PETUNJUK TEKNIS
INSTALASI WINDOWS DEFENDER

PUSAT INFORMASI DAN TEKNOLOGI KEUANGAN

SEKRETARIAT JENDERAL

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

2018

Windows Defender

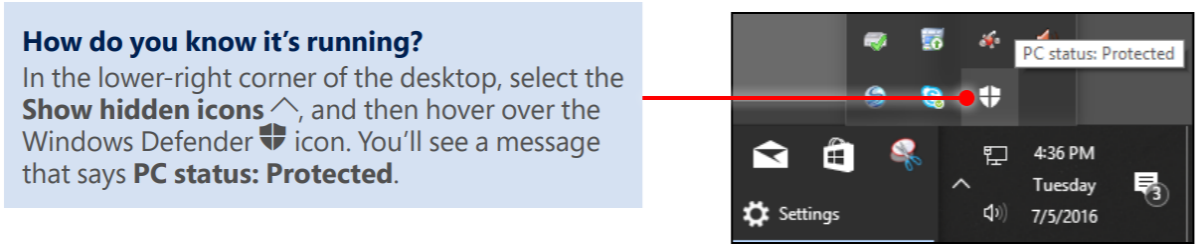
Windows Defender adalah perangkat lunak yang berfungsi memberikan perlindungan dari *malware*. Sejak Windows 8, Windows Defender merupakan bagian dari sistem operasi (*pre-installed*). Perangkat lunak ini berfungsi mengidentifikasi dan menghapus virus, *spyware*, serta perangkat lunak berbahaya lainnya (*malware*).

Berikut ini penjelasan tentang aktifasi Windows Defender pada Windows 8, 8.1 dan 10

Windows Defender versi Windows 8, 8.1 dan 10

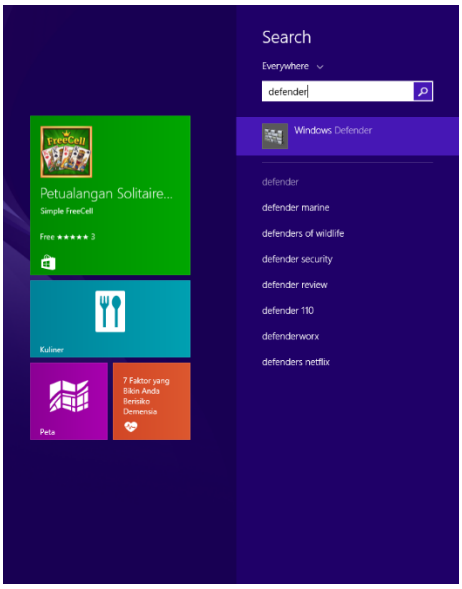
Pada Windows 8 hingga terbaru, Anda hanya perlu mengaktifkan Windows Defender tanpa perlu *install* karena sudah menjadi bagian sistem operasi. Berikut ini langkah mengaktifkan Windows Defender.

1. Berikut ini adalah tanda bahwa Windows Defender sedang aktif, yaitu tanda perisai putih dan apabila tetikus diarahkan ke *icon* tersebut akan muncul pesan *PC status: Protected*



