



User Guide v 4.0.1
November 2020

Table of Contents

Introduction	1
What's new?	1
Optimal System Requirements	2
Known Conflicts	2
Product Options	3
Optimal System Settings	4
Scan Components	4
Management Portal Access	4
Best Practices	4
Onboarding Support	5
Sidebar Navigation	5
Installation	6
Installer Customizations	6
Installation Methods	7
Device Manager Procedure	8
Device Manager Installer	12
Account Home Page	16
Payment Settings	17
Manage Users	18
Roles & Rights	18
Authentication	19
Portal Home Page	21
Prospecting Tool	22
Customer Home Page	24
Dashboard	24
Notifications	24
Device Activity	24
Reporting	24
Endpoint Vulnerabilities	25
Computer Management	25

Table of Contents

Device Actions	26
Icon Descriptions	28
Patch Management	29
Scheduling a Scan	30
Live Scan Status	30
Allow Listing	31
RDP Lifeline	33
Groups	35
Changing Groups	35
Notifications	36
SuperShield Options	38
Remote Desktop	39
Command Prompt	39
Local Endpoint Options	41
Removing Customers	42
Firewall Settings	42
Server Security	44
White Label	46
Quarantine	47
Clones and Images	48
Workspace Customizations	49
PC Matic Ad Blockers	49
macOS Devices	50
Uninstall PC Matic MSP	54
Support	55
Unsupported Operating Systems	56
Troubleshooting	56
Frequently Asked Questions	57

Introduction

PC Matic MSP is for managed service providers looking to manage and protect their customer's computers remotely from a single location. There is no user interface at the workstation, and control can be restricted at the endpoint level.

PC Matic MSP consists of several parts:

- Real time whitelist based malware protection known as *SuperShield*.
 - ◊ SuperShield is active and protects the computer 24/7.
- An on demand scanner that will clean, maintain, and optimize each endpoint.
 - ◊ You can schedule scans at several different intervals: one time, daily, weekly or monthly. Choose a start day and time and insert an email address to receive the clean reports after the scan completes.
- A modified VNC agent, which allows remote access to your endpoints.
 - ◊ The remote desktop ability will allow you to take control of endpoints on your account, and share files between them easily.

What's New?

Because we're frequently making changes to PC Matic MSP and the management console, you can find new features or additions below.

- **Brand New User Interface**
 - ◊ We're excited to launch our brand new user interface for PC Matic MSP. Our team has been hard at work gathering feedback for our product and redesigning the management console to be simple to navigate.
- **Improved Performance**
 - ◊ During the redesign, our development team dedicated substantial efforts to drastically improve the performance of your management console. This includes reducing load times, loading screens, and overall snappiness.
- **Automation**
 - ◊ Our third goal during the redesign was to automate as many things inside your account as possible. PC Matic MSP provides a different experience compared to any other security software by not requiring your constant intervention. A wealth of information is at your fingertips, if you so desire it.



Optimal System Requirements

- **Endpoint Operating System:** Windows 10 (32/64-bit), Windows 8 (32/64-bit), Windows 7 (32/64-bit).
- **Security Only Operating System:** Windows Vista (32/64-bit), Windows XP (32/64-bit).
- **Server Operating System:** Windows Server 2008 and up.
- **Mac Operating System:** macOS Sierra, High Sierra, Mojave, Catalina
- **Processor:** 1 GHz or faster | **Memory:** 1024 MB or more | **Hard Disk:** Need 1 GB or more of free space
- Active Internet Connection | .net Framework 3.5 [[Download](#)]
- **Current SuperShield Version:** 3.0.30.0 | **Current Push Controller Version:** 1.4.10.0
- **Current Mac Version:** 0.0.39 (Build 180)

Known Conflicts

SuperShield can be run alongside several other realtime protection components. However there are some that will cause problems for either our program or both programs. This can be conflicts with stability, performance, and security on the device.

In most cases Windows Defender will take a back seat to third party AV when it's installed but sometimes an update will cause Defender's realtime component to turn on and take precedent. This can cause stability problems for SuperShield, so make sure Defender is turned off.

The below software has been tested and shown issues in the past running alongside our product. We would strongly recommend against not only running these solutions in parallel with ours, but you should also make sure that they have been completely removed before installing our product.

Symantec

Even when uninstalled through the control panel, it can cause conflicts for our program and will often result in SuperShield being unstable. You may also see performance issues if Symantec is present on a machine with SuperShield running. It's important to use the removal tools below to ensure all pieces of the program are removed.

- Symantec Clean Wipe Tool: https://support.symantec.com/en_US/article.HOWTO74877.html

Product Options

Within your PC Matic MSP console, you will now have the opportunity to set a product type for each customer. Each customer can only have one product type assigned to it. This will adjust the features, licensing, etc. inside that customer to correspond with the product. You can change this product type at anytime to adjust the feature set for a customer even after you have done installs on their devices. Contact your PC Matic sales representative for more information on the different pricing for these products. You can find out more information about each product's features below:

- **PC Matic** - The product we all know and love, the main offering inside PC Matic MSP and the default for each new customer you create. PC Matic contains all possible features, reports, abilities, etc.
- **RDP Lifeline** - This new product offering focuses on just securing and managing RDP (Remote Desktop Protocol) for a customer. SuperShield, our realtime protection, is not included so there will be no endpoint security installed on the device. If a customer is using another security solution but you need a tool to manage, secure, and log RDP access, RDP Lifeline is the perfect option. This product also includes all of our EDR tools to remote into devices, utilize the CMD prompt, access the File Manager, and more
- **Ransomware Lifeline** - This new product offering encompasses our security components. With special adjustments to allow the product to run alongside other endpoint security clients, Ransomware Lifeline can be used to add a whitelist default-deny security level to any customer's environment. This product does not include many of the features of PC Matic that are not focused on endpoint security. At its core SuperShield will protect each machine and be the main component of Ransomware Lifeline. This product also includes all of our EDR tools to remote into devices, utilize the CMD prompt, access the File Manager, and more.

Optimal System Settings

In order to ensure PC Matic MSP is able to function at the highest level and provide all abilities in the product to you, there are optimal settings for Windows.

Sleep Settings

When a device is asleep it loses network connection. This will remove your ability to take immediate actions from within the management console. Until the device awakes from sleep, immediate scans, command prompt access, reboots, and VNC control will be disabled. Sleeping devices will still wake for a scheduled scan, but will not display real-time scan progress in the management console during the scan.

In order to ensure you always have access to the device when needed, we recommend adjusting the power plan to put the display to sleep but not the computer.

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 MSP contains several components that will help improve the overall performance of your endpoints. These can be seen in detail inside the reports section from your sidebar.

Management Portal Access

Access to your management portal is available at portal.pcmatic.com from any device with a web browser. You can view and manage your customers from anywhere that you are. However, in order to use the remote desktop feature you must be on a Windows computer with PC Matic MSP Installed.

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

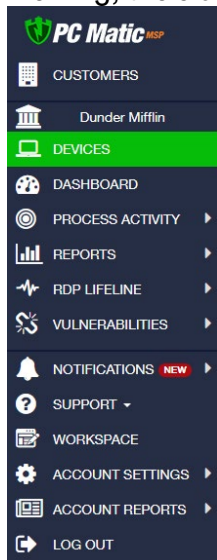
Before deploying out to a large number of devices or to all of your machines, we highly recommend consulting with our Onboarding Team. The onboarding team automatically works with new accounts to help make sure that getting PC Matic MSP installed and running is as simple as possible.

During initial installs, you may see unique tools you use blocked as unknown by PC Matic MSP. This is normal, and evidence of our whitelist based approach not allowing unknowns to run. However, 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 whitelisting them, please consult with the onboarding team.

- PC Matic MSP's Onboarding Team - onboarding@pcmatic.com

Sidebar Navigation

The new sidebar in PC Matic MSP is your home for all reports, views, options, and resources within the management console. No matter what page of your account you're currently viewing, the sidebar adapts to give you the links that are available.



Devices

The first tab in your sidebar, Devices, presents you with all of the information about each machine you are currently protecting and managing with PC Matic MSP.

Notifications

PC Matic MSPs Alerts have been moved to a new Notifications tab. This tab provides information about happenings inside your account, but these are not *Alerts* that need your present attention. PC Matic MSP automatically takes care of any item that needs immediate attention so you can relax and focus on other tasks.



Account Settings and Other

At the bottom of the sidebar you will find a new tab called Account Settings that will encompass all of your options that are available at the account level, along with any information about your account such as licensing or payment settings.

