PortBlocker Admin Guide and Reference Manual

SafeConsole Managed USB Port Endpoint Security: Monitor/Block/Read-Only/Allow

Table of Contents

About PortBlocker USB Port Control

PortBlocker by DataLocker is a management solution designed for controlling access to USB mass storage devices on Windows and macOS. PortBlocker integrates with SafeConsole, which is available for both Cloud and On-Premise deployments, allowing for the central management of USB device usage.

PortBlocker enables the management of USB mass storage devices by categorizing them as allowed, blocked, or read-only. This approach prevents the use of unauthorized USB devices and reduces the risk of malware transmission and data breaches.

The SafeConsole Admin Guide provides detailed instructions for setting policies and managing devices remotely, supporting data leakage prevention (DLP) strategies.

Features

- Endpoint Port Control - Restrict USB storage devices through a SafeConsole defined allow list of target USB devices, using VID (VendorID), PID (ProductID), and serial number..
- 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”-actions, etcetera 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.
- Audit Only (Stealth Mode) - allows administrators to run PortBlocker hidden in the background. The user interface and notifications will be inaccessible, which is indispensable to understanding a network's current USB security posture.
- Uninstall Password - Administrators can restrict PortBlocker from unauthorized uninstallation through an uninstall password.
- Geofence - Devices can be automatically blocked when the computer is outside the geolocation requirements.
- Offline Capability - The cached SafeConsole policy allows 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, and their usage is monitored and logged.

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

- An active SafeConsole account (version 5.5.0 or higher) with either Cloud or On-Premise setup.
- A valid PortBlocker license for each endpoint where it is installed.
- Windows™ 7, 10, 11 or macOS™ on Intel, M1, M2 or M3 processor with 12.x, 13.x, 14.x (Monterey, Ventura, Sonoma)
- 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 software installed on users' computers with the SafeConsole management platform.

Windows Installation

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

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>
```

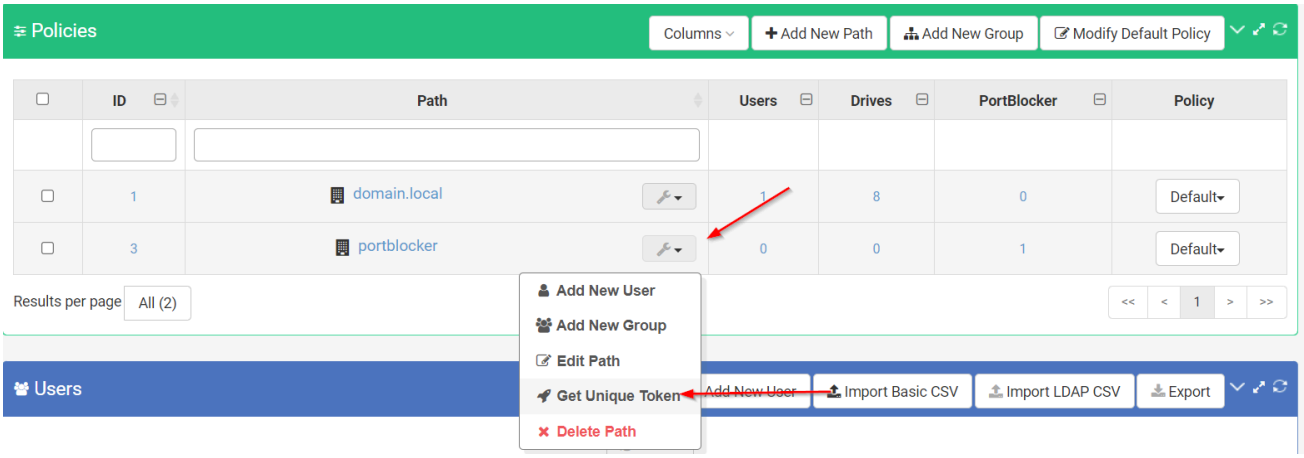
The SafeConsole connection token. The URL parameter should go at the end of the command for greater compatibility.

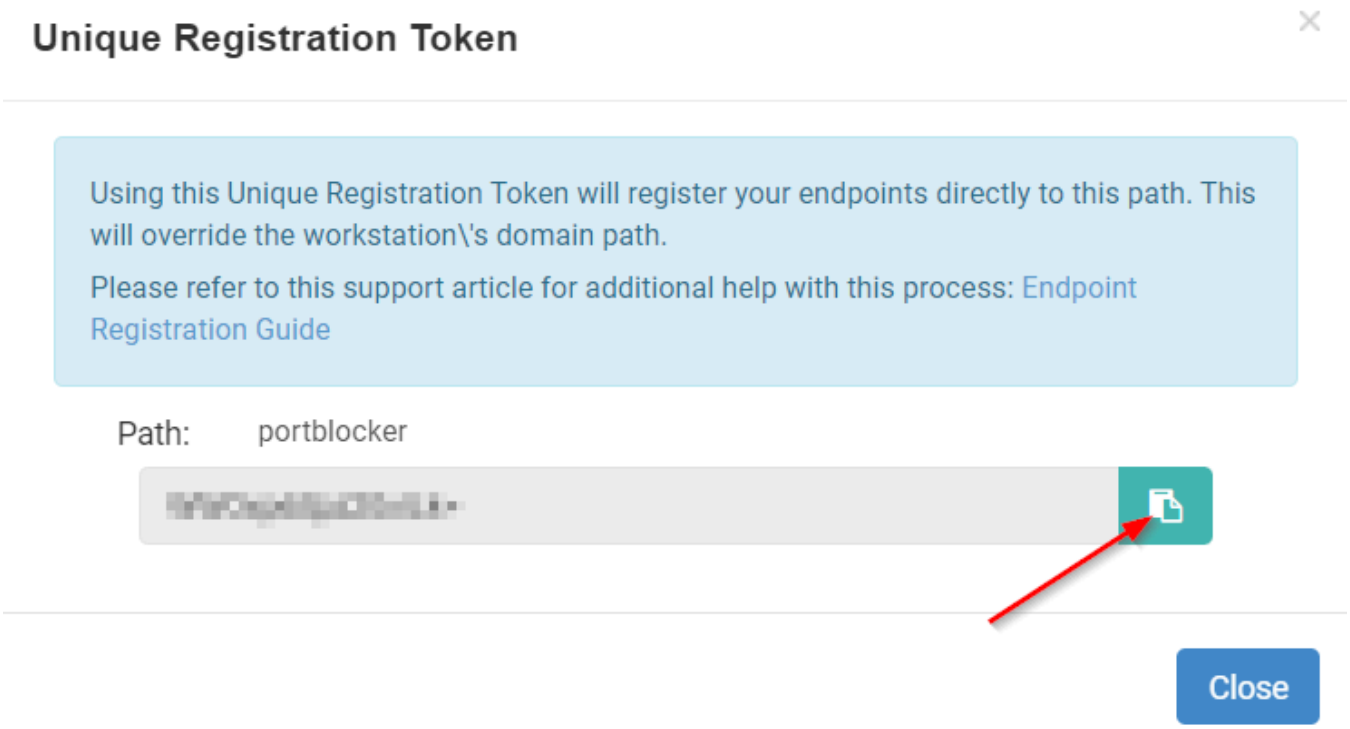
```
EULA=1
```

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






```
LAUNCH_CLIENT=1 | 0
```

Launch the Windows client application after installation. The default value is 1 (launch client application). It is recommended to set it to 0 (do not launch client application) for mass deployment scenarios to avoid an 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:

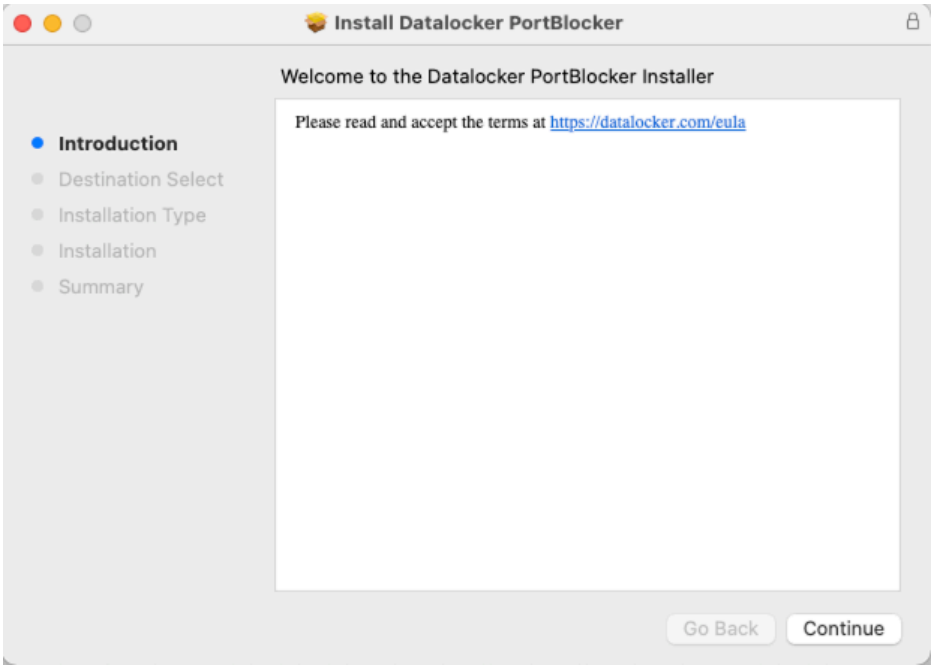
```
msiexec /i PortBlocker-Setup.msi /quiet EULA=1 ALLUSERS=1 /norestart
USER=pathuniquetoken URL=https://server.safeconsolecloud.io/connect
```

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 Wizardq

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.