Gambar 1 Tanda Windows Defender Aktif

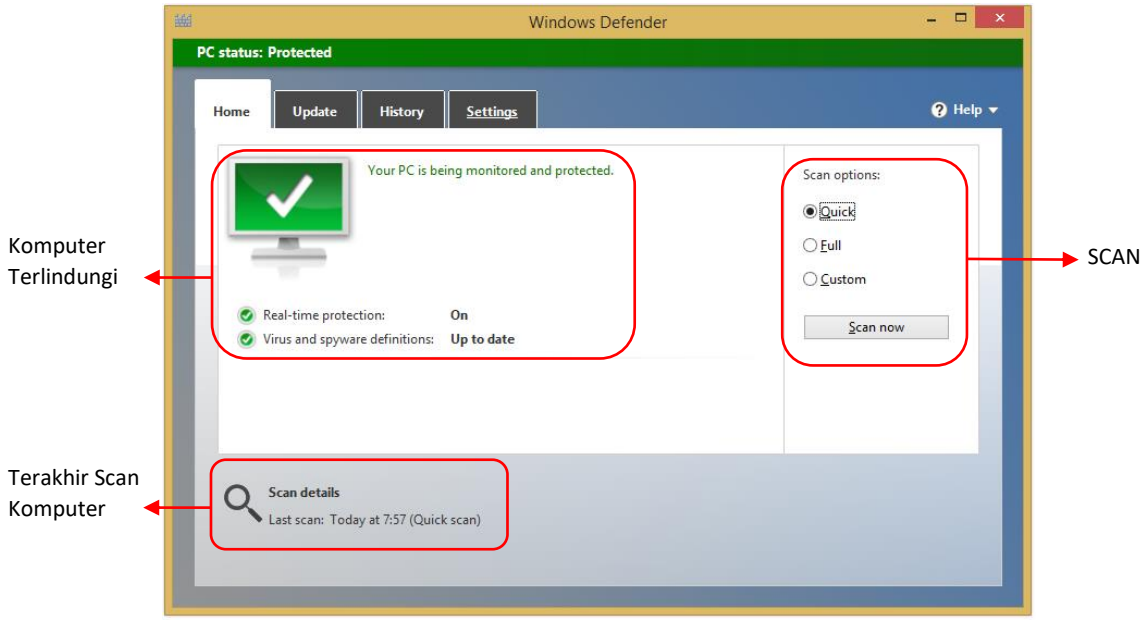
2. Berikut ini cara untuk membuka Windows Defender, yaitu dengan ketik "Defender" di kotak pencarian lalu pilih "Windows Defender"



Gambar 2 Mencari Windows Defender

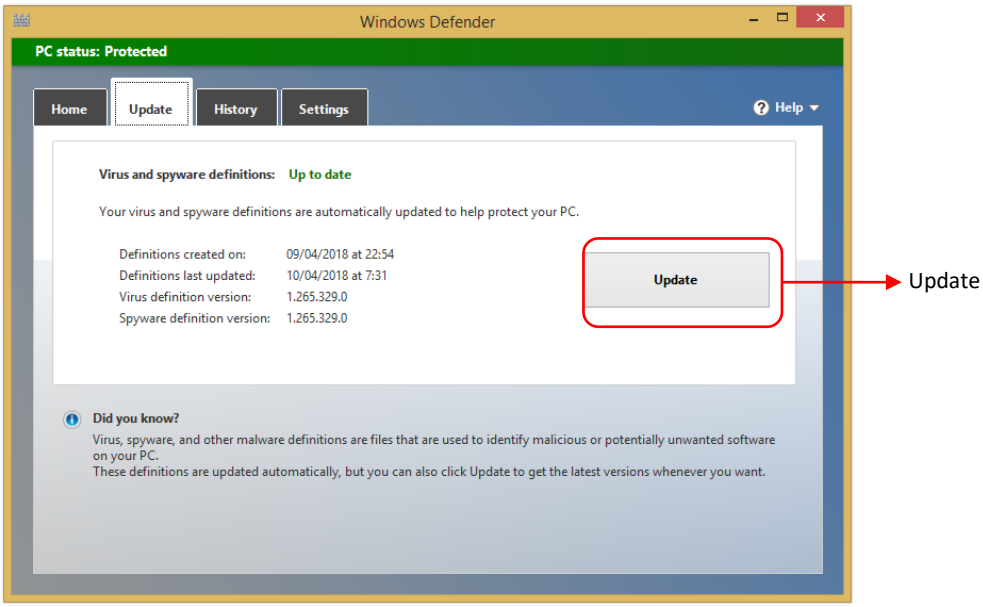
3. Berikut ini tampilan awal Windows Defender yang telah aktif. Pastikan ada tulisan **PC Status: Protected** di bagian atas dan tanda centang berwarna putih dengan latar hijau. Hal ini menandakan tidak ada masalah yang ditemukan oleh Windows Defender. Apabila Windows Defender menemukan program yang berbahaya seperti virus atau fitur yang tidak direkomendasikan seperti tidak aktifnya *Real-time protection* latar belakang tanda centang akan berwarna kuning atau merah dan akan menampilkan pesan.

