

**WEBROOT®**

Intelligent Cloud-Based Security  
for Mobile, Endpoint and Web



# คู่มือการใช้งาน

โปรแกรมป้องกันไวรัส (Webroot) บนเครื่องคอมพิวเตอร์

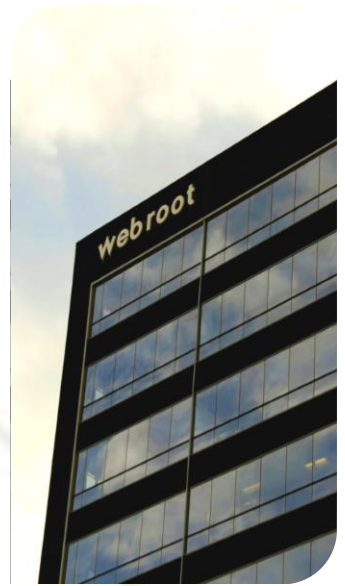
เวอร์ชัน 2.0

## สารบัญ

● ประวัติ	หน้า	3
● ความต้องการของระบบ	หน้า	3
● หน้าหลักโปรแกรมป้องกันไวรัส (Webroot) บนเครื่องคอมพิวเตอร์	หน้า	5
○ สถานะการทำงาน	หน้า	6
○ Stay informed Join the discussion	หน้า	7
○ Advanced settings	หน้า	7
■ Install settings	หน้า	7
■ Scheduler	หน้า	8
■ System Optimizer	หน้า	9
■ Scan Settings	หน้า	10
■ Firewall	หน้า	11
■ Access Control	หน้า	12
■ Proxy	หน้า	13
■ Heuristics	หน้า	14
■ Import / Export	หน้า	14
■ System Optimizer	หน้า	15
■ Secure Erase	หน้า	15
○ PC Security	หน้า	16
■ Scan & Shields	หน้า	16
■ Quarantine	หน้า	18
■ Block / Allow File	หน้า	19
○ Identity Protection	หน้า	20
■ Online Protection	หน้า	20
■ Application Protection	หน้า	21
○ Utilities	หน้า	21
■ Antimalware Tools	หน้า	22
■ Reports	หน้า	23
■ System Control	หน้า	25
■ System Optimizer	หน้า	27
○ My Account	หน้า	28
○ Keycode	หน้า	29
○ About SecureAnywhere	หน้า	29
○ Support / Community	หน้า	29

## Webroot SecureAnywhere®

- ก่อตั้ง ปี 1997 สำนักงานใหญ่อยู่ที่สหรัฐอเมริกา
- สำนักงาน อยู่ที่อเมริกา ยุโรปและเอเชีย
- ผลงานที่ดำเนินการผ่านระบบ Cloud Service ประกอบด้วย Endpoint, Web และ Mobile security
- ได้รับรางวัล Winning SaaS 2007 Award
- ได้รับรางวัล Winning Webroot SecureAnywhere Endpoint Protection Award
- ได้รับรางวัล Won IT Security Innovation & Product Excellence Awards
- มีผู้ใช้งานและพันธมิตรทั้งหมดมากกว่า 30 ล้าน
- เทคโนโลยีของ Webroot ที่มี Partner ต่างๆ นำไปใช้งาน



### ความต้องการของระบบ

Management Portal Access:

- Internet Explorer® version 8 and newer
- Mozilla® Firefox® version 3.6 and newer
- Chrome 11 and newer
- Safari 5 and newer
- Opera 11 and newer

Supported PC Platforms:

- Windows 8, 8.1, 32 and 64-bit
- Windows 7, 32 and 64-bit
- Windows Vista®, 32 and 64-bit
- Windows® XP Service Pack 2 and 3, 32 and 64-bit

- Windows XP Embedded
- Mac OS X v.10.10 "Yosemite"
- Mac OS X v.10.9 "Mavericks"
- Mac OS X v.10.8 "Mountain Lion"
- Mac OS<sup>®</sup> X v.10.7 "Lion"

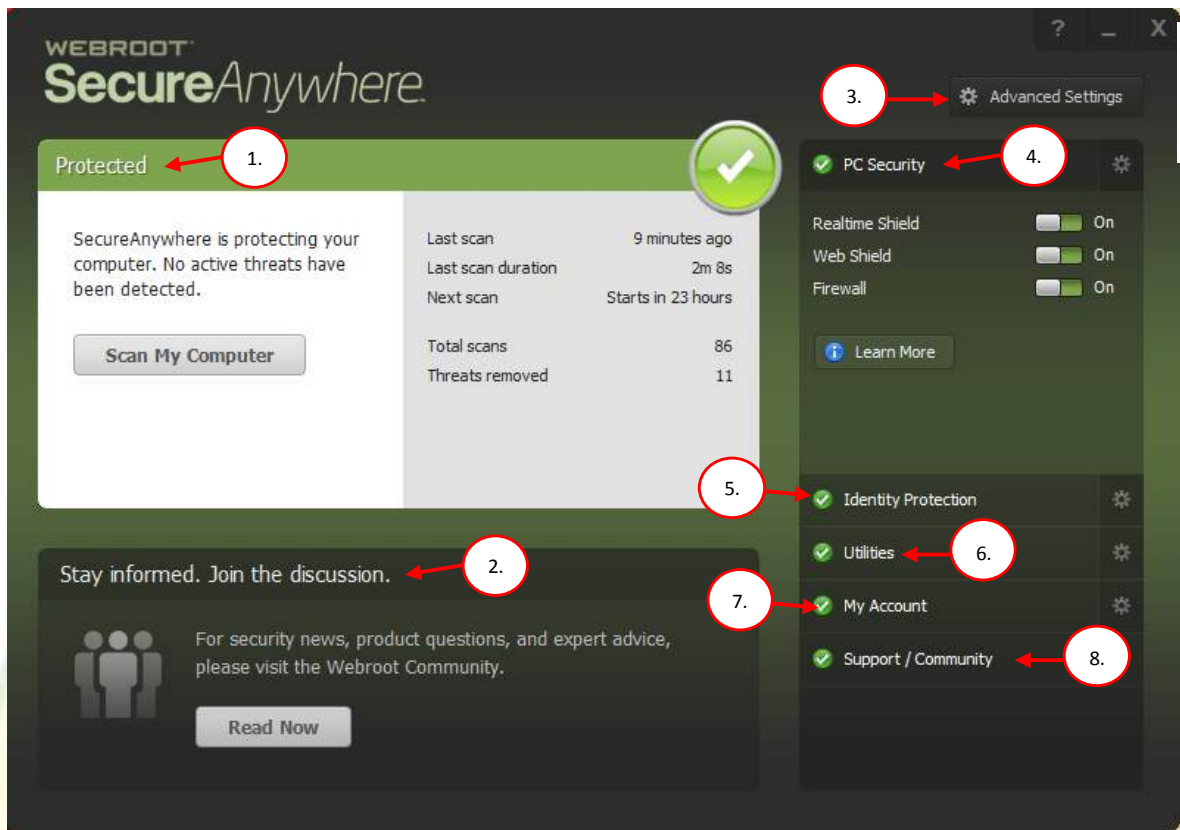
#### Supported Server Platforms:

- Windows Server 2012 Standard, R2
- Windows Server 2008 R2 Foundation, Standard, Enterprise
- Windows Server 2003 Standard, Enterprise, Service Pack2, 32 and 64-bit
- Windows Small Business Server 2008, 2011, 2012
- Windows Server Core 2003, 2008, 2012
- Windows Server 2003 R2 for Embedded Systems
- Windows Embedded Standard 2009 SP2
- Windows XP Embedded SP1, Embedded Standard 2009 SP3
- Windows Embedded for POS Version 1.0

#### Supported Virtual Server Platforms:

- VMware vSphere 5.5 and older (ESX/ESXi 5.5 and older), Workstation 9.0 and older, Server 2.0 and older
- Citrix XenDesktop 5; XenServer 5.6 and older; XenApp 6.5 and older
- Microsoft Hyper-V Server 2008, 2008 R2, 2012 and 2012 R2
- Virtual Box

## หน้าหลักโปรแกรมป้องกันไวรัส (Webroot) บนเครื่องคอมพิวเตอร์

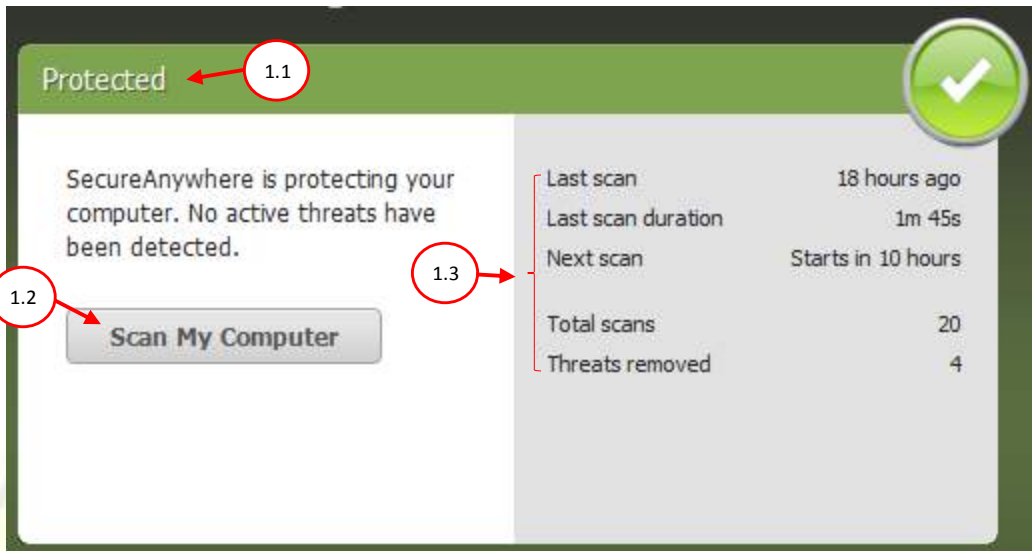


ภาพแสดงหน้าจอหลักโปรแกรมป้องกันไวรัส (Webroot)

หน้าจอหลักมีเมนูที่ใช้ควบคุมการทำงานดังรายการต่อไปนี้

1. สถานะการทำงาน
2. Stay informed Join the discussion
3. Advanced settings
4. PC Security
5. Identity Protection
6. Utilities
7. My Account
8. Support / Community

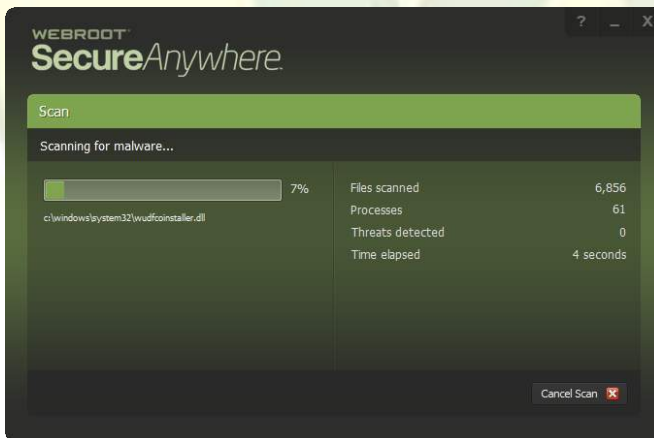
1. สถานะการทำงาน โปรแกรม แสดงสถานะการทำงานของ โปรแกรมป้องกันไวรัส (Webroot secure anywhere) ซึ่งมีการแสดงรายละเอียดดังนี้



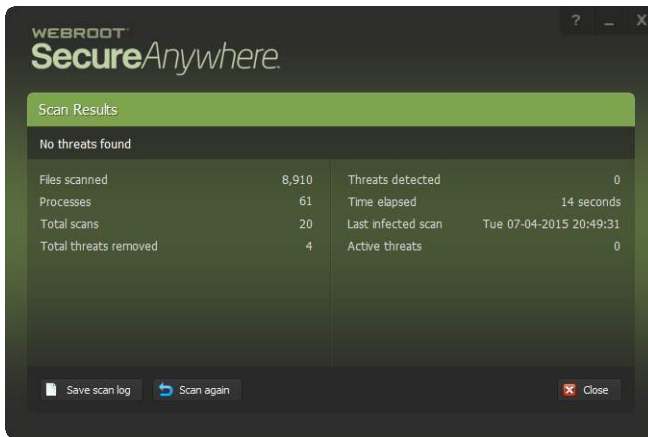
1.1. ส่วนที่แสดงสถานะการทำงานมี 2 ส่วน ได้แก่

- Protected โปรแกรมกำลังทำงาน
- Scanning โปรแกรมอยู่ระหว่างสแกนคอมพิวเตอร์

1.2. เมนู Scan My Computer ใช้กรณีที่ต้องการให้โปรแกรมทำการสแกนเครื่องคอมพิวเตอร์



1.2.1 เมื่อทำการคลิกปุ่ม Scan My Computer โปรแกรมจะทำการสแกนเครื่องคอมพิวเตอร์ โดยจะแสดงสถานะระหว่างที่โปรแกรมทำงาน



1.2.2 เมื่อโปรแกรมทำงานเสร็จเรียบร้อยแล้ว โปรแกรมจะแสดงผลการทำงานทั้งนี้ ผู้ใช้งานสามารถทำการบันทึก Log โดยคลิกปุ่ม Save Scan log หรือถ้าต้องการ สแกนอีกครั้งให้คลิกปุ่ม Scan Again

