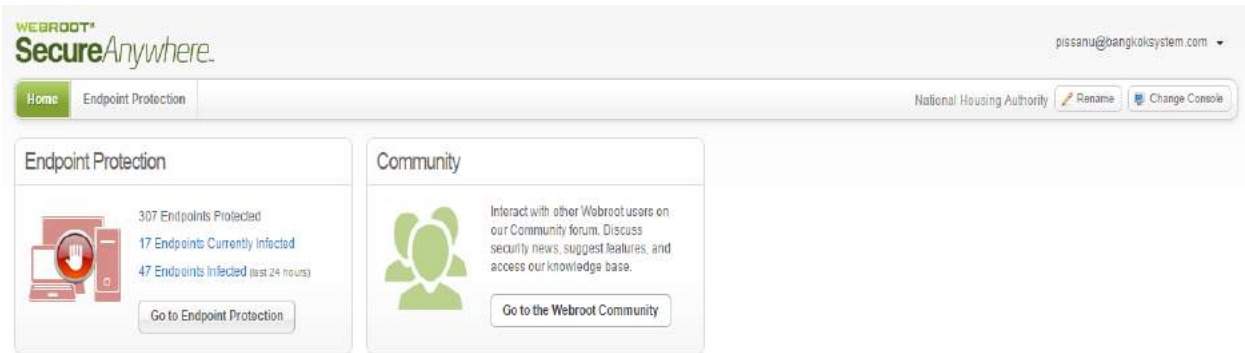


Console management



1.Home

แถบเมนูจะมี 2 เมนู ได้แก่

1.1 Endpoint Protection

- แสดง Endpoints ทั้งหมดที่ได้มีการติดตั้ง
- แสดง Endpoints ในปัจจุบันที่มีการตรวจเจอไฟล์ที่มีความเสี่ยง
- แสดง Endpoints ภายในภายใน 24 ชั่วโมงล่าสุดที่มีการตรวจสอบเจอไฟล์ที่มีความเสี่ยง

1.2 Community

กลุ่มแลกเปลี่ยนความรู้และปัญหาที่เกิดขึ้นของ Webroot Secure AnyWhere

2.Status

Hostname	Policy	Group	Status	Last Infected	Blocked Programs
1 M0010052008	User_NHA View	BU1_8	Protected	Dec 23rd 2014, 10:01	View
2 R3217053134	User_NHA View	Bu2_2	Infected	Dec 23rd 2014, 09:59	View
3 R1942053050	User_NHA View	Branch Office	Protected	Dec 23rd 2014, 09:58	View
4 R188-605-3028	User_NHA View	Branch Office	Infected	Dec 23rd 2014, 09:55	View
5 M0010051954	User_NHA View	BU1_10	Protected	Dec 23rd 2014, 09:31	View
6 R3217053063	User_NHA View	Bu4_2	Protected	Dec 23rd 2014, 09:30	View
7 R3217053215	User_NHA View	BU1_11	Infected	Dec 23rd 2014, 09:21	View
8 R3217053136	User_NHA View	Bu2_2	Infected	Dec 23rd 2014, 08:48	View
9 M0010051959	User_NHA View	Bu5_2	Protected	Dec 23rd 2014, 08:45	View
10 R3217053187	User_NHA View	Bu7_3	Overran	Dec 23rd 2014, 08:42	View

2.1 Status จะมีการแจ้งเตือน Endpoint ที่ตรวจพบไฟล์ที่มีความเสี่ยงและแนะนำให้ตรวจสอบ Endpoint ว่าจะอยู่ในกลุ่มนโยบายและรายละเอียดของไฟล์ที่มีความเสี่ยง และสามารถที่คลิกเข้าไปดูรายละเอียดของการแจ้งเตือนว่า Endpoint เครื่องไหนที่แจ้งเตือน สามารถที่ทำการ Clean up หรือ Restore และ Override ได้

1.3 Endpoint encountering threats

จะแสดงกราฟรายละเอียดการตรวจสอบเจอไฟล์ที่มีความเสี่ยงของ Endpoint ภายใน 7 วันล่าสุดและสามารถที่คลิกเข้าไปดูรายละเอียดของแต่ละกราฟ สามารถที่ทำการ Clean up หรือ Restore และ Override ได้

1.4 Agent Version Spread

จะแสดงเวอร์ชันทั้งหมดของ Endpoint และสามารถที่คลิกเข้าไปดูรายละเอียดของแต่ละ Endpoint ได้

1.5 Endpoint Activity

จะแสดงสถานะการตรวจสอบ Endpoint สถานะการออนไลน์และออฟไลน์และจำนวน Endpoint ทั้งหมด

1.6 Webroot Threat Blog

จะแสดงรายละเอียดข้อมูลที่มีการปรับปรุงล่าสุด Blog ของ Webroot

1.5 Help and Support

คู่มือการใช้งานของ Webroot และ วิดีโอแนะนำการใช้งานและร่วมไปถึงข่าวในการปรับปรุงไฟล์ที่มีความเสี่ยงและภัยคุกคามต่างๆ

Polices

Policy Name	Policy Description	Date Created	Draft Changes
AVPolicy	AVPolicy	Dec 28th 2014, 16:07	No
Recommended Defaults	Recommended setup with protection and remediation		
Recommended Server Defaults	Recommended setup for servers, protection enabled		
Silent Audit	Non-remediating Security Audit with limited protection enabled		
test	test	Nov 21st 2014, 15:41	Yes
Unmanaged	This policy is for all PCs that are user managed		

Group Name	Number of endpoints	Description
Select a policy to populate this window		

เมื่อกำหนดค่าการป้องกันและตรวจสอบเลือกหนึ่งในนโยบายเริ่มต้นของ กำหนดนโยบายการตั้งค่า SecureAnywhere บนอุปกรณ์ปลายทาง เช่น ตารางสแกนและพฤติกรรมการป้องกัน สามารถใช้นโยบายเริ่มต้นหรือคุณสามารถกำหนดนโยบายมากขึ้นและกำหนดให้กับอุปกรณ์ปลายทางตัวอย่างเช่น อาจต้องการที่จะให้ผู้บริหารระบบการควบคุมมากขึ้นกว่าที่จะพนักงานคนอื่น ๆ ในกรณีที่สามารสร้างนโยบายใหม่สำหรับผู้ดูแลระบบและให้ Endpoint

อื่น ๆ เกี่ยวกับนโยบายการเริ่มต้น

โดยจะแสดงเมนูดังนี้

- **Create** คือ เป็นการสร้าง Policy ขึ้นมาใหม่
- **Delete** คือ เป็นการลบ policy
- **Rename** คือ เป็นการตั้งชื่อให้กับ policy นั้นๆ
- **Copy** คือ สามารถทำการคัดลอก policy
- **Set default** คือ สามารถที่จะกำหนดการตั้งค่าให้ policy เป็นค่าเริ่มต้น
- **Import** คือ สามารถที่จะ import ค่า configure policy
- **Export** คือ สามารถที่จะ export ค่า configure policy

หมายเหตุ Policy Unmanaged ไม่สามารถที่จะทำการแก้ไขได้ (user จะทำการจัดการเองทั้งหมด)

โดยมีการตั้งค่า Policy ดังนี้

3.1 Basic configuring

Polices Details	รายละเอียด
Show a secure Anywhere shortcut on the desktop	แสดงที่หน้าจอ
Show a system tray icon	แสดงที่แถบเมนู
Show a splash screen on bootup	แสดงตอนเริ่มต้นคอมพิวเตอร์
Show SecureAnywhere in the Start Menu	แสดงที่แถบ Star Menu
Show SecureAnywhere in Add/Remove Programs	แสดงที่ Add/Remove Programs
Show SecureAnywhere in the Windows Action Center	แสดงที่ Windows Action Center
Hide the SecureAnywhere keycode and subscription information on-screen	ซ่อน Key code ในโปรแกรม
Automatically download and apply update	ดาวน์โหลดและปรับปรุง เวอร์ชัน โดยอัตโนมัติ
Operate background functions using fewer CPU resources	การทำงานของโปรแกรมให้ใช้ทรัพยากรน้อยกว่า CPU
Favor low disk usage over verbose logging (fewer details stored in logs)	การใช้งานดิสก์ให้ต่ำ
Lower resource usage when intensive applications or games are detected	เมื่อมีการใช้งานทรัพยากรมากหรือมีการเล่นเกมส์ โปรแกรมจะใช้ทรัพยากรที่ต่ำกว่า
Allow SecureAnywhere to be shut down manually	สามารถจะปิดโปรแกรมด้วยตนเองได้
Store Execution History details	เก็บ Log การทำงานของโปรแกรมทั้งหมด
Poll interval	ช่วงเวลาในการสำรวจ
Polices details	รายละเอียด

