



## Introduction

Essential Endpoint Protection is for organizations looking to manage and protect their computers remotely from a single location. There is no user interface at the workstation, and control can be restricted at the endpoint level.

### Essential Endpoint Protection consists of several parts:

- Real time whitelist-based malware protection known as *SuperShield*.
  - SuperShield is active and protects the computer 24/7.
- An on-demand scanner that will clean, maintain, and optimize each endpoint.
  - You can schedule scans at several different intervals:
    - One Time
    - Daily
    - Weekly
    - Monthly
  - Choose a start day and time and insert an email address to receive the clean reports after the scan completes.
- A modified VNC agent, which allows remote access to your endpoints.
  - The remote desktop ability will allow you to take control of endpoints on your account and share files between them easily.

## Optimal System Requirements

The operating systems below support the best overall security posture for your devices and our products operating. 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:** 8GB
- **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:** 2GB
- **Hard Disk:** 5GB of free space
- .net Framework 3.5 ([Download](#))

## Optimal System Settings

To ensure Essential Endpoint Protection can function at the highest level and provide all abilities in the product, there are optimal settings for Windows.

### Sleep Settings

When a device is asleep it loses network connection. This will remove your ability to take immediate actions from within the management console. Until the device awakes from sleep, immediate scans, command prompt access, reboots, and VNC control will be disabled. Sleeping devices will still wake for a scheduled scan but will not display real-time scan progress in the management console during the scan.

To ensure you always have access to the device when needed, we recommend adjusting the power plan to put the display to sleep but not the computer.

## Scan Components

- **Malware Scan** (Quick, Full, None): Choose to clean up malware and PUAs (Potentially Unwanted Applications).
- **Update Software Vulnerabilities:** We will automatically update 30 third party applications and make sure to keep each on the latest version and maintain the security of the program. (Java, Adobe, iTunes, Skype, etc.)
- **Update Drivers:** Update drivers to the latest version if necessary.
- **Improve Performance:** Essential Endpoint Protection contains several components that will help improve the overall performance of your endpoints. These can be seen in detail inside the reports section from your sidebar.

## Management Portal Access

Access to your management portal is available at <https://portal.pcpitstop.com> from any device with a web browser. You can view and manage your devices from anywhere that you are. However, to use the remote desktop feature, you must be on a Windows computer with Essential Endpoint Protection installed.

During initial installs, you may see unique tools you use blocked as unknown by Essential Endpoint Protection. This is normal, and evidence of our whitelist-based approach not allowing unknowns to run. If you have unknown files that are blocked and do not feel comfortable locally whitelisting them, please notify the Telesystem Support team.

- Toll Free: 888.808.6111
- Email: [support@telesystem.us](mailto:support@telesystem.us)

## Sidebar Navigation

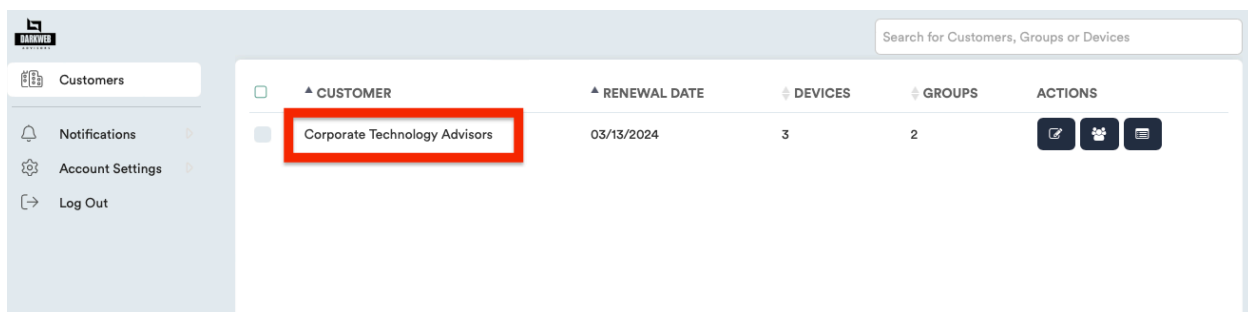
The sidebar in Essential Endpoint Protection is your home for all reports, views, options, and resources within the management console. No matter what page of your account you are currently viewing, the sidebar adapts to give you the links that are available.

