Pro User Guide

February 6, 2024

Contents

Introduction

PC Matic Pro is for organizations looking to manage and protect their computers remotely from a central location. A single agent is deployed to each device, allowing for full control by IT from the cloud-based console. Access to your management portal is available from any supported web browser.

https://portal.pcmatic.com

PC Matic Pro consists of several parts:

- Real-time allowlist based malware protection known as SuperShield.
  - SuperShield is active and protects the computer 24/7 from file and fileless based attacks.
- An on demand malware scanner that will clean, update, and optimize each endpoint.
  - Schedule scans at several different intervals: one time, daily, weekly or monthly. Choose a start date and time and enter an email address to receive reports after the scan completes.
- A set of remote management tools that allow for full control of any device on your account.
  - This includes a VNC Agent, CMD Prompt, File Manager, and remote Reboot and Shutdown commands.
- A suite of security features to protect and prevent unauthorized access through Remote Desktop Protocol (RDP).
  - Anti-tampering protection at the device ensures malicious actors can't remove your security, and RDP Authentication ensures unknown devices can't remote into your network.

System Requirements

Optimal System Requirements

The operating systems below support the the best overall security posture for your devices and our products. On Windows endpoints and servers this includes the ELAM (Early Launch Anti-Malware) Driver that lets SuperShield run as a protected process. This prevents end users from disabling, uninstalling, or restarting the protection service.

- **Endpoint Operating System:** Windows 10 (1703) - Windows 11
- **Server Operating System:** Windows Server 2019 - Windows Server 2022
- **Mac Operating System:** macOS Monterey, Big Sur, Catalina
- **Processor:** 1 GHz or faster | Memory: 8 GB | Hard Disk: 50 GB of free space
- High Speed Internet Connection
- .net Framework 3.5 [Download]

Minimum System Requirements

- **Endpoint Operating System:** Windows 7 - Windows 8.
- **Server Operating System:** Windows Server 2008 R2 - Windows Server 2016.
- **Mac Operating System:** macOS Mojave, High Sierra, Sierra
- **Processor:** 1 GHz or faster | Memory: 2 GB | Hard Disk: 5 GB of free space
- Active Internet Connection
- .net Framework 3.5 [Download]

Best Practices

If this is your first time setting up your account, we encourage you to read the Best Practices documentation. This will give you insight into setting your account up correctly for optimal ease of use and effectiveness.

Onboarding Support

Before deploying out to a large number of devices or to all of your machines, we highly recommend consulting with our Onboarding Team. The onboarding team works with new accounts to ensure that installation and setup is as simple as possible.

During initial installs, you may see unique software that you use blocked as unknown by PC Matic Pro. This is normal, and evidence of our allowlist based approach not allowing unknown files to run. The onboarding team will assist you in expediting these unknowns to our malware research team for analysis to be globally categorized. If you have unknown files that are blocked and do not feel comfortable locally allowlisting them, please consult with the onboarding team.

onboarding@pcmatic.com

Payment Settings

Setting up Auto Pay for your PC Matic Pro account is the easiest way to manage your account and the charges for all of your endpoints. This section can be skipped if you have prepaid your account, or purchased through a reseller partner.

From the sidebar, click on Account Settings. Now on the view that opens on the right side, select Update Invoice Autopay Settings. Put a check in the box next to: Turn Auto Pay On. Fill out all of the pertinent information and click the Save button.

Missed Auto Payment

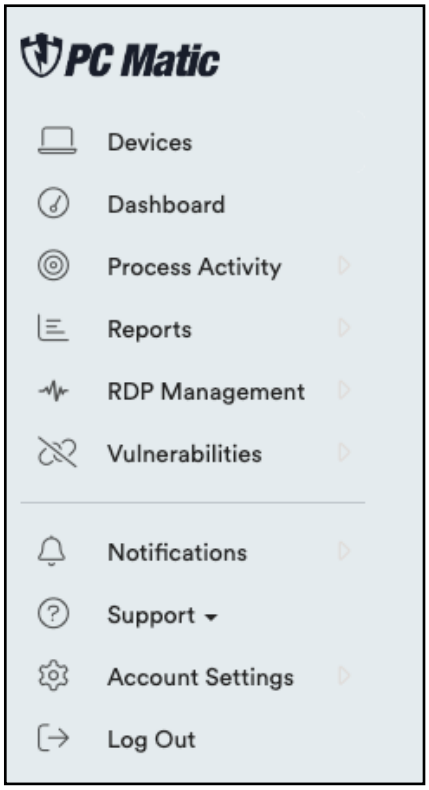
If you have overdue invoices that require payment, you must manually pay them before turning Auto Pay on. If Auto Pay is on it will not let you manually pay the invoices, but it will not automatically back pay them. Turn Auto Pay off, manually pay the overdue invoices, and then turn Auto Pay back on for future billing.

Sidebar Navigation

The sidebar in PC Matic Pro is your home for navigating your account. No matter what page of your account you're currently viewing, the sidebar adapts to give you the links that are available, and will expand into a sub sidebar to present current actions for your view.

Devices

The Devices page presents you with all of the information about each device that you are currently protecting and managing with PC Matic Pro.



Dashboard

The Dashboard page allows for customization of several account metrics and security reports so what you can see an overview of what is happening on your account.

Process Activity

The Process Activity Report is your central location to see all processes monitored in your environment. Here you can quickly see blocked processes and add exceptions for them to your local allow list.

Reports

There are several reports in this section containg details about your endpoints or activity inside management console.

RDP Management

RDP Management is a centralized location inside PC Matic Pro to manage and secure Remote
Desktop Protocol across your environment.

Vulnerabilities

The Vulnerabilities tab is home to several possible security holes or gaps in your environment.

Notifications

This tab provides information about happenings inside your account, including blocked processes, SuperShield status changes, and updates from PC Matic.

Account Settings

The Account Settings page encompasses all of your options that are available at the account level, along with any information about your account such as licensing or payment settings.

User Management

Click Account Settings from the sidebar, and then select User Management, here you can setup additional logins to your management console.

To set up a new user, click the Add User button and fill out the information for that user. Once you submit the information, a registration email will be sent to the email address so they can set a password. Now you can choose the role for the user and what levels of the account they should have access to.

User Activation/Deactivation

Next to each user there is a toggle that Activates them (when green) and deactivates them. When a user is deactivated they will automatically be logged out of any active sessions and will no longer be able to login. Users are also deactivated if:

- They have not logged in in the last 90 days.
- They attempt to log in with incorrect credentials 5 times in a 15 minute window.

User Management Notifications

User Management Notifications can be enabled for any user on the account. Turning this on will send that user email notifications about any changes that happen to users on the account. This includes creating, modifying, deleting, activating, and deactivating users.

Enforce Authentication

You can require all users on your account to use multifactor authentication when logging into the web portal by toggling this option on. Once this is toggled on, users will be prompted to enable authentication for their account on their next login. If you do not enforce the use of authentication for all users, each user will still be able to choose to use it for their own account.

User Roles & Rights

Roles

- **Account Admin** - Full account access and the ability to create and manage additional users.
- **Account Manager** - Full access to the account without the ability to create and manage additional users.
- **Group Admin** - Recommended for admin users that should be limited to certain groups.
- **Group Access** - Recommended for limited access users to certain groups.
- **Custom Roles** - Create your own Roles and assign any combination of Rights for each one.

From the Manage Roles tab you can create, edit, and delete any of the existing roles. Your account will come with the four predefined roles above. Setting up Custom Roles will allow you to choose between all of the available rights and set up a unique Role to use for each situation you have. Set your Role name and description and then assign each right that you want to save for this Custom Role.

Rights

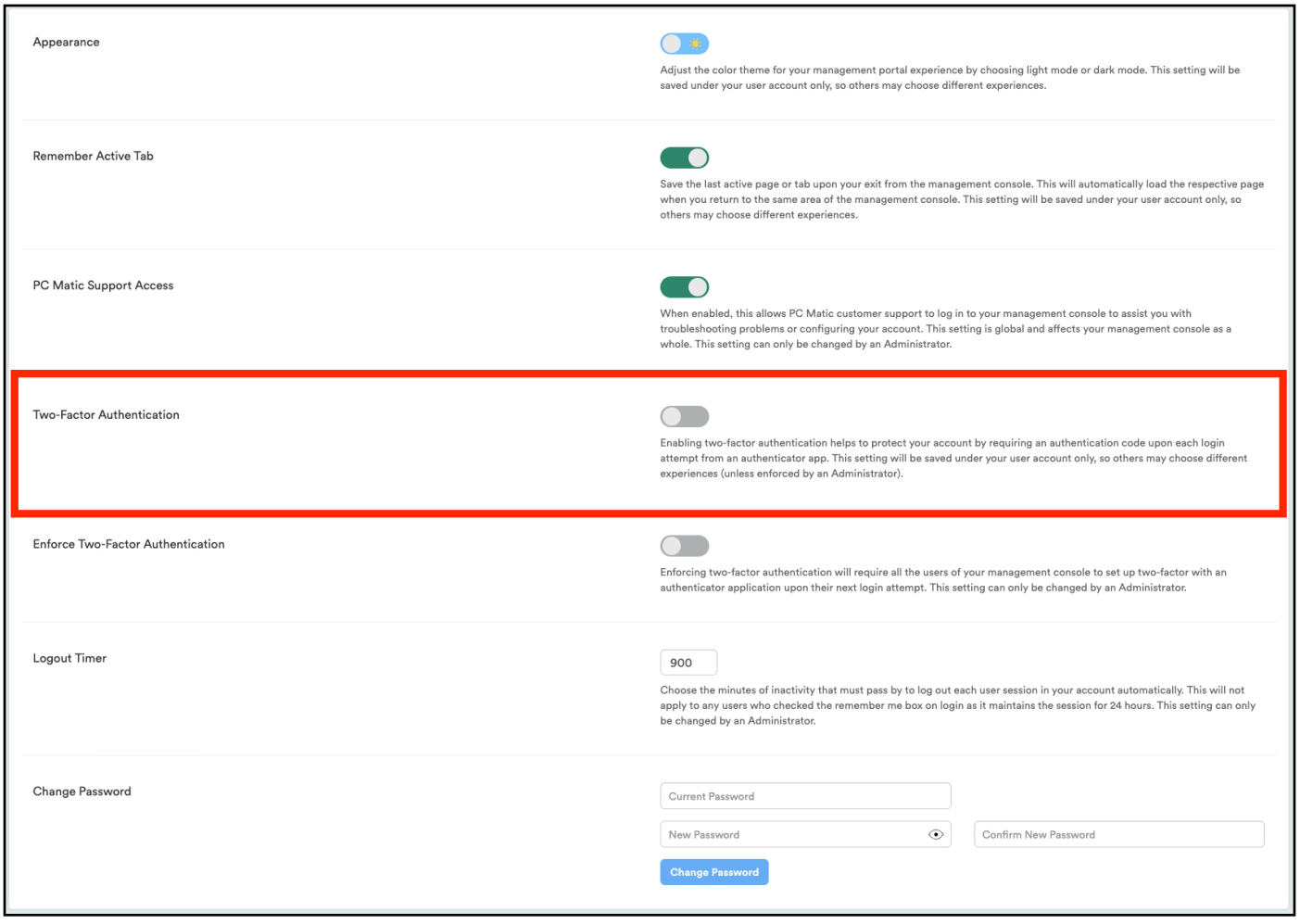
- Account Settings - Notification Contacts
- Account Settings - User Management
- Account Settings - VDI Mode Management
- Devices - Add Device Button
- Devices - Remove Device Action
- Notifications - Notification Setup
- Notifications - Security & Performance
- Notifications - PC Matic News
- Notifications - Renewal Tracking
- RDP Management - Control Center
- RDP Management - Device Allowlist
- RDP Management - Logs
- Realtime Actions - Ad Blocker
- Realtime Actions - Move Devices
- Realtime Actions - Quarantined Files
- Realtime Actions - Reboot
- Realtime Actions - Remote Desktop Protocol
- Remote Tools - Command Prompt
- Remote Tools - File Manager
- Remote Tools - Remote Access
- Scanning - Scan Now
- Scanning - Scan Scheduler
- Security - Lockout Settings
- Security - Patch Management
- Security - Uninstall/Install SuperShield
- Security - SuperShield Allow & Block
- Security - SuperShield Options
- Sidebar - Account Settings
- Sidebar - Vulnerabilities
- Account Settings - Manage Roles
- Account Settings - User Management

Authentication

Each user of your PC Matic web portal has the ability to enable Two-Factor Authentication. Once enabled, authentication requires a 6 digit code generated by a mobile app (iOS or Android) to log in to the web portal. ***Suggested authenticator apps: Google Authenticator, Microsoft Authenticator, Twilio Authy, LastPass, OneAuth, FreeOTP, andOTP, 2FAS***

Enabling Authentication

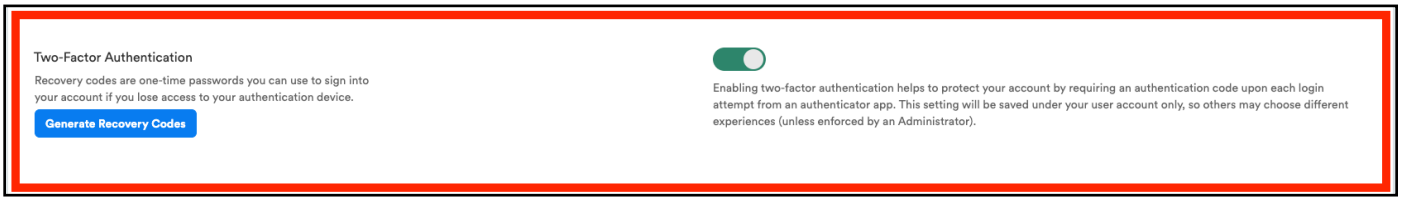
Each user can enable authentication from the **Account Settings > Preferences** page by toggling on **Two-Factor Authentication**.



The user will be prompted to scan a QR code using their chosen authenticator app. The app will generate a 6 digit code to be entered to complete setup.

Recovery Codes

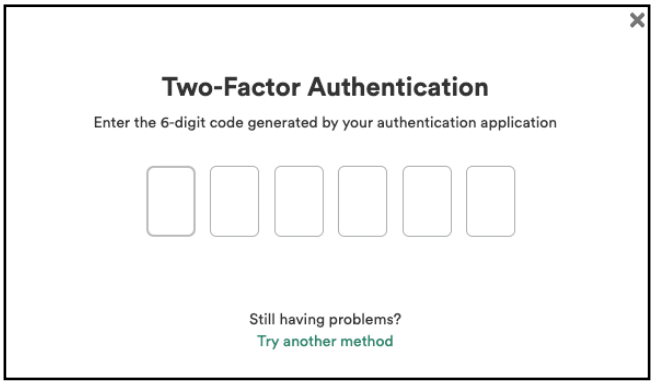
Once Authentication has been enabled, you can download backup codes that can be used if you lose access to your authenticator app. To create backup codes, navigate to **Account Settings > Preferences** and click on the **Generate Recovery Codes** button.



You will be provided with 5 backup codes that can be used as an alternative code to your authenticator app. To use the recovery code, select “Try another method” on the code prompt.

Using Authentication

Once enabled, after a user successfully enters their email address and password to login, they will be prompted to enter the 6 digit code generated by their authenticator application.



Enforce Authentication

Administrators can require all users to setup and use multifactor authentication on their account by going to **Account Settings > Preferences** and toggling the **Enforce Two-Factor Authentication** option on. Enforcing two-factor authentication will require all the users of your management console to set up two-factor with an authenticator application upon their next login attempt.

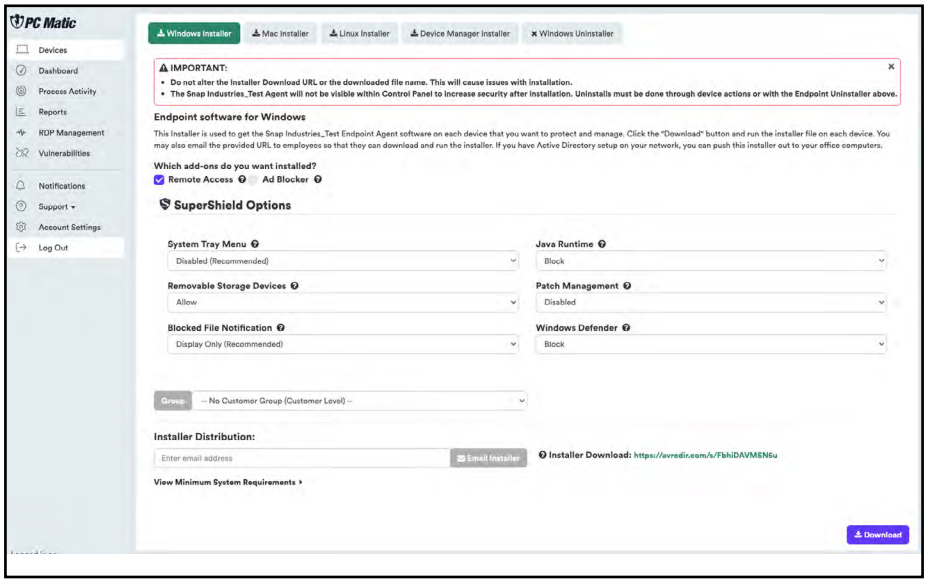
This setting can only be changed by an Administrator.