PortBlocker Endpoint Application 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**

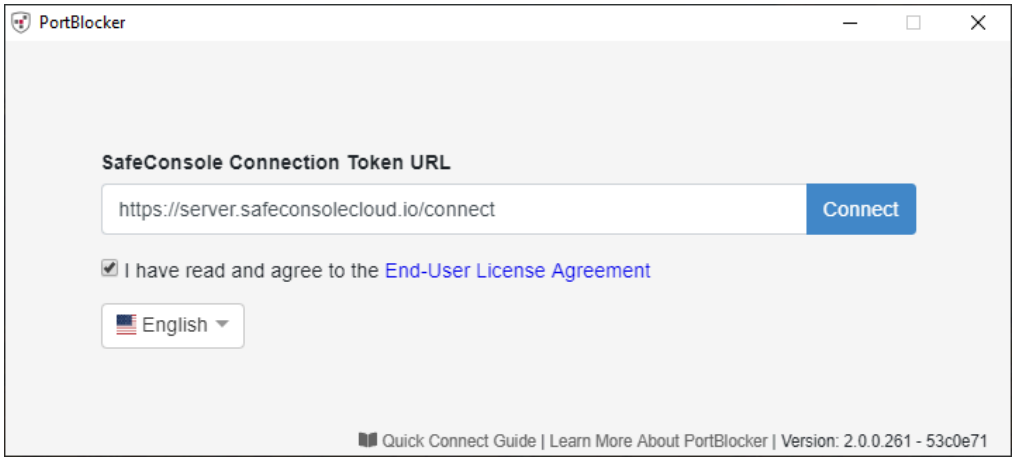
Registration

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.



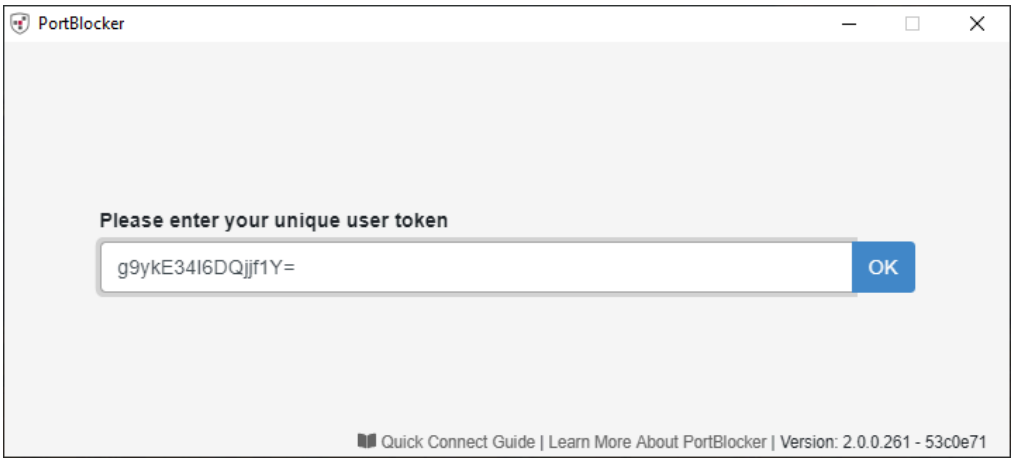
2. Select the desired language.

   Note: Changing the language requires PortBlocker to be restarted.

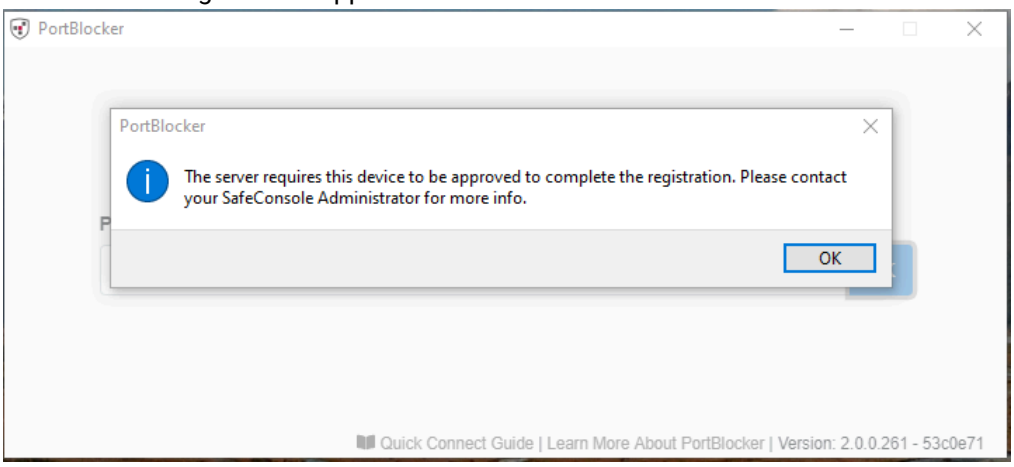
3. Review and accept the EULA by selecting the checkbox and click Connect.

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

– Unique User Token:



– Administrator Registration Approval:



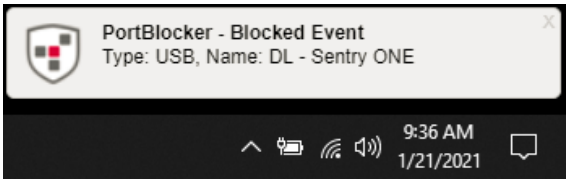
4. PortBlocker will register the application and apply the appropriate policies. The client will show the Settings page by default.

Expected Application Behavior Based on Policy Configuration

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.

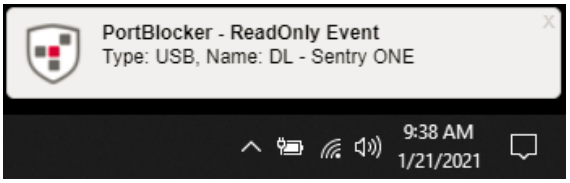


Read Only

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.