   Anda dapat melakukan *Scan* untuk mencari *virus*, *spyware* atau *malware* dengan cara klik **Scan.** Pastikan **Real Time Protection** bernilai **On**, hal ini berfungsi untuk melindungi komputer dari perangkat lunak berbahaya secara *real time*.



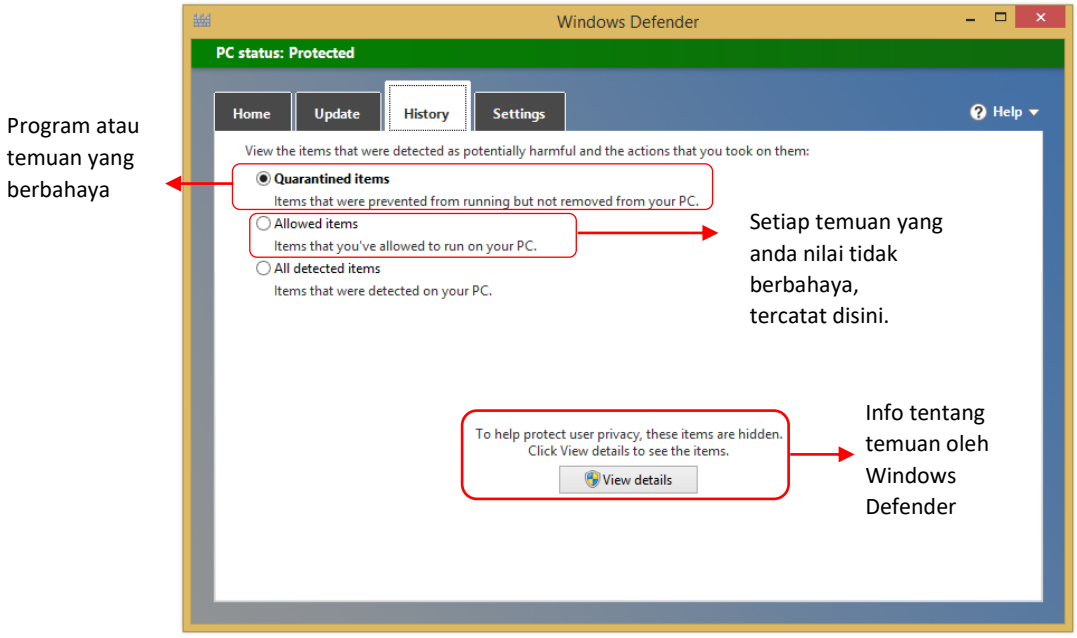
Gambar 3 Status Komputer Aman

4. Pengaturan standar Windows Defender terkait pembaruan database adalah otomatis. Anda juga dapat melakukan pembaruan database secara manual dengan klik **Update** pada tab **Update.**