Installation

Windows Installation

To create and download a custom MSI file, from the Devices tab, click Add a Device.

The first tab, Windows Installer, is where you can customize an MSI file and choose from several different methods for deployment. Before downloading the endpoint installer, you have several options that can be customized to increase flexibility and ease of installation.



SuperShield: Our real-time security component and will stop any program from running that is not on our allowlist. SuperShield will never allow an unknown application to execute on your computer without admin permission (SuperShield is always included in the installer).

Remote Desktop: This will install our VNC Agent allowing remote access to an endpoint or server through your cloud console.

Ad Blocker: Install PC Matic's ad blocker in Chrome, Firefox, Edge, and Internet Explorer

System Tray Menu: This removes the ability of a user at the endpoint to alter the configuration of SuperShield in the system tray.

Java Runtime: Allow or block all Java activity through SuperShield. Blocking all Java activity can increase your security posture.

Removable Storage Devices: Remove the ability to connect USB storage devices. When activated any USB storage device currently connected will eject. USB peripherals will remain functional.

Patch Management: Updates third party applications automatically through SuperShield according to your settings in Software Management.

Blocked File Notification: Control what's visible and accessible to the end user when an application is blocked by SuperShield.

Groups: You can select the group that you would like to associate this installer with. It will automatically add any computer using this installer to your chosen group. If you decide to leave this box blank, you can always associate an endpoint to a group at a later time.

There are several methods to deploy the installer that was just customized.

- **Email:** You can enter an email address and the installer link will be sent there with instructions to carry out the installation.
- **URL:** You may copy the actual URL link listed below the email box and manually email it out to a group, or save the link for use later.
- **Direct Download:** Download the file to the computer you are on. This can be used on that computer, sent to a shared directory, or copied to a thumb drive and then taken to the different endpoints and installed from the thumb drive. This downloadable file is an .msi file with a unique string as the file name. ***It is very important that you do not change the filename in any way. It will cause the install to not function correctly.***
- **Silent MSI Install:** The PC Matic Pro installer MSI can also be pushed out silently using a command string. Below you'll find an example of the command string to use, filling in details like msipath with the path of the msi on the machine.'

Command String: msiexec /i "msipath" /qn /norestart

Mac Installation

From the Devices tab, click Add a Device. Then click on the Mac Installer tab.

Similar to the Windows MSI installer, you can customize the options for System Tray Menu, Blocked File Notification, and Groups for the Mac installer.

At the bottom of the window, you can download the installer, email a link to the installer, or copy the installer URL.

To install:

1. Download the pkg file onto your Mac.
2. Double click the pkg file to begin the install.
3. Click Continue.
4. Click Install.
5. Type in your administrator password and click Install Software. (The install process may take several minutes to complete.)
6. Before completion, your Mac may prompt you to allow our system extension. The system
7. extension is critical for antivirus products and must be allowed for PC Matic to protect your
8. device. Click Open Security Preferences in the prompt. (If you don't see this prompt, skip to
9. step 12)
10. In the Security and Privacy window at the bottom you will see "System Software from Developer
11. "PC Matic Tray" was blocked from loading". Click the allow button.
12. After you click allow the option will disappear and you can close the Security and Privacy window.
13. Once completed, click Close.
14. You should now see our PC Matic Mac icon appear in the Status Bar at the top of your desktop. It will display as green to show that you are protected and fully installed.
15. The console window will automatically open after install and can be closed.
16. Installation is complete!

System Extensions

Beginning with the 10.13.2 update of macOS HighSierra, Apple now restricts apps that require access to the kernal of your device which is a core part of the operating system. Almost all antivirus products, like PC Matic Mac, require access to the kernal to protect the device. This requires additional steps of allowing the system extension from PC Matic Tray for PC Matic Mac to function properly.

In macOS 10.13.2 - 10.14.6, the user alert and approval option for the system extension only display in Security and Privacy for 30 minutes after your installation attempt, so it is important that you allow it during the initial install.

If you did not allow the extension in time, follow the manual steps below to bring the Allow button back in Security and Privacy:

1. Navigate to your Applications Folder and find the Utilities Folder inside it.
2. Double click the program Terminal inside that folder.
3. Within Terminal, copy and paste the code below and press enter.
   `sudo kextload /Library/Extensions/PCMaticListener.kext`
4. You may see an error appear on screen after this, that is normal.
5. Now return to System Preferences, and open Security and Privacy. You should see the option
6. to 'Allow' the blocked system software from PC Matic Tray. Click Allow.
7. Reboot your machine.

Without allowing the System extension for PC Matic Mac either during initial install or with the manual process above, your device will not be protected.

Device Manager Set Up

The device manager installer allows you to use Active Directory to install PC Matic Pro onto your Windows endpoints. Using PowerShell along with a GPO on your server, this push install method allows us to install the client on each endpoint without needing to reboot.

Device Manager Demonstration Video: https://pcmatic.me/DeviceDemo

Prerequisites

- Server: Requires PowerShell 3.0 or higher
- Server: Requires .net Framework 4.5
- Server: Execution Policy Set: RemoteSigned
- Endpoint: Requires PowerShell 2.0 or higher

The best way to check for prerequisites on your server is to run the script below. It willbe automatically check each prereq and let you know if it has been satisfied.

- https://support.pcmatic.info/files/deviceManager/prereqs.zip

1. Download the zip above, and extract it to your downloads folder.
2. Open PowerShell as an administrator, and run the script by using a command similar to the one below.
    - PS C:\users\Administrator\Downloads\prereqs> .\prereqs.ps1
3. Note: There needs to be a '.\' in front of the file name when running it inside PowerShell. You also may get a security warning about running the script, it is safe to run from PC Matic/PC Pitstop.
4. After the script finishes running, you should see an output similar to the one below.
    - VERBOSE: Checking the .Net Framework Requirement
    - VERBOSE: Result: Meets Minimum .Net Requirement - .Net Version 4.7.2 Found
    - VERBOSE: Checking version of PowerShell
    - VERBOSE: Result: Meets Minimum PowerShell Version - 4.0 Found
    - VERBOSE: Checking Execution Policy
    - VERBOSE: Result: Execution Policy is set to Unrestricted
    - VERBOSE: All the Minimum Requirements Have Been Met

If you did not meet all of the prerequisites, it's time to make sure they are all satisfied before installing the device manager. More details about each individual prerequisite are below.

PowerShell

We need to install at least PowerShell version 3.0 or higher to satisfy the requirements. Below you'll find the download link to install PowerShell 4.0 from Microsoft. Once complete, you can check the success by opening a command prompt as an administrator and running: `PowerShell -Command "$PSVersionTable.PSVersion"`

- https://www.microsoft.com/en-us/download/details.aspx?id=40855

.net Framework

The .net Framework requirement is a little different than PowerShell in that we need exactly version 4.5 to be installed. To download and install .net framework 4.5, visit the Microsoft site below.

- https://dotnet.microsoft.com/download/dotnet-framework-runtime/net472

RemoteExecution Policy

To set the RemoteExecution Policy to RemoteSigned on your server, follow the steps below.

- Open a PowerShell prompt as an administrator.
- Run the following command: `Set-ExecutionPolicy RemoteSigned -Force`
- After the command is run, you can check the success of it by running: `Get-ExecutionPolicy`

Once all of your prerequisites have been met, you can continue to the Device Manager steps!

Active Directory Connection with Device Manager

1. Download the Device Manager from your PC Matic Pro management console. To access it, open your management console and enter the Options > Install/Uninstall tab.
2. Before you download, it's very important to enter your Active Directory Administrator credentials at the bottom of the installer window (image below). These credentials will be used to run the Device Manager service with the correct authority. Leave "Create Remote PowerShell GPO" checked as well.
3. Now, download the Device Manager onto your domain controller and run it.
4. Once complete, you can click Finish and close the installer screen. Nothing else will pop up on the server as the Device Manager works in the background for you.
5. You will however, see a new Network Devices tab arrive in your PC Matic Pro console. When you enter that area, you should begin to see the devices from your network populating into the Devices tab.

Verifications Before Install

Before you begin installations, it's important to verify that the GPO was created correctly and the Domain Controller's scheduling service is running with the proper authority.

1. Open Services on your server, and look for the PC Pitstop Scheduling service. On the right side, it should show the Log On As value as your Admin account that you entered into the console before download.
2. If it says Local instead, right click and go to Properties and the Log On tab. You can then select This Account and make sure your credentials are present.
3. Enter Group Policy Management to verify the new GPO "PCMatic Agent EnableRemotePS" has been created successfully.
4. Then enter Active Directory Users and Groups for a new user group called "PC Matic Agent Devices". The endpoints in this group should be the same as the endpoints that show within Network Devices > Devices tab in your management console.
5. To kickstart the sync process between your server and the management console, you can always run the script below. Syncs happen automatically every 30 minutes to look for installs or uninstalls but if you want it to happen faster this script will reset the clock.
    - https://files.pcpitstop.com/DeviceManager/sync.bat

The last piece to verify is that endpoints have received the new GPO that was created. This will happen automatically but it depends on what your settings are locally for each endpoints to pull in GPO updates.

To manually force a GPO update on all machines from the domain controller, run the code below in an administrator PowerShell prompt, hitting enter after each one:

```
1. $computers = Get-ADComputer -Filter *
2. $computers | ForEach-Object -Process {Invoke-GPUpdate -Computer $_.name
   -RandomDelayInMinutes 0 -Force}
```

To then check that the GPO was applied correctly, you can run the following command to generate a text file on the desktop with the results:

```
gpresult /Scope Computer /v > c:\gpresult.txt
```

After the command runs the text file should contain the following:

```
Applied Group Policy Objects
    ---------------------------------
        PC Matic Agent EnableRemotePS
        Default Domain Controllers Policy
        Default Domain Policy
```

You can also verify the new GPO by going to the Windows Firewall, then advanced and then, Inbound Rules. There should be 2 new rules named `NameRes` and `WSMAn`

Pushing Installations

Now with all of the requirements satisfied and checked, we can begin pushing installations from within the management console. Navigate back to the Network Devices area and the Devices tab. From here, make sure each device has a credential assigned to it by selecting the devices and then clicking the blue key to choose your Admin credential.

Once ready, select the endpoints you'd like to deploy to and click the green install button. Choose your installation settings and click Install. This install process will not be immediate and will depend on the amount of devices selected and the speed of the domain controller. Again, to manually speed up the install process you can reset the sync clock using the script below.

- https://files.pcpitstop.com/DeviceManager/sync.bat

Each device will begin to appear in your management console after the install completes and will have the green SuperShield icon in it's system tray.

If you have questions during the Device Manager process or run into problems, please contact our dedicated onboarding team at the email below.

onboarding@pcmatic.com

Network Devices Deployment

After the installation has completed on your server, or if you set credentials for the Device Manager before downloading, you can access the Network Devices tab. Click Account Settings and then choose Network Devices. This will give you access to all of the devices that are on your active directory network. From this view you're able to set credentials and remote install or uninstall.

There are two tabs available from this view, the Devices tab that shows all of your computers and servers on the network, and Credentials which will allow you to store admin credentials for installation. From the Devices tab you can use the check boxes at the left for bulk selection. Each icon to the right of every endpoint gives different information on the device.

1. Bulk Options
   - Select individual devices or all devices to view bulk options for Install, Uninstall, Credential Set, and Removal.
2. Endpoint Status
   - Installed: PC Matic Pro is currently installed on the endpoint.
   - Uninstalled: PC Matic Pro is currently not installed on the endpoint.
   - Pending Install: PC Matic Pro will be installed on the endpoint when the scheduler service on the server runs (1 hour max).
   - Pending Uninstall: PC Matic Pro will be uninstalled on the endpoint when the scheduler service on the server runs (1 hour max).
3. Endpoint Details
   - Displays information about the endpoints AD network, as well as current PC Matic configurations after installation.

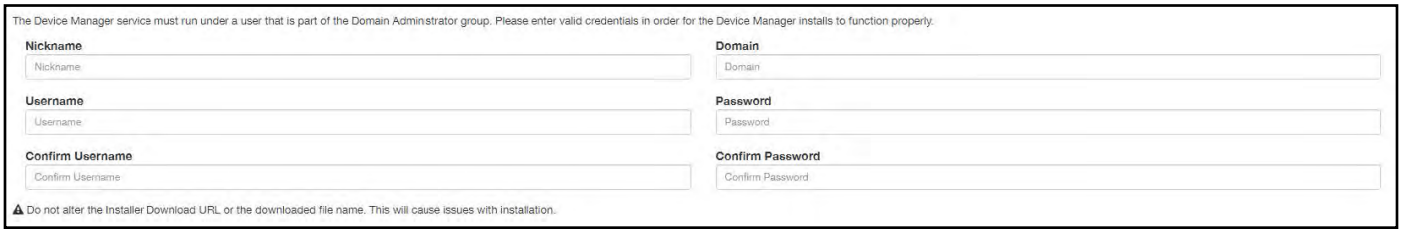
4. Install/Uninstall Endpoint Software
    - Green Icon: Push installation to the endpoint.
    - Red Icon: Pull (uninstall) client from the endpoint.
5. 5. Remove From Account
    - Before installing, this will remove the device from the device manager screen so you will no longer be able to push install to it.

Manually Add a Device

If you have any endpoints that are not currently on your active directory network, but the server with the device manager installed is able to see them they can be added by IP address or computer name. From the Devices tab you can input that device name or IP address and add the machine so that push installs can be made to that endpoint.

Credentials

The Credentials tab in the Network Devices window will allow you to save encrypted admin credentials for installation. The credentials can then be assigned to each endpoint in a bulk fashion or individually. This will allow you to push install to each endpoint even if the user doesn't have admin access on the computer.
While adding each encrypted credential, set a nickname that will help you remember each admin credential in the future. The nickname will be used to assign each credential to an endpoint before pushing out the installation. The credentials provided for each device must be domain administrator credentials for the install/uninstall to work correctly.



Use to Run Device Manager: When setting up a credential, if you haven't already chosen a credential to run the device manager under, check the box here if this credential is a Domain Administrator. **It is critical that the Device Manager is run with Domain Administrator access or installs will most likely not function correctly.**

If you change the password for a credential, the Device Manager will switch to running under the local user. Update your Credentials in this section or installs may stop working. After updating it may take 24 hours to update the service to no longer run as Local.

Push Installation Fallbacks

If the push installation attempt fails via Remote PowerShell, we have implemented two fallbacks to still attempt the install. These fallbacks will happen automatically without any need for action from you.

- PsExec
- RemoteWMI

Installing via Workgroup

You can also make use of the Device Manager to remotely deploy to your endpoints even if they're not on an active directory network. Instead of using AD we will be installing to all of the computers that are on your workgroup. This process takes a little more manual setup steps than using Active Directory but allows full push and pull control after setup.

To install via workgroup, you need to install the device manager onto a computer or server that is in the workgroup and has network access to the computers you would like to remote deploy to. This allows the device manager the access it needs to each endpoint to push or pull installations.

1. Beginning this process, make sure your workgroup is set up and all computers you would like to deploy to are in it.
2. From each endpoint, open a command prompt as an administrator and open a PowerShell prompt by typing PowerShell and pressing enter. Then type the command "Enable-PSRemoting" and answer yes to all prompts. Remember to only type what is inside the quotations.
3. Now begin the installation process by downloading the device manager and installing it on a computer or server that is in the workgroup. After installation completes, visit the Network Computers button on your group or company home page to view the list of computers on your workgroup.
4. Each endpoint is going to need it's own unique credential using this approach. You may want to nickname your credentials with the computer name so you remember which one to assign.
5. In the network devices window click the credentials tab to create or edit credentials.
6. Add in the computer's name as a Nickname so you remember which computer this is for, set the domain to the computer's name as well. Input the admin username and password and click save when complete. Repeat this for each endpoint.
7. Now from the devices tab with all endpoints and unique credentials created, assign the credentials to each computer by selecting it from the dropdown.
8. You can now push installations out to your endpoints!

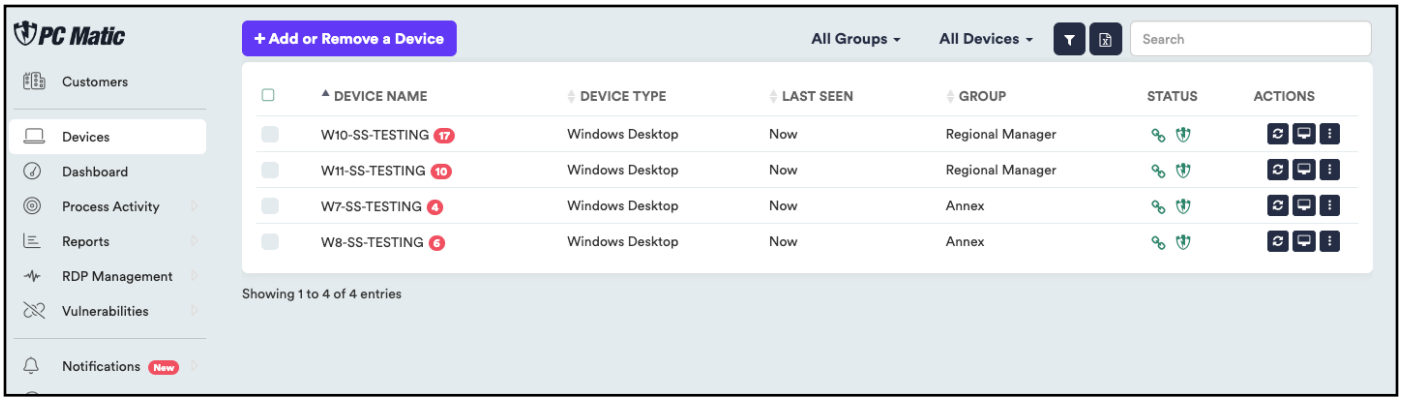
Troubleshooting Tools

The Device Manager syncs automatically with the web portal every 30 minutes to look for changes in settings or new installs/uninstalls to push out. However, if you want to manually force this sync to happen we have created a simple batch file you can run on the domain controller. You can download it below.

