# PortBlocker Admin Guide

*DataLocker Inc.*

*September 2020*

**PortBlocker**

# Contents



# About PortBlocker USB Port Control

PortBlocker by DataLocker is a managed solution that allows central management of USB mass storage devices through SafeConsole. It is a straightforward approach to preventing data breaches and keeping malware out of your workstations.

PortBlocker makes sure only allowed devices may be mounted as USB mass storage devices on the computers on which it is installed. This stops usage of insecure and unaudited USB drives and mass storage devices and ensures that viruses running on insecure USB devices cannot infect the computer or network. PortBlocker will also log all 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 in Active Directory. 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 Device Audit Logs.
- **Automatic Refresh** - PortBlocker automatically receives policy updates from SafeConsole every 10 minutes or manually as needed.
- **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 or macOS™ 10.13, 10.14, 10.15
- 1Mbps network connection to SafeConsole server for registration and policy updates

#### Proxy Requirements

On Windows, PortBlocker uses the WinINET (Internet Explorer) 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.

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=<UniqueToken>
```

OPTIONAL, register the PortBlocker Install to a specific user already in SafeConsole

```
SET_UNINSTALL_PASSWORD=<PortBlockerUninstallPassword>
```

OPTIONAL, requires the password to be entered when attempting to uninstall PortBlocker. The password would be requested later to be typed in the UI (or PASSWORD switch could be used to provide this password through the command line on uninstall). If a password is not defined during installation, the uninstall password will need to be obtained by contacting support@datalocker.com.

```
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:

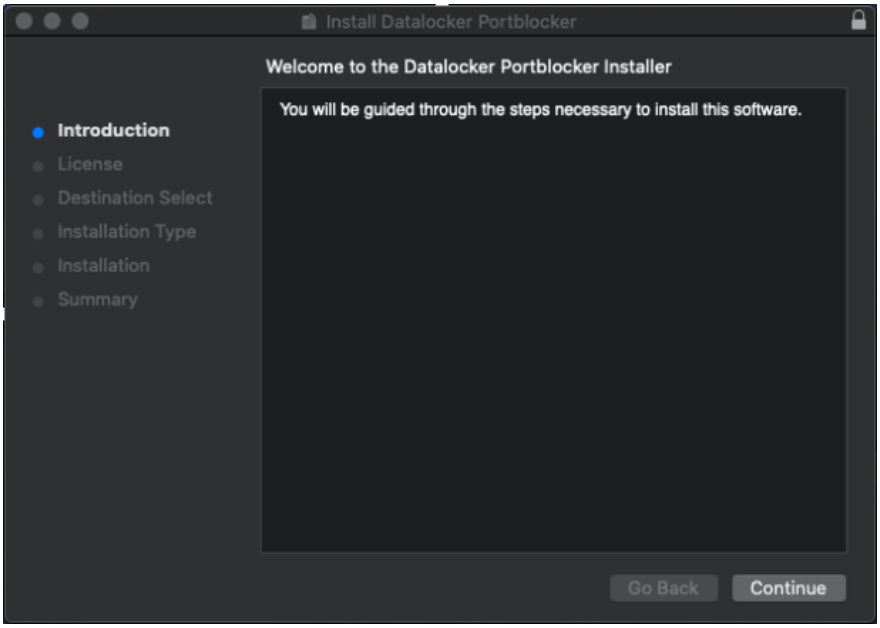
```
msiexec /i PortBlocker-Setup.msi /quiet EULA=1 ALLUSERS=1 /norestart
SET_UNINSTALL_PASSWORD=Secret URL=https://pbtest01.safeconsolecloud.io/connect
```

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.

