



Optimal System Requirements

The operating systems below support the best overall security posture for your devices and our product. On Windows endpoints and servers this includes the ELAM (Early Launch Anti-Malware) Driver that lets SuperShield run as a protected process. This prevents end users from disabling, uninstalling, or restarting the protection service.

- Endpoint Operating System: Windows 10 (1703) - Windows 11
- Server Operating System: Windows Server 2016 (1703) - Windows Server 2022
- Mac Operating System: macOS Monterey, Big Sur, Catalina
- Processor: 1 GHz or faster | Memory: 8 GB | Hard Disk: 50 GB of free space
- Active Internet Connection
- .net Framework 3.5 [[Download](#)]
- Current SuperShield Version: 3.0.44.0
- Current Mac Version: 1.0.24 (Build 196.96)

Minimum System Requirements

- Endpoint Operating System: Windows 7 - Windows 8.
- Server Operating System: Windows Server 2008 R2 - Windows Server 2016 (.)
- Mac Operating System: macOS Mojave, High Sierra, Sierra
- Processor: 1 GHz or faster | Memory: 2 GB | Hard Disk: 5 GB of free space
- Active Internet Connection
- .net Framework 3.5 [[Download](#)]

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 Essential Endpoint Protection. It is possible to install our real-time protection SuperShield on a device running Vista or XP, however there will be many features missing. All remote control or real-time controls from the web console will not be functional. Any statuses you typically see from a machine in real-time will show in a yellow or unsure status indefinitely.

This means that you will lose abilities in the web console including but not limited to:

- Current Connection Status
- Current Protection Status
- Quarantine Restore
- Command Prompt
- File Manager
- Immediate Scans

- VNC Access
- Remote Reboot/Shutdown

Installation

Before downloading the endpoint installers for your Essential Endpoint Protection 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.

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

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

The screenshot shows the 'Windows Installer' tab selected in the top navigation bar. Below the tabs, there is an 'IMPORTANT' warning box. The main content area is titled 'Endpoint software for Windows' and includes instructions for installation. Below this, there is a section for 'Which add-ons do you want installed?' with radio buttons for 'Remote Access' (selected) and 'Ad Blocker'. The 'SuperShield Options' section contains several dropdown menus: 'System Tray Menu' (Disabled (Recommended)), 'Removable Storage Devices' (Block), 'Blocked File Notification' (Display Only (Recommended)), 'Java Runtime' (Block), 'Patch Management' (Enabled (Automatic)), 'Windows Defender' (Allow), 'Customer to put computer under' (Corporate Technology Advisors), and 'Group' (*Default Group*). At the bottom, there is an 'Installer Distribution' section with an 'Enter email address' field, an 'Email Installer' button, and an 'Installer Download' link. A 'View Minimum System Requirements' link is also present. A 'Download' button is located at the bottom right of the page.

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.

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 Essential Endpoint Protection'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 setup as an administrator of multiple organizations, 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.

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 Essential Endpoint Protection 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://support.pcmatic.info/files/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 like the one below.
 - a. 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.
 4. After the script finishes running, you should see an output like the one below.
 - a. VERBOSE: Checking the .Net Framework Requirement
 - b. VERBOSE: Result: Meets Minimum .Net Requirement - .Net Version 4.7.2 Found
 - c. VERBOSE: Checking version of PowerShell
 - d. VERBOSE: Result: Meets Minimum PowerShell Version - 4.0 Found
 - e. VERBOSE: Checking Execution Policy
 - f. VERBOSE: Result: Execution Policy is set to Unrestricted
 - g. VERBOSE: All the Minimum Requirements Have Been Met

Now if you did not meet all 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 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.

[Windows Installer](#) [Mac Installer](#) [Device Manager Installer](#) [Windows Uninstaller](#)

Device Manager used for push installs/uninstalls (*requires remote powershell access)

This Installer is used to enable the ability to do push installs/uninstalls to devices on either an Active Directory or workgroup network. Download the installer and install on your domain controller. This software requires remote powershell scripting to be enabled on each endpoint.

