PortBlocker Admin Guide

version 1.0.0

DataLocker Inc.

January 2019

PortBlocker

Contents

About PortBlocker USB Port Control

DataLocker PortBlocker 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 workstation.

DataLocker PortBlocker makes sure only the whitelisted 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 that it blocks 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 the SafeConsole Whitelist policy, 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 policy can be created down to the computer level, if needed.
- **Quick Disable/Enable** - Administrators can remotely **Allow All** and **Block All** devices through SafeConsole.
- **Activity Audits** - Events such as blocked 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 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 without special configurations.

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 for users to charge portable devices via USB.

Minimum Requirements

- Active SafeConsole account (v5.4.0+)
- Valid PortBlocker license and active subscription per endpoint install
- Windows™ 7 or 10
- 512MB of RAM
- 1GB of available hard-disk space
- Connection to SafeConsole server for registration and policy updates
- 1Mbps network connection
- Intel Quad Core Atom processor, or equivalent x86 - x64 processor
- Uses the WinINET (Internet Explorer) system user's proxy settings. Can use either manual proxy settings or a pac script.

Best Practices

DataLocker recommends following the provided best practices guide for a secure deployment. These suggestions should be evaluated before deployment. The best practices guide can be found here: datalocker.com/portblocker/bestpractices

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.

Installation

To install, double click **PortBlocker-Setup.exe** and follow the installation wizard.

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

Silent installation

```
/S
```

Registration: SafeConsole Connection Token

```
/url <SafeConsoleConnectionToken>
```

Registration: Unique Token for user (optional)

```
/user <UniqueToken>
```

Registration: Accepts DataLocker EULA

```
/eula 1
```

Registration: Require user to accept EULA and complete registration

```
/eula 0
```

Please consult the SafeConsole Admin Guide to locate your SafeConsole Connection Token and Unique User Token.

Example:


```
PortBlocker-Setup.exe /S /url "https://server.safeconsolecloud.com/connect" /eula 1
```

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 promted to complete registration. All affected devices will be blocked until registration is complete.

Mass Deployment

For instructions on implementing mass deployment of the PortBlocker application, please see our mass deployment guide. It can be found here: datalocker.com/portblocker/massdeployment

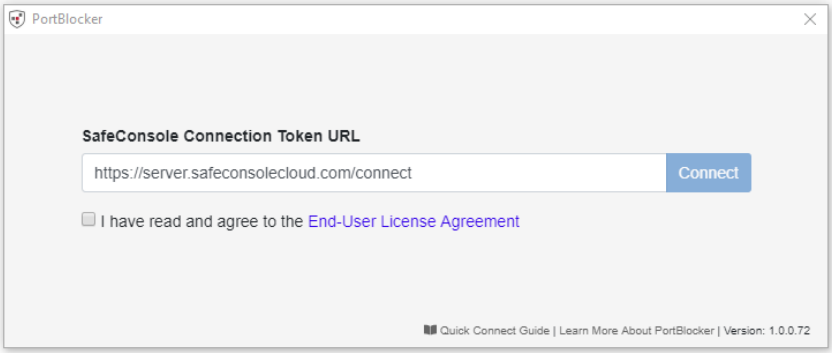
Registration

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.

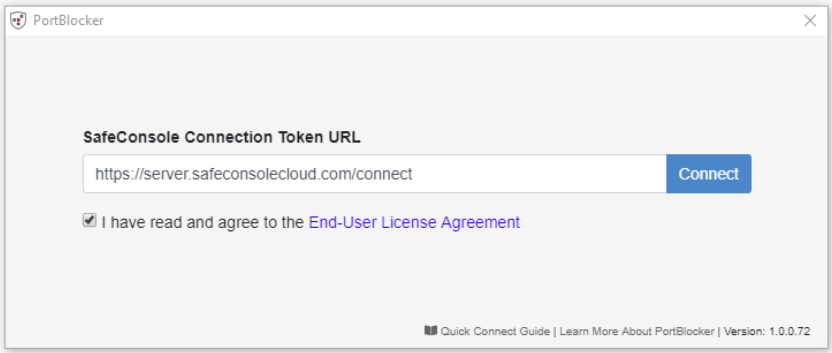
If PortBlocker is installed with the registration command line parameters, these steps can be skipped.

