



# PortBlocker Admin Guide and Reference Manual

November 2023

## Table of Contents

<b>About PortBlocker USB Port Control</b>	<b>3</b>
Features	3
Affected Devices	4
Minimum Requirements	4
Proxy Requirements	4
Getting Started	4
Windows Installation	4
Installation	5
Registration	5
macOS Installation - Manual and Mass Deployment	6
Manual Installation Wizard	6
Enable Full Disk Access for Manual Installations	6
macOS Deployment	7
Mass Deployment - Windows and macOS	7
Registration	8
Expected Behavior	9
Blocked	9
Read Only	10
Full Access	10
User Interface	10
Settings Tab	10
Show Notifications	11
UI visible on system startup (Windows only)	11
Enable debug logging	12
Language	12
Policy Updates	12
About Tab	12
Tray (Menu Bar) Icon	13
Managing With SafeConsole	13
Licensing	14



Server Settings	14
Endpoint Actions	15
Policies	15
PortBlocker	15
Uninstall Password	17
Hide Client (Background Stealth Mode)	17
Custom Policy Refresh Interval	17
User Defaults	17
Audit Logs	18
GeoFence	19
Trusted Network	20
Danger Zone	20
Device List	20
SafeConsoleReady Devices	21
Adding Serial Numbers	21
Set all unlisted devices to Read-Only	23
Other Devices	24
Finding The VID, PID, and Serial Number	24
Custom Device	24
Quick method	24
Manual method	25
Importing CSV	27
Uninstalling PortBlocker	27
Windows Uninstall:	27
Uninstalling from Command Line	28
macOS Uninstall	28
Troubleshooting	28
<b>Document Version</b>	<b>30</b>
<b>Notices</b>	<b>30</b>
Disclaimer	30
Patents	30



## About PortBlocker USB Port Control

PortBlocker by DataLocker is a managed solution that allows central management of USB mass storage devices through SafeConsole, the [SafeConsole Admin Guide](#) is the main document for policies and remote management. It is a straightforward approach to preventing data breaches and keeping malware out of your workstations.

PortBlocker ensures only allowed devices may be mounted as USB mass storage devices to the computers on which it is installed. This stops usage of unsecure and unaudited USB mass storage devices and ensures that viruses running on unsecure USB devices cannot infect the computer or network. PortBlocker will also log all approved and blocked USB events to the SafeConsole management server.

Note: PortBlocker requires a connection to the SafeConsole management platform and an available license seat. Licenses sold separately.

## Features

- Endpoint Port Control - Restrict USB storage devices through a SafeConsole defined allow list, using the VID, PID, and serial number of the device.
- Computer-Based Policy Enforcement - Policies are applied based on the computer location. Individual policies can be created down to the computer level, if needed.
- Read-only - Devices can be set to a read-only mode either through defined lists or as a fallback for unlisted devices.
- Quick Disable/Enable - Administrators can remotely Allow All and Block All devices through SafeConsole.
- Activity Audits - Events such as connected USB devices, registered endpoints, allow all devices, etc. are reported to SafeConsole in the User Audit Logs.
- Automatic Refresh - PortBlocker automatically receives policy updates from SafeConsole every 10 minutes or manually as needed.
- Hide Client (Stealth Mode) - allows administrators to run PortBlocker hidden in the background. The user interface and notifications will be inaccessible.
- Uninstall Password - Administrators can restrict PortBlocker from unauthorized uninstallation through the use of an uninstall password.
- Geofence - Devices can be automatically blocked when the computer is outside of the geolocation requirements.
- Offline Capability - The cached SafeConsole policy allows for offline functionality within PortBlocker.
- Easy Deployment - Deploy PortBlocker to multiple machines with little user interaction.
- Proxy Aware - Use PortBlocker in secure network environments.
- macOS Support - PortBlocker now runs on macOS based computers.



## Affected Devices

PortBlocker can filter USB mass storage, MTP, PTP, and UASP (USB Attached SCSI) 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 for users to charge portable devices, such as cell phones via USB.

## Minimum Requirements

- Active SafeConsole account (v5.5.0+)
- Valid PortBlocker license and active subscription per endpoint install
- Windows™ 7, 10, 11 or macOS™ on Intel, M1 or M2 processor with 11.x, 12.x, 13.x (Big Sur, Monterey, Ventura)
- 1Mbps network connection to SafeConsole server for registration and policy updates

## Proxy Requirements

On Windows, PortBlocker uses the WinINET system user's proxy settings. This can be defined either by manual proxy settings, pac script or, Web Proxy Auto-Discovery Protocol. See [Configuring Proxy for PortBlocker](#) for more information.

## Getting Started

There are two components of PortBlocker: the software application on each endpoint and the SafeConsole server. The administrator controls the management of the software installed on users' computers with the SafeConsole management platform.

## Windows Installation

To install, double click PortBlocker-Setup.msi and follow the installation wizard. If you run the installation as an administrator you will not need to reboot.

For a more advanced installation, call PortBlocker-Setup.msi using these optional command line parameters.:



## Installation

`/quiet`

Used for silent installations on new installs and version upgrades.

`/S`

Hides the notification that PortBlocker is already installed

`/norestart`

Prevents the machine from restarting automatically after the installation is completed.

`/forcerestart`

The machine will be restarted after the installation is complete.

`ALLUSERS=1`

Install PortBlocker for all users on the system.

## Registration

`URL=<SafeConsoleConnectionToken>`

The SafeConsole connection token. For greater compatibility, the URL parameter should go at the end of the command.

`EULA=1`

Accept the end-user license agreement on behalf of the user

`USER=<PathUniqueToken>`

Register the PortBlocker Install to a specific path already configured in SafeConsole

ID	Path	Users	Drives	PortBlocker	Policy
1	domain.local	1	8	0	Default
3	portblocker	0	0	1	Default



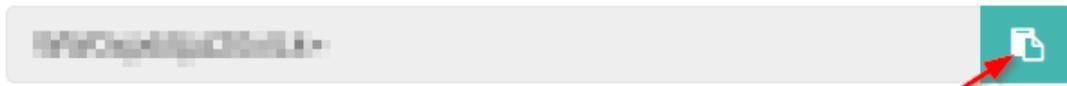
## Unique Registration Token



Using this Unique Registration Token will register your endpoints directly to this path. This will override the workstation's domain path.