### Sub Sidebar




When navigating your sidebar, a list of actions for that section will open into a sub sidebar so you can easily access anything you need without having to load different pages.

### Customers

The first tab in your sidebar, Customers, presents you with a high-level view of your environment displaying number of devices and groups assigned. There are also shortcut links that will take you into your customer info or allow you to make notes.

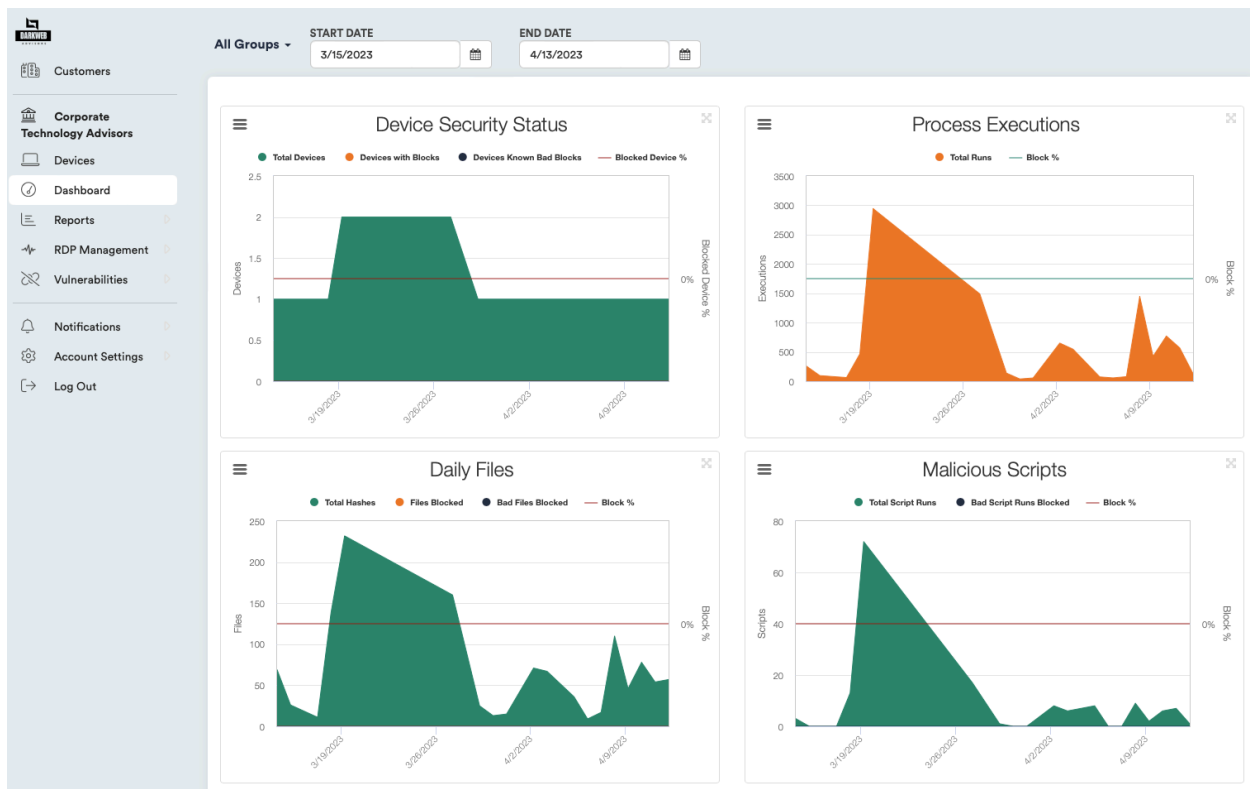


The screenshot shows the Management Portal interface. On the left is a sidebar with a 'Customers' tab selected. The main area displays a table with columns: CUSTOMER, RENEWAL DATE, DEVICES, GROUPS, and ACTIONS. The first row of data is for 'Corporate Technology Advisors', with a renewal date of 03/13/2024, 3 devices, and 2 groups. The 'Corporate Technology Advisors' text in the first row is highlighted with a red box. The ACTIONS column contains three icons: a pencil, a trash can, and a document.