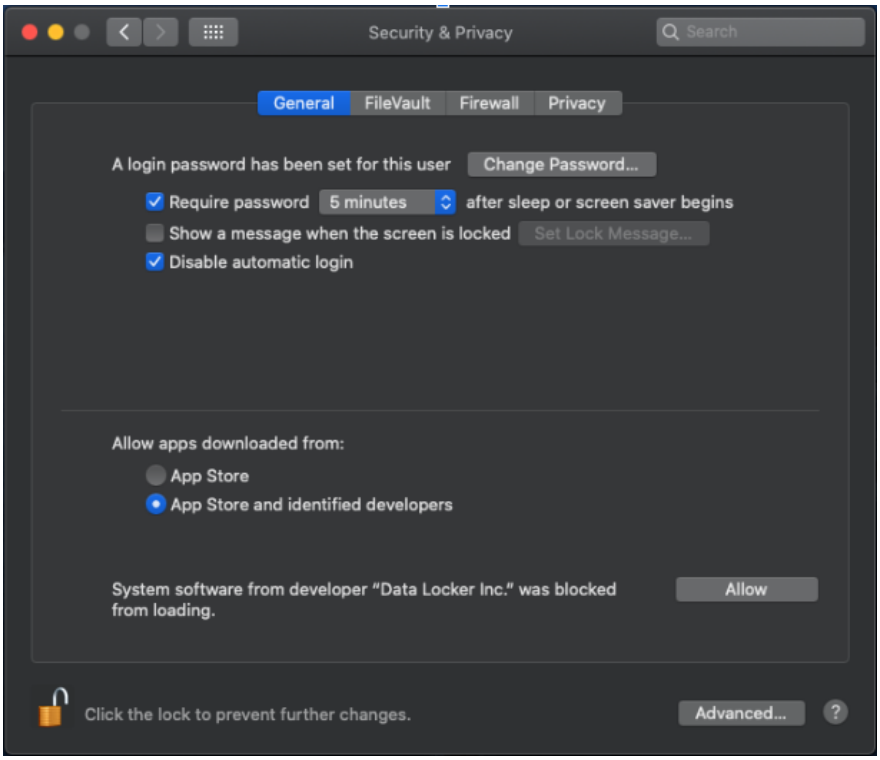
## macOS Installation

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 User Name and Password to continue. 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 User Name 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 **123ASDQWE** if required by your MDM

software.

#### 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.datalocker.portblocker "url";
defaults read com.datalocker.portblocker "eula";
```

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

It is also possible to pass these arguments to PortBlocker that is already installed