To register your application:

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

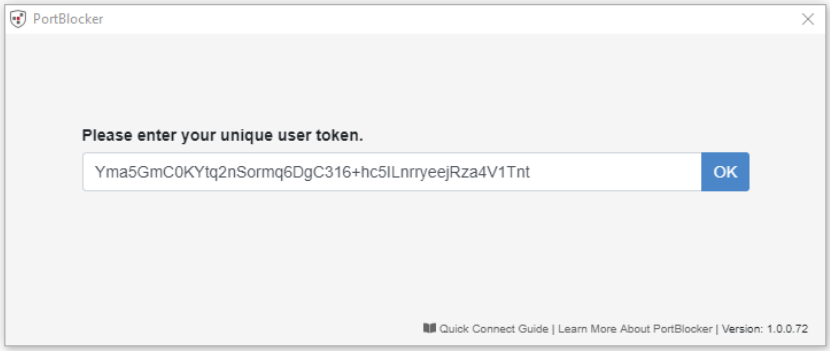


2. Check the **EULA** checkbox and click **Connect**.

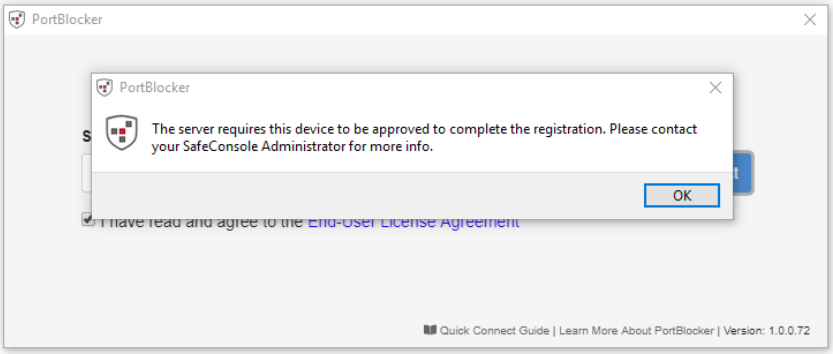


   Any optionally enabled policies will appear at this point. For more information on these policies, see Server Settings.

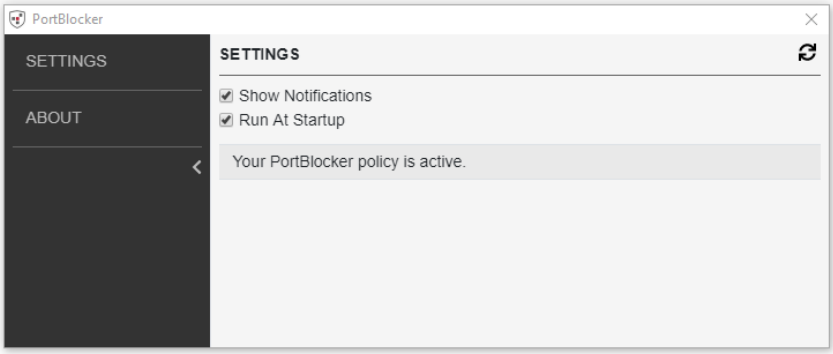
- Unique User Token:



- Administrator Registration Approval:



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

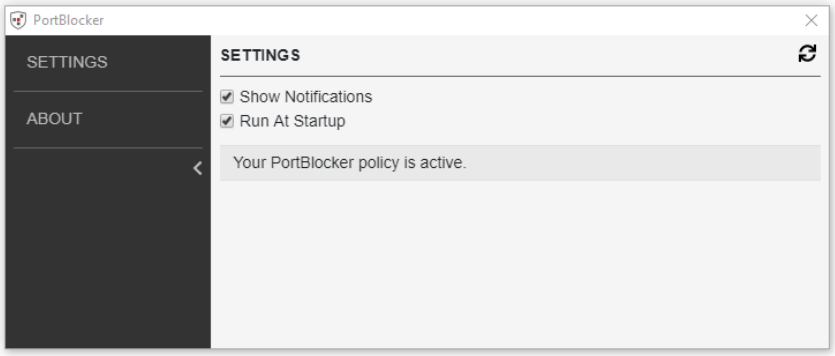


User Interface

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.

If a blocked device is inserted into the user's machine, the user 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

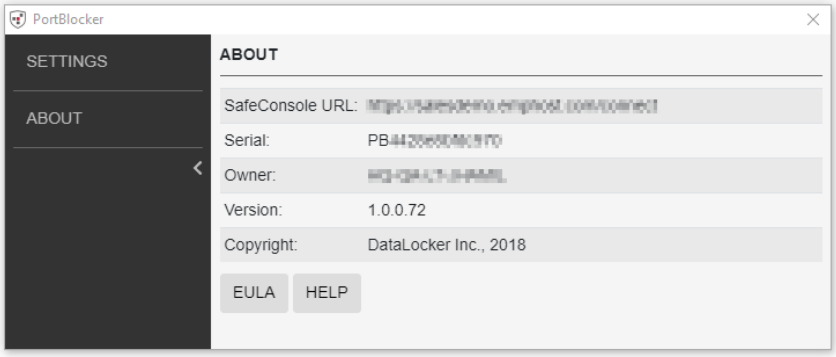
The policy will update when the **Refresh** icon is clicked. Automatic updates are applied every 10 minutes, even when the client is closed. If you wish to update the policy manually, click the **Refresh** icon at the top right.

