AVG Protection

Panduan Pengguna

Revisi dokumen 2015.03 (10/24/2014)

Hak cipta AVG Technologies CZ, s.r.o. Semua hak dilindungi undang-undang.
Semua merek dagang lain adalah hak milik dari pemiliknya masing-masing.

AVG Protection

Daftar Isi

1. Pendahuluan

Selamat Anda telah membeli paket AVG Protection! Dengan paket ini, Anda dapat menikmati semua fitur **AVG Internet Security 2015**, kini ditingkatkan dengan **AVG Zen**.

AVG Zen

Alat administrasi yang tak ternilai ini dapat menjaga Anda sekaligus seluruh keluarga Anda. Semua perangkat Anda dikumpulkan dengan rapi di satu tempat, jadi Anda dapat dengan mudah mengawasi status Protection, Performance, dan Privacy tiap perangkat. Dengan **AVG Zen** hari-hari memeriksa setiap perangkat satu per satu telah berakhir; Anda bahkan diperbolehkan untuk menjalankan tugas pemindaian dan pemeliharaan dan memperbaiki masalah keamanan yang paling mendesak dari jarak jauh. **AVG Zen** dibangun ke dalam paket Anda, jadi aplikasi ini bekerja otomatis langsung dari awal.

Klik di sini untuk mempelajari selengkapnya tentang AVG Zen

AVG Internet Security 2015

Aplikasi keamanan pemenang penghargaan ini menyediakan beberapa lapis perlindungan untuk segala hal yang Anda lakukan online, yang berarti Anda tidak perlu khawatir dengan pencurian identitas, virus, atau mengunjungi situs berbahaya. AVG Protective Cloud Technology dan AVG Community Protection Network disertakan, yang artinya kami mengumpulkan informasi ancaman terbaru dan membaginya dengan komunitas kami untuk memastikan Anda menerima perlindungan terbaik. Anda dapat berbelanja dan melakukan transaksi bank secara online dengan aman, menikmati kehidupan Anda di jejaring sosial, atau menjelajah dan melakukan pencarian dengan nyaman dengan perlindungan waktu nyata.

Klik di sini untuk mempelajari selengkapnya tentang AVG Internet Security 2015

1.1. Persyaratan perangkat keras

Persyaratan perangkat keras minimum untuk **AVG Internet Security 2015**:

- Intel Pentium CPU 1,5 GHz atau yang lebih cepat
- 512 MB (Windows XP) / 1024 MB (Windows Vista, 7 dan 8) dari memori RAM
- 1.3 GB ruang hard drive kosong *(untuk keperluan instalasi)*

Persyaratan perangkat keras yang disarankan untuk **AVG Internet Security 2015**:

- Intel Pentium CPU 1,8 GHz atau yang lebih cepat
- 512 MB (Windows XP) / 1024 MB (Windows Vista, 7 dan 8) dari memori RAM
- 1.6 GB ruang hard drive kosong *(untuk keperluan instalasi)*

1.2. Persyaratan perangkat lunak

AVG Internet Security 2015 ditujukan untuk melindungi workstation dengan sistem operasi berikut:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 dan x64, semua edisi)
- Windows 7 (x86 dan x64, semua edisi)
- Windows 8 (x32 dan x64)

  (dan mungkin service pack yang lebih tinggi untuk sistem operasi tertentu)

Komponen Identity tidak didukung pada Windows XP x64. Pada sistem operasi ini Anda dapat menginstal AVG Internet Security 2015 tetapi tanpa komponen IDP.

2. AVG Zen

Bagian manual pengguna ini menyediakan dokumentasi pengguna yang komprehensif untuk AVG Zen. Harap dicatat bahwa Manual ini hanya menjelaskan versi PC dari produk ini.

AVG, pengembang perangkat lunak pengamanan terkenal di dunia, kini melangkah lebih dekat pada pelanggannya dan memenuhi kepuasan akan kebutuhan keamanan mereka. AVG Zen yang baru secara efektif menyambungkan perangkat dari desktop ke bergerak, data, dan orang di belakangnya bersama-sama dalam satu paket sederhana dengan tujuan lebih menyederhanakan kehidupan digital kita yang canggih. Hanya dengan satu aplikasi, AVG Zen memudahkan pengguna untuk melihat pengaturan keamanan dan privasi semua perangkat mereka dari satu tempat.

Ide di balik AVG Zen adalah untuk memberikan kembali kontrol kepada individu dengan semua perangkat ini atas data dan keamanan mereka seperti yang kami yakini melalui kontrol beberapa pilihan. Pada kenyataannya, AVG hadir di sini bukan untuk mengatakan bahwa berbagi dan pelacakan itu buruk; tetapi kami ingin mempersenjatai pelanggan kami dengan informasi yang memungkinkan mereka untuk mengontrol apa yang mereka bagikan dan untuk membuat keputusan sendiri dengan tepat jika mereka dilacak. Pilihan akan kebebasan untuk menjalani kehidupan seperti yang mereka inginkan, dan untuk menyatukan keluarga atau melamar pekerjaan tanpa perlu takut privasi mereka diserang.

Hal hebat lain tentang AVG Zen adalah bahwa produk ini memberi pelanggan kami pengalaman pengguna yang konsisten pada semua perangkat jadi bahkan pemula dapat belajar dengan cepat tentang mudahnya cara mengatur dan mengamankan banyak perangkat. Setidaknya ada satu hal yang semakin simpel di dalam dunia yang semakin kompleks. Namun hal terakhir dan paling penting, AVG Zen dirancang untuk memberi orang-orang ketenangan saat mereka menjalani kehidupan sehari-hari mereka. Saat Internet menjadi pusat dunia kita yang salin berhubungan, AVG Zen hadir untuk menyambungkan titik-titiknya.

okumentasi ini berisi keterangan tentang fitur khusus dari fitur AVG Zen. Jika Anda membutuhkan informasi mengenai produk AVG lainnya, lihat bagian lain dari dokumentasi ini, atau bahkan panduan pengguna lainnya yang terpisah. Anda dapat mengunduh panduan ini dari situs web AVG.

2.1. Proses instalasi Zen

Instalasi adalah rangkaian jendela dialog yang berisi keterangan singkat mengenai apa yang dilakukan di setiap langkah. Berikut ini, kami menyediakan penjelasan untuk setiap jendela dialog:

2.1.1. Dialog Selamat Datang

Proses instalasi selalu dimulai dengan jendela ini. Di sini Anda memilih **bahasa** yang digunakan dalam aplikasi AVG Zen.

Jika Anda ingin mengubah folder tujuan instalasi, klik tautan ***Sesuaikan instalasi Anda*** dan lakukan di dialog yang baru terbuka.

Selanjutnya, Anda dapat membaca ***Persetujuan Lisensi Perangkat Lunak AVG*** dan ***Kebijakan Privasi dan Personalisasi AVG***. Cukup klik tautan yang sesuai dan keseluruhan teks akan ditampilkan untuk Anda pada jendela baru.

Jika Anda menyetujui ketentuan ini, lanjutkan dengan instalasi dengan mengeklik tombol **Setuju dan Instal**.

Setelah instalasi berhasil, komputer perlu dihidupkan ulang. Anda dapat menghidupkan ulang dari dialog akhir dari instalasi ini (dengan mengeklik tombol **Hidupkan ulang sekarang**) atau membatalkannya untuk nanti. Namun, perlu dicatat bahwa tanpa menghidupkan ulang komputer, beberapa produk AVG mungkin tidak ditampilkan dengan benar di antarmuka pengguna Zen dan aplikasi sebagai keseluruhan mungkin tidak berfungsi dengan benar!

2.1.2. Folder Tujuan

Dialog ini opsional, dipicu dengan mengeklik tautan ***Sesuaikan instalasi Anda*** di dialog instalasi sebelumnya.

Di dalamnya, Anda dapat mengatur ***folder tujuan*** untuk instalasi Anda. Jika tidak puas dengan lokasi default tempat AVG Zen akan diinstal (yaitu ke folder Program files yang berada di drive C:), Anda dapat mengetikkan jalur baru secara manual ke kotak teks, atau menggunakan tautan **Jelajah** (di sebelah kotak teks). Menggunakan tautan akan menampilkan struktur drive dan memungkinkan Anda memilih foldernya masing-masing.

Sekarang klik tombol **Setuju dan Instal** untuk memulai proses instalasi itu sendiri.

Setelah instalasi berhasil, komputer perlu dihidupkan ulang. Anda dapat menghidupkan ulang dari dialog akhir dari instalasi ini (dengan mengeklik tombol **Hidupkan ulang sekarang**) atau membatalkannya untuk nanti. Namun, perlu dicatat bahwa tanpa menghidupkan ulang komputer, beberapa produk AVG mungkin tidak ditampilkan dengan benar di antarmuka pengguna Zen dan aplikasi sebagai keseluruhan mungkin tidak berfungsi dengan benar!