Please refer to this support article for additional help with this process: [Endpoint Registration Guide](#)

Path: portblocker



Close

LAUNCH\_CLIENT=1 | 0

Launch Windows client application after installation. The default value is 1 (launch client application). It is recommended to set to 0 (do not launch client application) for mass deployment scenarios to avoid unresponsive client process in the background. The client application should be launched by the user or startup script on user login in this case.

Note: Please consult the [SafeConsole Admin Guide](#) to locate your SafeConsole Connection Token and Unique User Token.

Example:

```
msiexec /i PortBlocker-Setup.msi /quiet EULA=1 ALLUSERS=1 /norestart  
USER=pathuniquetoken URL=https://server.safeconsolecloud.io/connect
```

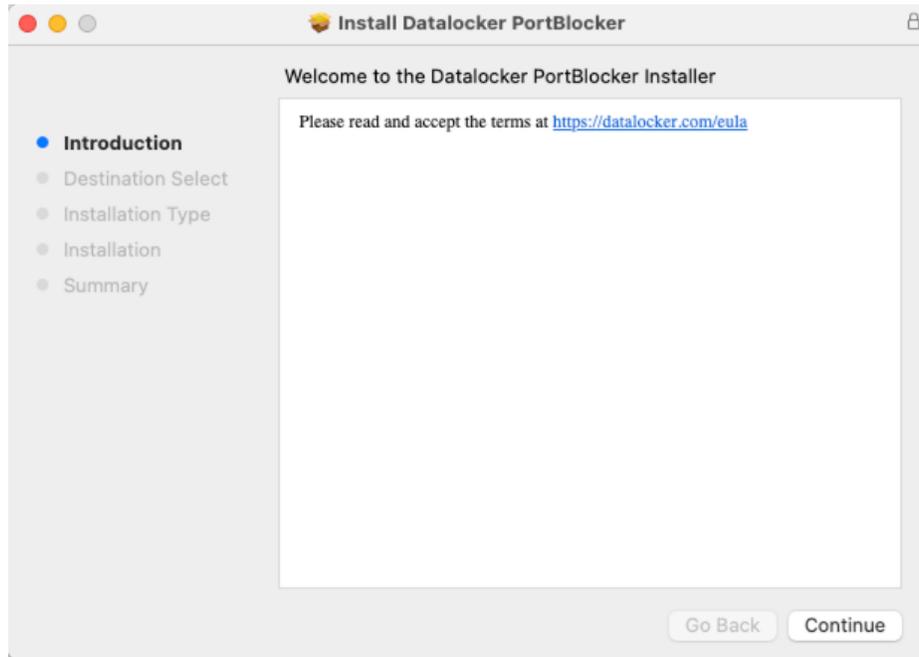
If PortBlocker is installed with these parameters, registration will be attempted after installation. If successful, PortBlocker will automatically apply the appropriate policy from SafeConsole. If unsuccessful, the user will be prompted to complete registration. All affected devices will be blocked until registration is complete. See [PortBlocker MSI Command Line Arguments](#) for more information.



## macOS Installation - Manual and Mass Deployment

### Manual Installation Wizard

PortBlocker for macOS is distributed as a PKG installer inside of a DMG file. To start the installation process double-click on the .dmg file then double-click on Install.pkg.



Follow the installation wizard and agree to the license agreement. You will be prompted to enter your Username and Password to continue.

Note: During installation, you may receive a notification that System Extensions are blocked. As indicated on this notification, open the Security & Privacy System Preferences. Click the lock icon to make changes and re-enter your admin Username and Password. Finally, click Allow to load the blocked software from “Data Locker Inc.”

PortBlocker will now be installed and block all affected devices until registration is complete.

Note: The TeamID to allow the DataLocker Kernel extension is 8D75V5J2K9 if required by your MDM software.

### Enable Full Disk Access for Manual Installations

When installing manually you must give PortBlocker Full Disk Access in the macOS System Settings.

The following steps will enable Full Disk Access on **macOS 13 and later**:

1. Open **System Settings** from the Apple menu.
2. Click the **Privacy & Security** icon in the left-hand menu.
3. Scroll down and select **Full Disk Access**.



4. Click the "+" button and enter your admin password to make changes. Press **Cmd+Shift+G** on your keyboard and navigate to **/usr/local/bin/**
5. Select the **PortBlockerDaemon** and click **Open**.
6. PortBlocker should now have full disk access and can access files and folders on your Mac without restrictions.

The following steps will enable Full Disk Access on **macOS 12 and earlier**:

1. Open **System Preferences** from the Apple menu.
2. Click the **Security & Privacy** icon.
3. Click the **Privacy** tab.
4. Scroll down and select **Full Disk Access** from the left-hand menu.
5. Click on the **lock icon** in the bottom left corner and enter your admin password to make changes.
6. Click the "+" button and press **Cmd+Shift+G** on your keyboard
7. Navigate to **/usr/local/bin/**
8. Select **PortBlockerDaemon** and click **Open**.
9. Click on the **lock icon** in the bottom left corner

PortBlocker should now have full disk access and can access files and folders on your Mac without restrictions.

## macOS Deployment

PortBlocker will look for default values in `com.safeconsole.massdeploy`. These values can be defined by using the following commands. These values should be defined before installing PortBlocker.

```
defaults write com.safeconsole.massdeploy '{
    "url" = https://server.safeconsolecloud.io/connect;
    "eula" = true;
}';

defaults read com.safeconsole.massdeploy "url";
defaults read com.safeconsole.massdeploy "eula";
```

- "user" can be defined with the user unique token if the server settings require a valid user token.

If PortBlocker is not yet registered, it will use these values to attempt registration.

## Mass Deployment - Windows and macOS

For more instructions on implementing mass deployment of either the Windows or macOS version of PortBlocker, please see our mass deployment guides. They can be found here: [DataLocker.com/portblocker/massdeployment](https://DataLocker.com/portblocker/massdeployment)

## Registration

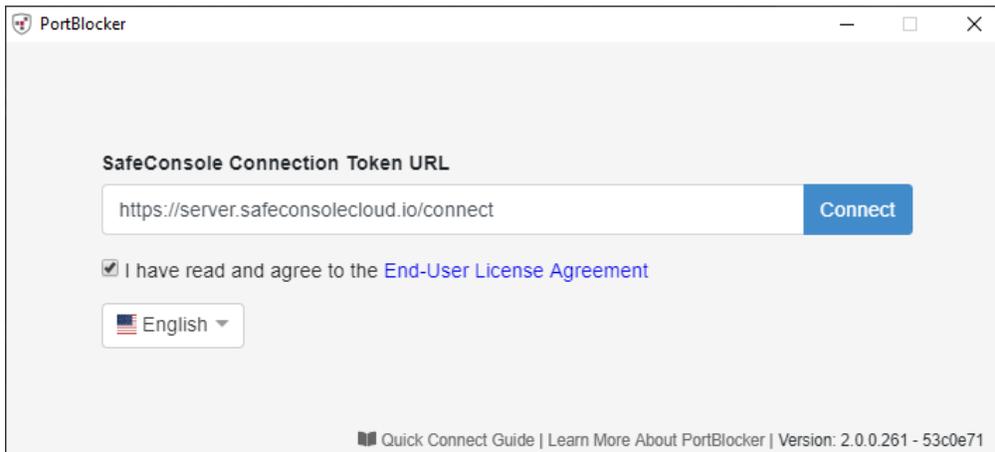
On the first launch, registration will be the only option available. All affected devices will be blocked until registration is completed. See the [Affected Devices](#) section for more details.