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 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.

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.

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

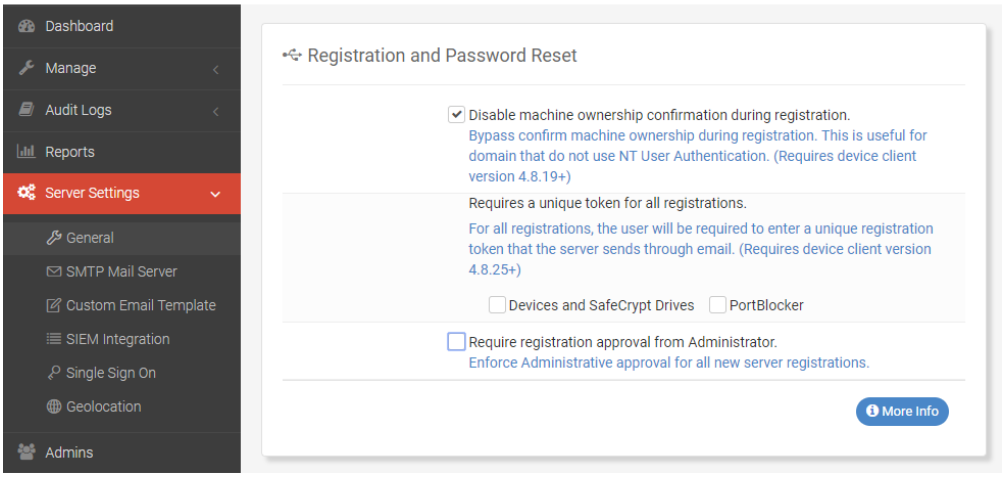
PortBlocker requires an active SafeConsole subscription and one available license seat per endpoint.

Users without access to a management server, please contact the DataLocker Sale Department at sales@datalocker.com or (913)310-9088

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.

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 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 register their PortBlocker application.
- Block All Devices: Sets the endpoint to deny all devices. This action overwrites all policy whitelist settings.
- Allow All Devices: Sets the endpoint to allow all devices. This action overwrites all policy whitelist 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.