```
open /Applications/PortBlocker.app --args --eula
     --url=https://server.safeconsolecloud.io/connect
```

**Note:** –eula does not need =1 added to the parameter.

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

## Mass Deployment

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

## Registration

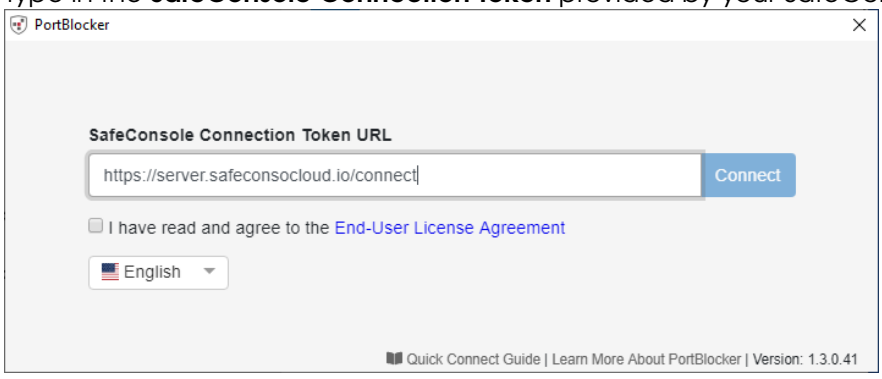
On the first launch, registration will be the only option available. **All affected devices will be blocked until registration is completed.** See the Affected Devices section for more details.

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.



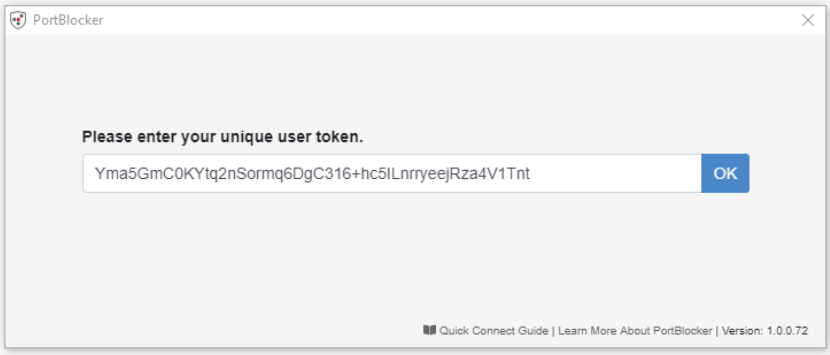

2. Select the desired language.

   **Note:** Changing from the default may require PortBlocker to be restarted.

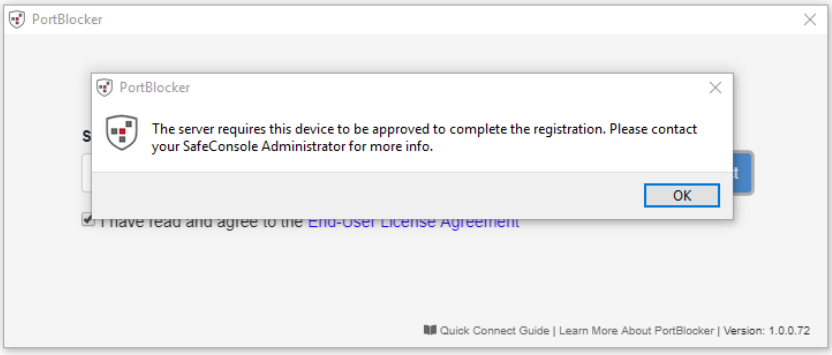
3. Check the **EULA** checkbox and click **Connect**.

   Any optionally enabled policies will appear at this point. For more information on these policies, see Server Settings.

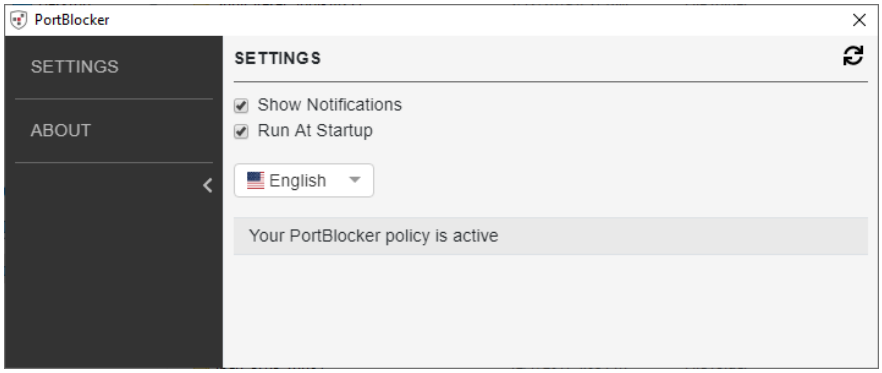
   - Unique User Token:




   - 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

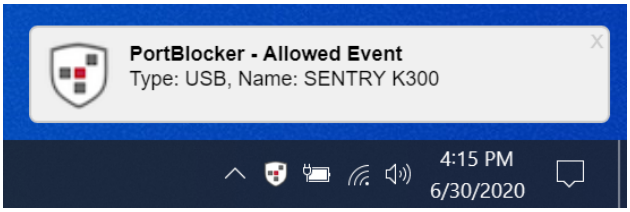
When a device, which is set to *Read Only*, is inserted into the computer, the device will be mounted. No data will not be able to be transferred to the device in this state. If configured, PortBlocker will display a notification indicating that the device is in read-only mode.

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.