If PortBlocker is installed with the registration command line parameters, these steps can be skipped.

To register your application:



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



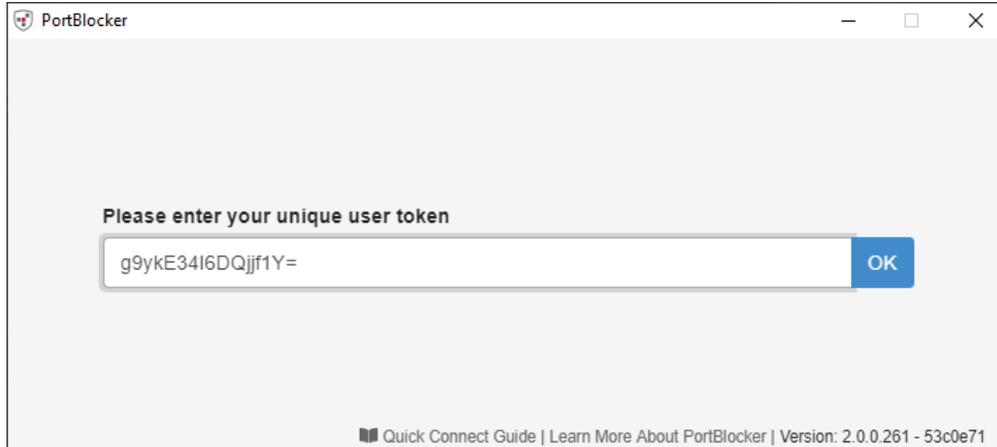
2. Select the desired language.

Note: Changing the language requires PortBlocker to be restarted.

3. Review and accept the EULA by selecting the checkbox and click Connect.

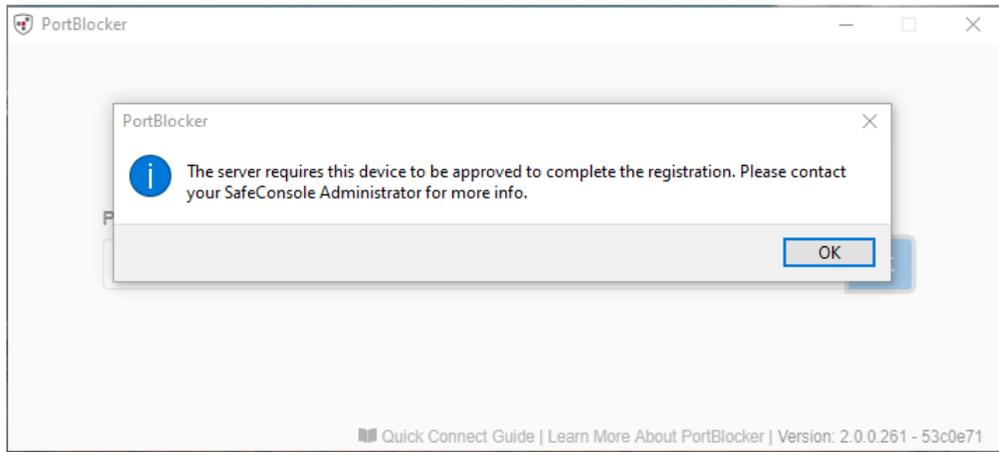
Any optionally enabled policies will appear at this point. For more information on these policies, see [Server Settings](#).

- Unique User Token:





- Administrator Registration Approval:



- 4. PortBlocker will register the application and apply the appropriate policies. The client will show the Settings page by default.

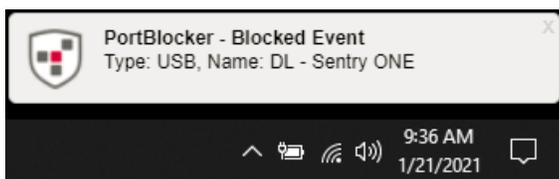


## Expected Behavior

A SafeConsole Admin can set policies that will match USB devices to one of three behaviors.

### Blocked

When a device, which is set to Blocked, is inserted into the computer, the device will not be mounted. No data will be able to be transferred in this state. If configured, PortBlocker will display a notification indicating that the device was blocked.



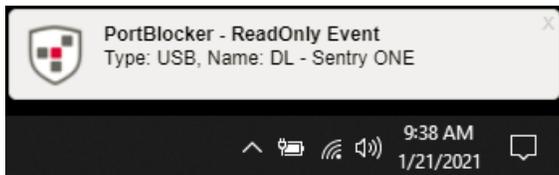


## Read Only

When a device, which is set to Read Only, is inserted into the computer, the device will be mounted. No data will not be able to be transferred to the device in this state. If configured, PortBlocker will display a notification indicating that the device is in read-only mode.

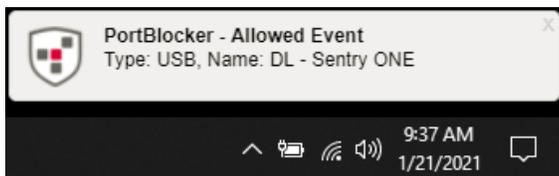
It is recommended that when used in conjunction with SafeConsole Ready Devices, the device should be put into read-only mode through the device policy and full-access should be granted for the device in PortBlocker.

Warning: Some hardware devices, such as cameras and phones will present their own file system controls to the operating systems. In these situations, the user will still have full read-write access to the device. For maximum security, it is recommended to completely block these devices to prevent users from writing to the file system.



## Full Access

When a device, which is set to Full Access, is inserted into the computer, the device will be mounted like normal. No modifications will be made to limit data transfer. If configured, PortBlocker will display a notification indicating that the device was allowed.