| CUSTOMER                      | RENEWAL DATE | DEVICES | GROUPS | ACTIONS   |
|-------------------------------|--------------|---------|--------|---|
| Corporate Technology Advisors | 03/13/2024   | 3       | 2      |    |

Click on the name of your org (as shown above) to go to the Device list and access an expanded Sidebar menu with items including:

- **Devices**
- **Dashboard**
- **Process Activity**
- **Reports**
- **RDP Management**
- **Vulnerabilities**



## Devices

The Devices menu will allow admins to add, edit, or remove devices assigned within their org.

| DEVICE NAME                           | DEVICE TYPE    | LAST SEEN           | GROUP           | STATUS | ACTIONS |
|---------------------------------------|----------------|---------------------|-----------------|--------|---------|
| Hunter Gaming Laptop                  | Windows Laptop | 2023/04/13 19:15:51 | *Default Group* |        |         |
| Ira Home Laptop                       | Windows Laptop | 2023/01/26 10:58:18 | *Default Group* |        |         |
| Jason Dickheiser (Windows 10 Machine) | Windows Laptop | 2023/03/28 12:13:14 | *Default Group* |        |         |

Devices will display a list of all devices currently setup with the SuperShield Agent installed. From this page admins can see the device type, last time the SuperShield Agent connected from that device, group that the device is assigned to, and status of the device.

Use the Actions buttons to make notes about a device, schedule a scan for the device, refresh virus definitions, access remote desktop (if enabled), or remove the device from your account.

Add or Remove Devices by clicking the button at the top of the page. From here admins can configure settings for the SuperShield Agent and generate install files for Windows, Mac, Device Manager, or Windows Uninstaller. At the bottom of the Windows Installer and Mac Installer pages, admins can find updated Minimum System Requirement information for each platform.

**IMPORTANT:**

- Do not alter the Installer Download URL or the downloaded file name. This will cause issues with installation.
- The DarkWeb Advisors Agent will not be visible within Control Panel to increase security after installation. Uninstalls must be done through device actions or with the Endpoint Uninstaller above.

### Endpoint software for Windows

This Installer is used to get the DarkWeb Advisors Endpoint Agent software on each device that you want to protect and manage. Click the "Download" button and run the installer file on each device. You may also email the provided URL to employees so that they can download and run the installer. If you have Active Directory setup on your network, you can push this installer out to your office computers.

Which add-ons do you want installed?

☒ Remote Access ☐ Ad Blocker

### SuperShield Options

|                                |                     |
|--------------------------------|---------------------|
| System Tray Menu               | Java Runtime        |
| Disabled (Recommended)         | Block               |
| Removable Storage Devices      | Patch Management    |
| Block                          | Enabled (Automatic) |
| Blocked File Notification      | Windows Defender    |
| Display Only (Recommended)     | Allow               |
| Customer to put computer under | Group               |
| Corporate Technology Advisors  | *Default Group*     |

Installer Distribution:

Enter email address   Installer Download: <https://avredir.com/s/ePztNnV6diSI>

[View Minimum System Requirements](#)

### Generating an Install File

To generate an install file, choose the appropriate platform from the tabs along the top of the page for Windows, Mac, Device Manager or Windows Uninstaller.

NOTE: Device Manager is used for push installs/uninstalls and requires remote PowerShell access. It is used to enable the ability to do push the installs/uninstalls to devices on either an Active Directory or workgroup network. Admins must download the installer and install on their domain controller.

Choose if you want to install the add-ons for Remote Access or Ad Blocker using the checkboxes.