Sub Sidebar

When navigating your sidebar, a list of actions for that section will open into a sub sidebar so you can easily access anything you need without having to load different pages.

Installation

Before downloading the endpoint installers for your PC Matic MSP account, you have several options that can be customized to increase flexibility and ease of installation. For installing on Mac devices, see the Mac section.

The screenshot displays the 'Windows Installer' configuration page. At the top, there are tabs for 'Windows Installer', 'Mac Installer', 'Device Manager Installer', and 'Endpoint Uninstaller'. A prominent 'IMPORTANT!' warning box contains the following instructions:

- Do not alter the Installer Download URL or the downloaded file name. This will cause issues with installation.
- The PC Matic Agent will not be visible within Control Panel to increase security after installation. Uninstalls must be done through device actions or with the Endpoint Uninstaller above.
- Before deploying to all of your devices, we strongly recommend consulting with our onboarding team - onboarding@pcmatic.com.

Below the warning, the page is titled 'Endpoint software for Windows' and includes a brief description of the installer's purpose. Under 'Which add-ons do you want installed?', the 'Remote Access' and 'Ad Blocker' options are checked. The 'SuperShield Options' section features several dropdown menus: 'System Tray Menu' (Disabled (Recommended)), 'Removable Storage Devices' (Block), 'Blocked File Notification' (Display Only (Recommended)), 'Java Runtime' (Block), and 'Patch Management' (Enabled (Automatic)). The 'Customer to put computer under' dropdown is set to 'Dunder Mifflin', and the 'Group' dropdown is set to '-- No Customer Group (Customer Level) --'. At the bottom, there is an 'Installer Distribution' section with an 'Email Installer' button and an 'Installer Download' link. A 'View Minimum System Requirements' link is also present. A green 'Download' button is located at the bottom right of the page.

Once logged in, there are two primary methods of installation. The first is to create and download a custom executable. Navigate to a customer's home page and click on the Add a Device button inside the Device tab.

Let's take a look through the first tab, "Windows Installer" and the add-ons that are selected by default in the image below.

SuperShield: This is our real time security component and will stop any program from running that is not on our whitelist. SuperShield will never allow an unknown application to execute on your computer without user or admin permission (SuperShield is now always included in the installer and will no longer have a checkbox (7/31/20)).

Remote Desktop: This will allow you to gain remote access to an endpoint on your account and control it from your current computer.

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.

Removeable Storage Control: 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 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.

Customer/Groups: If you are accessing this screen from your MSP page, you will need to select the customer this installer should associate with. If you have groups set up, you can also select the group. It will automatically add any device using this installer to your chosen customer and group. It is not recommended to leave the customer dropdown blank.

Now you're ready to download the installer. You can enter an email address and the installer link will be sent there with instructions to carry out the installation. You may copy and paste the URL link into an email yourself, or save it for later. Lastly, there is a download button available at the bottom.

Clicking this will 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 filename. *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 MSP 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

Device Manager Procedure

The device manager installer allows you to use Active Directory to install PC Matic MSP onto your 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.

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 will automatically check each prereq and let you know if it has been satisfied.

- <https://files.pcpitstop.com/support/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.
 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

Now if you did not meet all of the prerequisites, it's time to make sure they are all satisfied before we move on to 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.

1. Open a PowerShell prompt as an administrator.
2. Run the following command: Set-ExecutionPolicy RemoteSigned -Force
3. 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 MSP management console. To access it, open your management console and enter the Account Settings > 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. 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 MSP console. When you enter that area, you should begin to see the devices from your network populating into the Devices tab.

The Device Manager service must run under a user that is part of the Domain Administrator group. Please enter valid credentials in order for the Device Manager installs to function properly.

Nickname	Domain
<input type="text" value="Nickname"/>	<input type="text" value="Domain"/>
Username	Password
<input type="text" value="Username"/>	<input type="text" value="Password"/>

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-GPUdate -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:\gpreult.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

Device Manager Installer

System Requirements

- Server: Requires PowerShell 3.0 or higher
- Server: Requires .net Framework 4.5
- Endpoint: Requires PowerShell 2.0 or higher

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

To access the device manager installer, expand Options from the sidebar and choose Install/Uninstall. Device Manager is located in the second tab of the popup window. Within the device manager installer, you have several options that can be configured.

Minimum Requirements Script: If you're not certain that your server has met the minimum requirements for PowerShell and .net framework you can download the zip file and run the minimum requirements script to check.

Create Remote PowerShell GPO: This option will create a GPO for your active directory network that enables remote PowerShell execution. In order to use the installer you must keep this option checked or create a GPO yourself that enables remote PowerShell execution for the computers you choose.

Group Dropdown: Assigning the Device Manager to a specific group allows you to set up multiple Active Directory networks with several different domain controllers. If you only have one domain controller, leave this set to unassigned so the Network Devices tab appears on your Company page.

Device Manager Credential: The device manager needs to be run under a user that is part of the Domain Administrator group. If a service is not entered here it will be run as the local system user and may not have the permissions to operate properly. You can always edit or change this credential later in Network Devices.

After you configure your options, choose the download button to download the executable. This will need to be run on your domain controller to install the device manager and configure the GPO if you selected that option.

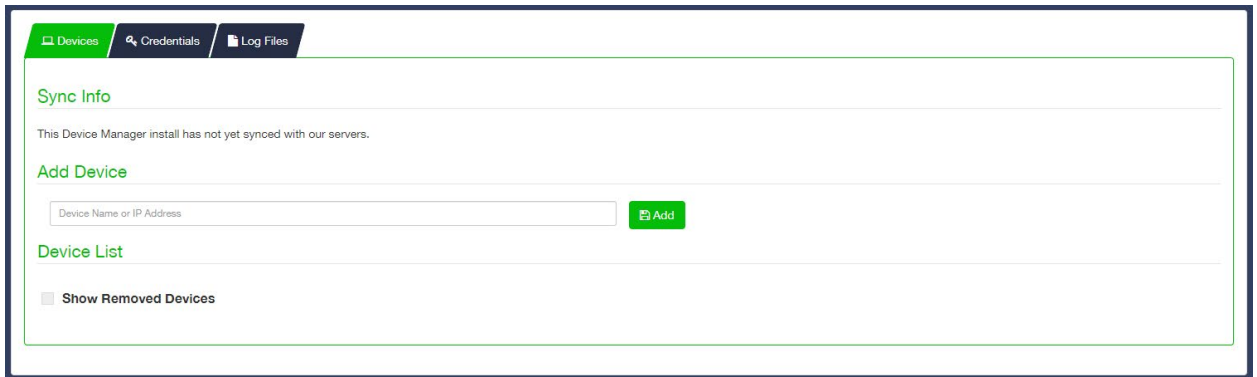
After installation, the device manager will find computers on your AD network and display them in the Network Devices tab. This is the yellow tab shown below; if you chose a specific group, remember to filter by that group in order to see the Network Devices tab.

Network Devices

After the installation has completed on your server, or if you set credentials for the Device Manager before download, you can access the Network Devices tab.

There are two tabs available from this view, the Devices tab that shows all of your computers 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.

The devices tab will also show the current sync status of the device manager. If a sync is actively happening you will see the progress as it reads devices and checks for new installs/uninstalls to be made.



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 MSP is currently installed on the endpoint.
- Uninstalled: PC Matic MSP is currently not installed on the endpoint.
- Pending Install: PC Matic MSP will be installed on the endpoint when the scheduler service on the server runs (1 hour max).
- Pending Uninstall: PC Matic MSP 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. 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.

The screenshot shows the 'Credentials' tab in the PC Matic interface. At the top, there are navigation tabs for 'Devices', 'Credentials', and 'Log Files'. Below the tabs, a message states: 'This is a list of admin credentials that we can use in order to remote install or uninstall the PC Matic Agent software from each endpoint. These credentials are stored encrypted in our system and sent over to your server encrypted as well. Each device should have a credential attached to it in order to do a remote install or uninstall.' A note below reads: '*Please note that the GPO will not be created unless you set a credential to run the service. It is recommended that you use a credential with domain administrator permissions.' There is a green link 'Add New Credential'. Below this is a checkbox 'Use To Run Device Manager Service (Domain Administrator Recommended)'. The form contains several input fields: 'Nickname' (with a placeholder 'Nickname'), 'Domain' (with a placeholder 'Domain'), 'Username' (with a placeholder 'Username'), 'Password' (with a placeholder 'Password'), 'Confirm Username' (with a placeholder 'Confirm Username'), and 'Confirm Password' (with a placeholder 'Confirm Password'). A green 'Save' button is located below the form. At the bottom, there is a table titled 'Credentials' with the following columns: Nickname, Domain, Username, Create Date, and Update Date. The table contains one row with the following data: Nickname: test, Domain: test, Username: test, Create Date: 2019/10/15, Update Date: 2019/10/15. There is a green checkmark icon to the left of the row and a red 'X' icon to the right.