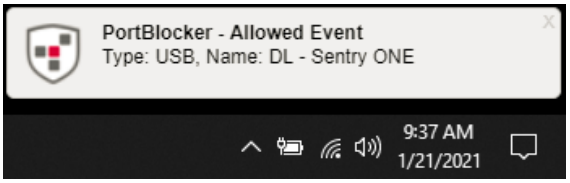
It is recommended that when used in conjunction with SafeConsole Ready Devices, the device should be put into read-only mode through the device policy and full-access should be granted for the device in PortBlocker.

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.

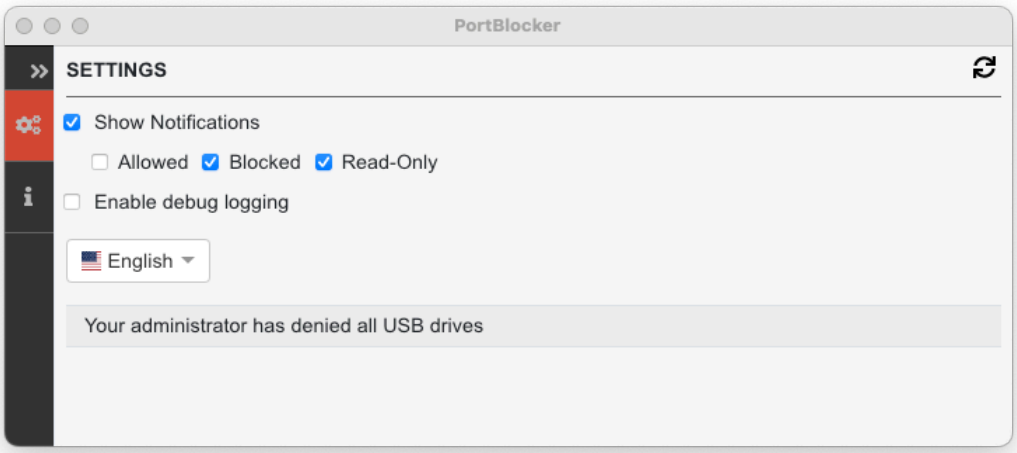
PortBlocker Endpoint Application User Interface

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 the Allowed, Blocked, Read-Only, and Unfilterable (Windows only) checkboxes.

Blocked and Read-Only notifications are enabled by default for all newly installed endpoints. All enabled notifications will appear only once per session and will not repeat until the user reboots. Clicking on a notification will bring up the client.

This setting can be controlled by the administrator 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.

Or

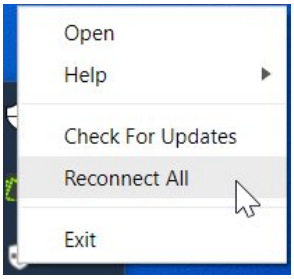
1. In the System tray right click on the PortBlocker icon.
2. In the Portblocker menu popup select > Check For Updates
3. PortBlocker will check for updates from the SafeConsole server and apply them.

Reconnect All (Windows only)

To ensure a new policy is enforced correctly for all plugged-in devices without the need to physically reconnect the device, the user can manually refresh the policy by selecting the 'Reconnect All' option from the systray icon menu.

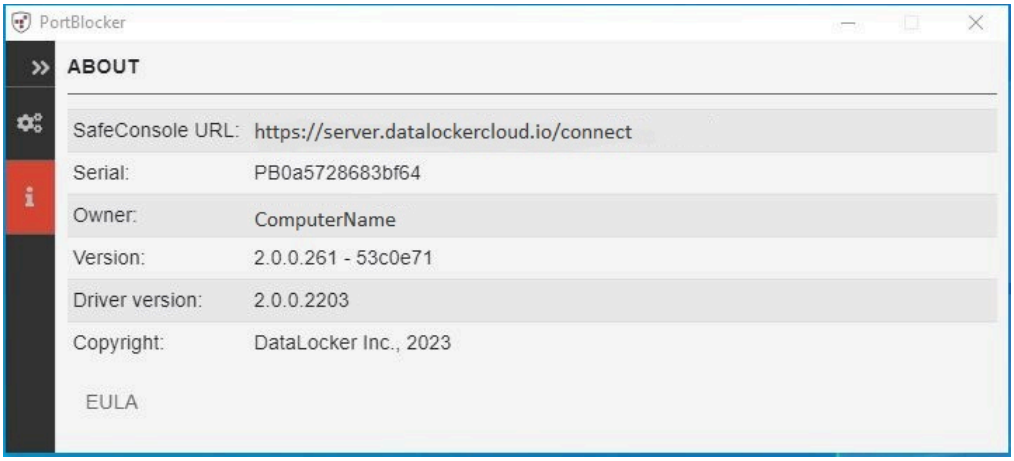
To refresh the policy for all plugged-in devices:

1. In the System tray right-click on the PortBlocker icon.
2. In the Portblocker menu popup select > Reconnect All.
3. The policy for all plugged-in devices is refreshed.



Application 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.

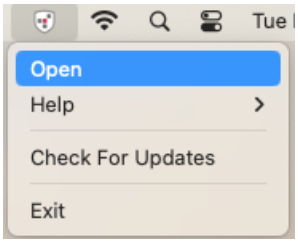
A link to the EULA is listed below the technical details.

Application Tray (Menu Bar) Icon

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



Manage PortBlocker in 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**.

SafeConsole Licensing

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

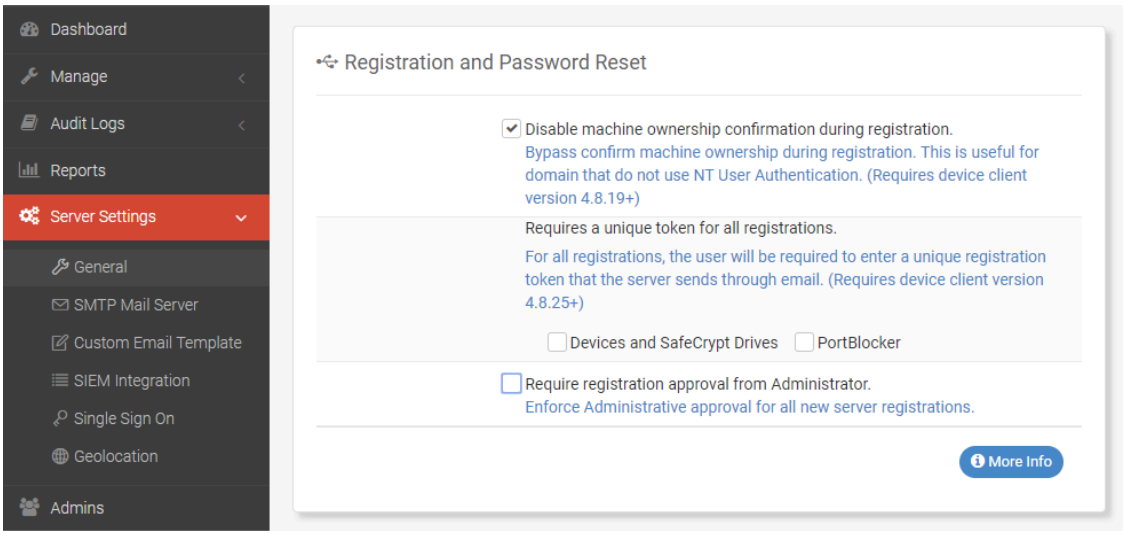
Users without access to a management server, please contact the DataLocker Sales Department by emailing **sales@datalocker.com** or calling +1 (913) 310-9088. For customers in EMEA please email **eulicensing@datalocker.com** or call +31 467 111 205.

If a SafeConsole license 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** 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.

SafeConsole 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.

PortBlocker Endpoint SafeConsole 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.