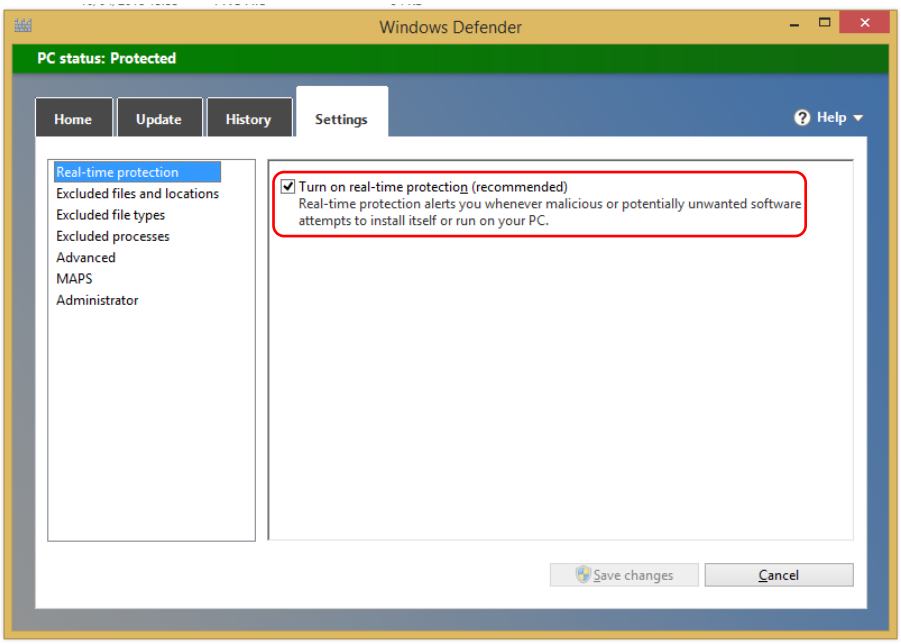
Gambar 4 Pilihan Update Database

5. Berikut ini tab **History** yang berisi data riwayat aksi Windows Defender atas temuan virus, *spyware* dan *malware*. Pada tab ini anda dapat melihat program



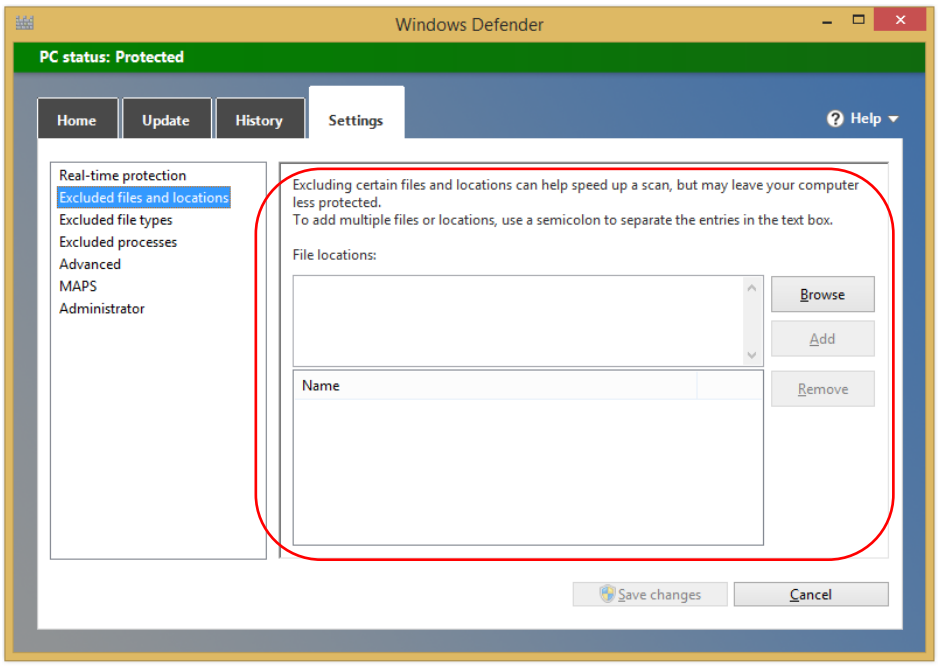
Gambar 5 Riwayat Temuan dan Aksi

6. Berikut ini pengaturan untuk mengaktifkan atau mematikan Windows Defender dengan memberikan tanda centang pada pengaturan **Turn on real-time protection (recommended)**