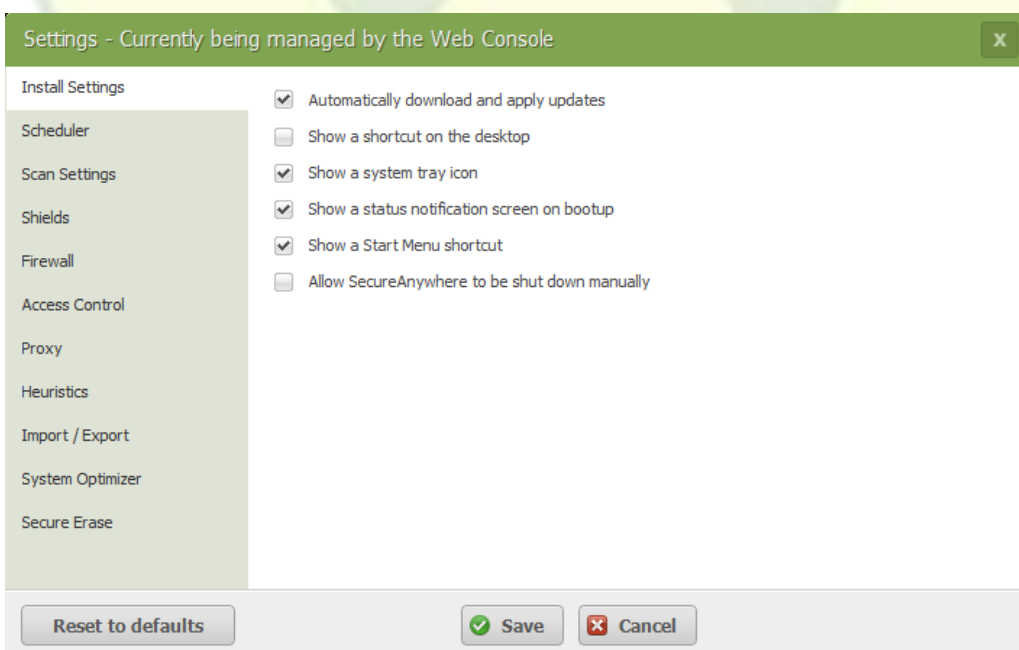
### 1.3. แสดงผลการทำงานของโปรแกรมโดยมีรายละเอียดดังนี้

- Last scan จำนวนชั่วโมงที่โปรแกรมทำการสแกนล่าสุด
- Last scan duration จำนวนระยะเวลาที่โปรแกรมทำการสแกนล่าสุด
- Next scan เวลาที่โปรแกรมจะทำการสแกนครั้งต่อไป
- Total scans รวมจำนวนที่โปรแกรมทำการสแกนทั้งหมด
- Threats removed จำนวนที่โปรแกรมได้ทำการลบไฟล์ที่เป็นอันตรายต่อเครื่องคอมพิวเตอร์

2. **Stay informed Join the discussion** เว็บไซต์เพื่อแจ้งปัญหาและแลกเปลี่ยนความรู้รวมไปถึงปัญหาที่เกิดขึ้น

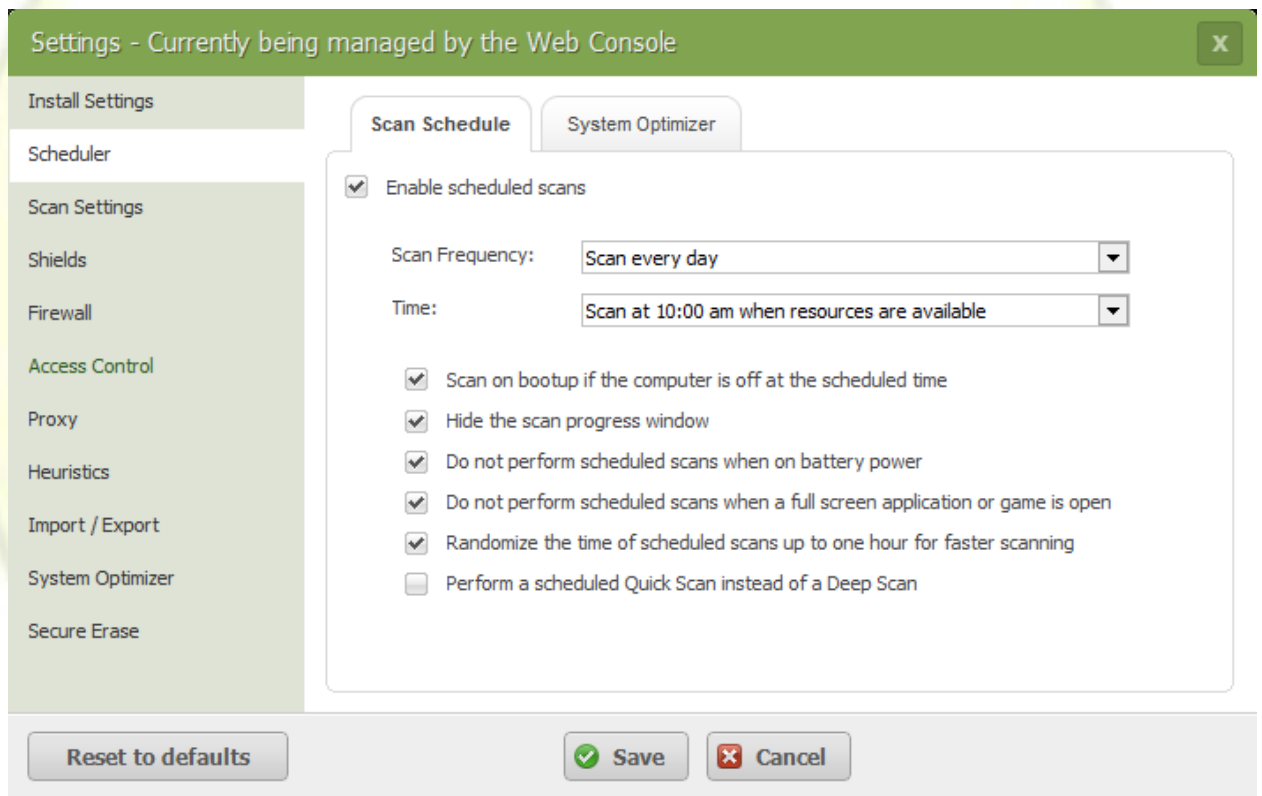
3. **Advanced setting** เมนูสำหรับกำหนดการตั้งค่าโปรแกรมป้องกันไวรัส (Webroot Secure Anywhere) โดยมีแถบเมนูดังนี้

- Install settings การตั้งค่าการติดตั้งโปรแกรมโดยมีรายละเอียดดังนี้



- Automatically download and apply updates      อัปเดตและดาวน์โหลดอัตโนมัติ
- Show a shortcut on the desktop      แสดงไอคอน โปรแกรมที่หน้าจอหลัก
- Show a system tray icon      แสดงไอคอน โปรแกรมที่แถบเมนู
- Show a status notification screen on bootup      แสดงสถานการณ์แจ้งเตือนเมื่อคอมพิวเตอร์เริ่มต้นเครื่องใหม่
- Show a Start Menu shortcut      แสดงโปรแกรมที่ Start menu
- Allow SecureAnywhere to be shut down manually      อนุญาตให้ปิดการทำงานของโปรแกรมด้วยตัวเอง

● **Scheduler** การกำหนดตารางเวลาในการสแกนและการเพิ่มประสิทธิภาพในการทำงาน โดยมีรายละเอียดดังนี้



#### แถบเมนู Scan schedule

- Enable Scheduled Scans      เปิดการใช้งานการสแกนอัตโนมัติ
- Scan Frequency      กำหนดความถี่ในการสแกน
- Time      กำหนดเวลาของการสแกน
- Scan on bootup if the computer is off at the scheduled time      ทำการสแกนเมื่อคอมพิวเตอร์ถูกปิดในเวลาที่กำหนดให้โปรแกรมทำงาน

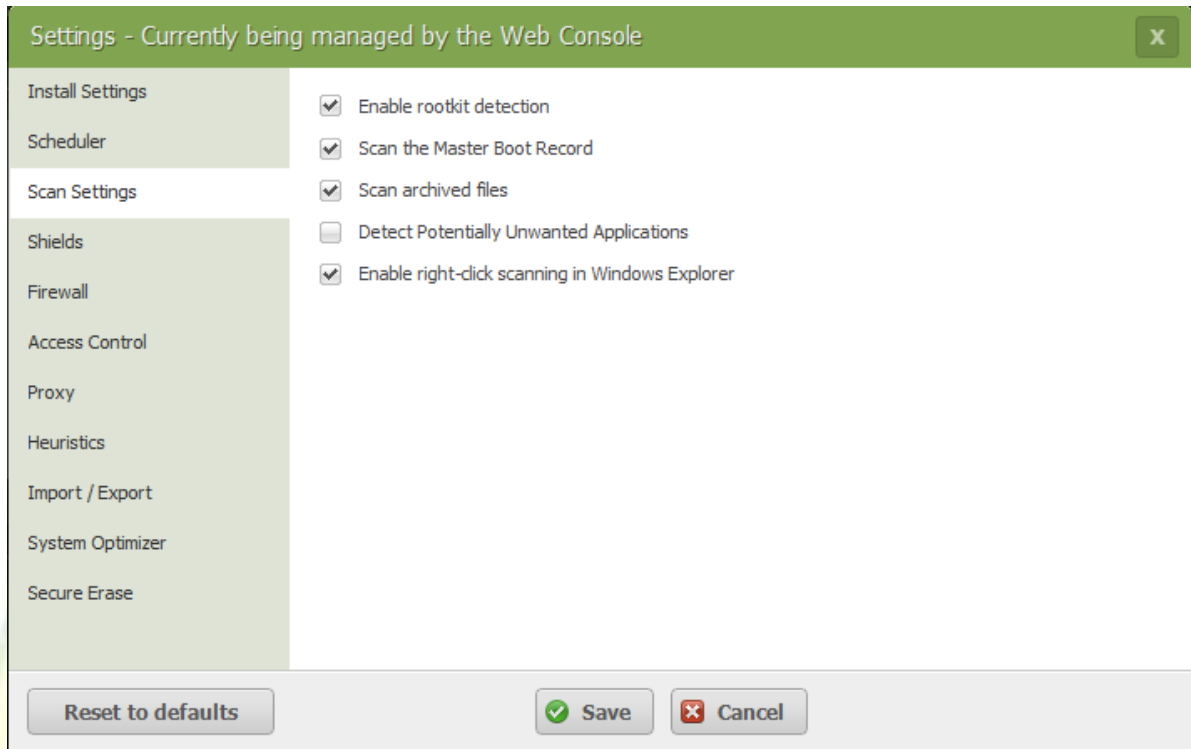


- Hide the scan progress window      ซ่อนหน้าต่างการทำงาน
- Do not perform scheduled scans when on battery power      กำหนดห้ามทำการสแกนเมื่อคอมพิวเตอร์ใช้พลังงานจากแบตเตอรี่
- Do not perform scheduled scans when a full screen application or game is open      กำหนดห้ามทำการสแกนเมื่อโปรแกรมอื่นๆ หรือ เกมส์ทำงาน
- Randomize the time of scheduled scans up to one hour for faster scanning      กำหนดให้โปรแกรมสุ่มการสแกนภายใน 1 ชม
- Perform a scheduled Quick Scan instead of a Deep Scan      กำหนดให้ทำการสแกนเชิงลึก

### แถบเมนู System Optimizer

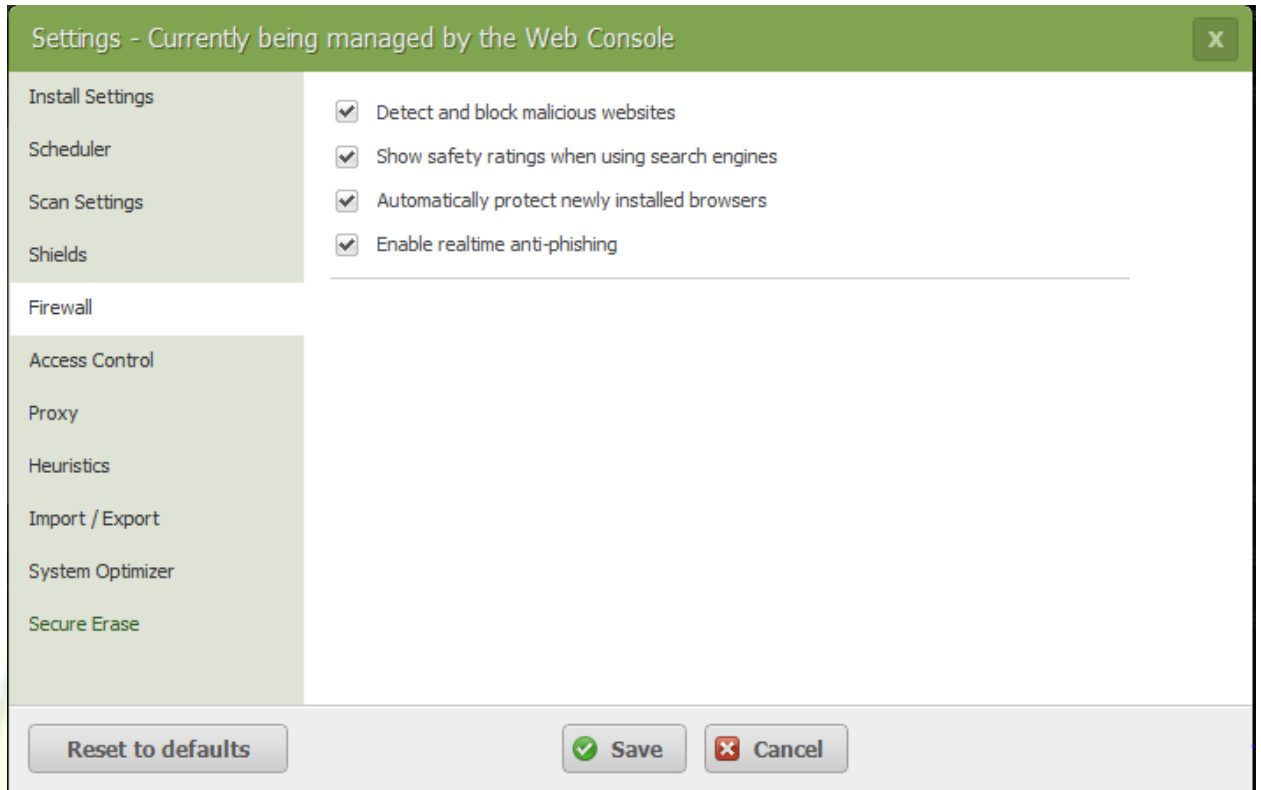
- Enable scheduled optimization      เปิดการเพิ่มประสิทธิภาพของโปรแกรมโดยอัตโนมัติ
- Optimize only on the following days      กำหนดวันที่ต้องการให้โปรแกรมทำงาน
- Optimize at specific time of day      กำหนดเวลาที่ต้องการให้โปรแกรมทำงาน
- Optimize every      กำหนดช่วงระยะเวลาที่ต้องการให้โปรแกรมทำงานต่อชั่วโมง
- Run on bootup if the system was off at the scheduled time      กำหนดให้โปรแกรมทำงานเมื่อคอมพิวเตอร์เริ่มทำงานถ้าคอมพิวเตอร์ไม่เปิดใช้งานตามเวลาที่กำหนด

