# Table of Contents

**Account Structure**
- Groups 1
- Device Organization 1

**Implementation**
- Previous AV Removal 1
- Configurations 1
- Diagnostic Mode 2
- Timing 3

**SuperShield Settings** 4

**Whitelisting Mechanism** 5

**Scan Recommendations**
- Configurations 6
- Scan Frequency 7

**Base Alert Notifications** 8

**Security Practices** 8

**Support** 9
Account Structure

The way you initially set up your account can keep the initial deployment process very smooth and limit work you may need to do in the future. Creating groups, organizing our devices, and setting policies are all great ways to get our account started.

Groups

Enabling groups before beginning your deployment can make it easier to organize all of your devices in one fluid motion. With the groups created, you’ll be able to make unique installers and rollout for each group. Groups aren’t required but we recommend them for breaking out devices and enforcing policies.

Device Organization

Even with groups enabled if you have multiple types of devices in the same group there may be individual options available to specific devices. For example, if you create a scheduled scan for a group which has servers and computers in it, the servers will still not take part in the driver updates, patch management, or full performance suite just like if you scheduled and individual scan from a server page.

Implementation

There are several methods to complete the rollout of PC Matic Pro and the best choice will vary by environment. Here we will focus on configurations, timing, and diagnostic modes for the implementation, all of which will apply no matter the method you choose to deploy.

Previous AV Removal

Before we start our configurations, or rollout it is important to remove the previous antivirus that was in use. Running two realtime protection programs could cause conflict between them or improper functions. This can also lead to decreased performance of the device. The PC Matic Pro installer will attempt to remove any antivirus currently installed, however it is often unsuccessful uninstalling enterprise level software.

Configurations

SuperShield - *(Default: On / Recommendation: On)*

- Nothing to adjust here, SuperShield is a critical component of our security providing the
default deny realtime protection.

Remote Desktop - *(Default: On | Recommendation: On)*
- Installing the VNC client initially will allow easy access into all of your devices from anywhere.

Ad Blocker - *(Default: Off | Recommendation: On)*
- Installing the PC Matic adblockers for Chrome, Firefox, Edge, and Internet Explorer.

Disable User Control - *(Default: On | Recommendation: On)*
- After initial rollout, you can adjust specific devices to turn this setting off and give escalated privileges.

Enable Java - *(Default: Off | Recommendation: Off)*
- Allow or block all Java activity through SuperShield. Blocking all Java activity can increase your security posture.

Device/USB Control - *(Default: Off | Recommendation: Off)*
- Enabling USB Control will block removable USB storage devices and SD cards from being accessible.

Vulnerability Protection - *(Default: Automatic | Recommendation: Automatic)*
- Updates third party applications through SuperShield according to your settings in Software Management.

Block Notification Method - *(Default: Display Only | Recommendation: Display Only)*
- Control what’s visible and accessible to the end user when an application is blocked by SuperShield.

Group - *(Default: Unassigned | Recommendation: Group Selected)*
- Depending on your rollout strategy, selecting your groups in the installer will save you work down the road as they will arrive in the console preorganized.
Diagnostics

Diagnostic Scan - Running the first scan on your initial deployment in diagnostic mode will help uncover any coming changes before they happen. It’s highly recommended you utilize this feature before running automatic scheduled scan and cleans. *(Can be enabled at the top of your scan configuration window)*

Timing

Rolling out across your environments works best in stages. We recommend beginning with the Diagnostic/Onboarding stage, and then moving into your Environment based stages.

Diagnostic Stage - During the diagnostic phase we should be deploying out to a small group of devices and taking advantage of the Diagnostic mode for your scans. A good rule of thumb for this rollout is to deploy out onto devices that you know are running a majority of the software used in your environment.

Oboarding Stage - While you have deployed out to a subset of devices, our onboarding team will be in contact to work with you individually and make sure that any unique software is being whitelisted or assist with installations in your environment.