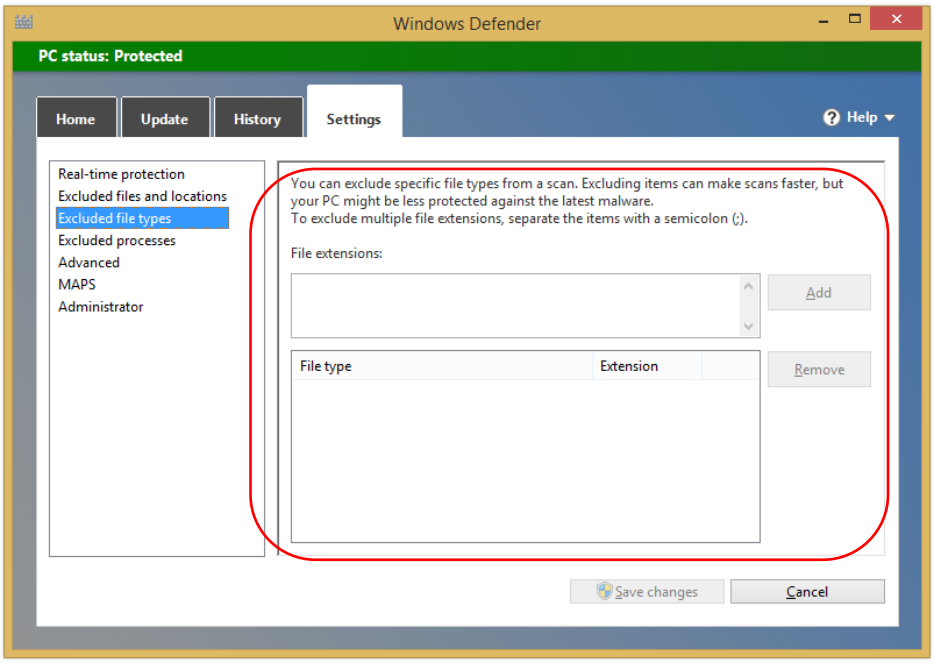
Gambar 6 Opsi Mematikan Perlindungan Real-time

7. Berikut ini pengaturan untuk mengecualikan *file* atau *folder* dari proses scan oleh Windows Defender. Pengecualian ini dapat mempercepat proses *scanning* namun meningkatkan kerentanan komputer anda terhadap serangn virus, *malware* atau *spyware*.



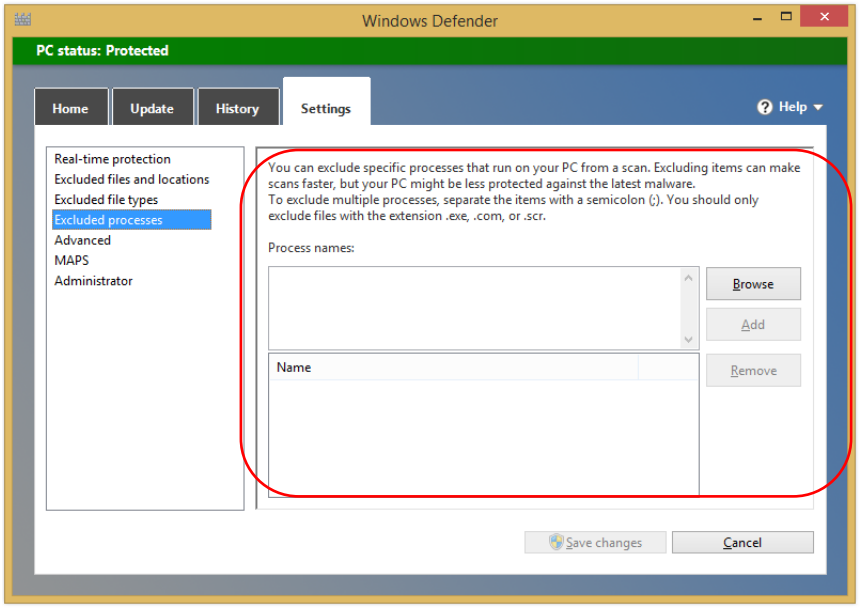
Gambar 7 Pengecualian Scan File atau Folder

8. Berikut ini pengaturan untuk mengecualikan tipe *file* tertentu dari proses scan oleh Windows Defender. Pengecualian ini dapat mempercepat proses *scanning* namun meningkatkan kerentanan komputer anda terhadap serangn virus, *malware* atau *spyware*.