Configure the SuperShield Options from the following settings:

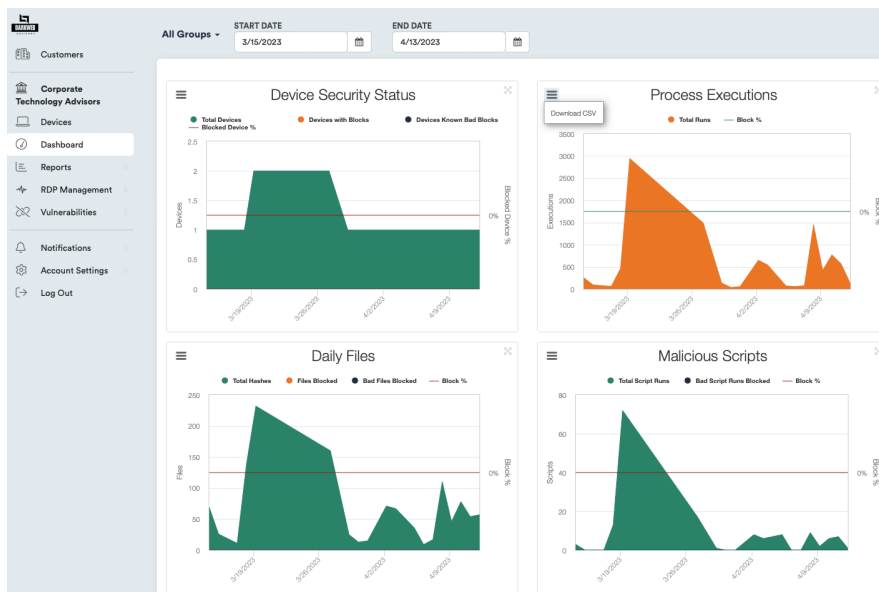
- System Tray Menu** – Choose to enable or disable the SuperShield System Tray Menu icon on an end-user's device.
- Removable Storage Devices** – Allow or block removable storage devices on the end user device. By default, this option is set to block which will prevent devices from utilizing things like USB drives.
- Blocked File Notification** – Choose the type of notification you want to display to end users when a file is blocked by the SuperShield agent.
- Java Runtime** – Allow or block Java application, runtime, and script execution on the end user device.

- **Patch Management** – Enable or disable application patch management through SuperShield.
- **Window Defender** – Allow or block Windows Defender from running alongside SuperShield.
- **Customer to put computer under** – Use the drop-down box to select the account you are assign the computer(s) to if you manage multiple customer accounts. If you only manage a single account, it will already be selected for you.
- **Group** – Choose the Group within the account to assign the computer to.
- **Installer Distribution** – Enter an email address where the installer file will be sent for distribution or use the link provided to download directly from this page or to send in a custom message. There is also a download button at the bottom of the page to begin the download process.
- **View Minimum System Requirements** – For Windows and Mac menus, you can expand this section to view the most current minimum requirements to run SuperShield on the selected device platform.

## Dashboard

The Dashboard displays graphs showing the following information:

- Device Security Status
- Process Executions
- Daily Files
- Malicious Scripts



Use the drop-down menu at the top of the page to narrow results to show only specific Groups and use the Start Date and End Date fields to customize the output information shown in the graphs.

Each graph has its own hamburger menu (3 horizontal lines) in the top-left corner that allows you to download the information for the graph into a CSV File.

## Reports

The Reports menu allows admins to view reports on the following items:

- Security Summary
- Maintenance Summary
- Hardware Inventory
- Software Inventory

Administrators can select from date ranges of the past week, past month, past 6 months, or specify a custom date range.


Reports can be setup to be emailed out on a schedule, exported to PDF, or exported to Excel format.


### Security Summary


This report will list each device, show the number of days it has been online during the reported date range, number of malware quarantined, security patches installed, processes checked, processes blocked, files checked, files blocked, scripts checked, scripts blocked.


Corporate Technology Advisors ▾

Email









Search

Device Summary

| Total | Windows Computers | Mac Computers | Windows Servers | Chrome Books |
|-------|-------------------|---------------|-----------------|--------------|
| 3     | 3                 | 0             | 0               | 0            |