Note: Allowed event notifications will be shown for all USB devices.

## User Interface

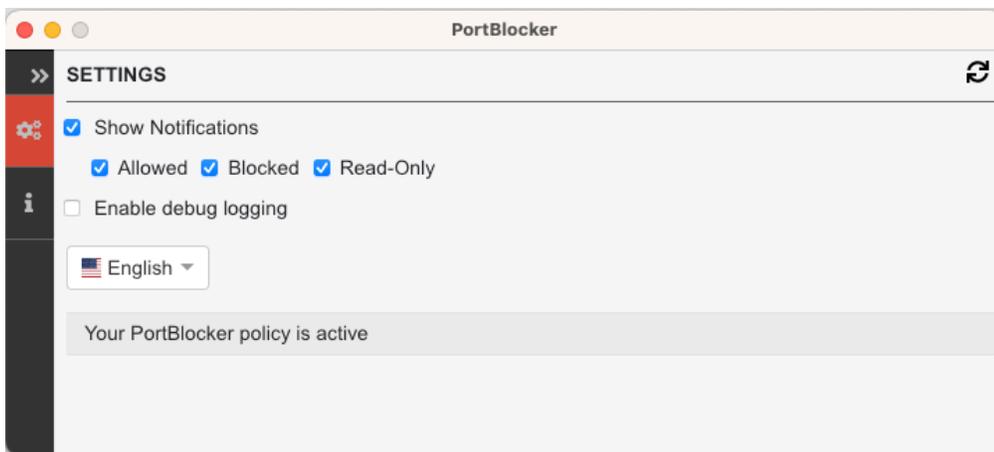
Launching the PortBlocker application will allow users to interact with PortBlocker, including managing optional settings.

## Settings Tab

There are several options for configuring the settings on the PortBlocker application. 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.



### Windows User Interface



### macOS User Interface

## 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. Notifications are shown when a device is inserted into the user's machine, with information regarding the status of the inserted device. The user can control which notifications will be displayed by checking or unchecking Allowed, Blocked, Read-Only, Unfilterable (Windows only) checkboxes. Clicking on the notification will bring up the client.

This setting can be controlled with the PortBlocker policy in SafeConsole.

## Enable debug logging

Checking the Enable debug logging option will write the application logs to the local machine for investigation. Reboot might be needed to enable driver level logging. DataLocker Support may ask that you enable this for troubleshooting purposes.



## Language

Allows changing the language of the PortBlocker User Interface.

Note: Changing the language requires PortBlocker to be restarted.

## Policy Updates

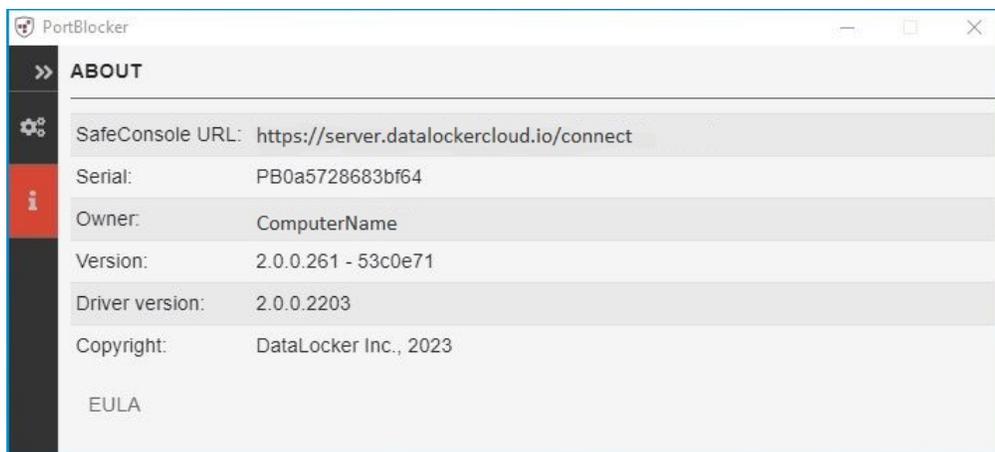
The policy will update when the Refresh icon is clicked. Automatic updates are applied every 10 minutes by default, even when the client is closed. The refresh frequency can be updated in the PortBlocker policy settings in SafeConsole. If you wish to update the policy manually, click the Refresh icon 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 icon 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 application is registered to
- Serial number of the application
- Owner of the application
- Version number



- Driver version
- Copyright information

A copy of this information can be provided to support during additional troubleshooting.

A link to the EULA is listed below the technical details.

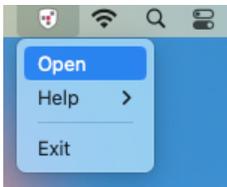
## Tray (Menu Bar) Icon

PortBlocker launches automatically on startup, displaying a tray icon on Windows or menu bar icon on macOS.

On Windows, clicking on the tray icon or selecting the application from the start menu will bring up the client.



On macOS, clicking on the menu bar icon and selecting Open or clicking on the application from the Application folder will bring up the client. Note: If the Show Notifications option is disabled, the menu bar icon will not be present when a device is plugged in.



## Managing With SafeConsole

PortBlocker is a forced managed application, meaning it must be used in conjunction with the SafeConsole Management Platform. Managing PortBlocker with SafeConsole allows administrators to control which devices are allowed or blocked, set policies for different groups, see audit logs and activity, and much more.

SafeConsole allows administrators to set policies to manage PortBlocker. This manual will only cover the policies directly related to PortBlocker. For more information on the other SafeConsole policies, see the complete [SafeConsole Admin Guide](#).

## Licensing

PortBlocker requires an active SafeConsole subscription and one available license seat per endpoint. Users without access to a management server, please contact the DataLocker Sales Department by emailing [sales@datalocker.com](mailto:sales@datalocker.com) or calling +1 (913) 310-9088. For customers in EMEA please email [eulicensing@datalocker.com](mailto:eulicensing@datalocker.com) or call +31 467 111 205.