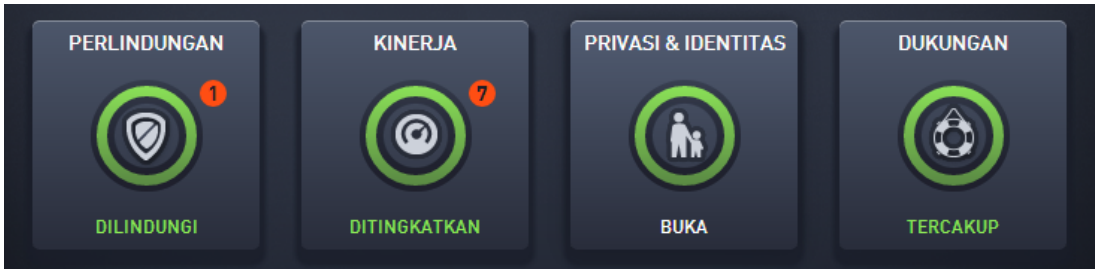
2.2. Antarmuka Pengguna Zen

Ini adalah dialog utama antarmuka pengguna AVG Zen Anda. Pada tiap dialog lain, selalu ada tombol  di sudut kiri atas – mengekliknya mengembalikan Anda ke layar utama ini (di beberapa dialog selanjutnya tombol ini hanya mengembalikan Anda satu langkah ke belakang, yaitu ke dialog sebelumnya dari rangkaian tersebut).

Dialog ini terdiri dari beberapa bagian berbeda:

- Ubin Kategori
- Pita Perangkat
- Tombol Pesan
- Tombol Status
- Tombol Segarkan
- Tombol Pengaturan

2.2.1. Ubin Kategori



Ubin Kategori memungkinkan Anda menginstal produk perangkat lunak AVG, untuk melihat statusnya, dan hanya untuk membuka antarmuka penggunanya. Administrator jaringan Zen juga dapat menggunakannya untuk melihat dan mengatur produk AVG yang diinstal pada perangkat jauh. Gunakan pita Perangkat untuk menjelajahi semua perangkat jauh yang tersedia di jaringan Zen Anda.

Di dalam setiap ubin, terdapat lingkaran, yang warnanya bergantung pada status produk di dalam kategori ini (Anda harus menjaganya tetap hijau). Untuk beberapa kategori, Anda mungkin hanya melihat semi lingkaran, yang berarti bahwa Anda telah memiliki produk untuk kategori ini, tetapi ada produk lain yang perlu diinstal.

Meskipun Anda selalu melihat rangkaian ubin yang sama apa pun perangkat yang Anda lihat, isi ubin mungkin berbeda bergantung pada perangkat yang diawasi (perangkat PC, Android atau Mac).

PROTECTION

AVG Internet Security – perangkat lunak keamanan ini menyediakan beberapa lapis perlindungan untuk segala hal yang Anda lakukan online, yang berarti Anda tidak perlu khawatir dengan pencurian identitas, virus, atau mengunjungi situs berbahaya. AVG Protective Cloud Technology dan AVG Community Protection Network disertakan, yang artinya kami mengumpulkan informasi ancaman terbaru dan membaginya dengan komunitas kami untuk memastikan Anda menerima perlindungan terbaik. Anda dapat berbelanja dan melakukan transaksi bank secara online dengan aman, menikmati kehidupan Anda di jejaring sosial, atau menjelajah dan melakukan pencarian dengan nyaman dengan perlindungan waktu nyata.

Gambaran umum dari status

- jika AVG Internet Security tidak diinstal, ubin ini tetap berwarna abu-abu dan teks di bawahnya tertulis "Not protected", tetapi Anda dapat mengekliknya untuk menginstal aplikasi AVG ini dengan mudah.
- jika ada terlalu banyak masalah untuk diperhatikan (seperti saat keseluruhan AVG Internet Security tidak aktif), lingkaran di dalam ubin ini ditampilkan dalam warna merah dan teks di bawahnya bertuliskan "Not protected". Apabila Anda hanya menghadapi beberapa masalah kecil, ubin ditampilkan dengan warna hijau, tetapi teks di bawahnya bertuliskan "Partially protected". Pada kedua situasi tersebut, Anda akan melihat angka dalam lingkaran oranye (di sudut kanan atas ubin) yang menunjukkan jumlah masalah yang mungkin perlu perhatian Anda. Gunakan tombol Messages untuk melihat daftar masalah dan kemungkinan penyelesaiannya.
- jika tidak ada masalah dengan AVG Internet Security, lingkaran di dalam ubin ditampilkan dalam warna hijau dan teks di bawahnya bertuliskan "Protected".

Apa yang terjadi setelah Anda mengeklik ubin ini:

- jika AVG Internet Security belum diinstal – dialog baru terbuka, memungkinkan Anda menginstal AVG Internet Security. Baca selengkapnya tentang menginstal produk AVG.
- Jika Anda melihat perangkat Anda sendiri dengan AVG Internet Security terinstal – antarmuka pengguna AVG Internet Security terbuka.
- jika Anda (sebagai administrator) melihat perangkat jauh dengan AVG Internet Security terinstal – membuka dialog berisi gambaran umum singkat dari status AVG Internet Security pada perangkat jauh. Dialog ini memperbolehkan Anda untuk melakukan beberapa tindakan jarak jauh, seperti menjalankan pemindaian (tombol **Scan Now**) atau melakukan pembaruan (tombol **Update**). Tindakan jarak jauh lainnya, seperti mengaktifkan komponen perlindungan yang sebelumnya nonaktif, dapat diakses dengan mengeklik tombol **Tampilkan Show details**, yang membuka dialog Messages di perangkat yang dipilih saat ini. Baca selengkapnya tentang melihat dan mengatur perangkat jauh.

PERFORMANCE

AVG PC TuneUp – dengan aplikasi ini, Anda dapat memulihkan kemampuan kinerja penuh dari sistem operasi, game, dan program Anda. AVG PC TuneUp juga dapat menjalankan tugas pemeliharaan secara otomatis, seperti membersihkan hard disk dan registri, atau Anda bisa menjalankannya sendiri secara manual. AVG PC TuneUp dengan cepat akan mengenali apakah ada masalah pasa sistem Anda dan menawarkan solusi sederhana. Anda juga dapat menggunakan AVG PC TuneUp untuk menyesuaikan penampilan sistem Windows sesuai kebutuhan pribadi Anda.

Gambaran umum dari status

- jika AVG PC TuneUp tidak diinstal, ubin ini tetap berwarna abu-abu dan teks di bawahnya tertulis "Not tuned up", tetapi Anda dapat mengekliknya untuk menginstal aplikasi AVG ini dengan mudah.
- Jika ada terlalu banyak masalah yang harus diselesaikan (seperti saat seluruh AVG PC TuneUp dinonaktifkan), lingkaran di dalam ubin ini tampil dengan warna merah dan teks di bawahnya bertuliskan “Not tuned up”. Apabila Anda hanya menghadapi beberapa masalah kecil, ubin ditampilkan dengan warna hijau, tetapi teks di bawahnya bertuliskan "Partially tuned up". Pada kedua situasi tersebut, Anda akan melihat angka dalam lingkaran oranye (di sudut kanan atas ubin) yang menunjukkan jumlah masalah yang mungkin perlu perhatian Anda. Gunakan tombol Messages untuk melihat daftar masalah dan kemungkinan penyelesaiannya.
- Jika tidak ada masalah dengan AVG PC TuneUp, lingkaran di dalam ubin ini tampil dengan warna hijau dan teks di bawahnya bertuliskan “Tuned up”.

Apa yang terjadi setelah Anda mengeklik ubin ini:

- jika AVG PC TuneUp belum diinstal – dialog baru terbuka, memungkinkan Anda menginstal AVG PC TuneUp. Baca selengkapnya tentang menginstal produk AVG.
- Jika Anda melihat perangkat Anda sendiri dengan AVG PC TuneUp terinstal – antarmuka pengguna AVG PC TuneUp terbuka.
- jika Anda (sebagai administrator) melihat perangkat jauh dengan AVG PC TuneUp terinstal – membuka dialog berisi gambaran umum singkat dari status AVG PC TuneUp pada perangkat jauh. Dialog ini memperbolehkan Anda untuk melakukan beberapa tindakan jarak jauh, seperti menjalankan pemeliharaan (tombol **Run Maintenance**) atau melakukan pembaruan (tombol **Update**). Tindakan jarak jauh lainnya dapat diakses dengan mengeklik tombol **Show details**, yang membuka dialog Messages di perangkat yang dipilih saat ini. Baca selengkapnya tentang melihat dan mengatur perangkat jauh.