Download this Windows Powershell script to check your system for the minimum requirements, Instructional ReadMe File is included in the zip file

Script Download: [Zip File](#)

Options

☒ Create Remote PowerShell GPO

Customer to put computer under

Corporate Technology Advisors

Customer Group to put computer under

"Default Group"

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

Nickname

Username

Username

Confirm Username

Confirm Username

Domain

Domain

Password

Password

Confirm Password

Confirm Password

⚠ Do not alter the Installer Download URL or the downloaded file name. This will cause issues with installation.

Download

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 console. When you enter that area, you should begin to see the devices from your network populating into the Devices tab.

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 Scheduling service. On the right side, it should show the “Log On As” value as your Admin account that you entered 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 endpoint 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-GPUpdate -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:\gpresult.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 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 number 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 its system tray.

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, choose Add a Device from the devices list and click the Device Manager Tab. Device Manager is in the second tab of the popup window. Within the device manager installer, you have several options that can be configured.

Windows Installer

Mac Installer

Device Manager Installer

Windows Uninstaller

Device Manager used for push installs/uninstalls (*requires remote powershell access)

This Installer is used to enable the ability to do push installs/uninstalls to devices on either an Active Directory or workgroup network. Download the installer and install on your domain controller. This software requires remote powershell scripting to be enabled on each endpoint.

Download this Windows Powershell script to check your system for the minimum requirements, Instructional ReadMe File is included in the zip file

Script Download: [Zip File](#)

Options

Create Remote PowerShell GPO

Customer to put computer under

Corporate Technology Advisors

Customer Group to put computer under

Default Group

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

Nickname

Domain

Domain

Username

Username

Password

Password

Confirm Username

Confirm Username

Confirm Password

Confirm Password

⚠ Do not alter the Installer Download URL or the downloaded file name. This will cause issues with installation.

Download

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. 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.

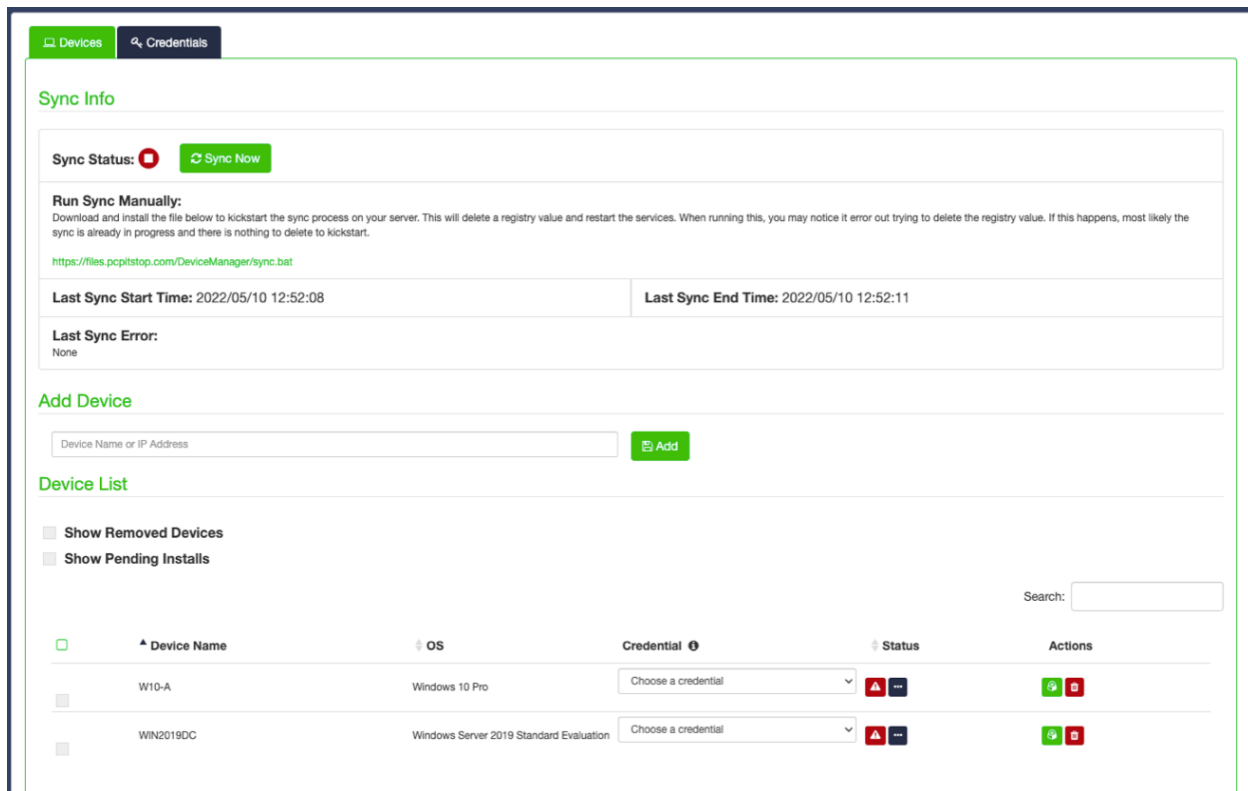
After you configure your options, choose the download button to download the executable. This will need to be run on your domain controller to install the device manager and configure the GPO if you selected that option.