SafeConsole PortBlocker Policies

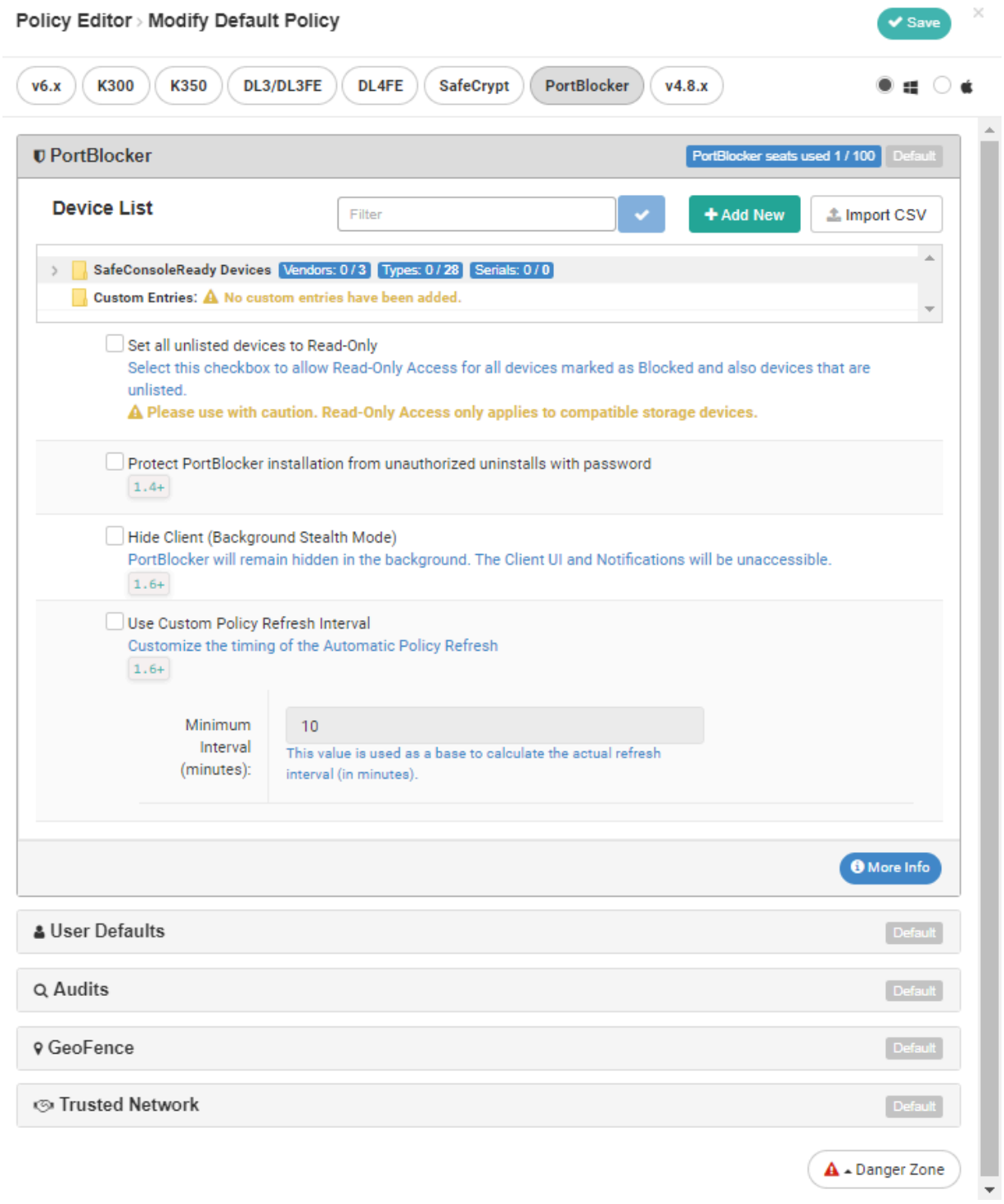
1. Access the Policy Page by clicking **Manage**, then **Policies** on the left side menu.
2. Click the relevant custom policy or default policy that is applied to the affected PortBlocker endpoint.
3. Navigate to the PortBlocker tab within the policy editor to see available policies.

PortBlocker Section of the SafeConsole Policy Editor

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

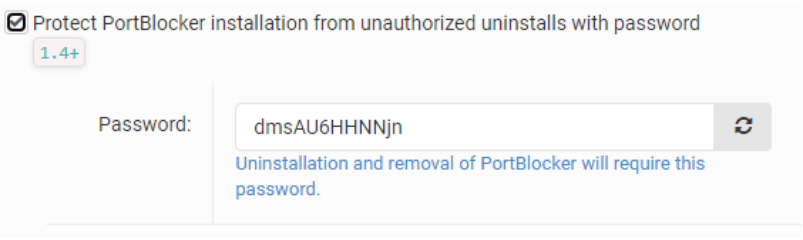
The list of devices will appear nested and administrators can expand the menu by clicking the dropdown arrows.

For more information on adding a device, see Configuring the Allowed/Blocked/Read-Only Device List.



PortBlocker Endpoint Application Uninstall Password

The PortBlocker endpoint agent can be restricted from unauthorized uninstallation through the use of an uninstall password. You can set the PortBlocker 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.



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. Keep a record of the Uninstall Password for reference as it will be required for uninstalls.

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

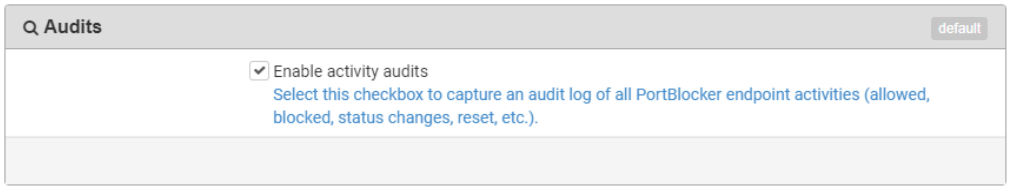
The User defaults policy allows management of the user interaction with PortBlocker.

- 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.



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
- detects repeating event
- performs regular health check
- reconnects all devices

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

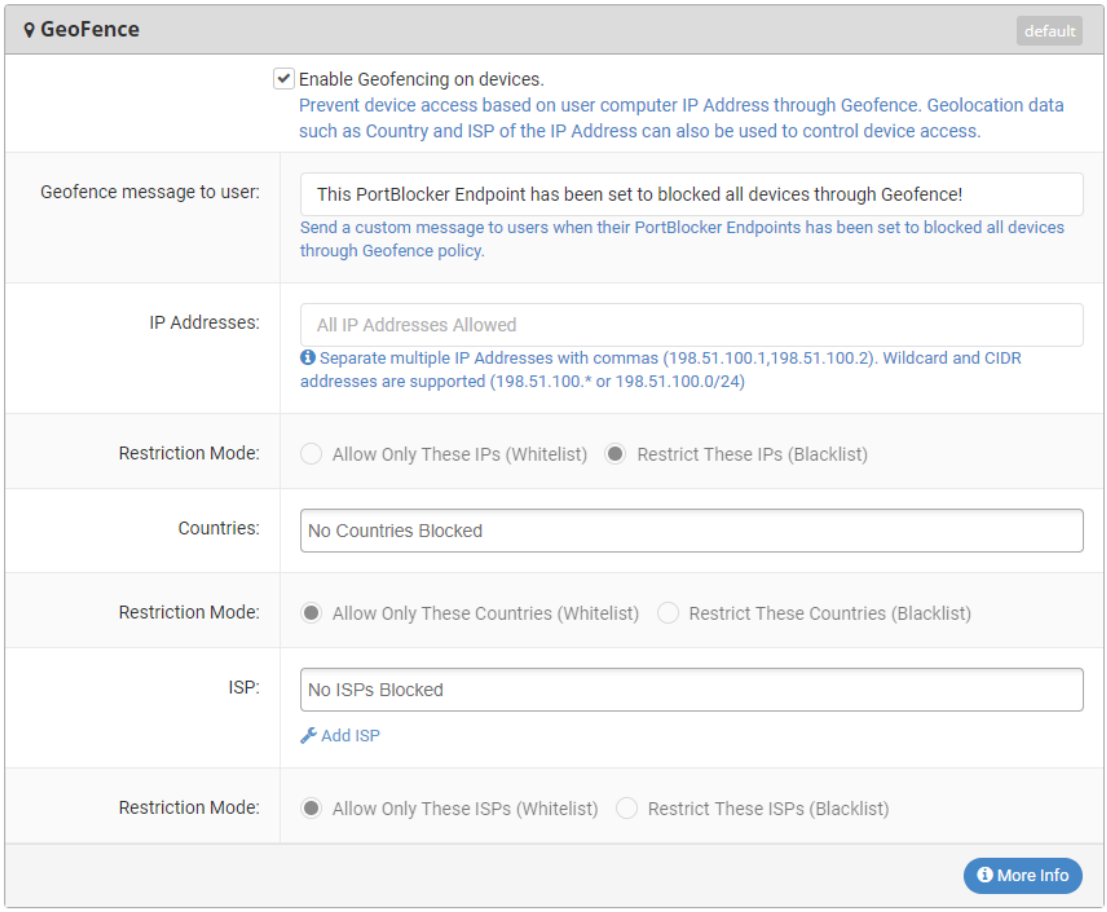
To manage the audit log settings:

1. Navigate to the Policy editor. See **Policies** for more information.
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.