Nickname	Domain	Username	Create Date	Update Date
test	test	test	2019/10/15	2019/10/15

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>

Account Home Page

Your company home page is a great place to adjust settings across all customers at one time as well as adjust settings for your own company. Several features need to be customized from your company home page before you can use them at a customer level. Access this page by selecting Account Settings from the sidebar.

Account Reports

Here you can track a variety of stats for your maintenance and security dashboard. Get an overview from all computers across all customers or a filtered look at a specific time period using the All Time dropdown. Interact with each tile to get more detail about what has been updated, cleaned, removed or optimized on each device.

Unassigned Computers

This tab will show computers that are not currently assigned to a customer. If the installer was created without selecting a customer, the computer will appear in this tab and need to be assigned to the correct customer by clicking on "Unassigned" under Group.

Invoices

View all invoices from PC Matic MSP to you. Here you can view the invoice and download it as

a PDF for your own records.

The screenshot displays the PC Matic MSP interface. On the left is a sidebar menu with categories like CUSTOMERS, DASHBOARD, REPORTS, and ACCOUNT SETTINGS. The main content area shows account details for 'PC Matic MSP' with fields for Company, Name, Title, Invoice Date, Payment Terms, and AutoPay. Below this is a grid of security reports including RDP Lifetime, Ransomware Lifetime, Available Cabrand 1, Education Pager, Local Government Pager, Securing Healthcare, Whistleblasting, Law Enforcement, Securing Finance, and Ransomware Pager. At the bottom, there is a section for 'AutoPay: Off' with a green button to 'Update Invoice AutoPay Settings'.

Payment Settings

Setting up Auto Pay for your PC Matic MSP account is the easiest way to manage your account and the charges for all of your devices.

Navigate to your MSP page by clicking on Account Settings in the sidebar menu. On this subsequent screen, look to the right and click on: Update Invoice Auto Pay 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.

AutoPay: Off

[Update Invoice AutoPay Settings](#)

Manage Users

Open Account Settings from the sidebar menu and click the button labeled “Manage Users” to edit existing users for your web portal. To set up a new user, click “Add User” from the sub sidebar, 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.

Authentication

For each user you can choose to enable Authentication when editing or creating the user. In addition, you can choose to preauthorize all devices on the account for that user. This allows them to easily login to your PC Matic MSP console from any device on your account without needed action from an Administrator to approve the device. Any devices that are not currently on your account will still be blocked by default and need to be authorized manually.

Roles

- Account Admin - Full account access and the ability to create and manage additional users.
- Group Admin - Recommended for users with access to groups only.
- Admin for Customer(s) - For users that need full access but not for all customers.
- Group Access - Recommended for users with limited access needed.
- Customer Access - Customer management tools and actions.
- 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 three 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

1. Installers
2. Uninstall/Install SuperShield
3. Master Scheduler Access
4. Command Prompt
5. Move Device Action
6. Notification Options
7. Remote Desktop Action
8. Notifications Setup

- 9. Reboot Action
- 11. Software Management
- 13. SuperShield Options
- 15. Endpoint Vulnerabilities Report
- 17. Remove Device
- 10. Whitelist
- 12. Scan Now Action
- 14. Account Settings
- 16. File Manager
- 18. Lockout Settings

Role Details

Role Name Role Description

Assign Rights:

<input type="checkbox"/> Installers	<input type="checkbox"/> Master Scheduler Access
<input type="checkbox"/> Move Device Action	<input type="checkbox"/> Remote Desktop Action
<input type="checkbox"/> Reboot Action	<input type="checkbox"/> Uninstall/Install Supershield
<input type="checkbox"/> Command Prompt Access	<input type="checkbox"/> Alert Options
<input type="checkbox"/> Alert Notifications	<input type="checkbox"/> Whitelist
<input type="checkbox"/> Software Management	<input type="checkbox"/> SuperShield Options
<input type="checkbox"/> Scan Now Action	<input type="checkbox"/> Account Settings
<input type="checkbox"/> Endpoint Vulnerabilities	<input type="checkbox"/> Lockout Settings
<input type="checkbox"/> Uninstall Agent	<input type="checkbox"/> File Manager
<input type="checkbox"/> Install Ad Blocker	

Authentication

To increase the security of your management console you can enable Multi-Factor Authentication within PC Matic MSP. This authentication will be for anyone on your team that logs into the PC Matic MSP cloud console. Because your cloud console has access and control over your devices and sometimes your network, we strongly recommend enabling this setting for added security.

Our Multi-Factor Authentication centers around devices. Not only must a user have credentials to access the account, but their Windows or macOS device must also be authorized by our software before the login can be successful. Each user gets 1 free device upon their initial login. The first device they sign in on will be authorized automatically but any subsequent devices they attempt to access from will need to be approved by the administrator within the Pro console.

To authenticate each device, the user must install a small piece of software from PC Matic MSP when they attempt to login (below). This is used to set and monitor a unique identifier for

that device and only needs to be installed one time.

⚠ PC Matic Authentication is not installed! ⚠

To protect your account with PC Matic Authentication, you must download and install the PC Matic Authentication software.

You can download PC Matic Authentication by clicking the button below:

[Download](#)

When the download is finished, run the installer.

Once PC Matic Authentication is installed you will be automatically logged into your account.

Enabling Authentication

The authentication setting is done on a user level in PC Matic MSP and can be enabled in two different places.

- Account Settings > Authentication: Here you can click Enable Authentication to turn it on for your main Admin account.
- Account Settings > Manage Users: Edit existing users and check the box to turn on Authentication for that user.

Preauthorize Devices

When enabling authentication, you will have the option to preauthorize devices. Checking this box will automatically preauthorize any devices that are on your PC Matic MSP account and that user has access to inside the console. This will allow them to open the management console and login with their credentials from any machine you are already installed on without action required from an Admin. If they attempt to login from a device not on your account, you can still manually authorize it using the Authentication area below.

Managing Authentication

To manage all your authenticated devices, head to Account Settings and Authentication. This new report will not only show you all login activity, but it is also where you can authorize and deauthorize devices. This process happens in real-time, so you can quickly authorize devices for your staff. Atop the report, you can enable Authentication for the main login on your account by clicking Enable Authentication. Only Admins on your account can see this report.

There are four possible statuses for a login attempt from your user.

- **Authorized Device** - The user successfully logged in on an authorized device. You can deauthorize that device by clicking the red Deauthorize Device button.
- **Preauthorized Device** - The user successfully logged in on a preauthorized device. You can deauthorize that device by clicking the red Deauthorize Device button.
- **Unauthorized Device** - The user attempted to log in with correct credentials on an unauthorized device. You can authorize that device by clicking the green Authorize Device button.
- **Incomplete Device** - The user attempted to log in with correct credentials but either did not install the authentication software, or it is not running properly.
- **Incorrect Credentials** - The user attempted to log in with incorrect credentials.