Security Summary

| Days Online | Malware Quarantined | Security Patches | Processes Checked | Processes Blocked | Files Checked | Files Blocked | Scripts Checked | Scripts Blocked |
|-------------|---------------------|------------------|-------------------|-------------------|---------------|---------------|-----------------|-----------------|
| 6           | 0                   | 0                | 3K                | 0                 | 362           | 0             | 25              | 0               |

| DEVICE NAME  | DAYS ONLINE | MALWARE QUARANTINED | SECURITY PATCHES | PROCESSES CHECKED | PROCESSES BLOCKED | FILES CHECKED | FILES BLOCKED | SCRIPTS CHECKED | SCRIPTS BLOCKED |
|--|-------------|---------------------|------------------|-------------------|-------------------|---------------|---------------|-----------------|-----------------|
| Hunter Gaming Laptop<br>*Default Group*                  | 6           | 0                   | 0                | 3,420             | 0                 | 362           | 0             | 25              | 0               |
| Ira Home Laptop<br>*Default Group*                       | 0           | 0                   | 0                | 0                 | 0                 | 0             | 0             | 0               | 0               |
| Jason Dickheiser (Windows 10 Machine)<br>*Default Group* | 0           | 0                   | 0                | 0                 | 0                 | 0             | 0             | 0               | 0               |


### Maintenance Summary


This report will list each device, show the number of days it has been online during the reported date range, and show the size of junk files, number of services stopped, number of scheduled tasks, number of startups disabled, number of drivers updated, and the world rank.





Corporate Technology Advisors ▾

Email









Search

Device Summary

| Total | Windows Computers | Mac Computers | Windows Servers | Chrome Books |
|-------|-------------------|---------------|-----------------|--------------|
| 3     | 3                 | 0             | 0               | 0            |

Maintenance Summary

| Days Online | Junk Files | Services Stopped | Scheduled Tasks | Startups Disabled | Drivers Updated | World Rank |
|-------------|------------|------------------|-----------------|-------------------|-----------------|------------|
| 6           | 0 MB       | 0                | 0               | 0                 | 0               | ---        |

| ⚙️ DEVICE NAME ▾   | DAYS ONLINE ⚙️ | JUNK FILES ⚙️ | SERVICES STOPPED ⚙️ | SCHEDULED TASKS ⚙️ | STARTUPS DISABLED ⚙️ | DRIVERS UPDATED | WORLD RANK |
|--|----------------|---------------|---------------------|--------------------|----------------------|-----------------|------------|
| Hunter Gaming Laptop<br>*Default Group*                  | 6              | 0 MB          | 0                   | 0                  | 0                    | 0               | No Data    |
| Ira Home Laptop<br>*Default Group*                       | 0              | 0 MB          | 0                   | 0                  | 0                    | 0               | No Data    |
| Jason Dickheiser (Windows 10 Machine)<br>*Default Group* | 0              | 0 MB          | 0                   | 0                  | 0                    | 0               | No Data    |

### Hardware Inventory

This report will list the number of unique types of devices by manufacturer and model and show the number of devices that meet those criteria. Click on the green plus sign at the beginning of the row to expand the section and display information about each device type to list the individual devices and view additional information including the computer name, serial number, OS Version, BIOS date, and install date for the Essential Endpoint Protection.

|                    |                                       |              |                |            |               |                 |
|--------------------|---------------------------------------|--------------|----------------|------------|---------------|-----------------|
| Hardware Inventory |                                       |              |                |            |               |                 |
| ⬆️ PLATFORM        | ⚙️ MANUFACTURER                       | ⚙️ MODEL     | ⚙️             | QUANTITY   |               |                 |
| ⊕ Laptop           | ASUSTeK COMPUTER INC.                 | N501VW       |                | 1          |               |                 |
| ⊕ Laptop           | GIGABYTE                              | AORUS 15P YD |                | 1          |               |                 |
| ⊖ Laptop           | LENOVO                                | 20B6005EUS   |                | 1          |               |                 |
| COMPUTER NAME      | ALIAS                                 | SERIAL       | OS VERSION     | BIOS DATE  | PC MATIC DATE | GROUP NAME      |
| DESKTOP-EMK27C5    | Jason Dickheiser (Windows 10 Machine) | PF019NDR     | Windows 10 x64 | 2014/03/28 | 2023/01/23    | *Default Group* |

Showing 1 to 3 of 3 entries

### Software Inventory

This report lists all unique software across all endpoint computers running Essential Endpoint Protection with a quantity showing the total number of devices where that software was installed and the number of unique versions across all devices.