Enable Scheduled Scans	เปิดการใช้สแกนตามระยะเวลาที่กำหนด
Scan Frequency	ช่วงเวลาในการสแกน
Time	เวลา
Scan on bootup if the computer is off at the scheduled time	สแกนเมื่อบูตเครื่องคอมพิวเตอร์หากเครื่องถูกปิดในเวลาที่กำหนด
Hide the scan progress window during scheduled scans	ซ่อนหน้าต่างความคืบหน้าการสแกนที่กำหนดไว้
Only notify me if an infection is found during a scheduled scan	แจ้งเตือนให้ทราบถ้าพบไวรัสในช่วงการสแกนที่กำหนดไว้เท่านั้น
Do not perform scheduled scans when on battery power	ห้ามทำการกำหนดการสแกนเมื่อใช้พลังงานจากแบตเตอรี่
Do not perform scheduled scans when a full screen application or game is in open	ห้ามทำการกำหนดการสแกนเมื่อโปรแกรมประยุกต์หรือเกมส์ทำงานอยู่
Randomize the time of scheduled scans up to one hour for distributed scanning	สุ่มเวลาของการสแกนที่กำหนดไว้ถึงหนึ่งชั่วโมงสำหรับการสแกน

3.2 Scan schedule

3.3 Scan settings

Polices details	รายละเอียด
Enable Realtime Master Boot Record (MBR) Scanning	เปิดการใช้งานสแกน Master Boot Record (MBR) ตลอดเวลา
Enable Enhanced Rootkit Detection	เปิดใช้งานการตรวจหา Rookit ที่เพิ่มขึ้น
Enable " right-click " scanning in Windows Explorer	เปิด " คลิกขวา " สแกนใน Windows Explorer
Update the currently scanned folder immediately as scanned	อัปเดตสแกนโฟลเดอร์ปัจจุบันทันทีที่สแกน
Polices Details	รายละเอียด

Favor low memory usage over fast scanning	การใช้งานหน่วยความจำที่ต่ำเมื่อใช้การสแกนแบบรวดเร็ว
Favor low CPU usage over fast scanning	การใช้งาน CPU ต่ำเมื่อใช้การสแกนแบบรวดเร็ว
Save non-executable file details to scan logs	บันทึกรายละเอียดไฟล์ที่ไม่ทำงานลงในรายละเอียดการสแกน
Save the “ Authenticating File “ popup when a new file is scanned on-execution	แสดงการดำเนินการ ป๊อปอัพ "Authenticating Files" เมื่อไฟล์ใหม่ถูกสแกน
Scan archived files Automatically reboot during cleanup without prompting	สแกนไฟล์ที่เก็บไว้และรีทสตาร์ทเครื่องโดยอัตโนมัติโดยระหว่างการทำความสะอาดเสร็จโดยไม่ต้องแจ้งเตือน
Never reboot during malware cleanup	ไม่ต้องรีทสตาร์ทเครื่องใหม่โดยระหว่างการทำความสะอาดมัลแวร์เสร็จเรียบร้อยแล้ว
Automatically remove threats found during background scans	ลบภัยคุกคามโดยอัตโนมัติที่พบในระหว่างการสแกน
Enable Enhanced Support	เปิดใช้งานการสนับสนุนการช่วยเหลือ
Show Infected Scan Results	แสดงผลการสแกนที่พบภัยคุกคาม
Detect Possibly Unwanted Applications (PUAs) as malicious	ตรวจจับโปรแกรมที่ไม่พึงประสงค์อาจจะเป็น (Puas) ที่เป็นอันตราย

3.4 Self Protection

Polices Details	รายละเอียด
Enable self protection response cloaking	เปิดใช้งานการป้องกันตัวเอง
Self protection Level	ระดับการป้องกันตนเอง

3.5 Heuristics

Polices Details	รายละเอียด
Enable infrared	เปิดใช้งาน
Local heuristics	
Heuristics	
Advanced Heuristics	
Popularity heuristics	
USB heuristics	
Heuristics	
Advanced Heuristics	
Popularity heuristics	
Internet heuristics	
Heuristics	
Advanced Heuristics	
Popularity heuristics	
Network heuristics	
Heuristics	
Advanced Heuristics	
Popularity heuristics	
CD/DVD heuristics	
Heuristics	
Advanced Heuristics	
Popularity heuristics	
Offline heuristics	

Polices Details	รายละเอียด
Heuristics	
Advanced Heuristics	
Popularity heuristics	

3.6 Real Time Shield

Polices Details	รายละเอียด
Realtime Shield Enabled	เปิดการใช้งานการป้องกันตลอดเวลา
Enable Predictive Offline Protection from the central Secure-AnyWhere database	เปิดใช้งานการป้องกันแบบออฟไลน์จากฐานข้อมูลกลาง
Remember actions on blocked files	จดจำการดำเนินการไฟล์ที่ถูกปิดกั้น
Automatically quarantine previously blocked files	บล็อกไฟล์ที่มีความเสี่ยงให้เป็นไฟล์ที่ถูกปิดกั้นโดยอัตโนมัติ
Automatically block files when detected on execution	เมื่อตรวจพบไฟล์ที่มีความเสี่ยงจะดำเนินการป้องกันไฟล์โดยอัตโนมัติ
Scan files when written or modified	สแกนไฟล์เมื่อเขียนหรือแก้ไข
Block threats automatically if no user is logged in	บล็อกไฟล์อัตโนมัติถ้าผู้ใช้งานไม่มีการเข้าสู่ระบบ
Show real time event warnings	โชว์การแจ้งเตือนเหตุการณ์ตลอดเวลา
Show real time block modal alerts	โชว์การแจ้งเตือนการบล็อกตลอดเวลา
Show real time block notifications	โชว์การแจ้งเตือนการบล็อกตลอดเวลา

3.7 Behavior Shield

Polices Details	รายละเอียด
Behavior Shield Enabled	เปิดการป้องกันพฤติกรรม
Assess the intent of new programs before allowing them to execute	ประเมินความตั้งใจของโปรแกรมใหม่ก่อนที่จะปล่อยให้ดำเนินการต่อ
Enable advanced behavior interpretation to identify complex threats	เปิดการใช้งานการตรวจสอบพฤติกรรมขั้นสูงเมื่อระบุภัยคุกคามที่ซับซ้อน
Track the behavior of untrusted programs for advanced threat removal	ติดตามพฤติกรรมของโปรแกรมที่ไม่น่าเชื่อถือในการจัดการภัยคุกคาม
Automatically perform the recommended action instead of showing warning messages	ดำเนินการโดยอัตโนมัติในข้อความแนะนำแทนข้อความเตือน
Warn if untrusted programs attempt low-level system modifications when offline	เตือนถ้าโปรแกรมที่ไม่น่าเชื่อถือพยายามปรับเปลี่ยนในระดับต่ำเมื่อทำงานในระบบออฟไลน์

3.8 Core System Shield Enabled

Polices Details	รายละเอียด
Core System Shield Enabled	เปิดการป้องกันระบบปฏิบัติการ
Assess system modifications before they are allowed to take place	ประเมินการปรับเปลี่ยนระบบปฏิบัติการก่อนที่จะได้รับอนุญาตให้ดำเนินการ
Detect and repair broken system components	ตรวจสอบและซ่อมแซมระบบปฏิบัติการที่มีความเสียหาย
Prevent untrusted programs from modifying kernel memory	ป้องกันไม่ให้โปรแกรมที่ไม่น่าเชื่อถือจากหน่วยความจำในการปรับเปลี่ยน
Prevent untrusted programs from modifying system processes	ป้องกันไม่ให้โปรแกรมที่ไม่ได้เชื่อถือจากการปรับเปลี่ยนระบบปฏิบัติการ
Polices Details	รายละเอียด