PRIVASI & IDENTITAS

Kategori ini terdiri dari dua bagian yang berbeda – AVG PrivacyFix (add-on browser keamanan) dan Identity Protection (komponen dari aplikasi AVG Internet Security). Agar mendapatkan lingkaran penuh (hijau jika dimungkinkan) di dalam ubin ini, Anda harus memiliki kedua aplikasi tersebut terinstal.

AVG PrivacyFix – add-on browser ini membantu Anda memahami dan mengontrol pengumpulan data. Aplikasi ini memeriksa paparan privasi Anda pada Facebook, Google, dan LinkedIn, dan dengan sekali klik, membawa Anda ke pengaturan tempat Anda dapat memperbaikinya. Lebih dari 1200 pelacak dicegah dari mengikuti gerakan online Anda. Selain itu, Anda dapat melihat situs web mana yang memegang hak untuk menjual data pribadi Anda dan mudah meminta mereka menghapus apa yang mereka miliki tentang Anda. Akhirnya, Anda diperingatkan akan risiko privasi saat Anda mengunjugi situs dan diberi tahu saat kebijakan berubah.

AVG Internet Security – komponen Perlindungan Identitas – komponen ini (bagian dari aplikasi AVG Internet Security) memberi komputer Anda perlindungan waktu nyata dari ancaman baru dan bahkan tidak dikenal. Komponen ini memantau semua proses (termasuk yang tersembunyi) dan ratusan pola perilaku yang berbeda, serta dapat menentukan apakah sesuatu yang membahayakan terjadi dalam sistem Anda. Oleh karena itu, ia dapat mengetahui ancaman yang bahkan belum diterangkan dalam basis data virus.

Gambaran umum dari status

- jika tidak satu pun aplikasi di atas terinstal, ubin ini tetap berwarna abu-abu dan teks di bawahnya bertuliskan "Not set up", tetapi Anda dapat mengekliknya untuk menginstal aplikasi AVG ini dengan mudah.
- jika hanya salah satu dari dua aplikasi ini yang terinstal, hanya akan ada semi lingkaran di dalam ubin ini. Warnanya bergantung pada status aplikasi yang terinstal – bisa berwarna hijau (“Aktif” / “Protected”), atau merah (“Disabled” / “Not protected”).
- jika kedua aplikasi terinstal, satunya aftif dan lainnya nonaktif, lingkaran di dalam ubin ini akan bewarna merah, dengan teks bertuliskan “Partially protected”.
- jika kedua aplikasi tersebut terinstal dan aktif, Anda akan melihat lingkaran hijau penuh di dalam ubin ini, dengan teks bertuliskan “Protected”. Selamat, privasi dan identitas Anda terlindungi sepenuhnya!

Setelah Anda mengeklik ubin ini, dialog baru terbuka, berisi dua ubin tambahan – untuk AVG Identity Protection dan untuk AVG PrivacyFix. Ubin ini sama interaktif dan dapat diklik seperti ubin utama di antarmuka pengguna utama aplikasi AVG Zen Anda.

- jika salah satu atau kedua aplikasi ini belum diinstal, Anda dapat mengeklik tombol **Get It FREE** untuk memperbaikinya. Baca selengkapnya tentang menginstal produk AVG.
- jika setidaknya salah satu dari aplikasi ini terinstal, Anda dapat mengeklik ubinnya untuk membuka antarmuka penggunanya.
- jika Anda (sebagai administrator) melihat perangkat jauh dengan aplikasi ini terinstal – membuka dialog berisi gambaran umum singkat dari status kedua aplikasi ini pada perangkat jauh. Namun, dialog ini murni informatif dan Anda tidak dapat mengubah apa pun. Baca selengkapnya tentang melihat dan mengatur perangkat jauh.

SUPPORT

(lingkaran di dalam ubin berwarna hijau, saat dukungan tersedia, saat teks di bawahnya bertuliskan "Covered")

Mengeklik ubin ini membuka dialog baru yang berisi tautan browser ke sumber daya dukungan paling umum. Untuk membaca tentang opsi dukungan yang ditawarkan oleh AVG, klik di sini.

Anda mungkin perlu memeriksa topik terkait berikut:

- Bagaimana cara menginstal produk AVG?
- Bagaimana cara melihat dan/atau mengatur produk AVG?

Manual ini hanya berhubungan dengan aspek AVG Zen terkait PC; tetapi, sebagai administrator, kemungkinan Anda juga memiliki beberapa perangkat Android™ dalam jaringan Anda. Dalam kasus tersebut, jangan terkejut jika melihat konten yang berbeda dalam ubin Kategori perangkat ini.

Aplikasi mobile AVG yang saat ini tersedia:

- ***AVG AntiVirus*** (gratis atau berbayar) – aplikasi ini melindungi dari virus, malware, spyware dan pesan teks berbahaya dan membantu mengamankan data pribadi Anda. Dengan aplikasi ini, Anda akan mendapatkan perlidungan yang efektif dan mudah digunakan terhadap virus dan malware, serta pemindai aplikasi waktu nyata, pencari telepon, penghenti tugas, dan pembersih perangkat lokal untuk membantu membentengi Anda dari ancaman terhadap privasi dan identitas online. Perlindungan pemindai keamanan waktu nyata melindungi Anda dari aplikasi dan permainan unduhan.
- ***AVG Cleaner*** (gratis) – aplikasi ini memungkinkan Anda secara cepat menghapus dan membersihkan

browser, riwayat panggilan dan teks, serta mengenali dan menghapus data aplikasi dengan cache yang tidak diinginkan dari memori internal perangkat dan kartu SD. Penting untuk mengoptimalkan ruang disk untuk membantu perangkat Android™ Anda bekerja lebih baik dan berjalan lebih lancar.

- ***AVG PrivacyFix*** (gratis) – aplikasi ini memberi Anda cara sederhana untuk mengatur pengaturan privasi online melalui perangkat mobile Anda. Aplikasi ini memberi Anda akses ke satu dashboard utama yang menampilkan dengan cepat dan mudah apa yang Anda bagikan dan dengan siapa Anda berbagi data di Facebook, Google dan LinkedIn. Jika Anda ingin mengubah sesuatu, satu klik membawa Anda langsung ke tempat Anda dapat mengubah pengaturan Anda. Perlindungan pelacakan WiFi baru memungkinkan Anda menyetel jaringan WiFi yang Anda kenal di awal dan menyetujui serta menghentikan perangkat Anda dilacak melalui jaringan lain.

Kategori individual adalah sebagai berikut:

PROTECTION

Mengeklik ubin ini menampilkan info terkait **AVG AntiVirus** – tentang pemindaian dan hasilnya, sekaligus tentang pembaruan definisi virus. Sebagai administrator jaringan, Anda juga diperbolehkan untuk menjalankan pemindaian (tombol **Scan Now**) atau melakukan pembaruan (tombol **Update**) terhadap perangkat Android jarak jauh.

PERFORMANCE

Mengeklik ubin ini menampilkan data terkait kinerja, yaitu fitur kinerja mana dari **AVG AntiVirus** yang aktif (***Task Killer***, ***Status Battery Status***, ***Data Plan*** (versi berbayar saja) dan ***Storage Usage***), dan apakah aplikasi **AVG Cleaner** diinstal dan berjalan (sekaligus beberapa statistiknya).

PRIVACY

Mengeklik ubin ini menampilkan data terkait Privasi Anda, yaitu fitur Privasi mana dari **AVG AntiVirus** yang aktif (***App Lock***, ***App Backup*** dan ***Call and Message Blocker***), dan apakah aplikasi **AVG PrivacyFix** diinstal dan berjalan.

ANTI-THEFT

Mengeklik ubin ini menampilkan info tentang fitur ***Anti-Theft*** dari **AVG AntiVirus**, yang memungkinkan Anda menemukan perangkat mobile Anda yang dicuri menggunakan Google Maps. Jika ada versi berbayar (**Pro**) dari **AVG AntiVirus** terinstal pada perangkat yang tersambung, Anda akan melihat tambahan status fitur ***Camera Trap*** (mengambil foto rahasia dari siapa saja yang mencoba menimpa kunci mobile) dan fitur ***Penguncian Device Lock*** (memungkinkan pengguna mengunci perangkat mobile apabila kartu SIM diganti).

Anda mungkin perlu memeriksa topik terkait berikut:

- Bagaimana cara menyambungkan perangkat mobile Android Anda ke jaringan Zen yang ada?
- Bagaimana cara melihat dan/atau mengatur produk AVG?

Manual ini hanya berhubungan dengan aspek AVG Zen; terkait PC; tetapi, sebagai administrator kemungkinan Anda juga memiliki beberapa perangkat Mac dalam jaringan Anda. Dalam kasus tersebut, jangan terkejut jika melihat konten yang berbeda dalam ubin Kategori perangkat ini.