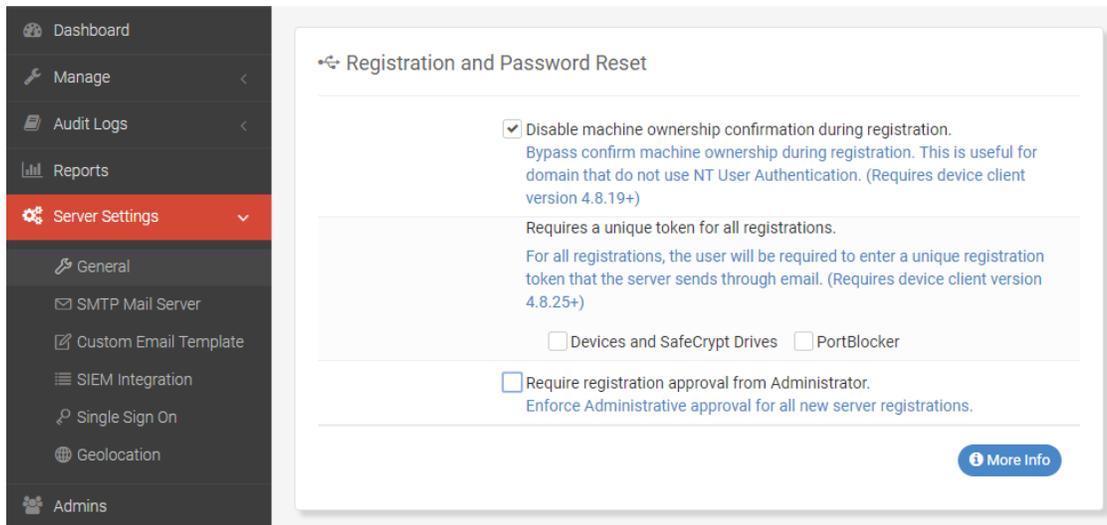
If a SafeConsole license becomes invalid, all affected devices will be blocked. A message stating that the SafeConsole license is out of compliance will be shown on each endpoint. Please contact [licenseteam@datalocker.com](mailto:licenseteam@datalocker.com) to resolve this. If the product is no longer being licensed, it should be uninstalled and removed from the system.



To free up a SafeConsole license, the uninstaller must be run while a valid connection to SafeConsole can be established.

## Server Settings

Several server settings are applicable to the PortBlocker application and can be found by clicking on the Server Settings button on the side menu in SafeConsole and going to General.



Applicable settings:

- **Require Registration Approval from Administrator (checkbox):** Requires an administrator's approval before PortBlocker can be registered. See the [SafeConsole Admin Guide](#) on where to approve registration.
- **Require Unique User Token (checkbox):** Requires users to input their unique user token during registration, obtained from the administrator. See the [SafeConsole Admin Guide](#) on where to find the Unique Token.
- **Disable ALL Device Audit Logs (checkbox):** Prevents the server from logging all PortBlocker application activities. This setting can only be changed by the SafeConsole account owner.
- **Disable ALL System Audit Logs (checkbox):** Prevents the server from logging all administrator and system activities. This setting can only be changed by the SafeConsole account owner.
- **Device List Limit (input field):** Controls Device List items to show in the PortBlocker policy (default: 3000). If the Device List is not visible in the PortBlocker policy, increase this value to display all Device List entries.

## Endpoint Actions

These allow the administrator to perform actions on one endpoint at a time. These actions can be located by clicking Manage -> PortBlocker on the left side menu, and then clicking the blue Action menu in the affected endpoint's row.

The following actions are available, however, depending on the circumstances, all may not show up in all instances.



- **Approve:** Approves registration so users can register their PortBlocker application.
- **Allow all devices as Read-only:** Sets the endpoint to all devices in a read-only state. See [Read Only](#) for more information. This action overwrites all policy allow list settings.
- **Block all devices:** Sets the endpoint to deny all devices. This action overwrites all policy allow list settings.
- **Allow all devices:** Sets the endpoint to allow all devices. This action overwrites all policy allow list settings.
- **Restore Status:** Undoes temporary or pending actions.
- **Reset:** Unregisters the endpoint from SafeConsole, removing all policies and denying access to all devices. If PortBlocker was installed using the registration command line parameters, registration will be attempted again immediately following the reset. To avoid this, PortBlocker will need to be uninstalled. See [Uninstalling PortBlocker](#) for more information.

## Policies

1. Access the Policy Page by clicking Manage, then Policies on the left side menu.
2. Click the relevant custom policy or default policy that is applied to the affected PortBlocker endpoint.
3. Navigate to the PortBlocker tab within the policy editor to see available policies.

## PortBlocker

Click on the PortBlocker section to see, add, and remove devices.

The list of devices will appear nested and administrators can expand the menu by clicking the dropdown arrows. For more information on adding a device, see the [Device List](#) section.



Policy Editor > Modify Default Policy Save

v6.x K300 K350 DL3/DL3FE DL4FE SafeCrypt **PortBlocker** v4.8.x

---

**PortBlocker** PortBlocker seats used 1 / 100 default

**Device List**   + Add New Import CSV

> **SafeConsoleReady Devices** Vendors: 0 / 3 Types: 0 / 25 Serials: 0 / 0

**Custom Entries:** ⚠ No custom entries have been added.

Set all unlisted devices to Read-Only  
Select this checkbox to allow Read-Only Access for all devices marked as Blocked and also devices that are unlisted.  
⚠ Please use with caution. Read-Only Access only applies to compatible storage devices.

Protect PortBlocker installation from unauthorized uninstalls with password  
1.4+

Automatically Check For Updates  
PortBlocker will automatically check if a new version is available.  
1.5+

Hide Client (Background Stealth Mode)  
PortBlocker will remaining hidden in the background. The Client UI and Notifications will be inaccessible.  
1.6+

Use Custom Policy Refresh Interval  
Customize the timing of the Automatic Policy Refresh  
1.6+

Minimum Interval (minutes):   
This value is used as a base to calculate the actual refresh interval (in minutes).

More Info

---

**User Defaults** default

**Audits** default

**GeoFence** default

**Trusted Network** default

⚠ Danger Zone



## Uninstall Password

PortBlocker can be restricted from unauthorized uninstallation through the use of an uninstall password. You can set the Uninstall password through the PortBlocker policy on SafeConsole. This password can be generated using the provided random password generation tool or manually assigned by the SafeConsole Administrator.

The screenshot shows a configuration panel for PortBlocker. At the top, there is a checkbox labeled "Protect PortBlocker installation from unauthorized uninstalls with password" which is checked. Below the checkbox is a version indicator "1.4+". The main area contains a "Password:" label followed by a text input field containing the password "dmsAU6HHNNjn". To the right of the input field is a refresh button (circular arrow icon). Below the input field, there is a blue text note: "Uninstallation and removal of PortBlocker will require this password."