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 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 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
 1. Select individual devices or all devices to view bulk options for Install, Uninstall, Credential Set, and Removal.
2. Endpoint Status
 1. Installed: Essential Endpoint Protection is currently installed on the endpoint.
 2. Uninstalled: Essential Endpoint Protection is currently not installed on the endpoint.
 3. Pending Install: Essential Endpoint Protection will be installed on the endpoint when the scheduler service on the server runs (1 hour max).
 4. Pending Uninstall: Essential Endpoint Protection will be uninstalled on the endpoint when the scheduler service on the server runs (1 hour max).
3. Endpoint Details
 1. Displays information about the endpoints AD network, as well as current PC Matic configurations after installation.
4. Install/Uninstall Endpoint Software
 1. Green Icon: Push installation to the endpoint.
 2. Red Icon: Pull (uninstall) client from the endpoint.
5. Remove From Account

1. 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.

Devices

Credentials

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.

*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.

Add New Credential

☐ Use To Run Device Manager Service (Domain Administrator Recommended)

Nickname

Nickname

Username

Username

Confirm Username

Confirm Username

Domain

Domain

Password

Password

Confirm Password

Confirm Password

Save

Credentials

	Nickname	Domain	Username	Create Date	Update Date	
✓	administrator	pcpitstop.com	administrator	2022/05/10	2022/05/10	 

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 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 its 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>

Uninstalling Essential Endpoint Protection – Windows

Essential Endpoint Protection 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 from a Windows device.

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

1. You can use the bulk uninstall option from the **Devices** tab by selected 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 web console:

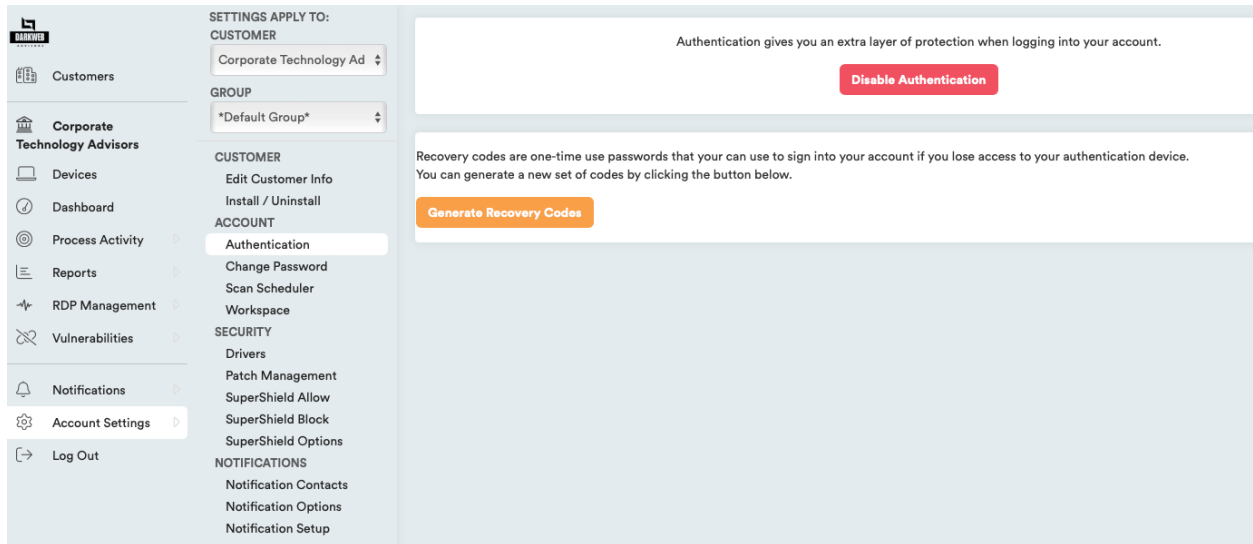
1. From **Options > Install/Uninstall > Endpoint Uninstaller** download the uninstaller .zip folder to the computer you wish to uninstall on.
2. Right-click and extract the .zip folder that you downloaded.
3. Inside the folder you will find an uninstaller executable and batch (.bat) file that contains unique details for your account.
4. Right-click the .bat file and select "Run as Administrator."
5. The uninstall is now complete.

Authentication

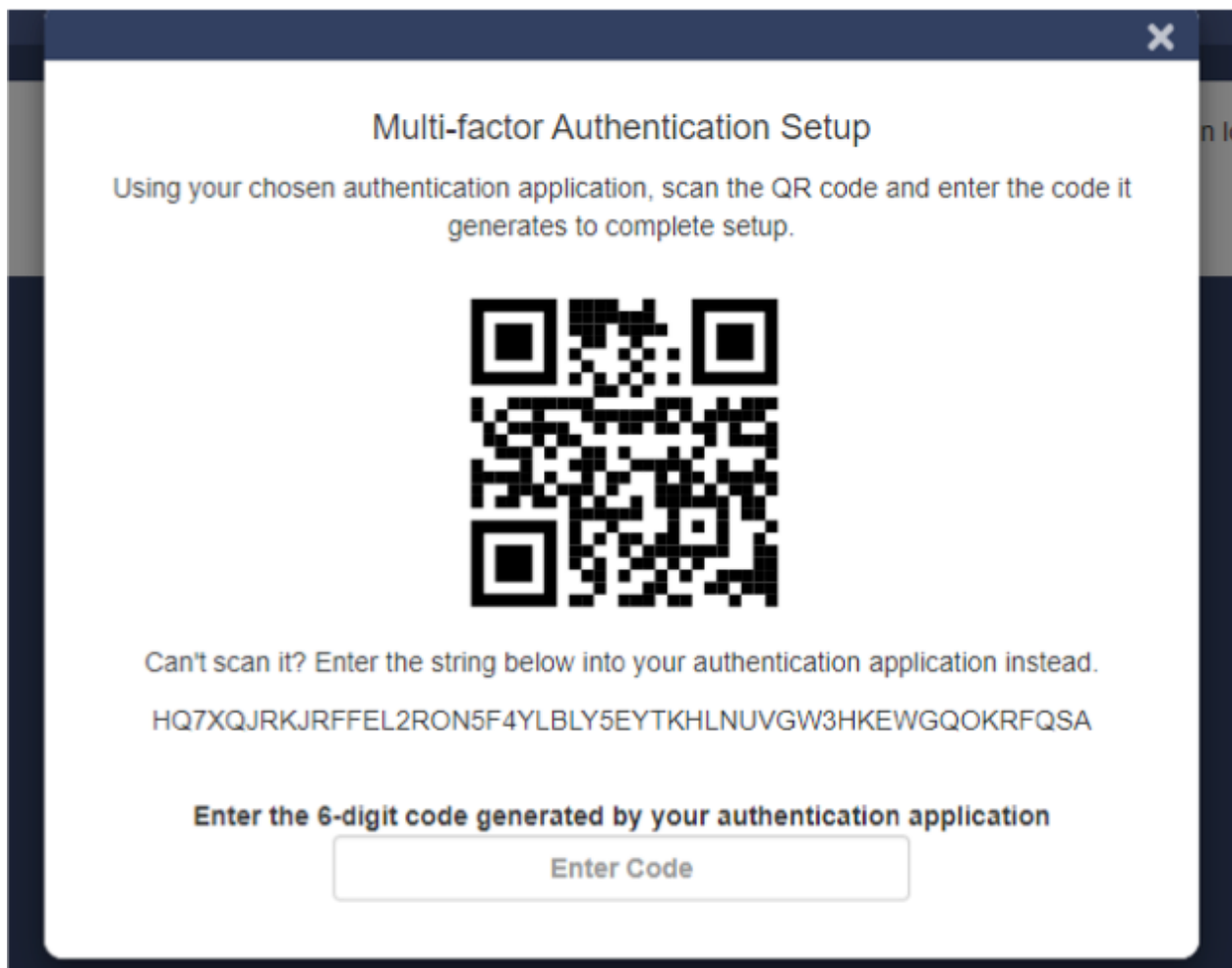
Each user of the web portal can enable multifactor authentication. Once enabled, authentication requires a 6-digit code generated by a mobile app (iOS or Android) to log in to the web portal. *Suggested authenticator apps: Google Authenticator, Microsoft Authenticator, Twilio Authy, LastPass, OneAuth, FreeOTP, and OTP, 2FAS.*