Verify the integrity of the LSP chain and other system structures	ตรวจสอบความสมบูรณ์ของ LSP และโครงสร้างอื่นๆ
Prevent any program from modifying the HOSTS file	ป้องกันไม่ให้โปรแกรมใดๆมีการปรับเปลี่ยนจากไฟล์โฮสต์

3.9 Web Threat Shield

Polices Details	รายละเอียด
Web threat shield enabled	เปิดการป้องกันภัยคุกคามเว็บ ไซค์
Analyze search engine results and identify malicious websites before visitation	วิเคราะห์ผลการค้นหาและระบุเว็บ ไซค์ที่เป็นอันตราย
Automatically protect newly installed browser	ตรวจสอบอัตโนมัติเว็บ ไซค์ที่มีการติดตั้งใหม่
Look for malware on websites before visitation	ตรวจสอบหา มัลแวร์ บนเว็บ ไซค์ ก่อนที่จะเข้าไปถึง
Look for exploits in website content before visitation	ตรวจสอบหา เนื้อหาของเว็บ ไซค์ ก่อนที่จะเข้าไปถึง
Suppress the user's ability to make local web threat shield overrides	ป้องกันผู้ใช้งาน ในการใช้เว็บ ไซค์ ที่เสี่ยงต่อภัยคุกคาม
Auto install browser addons when new browsers are installed	ติดตั้ง โปรแกรม Addon โดยอัตโนมัติ เมื่อมีการติดตั้ง Web-browser ใหม่
Only install the web filtering driver (do not install the web filtering browser addons)	ให้ติดตั้งโปรแกรมควบคุมการกรองเว็บเท่านั้น (ไม่ให้ติดตั้งเบราว์เซอร์ add on กรองเว็บ)

3.10 Identity Shield

Polices Details	รายละเอียด
-----------------	------------

Identity shield Enabled	เปิดการใช้งานการป้องกันที่ระบุตัวตน
Look for identity threats online	วิเคราะห์เว็บไซต์ที่ผู้ใช้ใช้เบราว์เซอร์และการเชื่อมโยงไปหาเว็บไซต์อื่นๆ
Analyze websites for phishing threats	วิเคราะห์เว็บไซต์สำหรับภัยคุกคามฟิชซิง
Verify websites when visited to determine legitimacy	ตรวจสอบเว็บไซต์เมื่อมีการใช้งานของเว็บไซต์ต่างๆ
Verify the DNS/IP resolution of websites to detect Man-in-the-Middle attacks	ตรวจสอบความละเอียด DNS/IP ของเว็บไซต์และตรวจการโจมตี
Block websites from accessing protected credentials	บล็อกเว็บไซต์ที่มีความเสี่ยงสูง
Prevent programs from accessing protected credentials	บล็อกโปรแกรมที่มีการเข้าถึงข้อมูลประจำตัวที่ได้รับการป้องกัน
Warn before blocking untrusted programs from accessing protected data	แจ้งเตือนก่อนที่จะบล็อกโปรแกรมจากการตรวจสอบ
Allow trusted screen capture programs access to protected screen contents	อนุญาตให้โปรแกรมจับภาพหน้าจอที่เชื่อถือได้เข้าถึงเนื้อหาของหน้าจอที่มีการป้องกัน
Enable identity Shield compatibility mode	เปิดการใช้งานการป้องกัน Compatibility Mode
Enable keylogging protection in non-Latin systems	เปิดการใช้งานการบันทึกการกดคีย์บอร์ดแบบ non-Latin

3.11 Firewall

Polices Details	รายละเอียด
Enabled	เปิดการใช้งาน

Firewall level	ระดับของไฟร์วอลล์
Polices Details	รายละเอียด
Show firewall management warnings	แสดงคำเตือนการจัดการไฟร์วอลล์
Show firewall process warnings	แสดงคำเตือนกระบวนการไฟร์วอลล์

3.12 User interface

Polices Details	รายละเอียด
GUI	(Graphical user interface) สามารถแสดงการรายละเอียดการ Configure

3.13 System Cleaner

Polices Details	รายละเอียด
Manage system cleaner centrally	จัดการทำความสะอาดระบบจากส่วนกลาง
Scheduled cleanup	กำหนดเวลาทำความสะอาด
Cleanup at specific time of day – hour	การล้างข้อมูลในช่วงเวลาที่เฉพาะเจาะจงของวัน (ชั่วโมง)
Cleanup at specific time of day - minute	การล้างข้อมูลในช่วงเวลาที่เฉพาะเจาะจงของวัน (นาที)
Enable windows explorer right click secure file erasing	เปิดใช้งาน Windows Explorer คลิกขวาลบไฟล์ที่ปลอดภัย
Windows desktop	
Recycle Bin	ถังรีไซเคิล
Recent document history	ประวัติการใช้งานเอกสารล่าสุด
Start menu click history	ประวัติการคลิก
Run history	ประวัติการเรียกใช้

Search history	ประวัติการค้นหา
Start menu order history	ประวัติการเริ่มต้นเมนู
Windows system	
Clipboard contents	เนื้อหาของคลิปบอร์ด
Windows temporary folder	โฟลเดอร์ Windows Temporary
System temporary folder	โฟลเดอร์ System Temporary
Windows update Temporary folder	โฟลเดอร์ Windows Update Temporary
Windows registry streams Windows Registry	Windows Registry
Default logon user history	ค่าเริ่มต้นประวัติของผู้ใช้เข้าสู่ระบบ
Memory dump files	แฟ้มการถ่ายโอนหน่วยความจำและ
CD burning storage folder	โฟลเดอร์จัดเก็บข้อมูลการเขียนซีดี
Flash cookies	คุกกี้แฟลช
Internet explorer	
Address bar history	ประวัติแถบบาร์ (Address bar)
Cookies	คุกกี้
Temporary internet files	
URL history	ประวัติ URL
Setup log	ประวัติการติดตั้งโปรแกรม

Microsoft download folder	ไมโครซอฟท์ดาวน์โหลดโฟลเดอร์
MediaPlayer Bar history	ประวัติ Media Player Bar
Autocomplete form information	ข้อมูลรูปแบบอัตโนมัติ
Clean index.dat (cleaned on reboot)	ทำความสะอาด index.dat (ทำความสะอาดในการบูตเครื่อง)
Secure file removal	
Control the level of security to apply when removing files. Higher security levels reduce the possibility of recovering data but will require longer to clean.	ควบคุมระดับความปลอดภัยที่จะใช้เมื่อการลบไฟล์ ระดับความปลอดภัยที่สูงขึ้นลดความเป็นไปได้ของการกู้คืนข้อมูล แต่จะต้องใช้เวลานานในการทำความสะอาด

Group Management

The screenshot displays the Group Management interface with the following components:

- Navigation Tabs:** Status, Policies, Group Management (selected), Reports, Alerts, Overrides, Logs, Resources.
- Search:** Search for hostname... and Advanced Search.
- Left Panel (Groups):**
 - Create, Actions
 - Group Name | No.
 - All Endpoints | 28
 - Deactivated Endpoints | 2
 - Default Group | 7
 - Accounting | 2
 - Admin | 1
 - HR | 0
 - IT | 6
 - Macbook | 2
 - Manager | 2
 - Project test | 1
 - Sales | 1
 - Server | 6
- Main Panel (All Endpoints):**
 - Save Changes, Undo Changes, Move endpoints to another group, Apply policy to endpoints, Agent Commands, Deactivate
 - Table with columns: Hostname, Policy, Group, Status, Last Seen, L..., A, Internal IP Addr...
 - Endpoint 1: ADWIN-PC, Recommended Defaults, Default Group, Protected, Mar 13th 20...
 - Endpoint 2: AUN-NS-LENOVO, Unmanaged, Default Group, Not Seen, Jan 9th 201...
 - Endpoint 3: BREFCAL-PC, Recommended Server Defaults, Project test, Not Seen, Jan 27th 20...
 - Endpoint 4: BSS-07, Unmanaged, Default Group, Protected, Mar 13th 20...
 - Endpoint 5: BSS-09, Recommended Defaults, Accounting, Protected, Mar 13th 20...
 - Endpoint 6: BSS-10, Unmanaged, Accounting, Protected, Mar 13th 20...
 - Endpoint 7: BSS-11, Unmanaged, Default Group, Protected, Mar 11th 20...
 - Endpoint 8: BSS-14, Unmanaged, Manager, Protected, Mar 13th 20...
- Policies used in All Endpoints:**
 - Save Changes, Undo Changes
 - Table with columns: Policy Name, Endpoints using this policy, Policy Description
 - Unmanaged: 12 endpoints, This policy is for all PCs that are user managed
 - Recommended Server Defaults: 9 endpoints, Recommended setup for servers, protection enabled
 - Recommended Defaults: 5 endpoints, Recommended setup with protection and remediation