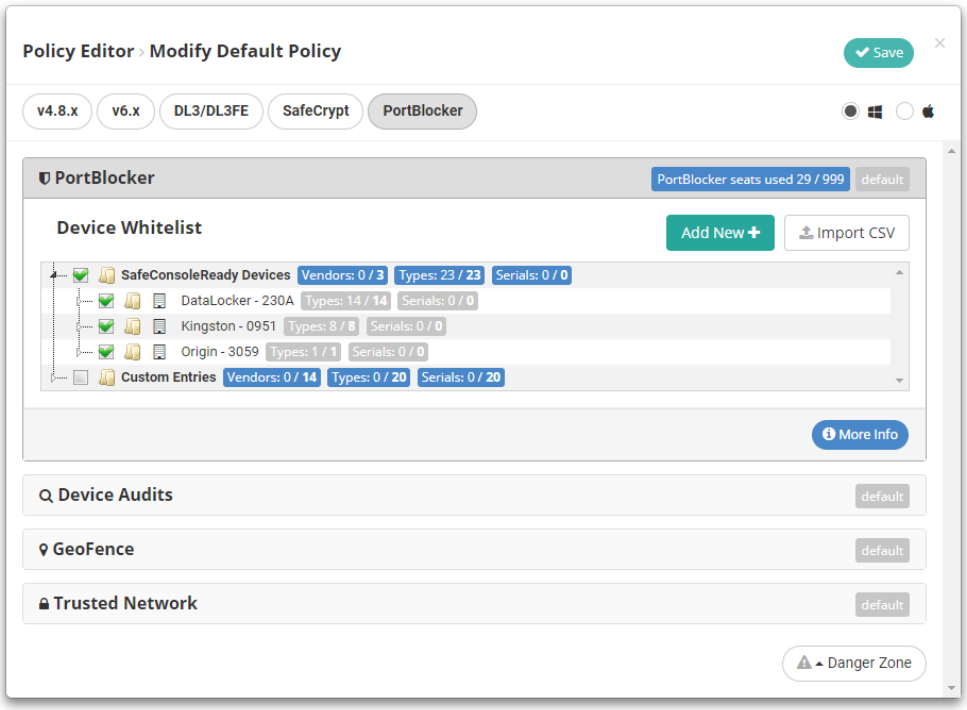
Policies

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

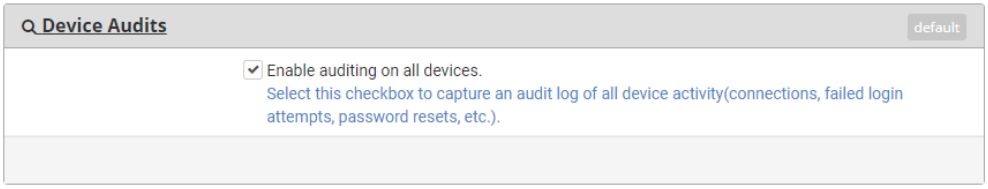
Click on the **PortBlocker** section to see, add, and remove whitelisted devices.

The list of whitelisted devices will appear nested and administrators can expand the menu by clicking the dropdown arrows. For more information on whitelisting, see the Whitelisting Devices section.



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 server
- has been reset
- has blocked a device
- has been set to allowed all devices
- has been set to block all devices
- needs registration approval

Information that is sent with the logs include:

- User Login
- Computer Name
- VID/PID of Device

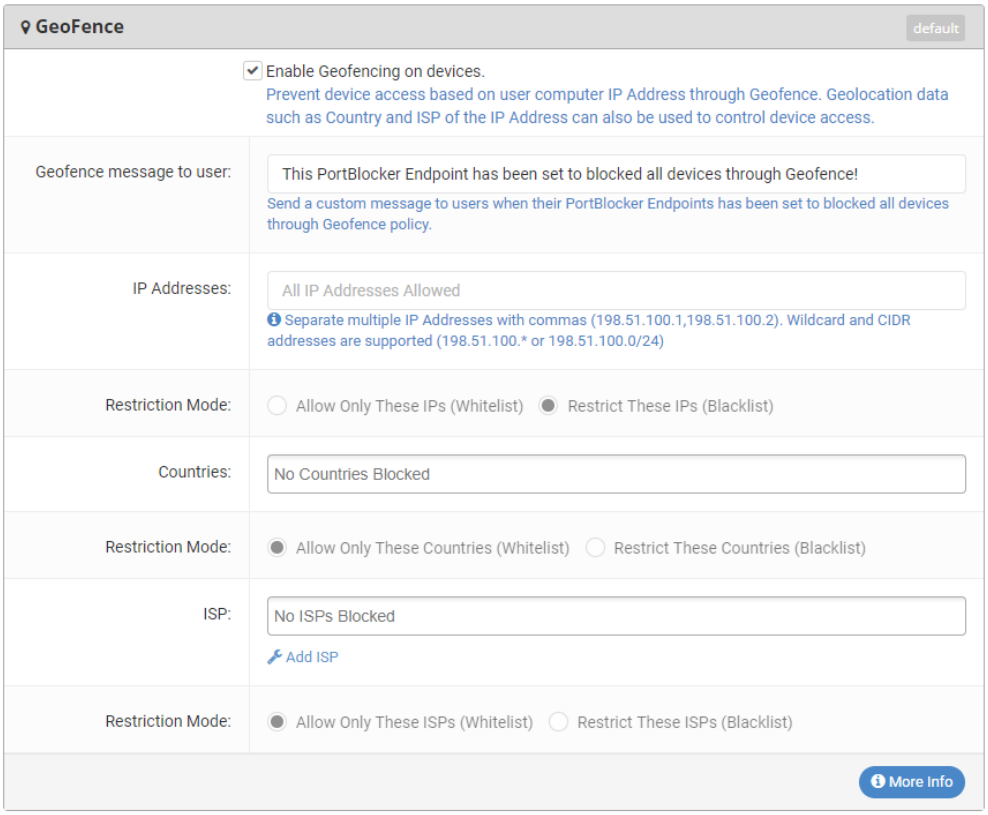
To manage the audit log settings:

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.