Status	Date/Time	User	Device	Action
	2020/06/04 11:58:53	businessdemo+channel@pcmatic.com	Jaime	
	2020/06/02 09:29:33	businessdemo+channel@pcmatic.com	Jaime	
	2020/06/02 09:29:11	businessdemo+channel@pcmatic.com	Devin	
	2020/06/02 09:12:54	businessdemo+channel@pcmatic.com	Devin	
	2020/06/01 16:06:34	businessdemo+channel@pcmatic.com	Jaime	
	2020/06/01 11:51:47	businessdemo+channel@pcmatic.com	Laura DEMO	
	2020/06/01 11:44:58	businessdemo+channel@pcmatic.com	Demo Remote	
	2020/06/01 11:42:52	businessdemo+channel@pcmatic.com	Demo Remote	
	2020/06/01 11:41:05	businessdemo+channel@pcmatic.com	Demo Remote	
	2020/06/01 11:39:35	businessdemo+channel@pcmatic.com	Jaime	

Showing 1 to 10 of 14 entries (filtered from 46 total entries)

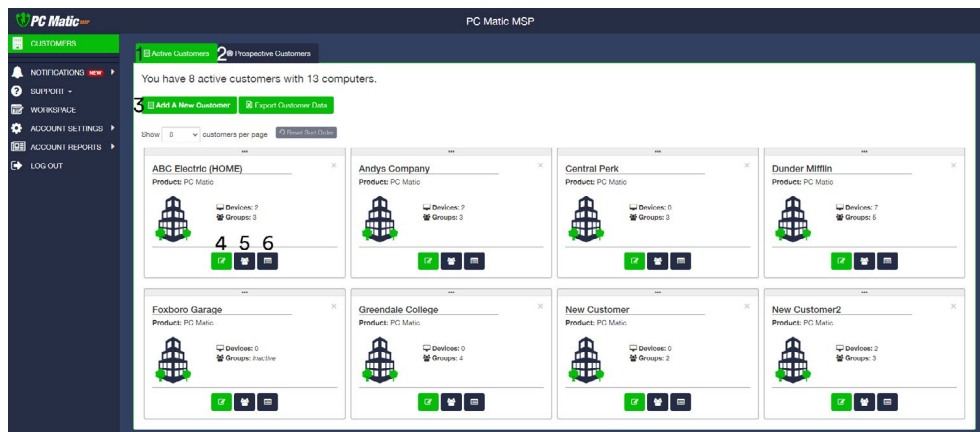
Previous 1 2 Next

Portal Home Page

The portal home page is the primary landing page in the portal and provides an overview of all Customers along with navigation links to dive deeper into the many available options provided when using PC Matic MSP.



1. View Active Customers
2. View Prospective Customers
3. Add a New Customer
4. Edit Customer Information
5. View Customer Contact Information
6. Add Notes Per Customer



Prospecting Tool

The prospecting tool is specifically designed for you to use for potential managed service customers. It allows you to offer free scans to easily demonstrate the potential of PC Matic and a part of the services you are offering.

You can install the prospecting tool on as many endpoints as needed, it will provide one free scan on each computer with a report of what changes would be made with an active license. This report can be used to demonstrate just part of the value you can bring to potential customers.

Utilizing the Prospecting Tool

From your portal home page, click on the Prospective Customers tab and choose Add A New Prospect at the top.

Now fill out the information form for this customer to create their entry in your management portal. If you would like to enable groups now, you can do that by checking the Use Groups box and assigning groups to the customer. Click save after you have completed the form and you will automatically arrive at the new customer's page.

This customer page will look different than an active customer, as all features are not enabled for prospective customers. You can access the installer window to download the Prospecting Tool and install it on each endpoint.

After installation on your endpoint, the endpoint will communicate with our servers and a diagnostic scan will be run. This can take up to an hour depending on the computer; its speed, hard drives capacity, etc., but typically takes about 10 to 15 minutes.

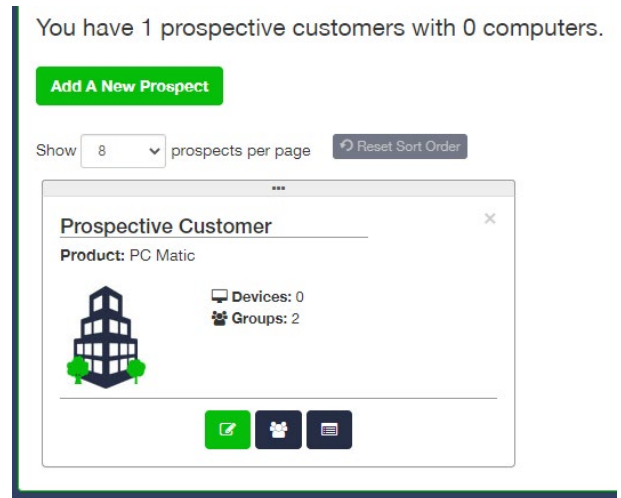
You will also see the endpoint appear in your management portal after the scan completes. There are several ways to view and demonstrate the results from the scan depending on your choice. Under each endpoint in your management portal there will be a PDF icon where you can view the full report from the scan.

You can also view a summary of all computers you put the prospect tool on for each potential customer using the Business IT Evaluation Report. The report gives an overview of changes that will be made on the endpoints with an active license.

Becoming an Active Customer

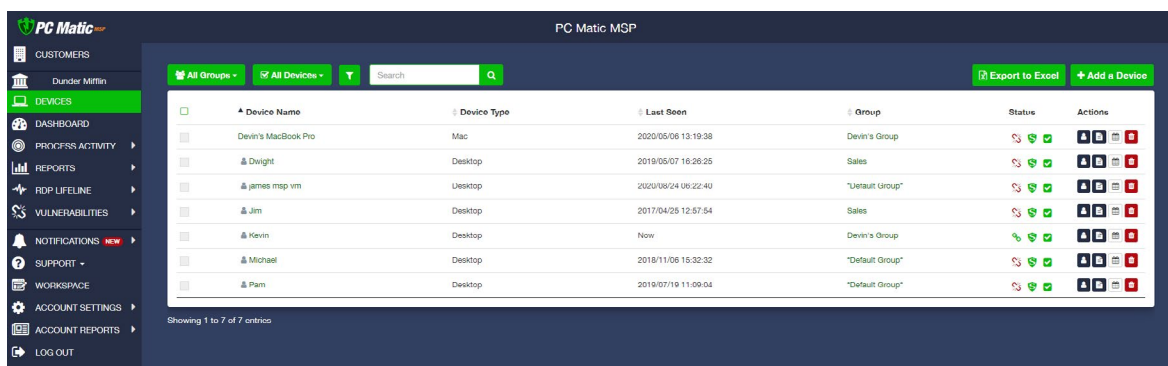
After your customer reviews the report and decides that they want to move forward using your services along with PC Matic, you can move them to an active customer. Open the client's page and click: Edit Customer Info. Uncheck the "Is Prospect" entry to officially make them an active customer. You will now be billed for any of the endpoints you install the protection on.

You may now use the agent Installer from the Active Customers listings to install the full version of the PC Matic software on remaining devices with the inclusion of our real-time antivirus program, SuperShield. For assistance with an active installation, check the Installation section of the User Guide. If there are devices with the prospect tool installed, navigate to the device page and visit the actions section to remotely install SuperShield.



Customer Home Page

The customer home page is the landing page in the portal where you can manage each customer individually, including setting up scans, whitelisting files, viewing SuperShield reports, etc.



Dashboard

The dashboard page can serve as the homepage for your company on each login. This page allows for customization of several account metrics and security reports so what you want to see is front and center on each login.

Notifications

The new Notifications tab presents general information from your devices. These are not Alerts that need immediate action, but rather suggestions that you can take a look at and decide if you want to take any action. Anything that requires fast or immediate action is done automatically by PC Matic MSP.

Process Activity

The new Process Activity report combines the previous EDR and Blocked Status reports. You can now open the Process Activity report and look at any and all processes that are in your network. Filter by processes that were blocked, allowed, or all and make decisions on locally whitelisting from this report quickly.

Reports

You can get a total summary of Security and Performance in the green row at the top, and a detailed view of each device in the group. To review a section in depth, click the header title in

green. For example, select the green 'Security Patches' label and a window will slide in with the specific machines that have received software patches.

- Download a PDF of the report, and schedule it to be sent out via email at your chosen interval.

Endpoint Vulnerabilities

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

- **Remote Desktop Enabled** - 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](#).
- **SuperShield User Options Enabled** - When SuperShield User Options are enabled at a device, the user can access admin controls through the system tray menu to turn off protection, enable override modes, and more.
- **SuperShield Blacklist Mode Enabled** - SuperShield should be running in whitelist mode at all times. If devices populate here, switch them back to the default: SuperShield Protection.
- **Lockout Thresholds Not Set** - PC Matic MSP 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](#).

Computer Management

To manage all devices for a customer, click the Devices tab from the customer home page. Using the group filter you can manage devices one group at a time, and sort the list by the method of your choosing.

To search for a certain device quickly, use the search box located at the top of your device list. This will allow you to search based on group or device name.

Click the filter icon above your list of devices 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 that can be used in conjunction: software installed, operating system, IP Address, software versions, and many more.

After selecting one or more devices from the list, bulk actions will become available. This will

allow you to bulk assign devices to groups, remote reboot, apply parent SuperShield options, adjust account lockout settings, delete or uninstall. You can also select all devices currently in this view by clicking the box with the green checkmark in the leftmost column.