เมื่อติดตั้ง SecureAnywhere บนอุปกรณ์ปลายทางเสร็จเรียบร้อยแล้ว นโยบายเริ่มต้นจะไปอยู่ใน Default Group (Group management คือชุดของอุปกรณ์ปลายทางซึ่งจะช่วยให้จัดระเบียบอุปกรณ์ให้สามารถจัดการได้ง่าย) endpoints เมื่อรายงานลงใน Group management (หลังจากดำเนินการสแกนครั้งแรก) สามารถย้ายไปยังกลุ่มที่แตกต่างกัน ตัวอย่างเช่น อาจจัดระเบียบจุดสิ้นสุดตามวันและเวลาเพื่อให้สามารถกำหนดเวลาการสแกนเดียวกันสำหรับพวกเขาทั้งหมด สามารถดูทุกกลุ่มในแท็บการจัดการกลุ่ม

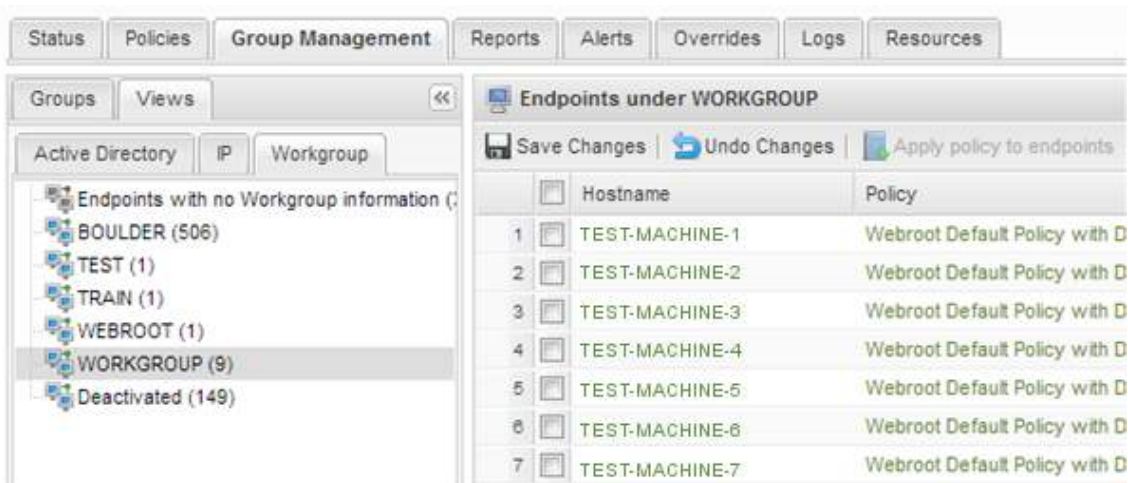
จะมีแถบเมนูทั้งหมด 5 เมนูหลักได้แก่

- Group
- Views
- Search
- All Endpoints
- Polices used in All endpoint

1.Group จะมีเมนู 3 เมนู

- Create จะเป็นการสร้าง Group เพื่อทำการ Join เข้ากับ Polices
- Actions เป็นการแก้ไขชื่อ Group ลบ และย้าย Group
- Group Name คือ เป็นเมนูที่แสดงแต่ละ Group

2.Views ดูข้อมูลที่เก็บรวบรวม Endpoint ภายใต้การบริหารจัดการกลุ่ม Domain ตามรายละเอียดตามรูปด้านล่าง



3. Search คือ เป็นการตรวจหา Endpoint โดยจะต้องการค้นหาจาก Hostname ,status, group, policy, Active directory , keycode , operation system

4. All Endpoint จะมีเมนู 6 เมนูได้แก่

1. Save Changes เป็นการบันทึกสำหรับมีมีการเปลี่ยนแปลง กลุ่ม หรือ Policies ได้
2. Undo Changes คือเป็นการกลับไปค่าเดิม หลังจากที่ได้ทำการเปลี่ยนแปลงต่างๆ
3. Move endpoints to another group คือ เป็นการย้าย Endpoint กลุ่มหนึ่งไปยังอีกกลุ่มหนึ่ง
4. Apply policy to endpoint คือ เป็นการใช้สำหรับ เมื่อต้องการเปลี่ยนแปลง Policies ให้กับ Endpoint
5. Agent commands คือ เป็นการใช้คำสั่ง โดยมีรายละเอียดดังนี้

Agent

- Scan คือ สแกนตรวจสอบไฟล์ที่มีความเสี่ยง
- Change scan time คือเปลี่ยนแปลงเวลาการสแกน
- Scan a Folder คือเป็นการเลือกโฟลเดอร์ที่ต้องการทำการสแกน
- Clean up คือทำการจัดการลบไฟล์ที่มีความเสี่ยงที่เก็บไว้ใน Quarantine
- System cleaner คือทำการจัดการไฟล์ที่ขยะ เช่น Temp history cookie
- Uninstall คือ ยกเลิกการติดตั้ง Endpoint
- Reset คือ การรีเซ็ต Endpoint ให้กลับไปเป็นการตั้งค่าเริ่มต้น
- Remove Password protection คือ การลบ password ออกจาก Endpoint

Clear data

- Clear log file คือ เป็นลบไฟล์ที่เก็บ log ที่เก็บใน Endpoint
- Disable proxy setting คือ เป็นการปิดการใช้ Proxy ที่มีการตั้งค่าไว้

Keycode

- Change keycode คือเป็นการเปลี่ยน keycode ของ Endpoint
- Change keycode temporarily คือ สามารถกำหนดระยะเวลาการใช้งานของ keycode

Power & User access

- Lock endpoint คือ สามารถที่จะทำการ Lock windows endpoint
- Log off คือ สามารถที่จะทำการ Log off windows
- Restart คือ สามารถที่จะทำการ Restart windows
- Restart in Safe Mode with Networking คือ สามารถที่จะทำการ Restart เพื่อเข้า Safe Mode network

- Shutdown คือ สามารถปิดเครื่อง endpoint

Antimalware Tools

- Reset desktop คือสามารถรีเซ็ตหน้าจอ
- Reset Screen saver คือสามารถรีเซ็ต Screen saver
- Reset system policies คือ สามารถที่จะทำการรีเซ็ตค่า registry ได้
- Restore file คือ สามารถที่ทำการ restore file ที่อยู่ใน Quarantine

Files & Processes

- Reverify all files and processes คือการตรวจตรวจสอบฐานข้อมูล
- Consider all items as good คือ เป็นการพิจารณารายการทั้งหมดที่ดีและทำงานอย่างปลอดภัย
- Allow processes blocked by firewall คือการอนุญาตให้การสื่อสารที่ถูกบล็อกที่มีการตั้งค่าในไฟร์วอลล์
- Stop untrusted processes คือหยุดการทำงานทั้งหมด และสามารถทำงานงานอีกครั้งได้

Identity Shield

- Allow application คือ สามารถอนุญาต Application ทำงานได้โดยไม่ต้องตรวจสอบ
- Deny application คือ สามารถที่ทำการบล็อก Application ไม่ได้ทำงานได้
- Allow All Denied Applications คือสามารถที่อนุญาตให้ Application ทำงานได้โดยที่ยังบล็อก
- Protect an Application คือ สามารถที่ให้การตรวจสอบ Application
- Unprotect an Application คือ สามารถยกเลิกการตรวจสอบ Application

