



---

Quick Start Guide  
March 2020

# 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 Account Details in the sidebar menu to navigate away from the main page, to your MSP page.

- Expand the Account Options, and open Edit Groups.
- Within Edit Groups you can configure your initial groups. These groups can be used 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 Options 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 Options 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 Implemtation

---

SuperShield's protection takes a default-deny approach based on our global whitelist. It is possible that during initial implementation you will see unique applications you use blocked as unknown. This is normal. We do strongly recommend that you contact our Onboarding Team before beginning your installations.

- [onboarding@pcmatic.com](mailto:onboarding@pcmatic.com)

Ideally you should test on 1-5 devices depending on the size and variety of your environment. Try to choose a few devices from different locations/departments. This will allow us to see all of the unique software you are using and let our onboarding team assist in expediting the whitelisting process to keep your install smooth.

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 your management console after installation.


# Installer Configurations


To access and configure the installer for your initial installs, navigate to the sidebar and expand the Options section. Select Install/Uninstall from the top of the list. Below you'll find the recommended settings for the installer, after configuring these you can click download at the bottom and run the installer file on each machine. It is important to note: Do not change the name on the installer file. It contains unique details for that installer configuration and your account.


Which add-ons do you want installed?


Supershield   Remote Desktop   Ad Blocker 

## Supershield Options


**Disable User Control** 

**Enable Java** 

**Device/USB Control** 

**Vulnerability Protection** 

Automatic (recommended) ▼

**Block Notification Method** 

Display Only (recommended) ▼

# Diagnostic Scan

After installation, you can run a diagnostic scan on each machine to review changes that our product is proposing before they automatically happen. To initiate a diagnostic scan, navigate to that device's page by clicking on the device name. Once on the device's page, select the Scan action from the list. Now to the right you can select the Scan Now option to configure an immediate manual scan.

At the top of the scan window, select the Diagnostic Scan Only checkbox. Now scroll to the bottom and click save. Once the scan finishes, you can review the scan report from the Test History tab.

Diagnostic Scan Only (No Cleaning)