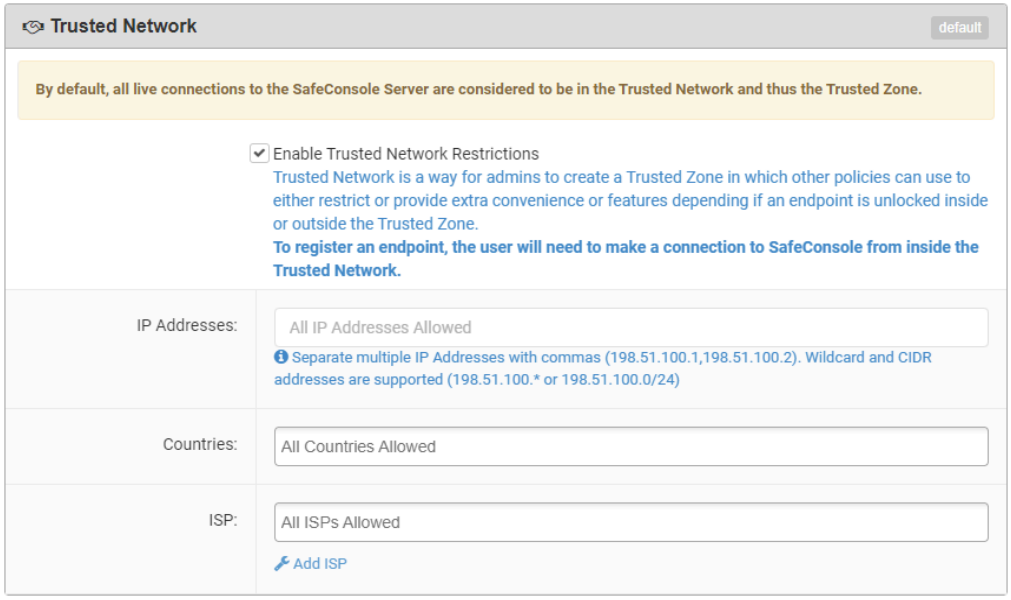
PortBlocker can allow or block endpoints by:

- 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, the registration to SafeConsole will be denied. Note: Trusted Network settings do not affect already registered endpoints.



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.

Configuring the Allowed/Blocked/Read-Only Device List

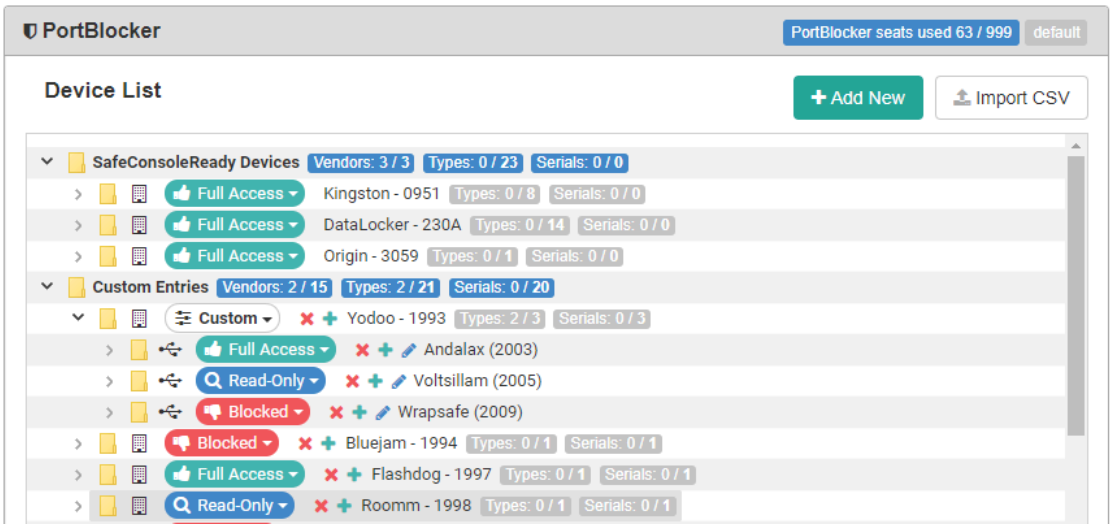
SafeConsole Admins can select which devices are allowed (Full Access), blocked, or forced into read-only mode. This can be configured by device type or serial number. Devices not on the list can either be blocked or forced into read-only mode.

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 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 for creating your PortBlocker policy.

1. Within SafeConsole, navigate to the Manage>Policies page.
2. Locate the policy used for PortBlocker and click Modify. If the default policy is used, navigate to the Policy page and click Modify Default Policy. If a custom or inherited 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.



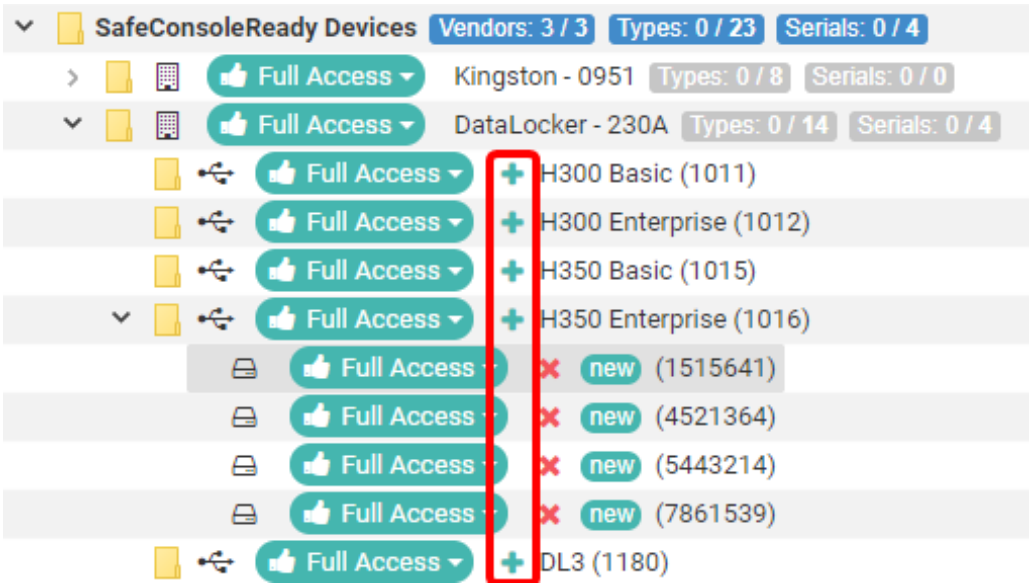
5. Click **Save** in the top right corner to apply the policy.
6. The policy will be automatically applied to the endpoint within 10 minutes. Or instantly if the policy is updated manually at the endpoint.

Adding SafeConsoleReady Device Serial Numbers Individually

1. 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.