Advanced

- Run customer support script คือ สามารถ Run script เพื่อทำการ Cleanup
- Customer support Diagnostics คือสามารถทำการส่ง Log ของ Endpoint ไปให้ Support วิเคราะห์ได้
- Download and run a file คือ สามารถที่จะให้ Endpoint ดาวน์โหลดไฟล์ด้วย Comment หรือ UR
- Run a DOS command คือสามารถที่ Run command เพื่อส่งไปยัง Endpoint
- Run a registry command คือ สามารถที่ Run command registry เพื่อส่งไปยัง Endpoint

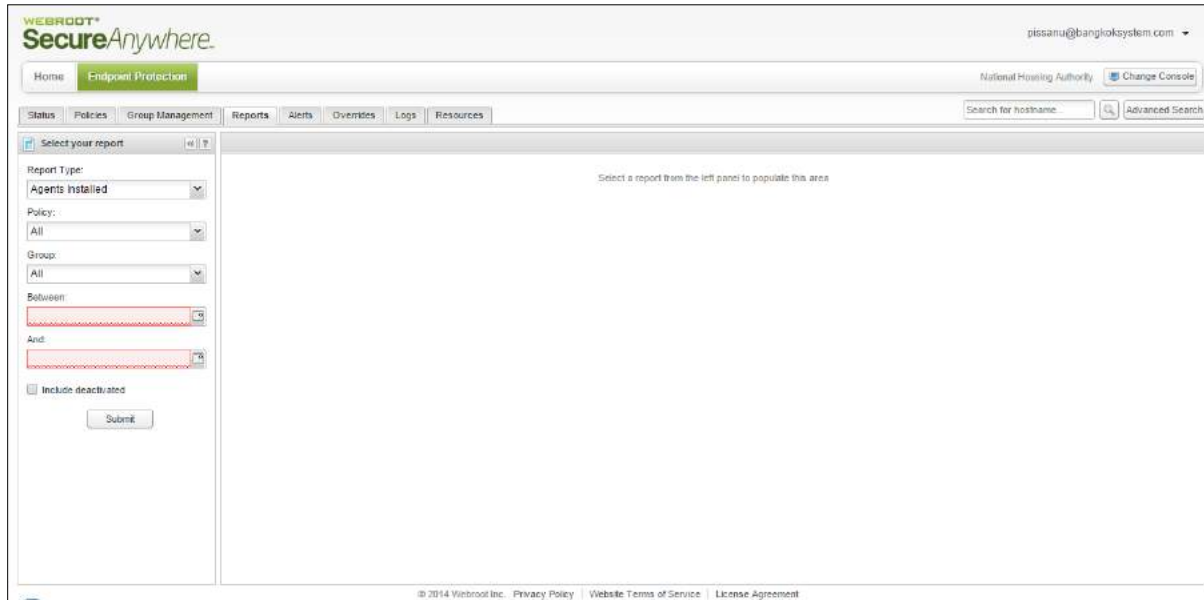
View commands for selected endpoints คือสามารถที่จะทำการตรวจสอบตรวจ คำสั่งที่มีการส่งไปให้ Endpoint ได้รับ คำสั่งไปให้หรือยัง

How to use Agent commands คือ แสดงวิธีการใช้งานคำสั่งต่างๆ (วิดีโอ)

6.Deactivate คือเป็นการจัดการคืน license และรวมไปถึงไม่ได้ถูกจัดการของ Webroot อีกต่อไป หลังจาก Deactivate endpoint จะย้ายไปกลุ่ม Deactivate ทันที

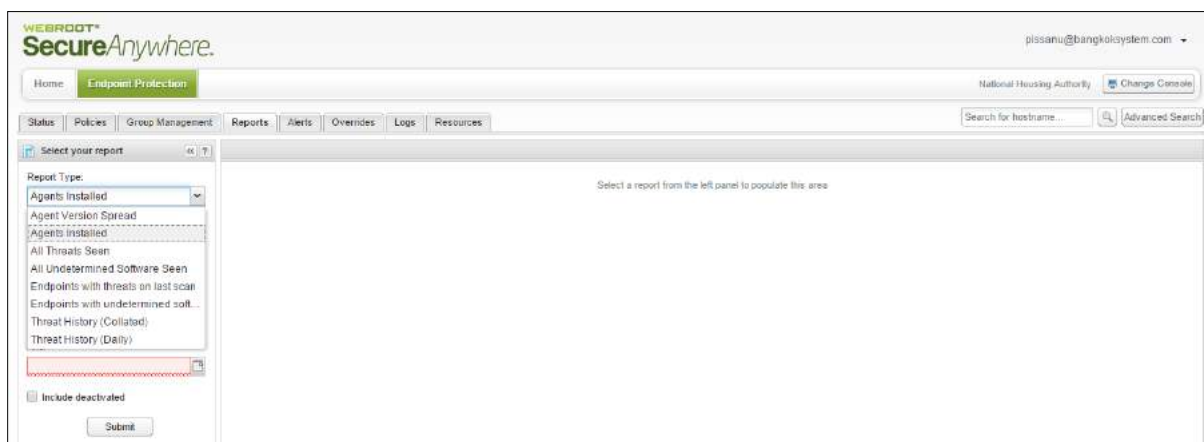
7. Polices used in All endpoint เป็นการแสดงรายละเอียดของกลุ่มและPolicy

Reports



การเรียกดูในส่วนของรายงาน (Reports) สามารถเลือก Reports ได้จากส่วนต่าง ๆ คือ

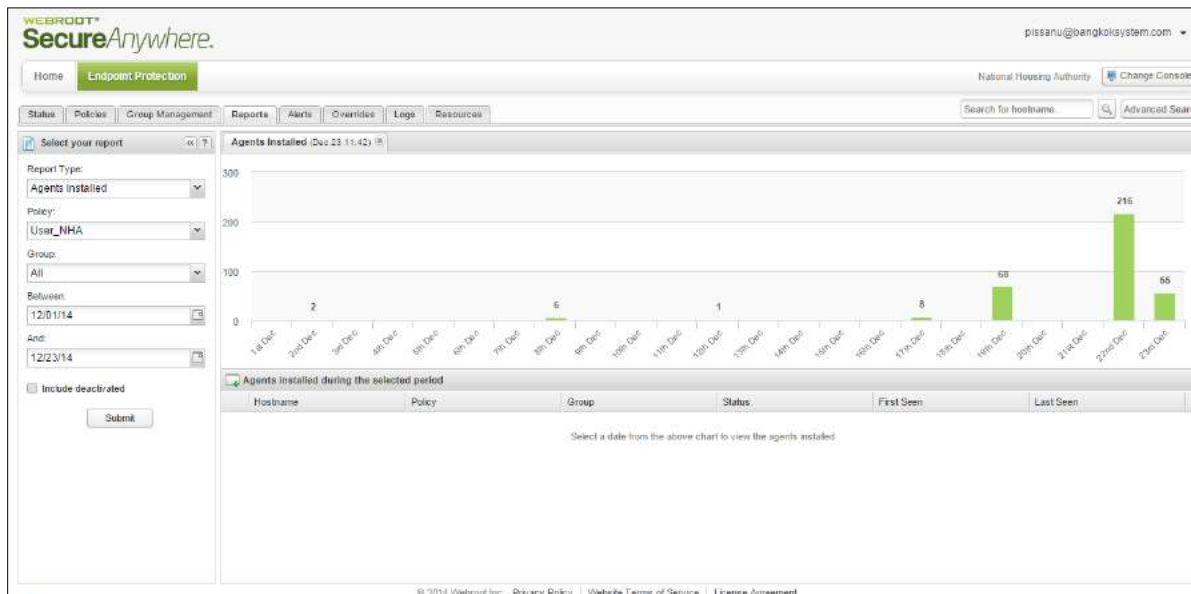
- **Report Type** แสดงรายงานตามรายการแต่ละประเภท
- **Policy** แสดงรายงานแต่ละ Policy ของผู้ใช้แต่ละกลุ่มที่ได้มีการกำหนดไว้
- **Group** แสดงตามกลุ่ม
- **ระหว่างวันที่** แสดงรายงานตามวันที่ ที่ระบุระหว่างวันที่เท่าไร ถึง เท่าไร
- **ส่วน Deactivated** แสดงในส่วนของผู้ใช้ที่ได้มีการ Deactivated