Enabling Authentication

MFA Authentication is enabled for all accounts. The configuration for this is under **Account Settings** on the **Authentication** page.

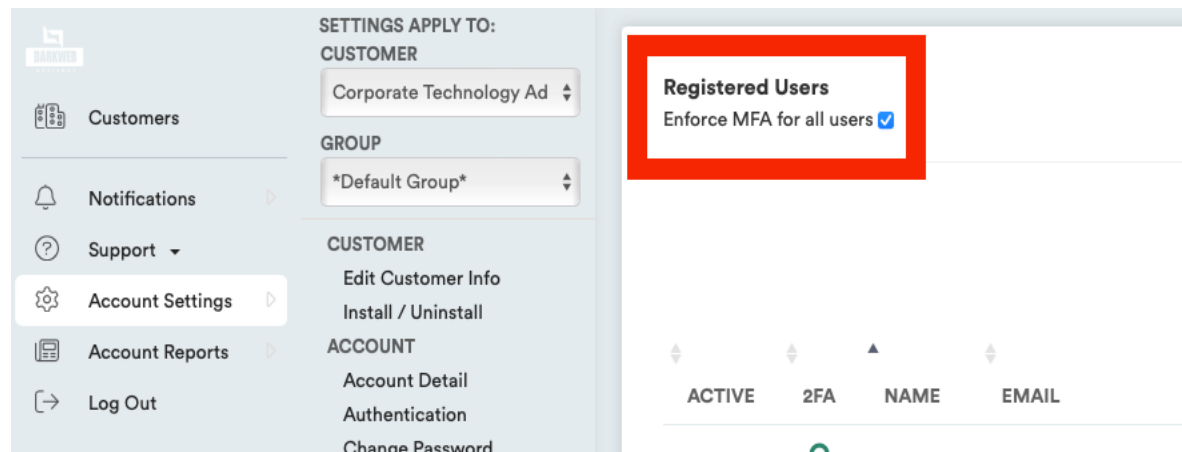


The user will be prompted to scan a QR code using their chosen authenticator app. The app will generate a 6-digit code. Enter the 6-digit code in the field.



