PC Matic MSP

Quick Start Guide

August 2018

Create Your Structure

To start things off in your new management console, lets build the frame for your account and setup your customers, groups and additional users. Click the settings gear to navigate away from the main page, to your MSP page.

- Expand the Options panel, and open the Account Setup Dropdown.
- Select Edit Groups to configure your initial groups. You can add groups here to use with any of your customers.
- Lets create a few groups that will tackle departments, locations, or any way you want to segment a customer's devices. (Sales, HR, Accounting, Building #7, etc.) Also create a Test Group which we'll use during implementation.
- Now open Account Setup again and select Add a Customer, lets create your first or test customer. Check the Use Groups checkbox and assign groups to this customer at the bottom. Make sure to add in the Test Group.
- Open Account Setup again and select Manage Users.
- Now you can create user accounts for the rest of your team/staff that needs access to manage devices.

Initial Implementation

Before our rollout begins for the test devices, lets set the testing permissions for our group. From your first Customer's page, use the filter by group dropdown and select your test group. Now expand the Options panel and open Super Shield Options. Set the Block Notification Method dropdown to Diagnostic mode and Save.

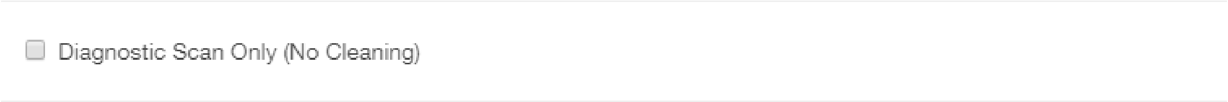
Remaining in your test group, open the Installer Downloads panel, the group dropdown should still be set to your test group. You can also check the Diagnostic Mode Preset to automatically make this installer put Super Shield in Diagnostic Mode. With the other default options checked, use download at the bottom to get the installer file for your testing machines.

Ideally you should test on 1-5 devices depending on the size and variety of your environments. Try to choose a few devices from different locations/departments.

Run the installer on each test machine so we can begin our audit phase while configuring the rest of our account. You should see each device arrive in the test group in your management console.

Learning Phase

During the learning phase we will be monitoring two separate areas to make sure PC Matic MSP is configured properly before doing a full deployment. This will start with scans and cleans. For your test group, set up either a manual scan for each device or a scheduled scan for the whole group at once. During the setup process for your scans enable the Diagnostic Scan Only checkbox at the top. This will ensure we’re doing a ‘read-only’ scan and not making changes.



☐ Diagnostic Scan Only (No Cleaning)

After the diagnostic scan runs for each device, visit the Test History tab and click on the date to open the report for that scan. Within this report, open any section without a green icon to view the recommended changes, or open the advice summary at the top. From within each section you can override the decision, for example if a Service will be optimized you can add that service to the whitelist for any level you choose so it will not be optimized.

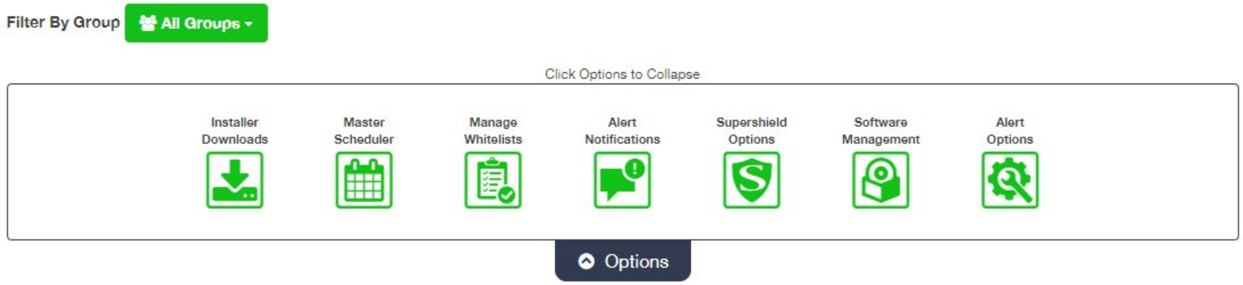
Super Shield Diagnostic

With Super Shield in diagnostic mode on our test machines, we’re looking for any unique or proprietary software that has not been seen by our software before, but is something known good. To find this, we’ll let Super Shield run for about 24 hours during a normal workflow. Then, navigate to that devices page and open the Super Shield Report. Expand the filters and change the Current Status Dropdown to Unknown. Apply the filter.

Now, we can look through any applications in the list filtered for unknowns. If any software appears to be something you use for normal business operations, you can click the green icon on the right side to add that application to any level of your whitelist. We recommend adding everything at either the Entire Account (MSP) level or Company level. Entire Account ensures that all customers will be allowed to run that software, while Customer will cover all devices that customer has.

Final Policy Configuration

Now that you've finished the diagnostic modes, you can jump back and complete the policy configuration and settings for each of your other groups before deployment. Be sure to set your Super Shield Options, any Alert Notifications, Patch Management Version Control, and Alert Options. Each of these can be configured after the devices are installed, but having them pre-configured can save you some time down the road!


Filter By Group
All Groups
Click Options to Collapse
Installer Downloads
Master Scheduler
Manage Whitelists
Alert Notifications
Supershield Options
Software Management
Alert Options
Options