Saat ini aplikasi AVG Mac tersedia (hanya dalam bahasa Inggris):

- ***AVG AntiVirus*** (gratis) – aplikasi tangguh ini memungkinkan Anda untuk memindai virus dan ancaman lain dalam file atau folder tertentu, atau bahkan menjalankan pemindaian mendalam atas Mac Anda secara keseluruhan dengan sekali klik. Perlindungan waktu nyata juga tersedia, berjalan dengan tenang di latar belakang. Setiap file yang Anda buka, salin atau simpan secara otomatis dipindai tanpa memperlambat Mac Anda.
- ***AVG Cleaner*** (gratis) – aplikasi ini memungkinkan Anda membersihkan kesemrawutan yang tidak perlu seperti cache, file sampah, riwayat file unduhan, daftar isi sampah dll, untuk mengosongkan ruang disk. Aplikasi ini juga dapat menemukan file duplikat di hard drive Anda dan menghapus salinan yang tidak dibutuhkan dengan cepat.

Kategori individual adalah sebagai berikut:

PROTECTION

Mengeklik ubin ini menampilkan info terkait **AVG AntiVirus** – tentang pemindaian dan hasilnya, sekaligus tentang pembaruan definisi virus. Anda juga dapat melihat apakah perlindungan waktu nyatanya aktif atau nonaktif. Sebagai administrator jaringan, Anda juga diperbolehkan untuk memperbarui AVG AntiVirus pada perangkat jauh (tombol **Update**) atau mengaktifkan perlindungan nyata yang sebelumnya nonaktif (lewat dialog Messages yang dapat diakses dengan mengeklik tombol **Show details**). Baca selengkapnya tentang melihat dan mengatur perangkat jauh.

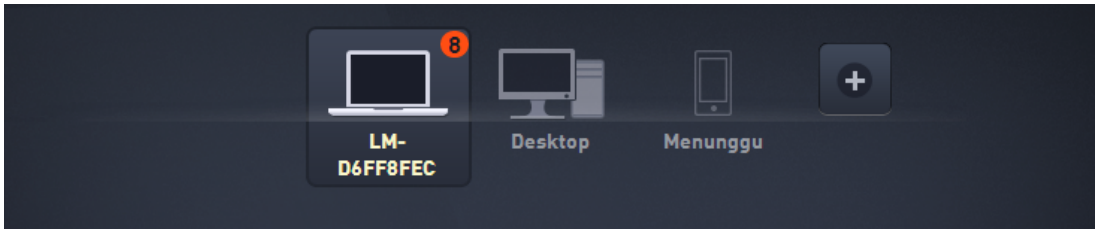
PERFORMANCE

Dengan mengeklik ubin ini, maka Anda akan melihat kinerja data, yaitu data tentang dua komponen **AVG Cleaner** – ***Disk Cleaner*** dan ***Duplicate Finder***. Anda dapat melihat pengujian dengan fitur kinerja yang terakhir dilakukan bersama dengan hasil pengujianya.

Anda mungkin perlu memeriksa topik terkait berikut:

- Bagaimana cara menyambungkan Mac Anda ke jaringan Zen yang ada?
- Bagaimana cara melihat dan/atau mengatur produk AVG?

2.2.2. Pita Perangkat



Bagian antarmuka pengguna AVG Zen ini menampilkan semua perangkat yang tersedia di jaringan Zen Anda. Jika Anda merupakan pengguna tunggal, atau Anda hanya tersambung ke jaringan Zen seseorang, Anda hanya akan melihat satu perangkat, perangkat Anda saat ini. Namun, sebagai Administrator jaringan, Anda bahkan dapat memiliki banyak perangkat untuk ditampilkan, sehingga Anda mungkin perlu menggunakan tombol panah untuk mengakses semua perangkat tersebut.

Pilih perangkat yang ingin Anda tampilkan dengan mengeklik ubinnya. Anda akan melihat bagian Kategori berubah

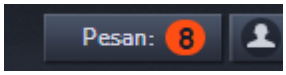
menyesuaikan, menampilkan status produk AVG di perangkat yang dipilih. Anda mungkin juga melihat nomor dalam lingkaran oranye muncul di sudut kanan atas pada beberapa ubin. Hal ini berarti bahwa ada masalah dengan produk AVG pada perangkat ini yang perlu Anda perhatikan. Klik tombol Pesan untuk melakukannya dan mendapatkan info selengkapnya.

Sebagai Administrator jaringan Zen, Anda mungkin perlu menambahkan perangkat baru ke jaringan Anda. Untuk melakukannya, klik  pada sisi kanan area.

Anda mungkin perlu memeriksa topik terkait berikut:

- Bagaimana cara menambahkan perangkat ke jaringan Anda?
- Bagaimana cara menghapus perangkat dari jaringan Anda?

2.2.3. Tombol Pesan



Tombol ini berada di atas pita Perangkat dan di sisi kiri tombol Status. Namun, tombol ini hanya muncul jika ada masalah dengan produk AVG pada perangkat Anda saat ini. Angka di lingkaran oranye menunjukkan jumlah masalah yang mungkin memerlukan perhatian Anda (lingkaran oranye ini bahkan dapat berisi tanda seru sebagai peringatan bahwa beberapa aplikasi AVG sama sekali tidak aktif).

Sebagai administrator jaringan, Anda juga dapat mengakses ***dialog Messages*** untuk perangkat jauh dengan mengeklik tombol **Show details** (di tampilan ubin Kategori). Perhatikan bahwa tombol ini hanya tersedia jika ada masalah mendesak yang memerlukan perhatian Anda. Klik di sini untuk membaca ini dan tindakan pengaturan jarak jauh lainnya.

Setelah mengeklik tombol ini, muncul dialog baru:

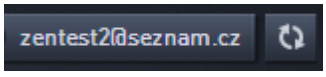
Dialog ini menampilkan daftar masalah yang diurutkan berdasarkan kategori produk. Masalah ditampilkan dalam warna berbeda (merah, kuning, atau hijau), memungkinkan untuk mengenali masalah darurat dari yang tidak terlalu mendesak.

Jika Anda merupakan administrator dengan lebih dari satu perangkat dalam jaringan Anda, dialog tampak sedikit berbeda. Ada gambaran umum perangkat pada sisi kiri, memungkinkan Anda melihat hanya pesan yang terkait dengan perangkat tertentu. Namun, jika Anda ingin melihat pesan dari semua perangkat dalam daftar urut, Anda dapat memilih opsi ***ALL DEVICES*** (ada di bagian paling atas gambaran umum).

Beberapa masalah dapat langsung ditangani dari dialog ini (biasanya disebut **Fix Now**) di sebelahnya. Sebagai administrator jaringan, Anda dapat memperbaiki beberapa masalah dari jarak jauh, langsung dari AVG Zen Anda. Sebagai pengguna tunggal atau tersambung Anda hanya dapat mengatur produk AVG pada perangkat Anda sendiri, walau tetap saja – akan lebih nyaman untuk melihat semua masalah sekaligus, tanpa harus membuka antarmuka aplikasi individual.

Sebagai contoh, saat Anda melihat teks ***"FIREWALL NEEDS RESTART - Untuk mengaktifkan Firewall, silakan hidupkan ulang komputer Anda"***, Anda dapat mengeklik tombol **Restart now**. Segera sesudahnya, komputer Anda akan dihidupkan ulang untuk mengaktifkan komponen Firewall.

2.2.4. Tombol Status



Tombol ini menampilkan mode pengguna saat ini. Sebagai administrator jaringan Zen Anda biasanya akan melihat email MyAccount yang Anda gunakan untuk menyambung ke jaringan.

Setelah mengeklik tombol ini, daftar tindakan tambahan ditampilkan. Tindakan yang tersedia bergantung pada mode pengguna yang saat ini Anda gunakan:

Sebagai pengguna tunggal:

- **Sambung** - memungkinkan Anda untuk menyabung ke jaringan Zen yang ada (atau untuk membuat jaringan baru).
- **Kunjungi AVG MyAccount** - memulai browser dan membuka situs web https://myaccount.avg.com/, memungkinkan Anda login ke AVG MyAccount.

Sebagai pengguna tersambung:

- **Login sebagai Admin** - klik untuk mendapatkan hak administrator, memungkinkan Anda melihat dan mengatur jaringan Zen ini (perlu login).
- **Tinggalkan Jaringan Ini** - klik untuk meninggalkan jaringan Zen ini (diperlukan konfirmasi).
- **Beritahu Saya Selengkapnya** - menampilkan dialog informatif tentang jaringan Zen yang saat ini tersambung dengan Anda dan menjadi administratornya.
- **Kunjungi AVG MyAccount** - memulai browser dan membuka situs web https://myaccount.avg.com/, memungkinkan Anda login ke AVG MyAccount.

Sebagai administrator:

- **Keluar sebagai Admin** - klik untuk melepaskan hak administrator Anda dan menjadi pengguna tersambung di dalam jaringan Zen yang sama.
- **Kunjungi AVG MyAccount** - memulai browser dan membuka situs web https://myaccount.avg.com/, memungkinkan Anda login ke AVG MyAccount.