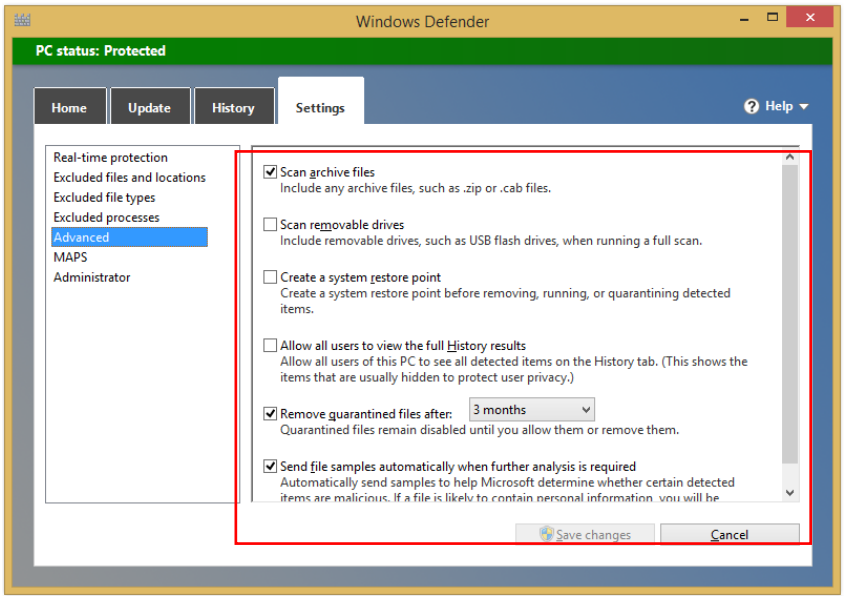
Gambar 8 Pengecualian Scan tipe File

9. Berikut ini pengaturan untuk mengecualikan proses tertentu dari proses scan oleh Windows Defender. Pengecualian ini dapat mempercepat proses *scanning* namun meningkatkan kerentanan komputer anda terhadap serangn virus, *malware* atau *spyware*.



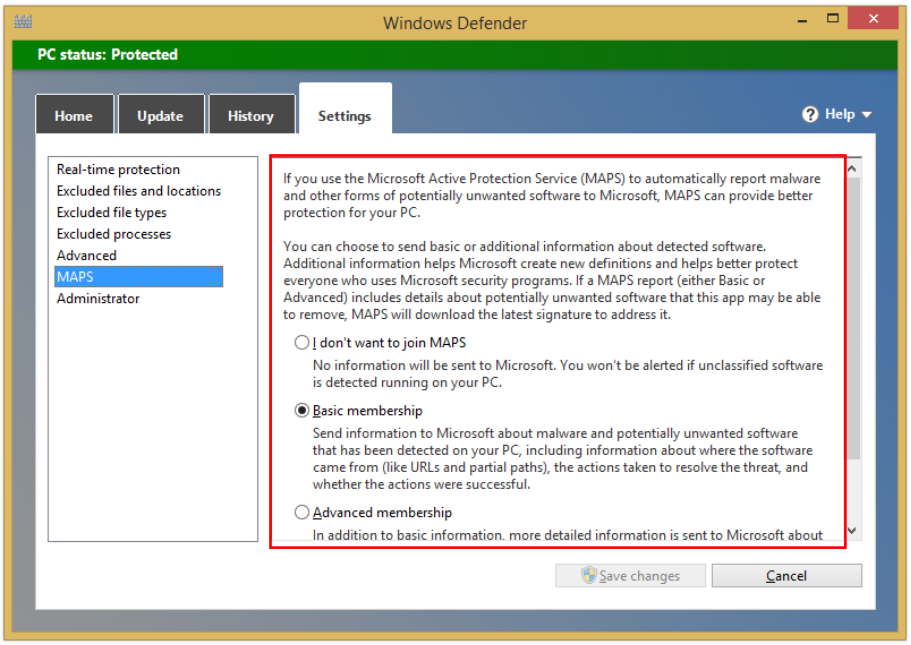
Gambar 9 Pengecualian Scan Proses Tertentu