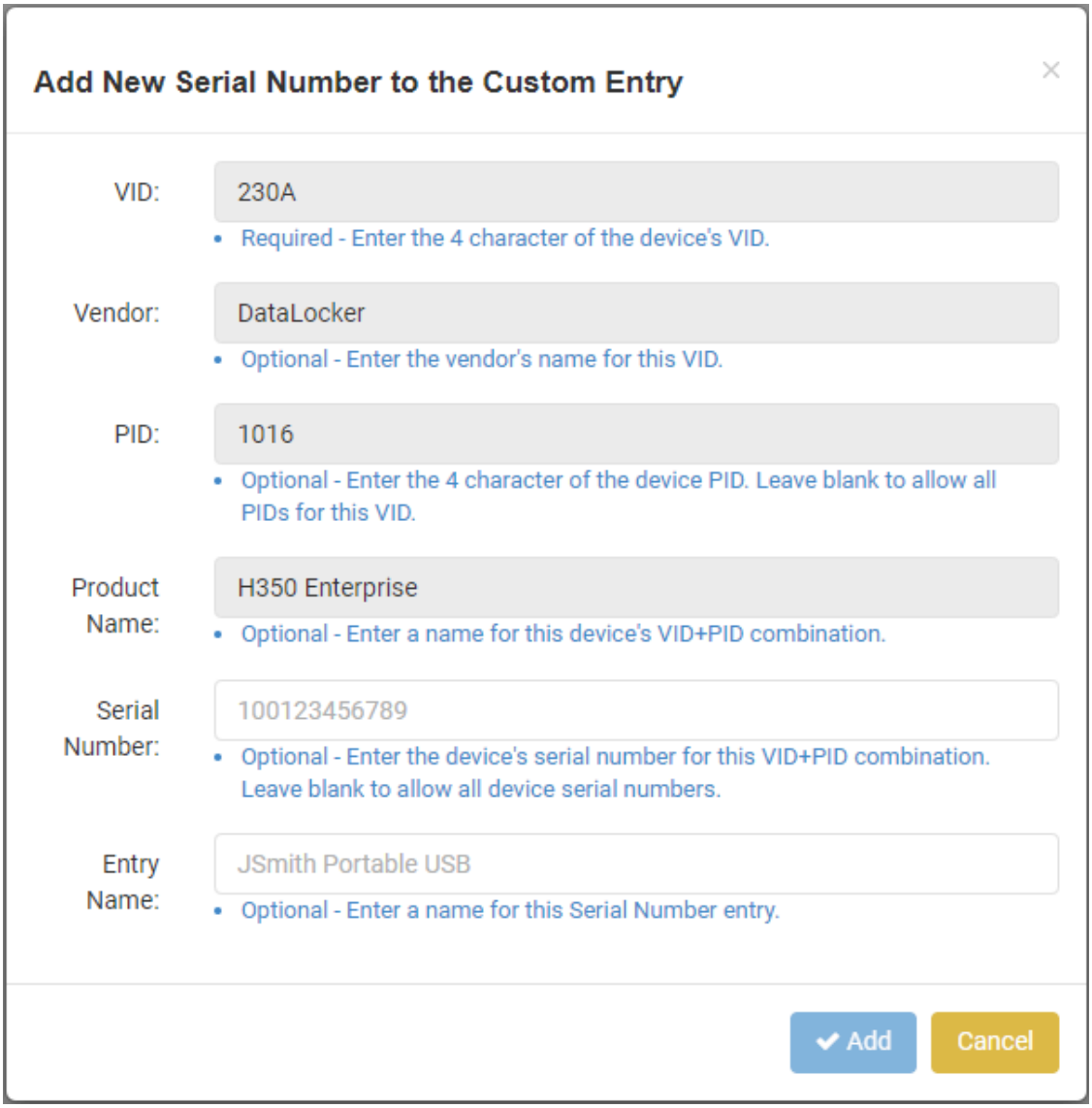
   Defined serial numbers are shared between policies, but the policies can be individually configured. If the serial number has already been entered, simply select it from the table.



   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.

2. Click Save in the top right corner to apply the policy.

3. The policy will be automatically applied to the endpoint within 10 minutes. Or instantly if the policy is updated manually at the endpoint.



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 the **Set all unlisted devices to Read-Only** checkbox is 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.

Handling Custom Entries of USB Storage Devices

Filtering of all USB storage devices can be defined in the policy. However, the process for adding Custom Entries to the Device List is different than adding a SafeConsoleReady device.

Any other USB Storage Devices are added to Custom Entries as Blocked. The full list of Custom- Entries is available and shared across all individual policies. Each policy can then have its own individual configuration for each device.

For easier configuration, make sure audit logging is enabled. For more information, see **Audit Logs And Reports**.

Workflow Overview

1. Add or confirm that the target USB device is present in the general Custom Entries list that is available in all policies.
2. Locate the PortBlocker endpoint policy you want to change.
3. Search for the target USB device by serial number, VID, or PID.
4. Configure the target USB device as Allow/Block/Read-Only and apply the policy.
5. The policy will be automatically applied to the endpoint within 10 minutes. Or instantly if the policy is updated manually at the endpoint.

Adding an Available Device Automatically to the Custom Entries List

1. When a target USB device is plugged into a computer that has PortBlocker installed, PortBlocker reports the event to SafeConsole. This requires **Audit Logs** to be activated.
2. Log on to SafeConsole.
   a. EITHER locate the target device in the Users log entry widget on the SafeConsole Dashboard, click on the **wrench icon** . Copy the serial number, or click **Copy to Clipboard** to copy all details, for later search. Click **Add**.
   b. OR locate the device in **Audit Logs > User Audit Logs.**
      - Type **PortBlocker** in the **Action** column to filter only PortBlocker audit logs. You may need to navigate to the right with the arrows.
      - In the **Data** column click on the **wrench icon** .
      - Click **Add Device to List**, copy the serial number for later search.
      - Click **Add**.
      - If the dropdown says **Modify Custom Device,** the device is already in the Custom Entries List. Click **Modify Custom Device** and copy the serial number for later search.
3. The device has now been added to Custom Entries in all PortBlocker policies as Blocked (the Block action can be overridden by the Allow All setting for a PortBlocker endpoint.)
4. Now, locate the PortBlocker policy in SafeConsole and configure the target USB device behavior.
   a. EITHER locate the target device in the Users log entry widget on the SafeConsole Dashboard Click on the user name, the Endpoint Details Panel opens. Click on the Policy and select Modify.

b. OR locate the endpoint in **Audit Logs > User Audit Logs.** Click the **Device ID** to access the **Endpoint Details Panel,** click on the Policy, and select Modify.

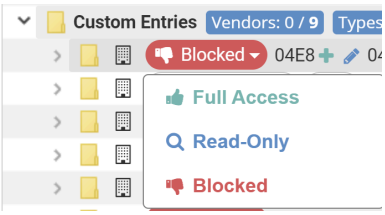
c. You can also configure the Policy in **Manage>Policies,** or under **Manage>PortBlocker** in the Policies column**.**

d. At the top of the Policy Editor window, click the PortBlocker tab.

e. In the Device List Filter box enter the serial number you have copied previously and click on the blue checkmark icon next to the box.