Report Type

- **Agent Version Spread** เวอร์ชันของแต่ละEndpoints
- **Agents Installed** การติดตั้งโปรแกรมของ Agent
- **All Threats Seen** ไฟล์ที่มีความเสี่ยงทั้งหมด
- **All Undetermined Software Seen** ไฟล์ที่มีความเสี่ยงที่ถูกกักเก็บไว้
- **Endpoints with threats on last scan.** Endpoints ที่มีภัยคุกคามที่ตรวจพบล่าสุด
- **Endpoints with undetermined software on last scan.** Endpoints และไฟล์ที่มีความเสี่ยงที่ถูกกักเก็บไว้ ที่มีการตรวจพบล่าสุด
- **Threat History (Collated)** ประวัติไฟล์ความเสี่ยงทั้งหมด
- **Threat History (Daily)** ประวัติไฟล์ความเสี่ยง (แสดงเป็นรายวัน)

แสดงตัวอย่างรายงาน



Log

แสดงรายละเอียด 2 ส่วน คือ **Change Log** และ **Command log**

1. Change Log

The screenshot shows the Webroot SecureAnywhere console interface. At the top, there's a navigation bar with 'Home' and 'Endpoint Protection' tabs. Below that, there are tabs for 'Status', 'Policies', 'Group Management', 'Reports', 'Alerts', 'Overrides', 'Logs', and 'Resources'. A search bar is present with the text 'Search for hostname...'. The main content area is titled 'Change Log' and contains a table with the following data:

Date	Event Type	Description
1 Dec 23rd 2014, 13:33	Logon	pissanu@bangkoksystem.com logged on
2 Dec 23rd 2014, 13:11	Logon	pissanu@bangkoksystem.com logged on
3 Dec 23rd 2014, 12:57	Endpoint	webroot@nha.co.th moved R3217053402 (Policy: User_NHA) to Branch Office
4 Dec 23rd 2014, 12:57	Endpoint	webroot@nha.co.th moved R3217053409 (Policy: User_NHA) to Branch Office
5 Dec 23rd 2014, 12:57	Endpoint	webroot@nha.co.th moved R3217053402 (Policy: User_NHA) to Branch Office
6 Dec 23rd 2014, 12:57	Endpoint	webroot@nha.co.th moved R3217053400 (Policy: User_NHA) to Branch Office
7 Dec 23rd 2014, 12:57	Endpoint	webroot@nha.co.th moved R3217053410 (Policy: User_NHA) to Branch Office
8 Dec 23rd 2014, 12:57	Endpoint	webroot@nha.co.th moved R321-705-3405 (Policy: User_NHA) to Branch Office
9 Dec 23rd 2014, 12:57	Endpoint	webroot@nha.co.th moved R3217053409 (Policy: User_NHA) to Branch Office
10 Dec 23rd 2014, 12:57	Endpoint	webroot@nha.co.th moved R3217053397 (Policy: User_NHA) to Branch Office
11 Dec 23rd 2014, 12:57	Endpoint	webroot@nha.co.th moved R3217053407 (Policy: User_NHA) to Branch Office
12 Dec 23rd 2014, 12:57	Endpoint	webroot@nha.co.th moved R3217053415 (Policy: User_NHA) to Branch Office
13 Dec 23rd 2014, 12:57	Endpoint	webroot@nha.co.th moved R3217053431 (Policy: User_NHA) to Branch Office
14 Dec 23rd 2014, 12:57	Endpoint	webroot@nha.co.th moved R3217053445 (Policy: User_NHA) to Branch Office
15 Dec 23rd 2014, 12:57	Endpoint	webroot@nha.co.th moved R3217053398 (Policy: User_NHA) to Branch Office
16 Dec 23rd 2014, 12:57	Endpoint	webroot@nha.co.th moved R3217053411 (Policy: User_NHA) to Branch Office
17 Dec 23rd 2014, 12:57	Endpoint	webroot@nha.co.th moved R3217053394 (Policy: User_NHA) to Branch Office
18 Dec 23rd 2014, 12:57	Endpoint	webroot@nha.co.th moved R3217053438 (Policy: User_NHA) to Branch Office
19 Dec 23rd 2014, 12:57	Endpoint	webroot@nha.co.th moved R3217053416 (Policy: User_NHA) to Branch Office

The filter sidebar on the left includes sections for 'Between', 'And', 'Event Type', 'Involving User', 'Involving Group', and 'Involving Policy', each with a dropdown menu and a 'Submit' button.

การ Filter Change log สามารถ Filter ได้โดย

- การระบุ ช่วงเวลาที่ต้องการ
- **Event Type** ตามประเภทเหตุการณ์ เช่น Group, Endpoint, Policy, Override และ Logon
- **Involving User** โดยผู้ที่เกี่ยวข้อง
- **Involving Group** โดยกลุ่มที่เกี่ยวข้อง
- **Involving Policy** โดยนโยบายที่เกี่ยวข้อง

WEBROOTSM SecureAnywhere. pissanu@bangkoksystem.com

Home **Endpoint Protection** National Housing Authority [Change Console](#)

Status Policies Group Management Reports Alerts Overrides **Logs** Resources Search for hostname [Advanced Search](#)

Change Log **Command Log**

Recent & Outstanding Commands

Hostname	Command	Parameters	Date Requested	Status
1 CN-PC	Uninstall		Dec 3rd 2014, 13:11	Not yet received
2 CN-PC	Restore file	MDS: CAB8BF094DEBDC8BAF110130E082	Nov 26th 2014, 11:06	Elapsed
3 CN-PC	Restore file	MDS: CAB8BF094DEBDC8BAF110130E082	Nov 25th 2014, 10:29	Elapsed
4 CN-PC	Restore file	MDS: CAB8BF094DEBDC8BAF110130E082	Nov 24th 2014, 15:07	Elapsed
5 ISC	Uninstall		Nov 24th 2014, 11:28	Executed
6 ISC	Uninstall		Nov 24th 2014, 11:29	Executed
7 KKD-20140718ESR	Log off		Dec 3rd 2014, 13:51	Executed
8 MD010051959	Scan		Dec 23rd 2014, 13:33	Not yet received
9 MD010051993	Restore file	MDS: C915C717919F5828F5E343FDA16A84F6	Dec 22nd 2014, 11:26	Executed
10 MD010051988	Restore file	MDS: C915C717919F5828F5E343FDA16A84F6	Dec 23rd 2014, 10:19	Not yet received
11 MD010051999	Restore file	MDS: C915C717919F5828F5E343FDA16A84F6	Dec 23rd 2014, 10:19	Executed
12 MD010052016	Restore file	MDS: C915C717919F5828F5E343FDA16A84F6	Dec 23rd 2014, 10:19	Executed
13 N_S	Uninstall		Dec 12th 2014, 10:42	Not yet received
14 R-232-505-3064	Clean up		Nov 24th 2014, 15:42	Executed
15 R-232-505-3064	Clean up		Nov 24th 2014, 09:42	Executed
16 R-232-505-3077	Clean up		Dec 19th 2014, 14:10	Executed
17 R1542053395	Scan		Dec 3rd 2014, 15:07	Executed
18 R1542053395	Scan		Dec 3rd 2014, 14:53	Executed
19 R1542053395	Scan		Dec 3rd 2014, 14:52	Executed

Page 1 of 2 Displaying 1 - 50 of 53

2. Command log คือ แสดงรายการ log ที่เกิดจากการ Command ที่มีการส่งคำสั่งไปที่ Endpoints

สามารถที่จะทำการ Export เป็นไฟล์ CSV.