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

Device Actions

From an individual device page the available controls are drastically expanded. From the Actions section you can make changes to a device as if you were sitting in front of it in several different ways; no matter where it's physical location is. This process does require that the device be online and connected to our servers. You can verify it's connection by checking the status icons.

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.

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.*

Lockout Settings

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

Move Device

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

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 MSP.

Remote Access

- Initiate a remote session using our modified VNC client. The PC Matic MSP 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.

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.

Scan

- Scan Now
 - ◊ Run a scan on this machine with the time set to 'Now'. You can adjust the configurations for the scan before executing it.
- 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.

Sleep Settings

- The sleep settings action allows you to override the current sleep settings and prevent an endpoint from becoming disconnected while sleeping. When enabled, the device will follow your current Windows sleep settings instead.

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 whitelist or blacklist 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 whitelist. 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.

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 whitelist this item locally as well to avoid future quarantines.

Icon Descriptions

	Device Powered Off		“SuperShield is installed & running properly”
	Device Powered On		Scan in Progress
	<ul style="list-style-type: none"> “SuperShield is paused” “SuperShield is not unlicensed and inactive” “SuperShield is starting” “SuperShield is disabled” “The SuperShield service is unavailable” “Cannot connect to the SuperShield service” “Unable to determine realtime status of SuperShield” 		<ul style="list-style-type: none"> “SuperShield is operational and detects applications that need updates” “SuperShield is updating definitions” “SuperShield definitions update failed”

	Notification		No Notifications
---	--------------	---	------------------

Status Details

In the image right you can see the details for the current connection. In this example the computer we have selected is connected to our servers. If it was powered off or offline, 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.

Patch Management

PC Matic MSP will maintain patches for 30 third party applications. In the security patches section of the Reports tab, you can view recent updates that have happened on all endpoints. The full list of applications we update is below.



- | | | |
|-------------------------------|-------------------------|-----------------------|
| 1. 7-Zip | 11. Adobe AIR | 21. PDF Creator |
| 2. Adobe Flash Player ActiveX | 12. Adobe Flash Player | 22. QuickTime |
| 3. Adobe Flash Player PPAPI | 13. Adobe Reader | 23. Safari |
| 4. Adobe Reader MUI | 14. Adobe Reader XI | 24. Winamp |
| 5. Adobe Shockwave | 15. FileZilla | 25. WinRAR5.x |
| 6. Foxit Reader | 16. Google Chrome | 26. PDFXChange Viewer |
| 7. iTunes | 17. Java 32 | 27. Real Player |
| 8. Java 64 | 18. Mozilla FireFox | 28. Skype |
| 9. Mozilla SeaMonkey | 19. Mozilla Thunderbird | 29. WinRAR |
| 10. OpenOffice | 20. Opera | 30. WireShark |

When looking at previously updated applications, you will see a result code on the right hand side. If this code is 0 then the application installed correctly and was updated. A different code may display if the updated 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 the Vulnerability Management tab, 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 MSP 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 Vulnerability Management section places restrictions on the updates that happen during the scan process and through SuperShield. Any restrictions that are placed here will affect updates through a scheduled scan and through our realtime protection component SuperShield. It's important that if you only want updates to happen at a certain time you turn Vulnerable Updates off in SuperShield Options.

Scheduling a Scan

Scans can be scheduled at different levels within your account. The Customer Master Scheduler will allow you to schedule a scan for all of the computers at that customer. This allows you to easily maintain a large amount of endpoints by only configuring one scan. The Master Scheduler is accessible from the customer home page.

Click Account Settings and open the Master Scheduler. Here you can choose to target a customer or group within a customer for that new scan. Lastly, from an individual device's page you can click Scan from the left sub sidebar and run a new scan.

Live Scan Status

From an individual device page you can now monitor the live status of a scan. This allows you more information on what stage the scan is in and when it will be closer to concluding. From this view you'll also see rotating messages with information about the scan process within PC Matic MSP. 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. *Note: On macOS devices you will see a small eye appear above the computer's connection icon on the device page to indicate a scan is currently running.*

Allow Listing

With PC Matic MSP, 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 for your customers so business can continue as usual. This is most useful when a customer is dealing with proprietary software that PC Matic or SuperShield may not yet recognize.

In this section we will cover the variety of ways you can allow list within PC Matic MSP, and all of the different components that can take advantage of a local allow list.

Process Activity

This report is the best place to locally allow something if you need to. Right from your home page you can access the tab and get a complete list of any process that was blocked across your environment.

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

Reports Tab

The reporting tab is the best place to locally whitelist items from your scheduled scans and cleans. From the Reporting tab you can view details for items that were stopped or removed by clicking on the green link for the column name. For example, if you had a service that was optimized in your environment and need to whitelist locally, click the Services Stopped header

to view the Services Stopped Details. Once here, you can click the Add to Whitelist button for any service and choose the level that you would like to whitelist it for.

SuperShield Allow & Block

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

- **MD5** - 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.
- **Digital Signature** - 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 Serial Number for the signature and the Issuer ID. Issuer ID is a unique value from PC Matic that can be obtained from the Blocked Status report by hovering over a blocked files Digital Signature icon.
- **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 allow listed if absolutely necessary. Any folder or file below that path will be allowed to execute even if it is unknown or known bad.

SuperShield Report

If an application that you know is good was blocked on a users computer, it can quickly and easily be added to the local allow list at any level you choose. From your portal home page, choose the devices tab and navigate to the device that the application was blocked on by clicking the device name.

Now from that you have selected a device, choose the tab labeled “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 protections mode.

Be sure to adjust your search type between “All Fields” and “Any Fields” depending on your search.

1. Process Name – Find your application using the name of the process.

2. Vendor – Find your application using the name of the software vendor.
3. Product Name – Find your application using the name of the application.
4. Current Status – Current status uses the current known good, bad, or unknown value according to PC Matic MSP.
5. Runtime Status – Runtime Status uses the known good, bad, or unknown value at the time of execution according to PC Matic MSP.
6. 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 green 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 whitelist at that level. Now use the Allow button to add it to your local allow list, or Block to add it to your local block list.

Scan Report

Allow listing can also be done from a scan report for the individual endpoint across all of the categories listed above. Navigate to the affected computer in the portal and pull up the relevant scan report. Depending on which category you need to allow for, navigate to that section of the scan report to dial in to the details.

Individual Endpoint

If you have not restricted the client options within SuperShield on your endpoints, you can locally allow things right from your endpoint. Navigate to the SuperShield icon in your system tray and click it to open the options menu. Then hover over Protection Level > Block Notification Method and select Prompt for Override. Now, try to run the software that was blocked by SuperShield again.

When you execute the application, you will receive a pop up window from SuperShield that allows you to make a decision on the file yourself. Keep in mind that this application is unknown to our program and you should only be whitelisting software you absolutely know is good. You can make several determinations on the file.

1. Block – Locally block the file on your endpoint temporarily.
2. Block Forever – Locally block the file on your endpoint forever.
3. Allow – Locally allow the file on your endpoint temporarily.
4. Allow Forever – Locally allow the file on your endpoint forever.

In order to edit these choices in the future, you will need to access your full local whitelist from

SuperShield Allow.

RDP Lifeline

RDP Lifeline is a centralized location inside PC Matic MSP to manage and secure Remote Desktop Protocol across your environment. You can access RDP Lifeline by clicking it in the sidebar on the left hand side of your management console. Inside, you'll find three main components, RDP Management, RDP Logging, and RDP Security. Throughout PC Matic MSP 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.

RDP Management - Remote Desktop Devices

The first tab inside RDP Lifeline is where you will manage RDP on the machines in your environment. Remote Desktop Devices will display all of the devices that are currently on your account and information about the current RDP status and schedule for each device.

Working left to right in the image above, we'll breakdown what each different piece of this

RDP Enabled?	Active Session?	Device Name	Group Name	Port	RDP Schedule	Hours Per Week	Set Schedule
🟡	👁️	2019-WinSrv	Administration	3389		168.00	🔌📅⊙
🟡	👁️	7-Win	"Default Group"	3389		168.00	🔌📅⊙
🟡	👁️	8-Win	"Default Group"			0.00	🔌📅⊙
🟡	👁️	Andy	Devops			0.00	🔌📅⊙
🟡	👁️	Andy Paul	"Default Group"	3389		0.00	🔌📅⊙
🟡	👁️	Dell	"Default Group"	3389		0.00	🔌📅⊙
🟡	👁️	Demo Remote	Engineering	3389		10.00	🔌📅⊙
🟡	👁️	Devin's iMac	"Default Group"			0.00	🔌📅⊙
🟡	👁️	Devin's MacBook Pro	"Default Group"			0.00	🔌📅⊙
🟡	👁️	Hope	"Default Group"	3389		0.00	🔌📅⊙

table does.