Enforce Authentication

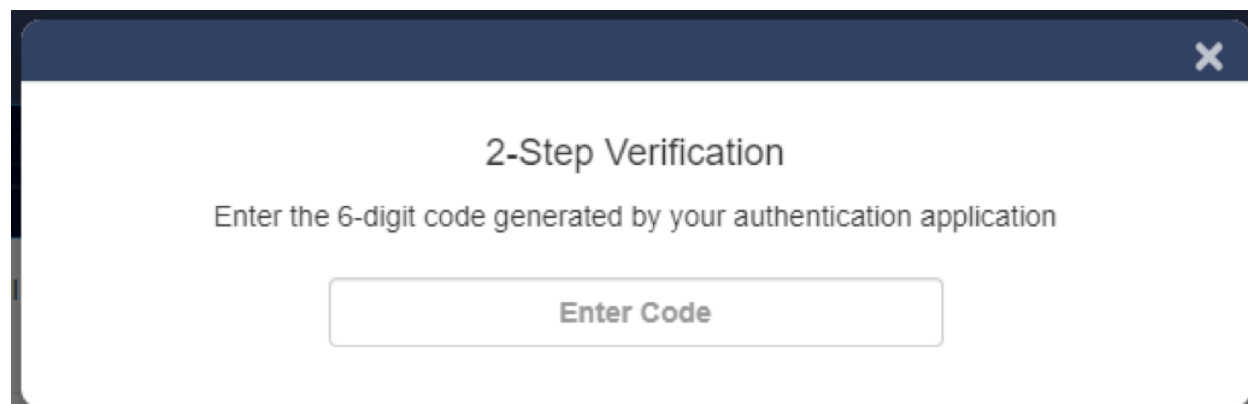
Administrators can require all users to setup and use multifactor authentication on their account by going to **Account Settings > User Management** and toggling the **Enforce MFA for all users** option on.



The next time a user logs in they will be prompted to setup multifactor authentication if they don't already have it enabled.

Using Authentication

Once enabled, after a user successfully enters their email address and password to login, they will be prompted to enter the 6-digit code generated by their authenticator application.



Remote Uninstall – Device Manager

If your initial install process was done using the Device Manager component of Essential Endpoint Protection, then you can remotely uninstall the product in full using a similar process to the install. Navigate to the home 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.

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 Essential Endpoint Protection 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.

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 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.