10. Berikut ini pengaturan tingkat lanjut untuk Windows Defender, seperti:
    a. Scan file arsip
    b. Scan *removable drives* seperti Flashdisk
    c. Membuat titik *restore* sebelum menghapus, menjalankan atau karantina temuan dari Windows Firewall.
    d. Menghapus temuan dari Windows Defender yang telah dikarantina setelah beberapa waktu, sesuai pengaturan.
    e. Kirim hasil temuan ke Microsoft bila dibutuhkan Analisa lebih lanjut terkait temuan Windows Defender untuk menentukan bahwa file tersebut berbahaya untuk komputer.



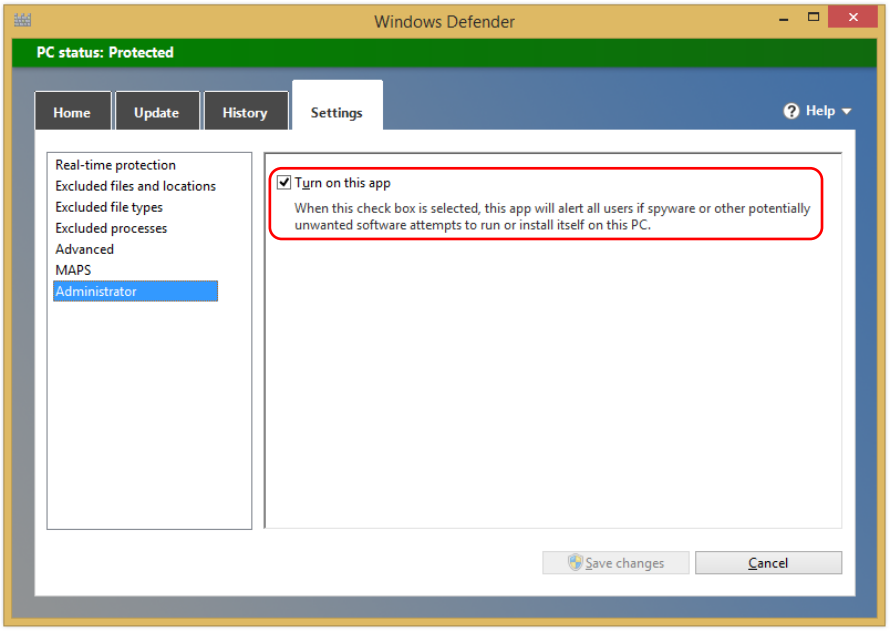
Gambar 10 Pengaturan Lebih Lanjut

11. Berikut ini pengaturan untuk menggunakan Microsoft Active Protection Service (MAPS) yang berfungsi untuk secara otomatis melaporkan *malware* atau perangkat lunak berbahaya lainnya ke Microsoft. Anda dapat memilih untuk tidak mengaktifkan pengaturan ini, mengirim informasi dasar atau informasi lengkap.



Gambar 11 Microsoft Active Protection Service

12. Pengaturan ini menentukan apakah Windows Defender akan memberikan notifikasi ketika *spyware* atau perangkat lunak berbahaya lainnya mencoba untuk menjalankan proses atau *install* sesuatu yang berbahaya di komputer.



Gambar 12 Pengaturan Notifikasi