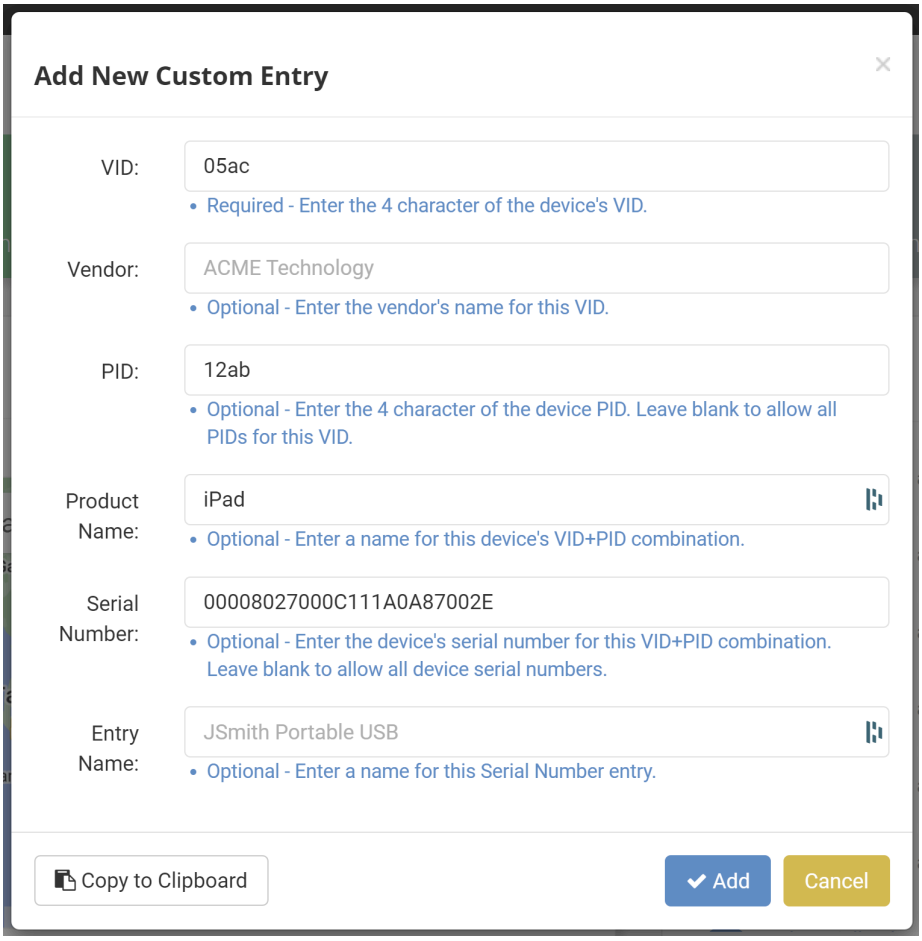
f. Expand the **Custom Entries.**

g. Select your configuration **Full Access/Read-Only/Blocked**



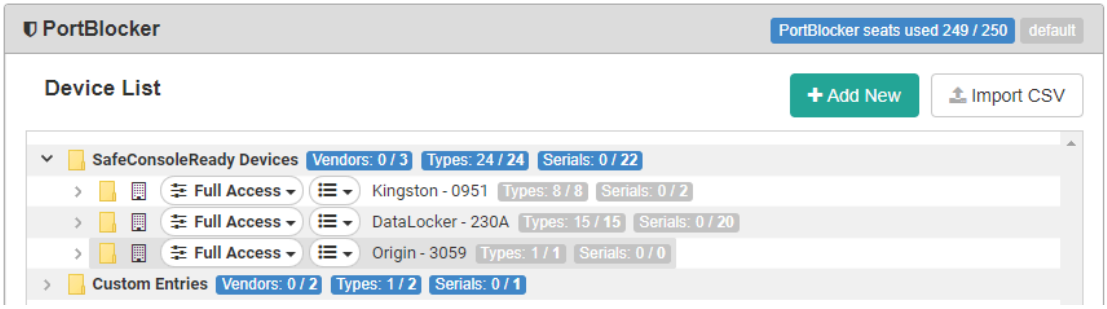
h. Click **Save** in the **Policy Editor** in the top right corner.

i. The policy will be automatically applied to the endpoint within 10 minutes. Or instantly if the policy is updated manually at the endpoint.



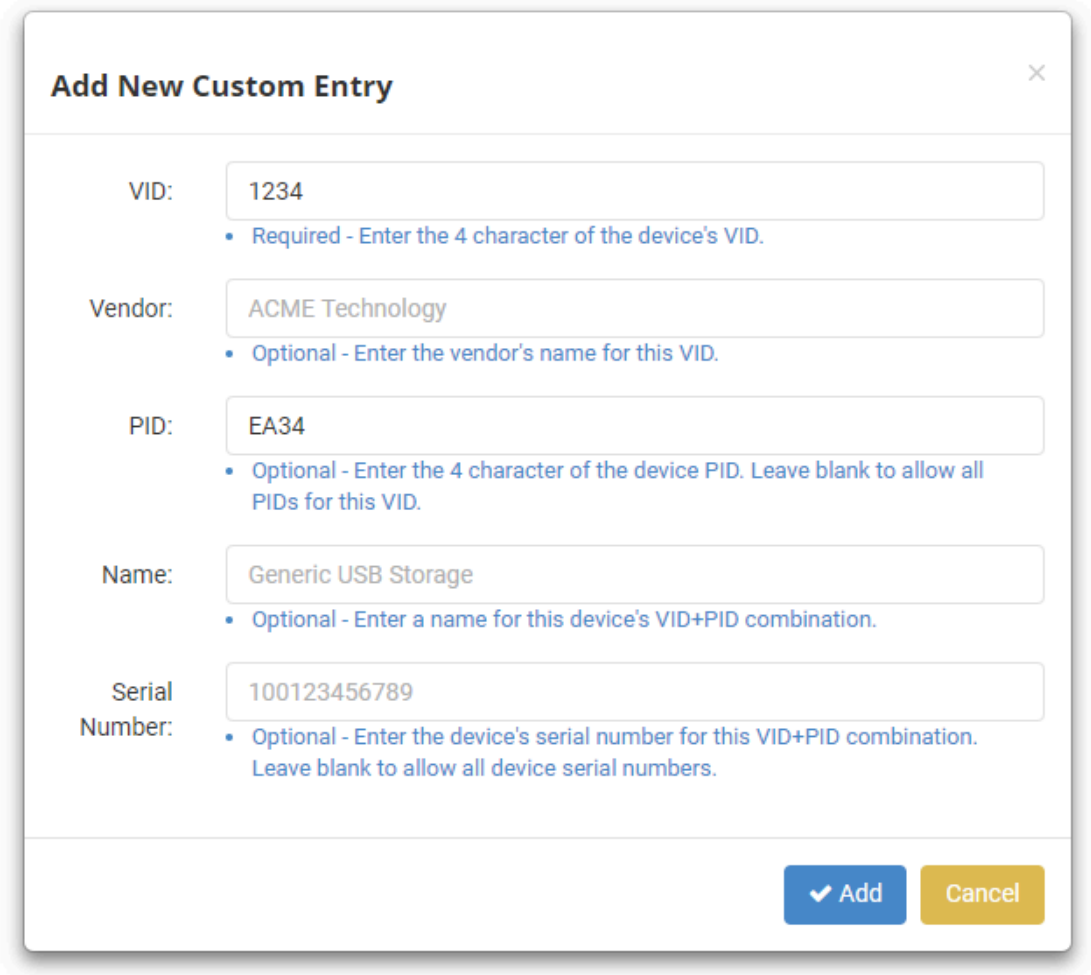
Adding a Device Manually Based on VID/PID/Serial

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

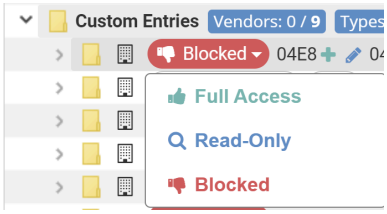


2. Enter the device information.

   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, and Serial Number as well.