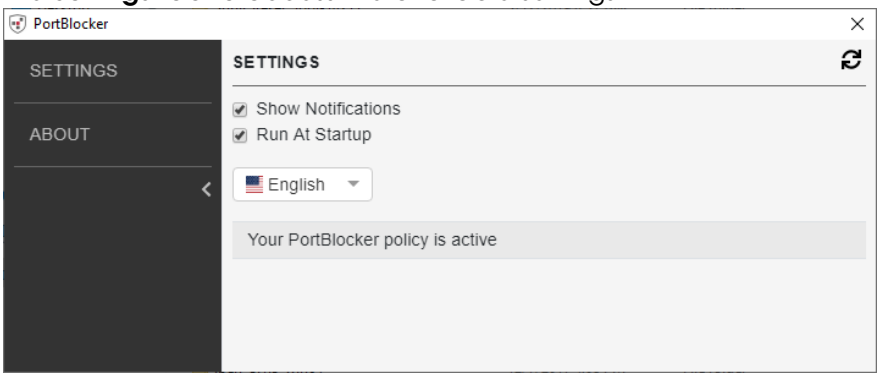
**Note:** Allowed event notifications will be shown for all USB devices.

# 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.




### 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. Clicking on the notification will bring up the client.

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

### 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 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.

### Language

Allows changing the language of the PortBlocker User Interface.

**Note:** Changing from the default may require PortBlocker to be restarted.

### Policy Updates

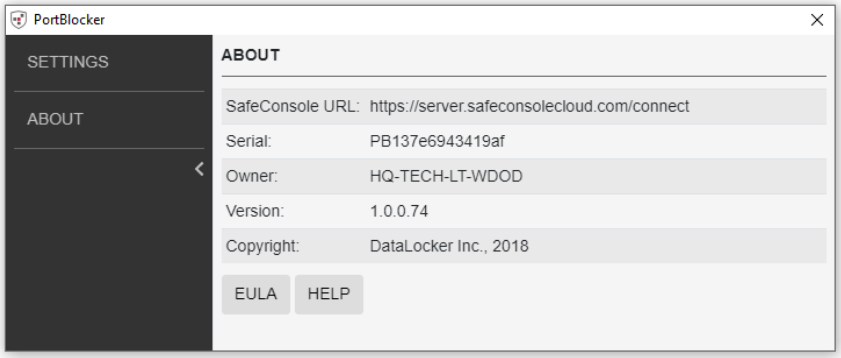
The policy will update when the **Refresh** icon is clicked. Automatic updates are applied every 10 minutes, even when the client is closed. If you wish to update the policy manually, click the **Refresh** icon at the top right.

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 application is registered to
- Serial number of the application
- Owner of the application
- Version number
- Copyright information

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

EULA and Help links are listed below the technical details.

## 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 device is plugged in or the administrator issues a reset command.

# 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

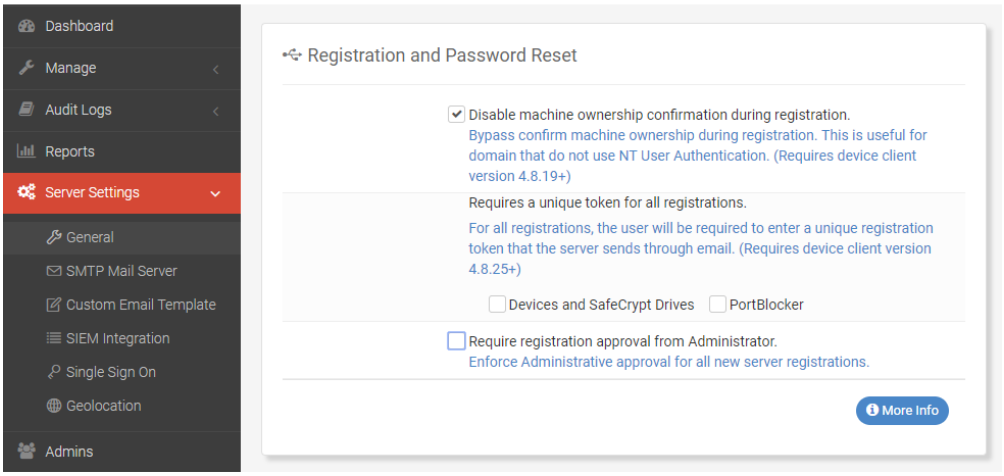