- https://files.pcpitstop.com/DeviceManager/sync.bat

Devices Page

The devices page serves as the default homepage of your portal and lists all devices in your network.



Click the device name to visit the Device Options page to view device details including device status, SuperShield settings and report, and to use Realtime Tools.

Use the Actions features in the right side column to create an alias, add notes, schedule a scan, use Remote Access, and remove the endpoint from your account.

Along the top row you can filter by group, device type, or search among your list of devices. Click the filter icon above your list of computers to access the Filter Devices window. From here you are able to choose a search field and query your endpoints by using and/or along with several criteria in conjunction: software installed, operating system, IP Address, software versions, and many more.
After selecting one or more endpoints from the list, bulk actions will become available. This will allow you to bulk assign computers to groups, reboot computers, inherit parent SuperShield settings, customize account lockout settings, uninstall or delete computers. You can also select all endpoints currently in this view by clicking the box with the green checkmark in the leftmost column.

After choosing a computer's name, more detailed information is available including more control over the individual endpoint. The performance meters for CPU, RAM, and available Disk Space are updated roughly every 15 seconds only while the computer is powered on and you are viewing this page.

Reports

There are several reports in this section containing details about your endpoints or activity inside your management console.

Security Summary

Displays security related events from SuperShield or the scan engine. Clicking the green headers will reveal more details about each item in that dataset.

Maintenance Summary

Displays events from manual or scheduled scans that relate to endpoint performance.

Activity

Displays account events, including deleted devices, SuperShield options changes, user login/log off and more.

Hardware Inventory

Lists all devices currently your account and their details.

Software Inventory

Lists all software installed on your devices.

Note: The information in the Software Inventory report is generated by PC Matic scans. Software from devices with no scans will not be included. For the most up-to-date report, ensure that all devices have recently been scanned.

Vulnerabilities

The Vulnerabilities tab is home to several possible security holes or gaps in your environment.

System Tray Menu

When System Tray Menu is enabled at a device, the user can access admin controls through the system tray menu to turn off protection, enable override modes, and more.

Prompt for Override

With prompt for override enabled, the user can choose to allow or always allow an application that PC Matic is going to block.

Remote Desktop Protocol

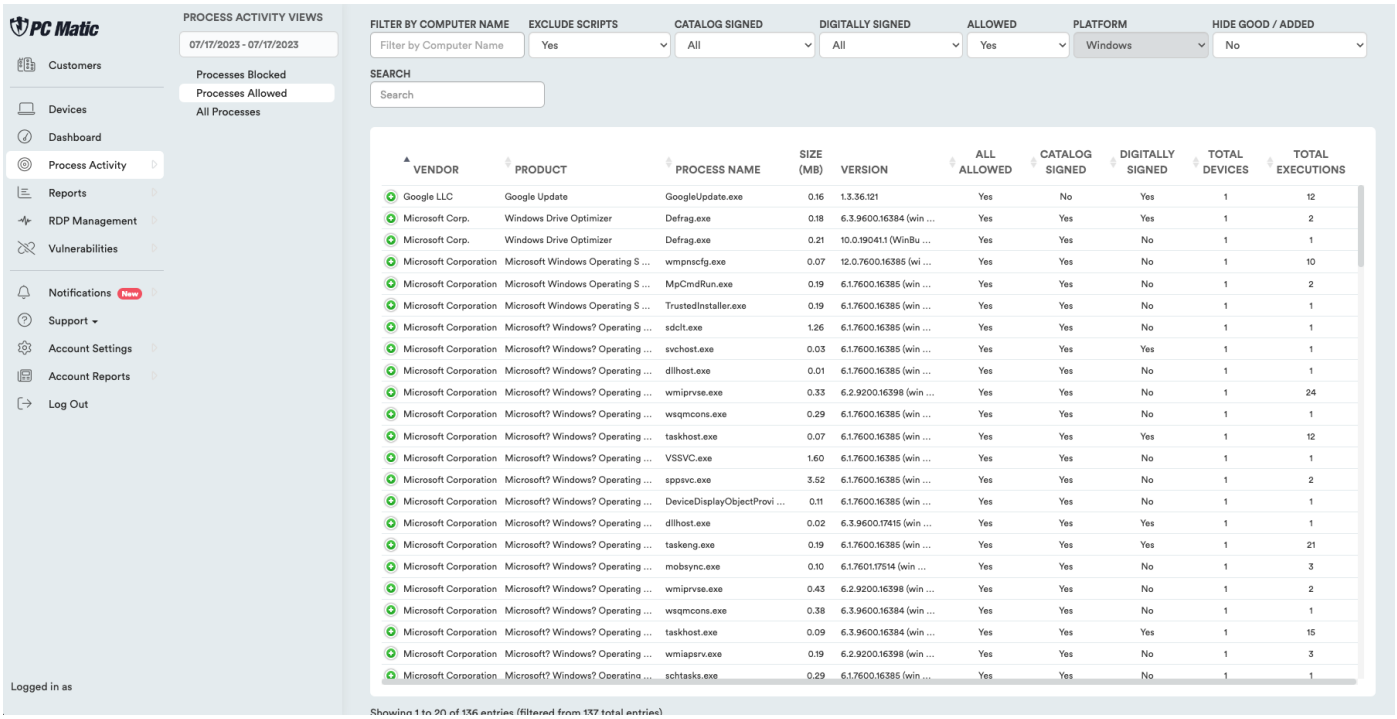
Remote Desktop Protocol can open opportunities for brute force attackers to gain control of an endpoint. This report shows all devices with RDP enabled, what port it is enabled on and a toggle to turn it off. You can read more about RDP security here.

Account Lockout Settings

PC Matic Pro automatically sets the Windows Account Lockout Threshold to stop brute force attacks. Our default settings/recommendations are 10 incorrect attempts (Threshold) within 5 minutes (Duration) to lock the account for 5 minutes (Observation). You can read more about this setting here.

Process Activity

The process activity report displays all available information about processes, blocked or allowed, across each machine on your account. You can filter this report in several different ways to review this activity, and allow applications that were blocked from running.



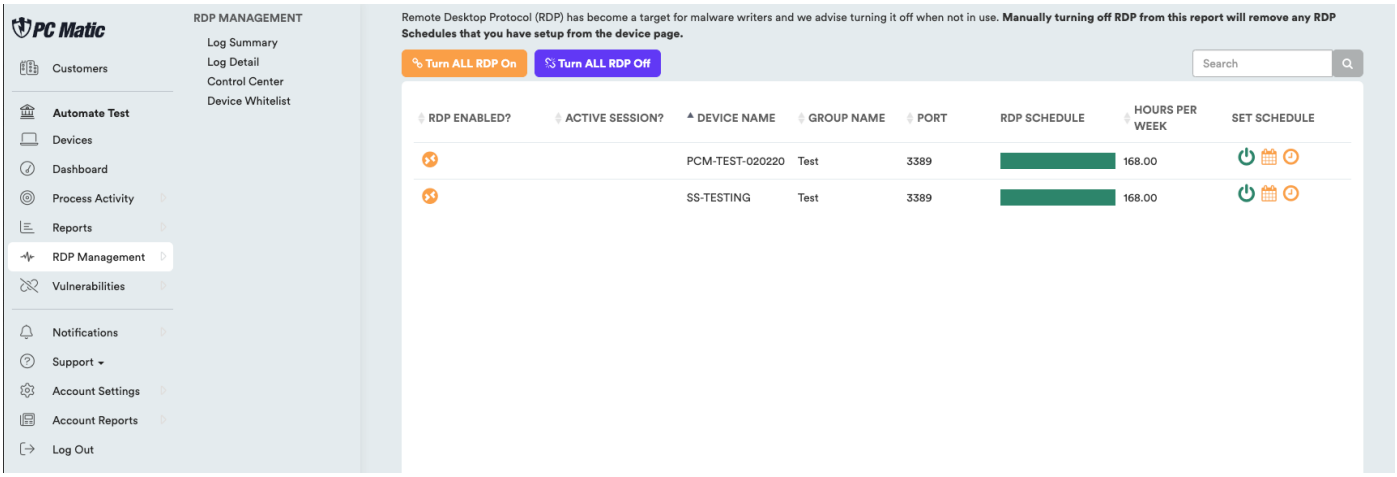
Using the sub sidebar on the left side, quickly navigate to sub sections of this report that you want to see. To allowlist a process that was blocked, select Recent Processes Blocked (today) or Past Processes Blocked (last 7 days) and expand the item you wish to allowlist. The fourth tab, Block/Allow will let you see what levels this process is already allowlisted for and add it or remove it from levels in your account.

At the top of the report you will find several filters you can use to adjust the results, these will correspond with the tabs on the left hand side as well.

- Catalog Signed - Catalog Signing is another method of digitally signing a large amount of files together.
- Digitally Signed - If a file is digitally signed by the publisher, it provides an extra layer of security and another way to identify the file itself. This also means that you could locally allowlist that publisher's digital signature and any software that they sign with that certificate would be allowed to run at the level you chose.
- Allowed - Set to Yes or No, this filter will only show you processes that were either allowed to execute on your machine, or were not allowed to execute.

RDP Management

RDP Management is a centralized location inside PC Matic Pro to manage and secure Remote Desktop Protocol across your environment. You can access RDP Management by clicking it in the sidebar on the left hand side of your management console. Inside, you'll find four main components, Control Center, Log Summary, Log Detail, and Device Allowlist. Throughout PC Matic Pro you will also notice other areas where RDP can be managed and monitored such as in the Device list or on each device's page.



Log Summary

The Log Summary provides a summary of all RDP sessions on your account.

Log Detail

The second tab inside RDP Management provides a central place to audit your RDP history. The RDP Log maintains a permanent record of attempted and successful RDP sessions on any of your devices that are secured by PC Matic Pro. This includes IP Address, Device Name, Location, Session Duration, Login Username, Active Status, and more.

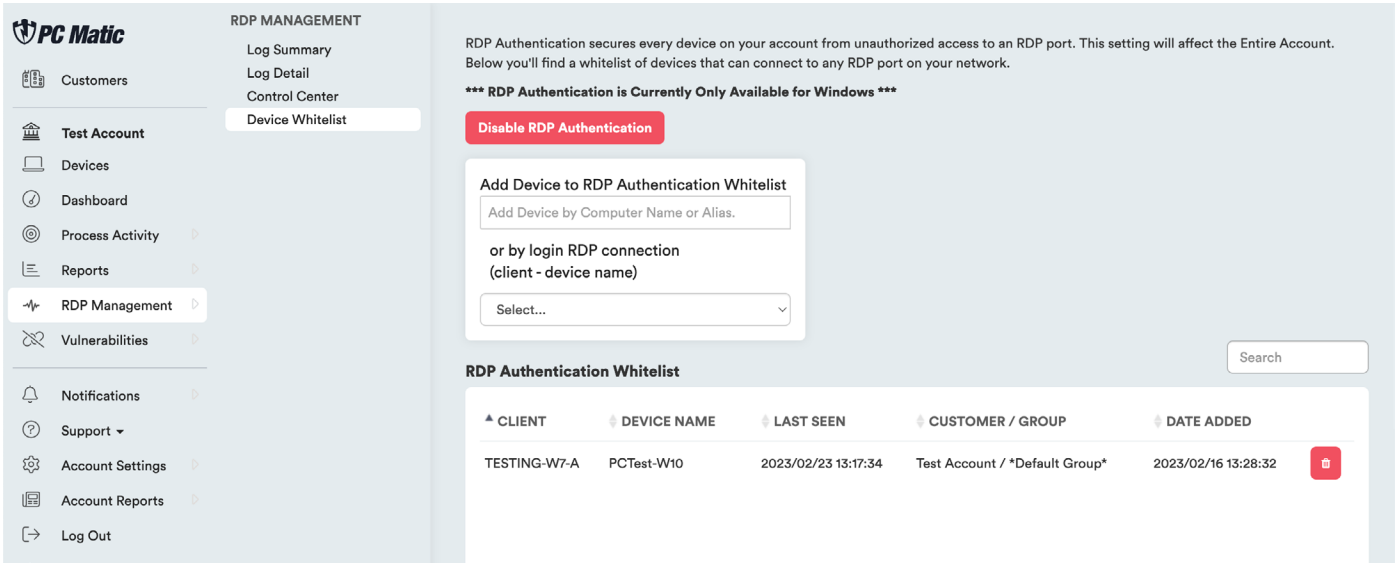
Control Center

The Control Center is where you will manage RDP on the machines in your environment. Control Center will display all of the devices that are currently on your account and information about the current RDP status and schedule for each device.
Left to right in the image above:

- RDP Enabled? - An orange icon indicates RDP is currently set to enabled on this device.
- Active Session? - During an active session, a green eye will display where you can click to view information about and kill the current session.
- Device/Group Name - Device and Group name of that machine.
- Port - The current port that RDP is configured for, whether enabled or disabled.

- RDP Schedule - This graphically shows the current schedule for RDP on each device with green representing time that RDP is enabled.
- Hours Per Week - The total number of hours per week that RDP is set to be enabled.
- Actions - A set of three actions, a toggle to fully enabled or disable RDP, a calendar to set a reoccurring schedule, and a clock to set a temporary window in the future that RDP will be enabled.

Device Allowlist



PC Matic Pro uses allowlisting to protect your RDP ports on your network. The RDP Allowlist Client Devices tab allows you to enable our RDP Security and control your device allowlist.

Using a default-deny approach, any device that is not on the allowlist and attempts to initiate an RDP session will be blocked. You can receive realtime alerts about these sessions as well that include quick actions to take and all information about the session attempt right inside the alert.

With RDP Authentication enabled, unknown devices that attempt to establish an RDP connection to any of your devices will be blocked.

You can add a device to your RDP Allowlist by device name or alias, or you can select a device from a previously blocked connection attempt.

Device Options

From an individual device page the available controls are significantly expanded. In the Options menu you can make changes to a device no matter where it's physical location is. Some of these options will be further detailed in their own chapters. Scanning, Remote Tools, and Realtime Actions require that the device is online and connected to our servers. You can verify it's connection by checking the status icons.

Scanning

Scan History

View the results from previous scans.

Scan

- **Scan Now** - Run a scan on this machine with the time set to 'Now'. This scan will run instantly with the default PC Matic Pro scan settings.
- **Next Test** - View the time and date for the next scheduled scan, or view and edit all scheduled scans for this device by clicking the date.
- **Last Test** - View the most recent scan report for this device by selecting the date and time.

Notifications

Notification Options

Toggle notifications on/off and adjust frequency settings.

Notification Setup

Select which notifications to send to contacts. (Contacts are managed under Account Settings > Notification Contacts.)

Notifications

View the notifications for this device.

Remote Tools

Command Prompt

Access an administrator command prompt from your management console to take action and query information from your endpoints without having to remote in or physically visit that machine.

File Manager

The file manager allows you to easily copy files back and forth between your machine and any device on your account. This ability is only recommended for skilled users, and PC Matic is not responsible for any issues resulting from modifications you make.

Remote Access

Initiate a remote desktop session using our modified VNC client. The PC Matic Pro client must

be installed on both the target device and the host. The target computer must also be online and connected to our servers for the session to begin. This session does not require user approval but it will notify the user that someone is currently connected.

Reports

Device Status - Displays the current device status.
Installed Software - A list of all installed software.
Largest Files - List of the largest files on the device. (Requires a PC Matic scan.)
Maintenance Statistics - A summary of removed malware, patched vulnerabilities, blocked files, junk removed, etc.
Performance Trends - Comparison over time of Processor Clock Speed, Memory Speed, CPU Load, Memory Load, Hard Drive Space, and Internet Download Speed.
RDP History - If RDP is enabled, RDP connection history is reflected here.
System Specs Report - Displays system hardware specs.

Security

Custom Allowlist

Add files to your Custom Allow List using the MD5 file hash, Digital Signature, Script, or File Path.

Custom Blocklist

Add files to your Custom Block List using the MD5 file hash, Digital Signature, Script, or File Path.

Lockout Settings

Account Lockout Settings lets you apply or override the PC Matic Pro defaults. We automatically set the threshold for each device but here or in the device tab, you can customize or turn off our defaults.

Patch Management

PC Matic Pro will maintain patches for 33 third party applications. You can enable/disable and set the max version for individual devices here.

SuperShield

Uninstall - Remove SuperShield from a device from the management console. This will remove our real time protection component, it can be re-installed through the console after uninstall.
Restart - Send a remote command to restart the SuperShield realtime service. This can be used to troubleshoot any issues with a red shield displaying in the web portal or at the users device.
Bandwidth Control - Restrict the amount of network communication SuperShield has on your devices. This feature will impair overall product functions but will not compromise security.

- Level 1 - Ignoring activity uploads will not send information to your management console about all of the applications SuperShield is monitoring. This may affect your ability to locally allowlist or blocklist applications.