Apakah AVG MyAccount itu?

AVG MyAccount merupakan layanan berbasis web (cloud) dari AVG yang memungkinkan Anda untuk:

- melihat informasi lisensi dan produk Anda yang telah didaftarkan
- mudah memperpanjang langganan Anda dan mengunduh produk Anda
- meriksa pesanan dan faktur yang lalu
- mengatur informasi pribadi dan kata sandi Anda
- gunakan AVG Zen

AVG MyAccount dapat diakses langsung di situs web https://myaccount.avg.com/.

Pada dasarnya, ada tiga mode pengguna di AVG Zen. Teks yang ditampilkan pada **tombol Status** bergantung pada mode mana yang saat ini Anda gunakan:

- **Pengguna tunggal** (tombol Status menampilkan ***Connect***) – yang baru saja Anda instal AVG Zen. Anda bukan administrator AVG MyAccount, atau tidak tersambung ke jaringan apa pun, jadi Anda hanya dapat melihat dan mengatur produk AVG yang terinstal pada perangkat ini.

- **Pengguna Tersambung** (tombol Status menampilkan ***Connected***) Anda telah menggunakan kode pemasangan, dengan demikian menerima undangan ke jaringan seseorang. Semua produk AVG pada perangkat Anda sekarang dapat dilihat dan diatur oleh administrator jaringan ini. Sedangkan Anda sendiri

masih dapat melihat dan mengatur produk AVG yang terinstal pada perangkat ini (apabila Anda adalah pengguna tunggal). Jika tidak lagi ingin tetap dalam sebuah jaringan, Anda dapat meninggalkannya dengan mudah.

- **Administrator** (tombol Status menampilkan ***nama AVG MyAccount*** saat ini) – Anda telah login menggunakan MyAccount Anda (mungkin sebelumnya Anda telah membuat yang baru). Artinya Anda memiliki akses ke semua fitur AVG Zen . Anda dapat menambah perangkat ke jaringan Anda, melihat dari jauh produk AVG yang terinstal pada perangkat dan, bila perlu, menghapusnya dari jaringan Anda. Anda bahkan dapat melakukan berbagai tindakan jarak jauh pada perangkat tersambung.

Anda mungkin perlu memeriksa topik terkait berikut:

- Bagaimana cara menerima undangan?
- Bagaimana cara menyambung ke jaringan Zen yang ada?
- Bagaimana cara membuat jaringan Zen baru?
- Bagaimana cara meninggalkan jaringan?
- Bagaimana cara melihat dan/atau mengatur produk AVG?

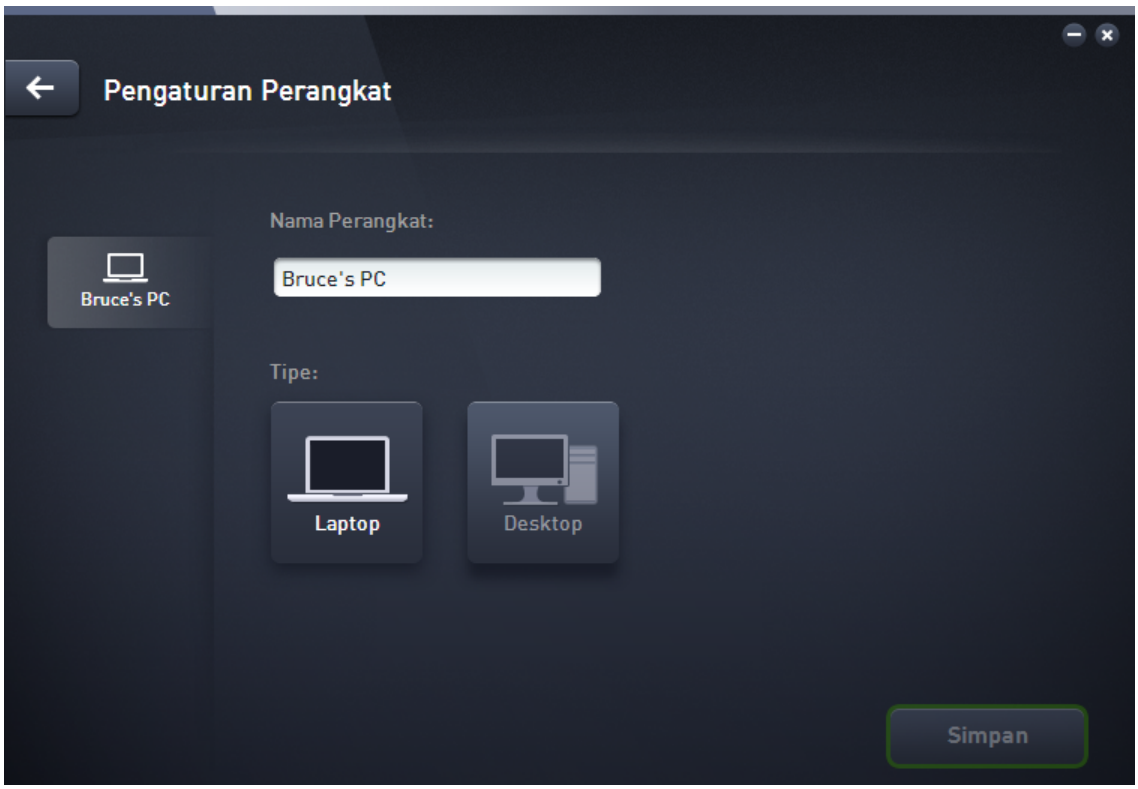
2.2.5. Tombol Segarkan

Mengeklik tombol kecil ini (di sebelah kanan tombol Status) akan segera menyegarkan semua data untuk semua perangkat dan kategori. Ini mungkin contoh yang berguna dalam kasus beberapa perangkat baru ditambahkan belum muncul pada pita Perangkat, tetapi Anda tahu bahwa perangkat tersebut sudah tersambung dan ingin melihat rinciannya.

2.2.6. Tombol Pengaturan

Mengeklik tombol kecil ini (ada di kanan tombol Segarkan) memicu munculnya dialog pop-up.

Anda dapat mengeklik opsi ***Pengaturan perangkat*** untuk membuka dialog Pengaturan Perangkat, emunkinkan Anda untuk mengubah nama dan tipe perangkat (sekaligus perangkat lain di jaringan Zen Anda, jika ada dan jika Anda merupakan administrator jaringan ini). Dialog ini juga memungkinkan Anda untuk menghapus perangkat dari jaringan Anda.



Selain itu, Anda dapat mengeklik opsi ***Tentang AVG Internet Security 2015*** untuk melihat info tentang produk perangkat lunak Anda atau bahan membaca Perjanjian Lisensi.

Anda mungkin perlu memeriksa topik terkait berikut:

- Bagaimana cara mengubah nama atau tipe perangkat?
- Bagaimana cara menghapus perangkat dari jaringan Anda?

2.3. Panduan langkah demi langkah

Bab ini berisi beberapa panduan langkah demi langkah yang menjelaskan operasi paling umum dalam lingkungan Zen.

2.3.1. Bagaimana cara menerima undangan?

Jika Anda menggunakan produk AVG di lebih dari satu perangkat, atau Anda merasa tidak cukup mampu dan ingin seseorang memantau produk AVG dan membantu Anda memperbaiki masalah apa pun, Anda mungkin perlu menambahkan PC atau perangkat bergerak Android™ Anda ke beberapa jaringan Zen yang ada. Namun, pertama-tama, Anda harus diundang oleh orang yang akan menjadi Administrator jaringan Anda, jadi minta dia untuk mengirimkan email undangan kepada Anda. Setelah Anda menerimanya, buka dan temukan **kode undangan** di dalamnya.