PortBlocker requires an active SafeConsole subscription and one available license seat per endpoint. Users without access to a management server, please contact the DataLocker Sales Department by emailing sales@datalocker.com or calling +1 (913) 310-9088. For customers in EMEA please email euLicensing@datalocker.com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

If a SafeConsole license is currently or 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 licensing@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.

## 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** box 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.
- **Disapprove:** Disapproves registration so users will be unable to 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

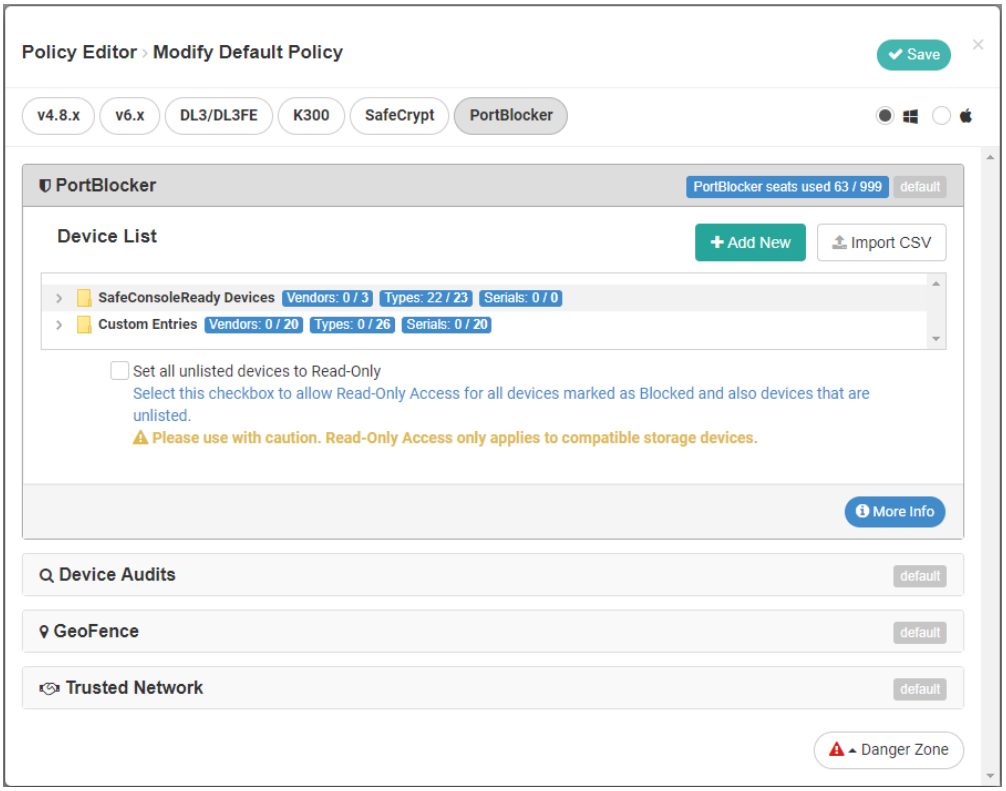
1. Access the Policy Page by clicking **Manage**, then **Policies** on the left side menu.
2. Click the relevant custom policy or default policy that is applied to the affected PortBlocker endpoint.
3. Navigate to the **PortBlocker** tab within the policy editor to see available policies.

### 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.



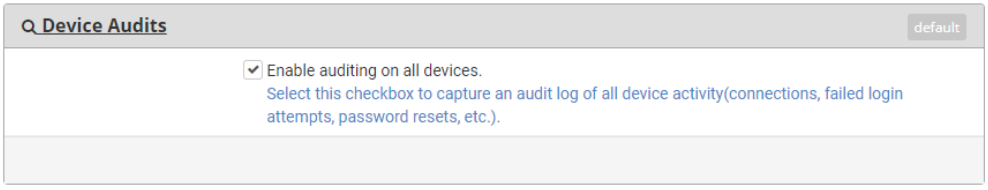

### User Defaults

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.
  - Users may also change this setting in PortBlocker Settings, if needed. Leave the "System Default"(English) if you do not wish to define a language.
  - English, Korean, and German are available (if the language is not available in the user's version of PortBlocker it will default back to English).