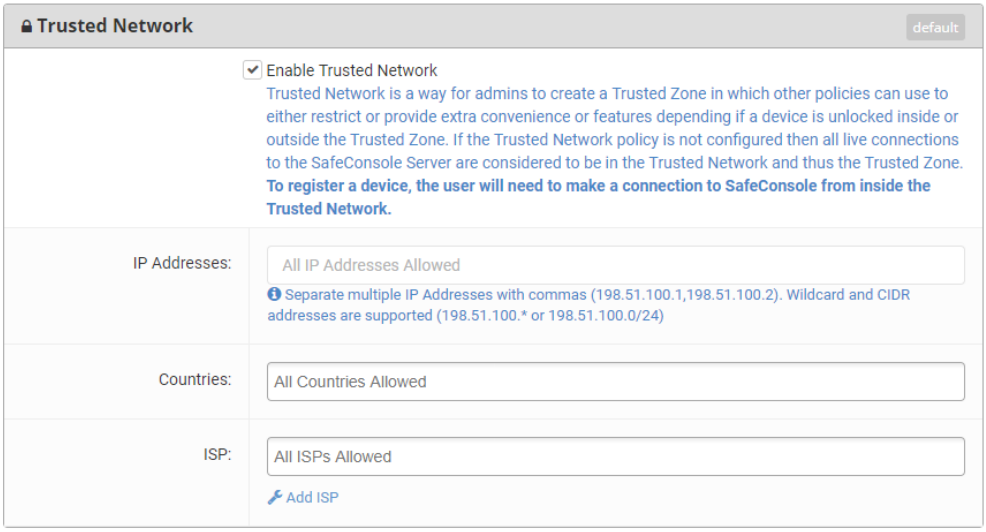


PortBlocker can allow or block endpoints by:

- 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.

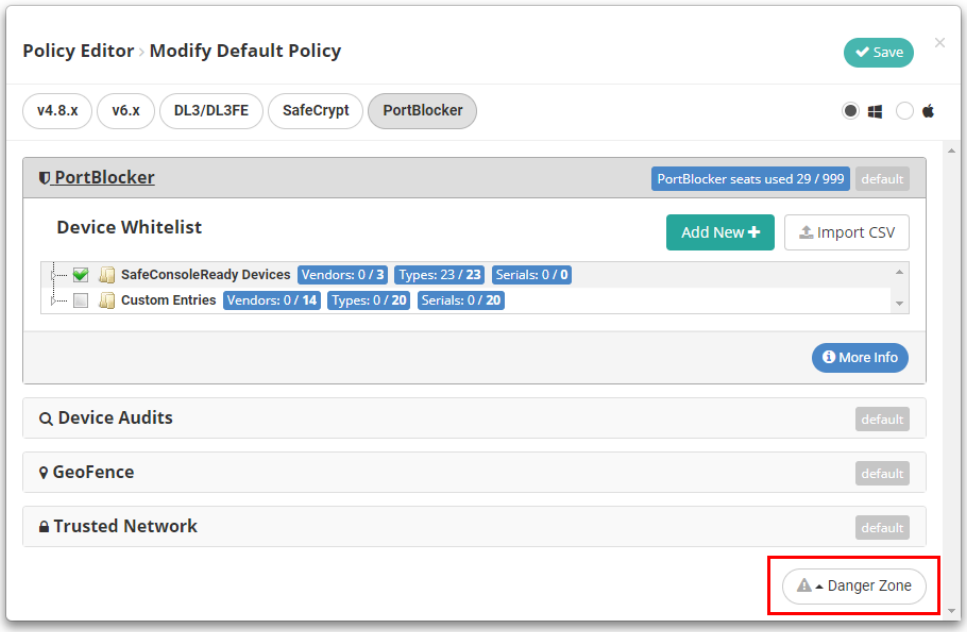


Trusted network allows a trusted zone to be created by:

- 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.