- Level 2 - Ignoring sample uploads will stop our malware research team from being able to analyze your unknown files quickly. They could still receive the same sample from another user, but this may increase the time it takes for your false positives to be globally categorized.
- Level 3 - Ignoring file information uploads will result in our malware research team not knowing information about the unknown files SuperShield is blocking on your machine Unknown files cannot be globally categorized without this information.
- Level 4 - Ignoring definition updates will prevent your machine from downloading updates to our global allowlist. You may see an increase in false positives.
- Level 5 - Ignoring SuperShield updates will restrict you from receiving our software updates. These updates often add features, security, or stability fixes to our products.

SuperShield Options

SuperShield Options will allow you to set security settings at the device level and will take immediate effect.

SuperShield Report

The SuperShield shows every application that SuperShield is monitoring on your device and will also show any that have been blocked. Here you can locally allowlist an application for your device.

Realtime Actions

Ad Blocker

Install or Uninstall the PC Matic Ad Blocker on this device. The Install action will add the Ad Blocker to Chrome, Firefox, Edge, and Internet Explorer.

Move Device

Individually assign this device to a group or move it to a new group.

Quarantined Files

After a scan has quarantined a file you can restore it back to its original location or delete it forever. Be sure to allowlist this item locally as well to avoid future quarantines.

Reboot

Execute a remote reboot on this device. This reboot will cause a window to appear on the device that warns the user of a reboot in 30 seconds by PC Matic Pro.

Refresh Definitions

Updates the SuperShield virus definitions.

Remote Desktop Protocol

Fully control RDP on this individual device. On/Off allows you to completely turn RDP on or off. Temporary provides a one time opening period for RDP on this device; while schedule allows you to set a reoccurring time period that RDP will be enabled. If a schedule is set and you fully enable or disable RDP using On/Off it will clear your schedule.

Command Prompt

The Command Prompt in PC Matic Pro is available from the Actions section for an online device. This is a 32bit command prompt operating out of the SysWow folder with administrator privileges. You can use the command prompt to carry out a wide variety of actions, but we have included some suggested commands below that may be beneficial.

Command	Description
ipconfig	Check IP information for this device.
dir	View the current directory.
cd	Change to another directory.
sc start	Start a service. (Ex: sc start “PCPitstop Realtime”)
sc stop	Stop a service. (Ex: sc stop “PCPitstop Realtime”)
ping	Ping another IP address.
ver	Check the current Windows Version.
tasklist.exe	Check running tasks.
Taskkill /IM <taskname.exe> /F	Kill a task.
schtasks /delete /tn “task name” /f	Delete a scheduled task.
powershell -Command “restart-service ‘PCPitstop Scheduling’ -force”	Force a full restart of the PC Pitstop Scheduling service with powershell.
%SystemRoot%\Sysnative\msg.exe * Message goes here.	Send a popup message to a 64 bit machine.
%SystemRoot%\System32\msg.exe * Message goes here.	Send a popup message to a 32 bit machine.

There are several commands you can use to help troubleshoot problems within PC Matic Pro, or to get more information about your PC Matic Pro installation.

Show SuperShield version number:

wmic datafile where name=”C:\\Program Files (x86)\\PCPitstop\\SuperShield\\PCMaticRT.exe” get Version /value

Stop/Start PC Matic Pro’s Scheduling service:

sc stop “PCPitstop Scheduling” && sc start “PCPitstop Scheduling”
or
wmic SERVICE WHERE Name=”PCPitstop Scheduling” call startservice
wmic SERVICE WHERE Name=”PCPitstop Scheduling” call stopservice

Ad Blocker

PC Matic Pro includes ad blockers for your favorite web browsers (Chrome, Firefox, Edge, and Internet Explorer). These extensions can help cut down on network traffic and annoying ads you see browsing the web. In Chrome, you'll also be protected from Tech Support Scams locking down your web browsing session.

You can install the PC Matic Ad Blocker on every browser we support on the device by selecting the Ad Blocker option within Install/Uninstall. However, the Edge extension will not automatically install like Chrome and Firefox. After installation and the machines first reboot, Edge will automatically open to a landing page with instructions for the user to finish installing the PC Matic Ad Blocker.

You can also manually install the Ad Blocker on any device by visiting the links below on that device for Chrome and Edge.

Chrome - https://chrome.google.com/webstore/detail/pc-matic okmhneofinpilciglijihehjpaegledb

Edge - https://www.microsoft.com/en-us/p/pcmatic-for-edge/9pddhxb4×8p6

Remote Access

In order for the remote desktop application to function properly, the host as well as the client must have the PC Matic Pro VNC agent installed. The VNC agent that runs this feature is embedded in the installer under Remote Desktop and uses port 5500 & 5900.

1. Select the Devices tab from the sidebar, and select the device name that you wish to remote into. You can also click the Remote Access shortcut from the device list in the Actions row.
2. Click Remote Access from the sub sidebar and then choose the blue Remote Login button to initiate the session and approve the dialog boxes that ask if you wish to proceed.

The VNC client will open a new window, and within a few seconds give you access to the selected computer to control the desktop. This does not require user approval at the device but will notify the user of an active remote connection.

Icon Descriptions

	Device Powered Off		Number of Notifications
	Device Powered On		RDP Active
	“SuperShield is paused, please start it.” “SuperShield is unlicensed, contact your administrator immediately.” “SuperShield is not installed, please install it.” “SuperShield is turned off, please turn it on.”		“SuperShield is operational and detects applications that need updates”
	“SuperShield is installed & running properly”		SuperShield

Status Details

With the use of WebSockets in PC Matic Pro, we are able to see live information about each endpoint from within the management console. To give you more information about this connection, and troubleshoot problems, you can consult the connection status row.

In the image below, you can see the details for your current connections. In this example the computer we have selected is connected to our servers. If it was disconnected, a red X will display between two entities that are currently disconnected. The icon will also turn gray if it is not currently connected. The only exception is our server icon, which will always display as orange.

Scan Components

Malware Scan (Quick, Full, None)

Choose to clean up malware and PUAs (Potentially Unwanted Applications).

Update Software Vulnerabilities

We will automatically update 30 third party applications and make sure to keep each on the latest version and maintain the security of the program. (Java, Adobe, iTunes, Skype, etc.)

Update Drivers

Update drivers to the latest version if necessary.

Improve Performance

PC Matic Pro contains several components that will help improve the overall performance of your endpoints.

- Scan System Restore
- Scan Startup Programs
- Scan and Clean Junk Files
- Scan Benchmarks
- Scan Internet Settings
- Scan Installed Software
- Scan and Apply Performance Tweaks
- Scan Running Processes
- Scan Services
- Scan Memory Utilization
- Scan and Clean Sched Tasks
- Scan Bandwidth

Scheduling a Scan

Scans can be scheduled at multiple levels. The Scan Scheduler tab allows you to schedule or edit a scan for any level of your account. This allows you to easily maintain a large amount of endpoints by only configuring one scan or manage several different scans in one place. The Scan Scheduler is accessible from the Account Settings tab. Here you can also set up a group scheduled scan for a target group inside your account.

Lastly, from the devices tab under each device, click Scan in the Actions menu and then Next Test. This will allow a scheduled scan for the individual machine independent of all other endpoints.

Scheduling a Scan

1. Click Account Settings and choose Scan Scheduler.
2. Select Add Schedule in the upper right and choose your level and frequency options.
3. Adjust your scan settings to suit your needs and press the “Save” button when finished. After the scan finished, the results will be emailed to your registered email address shown. You may add another email address and delete the original if you wish.

Live Scan Status

From an individual device page you can now monitor the live status of a scan. This provides more information on what stage the scan is in and when it will be close to concluding. From this view you’ll also see rotating messages with information about the scan process within PC Matic Pro. It’s important to note that these messages don’t coordinate with the running scan. The same sections will rotate through, and this doesn’t mean that the section displayed is included in the scan currently running.

Patch Management

PC Matic Pro will maintain patches for the selected third party applications listed below:

- 7-Zip
- Adobe AIR
- Adobe Flash Player ActiveX
- Adobe Flash Player Plugin
- Adobe Flash Player PPAPI
- Adobe Reader
- Adobe Reader MUI
- Adobe Reader XI
- Adobe Shockwave
- FileZilla
- Foxit Reader
- Google Chrome
- iTunes
- Java 32
- Java 64
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019
- Mozilla Firefox
- Mozilla SeaMonkey
- Mozilla Thunderbird
- OpenOffice
- Opera
- PDF Creator
- PDF XChange Viewer
- QuickTime
- Real Player
- Safari
- Skype
- Winamp
- WinRAR
- WinRAR5.X
- WireShark

Within the reporting section you can view recent updates that have happened on all endpoints. On the right hand side will be a result code. If this code is 0 then the application installed correctly and was updated. A different code may display if the update did not complete and can appear for a variety of reasons. If you're concerned about a result code that is not 0 please reach out to our support team. Contact information for our team can be found in the Support section of this user guide.

Adjusting Application Updates

Within Account Settings > Patch Management, you are able to toggle each piece of software off at the level you choose from the top of the window. For example, you can select a certain endpoint from the list, and toggle off Adobe Reader if you do not want PC Matic Pro to update Adobe Reader on that endpoint.

To implement version controls, you can enter the version for that piece of software across your desired level that you would like it to remain at. This means we will not update past that version number. Then when you decide you would like to push out updates you can increase that version number.

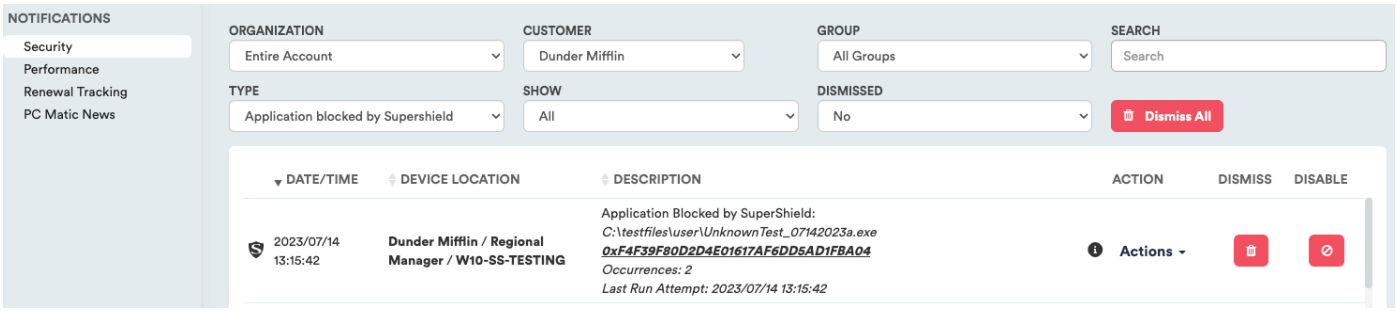
The Patch Management section places restrictions on the updates that happen during the scan process and through SuperShield. It's important that if you only want updates to happen during your scheduled scan time, you turn Patch Management off in SuperShield Options.

Microsoft Exchange Updates

PC Matic will update Microsoft Exchange Server 2013, 2016, and 2019 if they are 2 revisions behind the latest version. PC Matic will only perform the update if we are able to with the correct permission on the machine. Once the update begins PC Matic will automatically reboot the machine each time required and display the progress on the screen depending on what step of the process we are in.

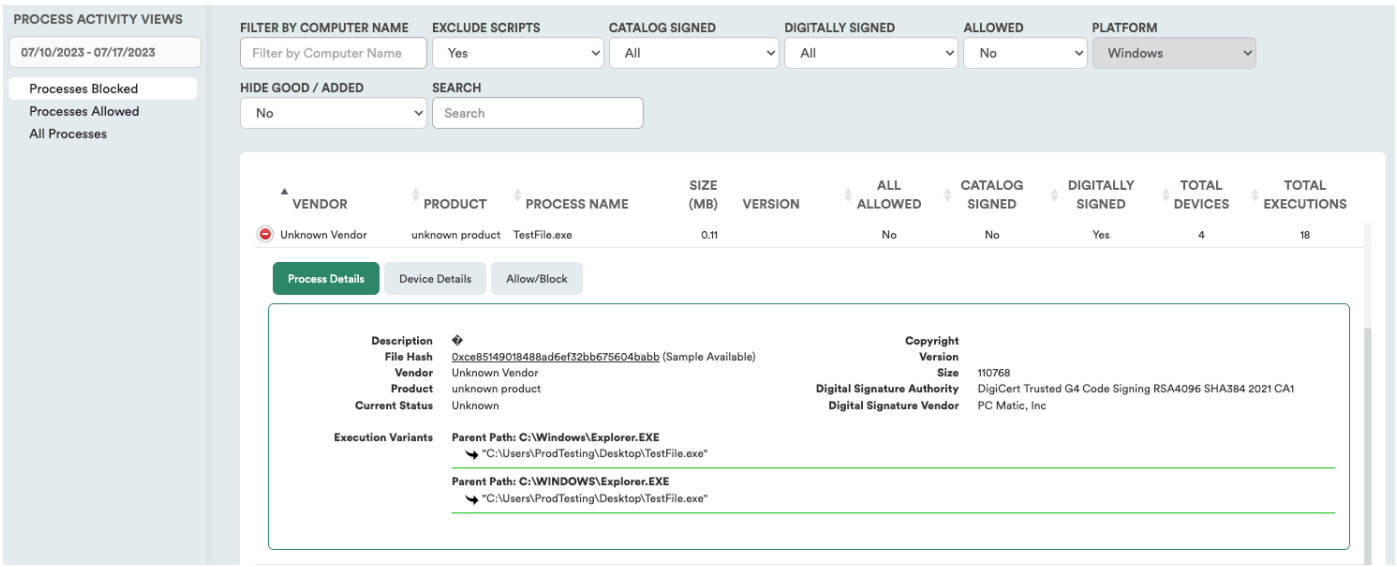
Allowlisting

With PC Matic Pro, you get full control over local allow and block lists for several different components of the program. This allows you to immediately handle a false positive from your management portal so business can continue as usual. This is most useful when dealing with your own proprietary software that PC Matic or SuperShield may not yet recognize.
In this section we will cover the variety of ways you can allow within PC Matic Pro, and all of the different components that can take advantage of a local allowlist.



Security Notifications

The quickest way to allowlist a file is from the Notifications page on the Security tab. By default, the notifications are arranged with most recent at the top and can be filtered by Type to display files blocked by SuperShield. To allowlist (or blocklist) a file or script, select the Actions dropdown in the Actions column and select a level to add it to the Custom Allowlist (or Blocklist).

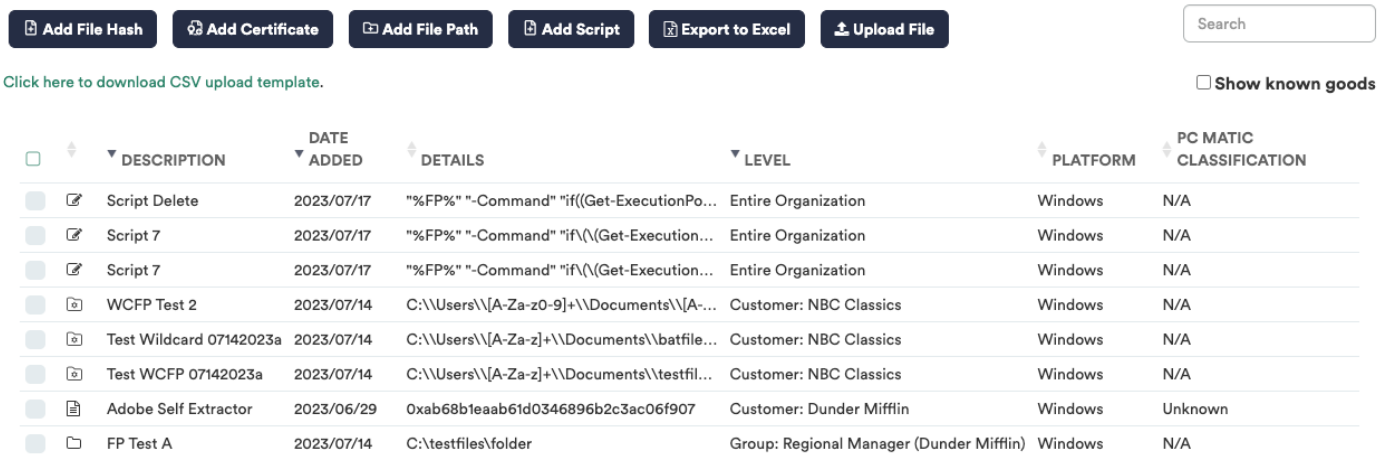


Process Activity

This report contains the most detailed information about blocked and allowed processes. Right from your home page you can access the tab. Inside the Processes Blocked report you can review any process that was blocked inside your environment and add it to your Custom Allowlist.

Custom Allowlist & Custom Blocklist

After selecting Account Settings or a single Device, you can now navigate to the Custom Allowlists or Custom Blocklist tab in the sub sidebar. We will use Custom Allowlist for this example. You can add an item to the local allowlist by selecting either MD5, Digital Signature Thumbprint, or File Path from the dropdown menu.