- **Disable desktop notifications**
  - 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 locally.

### Audit Logs And Reports

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



The following logs are reported when PortBlocker:

- is registered to the server
- 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:

- User Login
- Computer Name
- VID/PID of Device
- Device Serial Number
- Device Hardware Name

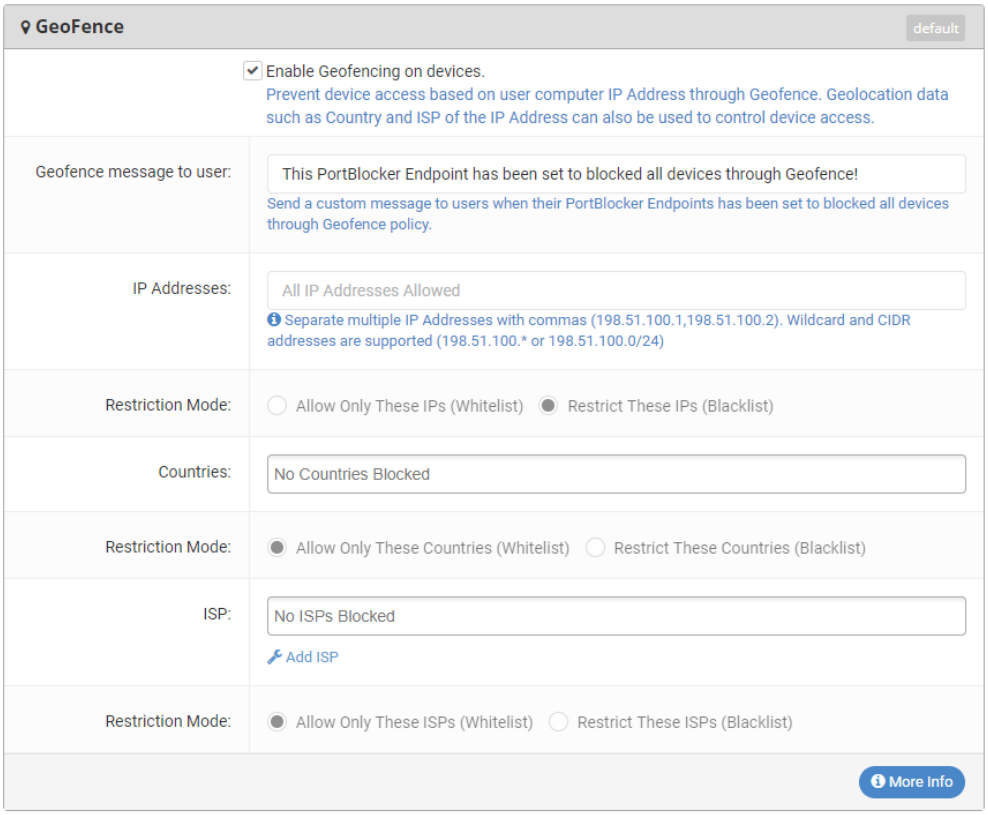
To manage the audit log settings:

1. Navigate to the Policy editor. See Policies for more information.
2. Click the **Device Audits** heading.
3. 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.

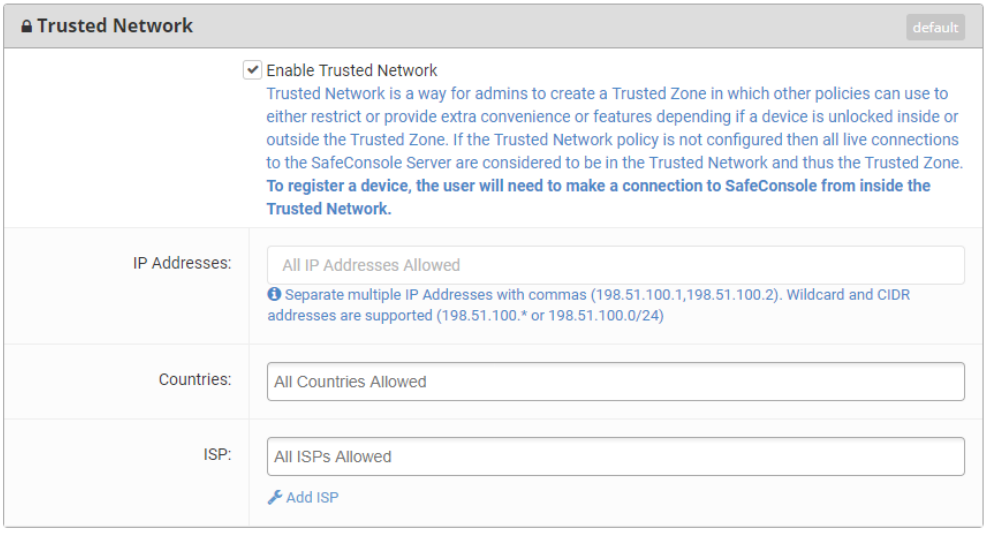



PortBlocker can allow or block endpoints by:

- 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, all devices will be denied access.




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.

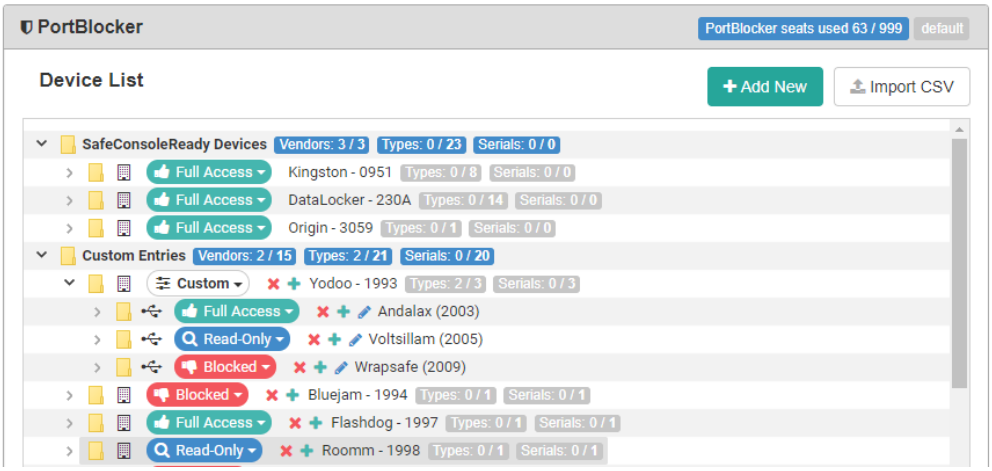
### SafeConsoleReady Devices

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.

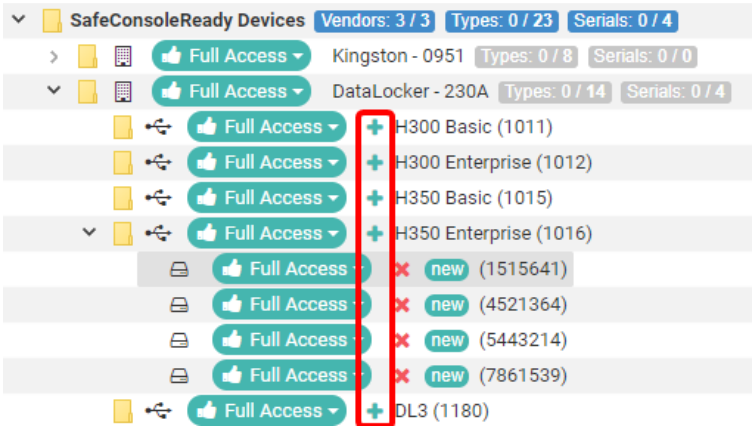
 

2. Locate the policy to be used for PortBlocker and click **Modify**. If the default policy is being used, this can be found by navigating to the Policy page and clicking **Modify Default Policy**. If a custom or inherit policy is being used, navigate to the Policy page, click the policy desired, then 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.



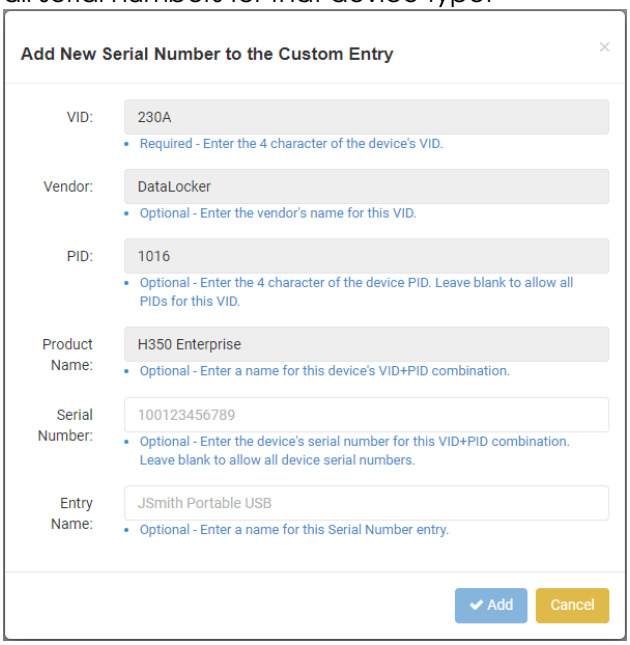