- **Scan Settings** การตั้งค่าการสแกนโดยมีรายละเอียดดังนี้



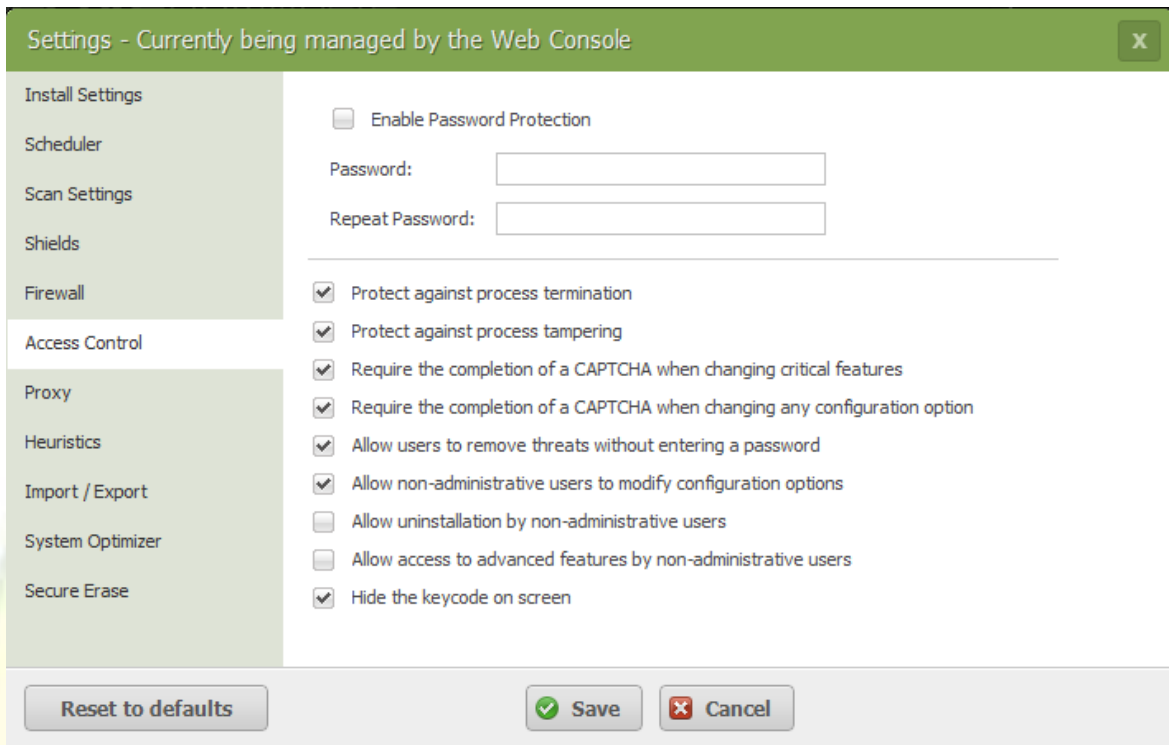
- |   |   |
|---|---|
| <input type="radio"/> Enable rootkit detection                        | กำหนดการเปิดใช้งานการตรวจสอบ Rookit                               |
| <input type="radio"/> Scan the Master Boot Record                     | กำหนดให้ทำการสแกน Master boot Record                              |
| <input type="radio"/> Scan archived files                             | กำหนดให้ทำการสแกนไฟล์ที่จัดเก็บ                                   |
| <input type="radio"/> Detect Potentially Unwanted Applications        | กำหนดให้ทำการตรวจสอบโปรแกรมที่อาจเป็นภัยคุกคามเครื่องคอมพิวเตอร์  |
| <input type="radio"/> Enable right-click scanning in Windows Explorer | กำหนดให้โปรแกรมทำงาน เมื่อมีการคลิกขวาที่เมนูของ Windows Explorer |

- **Firewall** กำหนดการตั้งค่า Firewall มีรายละเอียดการตั้งค่าดังนี้



- |  |  |
|--|--|
| <input type="radio"/> Detect and block malicious websites            | กำหนดให้ทำการตรวจสอบและป้องกันเว็บไซต์ที่เป็นอันตราย             |
| <input type="radio"/> Show safety ratings when using search engines  | แสดงอันดับความปลอดภัยเมื่อมีการใช้เครื่องมือการค้นหาผ่านเว็บไซต์ |
| <input type="radio"/> Automatically protect newly installed browsers | กำหนดให้ป้องกันการลงโปรแกรมเว็บเบราว์เซอร์ ที่ทำการติดตั้งใหม่   |
| <input type="radio"/> Enable realtime anti- phishing                 | กำหนดให้เปิดใช้งานการป้องกันการโจรกรรมข้อมูลผ่านเว็บไซต์ตลอดเวลา |

- **Access Control** การควบคุมการเข้าถึงคอมพิวเตอร์สามารถกำหนดสิทธิ์ให้ใช้หรือปฏิเสธการเข้าถึงฟังก์ชันบางอย่าง การควบคุมการเข้าถึงเหล่านี้ยังปกป้องคอมพิวเตอร์ของคุณจากโปรแกรมภัยคุกคามที่พยายามจะเปลี่ยนการตั้งค่าในโปรแกรมโดยมีรายละเอียดดังนี้



- |  |  |
|--|--|
| <input type="radio"/> Enable Password Protection   | เปิดใช้งานการป้องกันด้วยรหัสผ่าน   |
| <input type="radio"/> Password:  | กำหนดรหัสผ่าน  |
| <input type="radio"/> Repeat Password  | ทำการกรอกรหัสผ่านที่กำหนดอีกครั้ง  |
| <input type="radio"/> Protect against process termination  | กำหนดห้ามผู้ใช้งานทำการยกเลิกกระบวนการทำงานใดๆ ของโปรแกรม                    |
| <input type="radio"/> Protect against process tampering  | กำหนดห้ามผู้ใช้งานทำการปลอมแปลงกระบวนการทำงานใดๆ ของโปรแกรม                  |
| <input type="radio"/> Require the completion of a CAPTCHA when changing critical features        | กำหนดให้กรอก CAPTCHA (การยืนยันตัวตน) เมื่อทำการเปลี่ยนแปลงคุณลักษณะที่สำคัญ |
| <input type="radio"/> Require the completion of a CAPTCHA when changing any configuration option | กำหนดให้มีกรอก CAPTCHA (การยืนยันตัวตน) เมื่อมีการเปลี่ยนการตั้งค่าต่างๆ     |
| <input type="radio"/> Allow users to remove threats without entering a password                  | อนุญาตให้ผู้ใช้งานทำการย้ายไฟล์โดยไม่ต้องใส่รหัสผ่าน                         |
| <input type="radio"/> Allow non-administrative users to modify configuration options             | อนุญาตให้ผู้ใช้งานที่ไม่ใช่ผู้ดูแลระบบเปลี่ยนแปลงการตั้งค่าต่างๆ ได้         |

- Allow uninstallation by non - administrative users      อนุญาตให้ผู้ใช้งานที่ไม่ใช่ผู้ดูแลระบบถอนการติดตั้งโปรแกรมได้
- Allow access to advanced features by non-administrative users      อนุญาตให้ผู้ใช้งานที่ไม่ใช่ผู้ดูแลระบบเข้าใช้งานคุณลักษณะขั้นสูงได้
- Hide the keycode on screen      กำหนดให้ซ่อน Keycode จากหน้าจอ

- Proxy มีรายละเอียดการตั้งค่าดังต่อไปนี้

Settings - Currently being managed by the Web Console

Install Settings

Scheduler

Scan Settings

Shields

Firewall

Access Control

Proxy

Heuristics

Import / Export

System Optimizer

Secure Erase

Proxy Type: Do not use a proxy server

Authentication Method: Any authentication

Host:

Port:

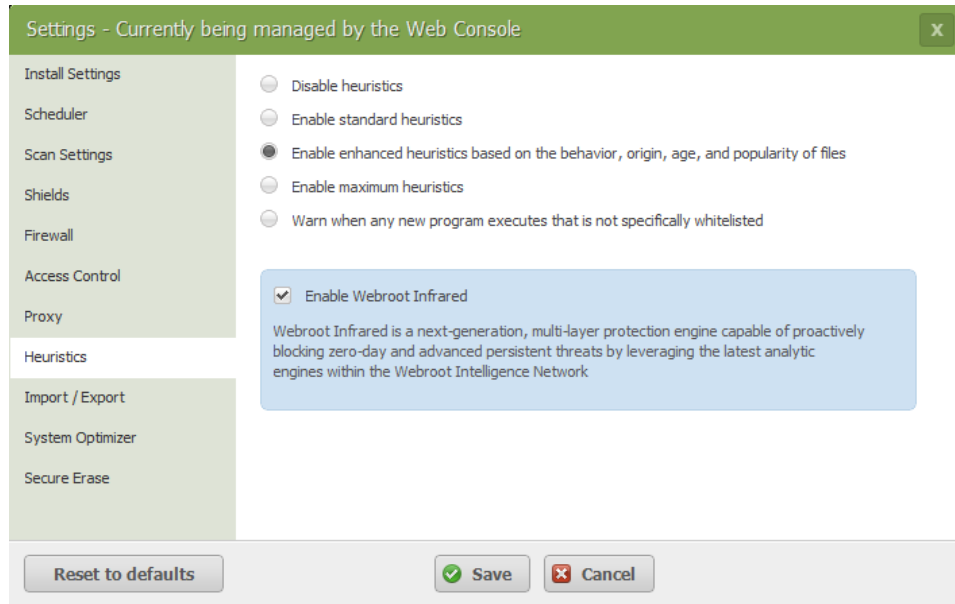
Username:

Password:

Reset to defaults      Save      Cancel

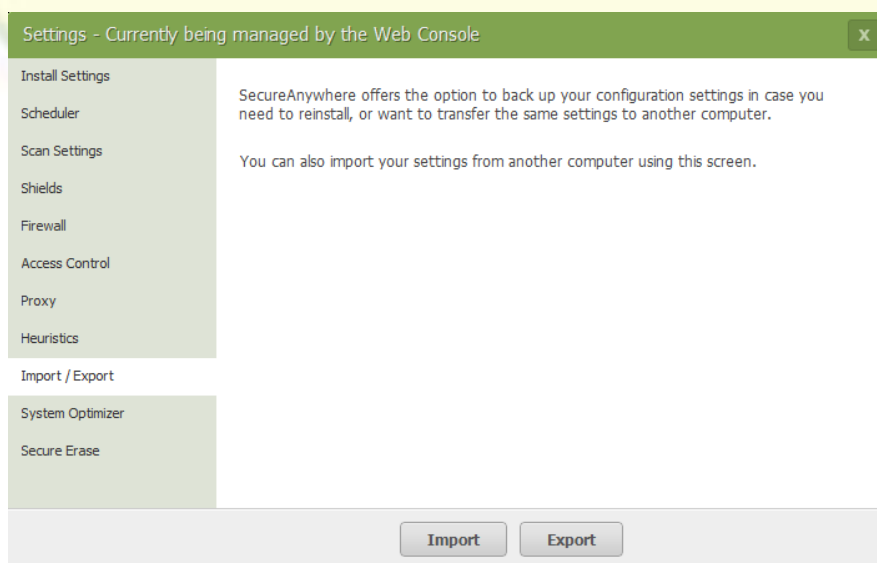
- Proxy Type      เลือกชนิดของ Proxy
- Authentication Method      กำหนดวิธีการตรวจสอบ
- Host      ระบุโฮส
- Port      ระบุพอร์ต
- Username      ระบุ Username
- Password      ระบุ Password

- **Heuristics** การตั้งค่าการวิเคราะห์พฤติกรรมการใช้งานของผู้ใช้งาน ซึ่งมีรายละเอียดดังต่อไปนี้