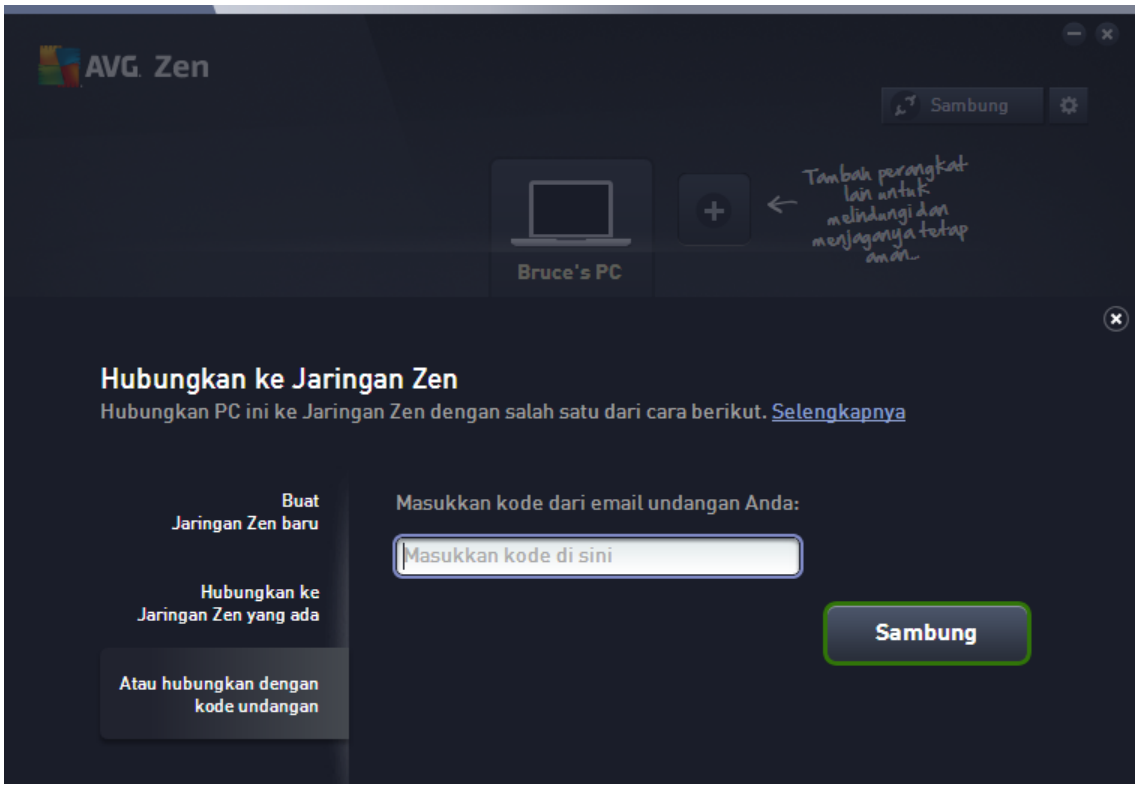
Yang Anda lakukan berikutnya bergantung pada apakah Anda ingin menambahkan PC atau perangkat bergerak Android™:

Perangkat PC:

1. Instal AVG Zen (jika Anda belum melakukannya).

2. Klik tombol Status (dengan teks bertuliskan ***Sambung***) dan konfirmasikan dengan mengeklik tombol ***Lanjutkan*** di dialog pop-up kecil.

3. Pilih panel ***Sambung dengan kode undangan*** pada sisi kiri subdialog yang baru terbuka.



4. Gunakan metode salin/tempel untuk menyalin kode undangan dari email ke kotak teks yang benar di subdialog Zen (atau ketik ulang secara manual).

Metode salin/tempel merupakan prosedur umum, memungkinkan Anda memasukkan hal yang dapat disalin (teks, gambar, dll.) ke Clipboard Windows, untuk ditempelkan ke tempat lain. Cara kerjanya sebagai berikut:

i. Sorot bagian teks, dalam hal ini kode undangan Anda di dalam email. Anda dapat melakukan itu dengan menahan tombol mouse sebelah kiri, atau tombol Shift.
ii. Tekan ***Ctrl+C*** pada keyboard (harap dicatat bahwa pada tahap ini, tidak akan ada bukti yang terlihat yang menandakan teks tersebut berhasil disalin).
iii. Pindah ke lokasi yang diinginkan, dalam hal ini dialog **Bergabung ke Jaringan Zen** dan kli kotak teks tempat Anda ingin menempelkan teks tersebut.
iv. Tekan ***Ctrl+V***.
v. Teks yang ditempelkan, dalam hal ini kode undangan Anda akan muncul. Selesai.

5. Klik tombol **Sambung**. Setelah beberapa saat, Anda akan menjadi bagian dari jaringan Zen pilihan Anda. Untuk Anda sendiri, tidak ada yang benar-benar berubah (hanya teks pada tombol Status Anda yang akan berubah ke ***Tersambung***). Namun, perangkat Anda akan diawasi oleh administrator jaringan mulai dari sekarang, yang memungkinkan administrator mengidentifikasi kemungkinan masalah dan membantu Anda memperbaikinya. Tetap saja, jika ingin meninggalkan jaringan ini, Anda mudah melakukannya kapan saja.

Perangkat bergerak Android:

Tidak seperti perangkat PC, koneksi jaringan pada perangkat bergerak Android dilakukan langsung di dalam aplikasi itu sendiri:

1. Pertama-tama, Anda harus menginstal salah satu aplikasi seluler AVG dan menyambungkannya ke beberapa jaringan Zen (klik di sini untuk mempelajari selengkapnya tentang koneksi seluler Android™ ke jaringan Zen yang ada). Pada kenyataannya, menerima undangan pada perangkat bergerak berarti bahwa Anda meninggalkan jaringan Zen saat ini dan beralih ke jaringan baru.

2. Buka aplikasi Anda dan ketuk ***ikon menu*** (yang merupakan logo aplikasi) yang berada di sudut kiri atas layar utama.

3. Setelah menu ditampilkan, ketuk opsi **Atur perangkat**.

4. Ketuk opsi **Gabung jaringan Zen lainnya** pada bagian paling bawah layar, lalu masukkan kode undangan yang sebelumnya dikirimkan kepada Anda oleh administrator jaringan ini dan ketuk **Gabung**.

5. Selamat! Anda kini menjadi bagian dari jaringan Zen. Namun, jika berubah pikiran, Anda dapat meninggalkannya dengan mudah kapan saja.

Perangkat Mac:

Tidak seperti perangkat PC, koneksi jaringan pada perangkat Mac dilakukan langsung di dalam aplikasi itu sendiri:

1. Pertama-tama, Anda harus menginstal salah satu aplikasi AVG Mac, bahkan mungkin menyambungkannya ke beberapa Zen jaringan (klik di sini untuk mempelajari selengkapnya tentang koneksi Mac ke jaringan Zen yang ada). Jika tersambung, klik tombol di ujung kanan atas layar aplikasi Anda (saat ini bertuliskan “Tersambung”) dan pilih **Tinggalkan Jaringan ini** dari menu turunan.

2. Tombol di ujung kanan atas layar aplikasi Anda kini bertuliskan “Tidak Tersambung”. Klik dan pilih opsi **Sambungkan** dari menu turunan.

3. Di dialog yang baru dibuka, klik opsi paling kanan **Gunakan kode undangan**.

4. Sebuah kotak teks muncul, memungkinkan Anda untuk memasukkan kode undangan yang sebelumnya dikirimkan pada Anda oleh administrator jaringan ini. Setelah memasukkan kode, klik tombol **Sambungkan**.

5. Selamat! Anda kini menjadi bagian dari jaringan Zen. Namun, jika berubah pikiran, Anda dapat meninggalkannya dengan mudah kapan saja.

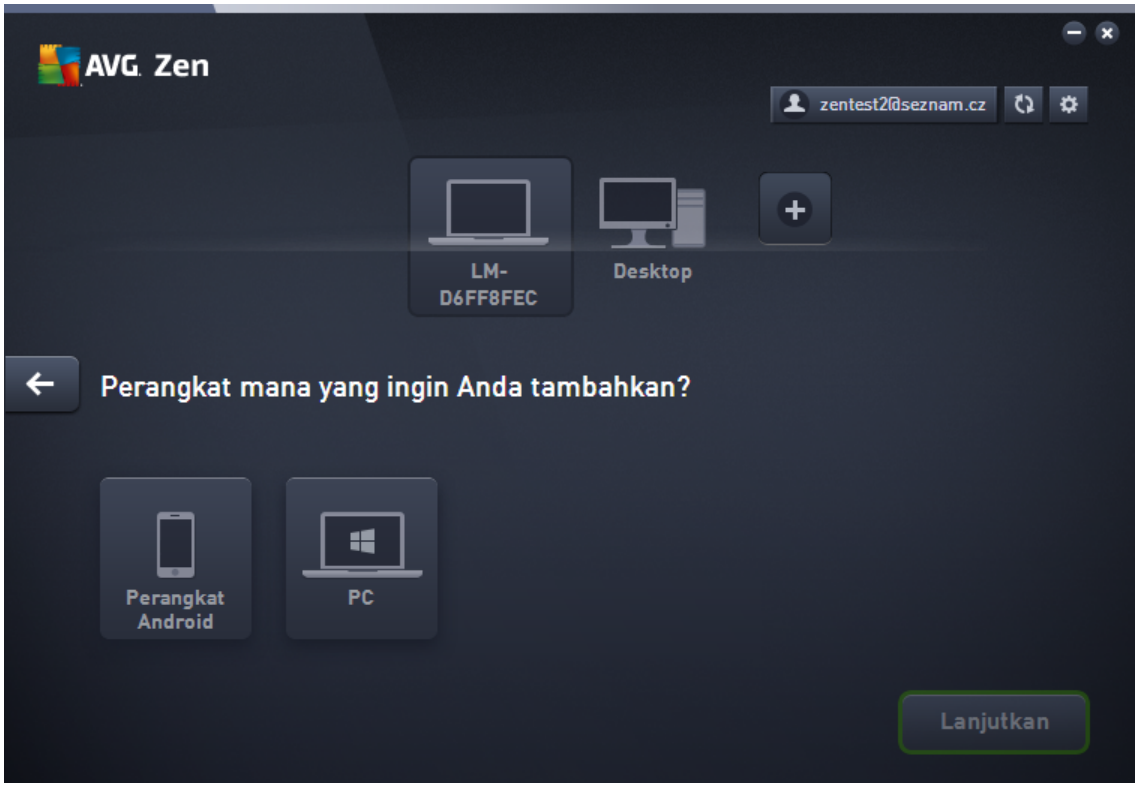
2.3.2. Bagaimana cara menambahkan perangkat ke jaringan Anda?

