Best Practices

January 2023

Copyright © 2022 PC Matic, Inc.

Table of Contents

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.

Configurations

Remote Access - *(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.

System Tray Menu - *(Default: Disabled | Recommendation: Disabled)*

- After initial rollout, you can adjust specific devices to enable this setting and give escalated privileges.

Java Runtime - *(Default: Block | Recommendation: Block)*

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

Removable Storage Devices - *(Default: Allow | Recommendation: Allow)*

- Selecting Block will block removable USB storage devices and SD cards from being accessible.

Patch Management - *(Default: Enabled | Recommendation: Enabled)*

- Updates third party applications through SuperShield according to your settings in Software Management.

Block File Notification - *(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.

Timing

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

Oboarding Stage - While you have deployed out to a subset of devices, our onboarding team will be in contact to work with you indvidiually 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 Mode - *(Default: SuperShield Protection | Recommendation: SuperShield Protection)*

- Protection level is this most critical setting to maintain your security. SuperShield protection should always be enabled.

Patch Management - *(Default: Enabled | Recommendation: Enabled)*

- 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.

Removable Storage Devices - *(Default: Allow | Recommendation: Varies)*

- USB Device 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.

Blocked File Notification - *(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.

System Tray Menu - *(Default: Disabled | Recommendation: Disabled)*

- 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 enabling if necessary.

Java Runtime - *(Default: Block | Recommendation: Block)*

- 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.

Allow Listing Mechanism

After installing SuperShield, the best mechanism to allow an application before full deployment is from the Process Activity report. This report shows all processes that SuperShield is monitoring or blocking.

1. Filter the report by Recent Processes Blocked
2. Select a process that you know needs to run in your environment and add it to your local allow list.

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.

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.

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)