National Housing Authority [Change Console](#)

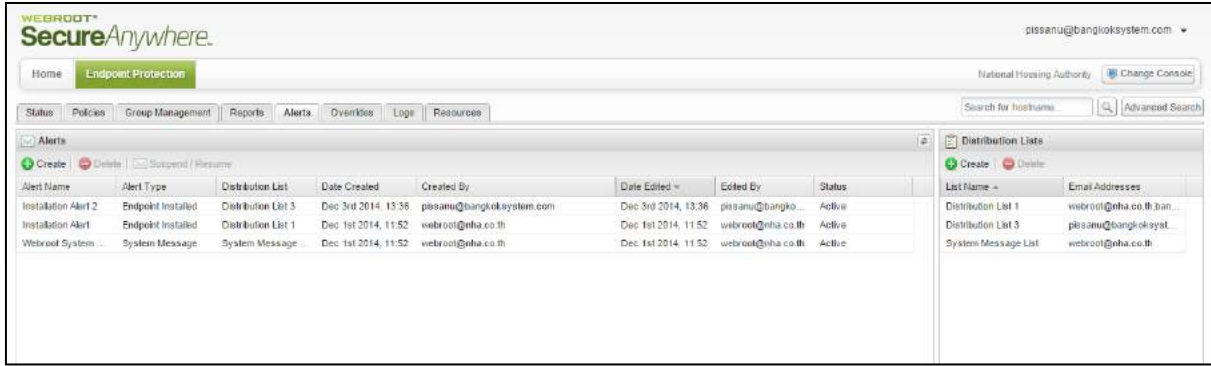
Reports Alerts Overrides **Logs** Resources Search for hostname... [Advanced Search](#)

Change Log

Date	Event Type	Description
1 Dec 23rd 2014, 13:33	Logon	pissanu@bangkoksystem.com logged on
2 Dec 23rd 2014, 13:11	Logon	pissanu@bangkoksystem.com logged on
3 Dec 23rd 2014, 12:57	Endpoint	webroot@nha.co.th moved R3217054012 (Policy: User_NHA) to Brance Office
4 Dec 23rd 2014, 12:57	Endpoint	webroot@nha.co.th moved R3217053429 (Policy: User_NHA) to Brance Office
5 Dec 23rd 2014, 12:57	Endpoint	webroot@nha.co.th moved R3217053402 (Policy: User_NHA) to Brance Office
6 Dec 23rd 2014, 12:57	Endpoint	webroot@nha.co.th moved R3217053400 (Policy: User_NHA) to Brance Office
7 Dec 23rd 2014, 12:57	Endpoint	webroot@nha.co.th moved R3217053410 (Policy: User_NHA) to Brance Office

Alerts

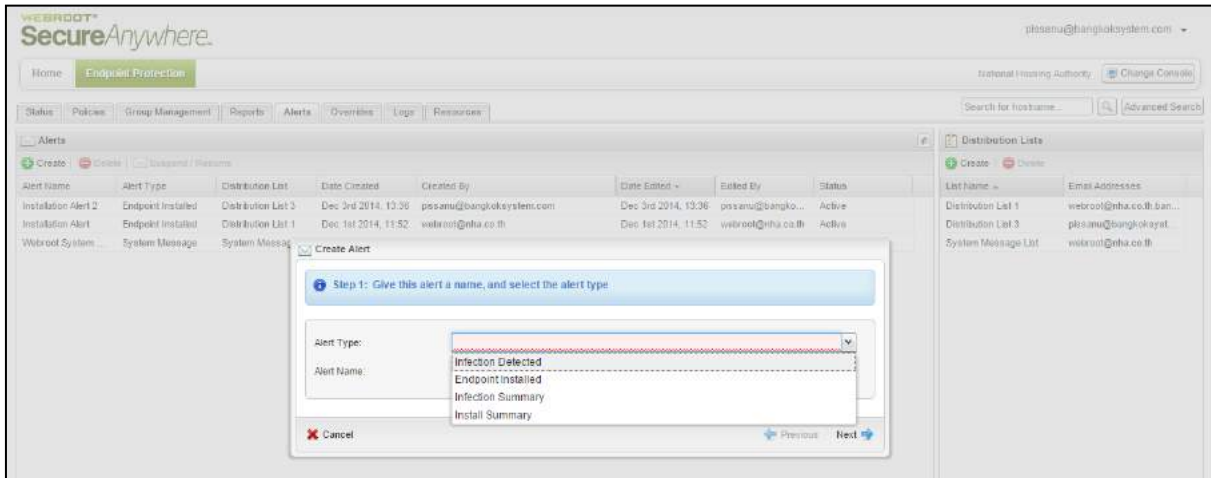
การแสดงผลการแจ้งเตือน สามารถทำการสร้างการแจ้งเตือนในลักษณะต่าง ๆ ได้



ในส่วนการ Create Alerts

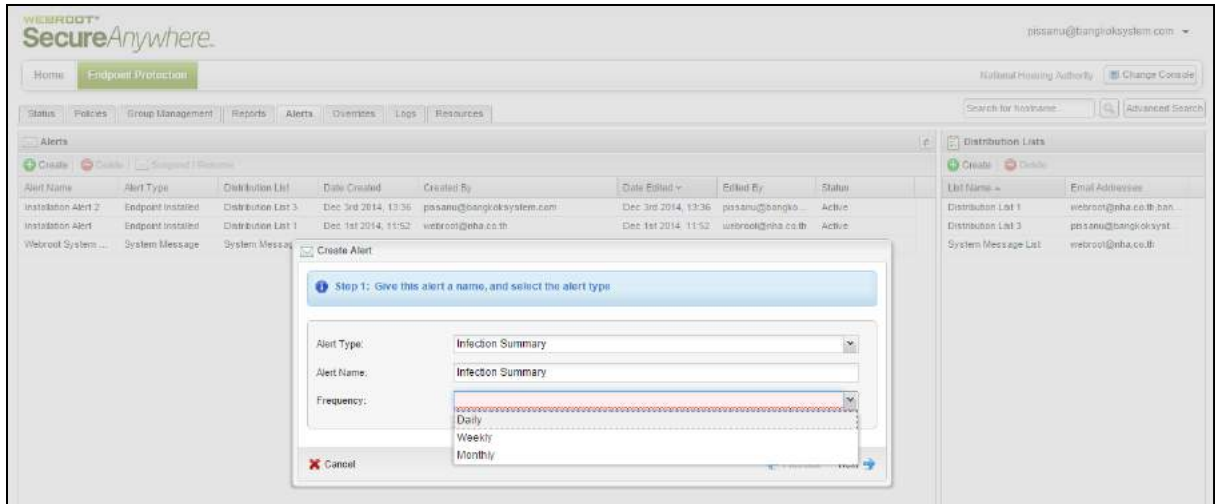
Create

- สามารถระบุตามชนิดแสดงคั้งหน้าจอด้านล่าง



- **Infection Detected** การตรวจพบไฟล์ที่เป็นความเสี่ยงทั้งหมด
- **Endpoint Installed** การติดตั้งที่เครื่อง Endpoint
- **Infection Summary** สรุปรายการทั้งหมด
- **Install Summary** สรุปรายการที่ได้ติดตั้ง

- ในส่วนรายการ Summary จะมี Frequency ให้ระบุความถี่เป็นรายวัน สัปดาห์ หรือเดือนได้ แสดงรายละเอียดคั้งหน้าจอด้านล่าง



ตัวอย่างการ สร้าง Alerts

1. ระบุประเภท , ชื่อ , ระยะเวลา , เวลา

2. ทำการระบุ List Name ที่มีอยู่เดิม หรือทำการสร้างขึ้นมาใหม่เพื่อสร้าง E-mail เพื่อส่งการแจ้งเตือน