DESCRIPTION	DATE ADDED	DETAILS	LEVEL	PLATFORM	PC MATIC CLASSIFICATION
Script Delete	2023/07/17	"%FP%" "-Command" "if((Get-ExecutionPo...	Entire Organization	Windows	N/A
Script 7	2023/07/17	"%FP%" "-Command" "if\(\(Get-Execution...	Entire Organization	Windows	N/A
Script 7	2023/07/17	"%FP%" "-Command" "if\(\(Get-Execution...	Entire Organization	Windows	N/A
WCFP Test 2	2023/07/14	C:\\Users\\[A-Za-z0-9]+\\Documents\\[A-...	Customer: NBC Classics	Windows	N/A
Test Wildcard 07142023a	2023/07/14	C:\\Users\\[A-Za-z]+\\Documents\\batfile...	Customer: NBC Classics	Windows	N/A
Test WCFP 07142023a	2023/07/14	C:\\Users\\[A-Za-z]+\\Documents\\testfil...	Customer: NBC Classics	Windows	N/A
Adobe Self Extractor	2023/06/29	0xab68b1eaab61d0346896b2c3ac06f907	Customer: Dunder Mifflin	Windows	Unknown
FP Test A	2023/07/14	C:\testfiles\folder	Group: Regional Manager (Dunder Mifflin)	Windows	N/A

File Hash

The MD5 is a unique hash for an individual file. Adding an item to the allow list by MD5 will ensure that one individual file will always run on the devices in the level you allow it for.

Certificate

Allowing a Digital Signature will allow all files to run that are signed by that signature. You can use this if you are developing your own software internally or have a publisher that is being blocked by PC Matic. Enter the thumbprint (fingerprint) for the signature.

File Path

This feature should be used with caution. Allowing an entire folder path will let anything run from within that folder. This will decrease your overall security posture. Specific folders can be allowed if absolutely neccesary. Any folder or file below that path will be allowed to execute even if it is unknown.

Script

If you are creating or using custom scripts that are blocked by PC Matic you can allowlist them by adding in the Command Line used and a description for the script.

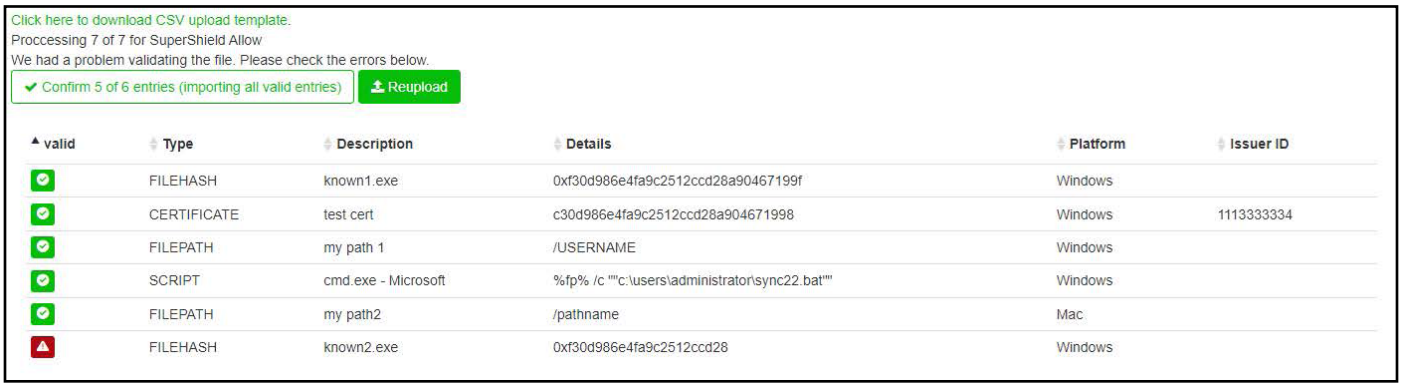
Options

- Export to Excel - Export your Custom Allowlist to an Excel spreadsheet.
- Show Known Goods - By default, files classified as Known Good by PC Matic are hidden from the list. Check the box to show them.

Bulk Upload

You can upload a CSV file with multiple items to be added to your allowlist or blocklist. The CSV upload feature supports adding files by MD5, Digital Signature Certificates, File Paths, and Scripts. You can download a sample CSV upload template to ensure correct formatting of the file for upload. To upload your CSV, click the Upload File button and select your file. The file will then be processed and the page will display the files to be added to your allowlist or blocklist.

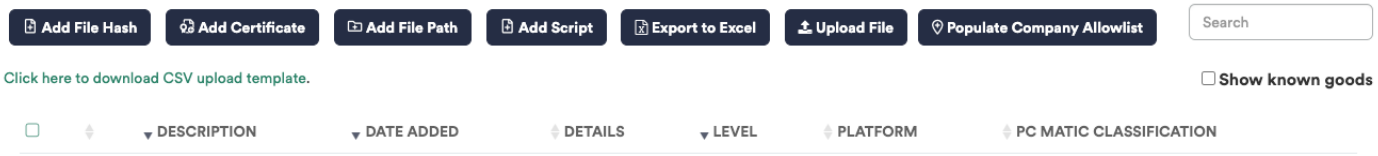
Properly formatted items will have a green checkmark and are automatically added to the allow/block list. You can click the Refresh SuperShield List button to see the updated list with your imported items.



Incorrectly formatted items will display a red alert icon. These items will not be imported. You can then click the Confirm button to import just the valid entries, or select the button to reupload a file with corrected data.

Populate Button

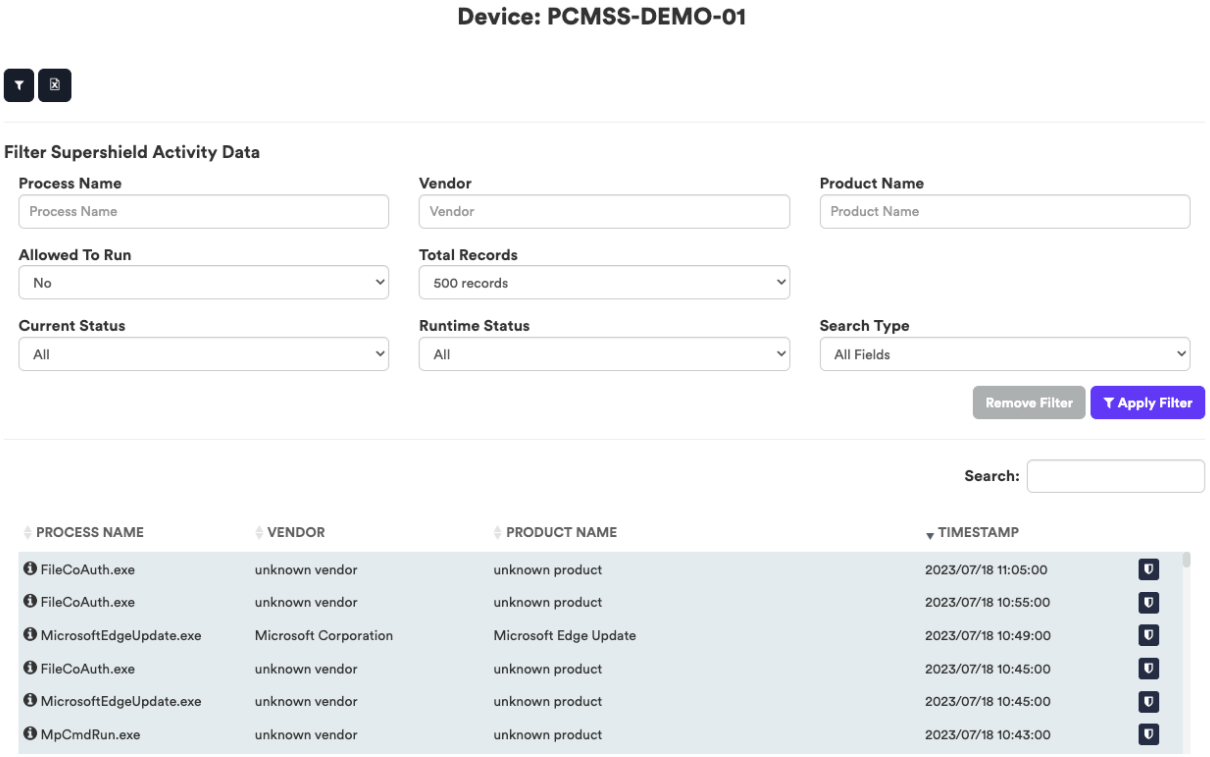
You can use the **Populate Company Allowlist** button to add all files that have run in your environment to your Custom Allowlist.



The first time you use the **Populate Company Allowlist** button, all files that have run in the past 24 hours on all endpoints will be added to the Custom Allowlist. Using the Populate Company Allowlist button in the future will add all files allowed to run since the previous time the button was used.

SuperShield Report

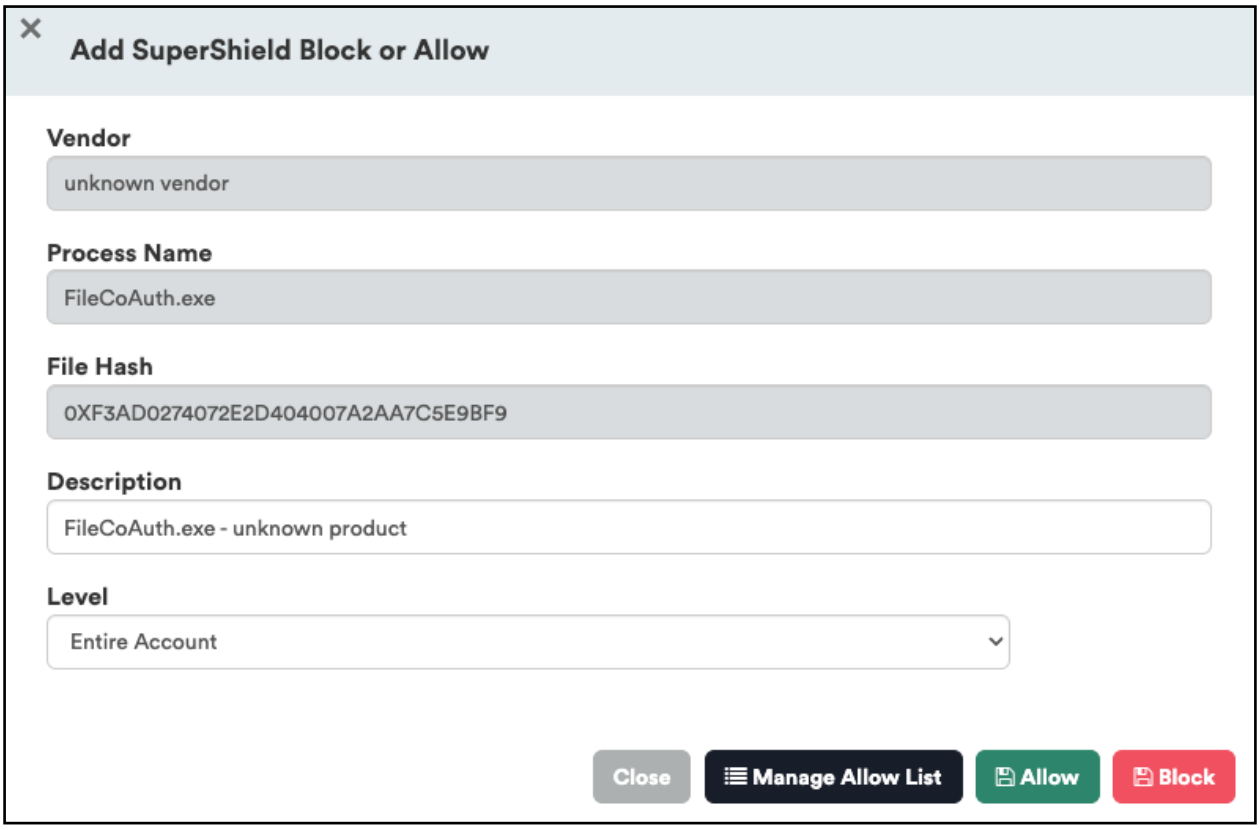
You can also add a file to the Custom Allowlist or Custom Blocklist from the device SuperShield Report. From the Devices page, click on the device name, then “SuperShield Report”.
This report shows all blocked applications on the endpoint by default. If you need to look at only unknown or good applications you can use the filter tool.



The most beneficial filter to use is Current Status. For example, setting the Current Status to unknown will provide a filtered report of just unknown applications that either ran or were blocked depending on the protection mode.
Be sure to adjust your search type between “All Fields” and “Any Fields” depending on your search.

- Process Name – Find your application using the name of the process.
- Vendor – Find your application using the name of the software vendor.
- Product Name – Find your application using the name of the application.
- Current Status – Current status uses the current known good, bad, or unknown value
- according to PC Matic Pro.
- Runtime Status – Runtime Status uses the known good, bad, or unknown value at the time
- of execution according to PC Matic Pro.
- Allowed To Run – Filter by if the application was allowed to run on the endpoint or not.

After using the filter to locate your application, click the shield icon on the right side of the SuperShield Report in the row for your application.



From the Add SuperShield Block Or Allow window, you can view information about the file including MD5, Process Name, Vendor, and Description. Using the level dropdown, select the company, group, or individual computer to add the application to your local allow list at that level. Now use the Allow button to add it to your Custom Allowlist, or Block to add it to your Custom Blocklist.

Groups

Grouping devices will allow you to find, identify and coordinate when and how you wish to have these endpoints scanned and configured.

Creating Groups

1. To turn on the ability to use groups, click Account Settings > Edit Customer Info and check the first box that says “Use Groups”.
2. Next, click Edit Groups in the Account Settings sidebar. Enter the name of a group in the field and click Add.

You may add, delete or rename as many groups as needed to organize your devices.

Changing Groups

Each device can be assigned to a group initially when the installer is being created. If the installer does not have a group assigned to it, you can assign each device to a group after installation has completed, or reassign them to a new group.

1. Navigate to the devices tab and locate the device that you would like to change groups.
2. Using the checkboxes on the left side of the device list, select the devices you want to move.
3. Choose Move Devices from the Bulk Actions dropdown.
4. In the Bulk Assign Devices panel, select the new group. Then, select whether the devices should keep the existing device settings or inherit the new group’s settings.
5. Click the Save button.

Notifications

PC Matic Pro is monitoring a lot of information about all of your devices to keep you informed. All available Notifications can be configured as Email or SMS Notifications or viewed within your management console. Our goal with notifications is never to fatigue you and overwhelm you with information or require your intervention for security. PC Matic Pro automates all critical decisions to keep your devices secure and let you spend time elsewhere.

From the Notifications tab inside your console you'll see three different sections - Security, Performance, and PC Matic News. These three sections contain all of the notifications about your account.

Security

The security section will contain all notifications that relate to the overall security of your devices. This includes notifications about the status of your realtime protection, malware removed, and processes blocked.

Performance

The performance section will contain notifications about device performance or status that have no impact on the security of your devices. This can include machines being offline for a duration of time, CPU spikes, etc.

PC Matic News

When our team launches new features or important updates we provide them to you inside the notifications section. Here you can get sneak peeks at what is coming soon, and learn more about a new feature or program.

The Notifications available in PC Matic Pro are detailed below:

- High CPU Usage - This will trigger after a scan runs and the CPU is above the set threshold.
- Running Low on HDD Space - This will trigger after a scan runs and the HDD space is above the set threshold.
- High Memory Usage (RAM) - This will trigger after a scan runs and the RAM used is above the set threshold.
- Reboot Required - This will trigger after a scan runs and a reboot is required.
- Scheduled Scan Failure - This will trigger if a scan fails while running.
- Scheduled Scan Not Run - This will trigger if a device missed a scheduled scan.
- Virus found - This will trigger when malware is quarantined during a scan.

- Vulnerability Install Failed - This will trigger if an application update fails to complete.
- SuperShield Definitions Incomplete - This will trigger if SuperShield fails to download the newest definitions.
- Computer Missing From Network - This will trigger if a computer is missing from the network longer than the set threshold.
- New RDP Session - This will trigger in realtime when a new RDP session is established.
- Application Blocked by SuperShield - This will trigger in summary every 24 hours if an application was blocked by SuperShield.
- SuperShield Status Change - This will trigger immediately if the status of SuperShield changes or becomes disabled.

Email & SMS Notifications

You can receive email or SMS notifications for any events on the account. To receive these, first add a notification contact. Open Notification Contacts from Account Settings in the sidebar. Then click Add New Contact.

Choose a contact type (email or SMS) and name for the recipient with the corresponding e-mail address or phone number. Select any “quiet times” that you do not wish to receive a notification and then click the save button. Quiet times will not lead to you missing out on alerts completely, at the end of the quiet time you’ll still receive the alerts from that time period.

To complete the process, you will receive an email to the entered email address; please validate the email address by clicking the link in that email. Once approved, the verification status will turn green.

Now to set your Email or SMS notifications select Account Settings > Notification Setup. Next to each contact or each notification type you can expand with a plus sign and adjust notifications.