Click the green plus symbol at the beginning of the row to expand and show a list of the computers where the application was found along with additional information about each device including the OS, software, version, manufacturer, and install date.

| Software Inventory                            |          |         |                                   |          |                  |               |                 |
|---|----------|---------|-----------------------------------|----------|------------------|---------------|-----------------|
| NAME  |          |         | QUANTITY                          |          |                  | # OF VERSIONS |                 |
| Office 16 Click-to-Run Localization Component |          |         | 9                                 |          |                  | 3             |                 |
| HP ePrint SW                                  |          |         | 7                                 |          |                  | 1             |                 |
| Intel(R) Management Engine Components         |          |         | 5                                 |          |                  | 3             |                 |
| Intel(R) Chipset Device Software              |          |         | 4                                 |          |                  | 2             |                 |
| Intel(R) Serial IO                            |          |         | 4                                 |          |                  | 3             |                 |
| Endpoint Protector Agent 1.2.17.0             |          |         | 3                                 |          |                  | 1             |                 |
| COMPUTER                                      | PLATFORM | OS      | SOFTWARE                          | VERSION  | MANUFACTURER     | INSTALL DATE  | GROUP NAME      |
| Hunter Gaming Laptop                          | Laptop   | Windows | Endpoint Protector Agent 1.2.17.0 | 1.2.17.0 | DarkWeb Advisors | 2022/06/03    | *Default Group* |
| Ira Home Laptop                               | Laptop   | Windows | Endpoint Protector Agent 1.2.17.0 | 1.2.17.0 | DarkWeb Advisors | 2022/09/29    | *Default Group* |
| Jason Dickheiser (Windows 10 Machine)         | Laptop   | Windows | Endpoint Protector Agent 1.2.17.0 | 1.2.17.0 | DarkWeb Advisors | 2023/01/23    | *Default Group* |
| Google Chrome                                 |          |         | 3                                 |          |                  | 2             |                 |
| Microsoft Edge                                |          |         | 3                                 |          |                  | 2             |                 |
| Microsoft Edge WebView2 Runtime               |          |         | 3                                 |          |                  | 2             |                 |
| Windows PC Health Check                       |          |         | 3                                 |          |                  | 2             |                 |
| Microsoft Edge Update                         |          |         | 3                                 |          |                  | 3             |                 |

## RDP Management

The RDP Management menu provides admins with information about Remote Desktop Protocol sessions and control settings for devices in the org using Essential Endpoint Protection.

Sub Sidebar Menu items include:

- Log Summary
- Log Detail
- Control Center
- Device Whitelist

### Log Summary and Log Detail

Control access to the Management Logs menu item inside of the RDP Management Sub-Sidebar menu.

The Log Summary will display RDP Connections by over a specified reporting period which can be customized at the top of the page.

The Log Detail will show additional information about RDP connections including active sessions, connect time, disconnect time, login username, RDP client, RDP server, IP Address, and location.

### Control Center

Manually turn enable or disable RDP access from this menu. Buttons at the top of the page allow admins to toggle RDP on or off for all devices.

The table allows admins to see if active RDP sessions are occurring across any individual device.

Use the buttons under “Set Schedule” to manually enable/disable RDP for individual devices or set a schedule for allowing RDP sessions to occur for known/expected times and dates.

Remote Desktop Protocol (RDP) has become a target for malware writers and we advise turning it off when not in use. **Manually turning off RDP from this report will remove any RDP Schedules that you have setup from the device page.**

| ⌵ RDP ENABLED? | ⌵ ACTIVE SESSION? | ⌵ DEVICE NAME                         | ⌵ GROUP NAME    | ⌵ PORT | ⌵ RDP SCHEDULE | ⌵ HOURS PER WEEK | ⌵ SET SCHEDULE |
|----------------|-------------------|---------------------------------------|-----------------|--------|----------------|------------------|----------------|
|                |                   | Hunter Gaming Laptop                  | *Default Group* | 3389   |                | 0.00             |                |
|                |                   | Ira Home Laptop                       | *Default Group* | 3389   |                | 0.00             |                |
|                |                   | Jason Dickheiser (Windows 10 Machine) | *Default Group* | 3389   |                | 0.00             |                |

## Vulnerabilities

The Vulnerabilities menu allows admins to view possible vulnerabilities for the devices using Essential Endpoint Protection based on best practice scenarios.