- RDP Enabled? - When an orange icon is displayed, 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.

Auditing - RDP Log

The second tab inside RDP Lifeline 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 MSP. This includes IP Address, Device Name, Location, Session Duration, Login Username, Active Status, and more.

Security - RDP Whitelist Client Devices

PC Matic MSP uses whitelisting to protect your RDP ports on your network. The RDP Whitelist Client Devices tab allows you to enable our RDP Security and control your device whitelist. By having our software installed on each machine you can add that device to your RDP whitelist, allowing it to RDP into any device on your network. Using a default-deny approach, any device that is not on the whitelist and attempts to initiate an RDP session will be blocked. You can receive realtime Notifications about these sessions as well that include quick actions to take and all information about the session attempt right inside the Notification.

Groups

Keeping your endpoints and servers coordinated and organized is essential to quickly managing your computers. Setting up groups of computers will allow you to find, identify and coordinate when and how you wish to have these endpoints scanned and configured. To begin, from your portal open Account Settings from the sidebar menu and click Edit Groups.

Now you can create as many groups as needed for use with your customers. In order to assign a group to a customer, it first needs to be added at this screen for your company. To use groups, you must turn it on for each customer in your MSP portal. Click Edit Customer Info under your customer's name on their home page and check the first box that says "Use Groups".

Simply select the group on the left hand side you wish to assign and click the arrow pointing to the right. Once assigned you can begin sorting that customer's endpoints into the groups.

Now that you have set up the groups you want to use, you can take advantage of them right from the installer window. While creating the executable for your installer, you can select a

customer and group from the dropdown to automatically associate the endpoint with that customer and group when it appears in your management portal.

Changing Groups

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

Navigate to the computers tab and locate the computer that you would like to change groups. In the individual computer's box, click on the link below the "Group" heading. Click on the drop-down arrow and choose a group, then save.

To change groups in bulk, navigate to the Devices tab (in table view) and select the checkbox to the left of each device you want to move together. Once checked you'll see new icons appear above the device list for Bulk Actions. Select the first icon, Bulk Assign Devices, and choose the Group you wish to assign to. Save to complete your choice.

Notifications

PC Matic MSP is monitoring a lot of information about all of your devices to keep you informed. All available Notifications can be configured as notifications via Email, SMS, or within your management console.

From the Notifications view inside your console, you can dismiss individual Notifications, dismiss all Notifications, or disable any Notification with the click of a button. Disabling a Notification will turn that Notification off for that level in the future and dismiss all existing Notifications of that type. Certain Notifications will also include a quick actions menu to remedy that Notification without having to leave this view. Once an action is taken the Notification will automatically dismiss.

The Notifications available in PC Matic MSP 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.
- **Device goes Online/Offline** - This will trigger immediately if a device goes online or offline depending on your configuration.
- **SuperShield Blacklist Mode** - This will trigger if SuperShield is left in blacklist mode for more than the set threshold.
- **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 messages for any Notifications on the account. To receive these, first add a notification contact. Select Notification Contacts from your Account Settings. Now select Add New Contact in the upper left hand corner.

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 you to missing out on Notifications completely, at the end of the quiet time you’ll still receive the Notifications 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 select Notification Setup from Account Settings. After selecting your notification from the dropdown list, select the contact person that you wish to receive the notification and click the assign button above your contact.

Next to each contact, you can select how many notifications they will receive per x amount of time. This can be used to create a specific amount of time (24 hours) that has to pass before you get another summary. No matter the choice, each time period will roll up into one email with all notifications from that time window.

Notification Options

You can adjust the threshold and turn off individual notifications by visiting the Notification Options tab. These options can be customized across all different levels including entire account, customer, group, and individual device.

SuperShield Options

SuperShield Options will allow you to set security settings for the company, group, or individual computer. Use the Group filter to drill down to an individual group level. Applying settings at the MSP, Customer or Group level will immediately attempt to apply those settings to every device that is online and within that level. *This will override 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.

Protection Level - Setting your malware protection level

- SuperShield Protection - Protection using our whitelist. (Default)
- Blacklist Only Mode - Protection using a blacklist, will not block unknown applications.

Vulnerability Protection - Patch Management integrated in SuperShield

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

Disable User Control - Remove all control from the user at the endpoint level and manage all settings from the web portal.

Block Notification Method - Notification settings for when unknown or bad software executes

- Display only - Small notification alerting the user that SuperShield blocked execution. (Default)
- No Block Notifications

- Prompt for Override - Gives the user the ability to whitelist unknown software at the endpoint level

Enable Java - 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 a customer still needs 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.

Device Control – Disable 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.

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.

Remote Desktop

In order for the remote desktop application to function properly, the host as well as the client must have the PC Matic MSP agent installed as the VNC agent that runs this feature is imbedded in the installer as Remote Desktop and uses port 5500 & 5900. While using the VNC, press **F8** to open the VNC options menu.

1. Select the Devices tab from the customer home page, and select the device name that you wish to remote into
2. Click Remote Access in the Actions section 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.

Command Prompt

The Command Prompt in PC Matic MSP 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 * <i>Message goes here.</i>	Send a popup message to a 64 bit machine.
%SystemRoot%\System32\msg.exe * <i>Message goes here.</i>	Send a popup message to a 32 bit machine.

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

Show SuperShield version number

wmic datafile where name="C:\\Program Files (x86)\\PCPitstop\\SuperShield\\PCMaticRT.