To set the PortBlocker uninstall password:

1. Navigate to the Policy editor. See [Policies](#) for more information.
2. Click the Protect PortBlocker installation from unauthorized uninstalls with password checkbox.
3. Manually input your desired password or click the Refresh button to randomly assign a password.
4. Click Save in the upper right.

## Hide Client (Background Stealth Mode)

If enabled in the policy, PortBlocker will remain hidden in the background. The user interface and notifications will be inaccessible.

## Custom Policy Refresh Interval

Automatic policy refresh interval can be increased or decreased in the policy. Default value: 10 minutes.

## User Defaults

The User defaults policy allows management of the user interaction with PortBlocker.

- Pre-Selected Language
  - Pre-set PortBlocker language instead of using the language of the host machine to test language settings.
  - For deployment the language must be set during the installation.
- Notification policy
  - User Configurable (default) - Allows the end user to modify the notification settings locally.



- Always Notify - Enables desktop notifications to always appear on the user's computer. If this option is enabled inside SafeConsole, the end-user will not be able to modify it locally.
- Never Notify - Disables desktop notifications from appearing on the user's computer. This option ensures that PortBlocker functions silently on the user's computer. If this option is enabled inside SafeConsole, the end-user will not be able to modify it locally.

## Audit Logs

PortBlocker sends audit logs to the SafeConsole server for administrators to see.

Q Audits default

Enable activity audits  
[Select this checkbox to capture an audit log of all PortBlocker endpoint activities \(allowed, blocked, status changes, reset, etc.\).](#)

The following logs are reported when PortBlocker:

- is registered to the server (with token)
- has been reset
- has blocked a device
- has allowed a device
- has allowed a device in read-only mode
- has allowed an unlisted device in read-only mode
- has been set to allow all devices
- has been set to block all devices
- has been set to allow all devices in read-only mode
- needs registration approval

Information that is sent with the logs include:

- Timestamp
- User Login and Owner info
- Computer Name and IP
- VID/PID of Device
- Device Serial Number
- Device Hardware Name

To manage the audit log settings:

1. Navigate to the Policy editor. See [Policies](#) for more information.



- Click the Device Audits heading.
- Select the checkbox if you would like to enable auditing for all instances of PortBlocker being managed by the selected policy.

Note: This setting will be overridden if the Disable ALL Device Audit Logs server setting checkbox is checked. See [Server Settings](#) for more information.

## GeoFence

Geofencing can be used to prevent devices from connecting outside of certain parameters. If an endpoint is outside the set parameters, all devices will be denied access.

GeoFence <span style="float: right;">default</span>	
	<input checked="" type="checkbox"/> Enable Geofencing on devices. <small>Prevent device access based on user computer IP Address through Geofence. Geolocation data such as Country and ISP of the IP Address can also be used to control device access.</small>
Geofence message to user:	<input type="text" value="This PortBlocker Endpoint has been set to blocked all devices through Geofence!"/> <small>Send a custom message to users when their PortBlocker Endpoints has been set to blocked all devices through Geofence policy.</small>
IP Addresses:	<input type="text" value="All IP Addresses Allowed"/> <small>Separate multiple IP Addresses with commas (198.51.100.1,198.51.100.2). Wildcard and CIDR addresses are supported (198.51.100.* or 198.51.100.0/24)</small>
Restriction Mode:	<input type="radio"/> Allow Only These IPs (Whitelist) <input checked="" type="radio"/> Restrict These IPs (Blacklist)
Countries:	<input type="text" value="No Countries Blocked"/>
Restriction Mode:	<input checked="" type="radio"/> Allow Only These Countries (Whitelist) <input type="radio"/> Restrict These Countries (Blacklist)
ISP:	<input type="text" value="No ISPs Blocked"/> <a href="#">Add ISP</a>
Restriction Mode:	<input checked="" type="radio"/> Allow Only These ISPs (Whitelist) <input type="radio"/> Restrict These ISPs (Blacklist)
<a href="#">More Info</a>	

PortBlocker can allow or block endpoints by:

- IP Address
- Country
- ISP



## Trusted Network

Trusted Network can be used to create a trusted zone in which other policies can be used to restrict or provide extra convenience for endpoints being used within it. If an endpoint is outside the trusted zone, the registration to SafeConsole will be denied. Note: Trusted Network settings do not affect already registered endpoints.

**Trusted Network** default

By default, all live connections to the SafeConsole Server are considered to be in the Trusted Network and thus the Trusted Zone.

Enable Trusted Network Restrictions  
Trusted Network is a way for admins to create a Trusted Zone in which other policies can use to either restrict or provide extra convenience or features depending if an endpoint is unlocked inside or outside the Trusted Zone.  
To register an endpoint, the user will need to make a connection to SafeConsole from inside the Trusted Network.

IP Addresses:	<input type="text" value="All IP Addresses Allowed"/> <small>Separate multiple IP Addresses with commas (198.51.100.1,198.51.100.2). Wildcard and CIDR addresses are supported (198.51.100.* or 198.51.100.0/24)</small>
Countries:	<input type="text" value="All Countries Allowed"/>
ISP:	<input type="text" value="All ISPs Allowed"/> <a href="#">Add ISP</a>

Trusted Network allows a trusted zone to be created by:

- IP Address
- Country
- ISP

## Danger Zone

Danger Zone is the button at the bottom of the Policy Editor window. Clicking this button will remove and reset all policies back to the default.

## Device List

SafeConsole Admins can select which devices are allowed, blocked, or forced into read-only mode. This can be configured by device type or serial number. Devices not on the list can either be blocked or forced into read-only mode.

Note: For SafeConsoleReady Devices, it is recommended to allow Full Access to the models used in your environment. If it is desired to use these devices in a read-only state the PortBlocker policy should be left in Full Access and that the device policy should make use of the Write Protection Policy. For more information see the [SafeConsole Admin Guide](#).



## SafeConsoleReady Devices

SafeConsoleReady Devices are pre-populated to the PortBlocker device list, this allows an easy starting point on creating your PortBlocker policy.

1. Within SafeConsole, navigate to the Policies page. This is listed under the Manage tab on the left side menu.
2. Locate the policy to be used for PortBlocker and click Modify. If the default policy is being used, this can be found by navigating to the Policy page and clicking Modify Default Policy. If a custom or inherit policy is being used, navigate to the Policy page, click the policy desired, then click Modify Custom Policy.
3. At the top of the Policy Editor window, click the PortBlocker tab.
4. In the PortBlocker section, all SafeConsoleReady devices are already defined. Each device can either be configured for Full Access, Read-Only, or Blocked. If devices from the same vendor are configured for different actions, then the label will show Custom. Changing the label for a vendor will change all devices for that vendor.