The following Sub-Sidebar Options include:

- System Tray Menu
- Prompt for Override
- Remote Desktop Protocol
- Account Lockout Settings

### System Tray Menu

This menu displays a list of devices where the System Tray Menu icon is enabled. This allows SuperShield settings to be changed on each individual device and could represent a security concern.

Admins can uncheck devices on this list to disable the System Tray Menu Icon for those devices.

### Prompt For Override

This menu displays devices that currently have a prompt for override enabled for Blocked File Notifications. We strongly recommend using the Display Only notification setting to display to a user when a file is blocked by SuperShield by disabling them here.

### Remote Desktop Protocol




This menu shows devices that have Remote Desktop Protocol (RDP) enabled. RDP has become a target for malware writers, and we advise turning it off. Manually turning off RDP from this menu will remove any RDP Schedules that you have setup from the RDP Management section.

### Account Lockout Settings

This menu shows devices that do not have Account Lockout thresholds set. This allows Windows to lock the computer after several failed login attempts.

Click the Update button to adjust the available settings.

The following devices do not have Account Lockout thresholds set. This allows Windows to lock the computer after several failed login attempts. ⓘ

| DEVICE TYPE   | MANUFACTURER | DEVICE NAME          | GROUP NAME      | UPDATE LOCKOUT SETTINGS   |
|---|--------------|----------------------|-----------------|---|
|  | GIGABYTE     | Hunter Gaming Laptop | *Default Group* |  |
|  | ASUS         | Ira Home Laptop      | *Default Group* |   |