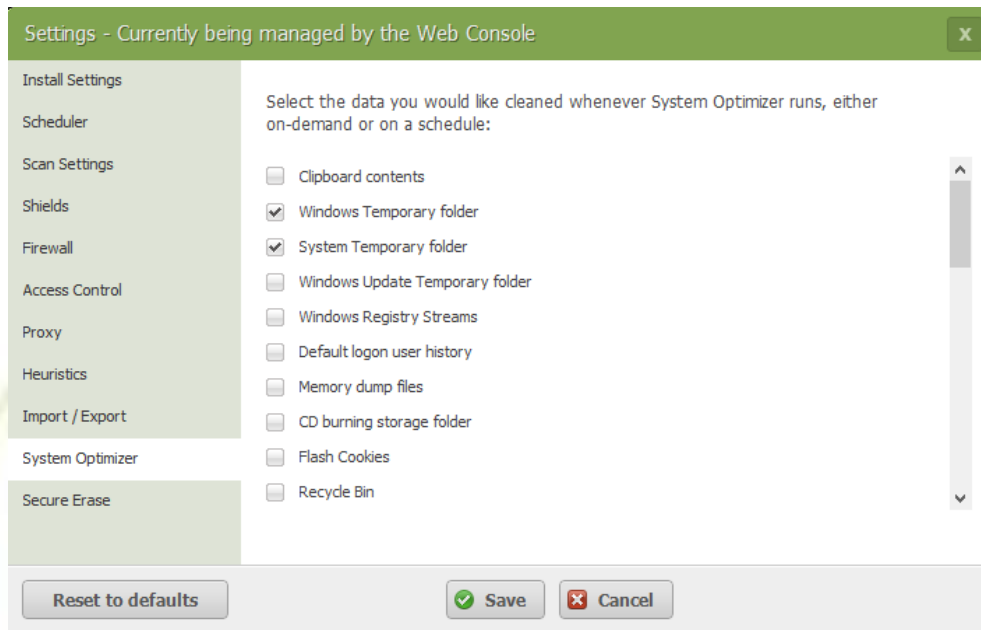


- Disable heuristics กำหนดให้หยุดการวิเคราะห์พฤติกรรมการใช้งาน
- Enable standard heuristics เปิดใช้งานมาตรฐานการวิเคราะห์พฤติกรรมการใช้งาน
- Enable enhanced heuristics based on, the behavior origin, age, and popularity of files เปิดใช้งานการตรวจสอบฐานข้อมูลเพื่อทำการวิเคราะห์พฤติกรรมการใช้งานที่เพิ่มขึ้นจากเดิม
- Enable maximum heuristics เปิดใช้งานการวิเคราะห์พฤติกรรมขั้นสูงสุด
- Warn when any new program executes that is not specifically whitelisted กำหนดให้มีการแจ้งเตือนเมื่อพบการทำงานของโปรแกรมที่ไม่ได้รับอนุญาต
- Enable Webroot Infrared เปิดการใช้งานฟังก์ชัน Infrared

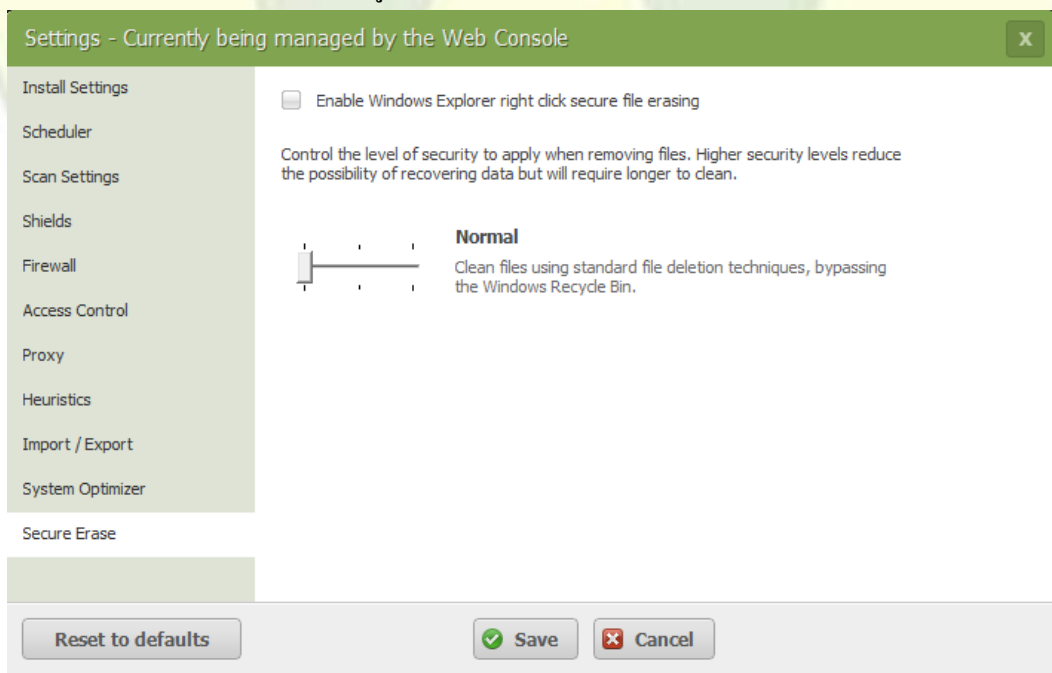
- **Import / Export** เป็นการถ่ายโอนการตั้งค่าไปยังคอมพิวเตอร์เครื่องอื่นและเป็นการนำเอาการตั้งค่าจากคอมพิวเตอร์เครื่องอื่นมาคัดลอกใหม่



- **System optimizer** สำหรับเลือกข้อมูลที่ต้องการทำความสะอาดเพื่อเพิ่มประสิทธิภาพอย่างไรใดอย่างหนึ่งในการทำงานของระบบ ทั้งนี้ โปรแกรม (Webroot) จะทำดิ่งข้อมูลของโปรแกรมต่างๆ ที่ผู้ใช้งานทำการติดตั้งบนเครื่องคอมพิวเตอร์โดยอัตโนมัติ

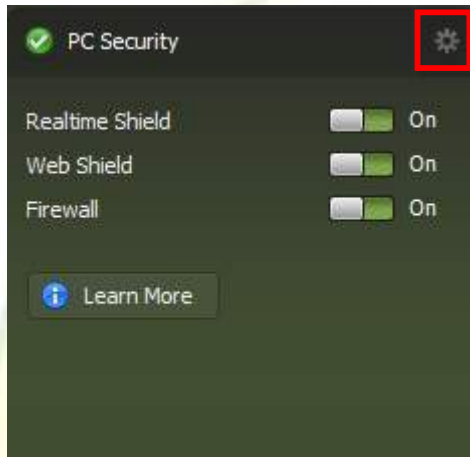


- **Secure Erase** การเพิ่มประสิทธิภาพในการลบไฟล์ เมื่อผู้ใช้งานได้ทำการลบไฟล์ ซึ่งระบบ จะทำการย้ายไปยังถังรีไซเคิล (Recycle Bin) และผู้ใช้งานสามารถ Restore กลับมาได้ หรือหากทำการ ถังถังขยะ (Recycle Bin) แต่ข้อมูลจะยังคงอยู่บนฮาร์ดดิสจนกว่าจะมีการเขียนทับด้วยข้อมูลอื่นๆ ทั้งนี้ การตั้งค่า Secure Erase ในการลบไฟล์ จะสามารถกำหนดไว้ที่เมนู Windows Explorer โดย ทาการคลิกขวาเพื่อลบไฟล์อย่าง คุณลักษณะ shredding นี้เป็นวิธีที่สะดวกเพื่อให้แน่ใจว่าไม่มีใคร สามารถ เข้าถึงไฟล์ด้วยเครื่องมือการกู้คืน โดยมีรายละเอียดดังนี้




- Enable Windows Explorer right click secure file erasing      เปิดใช้งานการลบไฟล์ด้วยโปรแกรม Webroot เมื่อทำการคลิกขวา
- ระดับการลบไฟล์แบ่งออกเป็น 3 ระดับดังนี้
  - Normal ระดับปกติ เป็นการลบไฟล์ที่ไม่ได้เขียนไฟล์ทับ
  - Medium ระดับปานกลาง เป็นการลบไฟล์และทำการเขียนไฟล์ทับจำนวน 3 ครั้ง
  - Maximumระดับสูงสุด เป็นการลบไฟล์และทำการเขียนไฟล์ทับจำนวน 7 ครั้ง

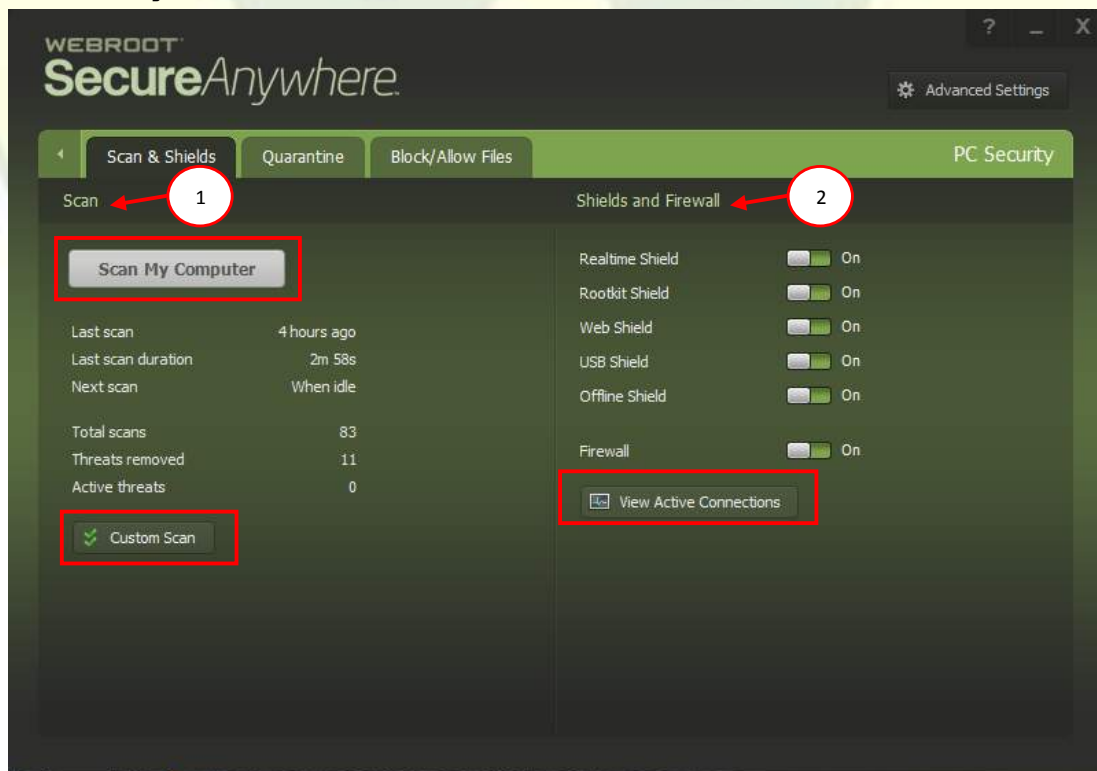
#### 4. PC security การกำหนดการป้องกันเครื่องคอมพิวเตอร์ของผู้ใช้งาน



- Realtime Shield      การป้องกันตลอดเวลา
- Web Shield          การป้องกันเว็บไซต์
- Firewall              การทำงานของ Firewall

การตั้งค่า PC Security เพิ่มเติมให้ทำการคลิก 

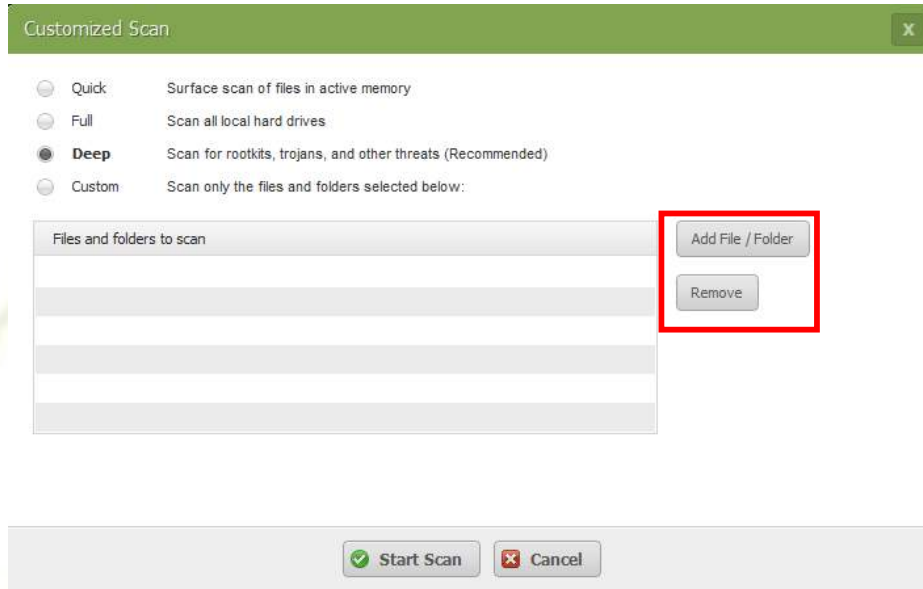
- แถบเมนู Scan & shields การตั้งค่าการสแกนและการป้องกันซึ่งมีรายละเอียดดังต่อไปนี้