PortBlocker seats used 63 / 999 default

### Device List

+ Add New Import CSV

- SafeConsoleReady Devices Vendors: 3 / 3 Types: 0 / 23 Serials: 0 / 0
  - Kingston - 0951 Types: 0 / 8 Serials: 0 / 0 (Full Access)
  - DataLocker - 230A Types: 0 / 14 Serials: 0 / 0 (Full Access)
  - Origin - 3059 Types: 0 / 1 Serials: 0 / 0 (Full Access)
- Custom Entries Vendors: 2 / 15 Types: 2 / 21 Serials: 0 / 20
  - Yodoo - 1993 Types: 2 / 3 Serials: 0 / 3 (Custom)
  - Andalex (2003) (Full Access)
  - Voltsillam (2005) (Read-Only)
  - Wrapsafe (2009) (Blocked)
  - Bluejam - 1994 Types: 0 / 1 Serials: 0 / 1 (Blocked)
  - Flashdog - 1997 Types: 0 / 1 Serials: 0 / 1 (Full Access)
  - Roomm - 1998 Types: 0 / 1 Serials: 0 / 1 (Read-Only)

## Adding Serial Numbers

To add SafeConsoleReady devices individually by serial number, click the + next to the device name. This will allow a serial number to be entered for the specified device. Once one serial number is defined, only the entered serial numbers will be allowed for that device. Defined serial numbers are shared between policies. If the serial number has already been entered, simply select it from the table.



SafeConsoleReady Devices Vendors: 3 / 3 Types: 0 / 23 Serials: 0 / 4

- Kingston - 0951 Types: 0 / 8 Serials: 0 / 0
- DataLocker - 230A Types: 0 / 14 Serials: 0 / 4
  - H300 Basic (1011)
  - H300 Enterprise (1012)
  - H350 Basic (1015)
  - H350 Enterprise (1016)
  - (1515641) new
  - (4521364) new
  - (5443214) new
  - (7861539) new
  - DL3 (1180)

When adding a device by serial number a custom Entry Name can be defined, to help identify a device by something other than the serial number. To remove a serial number click the red x next to the serial number. When all serial numbers are removed the policy will revert back to allowing all serial numbers for that device type.



### Add New Serial Number to the Custom Entry ✕

VID:   

- Required - Enter the 4 character of the device's VID.

Vendor:   

- Optional - Enter the vendor's name for this VID.

PID:   

- Optional - Enter the 4 character of the device PID. Leave blank to allow all PIDs for this VID.

Product Name:   

- Optional - Enter a name for this device's VID+PID combination.

Serial Number:   

- Optional - Enter the device's serial number for this VID+PID combination. Leave blank to allow all device serial numbers.

Entry Name:   

- Optional - Enter a name for this Serial Number entry.

## Set all unlisted devices to Read-Only

After the initial installation of PortBlocker, no affected devices will be allowed until they are added to the Device List and set to allowed unless Set all unlisted devices to Read-Only checkbox selected. If selected, undefined devices will be mounted as read-only instead of blocked.

Note: If devices are marked blocked in the Device List when this setting is enabled, then those devices will be allowed in read-only mode.

Warning: Some hardware devices, such as cameras and phones will present their own file system controls to the operating systems. In these situations, the user will still have full read-write access to the device. For maximum security, it is recommended to completely block these devices to prevent users from writing to the file system.



## Other Devices

All USB storage devices can be defined in the policy, however, the process for adding them to the Device List is different than adding a SafeConsoleReady device. If the VID and PID are known, skip to the [Custom Device](#) section. To find the VID and PID, see the steps below.

### Finding The VID, PID, and Serial Number

1. Make sure audit logging is enabled. For more information, see [Audit Logs And Reports](#).
2. Plug in a USB device to the computer and wait for PortBlocker notification.
3. Once the notification is shown, view the audit logs on SafeConsole by clicking Audit Logs on the left side menu and then clicking User Audit Logs.
4. Find the PortBlocker action and view the Data column.
5. The device's VID and PID are listed there. Keep in mind that VIDs and PIDs are always four characters and will only contain the numbers 0-9 and letters A-F.

When	Path	Computer	Login	Product	Device ID	Action	Data
From							
6 hours ago	non-domain	DataLockerQA-PC	DataLockerQA-PC\DataLockerQA	PortBlocker	PBd5ef0ddd37dd2	PortBlocker Blocked	USB\VID_230A&PID_1550&REV_0100

Example:

- VID: 230A
- PID: 1550
- sn: C7ECB2403

## Custom Device

### Quick method

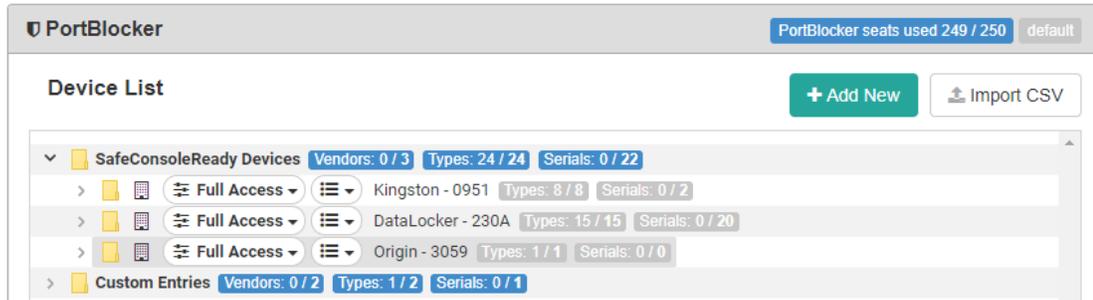
Custom devices can be added directly from the User Audit Logs table, this is where they will show up if blocked. This is the quickest method for adding custom devices to your policies

1. Navigate to Audit Logs - User Admin Logs
2. Locate a device you would like to add to the policy list
3. In the Data column click on the wrench icon
4. Select Add Device to List
5. Add New Custom Entry dialog opens and the device information is prefilled
6. Click Add



## Manual method

1. Within the PortBlocker section of the Policy Editor, click the Add New button.



2. Enter the device information.

Only the VID box is required. Entering only the VID will define all devices with the registered VID. To further limit device use, add the PID as well.