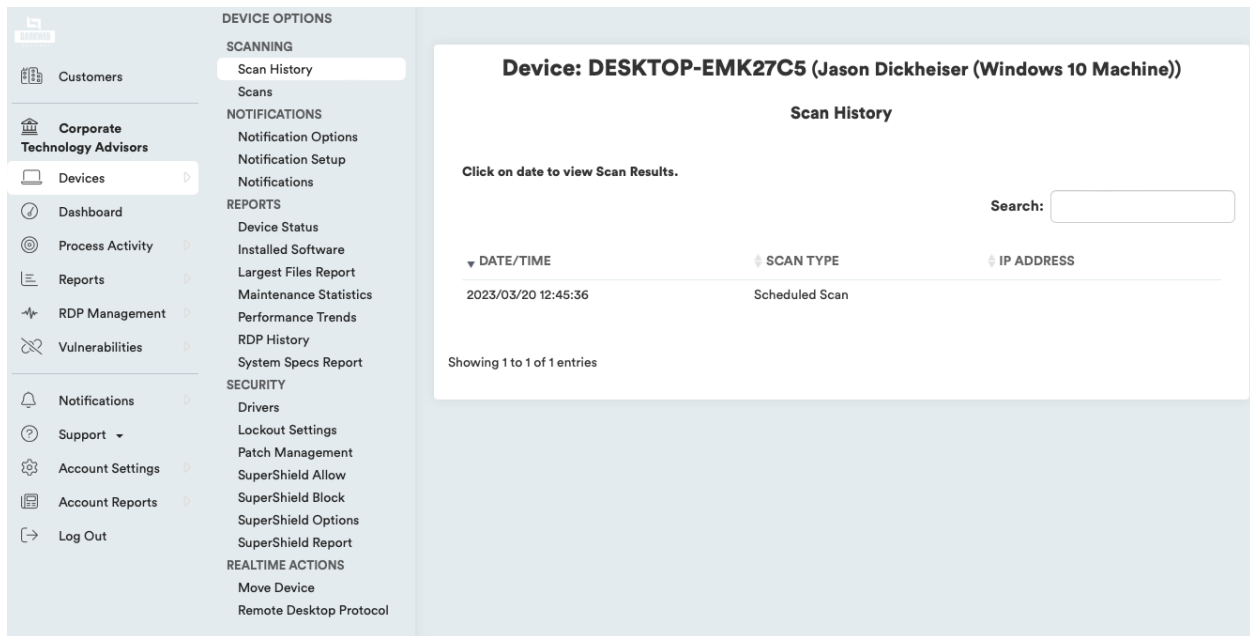
Refined Product Capabilities

Having a product that can protect 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.

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, 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

Essential Endpoint Protection 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 Essential Endpoint Protection 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 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.

Ad Blockers

Essential Endpoint Protection 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 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 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/okmhneofinpilciglijihehjpaeledb>

Edge - <https://www.microsoft.com/en-us/p/pcmatic-for-edge/9pddhxb4x8p6>

macOS Devices

Begin the installation process just like any other install for PC Matic MSP: Select Add a Device from your Devices tab inside a customer. 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 Essential Endpoint Protection 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 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 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, require access to the kernel to protect the device. This requires additional steps of allowing the system extension to function properly.

In macOS 10.13.2 - 10.14.6, 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.
 1. `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 Matic Tray. Click Allow.
6. Reboot your machine.

Shield Status

Essential Endpoint Protection Mac has different shield statuses 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 status unless it is green.

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

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 may be several options you can take advantage of right from the device. These options can be restricted by changing the same setting as your windows machines in the management console (SuperShield Options > System Tray Menu > Disabled). When restricted, you will only see the 'About' option on the device to check your version number. When unrestricted you will see all the options below.

- **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 Essential Endpoint Protection console.
- **Console** - The console 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 a browser session to the 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** – Essential Endpoint Protection 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 can adjust the notification setting 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.
- **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 Essential Endpoint Protection account credentials to confirm the uninstall.

Web Portal

All Mac devices will be 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, Process Activity, SuperShield Allow, and more. When drilled down to an individual Mac device, there are several actions you can take and real-time 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.
- **Remote Access** - If your Mac is online, you can use the Remote Access feature to take remote control of that Mac. If you did not originally choose to install the Remote Access feature on that Mac, request to remote into it and within 10 minutes it will put the component in place and request that the user grant it the proper permissions. If the

user does not grant it the proper permissions, you will not be able to see actual windows on the screen or gain control.

- **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.
- **SuperShield Allow & Block** - Here you can add items to the allow or block list for your Mac device specifically.
- **SuperShield Options** - Adjust any of the settings for SuperShield like protection mode or system tray menu. If the device is online the change will happen in real time.
- **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 results in the Test History tab.

Uninstalling Essential Endpoint Protection Mac

You can uninstall through the Status Bar icon or from the management console. To complete the uninstall process, you will need your Administrator password, and depending on your uninstall method, your Essential Endpoint Protection account credentials.

Option 1 – Uninstall from Status Bar

This option is only available if you have the System Tray Menu setting for your Mac set to enabled.

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. Confirm your PC Matic account details and click Uninstall; the process will begin in the background.

5. You may be prompted for your Mac Administrator password, once you're done typing the password press enter.
6. The uninstall process will complete in the background and once done you will no longer see the SuperShield icon in the Status Bar.
7. Reboot your Mac to finish the full uninstall.

Option 2 – Management Console

1. You can also uninstall from the web portal in the same fashion as a Windows device. Simply click the trash can next to your Mac device from your devices list and confirm the prompt.
2. This will begin the uninstall process and will require the user to enter their Mac credentials to approve the uninstall.