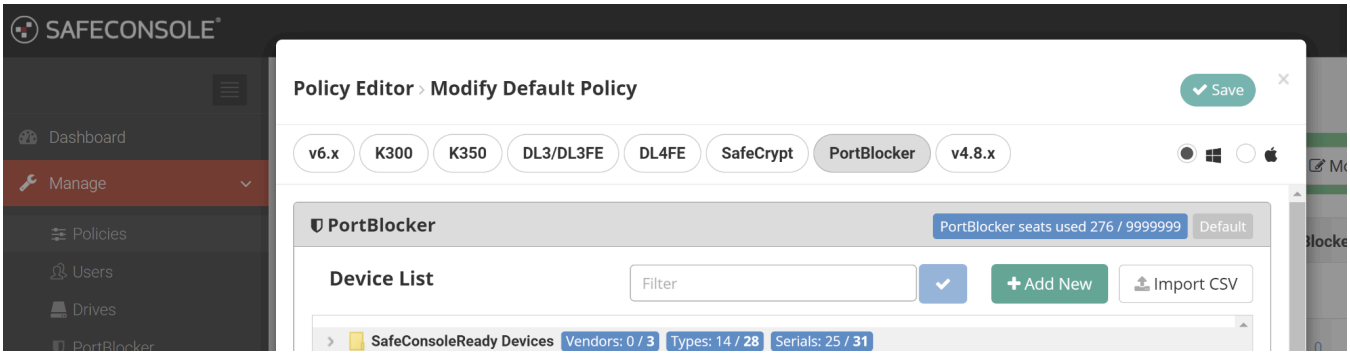
5. In the Device List Filter box enter the serial number you have copied previously and click on the blue checkmark icon next to the box.
6. Expand the **Custom Entries.**
7. Select your configuration **Full Access/Read-Only/Blocked**

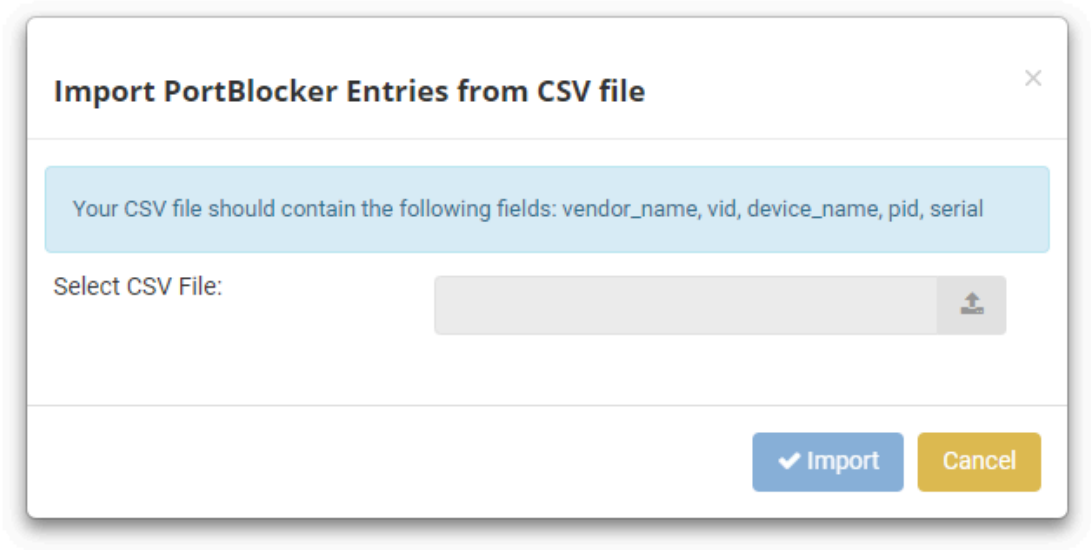


8. Click **Save** in the **Policy Editor** in the top right corner.
9. The policy will be automatically applied to the endpoint within 10 minutes. Or instantly if the policy is updated manually at the endpoint.

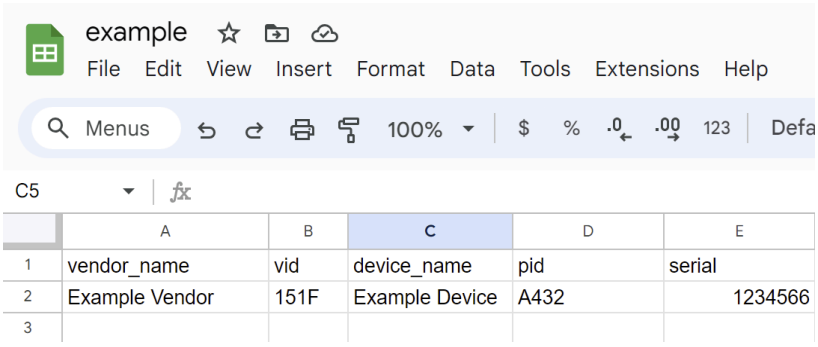
Importing Devices to Filter from a CSV-file

Administrators can add devices to the Device List by importing a CSV file. To do this, click the **Import CSV** button in the PortBlocker section of the Policy Editor, select the CSV file, and click **Import**.





The first line of the CSV file (comma-separated values) must contain the: column names: **vendor_name, vid, device_name, pid,** and **serial**, with each entry on a new row. The .csv-file is the easiest to create in any spreadsheet software. Save the created sheet as .csv.



Uninstalling PortBlocker

Uninstalling the PortBlocker endpoint application requires having admin permission to the local computer and (optional) the PortBlocker Uninstall Password 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 Microsoft **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:

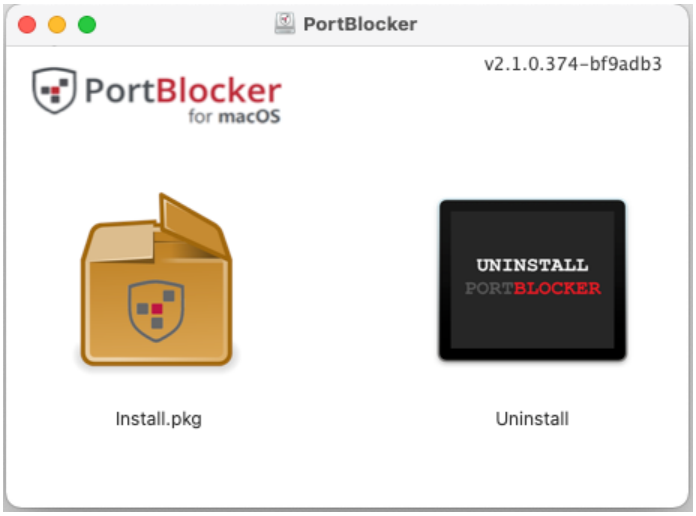
```
PASSWORD=<UninstallPassword>
```

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.

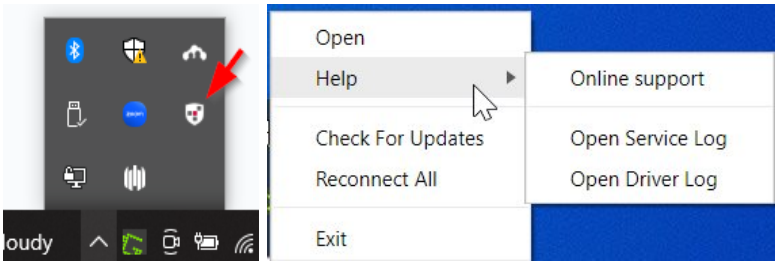


Troubleshooting

For help troubleshooting PortBlocker issues, visit the **PortBlocker Support Page**.
DataLocker Support may ask you to share the Portblocker Service and Driver Logs.

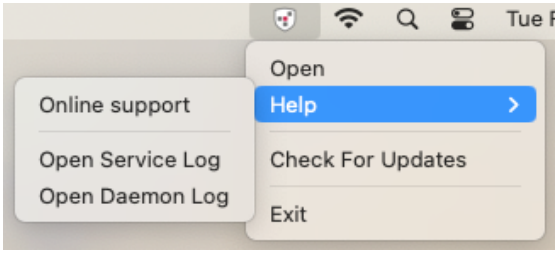
How to access the PortBlocker logs (Windows):

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 upload 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 upload to DataLocker Support.



Document Version

The latest version of this document resides at
https://media.DataLocker.com/manuals/portblocker/portblocker_admin_guide.pdf

This document was compiled on Mar 4, 2024

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**