1. Untuk menambahkan perangkat baru ke jaringan Zen, Anda perlu mengundang perangkat tersebut terlebih dahulu. Untuk melakukannya, klik tombol  pada sisi kanan pita Perangkat.

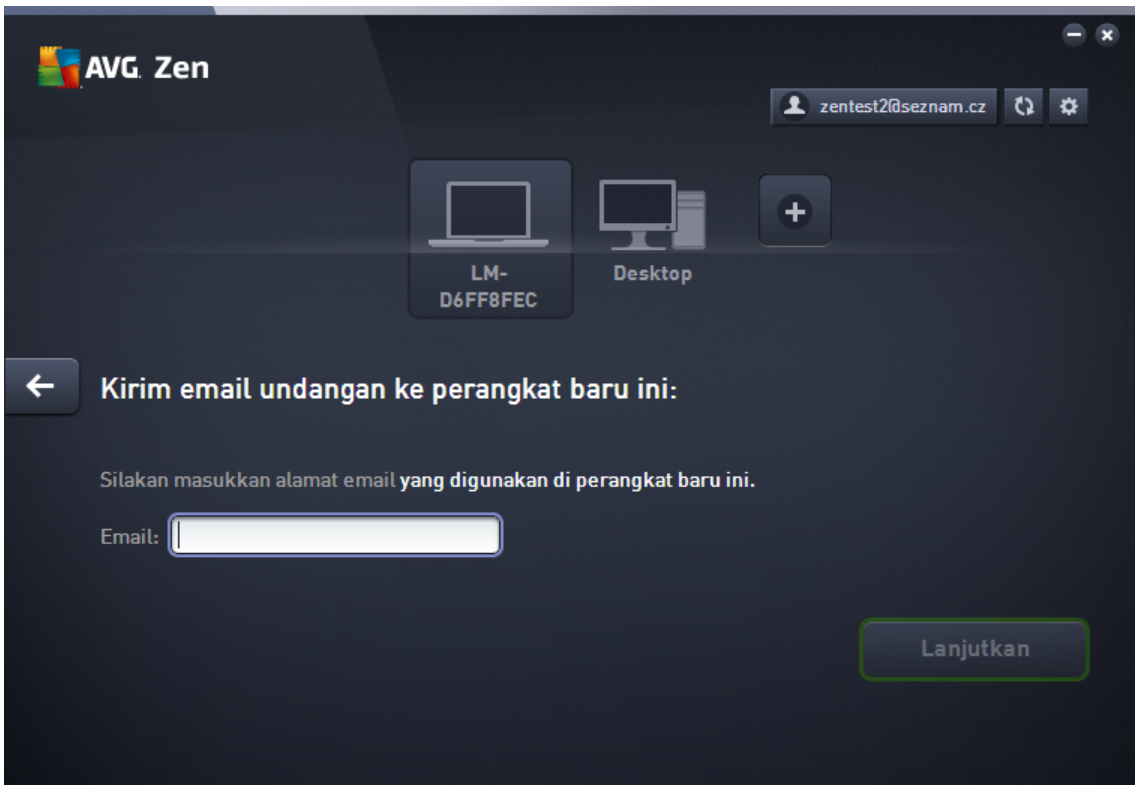
Harap dicatat bahwa hanya administrator yang dapat mengirim undangan dan menambahkan perangkat ke jaringan mereka. Jadi jika Anda saat ini tidak tersambung ke jaringan Zen apa pun, sambungkan, atau buat jaringan baru sendiri.

2. Muncul dialog baru. Pilih tipe perangkat yang ingin ditambahkan (misalnya PC atau perangkat bergerak

Android™) dengan menyorot ubin yang sesuai dan mengeklik tombol **Lanjutkan**.



3. Muncul dialog lain. Masukkan email yang digunakan pada perangkat baru dan klik tombol **Lanjutkan**.



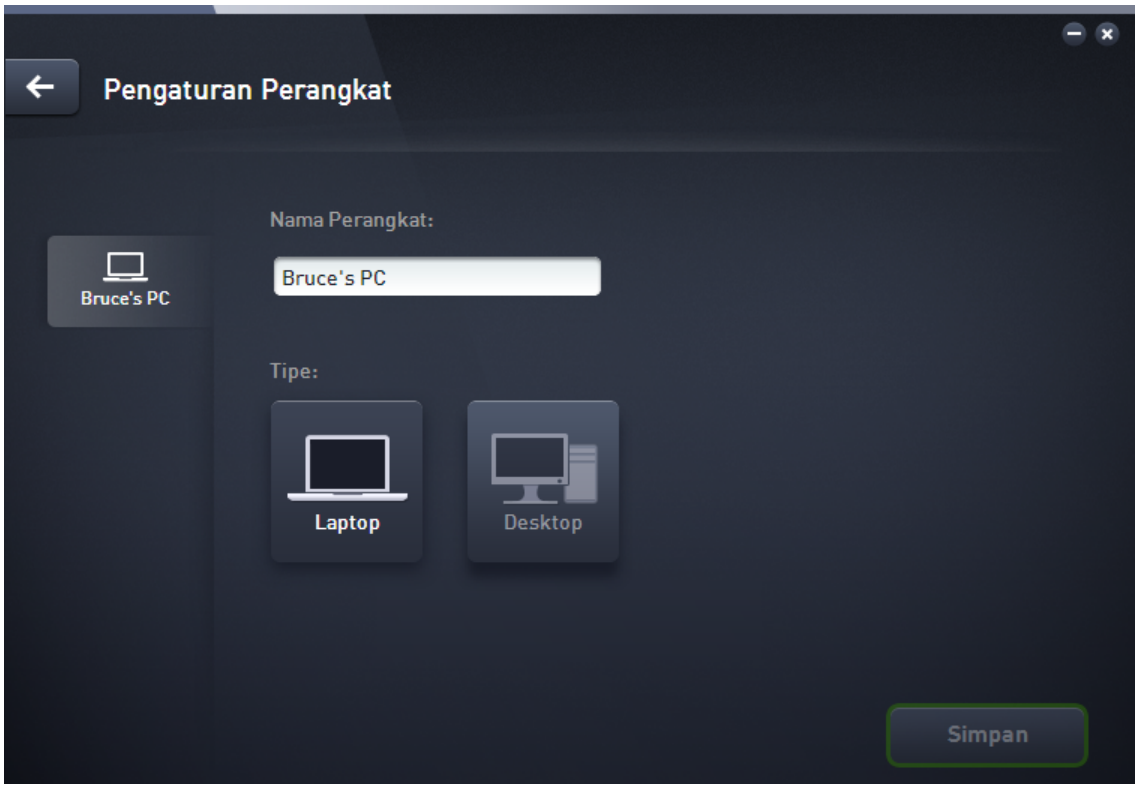
4. Email undangan terkirim. Perangkat kini ditampilkan pada pita Perangkat sebagai menunggu. Hal ini berarti undangan Anda menunggu untuk diterima.

Saat undangan Anda masih dalam status menunggu, Anda dapat memilih untuk **Mengirim Ulang Tautan Undangan**, atau **Membatalkan Undangan** secara keseluruhan.

5. Segera setelah undangan Anda diterima, Anda dapat mengubah nama dan tipe perangkat yang baru ditambahkan (Anda masih dapat melakukannya kapan saja di lain waktu). Sekarang, perangkat menjadi bagian dari jaringan Zen Anda dan Anda dapat melihat produk AVG yang terinstal di dalamnya dari jauh. Selamat, Anda telah menjadi administrator Zen yang sebenarnya!

2.3.3. Bagaimana cara mengubah nama atau tipe perangkat?

1. Klik tombol Pengaturan, lalu pilih ***Pengaturan Perangkat*** di dialog pop-up.



2. Pengaturan yang Anda lihat berlaku untuk perangkat yang saat ini Anda pilih. Daftar perangkat yang saat ini tersedia di jaringan Anda (yaitu perangkat yang telah menerima undangan) ditampilkan dalam kolom ubin pada sisi kiri dialog Pengaturan Perangkat. Cukup klik masing-masing ubin untuk beralih di antara mereka.