Environmental Stage - This will vary by size and composition of your environment but after the diagnostic stage has completed you can begin full scale rollout. Breaking it up by locations, departments, groupings, etc. may make your rollout smoother and easier to manage.
SuperShield Settings

The SuperShield Options contain several security settings as well as privileges you can assign out at various levels. It’s critical to understand these settings and keep them correctly configured for optimal security.

Protection Level - *(Default: SuperShield Protection | Recommendation: SuperShield Protection)*

- Protection level is this most critical setting to maintain your security. SuperShield protection should always be enabled as the blacklist only mode will suffer against unknown malware.

Vulnerability Protection - *(Default: Automatic | Recommendation: Automatic)*

- The automatic setting ensures that even if a scheduled scan doesn’t run third party applications will still be patched. Turning this off or to prompt could leave gaps in security.

Device Control - *(Default: Off | Recommendation: Varies)*

- Device Control can be turned on for individual groups or other levels for added security against removable USB storage devices copying or transferring data. Its primary use is for data protection against physical theft.

Block Notification Method - *(Default: Display Only | Recommendation: Display Only)*

- Keeping this setting on the default will allow your users to be informed when SuperShield has blocked something but not allow them to take an action on it. It’s important to understand that the Prompt for Override mode will let anyone on that device override a blocked application and allow it to run.

Disable User Control - *(Default: On | Recommendation: On)*

- Setting a base policy for the entire company here will be a great way to ensure users can’t override the protection in any way from their device. As devices inherit their policies from the lowest level, you can then give a group of admins or individual device higher privileges by turning this off if necessary.

Enable Java - *(Default: Off | Recommendation: Off)*

- SuperShield now blocks all Java activity by default on each machine to thwart a new style of malware that capitalizes on Java being present and functioning. Our recommendation is to leave this setting turned Off so that Java is not allowed. If you need to use Java, enable it individually on those devices.
Whitelisting Mechanism

After installing SuperShield, the best mechanism to whitelist an application before full deployment is from the Blocked Status report. Access the Blocked Status tab from your sidebar. This report shows blocked applications in your environment immediately and filters to unknown applications by default.

1. When the report opens you’ll see applications that are unknown to our research team still. These are automatically going through our categorization process but can be locally whitelisted as well.
2. To whitelist an application, find it in the list and navigate to the Actions menu along the right side.
3. From the actions menu select ‘Add to Whitelist’.
4. Now choose the level you want to whitelist at, device, group or entire organization and click save. This now updates to all devices you added it for and with a few minutes each device should be able to run that application.
Scan Recommendations

Setting up scheduled scans within PC Matic Pro will allow you to sit back and let us take care of the work, but in this section we’ll cover how to configure the scan options and how often you should be scanning.

Configurations

Recommended Daily or Weekly Scan Settings

<table>
<thead>
<tr>
<th>Security</th>
<th>Malware Scan:</th>
<th>Quick</th>
<th>Malware Clean:</th>
<th>Clean BHOs:</th>
<th>Viruses and Pests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan BHOs:</td>
<td>ON</td>
<td></td>
<td>ON</td>
<td></td>
<td>ON</td>
</tr>
</tbody>
</table>

Patch Management

<table>
<thead>
<tr>
<th>Security</th>
<th>Scan Vulnerable Apps:</th>
<th>ON</th>
<th>Update Vulnerable Apps:</th>
<th>ON</th>
</tr>
</thead>
</table>

Driver Updates

<table>
<thead>
<tr>
<th>Security</th>
<th>Scan Drivers:</th>
<th>ON</th>
<th>Update Drivers:</th>
<th>ON</th>
</tr>
</thead>
</table>