3. การสร้าง email แจ้งเตือน

☑ Create Alert

Step 3: Create your email

Email title: Data Inputs ▾

Email message body: Data Inputs ▾

4. เมื่อมีการสร้างเรียบร้อยแล้ว ก็จะส่งการแจ้งเตือนตามเงื่อนไขที่ได้รับ

WEBROOT® SecureAnywhere. pissanu@bangkoksystem.com ▾

Home **Endpoint Protection** National Housing Authority

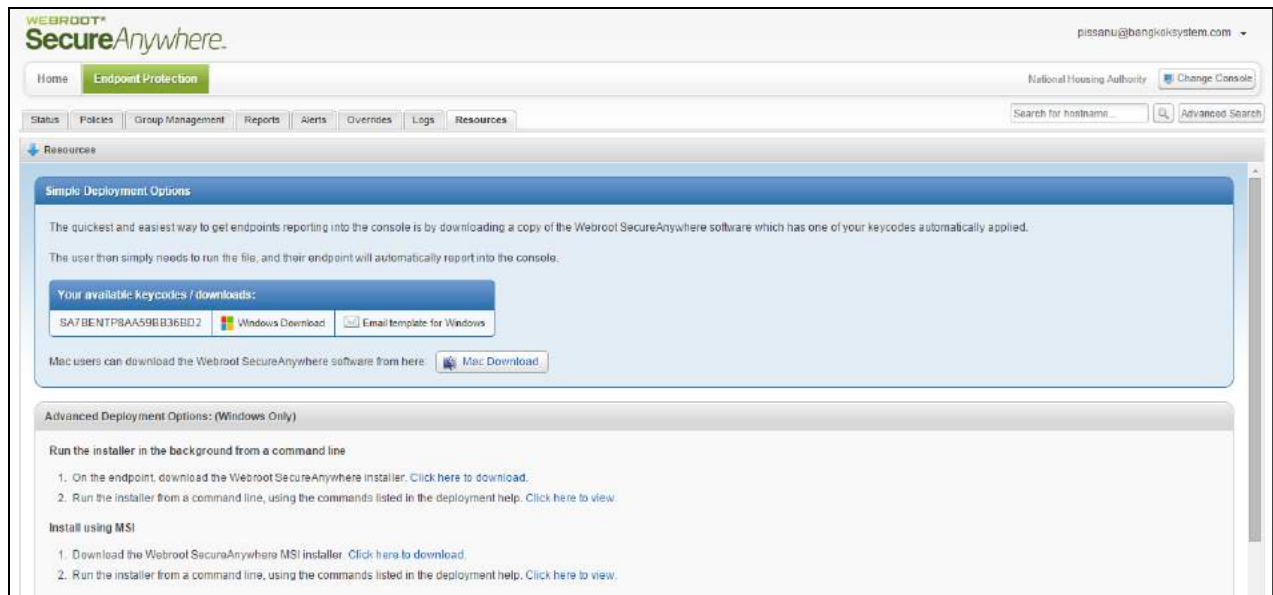
Status Policies Group Management Reports Alerts Overrides Logs Resources Search for hostname...

Alerts							
Alert Name	Alert Type	Distribution List	Date Created	Created By	Date Edited	Edited By	Status
Install Summary	Install Summary	Distribution List 4	Dec 23rd 2014, 1...	pissanu@bangkoksystem.com	Dec 23rd 2014, 1...	pissanu@bangkok...	Active
Installation Alert 2	Endpoint Installed	Distribution List 3	Dec 3rd 2014, 13...	pissanu@bangkoksystem.com	Dec 3rd 2014, 13...	pissanu@bangkok...	Active
Installation Alert	Endpoint Installed	Distribution List 1	Dec 1st 2014, 11...	webroot@nha.co.th	Dec 1st 2014, 11...	webroot@nha.co.th	Active
Webroot System ...	System Message	System Message List	Dec 1st 2014, 11...	webroot@nha.co.th	Dec 1st 2014, 11...	webroot@nha.co.th	Active

Distribution Lists	
List Name	Email Addresses
Distribution List 1	webroot@nha.co.th,bangk...
Distribution List 3	pissanu@bangkoksystem...
Distribution List 4	pissanu@bangkoksystem...
System Message List	webroot@nha.co.th

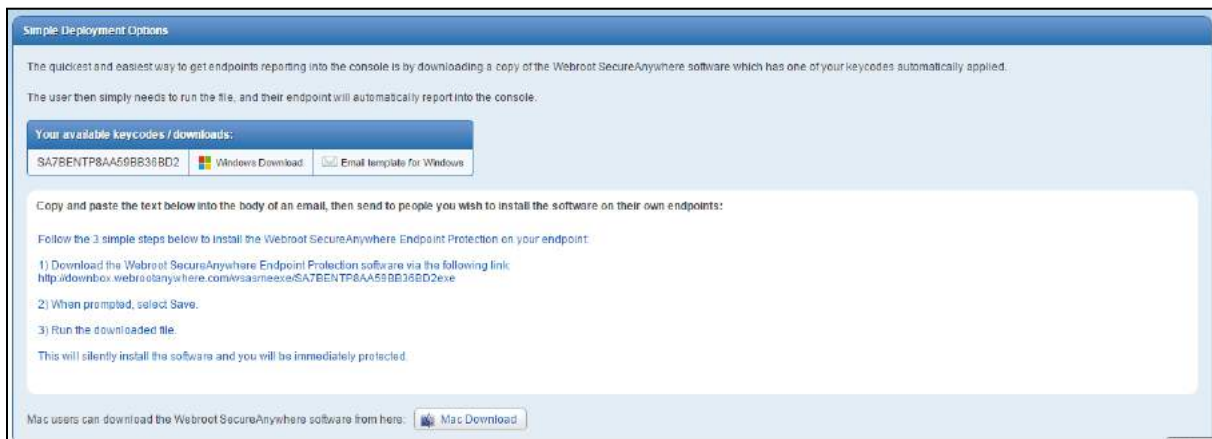
Resources

ส่วนแสดงทรัพยากร ที่สามารถ downloads



ประกอบด้วย 2 ส่วน คือ

- Simple Deployment Options



สามารถที่จะ Deploy ไฟล์ .EXE ไปยังเครื่อง Agent โดยมีการ add ส่วนของ Key codes โดยเลือกที่ **Windows Download** เพื่อ download สำหรับวินโดว หรือส่งรายละเอียดผ่าน email ให้ผู้ใช้คลิก link เพื่อทำการติดตั้งเองได้

ในส่วนนี้รองรับใช้งานที่เป็นเครื่อง Mac ด้วย โดยเลือกที่ Mac Download

- Advanced Deployment Options

Advanced Deployment Options: (Windows Only)

Run the installer in the background from a command line.

1. On the endpoint, download the Webroot SecureAnywhere installer. [Click here to download.](#)
2. Run the installer from a command line, using the commands listed in the deployment help. [Click here to view.](#)

Install using MSI

1. Download the Webroot SecureAnywhere MSI installer. [Click here to download.](#)
2. Run the installer from a command line, using the commands listed in the deployment help. [Click here to view.](#)

For further details about these deployment options, see the Deploying Webroot SecureAnywhere help guide. [Click here to view.](#)

เป็นการจัดการไฟล์โปรแกรมที่เป็น .MSI ที่สามารถนำไปใช้ Deploy ผ่าน Group Policy User

- สามารถดูรายละเอียดขั้นตอนการติดตั้งได้ โดยคลิกที่รายละเอียดด้านล่าง

Run the installer from a command line, using the commands listed in the deployment help. [Click here to view.](#)

The screenshot shows the Webroot Management Portal interface. On the left is a navigation menu with categories like 'Getting Started', 'Managing User Accounts', and 'Managing Endpoints'. The main content area is titled 'Deploying SecureAnywhere to endpoints'. It includes a tip about configuring alerts and a list of steps to follow. A 'Resources' tab is highlighted in the top navigation bar. Below the text, there is a screenshot of the 'Simple Deployment Options' section, which shows a table of available keycodes for download and email templates.

WEBROOT

Deploying SecureAnywhere to endpoints

You can deploy SecureAnywhere to endpoints using a variety of methods, depending on your business requirements and network size. An endpoint can be a Windows PC, laptop, server, or virtual server installed in your network. (A list of endpoint system requirements is provided in [Preparing for setup](#).)

Tip: You can configure alerts so that administrators receive notification whenever new endpoints are installed. See [implementing alerts](#).

To deploy SecureAnywhere to endpoints, follow these steps:

1. Find your keycode. If you don't know your keycode, look in the **Resources** tab of the Management Portal.

The screenshot shows the 'Resources' tab selected in the top navigation bar. Below it, the 'Simple Deployment Options' section is visible, containing the text: 'The quickest and easiest way to get endpoints reporting into the console is by downloading a copy of the user that simply needs to run the file, and their endpoint will automatically report into the console.' Below this text is a table of available keycodes for download and email templates.

Your available keycodes / downloads:	Download	Email template
SA23-TEST-TEST-TEST-TEST	Download	Email template
SAA2-TEST-TEST-TEST-TEST	Download	Email template

Advanced Deployment Options:

Run the installer in the background from a command line

1. On the endpoint, download the Webroot SecureAnywhere installer. [Click here to download.](#)
2. Run the installer from a command line, using the commands listed in the deployment help. [Click here to view.](#)

Note: Devices must use the Endpoint Protection keycode before they can report into the Management Portal. If there are endpoints in your network that already