exe" get Version /value

Stop/Start PC Matic MSP'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
```

Local Endpoint Options

With PC Matic MSP you have total control over local options available to your 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.

From the SuperShield icon by default several options are available to the user. This includes the ability to pause protection, turn it off, and override it. These options can be taken away from the local endpoints according to various different levels, which will be discussed in the next section. Below you can see the options that will be present on the endpoint if no restrictions are enabled.

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.

1. About SuperShield: Provides version information of the software installed.
2. Protection Level: View image below.
3. Security Report: View the files analyzed by SuperShield and their status.
4. Vulnerable Software Updates: Adjust local patch management settings.
5. White and Black lists: View and edit the local whitelist or blacklist.
6. Adjust SuperShield current status, turning real-time protection off or pausing it for a designated time period.
7. Switch between whitelist protection (SuperShield) and blacklist protection (Industry Standard).

8. Tweak notification settings and allow overriding of unknown or bad applications.
9. Turn patch management off or require authorization from the local endpoint before installation can occur.

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.

Removing Customers

PC Matic MSP wants to make it as easy as possible for you to off load a customer and their devices if you need to. There are several different ways you can remotely deactivate a customer so you are not charged for their devices anymore, or if a customer is overdue on their bill.

Remote Uninstall - Device Manager

If your initial install process for the customer was done using the Device Manager component of PC Matic MSP then you can remotely uninstall the product in full using a similar process to the install. Navigate to the customers page and group if one applies that has the Active Directory network attributed to it. Click Account Settings > Network Devices at the top and then choose the devices you want to uninstall from by selecting the box to the left of each one. After selection click the red uninstall button in the bulk options above the list to complete.

Remote Uninstall - Actions

If the customer's devices are still online, you can remotely uninstall from the device list. Select the checkbox next to each device you wish to uninstall and choose Remove Device from the bulk actions dropdown. This will remove all components from their machine remotely. It will then remove their device from your account

Firewall Settings

PC Matic 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
- master.pcpitstop.com

If you prefer to utilize IP addresses, then white listing 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
- 199.27.128.0/21
- 54.159.56.72

Server Security

Server Security is specifically engineered for server protection and alerting. When you attempt to use the normal installer on a server it will automatically recognize the operating system and install the server protection.

Within PC Matic MSP Server Security there are several added features and protection that is geared towards critical servers.

Device Control

We understand that your servers are often the vessel for your most valuable information, which needs to be kept secure from malware and physical theft. With Device Control, you can easily disable removable storage capabilities to thwart potential malicious actors from stealing files right inside your building.

In order to turn Device Control on for a server or group of servers, access the SuperShield options in your management portal. Once activated, Device Control will automatically eject any connected removable storage devices and block them from accessing any data. If you elect to deactivate this feature, connected drives will remount automatically.

Server Uptime Notifications

Making sure your server is always online for you or your customers is vital to business. If your server goes offline for any reason we'll immediately notify you over SMS or Email. You can set uptime Notifications just like any other Notification in the management portal. Visit your group of servers or individual server and select the notifications bell.

Here you can select the server uptime Notification from the list and select the method you would like us to notify you about it by. Important: If you previously set a quiet time for a certain contact, all Notifications will be silenced during that time period including server uptime Notifications.

Maintenance Mode

Enabling Maintenance Mode will automatically silence any Notifications for the servers it is applied to. This allows you to perform scheduled maintenance and updating on your servers without getting bombarded with Notifications to work through or check on your phone.

You can enable this mode by visiting the server's page in the management portal and clicking on the Notification options button to toggle maintenance mode on or off.

Priority Malware Analysis and Support

Servers can be the lifeblood of your business; with priority analysis any unknown applications stopped from running will receive categorization from our team within an hour. You don't need to take any action to use this feature, unknown files are automatically uploaded to our malware team and server applications are pushed right to the top of the priority list so categorizations come as soon as possible.

Refined Product Capabilities

Having a product that is capable of protecting a server is very important, but it can't also cause

interruptions or harm to business operations. We have specifically engineered the server protection to keep servers secure and running properly. The scan engine now intelligently cleans your server to remove malware, browser add-ons, and junk files that get left behind clogging up your storage.

White Label

With white labeling within PC Matic MSP you can replace our name and graphics with your own so that your customers see you are providing their protection and services. Once you provide the images to our team, we can move forward creating your customer installers. Below you'll find a full list of the benefits of white labeling PC Matic MSP.

1. White labeled MSI installer with opportunity to provide custom graphics.
2. White labeled Management Portal replacing the PC Matic header with your logo or custom banner created by your graphic designer.
 - This comes with a custom subdomain for access (<https://yourcompany-portal.pcmatic.com>).
3. Endpoint software gets a custom install directory name based on your vendor/product name provided.
4. Entry in Programs and Features uses your product name.
5. SuperShield real-time malware agent is generically labeled as SuperShield and all references to PC Pitstop & PC Matic are removed.

Pricing

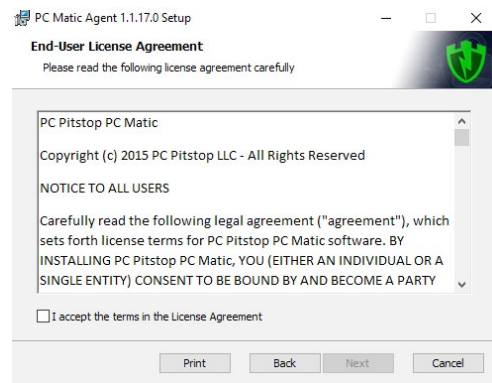
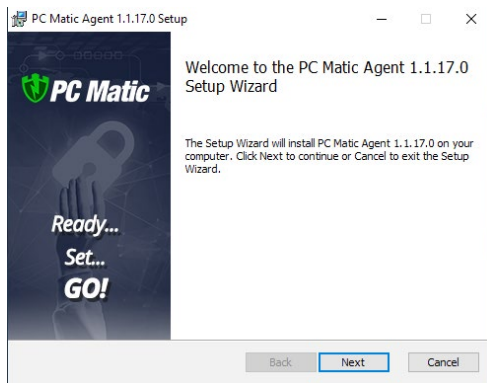
White labeling for your customer does come at an added cost compared to the normal MSP product. There is a one-time setup fee of **\$3,000.00** for the installer creation and two monthly fees costing \$0.10 per endpoint and a flat fee of \$50.00. We have outlined several pricing examples below for an endpoint count ranging from 5 to 100.

White Label Pricing Examples

Endpoint Number	MSP Price	Per Endpoint Fee	Flat Monthly Fee	Per Month Price
5	\$0.83	\$0.10	\$50.00	\$9.65
10	\$0.83	\$0.10	\$50.00	\$14.30
100	\$0.83	\$0.10	\$50.00	\$98.00

What Is Required?





1. Your Vendor and Product names.



PC Pitstop LLC

- These names will display in the Programs and Features list as well as installation directories.
2. A graphic for the side banner of the installer: 164px x 312px bmp format.
 3. A graphic for the top banner of the installer: 111px x 58px bmp format.
 4. An icon for the Programs and Features listing: 128px x 128px ico format.
 5. A logo for your management portal approximately 300px x 100px (Max height of 120px).

Where do I submit everything?

If you are currently working with a PC Matic sales representative you can provide the information requested to them once you have collected it all. You can also submit the requirements to our support team below and let them know you want to white label.

Email: business-support@pcmatic.com

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 add that application to the whitelist at your chosen level to avoid it being quarantined in the future.

Navigate to the individual computers page that had this file quarantined, or just one of them if there were several affected computers. Open the most recent scan, or the one that you believe

quarantined the application and click on the High Security Threat Test section. Once here, look for that application that was quarantined in the list, and click the “Add to Whitelist” button on the right side of the list. Make sure to select the level that you want to whitelist it at, MSP, customer, group, or individual computer.

If you believe the application was quarantined by SuperShield, allow it from the SuperShield Report by filtering for applications with a Bad status. Now, from the Actions section of the individual device page, scroll to the bottom and select Quarantined Files. 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 MSP 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 MSP 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. We accomplish this by only identifying a device by the name.

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.

Workspace Customizations

The management console workspace can now be customized for the preference of each user that logs in. From the sidebar, select Workspace at the bottom to access the customization settings.

Company Level Default - Default page when a customers page is accessed.

Devices	Blocked Status	EDR Status
Dashboard	Reports	
Notifications	Vulnerabilities	

Device Level Default - Default tab when a device page is accessed.

Notifications	Performance Trends
Maintenance Stats	Test History
Super Shield Report	Clean History

Account Level Default - Default tab when the MSP/Account page is accessed.

Notifications	Unassigned Computers
Reporting	Invoices

If you don't want to choose a default view, you can check the box to save the last active tab or page upon exit. This will keep your last view open when you return to the management console.

Beyond these customizations there are several other areas that will save your preferences while you use them. These will each save the last active state.

- **Options** - The options tab can also be saved to your preferred view on the customer, group or device page. If you leave it open it will stay that way for your login until you close it.
- **Device Filters** - The show/hide devices filter for computers, servers, and chromebooks will now remember your previous configuration.
- **Devices Tab** - On the customer or group page the devices tab will remember your preferred view of table or grid until you change it.
- **Device Gauges** - At the top of the device page when you either collapse or expand the device gauges, they will save to your user login. If you then visit another device it will load with your preferred view.
- **Device Actions** - The actions list on the device's page can be customized to maintain the order that you prefer. Use the handles on the left side of the list to drag and drop each action into the order that you prefer.

Color Schemes

You can also choose from custom color schemes for the accent colors in your management

console. Select the color you would like to use and save it to have that remain your preference no matter where you login. We will be adding more color options in the future.

PC Matic Ad Blockers

PC Matic MSP 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/9pddhxb4x8p6>

macOS Devices

PC Matic MSP is now available to protect your macOS devices. After the initial release, our support for macOS will continue to expand and include more features that you are familiar with on Windows devices.

To install, select Add a Device while in the Devices tab. Here you'll find a new tab labeled Mac Installer. At the bottom of the window, you can download the installer to run on each Mac device you wish to test on.

Note - Currently the Mac client does not restrict user interaction at the device. Each user will be able to change product settings within the status bar icon or uninstall the protection.

Installation

Begin the installation process just like any other install for PC Matic MSP - Select Options and



Install/Uninstall. Now choose the Mac Installer tab.

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 extension is critical for antivirus products and must be allowed for PC Matic to protect your device. Click Open Security Preferences in the prompt. (If you don't see this prompt, skip to step 12)