### Add New Custom Entry

VID:

- Required - Enter the 4 character of the device's VID.

Vendor:

- Optional - Enter the vendor's name for this VID.

PID:

- Optional - Enter the 4 character of the device PID. Leave blank to allow all PIDs for this VID.

Name:

- Optional - Enter a name for this device's VID+PID combination.



3. Adding both the VID and PID will display the Serial Number field, which allows restricting by serial number. If only the VID is entered, the Serial Number field will be hidden.

### Add New Custom Entry ✕

VID:   

- Required - Enter the 4 character of the device's VID.

Vendor:   

- Optional - Enter the vendor's name for this VID.

PID:   

- Optional - Enter the 4 character of the device PID. Leave blank to allow all PIDs for this VID.

Name:   

- Optional - Enter a name for this device's VID+PID combination.

Serial Number:   

- Optional - Enter the device's serial number for this VID+PID combination. Leave blank to allow all device serial numbers.



## Importing CSV

Administrators can add device types to the device list by importing a CSV file. To do this, click the Import CSV button and upload a file.

**Import PortBlocker Entries from CSV file** ✕

Your CSV file should contain the following fields: vendor\_name, vid, device\_name, pid, serial

Select CSV File:

The first line should contain vendor\_name, vid, device\_name, pid, and serial, with each entry in a new column

## Uninstalling PortBlocker

Uninstalling PortBlocker requires having admin permission to the local computer and (optional) the PortBlocker uninstall password. The PortBlocker Uninstall password will be found in the PortBlocker policy in SafeConsole.

Warning: Uninstalling PortBlocker on a Windows 7 computer which does not fully support SHA-2 code signing, will require the computer to initially reboot to a recovery prompt. After an automatic repair is done, the computer will be able to boot back to the Windows Desktop. To avoid this please make sure [KB4474419](#) is installed before uninstalling PortBlocker

### Windows Uninstall:

1. Go to the Control Panel, located in the Start menu, and click Programs and Features.
2. Locate PortBlocker and click Uninstall/Change.
3. If required, enter the uninstall password into the wizard and proceed.
4. (Optional) check CLEAN ALL to remove all leftover files, such as logs and configs.

Once completed, PortBlocker will be removed from the computer. Uninstalling PortBlocker will free up a license seat (if there is an active connection to the SafeConsole server) and all devices will be allowed access.



## Uninstalling from Command Line

To uninstall PortBlocker from the command line execute the following command.

```
msiexec /x PortBlocker_x64.msi /quiet
```

If the uninstall password option was enabled in the policy, append the following to the line above during uninstall:

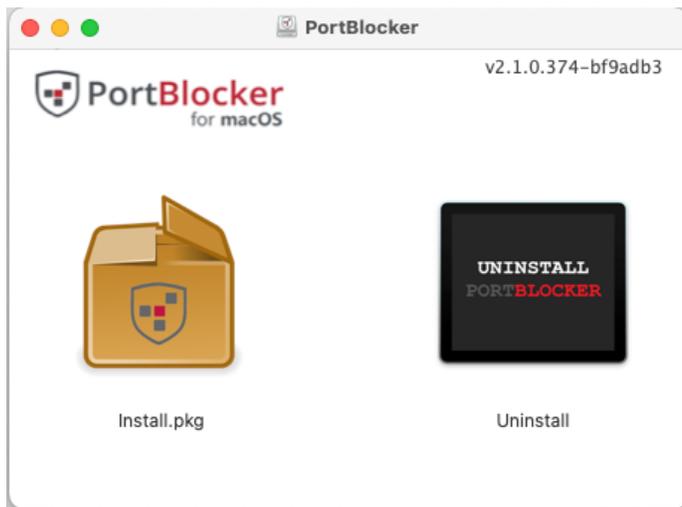
```
PASSWORD=<UninstallPassword>
```

Optional: To remove all leftover files, such as logs and configs, append the following to the line above during uninstall.

```
CLEANUP_ALL_DATA=1
```

## macOS Uninstall

Use the downloaded DMG file and double click Uninstall and follow any instructions shown.

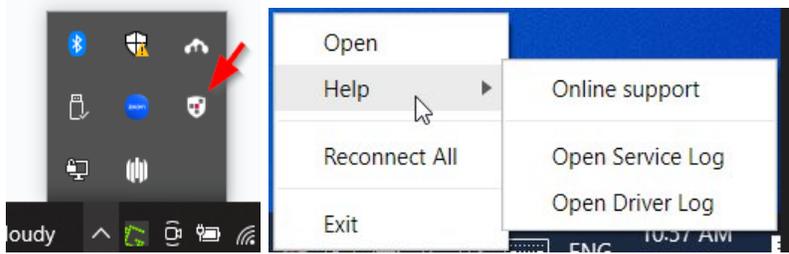


## Troubleshooting

For help troubleshooting PortBlocker issues, visit the [PortBlocker Support Page](#). DataLocker Support may ask you to share the Portblocker Service and Driver Logs.

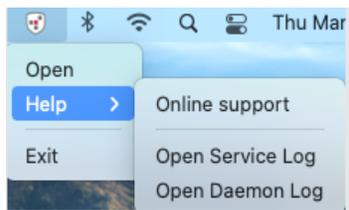
How to access the PortBlocker logs (Windows):

1. In the System tray right click on the PortBlocker icon
2. In the Portblocker menu popup select > Help
3. You should see the Open Service Log and Open Driver Log options
4. Click on the log file to open.
5. Save the file and email to DataLocker Support.



### How to access the PortBlocker logs (macOS)

1. On the Menu Bar click on the PortBlocker icon.
2. In the Portblocker menu popup select > Help.
3. You should see the Open Service Log and Open Daemon Log options.
4. Click on the log file to open.
5. Save the file and email to DataLocker Support.





## Document Version

The latest version of this document resides at

[https://media.DataLocker.com/manuals/portblocker/portblocker\\_admin\\_guide.pdf](https://media.DataLocker.com/manuals/portblocker/portblocker_admin_guide.pdf)

This document was compiled on Nov 9, 2023

## Notices

DataLocker is continuously updating its products, the images and text in this manual may vary slightly from the images and text displayed by your device. These changes are minor and should not adversely affect the ease of setup.

## Disclaimer

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, DataLocker Sentry, and the DataLocker logo are registered trademarks of DataLocker Inc. and its subsidiaries. All other trademarks are the property of their respective owners. All rights reserved.

## Patents

Patent: [DataLocker.com/patents](https://www.DataLocker.com/patents)