## 1. Scan แสดงรายละเอียดผลการทำงานของโปรแกรม (Webroot)

- Scan My Computer การสแกนคอมพิวเตอร์โดยทันทีตามที่โปรแกรมได้กำหนดไว้
- Custom Scan การเลือกไดรฟ์และโฟลเดอร์ที่ผู้ใช้งานต้องการสแกน โดยมีรายละเอียดดังนี้

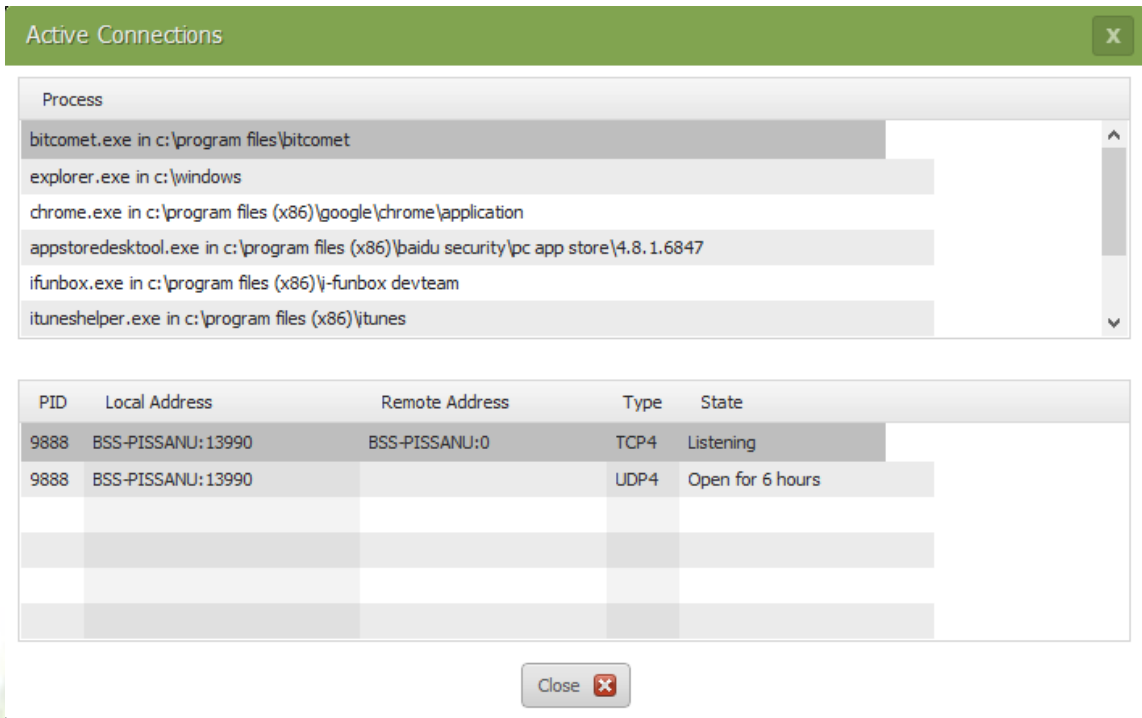


- Quick การสแกนไฟล์ที่ใช้งานอยู่ในหน่วยความจำอย่างรวดเร็ว
- Full การสแกนฮาร์ดดิสก์อย่างเต็มรูปแบบ
- Deep การสแกนหา Rootkit, โทรจันและภัยคุกคามอื่น ๆ อย่าง
- Custom จำกัดการสแกนไปยังโฟลเดอร์และไฟล์คลิกกำหนดเองปุ่มคลิกเพิ่มไฟล์ / โฟลเดอร์ปุ่มและคลิก Add เพื่อเลือกโฟลเดอร์และไฟล์ที่จะสแกน
- ปุ่ม Add File / Folder ทำการเพิ่มไฟล์ หรือโฟลเดอร์ที่ต้องการสแกน
- ปุ่ม Remove ทำการลบไฟล์ที่เลือกไว้

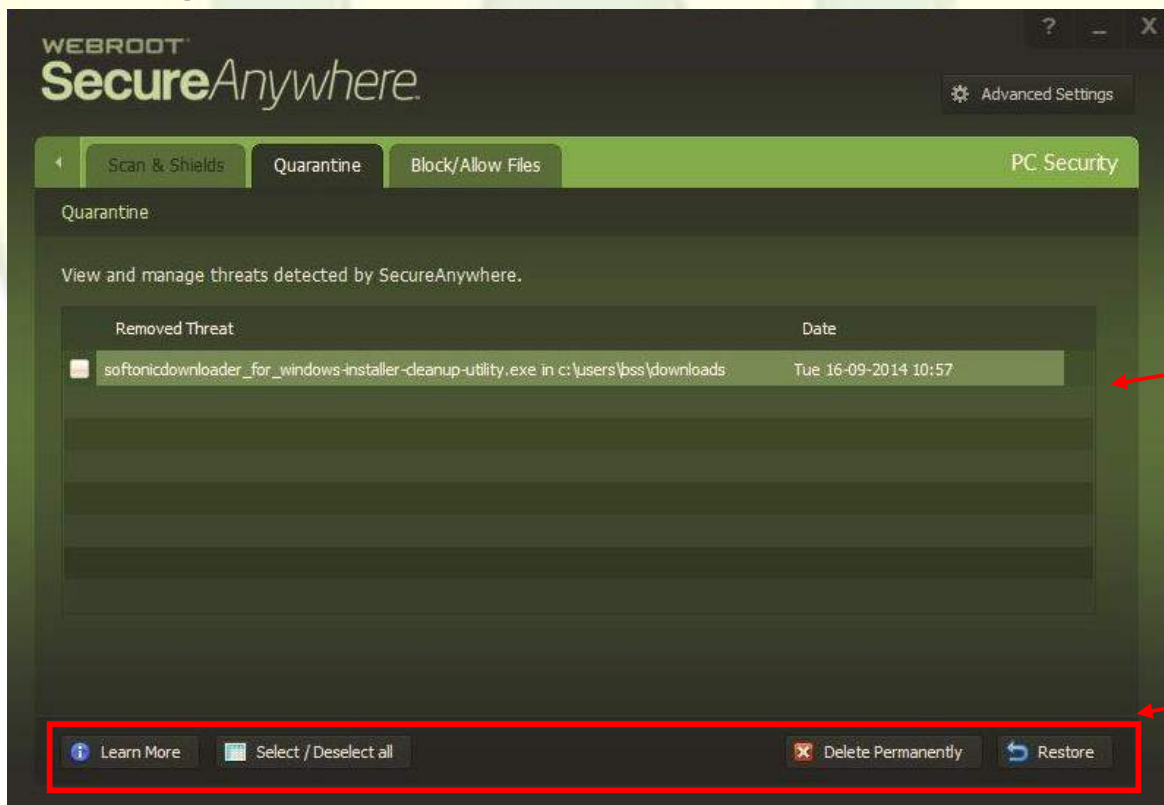
## 2. Shields and Firewall การป้องกันและการตั้งค่าไฟวอลล์

- Realtime Shield การป้องกันตลอดเวลา
- Rootkit Shield การป้องกัน Rootkit
- Web Shield การป้องกันเว็บไซต์
- USB Shield การป้องกัน USB
- Offline Shield การป้องกันแบบออฟไลน์
- Firewall เปิดการใช้งาน Firewall

- ปุ่ม View Active Connections ตั้งค่าการเชื่อมต่อของโปรแกรมต่างๆ



- แถบเมนู Quarantine รายการไฟล์ที่พบว่ามีความเสี่ยง

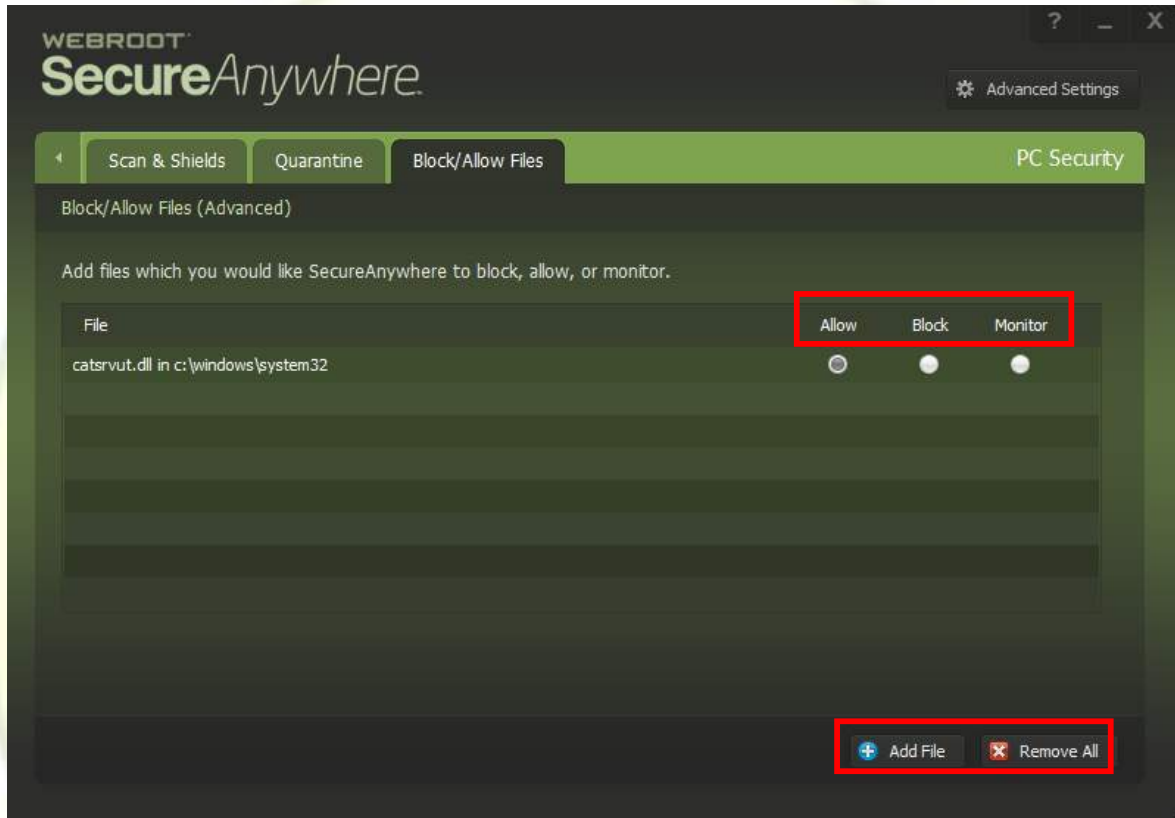


ส่วนที่ 1. รายการไฟล์ที่พบว่ามีความเสี่ยง

ส่วนที่ 2. การจัดการไฟล์

- |                           |                                    |
|---------------------------|------------------------------------|
| 2.1 Learn More            | ลิงค์เว็บไซต์ข่าวสาร               |
| 2.2 Select / Deselect all | การเลือกไฟล์หรือยกเลิกการเลือกไฟล์ |
| 2.3 Delete Permanently    | การลบไฟล์                          |
| 2.4 Restore               | การคืนค่าไฟล์                      |

- **แถบ Block / Allow File** การป้องกันหรืออนุญาตไฟล์ที่โปรแกรม (Webroot) ได้ทำการตรวจพบ



- |                                       |  |
|---------------------------------------|--|
| <input type="radio"/> Allow           | ละเว้นไฟล์ระหว่างการสแกนและการป้องกัน  |
| <input type="radio"/> Block           | ป้องกันไฟล์ออกจากระบบ  |
| <input type="radio"/> Monitor         | ตรวจสอบโปรแกรมว่าถูกต้องตามกฎหมายหรือเป็นโปรแกรมที่เกี่ยวข้องกับซอฟต์แวร์ที่อาจเป็นอันตรายเพื่อป้องกันหรืออนุญาต |
| <input type="radio"/> ปุ่ม Add File   | ทำการเพิ่มไฟล์ที่ต้องการดำเนินการ  |
| <input type="radio"/> ปุ่ม Remove All | ทำการลบไฟล์ที่เลือกไว้   |

## 5. Identity Protection การป้องกันข้อมูล

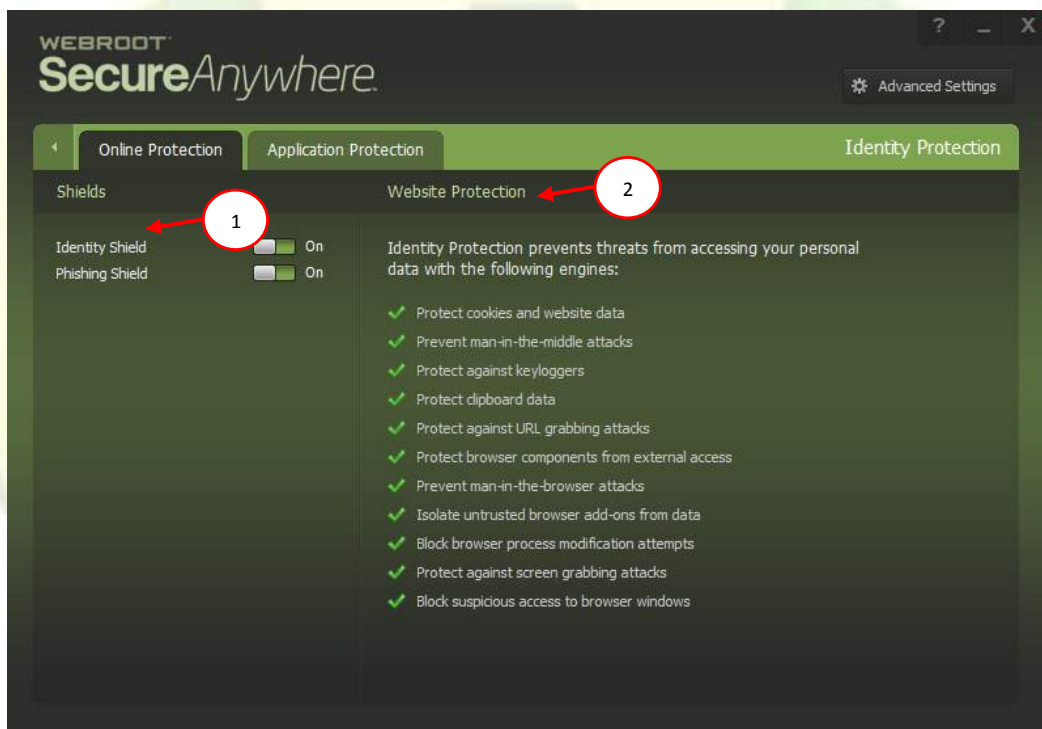


- Identity Shield เปิดการป้องกัน
- Phishing Shield เปิดการป้องกันการโจรกรรมข้อมูล
- Learn More ข่าวสารข้อมูลเพิ่มเติม