## Adding Serial Numbers

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.




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.




## 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.

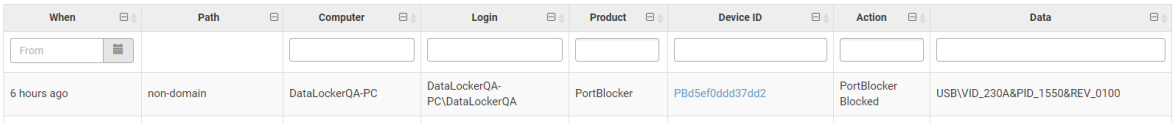
## Other Devices

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. Plugin 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.

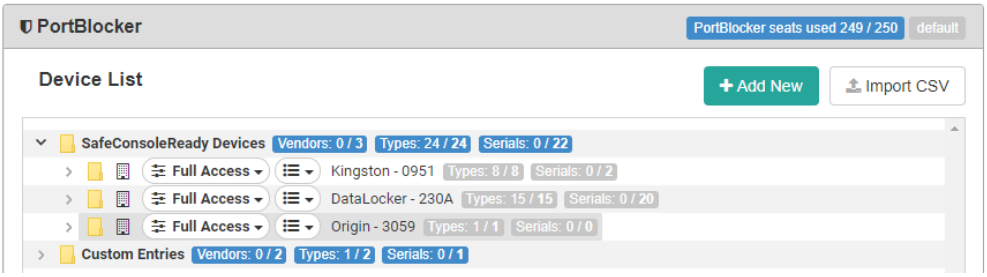



Example:

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

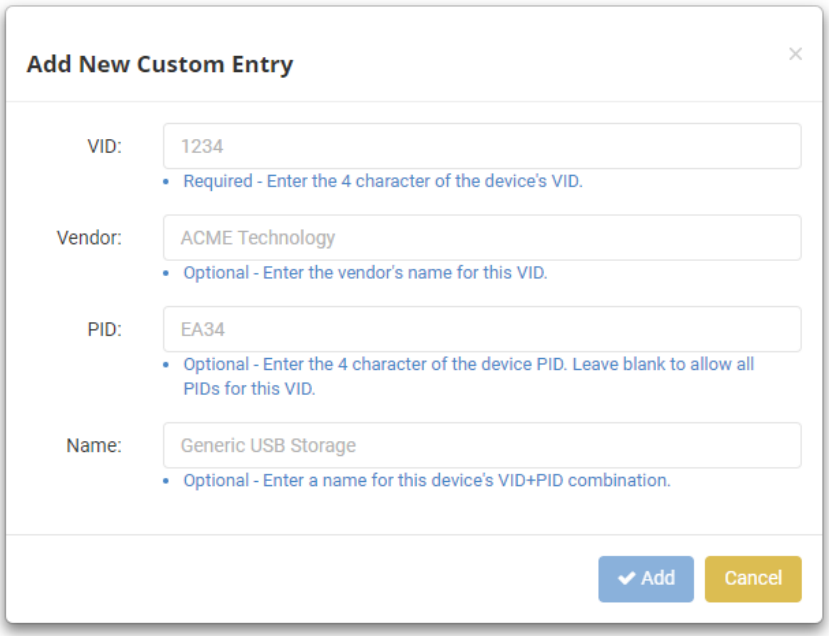
### Custom Device

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

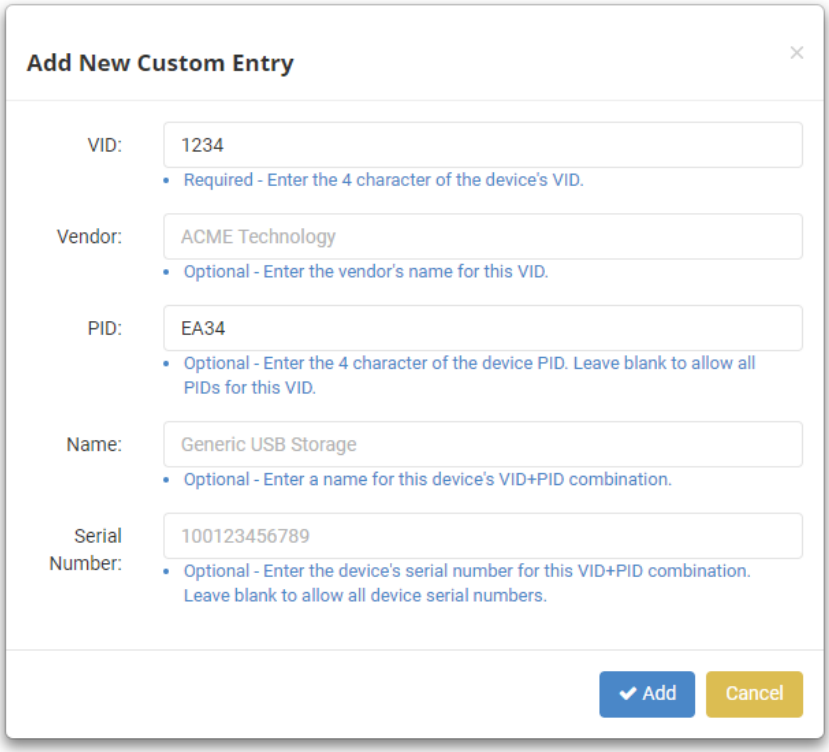



2. Enter the device information.

   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.

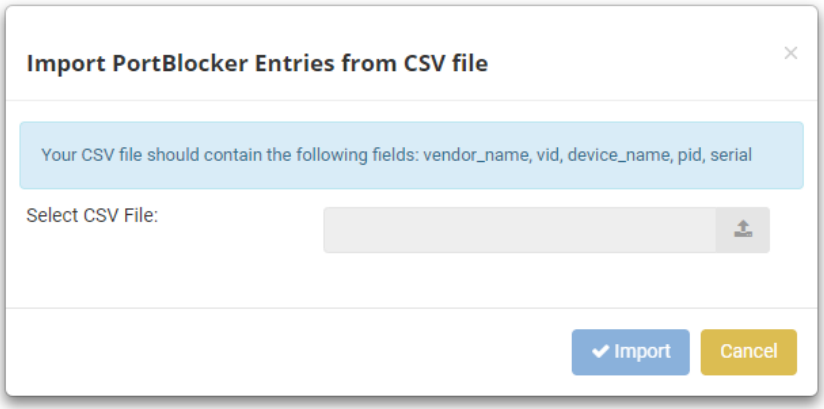



3. Adding both the VID and PID will display the Serial Number field, which allows restricting by serial number. If only the VID is entered, the Serial Number field will be hidden.




### 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.




The first line should contain vendor_name, vid, device_name, pid, and serial, with each entry in a new column

# Updating PortBlocker

PortBlocker will notify the user if an updated version if available on startup. If an update is found, the user will be prompted to download and install the newest version. If PortBlocker is already registered to SafeConsole, the registration will be preserved.