Showing 1 to 2 of 2 entries

Account Lockout Settings Disabled

-1


Account Lockout Threshold ⓘ

30

Account Lockout Duration (Minutes) ⓘ

30

Account Lockout Observation (Minutes) ⓘ



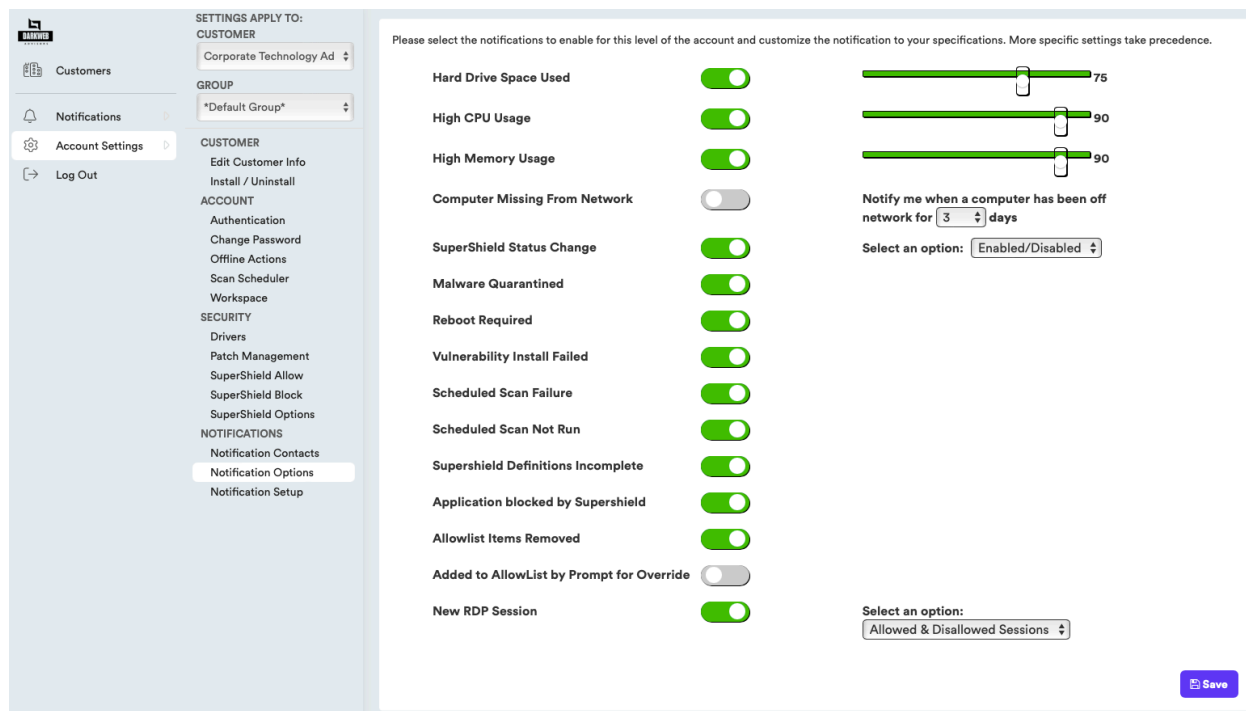
## Notifications

Essential Endpoint Protection Alerts are available in the Notifications tab. This tab provides information about happenings inside your account, but these are not *Alerts* that need your present attention. Essential Endpoint Protection automatically takes care of any item that needs immediate attention so you can relax and focus on other tasks.

Sub Sidebar Options include:

- **Security** – Displays any notifications associated with Security related events such as scan failure, malware quarantined, change in SuperShield Agent status, etc....
- **Performance** – Displays any notifications associated with Performance related events such as high CPU usage, high memory usage, hard drive disk space usage, and reboot required.

Note: Notification Contacts, Notification Options, and Notification Setup are all located in the Account Settings menu where administrators can configure who should receive urgent notifications and what criteria will trigger those notifications to be sent.



## Account Settings

At the bottom of the sidebar, you will find a tab called Account Settings that will encompass all your options that are available at the account level, along with any information about your account.

Sub Sidebar items for Account Settings include:

- **Customer Info** – Displays the name, address information, and available groups assigned to the account.
- **Install/Uninstall** – This is where you can generate the installer download for Windows, Mac, and Device Manager Installer, and the Uninstaller file for Windows deployments.
- **Authentication** – Allows you to disable or enable the multi-factor authentication (MFA) for all users who have access for your org. MFA is enabled by default for all users.
- **Change Password** – Update your portal login password.
- **Scan Scheduler** – Add, Edit, Delete scans for devices. Scans can be scheduled for individual devices, groups or select Customer to setup a scan for all devices in your org.
- **Workspace** – Allows you to configure the default page and views for when users login to admin portal for Essential Endpoint Protection
- **Drivers** – This menu allows admins to manually add a list of driver items to an Allow List for proactive approval.
- **Patch Management** – By default, Essential Endpoint Protection will check for these programs installed on each machine and if they are installed, updates them to their most recent version. Admins can also use this menu to customize the feature for the needs of their org by specifying a Max Version for upgrade or deselect applications from the list to do manual application management outside of Essential Endpoint Protection

- **SuperShield Allow/Block** – Use these two menus to view applications/files that the SuperShield agent installed for Essential Endpoint Protection that have been allowed or blocked. Admins can remove items from the Allow list if they find unwanted files/applications that have been approved or manually allow items that have been blocked but should be installed or run.
- **SuperShield Options** – Use this menu to manage the settings for the SuperShield agent that is installed on machines in your org. Options include enabling or disabling the System Tray Menu to give end users visibility that the agent is running on their machine, allow/block Windows Defender, Java Runtime, and Removable Storage Devices (example: USB Drives).
- **Notification Contacts** – Add, edit, remove contacts who will receive alerts via email and/or Text Message (SMS) for criteria setup under Notification Options and Notification Setup
- **Notification Options** – Select the notifications to enable for this level of the account and customize the notification to your specifications. Notifications criteria include:
  - Hard Drive Space Usage
  - CPU Usage
  - Memory Usage
  - SuperShield Status Change
  - Malware Quarantined
  - Reboot Required
  - Vulnerability Install Failed
  - Scheduled Scan Failure
  - Scheduled Scan Not Run
  - SuperShield Definitions Incomplete
  - Application blocked by SuperShield
  - AllowList Items Removed
  - Added to AllowList by Prompt for Override
  - New RDP Session
- **Notification Setup** – This is where admins can choose which alerts/notifications are sent to which Notification Contacts. You must add contacts to the Notification Contacts first and choose the Notification Options before you can complete the Notification Setup.