การตั้งค่า Identify Protection เพิ่มเติมให้ทำการคลิกเลือก



- Online Protection การป้องกันข้อมูลเมื่อคอมพิวเตอร์อยู่ในสถานะออนไลน์แบ่งออกเป็น 2 เมนูดังนี้

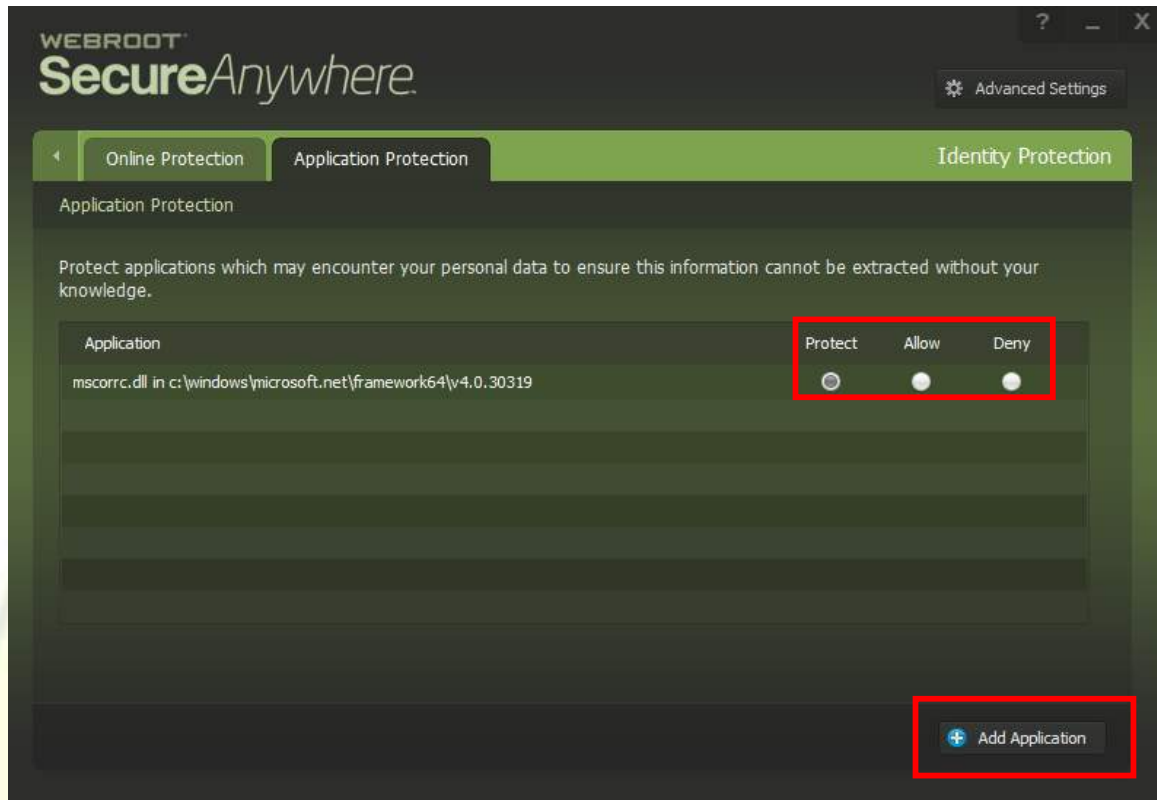


### 1. Shields

- Identity shields เปิดใช้งานการป้องกัน
- Phishing shields เปิดใช้งานการป้องกันการโจรกรรมข้อมูล

### 2. Website Protection แสดงรายละเอียดต่างๆ ที่มีการป้องกัน

- **แถบเมนู Application protection** การป้องกันโปรแกรมต่างๆ โดยสามารถจัดการโปรแกรมให้ทำการป้องกัน, ติดตาม หรืออนุญาตให้ใช้งานโดยไม่มีการติดตาม ซึ่งมีรายละเอียดดังนี้



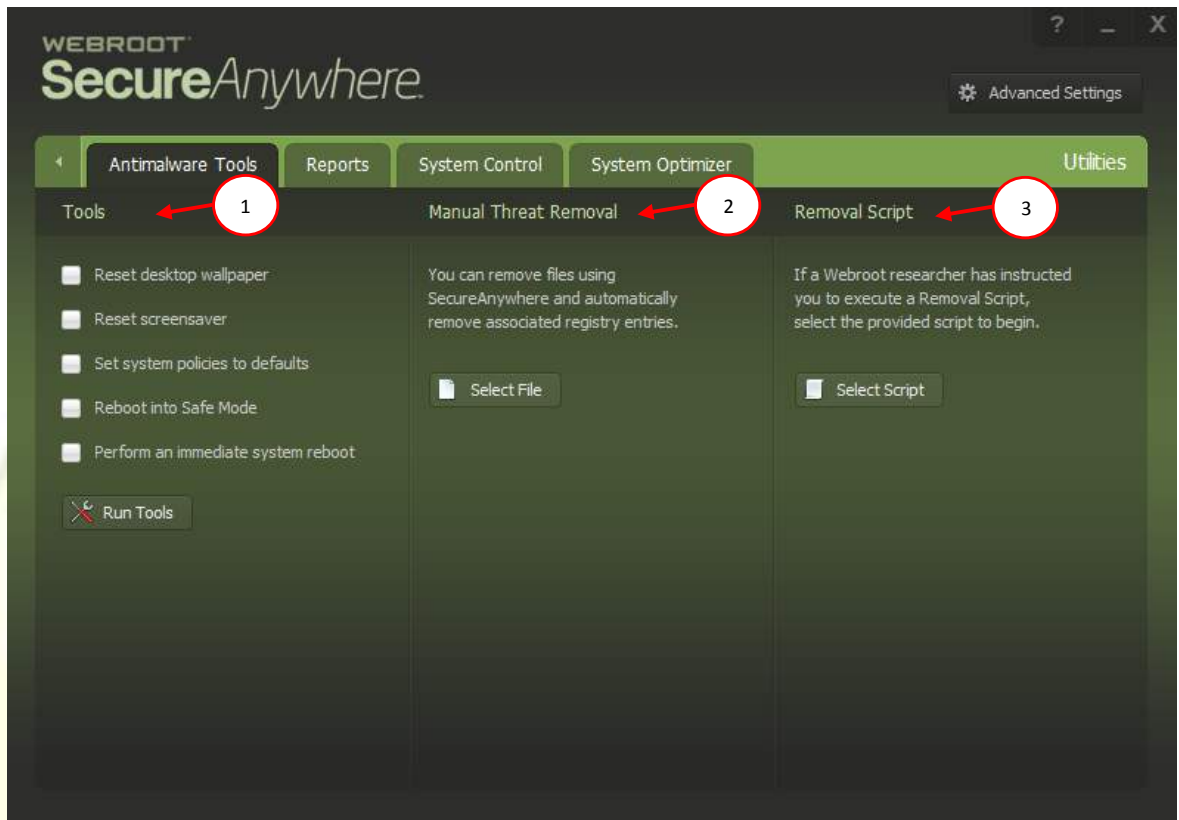
- **Protect** การติดตามพฤติกรรมการใช้งานเพื่อป้องกันซอฟต์แวร์ที่อาจเป็นอันตรายได้
- **Allow** การอนุญาตให้โปรแกรมที่ถูกเลือกไว้สามารถทำงานได้โดยไม่ต้องมีการตรวจสอบ
- **Deny** การใช้งานที่ถูกปฏิเสธไม่สามารถดูหรือเก็บข้อมูลที่มีการป้องกันในระบบ แต่อย่างอื่นสามารถทำงานได้ตามปกติ
- **ปุ่ม Add Application** เลือกโปรแกรมที่ต้องการให้ Webroot ดำเนินการป้องกันไฟล์

## 6. Utilities แสดงรายละเอียดประสิทธิภาพของระบบ



- **Optimize Now** การดำเนินการเพิ่มประสิทธิภาพของระบบ
- **Report** การจัดทำรายงาน
- **System Control** การควบคุมดูแลระบบ

- แถบ Antimalware Tools การจัดการเกี่ยวกับซอฟต์แวร์ที่อาจเป็นอันตรายต่อคอมพิวเตอร์ ซึ่งมีรายละเอียดดังนี้



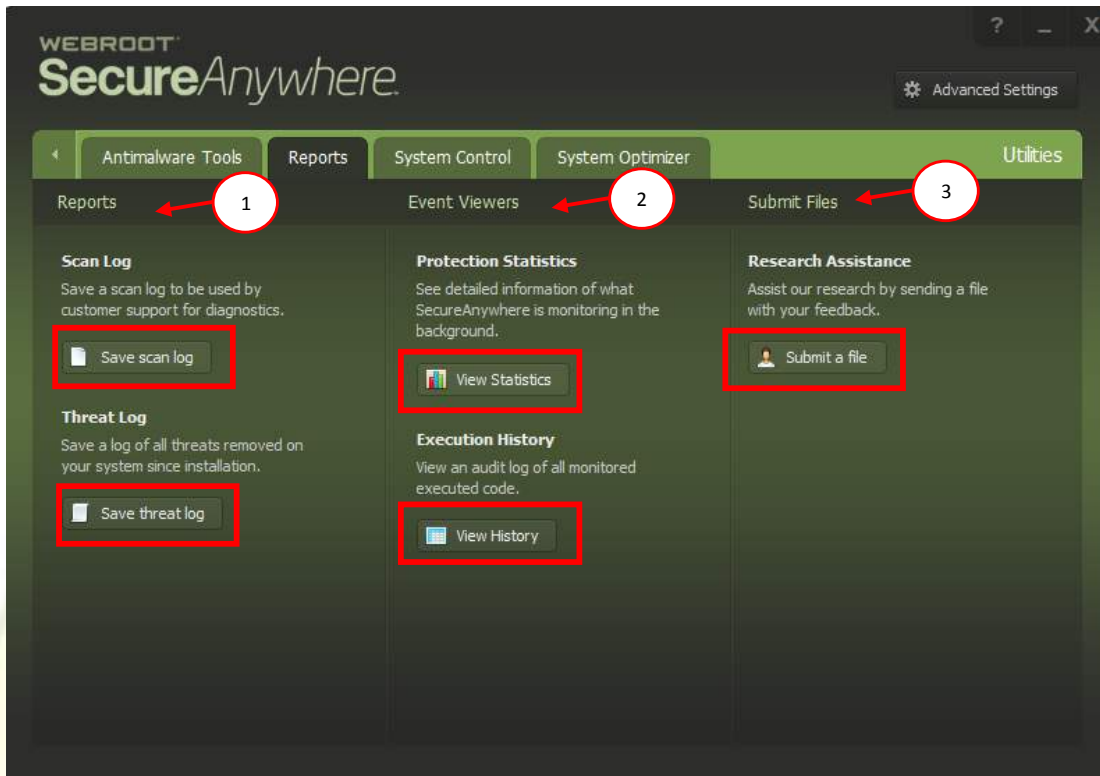
### ส่วนที่ 1 Tools

- |  |  |
|--|--|
| <input type="radio"/> Reset desktop                      | ตั้งค่าหน้าจอหลักใหม่                                  |
| <input type="radio"/> Reset screensaver                  | ตั้งค่า Screen Saver ใหม่                              |
| <input type="radio"/> Set system policies to defaults    | ตั้งค่าข้อกำหนด (Policy) ของระบบคอมพิวเตอร์เป็นค่าเดิม |
| <input type="radio"/> Reboot into Safe Mode              | เริ่มระบบใหม่ใน Safe mode                              |
| <input type="radio"/> Perform an immediate system reboot | ดำเนินการเริ่มระบบใหม่โดยทันที                         |

ส่วนที่ 2 Manual threat Remove สามารถเลือกลบไฟล์ที่มีความเสี่ยงรวมไปถึงคำริจิสทรีที่เกี่ยวข้อง