Performance

<table>
<thead>
<tr>
<th>Security</th>
<th>Scan Hard Drives:</th>
<th>ON</th>
<th>Disk Optimization:</th>
<th>Partial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan System Restore Points:</td>
<td>ON</td>
<td></td>
<td>Optimize System Restore Points:</td>
<td>ON</td>
</tr>
<tr>
<td>Scan Junk Files:</td>
<td>ON</td>
<td></td>
<td>Clean Junk Files:</td>
<td>ON</td>
</tr>
<tr>
<td>Scan Registry:</td>
<td>ON</td>
<td></td>
<td>Apply Registry Fixes:</td>
<td>ON</td>
</tr>
<tr>
<td>Scan Internet Settings:</td>
<td>ON</td>
<td></td>
<td>Optimize Internet Settings:</td>
<td>ON</td>
</tr>
<tr>
<td>Scan Performance Tweaks:</td>
<td>ON</td>
<td></td>
<td>Apply Performance Tweaks:</td>
<td>ON</td>
</tr>
<tr>
<td>Scan Services:</td>
<td>ON</td>
<td></td>
<td>Optimize Services:</td>
<td>ON</td>
</tr>
<tr>
<td>Scan Scheduled Tasks:</td>
<td>ON</td>
<td></td>
<td>Optimize Scheduled Tasks:</td>
<td>ON</td>
</tr>
<tr>
<td>Scan Startup Programs:</td>
<td>ON</td>
<td></td>
<td>Optimize Startup Programs:</td>
<td>ON</td>
</tr>
<tr>
<td>Informational Sections:</td>
<td>ON</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Recommended Monthly Scan Settings

<table>
<thead>
<tr>
<th>Security</th>
<th>Malware Scan:</th>
<th>Full</th>
<th>Malware Clean:</th>
<th>Viruses and Pests</th>
</tr>
</thead>
</table>

PC Matic PRO
Scan Frequency

Timing of scans will vary slightly depending on each environment so you will need to decide the best time to run your scheduled scans during the day. If computers are online 24/7 running scans in the off hours would be optimal.

Daily Quick Scans

- Running a quick scan on a daily basis is the most recommended option. With scans running during off hours this gives you a great way to keep each device cleaned, optimized, and secure. The daily scans will ensure that any malware sitting on a device is removed quickly, even though it is not allowed to execute quarantining it quickly is optimal.

Weekly Quick Scans

- If daily quick scans are not feasible you can run them on a weekly basis. This will sufficiently keep machines cleaned and optimized without letting bad software sit around on devices for a long amount of time.
Monthly Full Scans

- Full scans are very taxing on the machine and can sometimes take up to an hour to run. The scan looks very deep at every file, and should include a full disk defrag. With their long duration, running a full scan once a month on an off day is the most recommended approach. It can be combined with the weekly or daily quick scans.

Base Alert Notifications

Configuring alert notifications to come in over email or SMS can vary widely on your environment and need for alerts. However, our recommendation for alert notifications is to at least set up the base laid out below, and expand on it per your needs.

SuperShield Status Change

Configuring an alert notification for SuperShield Status Change with a frequency of 24 hours will give you one daily email report with alerts. This is the most important alert to receive and act on because if SuperShield is disabled for any reason it may mean your device is no longer protected and is vulnerable to threats.

Be sure to set up this alert at your Company level so that any machines with a change in SuperShield status will appear in the alert notification.

Application Blocked by SuperShield

Setting up an alert notification for when an application is blocked by SuperShield allows you to easily stay on top of any false positives on your account in the early stages. You can quickly go from your email to locally whitelisting a file for an employee.

Security Practices

There are best practices that you can implement in addition to our product’s settings to ensure a secure environment. Below you’ll find some actions within our product you can take to ensure a good security posture.

Remote Desktop Protocol

RDP can often be a crucial tool in the IT team’s tool belt, however it can also present a gaping vulnerability in your environment if not set up properly. Many environments don’t even realize
they have RDP enabled and publicly available. This presents a hole that cyber criminals commonly exploit to take control of a machine and manually turn off the security that is present and install ransomware.

Disabling RDP - Within PC Matic Pro you can now disable RDP on any computer from your management console. At the device’s page you’ll now find Remote Desktop Protocol in the Actions section. If RDP is currently enabled you will only see the disable button, and you can immediately close this security hole.

Support

To get support from our team, you can open the help center, which will always be in the lower right 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: 1-844-235-3301
- Hours: 8:00AM - 9:00PM ET (M-F)