7. In the Security and Privacy window at the bottom you will see "System Software from Developer "PC Pitstop LLC" was blocked from loading". Click the allow button.
8. After you click allow the option will disappear and you can close the Security and Privacy window.
9. Once completed, click Close.
10. 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.
11. The console window will automatically open after install and can be closed.
12. Installation is complete!

System Extensions

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

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 to 'Allow' the blocked system software from PC Pitstop LLC. Click Allow.
6. 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.**

Shield Status

PC Matic Mac has several different shield status that are designated by the color of our shield in your Status Bar. If you hover over the shield icon, it will provide details on why it is in the current status unless it is green.

- Green Shield - Your Mac is currently protected and your account status is good.
- Yellow Shield - Your Mac is currently protected, but your account is expiring soon.
- Red Shield - Your protection is not active. Your account may be expired.

If you're unsure how to diagnose or fix a problem with a certain shield color, please check the Support section of this guide and contact our customer service team for assistance.

Local Device Options

After installing our macOS client, you'll notice a SuperShield icon in the Status bar of your Mac. Inside this SuperShield icon there are several options you can take advantage of right from the device. Currently, these options cannot be restricted but that option will be implemented in the next release.

- **Scan** - The scan option allows you to run an immediate manual scan on the device. This scan will automatically use the defaults for a PC Matic scan and when finished, the results will display inside your PC Matic MSP console.
- **Console** - The console of PC Matic Mac provides insight into what is attempting to run on your device. You can open and view the Console by selecting it in the menu. You should always see activity filling up the console, which means that SuperShield is monitoring everything and keeping you secure. If nothing is populating in the console, your account may be expired or you did not allow the system extension after install.
- **Web Portal** - The web portal option will open up a browser session to the PC Matic MSP management console. This is not automatically logged in, so normal users will not be able to access your console unless they know your login credentials or have their own.



- **Check for Updates** - PC Matic MSP for Mac automatically looks for updates for our software and applies them. However you can manually check for updates to ensure you are on the latest version.
- **Settings** - Inside settings you will have your main SuperShield Options. Here you can change the protection mode for SuperShield between whitelist mode (default) and blacklist mode. You can also adjust the notification setting for PC Matic to show the user display messages about blocked applications or allow them to Prompt for Override and locally allow or block an unknown application.
 - ◊ **Display** - The default notification setting is to have Display turned on. Display will simply show a standard Mac notification when SuperShield blocks and application on your device. No action can be taken from this notification.
 - ◊ **Prompt** - With prompt turned on, a large window will pop up on your device when SuperShield is going to block an application. Inside this window, you can select to block or allow the application once or always. This will locally whitelist or blacklist the application on your device.
 - ◊ **Blacklist** - The current default for SuperShield while our whitelist mode is beta testing. Blacklist mode protects your Mac using a blacklist of known bad applications.
 - ◊ **Whitelist** - The whitelist mode protects your Mac using a global whitelist of known good software and blocks all bad and unknown applications by default.
- **Troubleshooting/Help** - Quick links to our customer support team and product resources will reside here. This is also where the product can be uninstalled, however, you must login with your PC Matic MSP account credentials to confirm the uninstall.

Web Portal

All Mac devices will be located in the same management portal user interface you're familiar with for Windows devices and servers. You will see Mac device information integrated into several reports, Notifications, device lists, scheduled scans, blocked status, local whitelisting, and more. When drilled down to an individual Mac device, there are several actions you can take and realtime information you will receive.

- **Performance Gauges** - At the top of the web portal you will see several performance gauges, these give you a real time idea of the current performance on your Mac. In all cases, the higher the percentage, the harder your Mac is currently working and thus may be running slower.
- **Connection Icons** - On the upper right hand side of the portal, you will find several connection icons. The person icon signifies if you are currently connected to the internet. The computer icon signifies if the device you are currently viewing is connected to the internet. The last icon, for SuperShield, will show if your device is currently secured
- **Scans** - From the Actions list you can adjust Scan settings or review the most recent test.

Scan Now allows you to set up and run an immediate manual scan on a device that's online. Next Test will allow you to schedule a scan for your Mac on a daily, weekly or monthly basis. Last Test will open the report for the most recent scan that ran on your Mac to review any findings.

- **Quarantine Files** - The Quarantine Files section will contain any KNOWN BAD files that PC Matic has removed from your Mac. These files are known to be malware and have been cleaned from your machine. If you suspect any file has been mistakenly removed, please contact our support team for assistance.
- **SuperShield Report** - The SuperShield report will mirror the Console that you can review on your device from the Status Bar icon. This report shows every application that SuperShield is monitoring on your device and will also show any that have been blocked. Here you can locally whitelist an application for your mac devices by clicking the green button on the right side.
- **Test History** - All scans and cleans that have been run on your Mac will display here to review the results and see any changes that were made.

Live Scan Status

While a scan is running on your mac, a scan status will appear in the middle of the device page. You will also see a small 'eye' appear above the computer's connection icon on the device page. Once the scan completes the eye and the scan progress section will disappear and you can review the result in the Test History tab.

Uninstalling PC Matic Mac

You can uninstall PC Matic through the Status Bar icon. In order to complete the uninstall process, you will need your Administrator password, and PC Matic account credentials.

1. Navigate to the SuperShield icon in your Mac's Status Bar.
2. Select the icon and hover over Troubleshooting/Help at the bottom.
3. Select Uninstall from the list.
4. In order to uninstall you must confirm your PC Matic account details.
5. Once you enter your PC Matic account information and click Uninstall, the process will begin in the background.
6. You may be prompted for your Mac Administrator password, once you're done typing the password press enter.
7. The uninstall process will complete in the background and once done you will no longer see the SuperShield icon in the Status Bar.
8. Reboot your Mac to finish the full uninstall.

Uninstalling PC Matic MSP

PC Matic MSP 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 MSP on a device.

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

1. You can use the bulk uninstall option from the Devices tab by selecting devices on the left and choosing Remove Device.
 - This does not require a reboot of the device to complete, uninstalls everything in the background without user interaction.
 - Any devices that are offline will prompt you to decide to either queue them for an uninstall, which will happen when they regain connection, or delete the device from your account without an uninstall.

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

1. Navigate to the Network Devices area and use the same process to uninstall that was used to install the client.
 - This does not require a reboot of the machine and will uninstall without user interaction.

If the device won't connect to the PC Matic MSP console:

1. From the Customer's page Options > 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.

Support

To get support from our team you can open the help center, which will always be in the lower left hand corner of your portal. From here you have several methods to contact our team.

- Click the sales or technical icon: This will automatically fill out a form for you with your information and allow you to enter any questions and submit a ticket to our team for assistance.

- Email: business-support@pcmatic.com
- Phone: 1-855-855-1964
- Hours: 8:00AM - 9:00PM ET (M-F)

Unsupported Operating Systems

Windows XP and Windows Vista are operating systems that are no longer fully supported by Microsoft and cannot be fully supported by PC Matic MSP. 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.

This means that you will lose abilities in the web console such as: 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. Endpoint Uninstaller Fails

- If you have downloaded the endpoint uninstaller to remove PC Matic MSP 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.

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 MSP compatible with servers?

Yes, Server Security 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 the correct product.

3. Do you have a management console?

Yes, PC Matic MSP 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 customers and their computers and take any actions necessary.

4. How do you deal with false positives?

You have the ability to whitelist any application that is being blocked from the cloud console. This is a flexible local whitelist 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 whitelist which is pushed out to all customers. This removes the normal overhead associated with a whitelist 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 MSP 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 whitelist 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 MSP 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. If you would like to read our full guide on Best Practices, click [here](#).

9. Will your product automatically remove my previous antivirus?

PC Matic MSP 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 MSP also installed on it. This feature requires the install on both ends so they can communicate securely between themselves.

13. Can I run another Antivirus program alongside PC Matic MSP?

We do not recommend running two antivirus programs at the same time. This is not a unique opinion, as many in the industry recommend running one solution at a time. If both programs are running real time protection, it can cause them to conflict over file access, permissions, etc. and may lead to both functioning improperly.

14. Will my Images, Documents, PDFs, etc. be stopped by PC Matic because they’re not on the whitelist?

No. PC Matic MSP’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!

15. How long do I wait after locally whitelisting an application before my computers will be able to run it?

Adding an item to your local whitelist will immediately sync it down to every device in the level you have whitelisted that application for. This often takes less than 1 second after you have clicked save inside your web portal.

16. 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).

18. How can I add additional licenses?

You can add computers at any time within your MSP account for your customers old and new. At the end of the month we'll tally up your amount used and bill you for it. This gives you flexibility to adapt to customer needs quickly.

19. How is the billing handled for PC Matic MSP?

PC Matic MSP uses a flexible monthly billing structure. This allows you to add and remove endpoints as you need to for new, old, and existing customers. At the end of the month we'll tally up your endpoints and servers and bill you \$0.83 per endpoint and \$1.66 per server. You then take care of the billing for your customers, charging them whatever you see fit for your services.

20. 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.