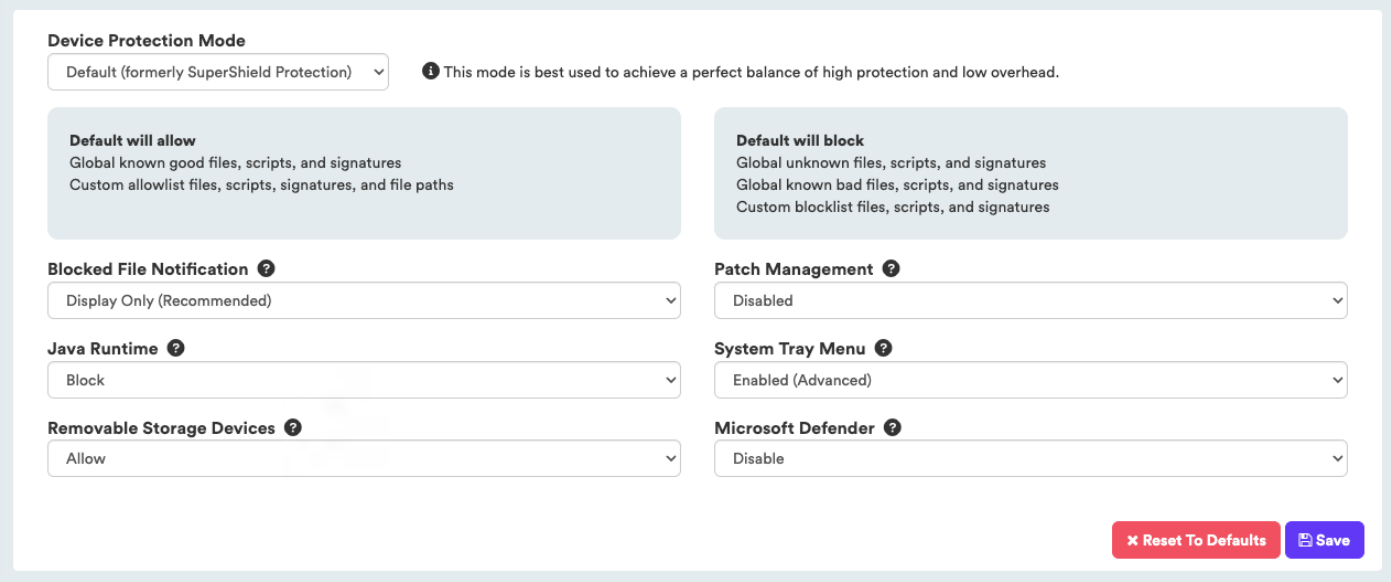
Notifications Options

Click the Account Settings tab from the sidebar and open Notification Options. From here, we are able to select which options we would like to see notifications for and tweak specific settings for several notifications. These options can be customized across all different levels including company, group, and individual endpoint.

SuperShield Options

SuperShield Options will allow you to set security settings for the company, group, or individual computer. Applying settings at the Company or Group level will immediately attempt to apply those settings to every device that is online and within that level. This will overwrite any current settings at lower levels. Saving settings at the device level will also take immediate effect.

Note: After saving SuperShield Options the icon on the device system tray may not redraw itself immediately. The protection is still running and the settings have been saved successfully.



SuperShield Options Structure

SuperShield options take priority by the lowest level set. This means that options changed at the individual device level take priority over group or company settings. To quickly change a setting at the computer level and then revert back to the group or company policies open the SuperShield options tab and click the red Reset to Defaults button.

Device Protection Mode

There are a few options available for the Device Protection Mode that allow you to control the lockdown state of your devices. Below we will explain the differences between the various modes.

Default (formerly SuperShield Protection)

This mode is best used to achieve a perfect balance of high protection and low overhead.

Default will allow
Global known good files, scripts, and signatures
Custom allowlist files, scripts, signatures, and file paths

Default will block
Global unknown files, scripts, and signatures
Global known bad files, scripts, and signatures
Custom blocklist files, scripts, and signatures

Custom Allowlist - Adaptive

This mode is best used to achieve a lockdown state with lower overhead than traditional allowlisting.

Custom Allowlist - Adaptive will allow
Custom allowlist files, scripts, signatures, and file paths
Global known good scripts
Global known good Operating System files
Update files associated with Custom allowlist files

Custom Allowlist - Adaptive will block
Everything else

Custom Allowlist - Standard

This mode is best used to achieve a lockdown state without managing operating system files.

Custom Allowlist - Standard will allow
Custom allowlist files, scripts, signatures, and file paths
Global known good scripts
Global known good Operating System files

Custom Allowlist - Standard will block
Everything else

Custom Allowlist - Strict

This mode is best used for full lockdown environments that require approval for all files.

Warning: This mode will block everything that is not currently in your custom allowlist, including operating system files. This could make the device unable to boot up properly.

Custom Allowlist - Standard will allow
Custom allowlist files, scripts, signatures, and file paths
Global known good scripts

Custom Allowlist - Standard will block
Everything else

Patch Management

PC Matic's patching of vulnerable applications can be integrated in SuperShield by enabling it in the SuperShield Options. For more detailed information, see Patch Management.

- Automatic - Update third party applications daily. (Default)
- Off - SuperShield will not update third party applications
- Prompt - Users need to approve updates at the endpoint.

System Tray Menu

Remove all control from the user at the endpoint level and manage all settings from the web portal.

Blocked File Notification

Notification settings for when unknown or bad software executes.

- Display only - Notification alerting the user that SuperShield blocked execution. (Default)
- No Block Notifications
- Prompt for Override - Gives the user the ability to allowlist unknown software at the endpoint level

Java Runtime

Our default setting is to block Java. This is in an attempt to further the security we provide for your devices and keep them safe from the newest strains of malware that capitalize on Java. If you still need access to Java, you can enable it here for any level of your account. We recommend only enabling it on devices where it is absolutely necessary.

Removable Storage Devices

Block the ability to connect removable storage devices. When this setting is activated any connected removable storage devices will automatically eject. Traditional USB peripherals will continue to function as normal. Turning Device Control off will automatically remount any removable storage devices that are still connected to the endpoint.

This option will only disable those classified as removable storage devices:

- Thumb Drives/Flash Drives/Jump Drives
- SD Cards

After making your selections, choose save. In the future if you want to completely clear out previously selected options, choose the company, group, or endpoint level and then use the Remove Settings button. This will ONLY remove the SuperShield Options for the selected level.

Local Endpoint Options

With PC Matic Pro the IT administrator has total control over local options available to the users. There is no User Interface on the local endpoint as all interfacing is done from the management portal. However, a SuperShield icon will be located in the system tray of each endpoint. This allows the user to verify they are currently protected in an easy fashion.

By default, there are no options available to the user via the SuperShield system tray icon. The System Tray Menu will be DISABLED. This can be ENABLED, to open up more options within the tray menu. Explore those options further below, keeping in mind opening this menu up to the user decreases your overall security posture.

System Tray Menu: Enabled

With System Tray Menu enabled, each user can access the menu below by clicking on the SuperShield icon located in the system tray.

- About SuperShield: Provides version information of the software installed.
- Protection Level: Allows user to change multiple SuperShield Options settings
  - Adjust SuperShield Protection Mode; turning real-time protection off or pausing it for a designated time period.
  - Change notification settings and allow overriding of unknown or bad applications.
  - Turn Patch Management off or require authorization from the local endpoint before installation can occur.
- Security Report: View the files analyzed by SuperShield and their status.
- Vulnerable Software Updates: Adjust local Patch Mmanagement settings.
- Allowlist and Blocklist: View and edit the Custom Allowlist or Blocklist.
- Allow Java: Enable the use of Java on the device

System Tray Menu: Disabled

With System Tray Menu disabled, you are able to remove all capabilities from the local endpoint in one setting adjustment. Instead of a menu of options being presented to the user, clicking on the SuperShield icon in the system tray only provides access to software version information.

Quarantine

Items can be quarantined either during a scan and clean, or if a known bad executable tries to run, SuperShield will block it and immediately quarantine. Items can be removed from quarantine if necessary. To begin this process you'll want to contact customer support to have the file re-evaluated.

- **business-support@pcmatic.com**
- **1-844-235-3301**
- **8:00AM - 9:00PM ET (M-F)**

Restore from Quarantine

Navigate to the individual device page that had this file quarantined, select Quarantine from the sub sidebar. This will give you the option to restore a file back to its original location or delete it forever. You will need to restore it for each machine it has been quarantined on.

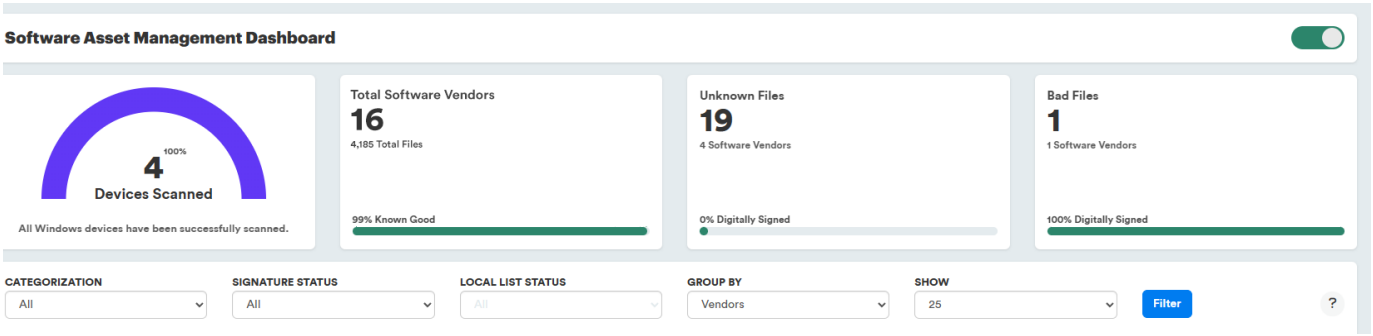
Clones and Images

PC Matic Pro uses a combination of the Machine GUID, Motherboard Serial Number and Computer Name to equal a unique device. For environments using Clones or Images that are created and destroyed frequently PC Matic Pro can recognize that it is a new clone and not create a new device in the management portal by using VDI Mode. This will allow your clones to still appear as the one 'device' they are instead of creating an abundance of duplicates each time a new Clone is used. We accomplish this by only identifying a device by the name, and not including the machine GUID or Serial Number.
There are several important distinctions when working with clones/images:

- **It's recommended that you use VDI Mode within groups.**
- Create your Group first and enable VDI Mode from the settings cog in the Filter by Group Dropdown.
- The "Golden Image" that PC Matic is installed on should be in this group so that when new clones are made they will be in the group where VDI Mode is enabled.

SWAM Dashboard

The Software Asset Management (SWAM) Dashboard provides details about the software installed across Windows devices in your customer's network and allows for easy management of the software allowed to execute on their devices. To access the SWAM Dashboard, select a customer from the Customers page, then select SWAM Dashboard in the sidebar.
Below is an overview of the SWAM Dashboard layout. More details in the following pages.



Enable/Disable Toggle

Use to turn Software Asset Management scanning ON/OFF

Devices Card

Displays the number of Windows devices that have been scanned for this customer. *Click the card to view the list of devices and additional details.*

Total Software Vendors Card

Displays the number of software vendors and files installed across all scanned Windows devices as well as the percentage of files that are categorized as Known Good by PC Matic. *Click the number to view files grouped by vendor. Click "Total Files" to view the list of all files. Click "Known Good" to view the files filtered by Known Good classification.*

Unknown Files Card

Displays the number of files that are categorized as Unknown by PC Matic and the percentage of files that are digitally signed. *Click the number to view the list of files. Click "Software Vendors" to view files grouped by vendor. Click "Digitally Signed" to view the files filtered to those that are digitally signed.*

Bad Files Card

Displays the number of files that are categorized as Bad by PC Matic and the percentage of files that are digitally signed. *Click the number to view the list of files. Click "Software Vendors" to view files grouped by vendor. Click "Digitally Signed" to view the files filtered to those that are digitally signed.*

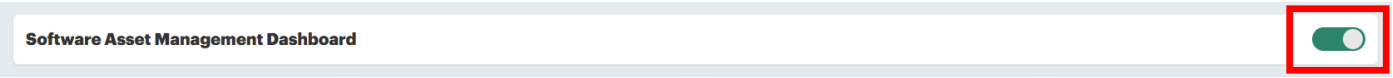
Devices/Files List

Displays the list of devices or files. Filter files by PC Matic Categorization, Digital Signature Status, Custom Allowlist Status, and Vendor. Also select how many files to show per pages.

Enable/Disable SWAM Scanning

By enabling Software Asset Management scanning, PC Matic scheduled scans will report the installed software and associated files found to the SWAM Dashboard. (Windows devices only)

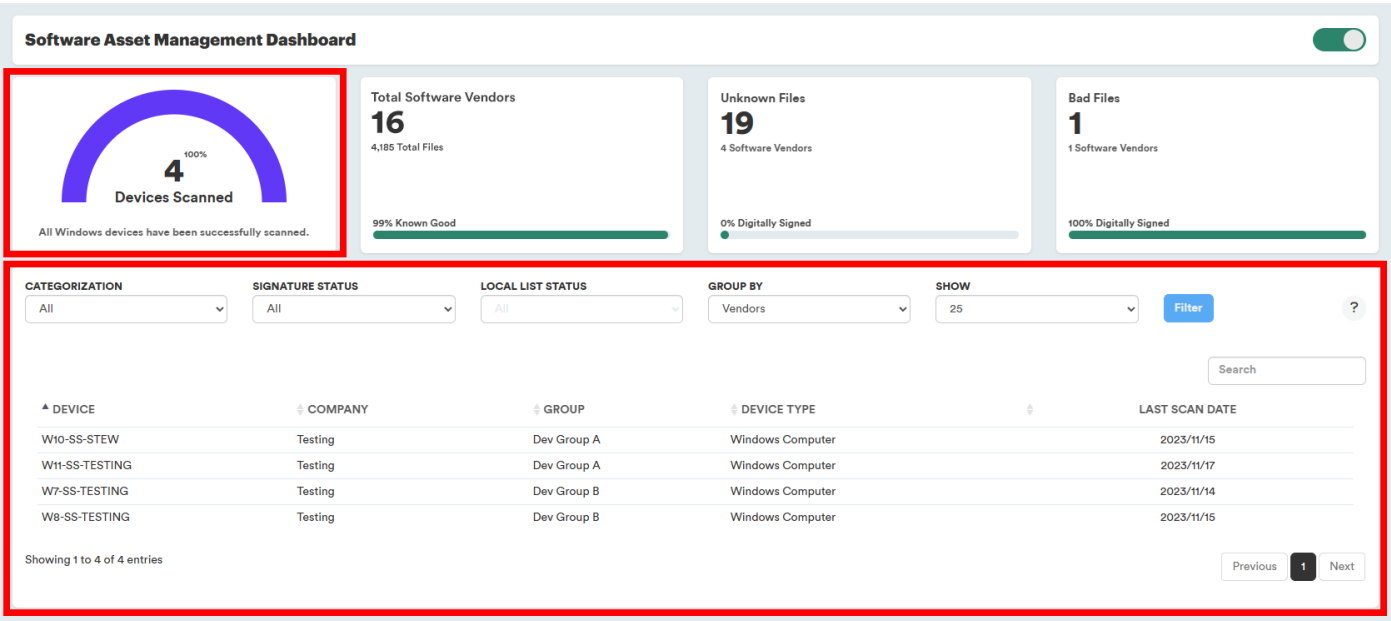
By disabling SWAM scanning, PC Matic scheduled scans will cease reporting file information to the SWAM Dashboard.



Scanning Devices

When first enabling SWAM for a company, the Devices card will display **0 Devices Scanned (0%)**. Once enabled, the next scheduled scan will update the number of devices scanned as well as report the files found to the Total Software Vendors card as well as the Unknown Files and Bad Files cards, if applicable.

To schedule a scan for a company, group, or device, navigate to **Account Settings > Scan Scheduler**. For more information on scheduling scans, see page



Clicking the Devices Card will display the scanned devices below. Here you will see the device name, the company (customer) name, the group the device belongs to, the device type (i.e.: Windows Computer, Windows Server), and the last scan date.

