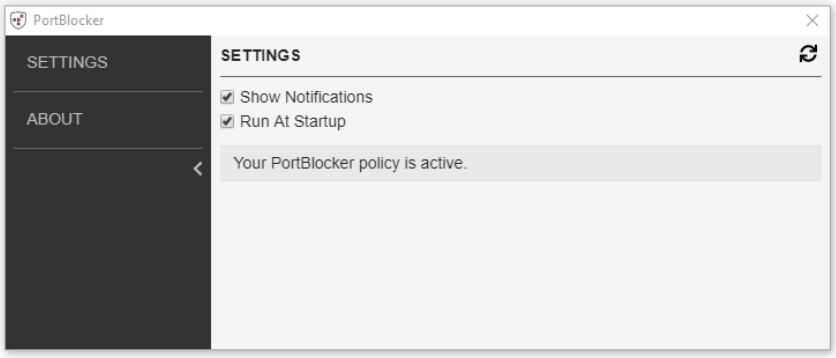
- **Optionally Enabled Policies** - These policies may or may not be enabled by your administrator. They will appear during registration if they have been enabled.
  - Unique User Token: This token is directly associated with the end user's account and will be provided by the administrator.



  - Administrator Registration Approval: The administrator may require their approval to proceed with registration.



3. The PortBlocker client will register and apply any policies set by the administrator. The client will show the Settings page by default.

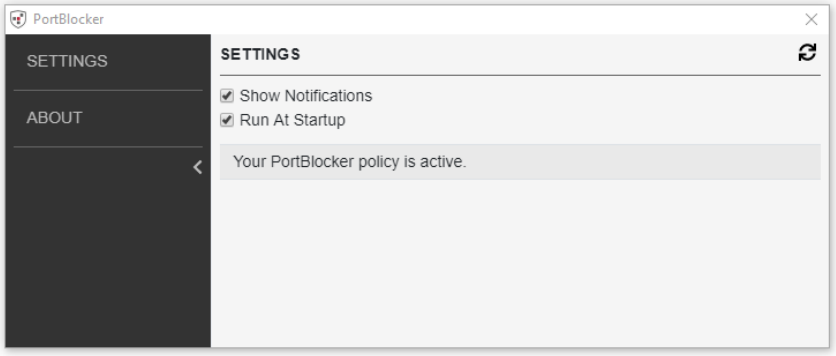


User Interface

Launching the PortBlocker client will allow interaction with PortBlocker, including managing optional settings.

Settings Tab

There are several options for configuring the settings on the PortBlocker client. The Settings page will be shown by default upon launching the PortBlocker client. If not already there, click on the **Settings** tab to access the available settings.



Show Notifications

By checking the **Show Notifications** checkbox, you will see desktop notifications regarding the PortBlocker application. These notifications will show on your desktop, regardless if the client is open or not.

If a blocked device is inserted into your machine, you will be notified that this is not allowed.

Clicking on the notification will bring up the client.

Run At Startup

The PortBlocker service launches automatically on startup, but the client does not. By checking the **Run At Startup** checkbox, PortBlocker will appear minimized with a tray icon. If this setting is disabled, the tray icon will not be present unless a blocked device is plugged in or the administrator issues a reset command.

Note: Disabling this option will not keep the PortBlocker application from running on the computer.

Policy Updates

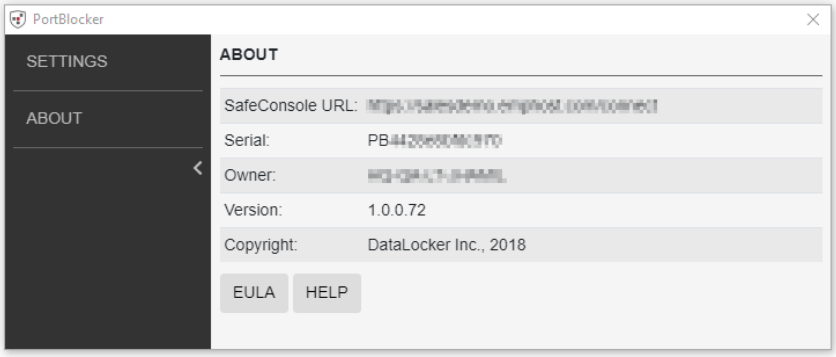
The policy will update when the **Refresh** icon is clicked. Automatic updates are applied every 10 minutes, even when the client is closed. If you wish to update the policy manually, click the **Refresh** icon at the top right.

To update the policy manually:

1. Click the **Settings** tab on the client. PortBlocker opens the Settings page by default upon launch.
2. Click the **Refresh** button in the upper right-hand corner.
3. PortBlocker will check for updates from the SafeConsole server and apply them.

About Tab

The About tab will show the technical details of the PortBlocker endpoint.



The information includes the following:

- SafeConsole URL that the client is registered to
- Serial number of the client
- Owner of the client
- Version number
- Copyright information

A copy of this information can be provided to your administrator or to technical support during additional troubleshooting.

A EULA and Help link are listed below the technical details.

Windows Tray Icon

PortBlocker launches automatically on startup, displaying a tray icon. Clicking on the tray icon or selecting the application from the start menu will bring up the client.

Note: By checking the **Run At Startup** checkbox on the Settings page, PortBlocker will appear minimized with a tray icon. If this setting is disabled, the tray icon will not be present unless a blocked device is plugged in or the administrator issues a reset command.

Whitelisting Devices

To get a specific device or a group of devices whitelisted so that they can be used, please contact your SafeConsole administrator. They may ask you to send the technical details from the PortBlocker client to assist in whitelisting your device. See the About Tab section for more information.

Troubleshooting

For help with PortBlocker, contact your SafeConsole administrator or visit the PortBlocker Support Page.

Where Can I Get Help?

The following resources provide more information about DataLocker products. Please contact your Help Desk or System Administrator if you have further questions.

- support.datalocker.com: Information, knowledgebase articles, and video tutorials
- support@datalocker.com: Email a support ticket
- datalocker.com: General information
- datalocker.com/eula: EULA information

NOTE: DataLocker is not liable for technical or editorial errors and/or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing or use of this material. The information provided herein is subject to change without notice. The information contained in this document represents the current view of DataLocker on the issue discussed as of the date of publication. DataLocker cannot guarantee the accuracy of any information presented after the date of publication. This document is for information purposes only. DataLocker makes no warranties, expressed or implied, in this document. DataLocker, and the DataLocker logo are trademarks of DataLocker Inc. and its subsidiaries. All other trademarks are the property of their respective owners. Ironkey™ is a registered trademark of Kingston Technologies, used under permission of Kingston Technologies. All rights reserved.

FCC Information This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Note: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.