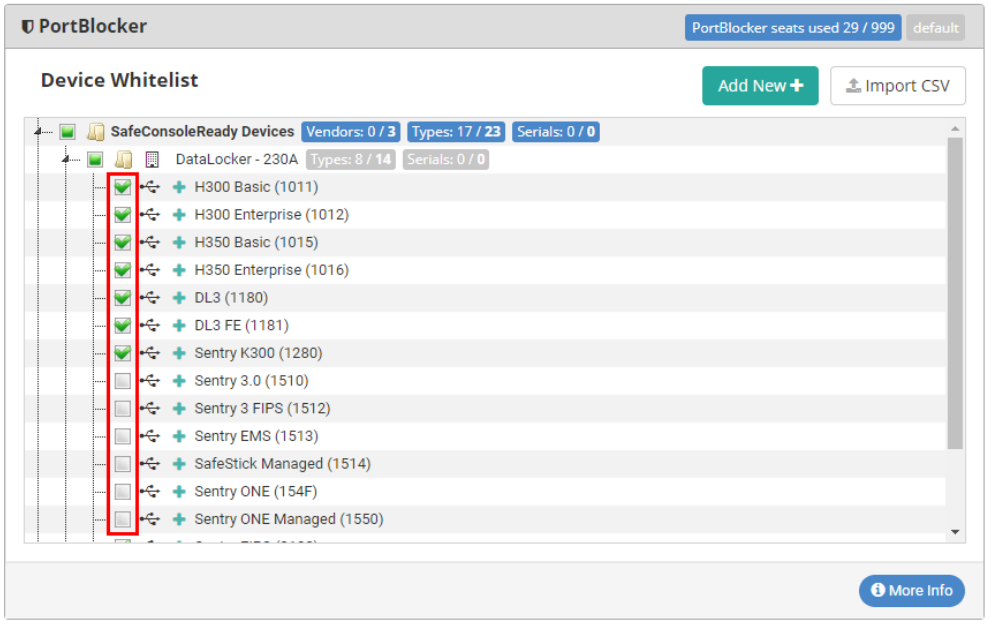


Whitelisting Devices

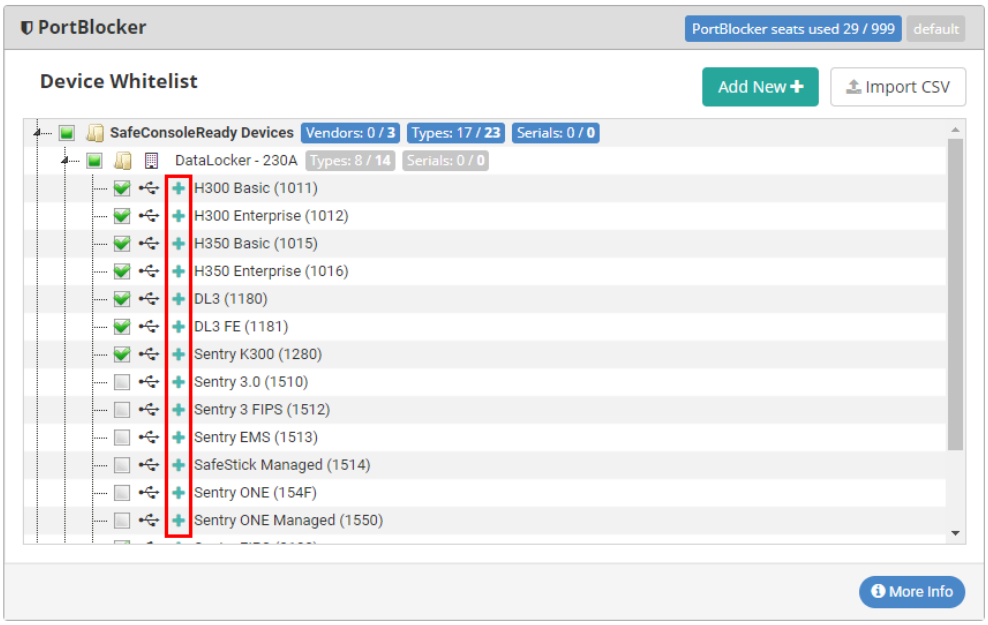
SafeConsoleReady Devices

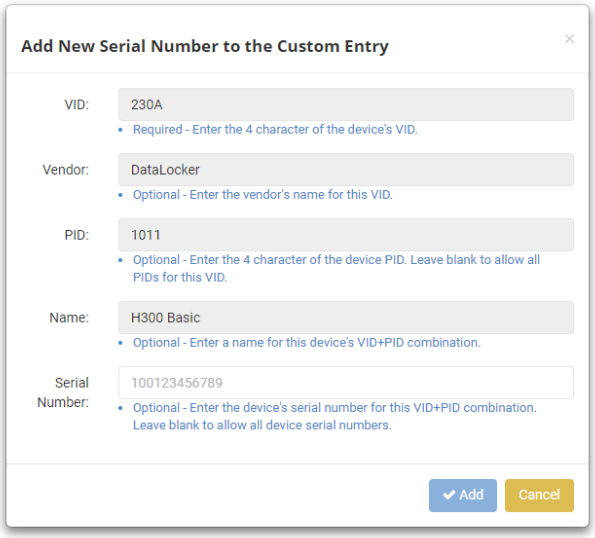
Devices can be whitelisted by an administrator within SafeConsole by device type and serial number.

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 available to choose from. By expanding each vendor subsection and clicking the checkbox next to the device name, all devices in that category will be whitelisted.