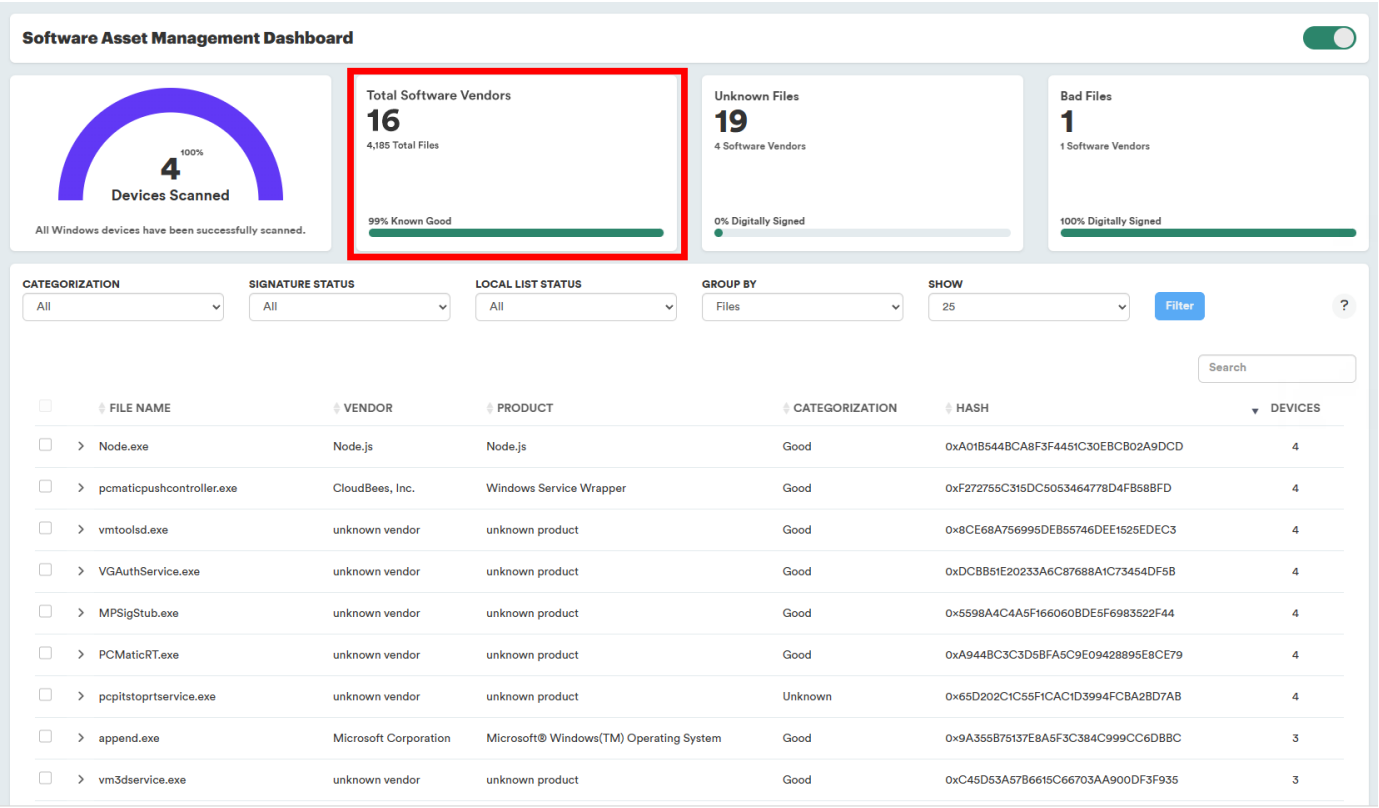
Managing Files

Once SWAM scanning has been enabled, and scheduled scans have begun running, you will see numbers begin to populate the Total Software Vendors card, as well as the Unknown Files and Bad Files cards, if applicable.

Total Files

The Total Files Card displays the number of files installed and the number of software vendors across all scanned Windows devices. It also displays the percentage of files that are categorized as Known Good by PC Matic.

Click the number to view the list of files, click “Software Vendors” to view files grouped by vendor, or click “Known Good” to view the files filtered by Known Good classification.

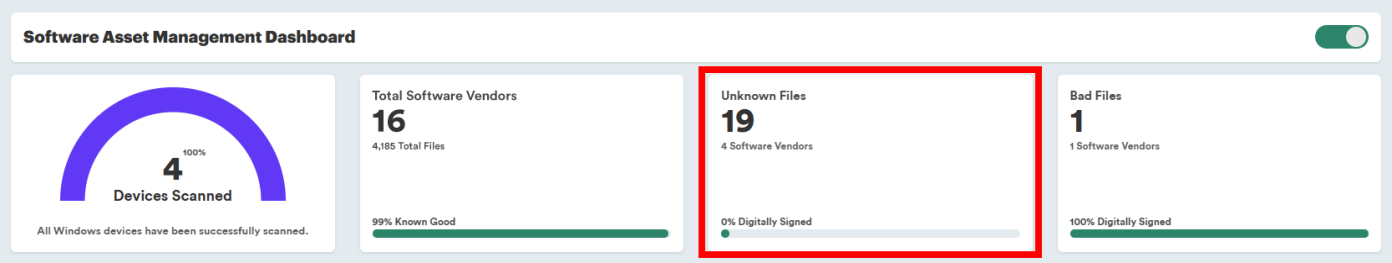


In the window below the cards, the files will be listed. The columns display the file name, vendor name, product name, PC Matic Categorization, MD5 hash value, and the number of devices that the file is installed on.

Use the filters at the top of this section to filter the list by PC Matic categorization, digital signature status, or local allowlist/blocklist status. You can also group the files by file or vendor.

Unknown Files

The Unknown Files Card displays the number of files installed and the number of software vendors across all scanned Windows devices that are categorized as Unknown by PC Matic. It also displays the percentage of these files that are digitally signed.



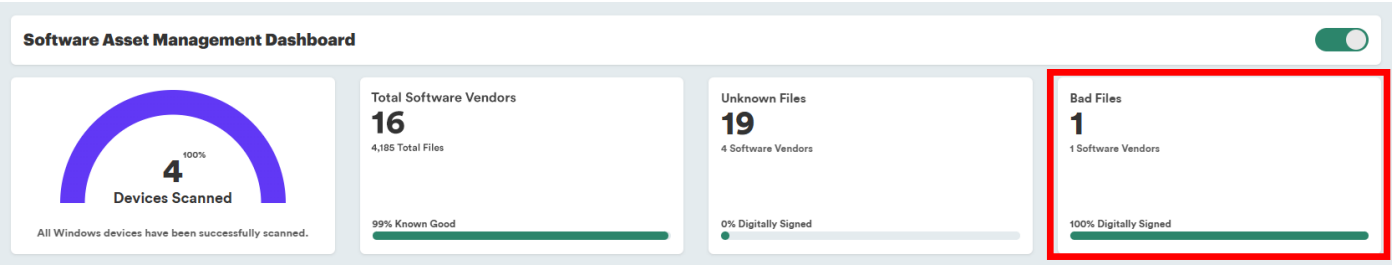
Click the number to view the list of files, click “Software Vendors” to view files grouped by vendor, or click “Digitally Signed” to view the files filtered by signature status.

In the window below the cards, the files will be listed. The columns display the file name, vendor name, product name, PC Matic Categorization, MD5 hash value, and the number of devices that the file is installed on.

Use the filters at the top of this section to filter the list by PC Matic categorization, digital signature status, or local allowlist/blocklist status. You can also group the files by file or vendor.

Bad Files

The Bad Files Card displays the number of files installed and the number of software vendors across all scanned Windows devices that are categorized as Bad by PC Matic. It also displays the percentage of these files that are digitally signed.



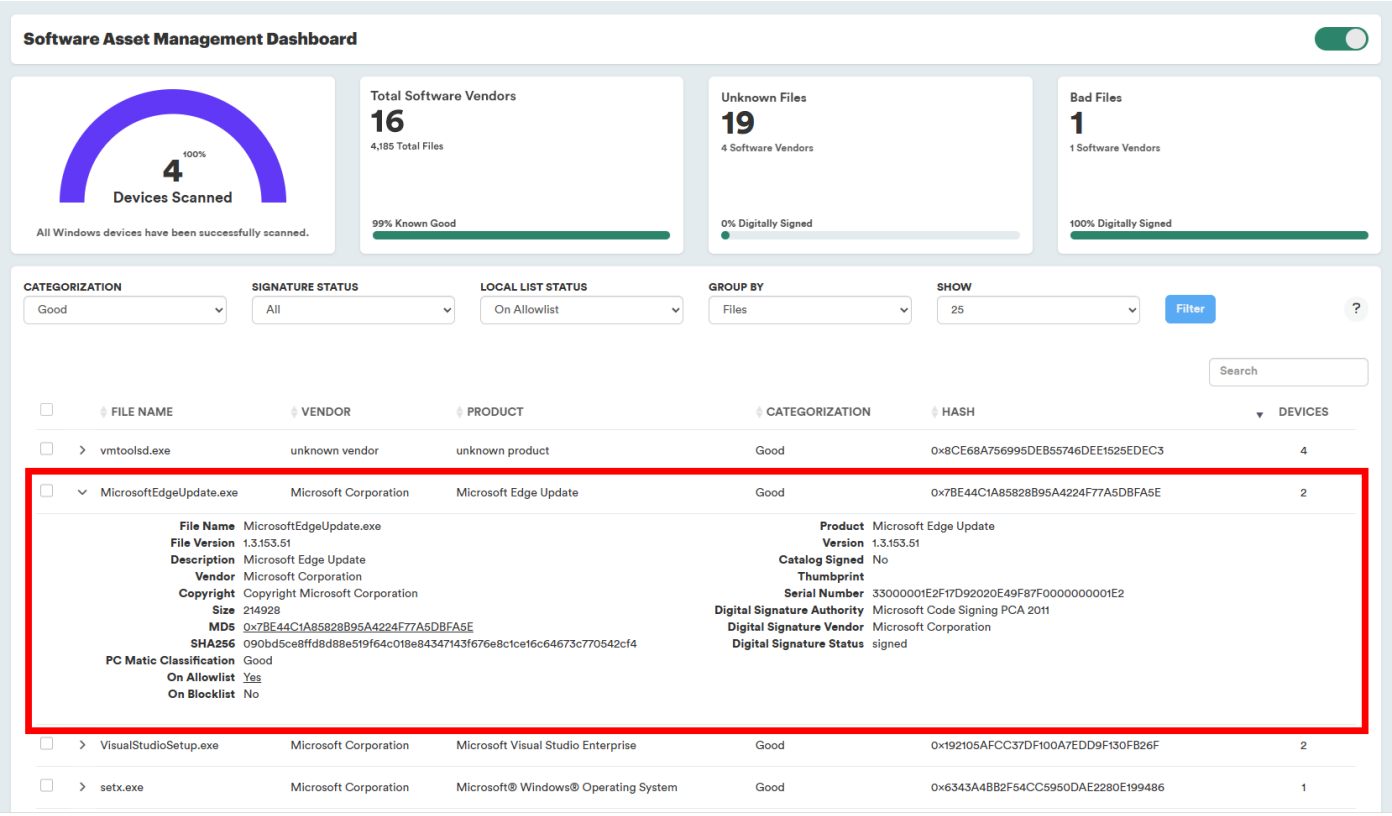
Click the number to view the list of files, click “Software Vendors” to view files grouped by vendor, or click “Digitally Signed” to view the files filtered by signature status.

In the window below the cards, the files will be listed. The columns display the file name, vendor name, product name, PC Matic Categorization, MD5 hash value, and the number of devices that the file is installed on.

Use the filters at the top of this section to filter the list by PC Matic categorization, digital signature status, or local allowlist/blocklist status. You can also group the files by file or vendor.

File Details

When viewing files, you can expand the file to view more details, including version number, description, size, MD5, SHA256, serial number, allowlist status, signature information, and more.

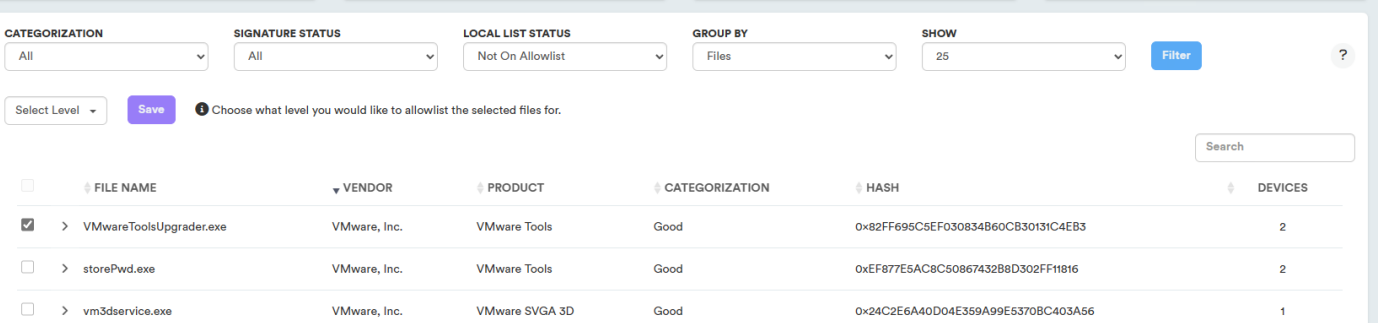


When a file is on your Custom Allowlist or Custom Blocklist it will be indicated with **Yes** in the On Allowlist or On Blocklist status.

Adding Files to Allowlist

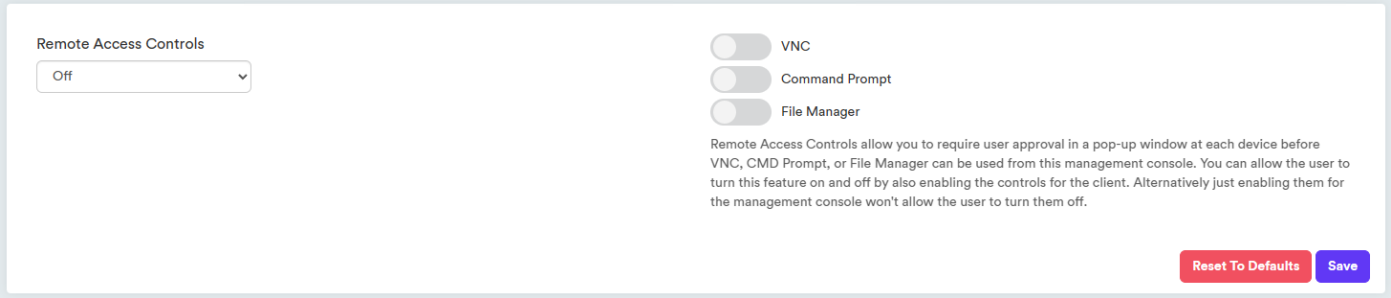
You can add files to your Custom Allowlist from the SWAM Dashboard.
To add a file/files to the allowlist:

1. Select file(s) using the check box on the right side of a file list.
2. In the drop-down that appears, select the level that you want to allowlist the file for.
3. Click the Save button.



Remote Access Tools

Remote tools can be configured to require end-user approval before granting remote access. This functionality provides the user with a sense of reassurance and control over their device. By implementing this requirement, individuals can have peace of mind, knowing that they have the ability to determine when their device is being accessed.



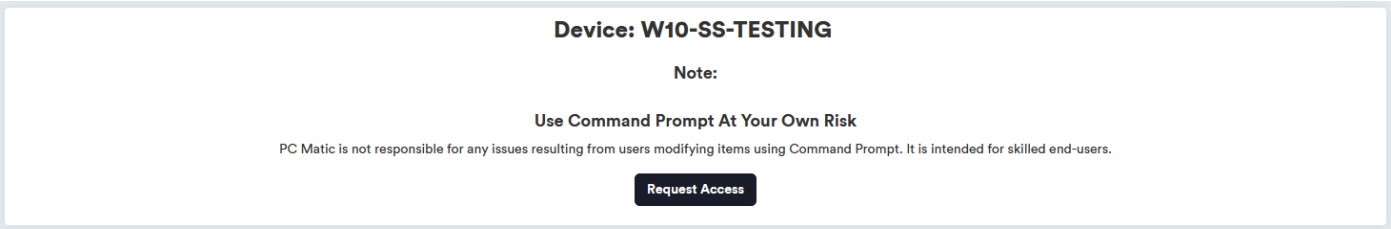
Remote Access Controls can be enabled and configured at the Company, Group, and Device levels.

When Remote Access Controls are enabled, each remote tool can then be toggled on individually to be included in the requirement for remote access prompts. There are two options available when enabling Remote Access Controls :

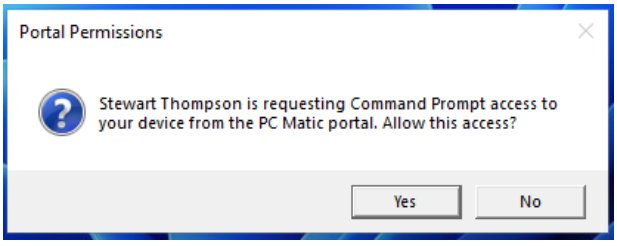
- Enabled
- Enabled with Client Control

Enabled

When Remote Access Controls are enabled, the remote tools features (Remote Access, Command Prompt, and File Manager will now require the portal user to request access from the end user of the device before permissions are granted and the portal user can make the remote connection.



The end user will see a prompt on their desktop screen indicating the portal user's name and what feature they are requesting to access.



The end user will have 10 seconds to provide a response to the prompt, either granting or denying permission. If they do not respond in that timeframe, the alert will be automatically dismissed and a new request must be sent from the web portal.