**Note:** Installing the newest version of PortBlocker will require local admin access. For enterprise environments it is recommended that the new version be pushed out using the same Mass Deployment Steps as the initial install.

# Uninstalling PortBlocker

Uninstalling PortBlocker requires having admin permission to the local computer and a special PortBlocker uninstall password. The PortBlocker Uninstall password will be found on in the PortBlocker policy on 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. Optionally, check *CLEAN ALL* to remove all leftover files, such as logs and configs, append the following to the line above during uninstall.

Once completed, PortBlocker will be removed from the computer. Uninstalling PortBlocker will free up a license seat and all devices will be allowed access.

### Uninstalling from Command Line

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

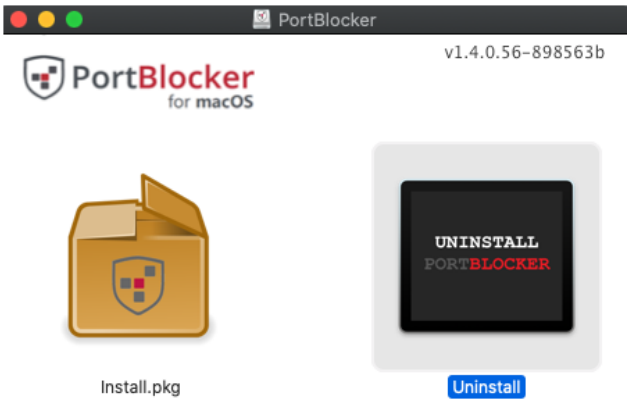
```
msiexec /x PortBlocker_x64.msi /quiet PASSWORD=<UninstallPassword>
```

**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.

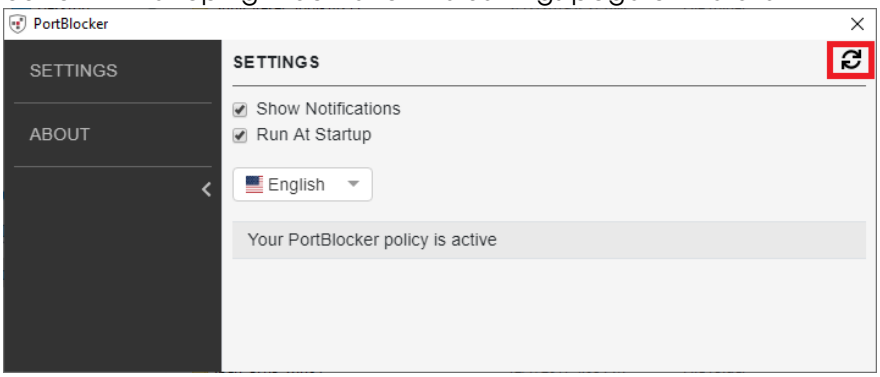



## Troubleshooting

For help with PortBlocker, visit the PortBlocker Support Page.

### Policy

SafeConsole policies update automatically every 10 minutes. If new policies haven't been applied, wait 10 minutes for the client to update or manually refresh the policy by clicking the **Refresh** button in the top right corner of the Settings page of the client.




## 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. All rights reserved.

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