To add SafeConsoleReady devices individually by serial number, click the **blue +** next to the device name instead of the checkbox. This will allow you to whitelist by serial number. Once one serial number is whitelisted, only the entered serial numbers will be allowed. Device serial numbers are shared between policies. If the serial number has already been entered, simply select it from the table.





After the initial deployment, no devices will be allowed until they are added to the whitelist.

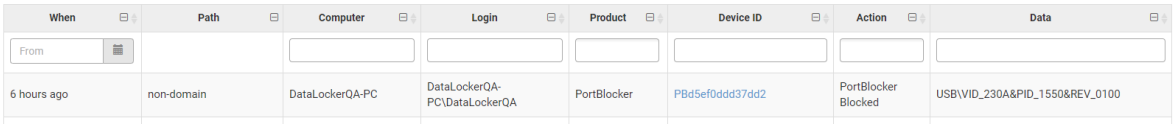
Other Devices

All USB storage devices can be allowed or blocked, however, the process for adding them to the whitelist is different than adding a SafeConsoleReady device. If the VID and PID are known, skip to the Whitelisting section. To find the VID and PID, see the steps below.

Finding The VID And PID

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 it to be blocked.

3. Once it has been blocked, view the audit logs on SafeConsole by clicking **Audit Logs** on the left side menu and then clicking **Device Audit Logs**.
4. Find the **PortBlocker Blocked** 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.



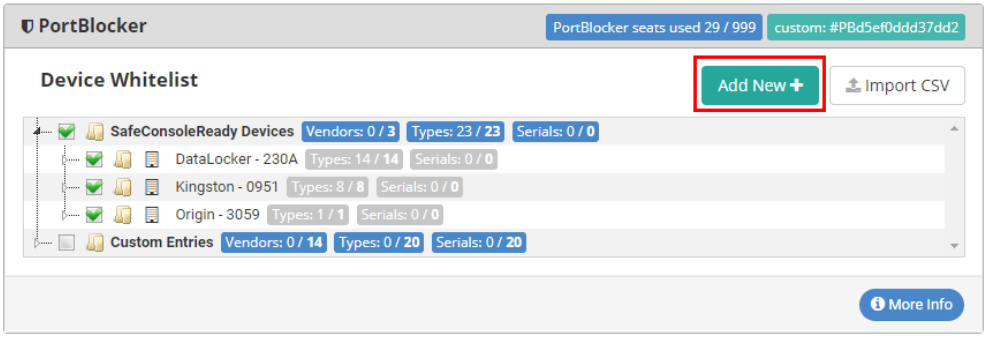
Example:

USB\VID_230A&PID_1550&REV_0100

- VID: 230A
- PID: 1550

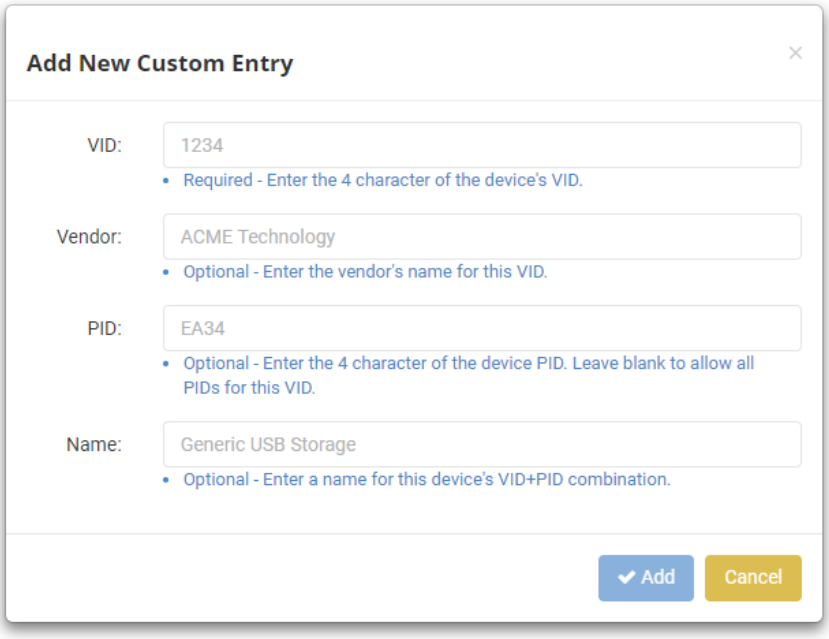
Whitelisting

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

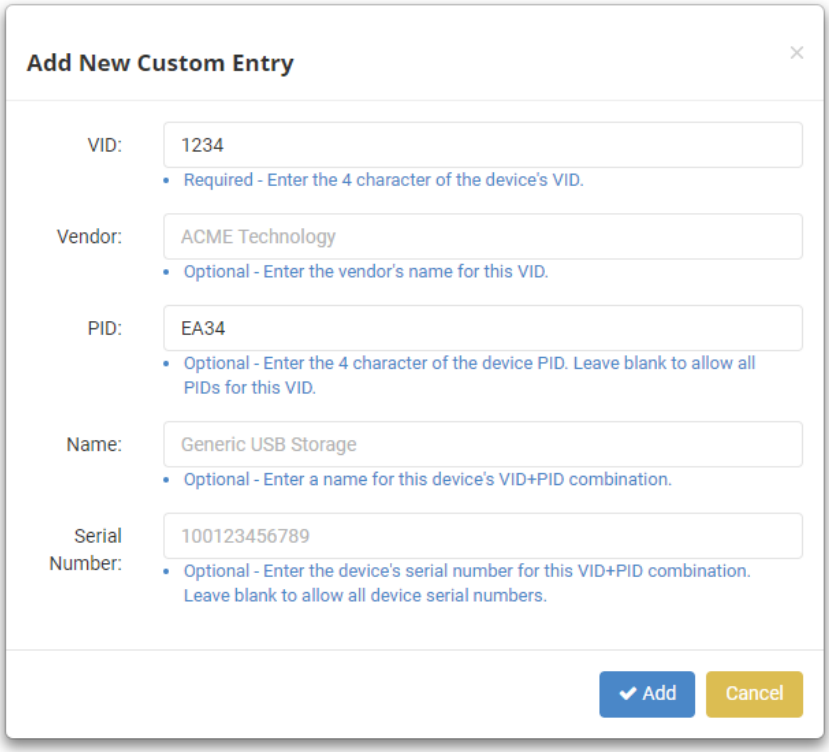


2. Enter the device information.

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

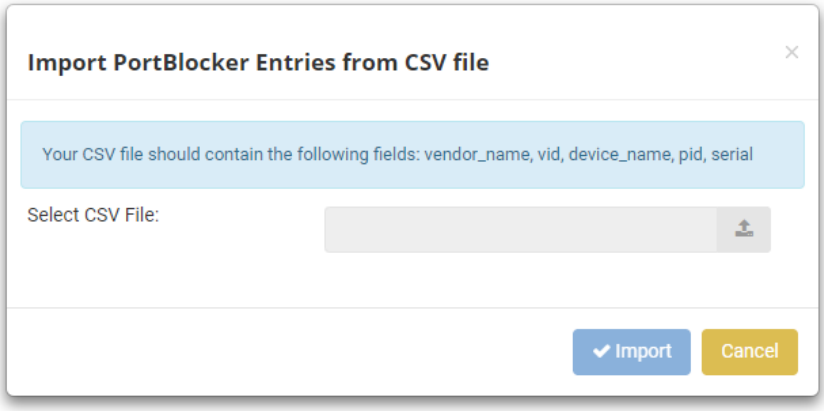


3. Adding both the VID and PID will display the Serial Number field, allowing whitelisting by serial number. If only the VID is entered, the Serial Number field will be hidden.



Importing CSV

Administrators can add device types to the whitelist 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

Uninstalling PortBlocker

Administrators can uninstall PortBlocker, provided they have the needed local permissions. After uninstalling, the USB ports will no longer be blocked.

To 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. The installation wizard will guide you through the uninstallation process. Once completed, PortBlocker will be removed from the computer.

   Uninstalling PortBlocker will free up a license seat and all devices will be allowed access.

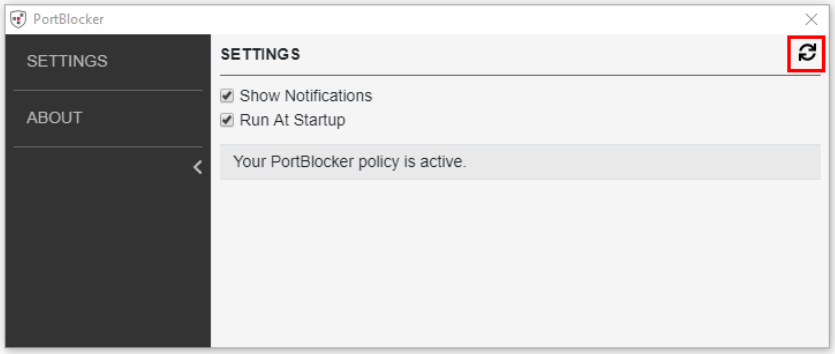
Troubleshooting

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. 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.