ส่วนที่ 3 Remove Script สามารถเลือกลบสคริปต์และกลับไปสคริปต์ค่าเริ่มต้น

- แถบ Report การจัดทำรายงาน มีรายละเอียดดังนี้

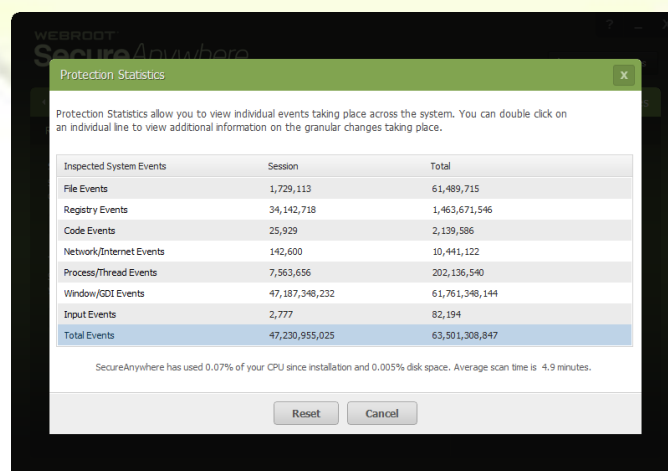


#### ส่วนที่ 1 Report รายงานการดำเนินการ

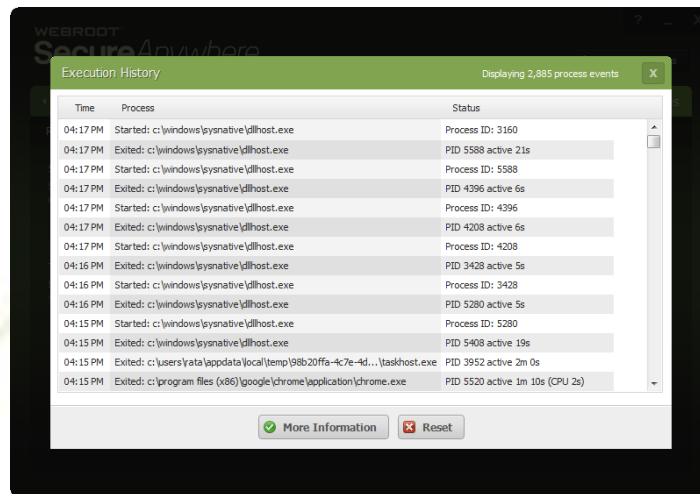
- Scan Log การบันทึก Log ที่โปรแกรม (Webroot) ได้ทำการสแกน
  - Save Scan Log (ทำการบันทึก Log ที่สแกน)
- Threat Log การบันทึกการลบไฟล์ที่อาจเป็นอันตรายจากระบบตั้งแต่ลง โปรแกรม
  - Save Threat Log (ทำการบันทึก Log ที่ลบไฟล์ที่อาจเป็นอันตราย)

#### ส่วนที่ 2 Event Viewers แสดงเหตุการณ์ต่างๆ

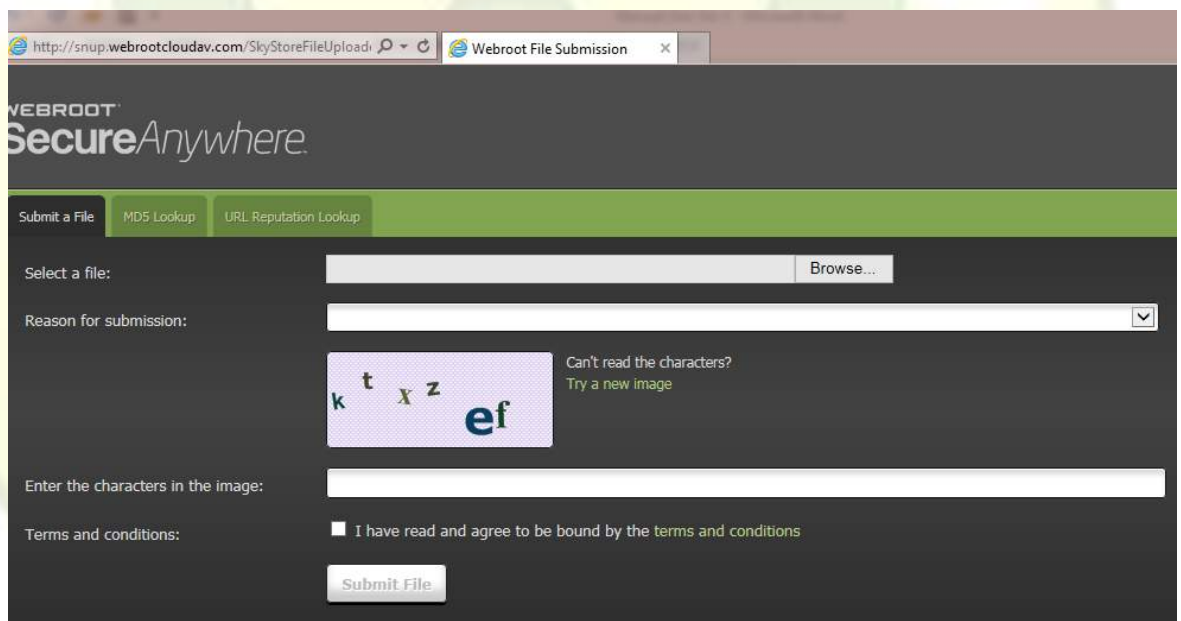
- Protection Statistics แสดงรายละเอียดที่โปรแกรม (Webroot) ได้ทำการป้องกัน
  - View Statistics แสดงสถิติการดำเนินการ



- Execution History แสดงประวัติการเข้าดำเนินการตรวจสอบรหัส
  - View History แสดงประวัติการดำเนินการ

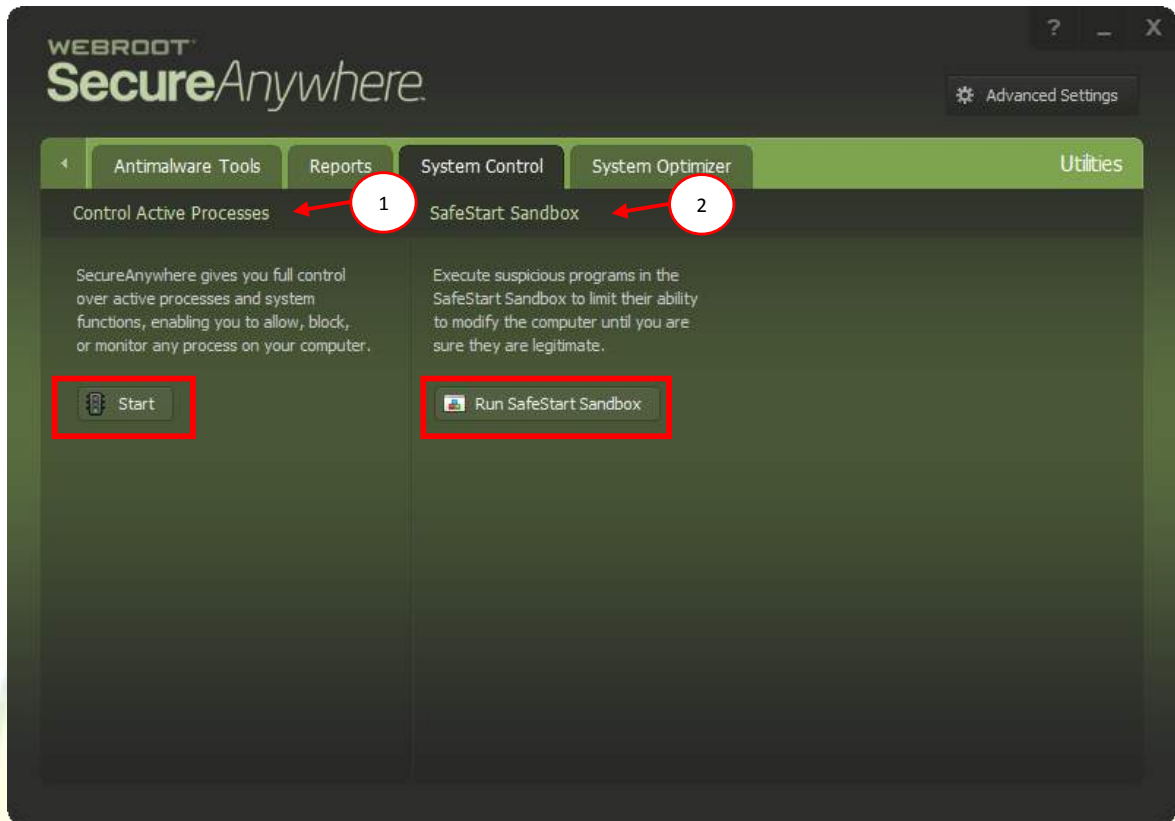


- Submit files คือ การส่งไฟล์ไปให้ Webroot ช่วยวิเคราะห์ความเสี่ยงที่อาจเกิดขึ้นต่อคอมพิวเตอร์
  - Submit a file การส่งไฟล์เพื่อทำการวิเคราะห์อันตรายเสี่ยง



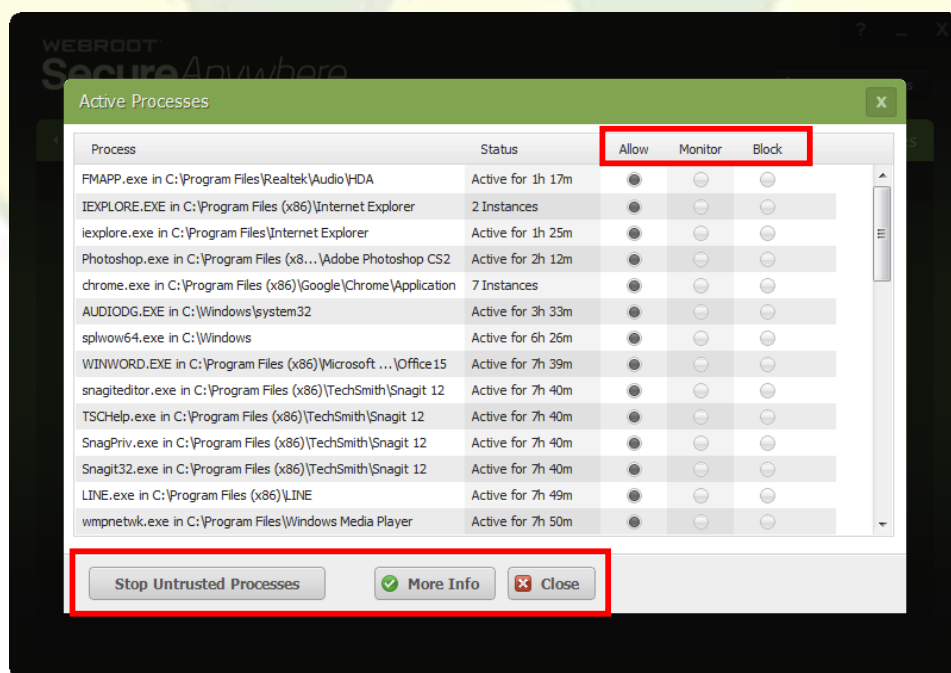


- แถบ System Control ควบคุมและดูแลการทำงานของเครื่องคอมพิวเตอร์ โดยมีรายละเอียดดังนี้

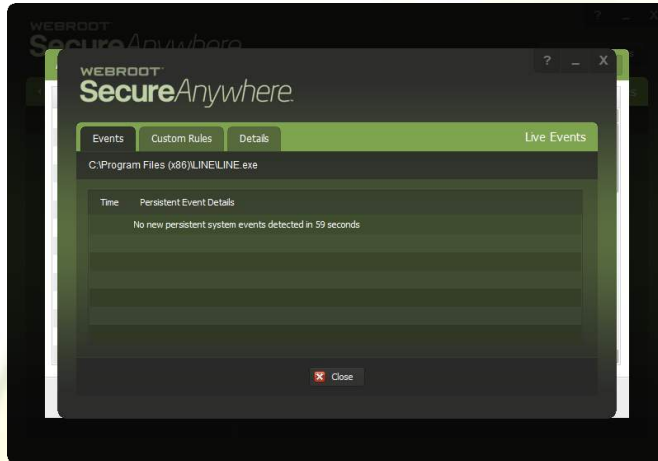


ส่วนที่ 1 Control Active Processes กำหนดกระบวนการทำงานของเครื่องคอมพิวเตอร์ อาทิ อนุญาตให้เปิดใช้งาน โปรแกรม, ปิดกั้นหรือติดตามกระบวนการทำงานของเครื่องคอมพิวเตอร์