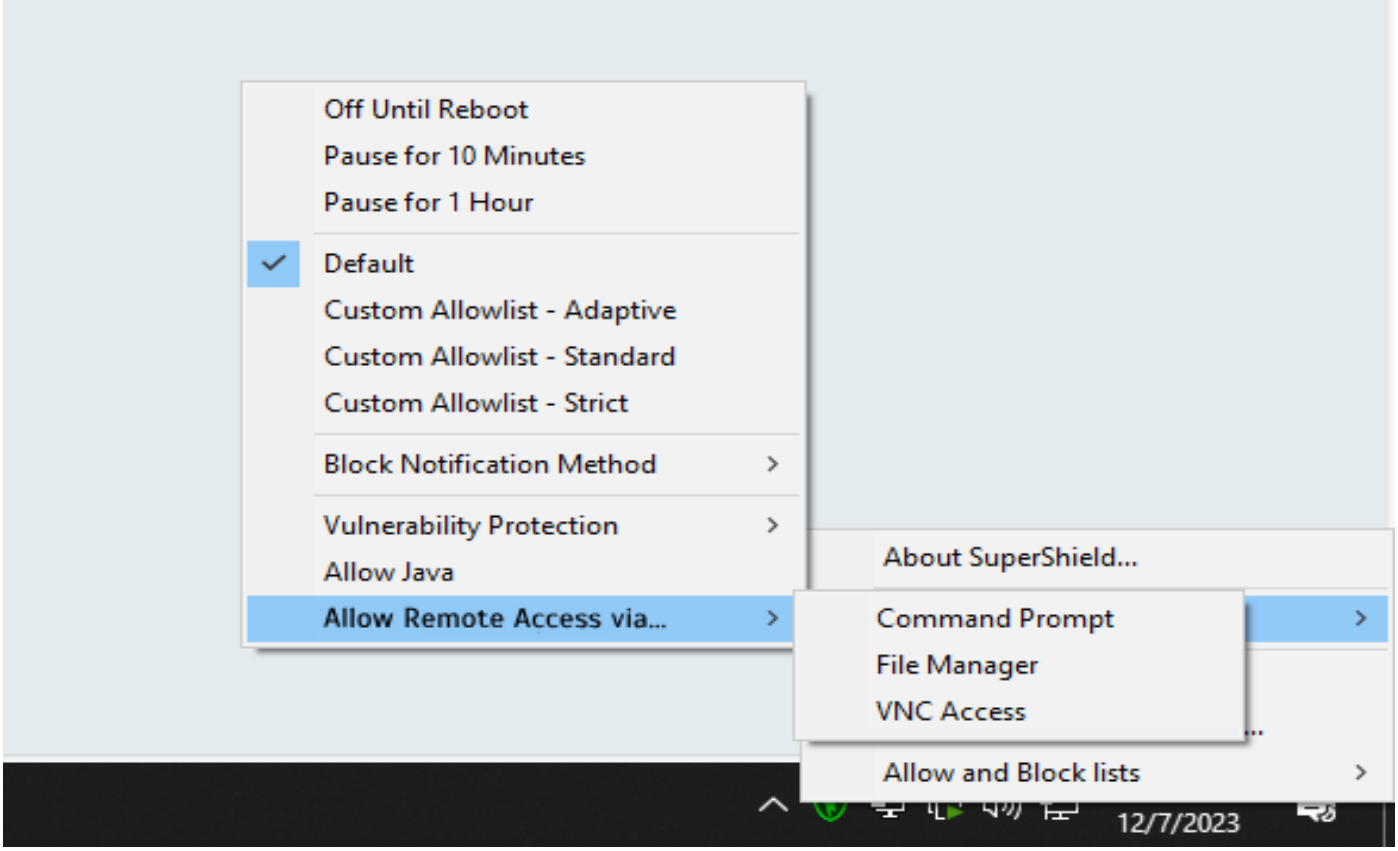
- When a user grants permission, the remote tool will open in the web portal for use.
- If a user denies permission, you will receive an alert in the web portal informing you of their decision.

Enabled with Client Control

The option to enable Remote Access Controls with Client Control has the same functionality in the web portal as when set to Enabled, but with the option for the end user to override the individual prompt messages on their device, effectively always granting approval whenever a request is made.

This feature is only available to end-users that have the SuperShield System Tray option enabled in SuperShield Options.

If the end-user has access to the SuperShield system tray, they will have a menu item called **Allow Remote Access via...** in the **Protection Level** menu.



End users can place a check mark next to the remote tools they wish to skip receiving permission prompts for, automatically granting remote access when requested via the web portal.

Unchecking the option the end user will receive prompts again to grant permission for each request.

Enabling and Configuring Remote Access Controls

To enable and configure Remote Access Controls, log in to the web portal and follow the steps below:

1. Navigate to the Remote Access Controls page.
2. To enable/configure for an individual device:
3. Navigate to the Devices page, select the device name, then navigate to Remote Access Controls located in the Security section of the Device Options menu.
4. To enable/configure at an Organization, Company, and/or Group level
5. Navigate to Account Settings > Remote Access Controls located in the Security section of the sub navigation menu.
6. From the drop-down, select either Enabled or Enabled with Client Control.
7. Toggle the prompt control on for the remote tools to be included in the requirement for remote access prompts.
8. VNC (Remote Access)
9. Command Prompt
10. File Manager
11. Click the Save button.

Preferences

The Preferences page contains settings and options that relate to preferences you can configure for your management console. You can access it at **Account Settings > Preferences**.

Appearance

This toggle control light mode and dark mode for your user account so when you log in to the console you get the experience you're looking for.

Remember Active Tab

You can toggle this on and it will remember the last page you viewed before leaving and automatically load that when you come back. For example, instead of loading the Devices list first (which is the default), it would load Process Activity if that was the last tab you viewed.

PC Matic Support Access

This setting offers you more control over your account and access to it from our support team. By setting the toggle to on, you allow our customer support team to log in to your account and help you troubleshoot, configure, etc. However, at any time you can toggle this setting off and our team will no longer be able to access your account. This setting can only be controlled by the Account Owner, as it has an effect across the entire account.

Two-Factor Authentication

This setting controls Two-Factor Authentication for your account. See page 10 for more information.

Enforce Two-Factor Authentication

This setting controls if users on your account are required to use Two-Factor Authentication. See page 10 for more information.

Logout Timer

This setting allows you to customize the amount of minutes used for the Inactivity Logout Timer. The default for this timer is 15 minutes of inactivity but can be customized to any value between 3 minutes and 1440 minutes (24 hours). The value can only be changed by an Account Administrator and will be ignored for users who check the Remember Me box on login as that maintains the session for 24 hours.

Change Password

You can change your account password here.

Uninstalling PC Matic Pro

PC Matic Pro cannot be uninstalled from the control panel on the device. We have restricted it to prevent mischievous users and cyber criminals that leverage remote access over RDP. There are three different ways you can uninstall PC Matic Pro on a device. Uninstalling does not require a reboot of the device to complete, uninstalls everything in the background without user interaction.

If the device is online and has a connection to your management console:

This does not require a reboot of the machine and will uninstall without user interaction.

Uninstall a Single Device

1. Navigate to the Devices page
2. Click the “more” menu icon in the Actions column
3. Select Remove Device
4. Confirm the uninstall

Bulk Uninstall

1. Navigate to the Devices page
2. Select the device(s) on the left with a checkmark
3. Select Remove Device from the Bulk Actions menu
4. Confirm the uninstall

Any devices that are offline will prompt you to either queue them up for an uninstall which will happen automatically the next time they regain connection, or delete them without uninstalling.

If the devices were installed using the Device Manager through Active Directory:

This does not require a reboot of the machine and will uninstall without user interaction.

1. Navigate to Account Settings > Network Devices
2. Click the red trash can icon under Actions to uninstall a single device, or select multiple devices then click the red trash can icon at the top to bulk uninstall
3. Confirm the uninstall

If the device won’t connect to the PC Matic Pro console:

1. From Add a Device > Install/Uninstall > Endpoint Uninstaller download the uninstaller .zip folder to the computer you wish to uninstall on.
2. Right click and extract the .zip folder that you downloaded.
3. Inside the folder you will find an uninstaller executable and a batch (.bat) file that contains unique details for your account.
4. Right-click the .bat file and select Run as Administrator.
5. The uninstall is now complete.

Firewall Settings

PC Matic Pro does not include a firewall, but if you're using a third party firewall you may need to configure it to ensure that our program can connect properly to our servers. You will find several different configurations below depending on the type of firewall you are currently using.

Please set your firewall to allow the following:

- Port 80 (http) and 443 (https) must be open outbound
- Port 5900 must be open inbound/outbound (for remote access over VNC)
- Port 5500 must be open inbound/outbound (for remote access over VNC)

These are the primary communicative ports for the following domains:

- www.pcpitstop.com
- pcpitstop.com
- api.pcpitstop.com
- portal.pcpitstop.com
- defs.pcpitstop.com
- drivers.pcpitstop.com
- files.pcpitstop.com
- supershield-files.pcpitstop.com
- supershield.pcpitstop.com
- push.pcpitstop.com
- utilities.pcpitstop.com
- vncproxy.pcpitstop.com
- satellite1.pcpitstop.com
- satellite2.pcpitstop.com
- satellite3.pcpitstop.com
- satellite4.pcpitstop.com
- software.pcpitstop.com
- logfiles.pcpitstop.com

If you prefer to utilize IP addresses, then allowing the following subnets will allow our traffic to flow properly:

- 103.21.244.0/22
- 103.22.200.0/22
- 103.31.4.0/22
- 104.16.0.0/12
- 104.20.16.196
- 104.20.71.199
- 104.20.82.39
- 104.20.83.39
- 108.162.192.0/18
- 131.0.72.0/22
- 141.101.64.0/18
- 162.158.0.0/15
- 172.64.0.0/13
- 173.245.48.0/20
- 188.114.96.0/20
- 190.93.240.0/20
- 197.234.240.0/22
- 198.41.128.0/17

Unsupported Operating Systems

Windows XP and Windows Vista operating systems are no longer supported by Microsoft and cannot be fully supported by PC Matic. It is possible to install our realtime protection, SuperShield, on a device running Vista or XP, however there will be a large number of features missing. All remote control or realtime controls from the web console will not be functional. Any statuses you typically see from a machine in realtime will show in a yellow or unsure status indefinitely. The following features will not be available: Current Connection Status, Current Protection Status, Quarantine Restore, Command Prompt, File Manager, Immediate Scans, VNC Access, Remote Reboot/Shutdown, and more. If you have concerns about Vista and XP support, please contact our support team.

Troubleshooting

1. ***Red SuperShield icon inside management console but a Green SuperShield icon on device in the system tray.***
   In SuperShield version 3.0.10.1 we introduced a new change to delay showing a red shield at the users device for 30 minutes to allow time for correction by the admin. If you're seeing a red shield for a device in the management console, use the Actions menu for that device and choose Restart SuperShield in the SuperShield section.

2. ***Red SuperShield on device says "Contact Network Administrator"***
   Also in SuperShield version 3.0.10.1 we made a change to the verbiage of the tray icon to let the user know to contact their admin for assistance.

3. ***Terminal Server connections show no SuperShield icon in the system tray.***
   Currently if you have over 60 connections to the terminal server, they will no longer have a SuperShield icon in the system tray. The connections over 60 are still protected, but the tray app won't display.

4. ***Scheduled Scan Error 940***
   When a scheduled scan fails with a 940 error it means the fault occurred at the device. This could have been related to the internet connection or data transfer from the device out to our server.

5. ***Scheduled Scan Error 202***
   When a scheduled scan fails with a 202 error it means the fault occurred at our server. This is likely an issue accepting the data from the device during and/or post scan.

6. ***Device Manager Manual Sync***
   The Device Manager syncs automatically with the web portal every 30 minutes to look for changes in settings or new installs/uninstalls to push out. However, if you want to manually force this sync to happen we have created a simple batch file you can run on the domain controller. https://files.pcpitstop.com/DeviceManager/sync.bat

7. ***Quarantine Tool Constantly Loading/Error***
   The quarantine tool, among a few other features in PC Matic Pro rely on .net Framework 3.5 being installed and enabled on the device. If the quarantine tool is not working correctly and just constantly loading or giving you an error that device most likely doesn't have .net 3.5 installed and enabled. You can download and install it from Microsoft here.

8. ***Endpoint Uninstaller Fails***
   If you have downloaded the endpoint uninstaller to remove PC Matic Pro from your device and it fails to uninstall you will have a brief period of time where the product can be uninstalled from the control panel manually. If it cannot be found in the control panel, turn off the PC Pitstop Scheduling Service and run the endpoint uninstaller again; then uninstall from the control panel.

Support

To get support from our team, you can click on Support in the web portal navigation.

https://portal.pcmatic.com

From here you have several methods to contact our team.

Email Support:

business-support@pcmatic.com
8:00AM - 8:00PM ET (M-F)
9:00AM - 5:00PM ET (Saturday-Sunday)

Phone Support:

1-844-235-3301
8:00AM - 8:00PM ET (M-F)

Frequently Asked Questions

1. ***What deployment methods are available?***
   There are a few ways to deploy PC Matic but the most common approach is with Active Directory and PowerShell. Our device manager is installed on a windows server with Active Directory and PowerShell scripts are then used to push an .msi file silently and install to the selected endpoints. Further details on this are available in the Remote Deployment document in the support section.
   You can also deploy by downloading or emailing an .exe file and manually installing it on each computer. This installation method works best for small rollouts and you can find more information about it here.

2. ***Is PC Matic Pro compatible with servers?***
   Yes, PC Matic Pro can be installed on Windows Servers version 2008 R2 and up. The install process works exactly the same as an endpoint but will intelligently recognize a server and install with the settings.

3. ***Do you have a management console?***
   Yes, PC Matic Pro is managed through a web based portal that is responsive on any device. You'll have a single pane of glass to view all of the information about your computers and take any actions necessary. Login here: https://portal.pcmatic.com

4. ***How do you deal with false positives?***
   You have the ability to allowlist any application that is being blocked from the cloud console.This is a flexible local allowlist that can be configured at any level of your account. Additionally, when an unknown application is blocked it is uploaded to our servers where our malware research team will review the application. They identify if it is good, and if so, add it to the global allowlist which is pushed out to all customers. This removes the normal overhead associated with a allowlist solution.

5. ***What are your support hours?***
   Our support team is available 5 days per week from 8:00 AM – 9:00 PM ET with support for weekend emergencies. (Email: business-support@pcmatic.com | Phone: 1-844-235-3301)

6. ***What is the performance impact on my devices?***
   PC Matic Pro has very little performance impact on the endpoints it is protecting. Our real time protection uses light static checks to determine if a file is on the allowlist or not, and if necessary uploads the unknown file to our malware team for further analysis. This conserves endpoint resources for your use instead!

7. ***How often should I run a scan on my machines?***
   Our team normally recommends at least one weekly scan for your machines to make sure they are cleaned up and optimized. If you would like to run scans on a daily basis or monthly basis you can configure that in the scan options.

8. ***What are the recommended settings?***
   In almost all cases, the recommended settings within PC Matic Pro will be labeled as such

or set as the default. By default there will be no scans set up on the account, you'll need to customize the first scan and your chosen level. To learn more, you can read our full guide on Best Practices.

9. ***Will your product automatically remove my previous antivirus?***
   PC Matic Pro will not automatically remove antivirus products before installing our protection.

10. ***I forgot my password, how can I reset it?***
    To reset your password, visit portal.pcmatic.com and click the "Forgot Password" button right next to "Log In". Then enter your email address and you'll receive an email shortly after with a link to reset your password.

11. ***Does my computer need to be turned on for a scan to run?***
    Yes, your computer must be powered on for the scan to run. If you put your computers to sleep instead of turning them off, our scan will wake up the computer and run. The computer may go back to sleep depending on your Windows sleep configurations.

12. ***Can I remote into my computers from any device?***
    No, you can only use the remote desktop feature from a Windows computer that has PC Matic Pro also installed on it. This feature requires the install on both ends so they can communicate securely between themselves.

13. ***Will my Images, Documents, PDFs, etc. be stopped by PC Matic because they're not on the allowlist?***
    No. PC Matic Pro's real time protection is focused on PE (Portable Executable) files that execute on your machine to run malware, or scripts that implement fileless malware or ransomware. You'll be able to access and create as many documents, pictures, movies, PDFs, etc. as you need!

14. ***How long do I wait after locally allowlisting an application before my computers will be able to run it?***
    Adding an item to your local allowlist will immediately sync it down to every device in the level you have allowlisted that application for. This often takes less than 10 seconds after you have clicked save inside your web portal.

15. ***How can I verify that a computer is being protected?***
    There are several ways to verify that a computer is currently being protected by SuperShield. You can do this from the individual endpoint, or from the web console.

    Web Console: Navigate to the computers tab and look for the computer's name that you want to verify protection on. Once you locate it you'll see three status icons at the bottom of the computer's information box. The middle icon will be green if SuperShield is installed and running properly. You can also see this status icon from the computer's page in your console.

    Individual Endpoint: After installation, a small shield will appear in the system tray of each endpoint. If you don't see it right away, don't panic. You may need to click the small arrow and expand the system tray to see all icons. This shield will display as either green (running correctly), yellow (updating), or red (not running).

16. How can I add additional licenses?

As a business you're always going to be looking to expand and grow over time and we are ready to grow with you! You can always purchase additional license through your reseller or by contacting our sales team through the Support tab. These additional licenses will be prorated to expire at the same time as your previous purchase.

17. How is the billing handled for PC Matic Pro?

PC Matic Pro can be purchased in 1, 2, or 3 year options along with the count of licenses needed for endpoints and servers. Longer contracts will often result in lower prices, evident with the 3 year selection. Additional endpoints purchased in the future will be prorated with the same expiration date as the original purchase.

18. When do SuperShield Options changes take effect?

There are two different timeframes when SuperShield Options may take effect. If changing them from the devices page with an active connection they will apply immediately. You can also change them from the Endpoint Vulnerabilities report with an active connection for immediate effect. Any other level when changed the SuperShield options will take effect when our scheduler runs next, which at max will be one half hour.

19. Does PC Matic have Continuous Diagnostics and Mitigation (CDM) Capabilities?

PC Matic Pro meets all the common requirements for the Continuous Diagnostics and Mitigation (CDM). PC Matic Pro addresses the Software Asset Management (SWAM) capability requirements as part of Continuous Diagnostics and Mitigation (CDM).

PC Matic Pro addresses and meets the System and Information Integrity capability requirements as part of Continuous Diagnostics and Mitigation (CDM).

For more specific details on these requirements and PC Matic Pro contact PC Matic Federal team at cdm@pcmatic.com