- Start กำหนดการทำงานของโปรแกรมในคอมพิวเตอร์ โดยมีรายละเอียดดังนี้



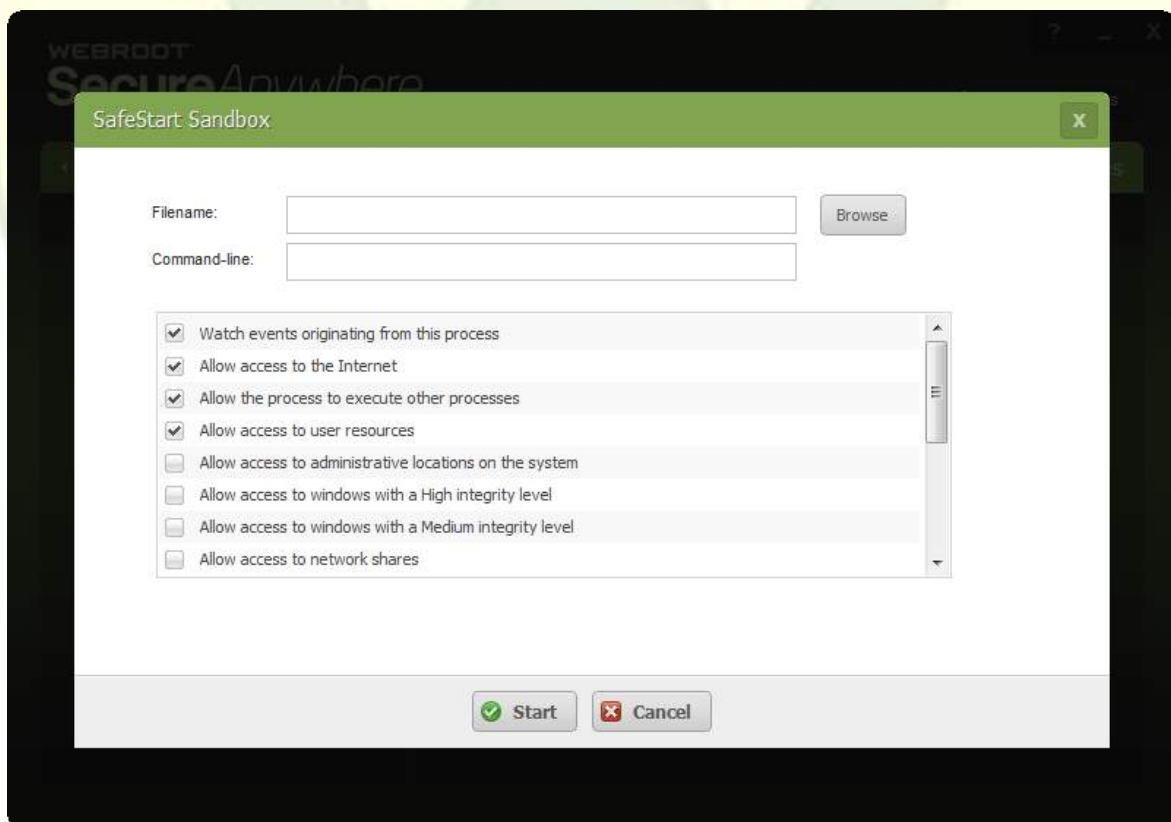
- Allow อนุญาตให้โปรแกรมทำงาน
- Monitor ตรวจสอบการทำงานของโปรแกรม
- Block ป้องกันการทำงานของโปรแกรม
- ปุ่ม Stop Untrusted Processes หยุดกระบวนการที่ไม่น่าเชื่อถือออกจากระบบ
- ปุ่ม More Info แสดงรายละเอียดข้อมูลของโปรแกรม



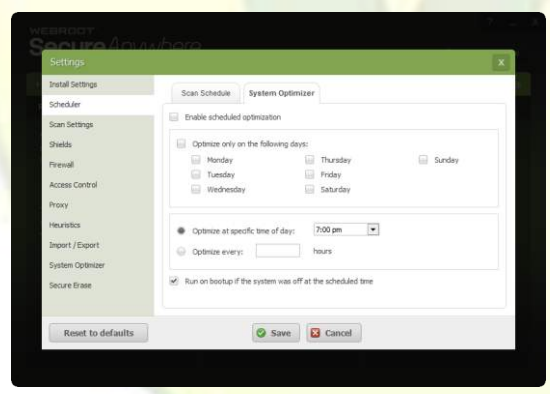
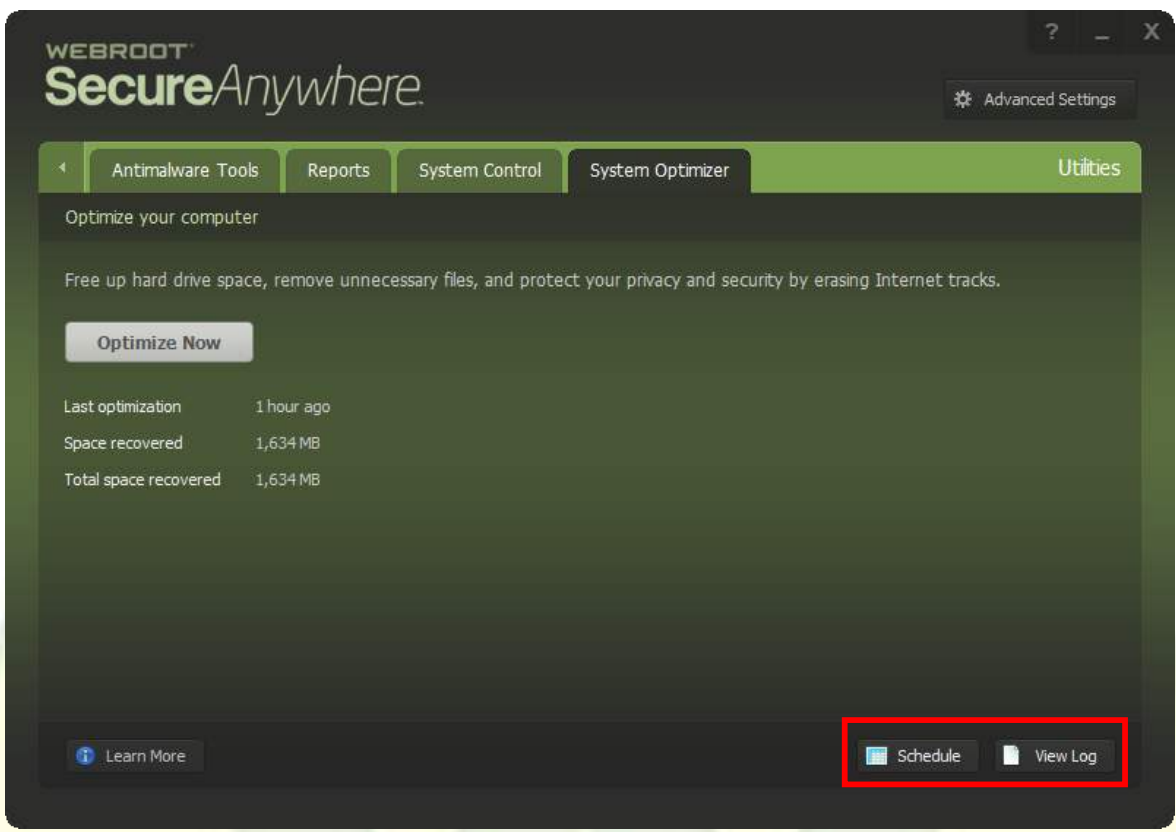
- Events แสดงเหตุการณ์ต่างๆ
- Custom Rules แสดงกฎข้อบังคับที่ได้กำหนดไว้
- Details แสดงรายละเอียดของโปรแกรม

- ปุ่ม Close ทำการปิดหน้าต่างโปรแกรม

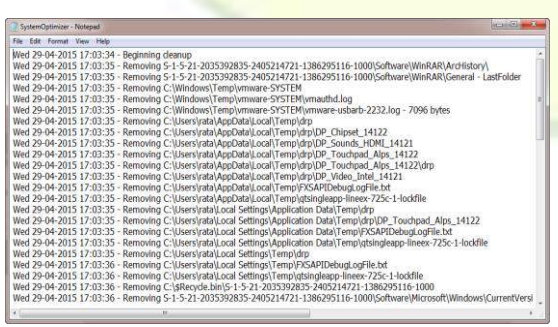
ส่วนที่ 2 SafeStart Sandbox การนำโปรแกรมทำการทดสอบตามข้อกำหนดที่ได้เลือกไว้



- แถบเมนู System Optimizer การเริ่มกระบวนการเพิ่มประสิทธิภาพการทำงานให้กับเครื่องคอมพิวเตอร์

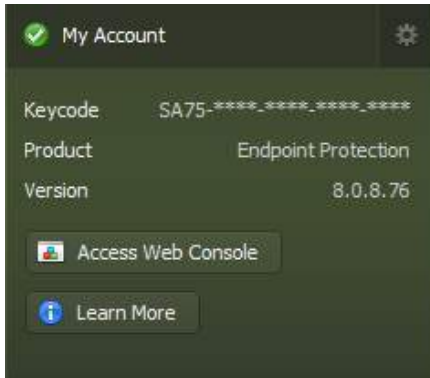


- ปุ่ม Schedule การกำหนดช่วงเวลาในการทำงาน



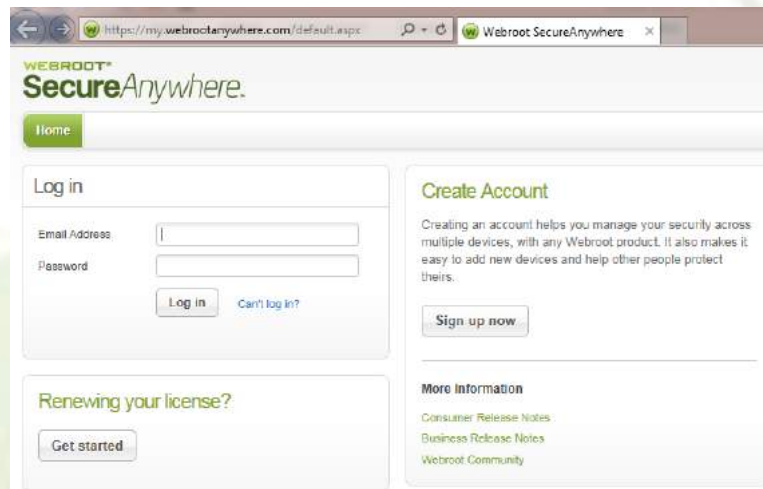
- ปุ่ม View Log แสดงรายละเอียดที่โปรแกรมได้ทำการเก็บ Log

## 7. My Account แสดงรายละเอียดและข้อมูลที่เกี่ยวข้องกับโปรแกรม โดยมีรายละเอียดดังนี้

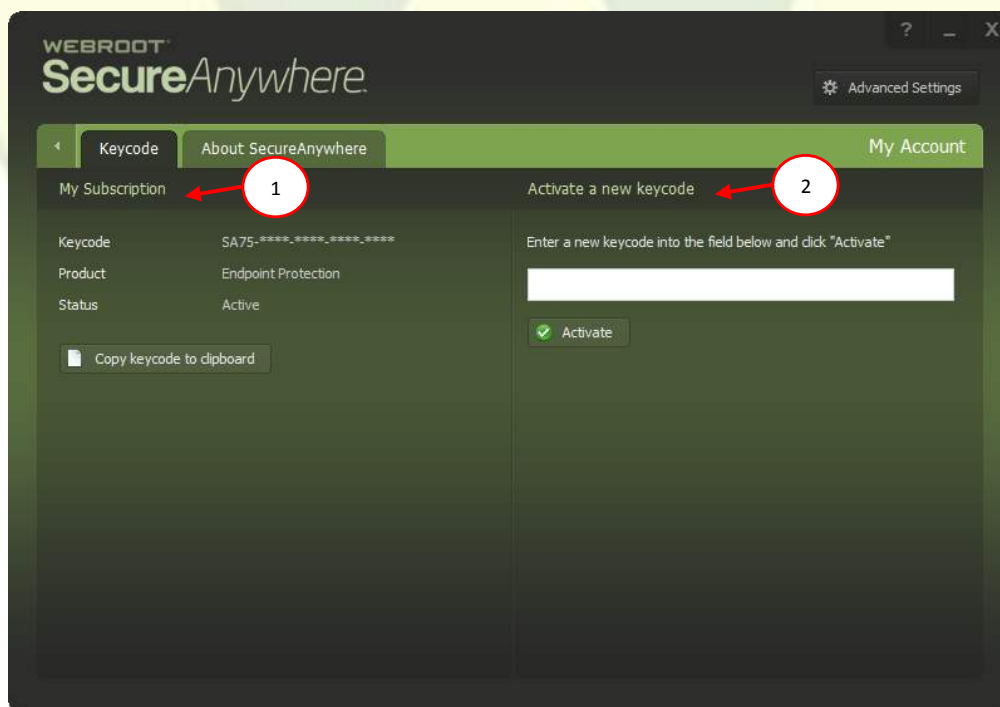


- Keycode แสดง Keycode
- Product แสดงชนิดโปรแกรมของ Webroot
- Version แสดงรุ่นของ Webroot

- ปุ่ม Access Web Console      ลิงค์ทำการเชื่อมต่อหน้าเว็บเข้าระบบของ Webroot



การตั้งค่า My Account เพิ่มเติมให้ทำการคลิกเลือก



- แถบเมนู Keycode แสดงรายละเอียดของ โปรแกรม Webroot

#### ส่วนที่ 1 My Subscription

- Keycode แสดงรายละเอียด Keycode
- Product แสดงชนิดโปรแกรมของ Webroot
- Status แสดงรุ่นของ Webroot
- ปุ่ม Copy keycode to clipboard ปุ่มทำการคัดลอก Keycode

#### ส่วนที่ 2 Activate a new keycode สำหรับทำการ Activate keycode

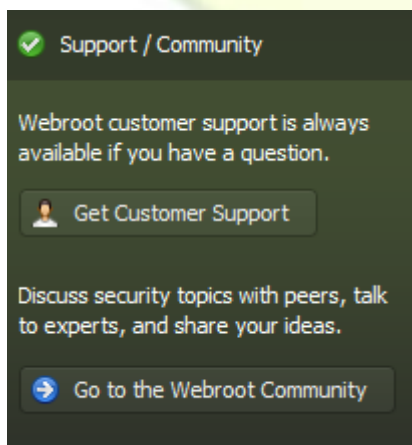
- แถบที่ 2 About SecureAnywhere



#### ส่วนที่ 1 Version แสดงรุ่นของโปรแกรม Webroot

#### ส่วนที่ 2 Legal แสดงรายละเอียดเกี่ยวกับกฎหมาย

### 8. Support / Community การสนับสนุนให้ความช่วยเหลือและข่าวสาร



- Get Customer Support ขอความช่วยเหลือจากเจ้าหน้าที่ Technical
- Go to the Webroot Community เยี่ยมเว็บไซต์ของ Webroot
-