3. Kotak teks ***Nama Perangkat*** menampilkan nama perangkat yang saat ini Anda pilih. Anda dapat menghapus dan menggantinya dengan nama apa pun yang Anda sukai.

4. Di bawah, Anda dapat menetapkan ***Tipe*** perangkat yang saat ini Anda pilih (Telepon, Tablet, Laptop, atau Desktop). Cukup klik ubin yang sesuai.

5. Klik tombol **Simpan** untuk mengkonfirmasi perubahan Anda.

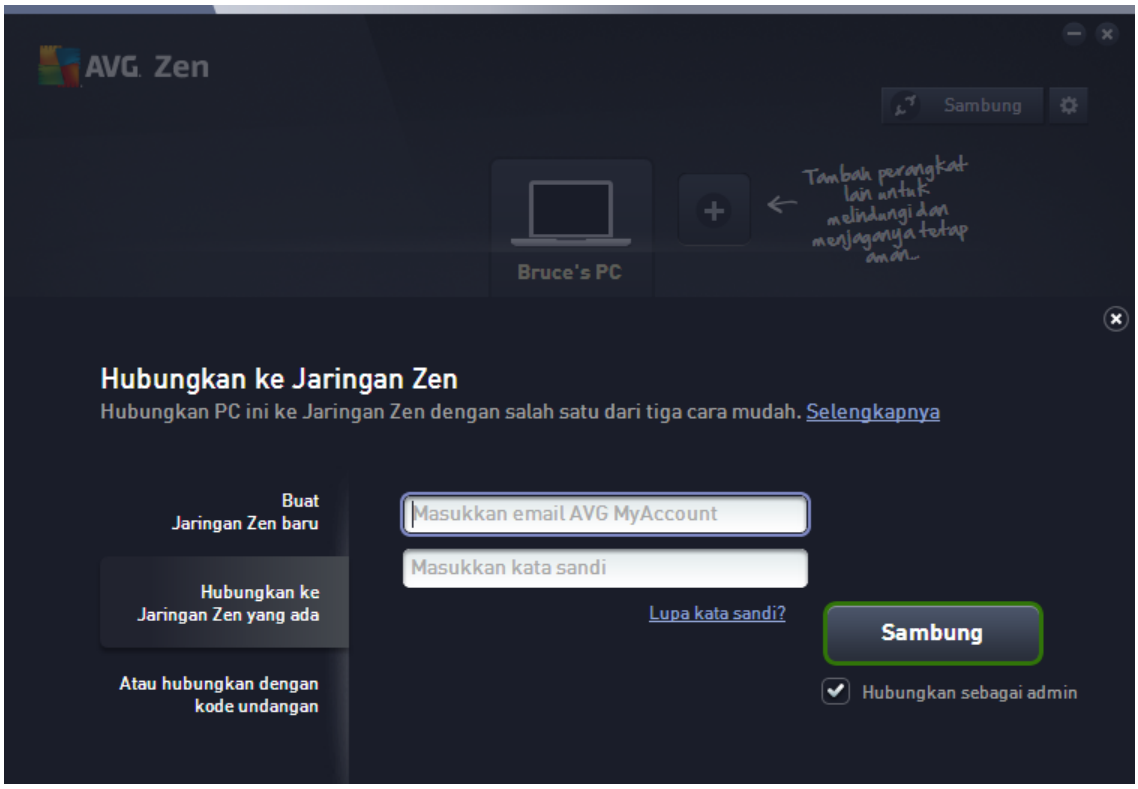
2.3.4. Bagaimana cara menyambung ke jaringan Zen yang ada?

Perangkat PC:

1. Jika Anda saat ini tidak login ke AVG MyAccount, klik tombol Status (dengan teks yang bertuliskan ***Connect***) dan konfirmasikan dengan mengeklik tombol **Continue** di dialog pop-up kecil.

Jika sudah tersambung ke beberapa AVG MyAccount, Anda perlu keluar terlebih dahulu agar tersambung ke MyAccount yang berbeda. Klik tombol Status (dengan nama AVG MyAccount Anda padanya) dan konfirmasikan dengan mengeklik tombol **Log Out** di dialog pop-up kecil.

2. Pilih panel ***Sambung to a existing Zen network*** pada sisi kiri subdialog yang baru terbuka.



3. Masukkan nama pengguna dan sandi AVG MyAccount Anda. Jika belum memiliki AVG MyAccount Anda sendiri, cukup buat yang baru sendiri. Jika Anda ingin login sebagai administrator, agar dapat melihat produk AVG pada perangkat jauh dalam jaringan Zen ini, tetap centang kontak ***Sambungkan sebagai admin***. Jika tidak, Anda hanya akan bertindak sebagai pengguna tersambung.

Jika Anda lupa sandi, klik tautan ***Forget password?*** (di bawah kotak teks sandi). Ini akan mengarahkan Anda ke situs web yang memungkinkan Anda memulihkan sandi Anda yang hilang.

4. Klik tombol **Connect**. Proses koneksi akan selesai dalam beberapa detik. Setelah koneksi berhasil, Anda akan melihat nama MyAccount Anda ditampilkan pada tombol Status.

Perangkat mobile Android:

Tidak seperti perangkat PC, koneksi jaringan pada perangkat mobile Android dilakukan langsung di dalam aplikasi itu sendiri:

1. Jika ingin menyambungkan perangkat mobile Android Anda ke jaringan Zen, Anda perlu mengunduh salah satu aplikasi mobile AVG (yaitu AVG AntiVirus, AVG Cleaner, dan/atau AVG PrivacyFix). Hal ini mudah dilakukan di Google Play, tempat semua aplikasi ini dapat diunduh dan diinstal secara gratis. Agar koneksi berfungsi dengan benar, pastikan Anda menggunakan versi terbaru yang tersedia.

2. Setelah aplikasi AVG Anda terinstal, buka aplikasi dan ketuk ***ikon menu*** (yang merupakan logo aplikasi) yang berada di sudut kiri atas layar utama.

3. Setelah menu ditampilkan, ketuk opsi **Manage devices**.

4. Di sini, ketuk tab **Login** dan masukkan kredensial AVG MyAccount yang benar (yaitu ***nama pengguna*** dan ***sandi*** Anda).

5. Selamat! Anda kini menjadi bagian dari jaringan Zen. Setelah mengeklik ikon menu, Anda kini akan melihat teks ***Tersambung sebagai:***, bersama dengan nama AVG MyAccount Anda saat ini pada bagian paling atas dari menu. Namun, jika berubah pikiran, Anda dapat meninggalkannya dengan mudah kapan saja.

Perangkat Mac:

Tidak seperti perangkat PC, koneksi jaringan pada perangkat Mac dilakukan langsung di dalam aplikasi itu sendiri:

1. Jika ingin menyambungkan perangkat Mac Anda ke jaringan Zen, Anda harus mengunduh salah satu aplikasi AVG Mac (misalnya AVG AntiVirus dan/atau AVG Cleaner). Hal ini mudah dilakukan misalnya di AVG Download Center atau di Mac App Store, tempat semua aplikasi ini dapat diunduh dan diinstal secara gratis. Agar koneksi berfungsi dengan benar, pastikan Anda menggunakan versi terbaru yang tersedia.

2. Setelah aplikasi AVG diinstal, bukalah. Anda akan melihat tombol oblong di ujung kanan atas layar aplikasi Anda (kini bertuliskan “Not Connected”). Klik dan pilih opsi **Connect** dari menu rentang-turun.

3. Di dialog yang baru dibuka, klik opsi tengah **Log in to AVG MyAccount** (pasti telah dipilih secara default).

4. Masukkan kredensial AVG MyAccount yang sesuai, misalnya ***nama pengguna*** (email MyAccount) dan ***sandi Anda***.

5. Selamat! Anda kini menjadi bagian dari jaringan Zen. Tombol di ujung kanan atas kini bertuliskan “Connected”; jika Anda mengekliknya, Anda dapat melihat jaringan mana yang saat ini sedang tersambung. Jika Anda berubah pikiran, Anda dapat dengan mudah meninggalkannya kapan pun.

2.3.5. Bagaimana cara membuat jaringan Zen baru?

Untuk membuat (dan mengelola) jaringan Zen baru, Anda harus membuat AVG MyAccount pribadi Anda terlebih dahulu. Pada dasarnya, ada dua cara untuk melakukannya - menggunakan browser web Anda atau langsung dari aplikasi AVG Zen itu sendiri.

Dari browser:

1. Gunakan browser untuk membuka situs web https://myaccount.avg.com/.

2. Klik tombol **Buat AVG MyAccount**.

3. Masukkan email yang Anda gunakan untuk login, atur sandi, ketik ulang, dan klik tombol **Buat akun**.

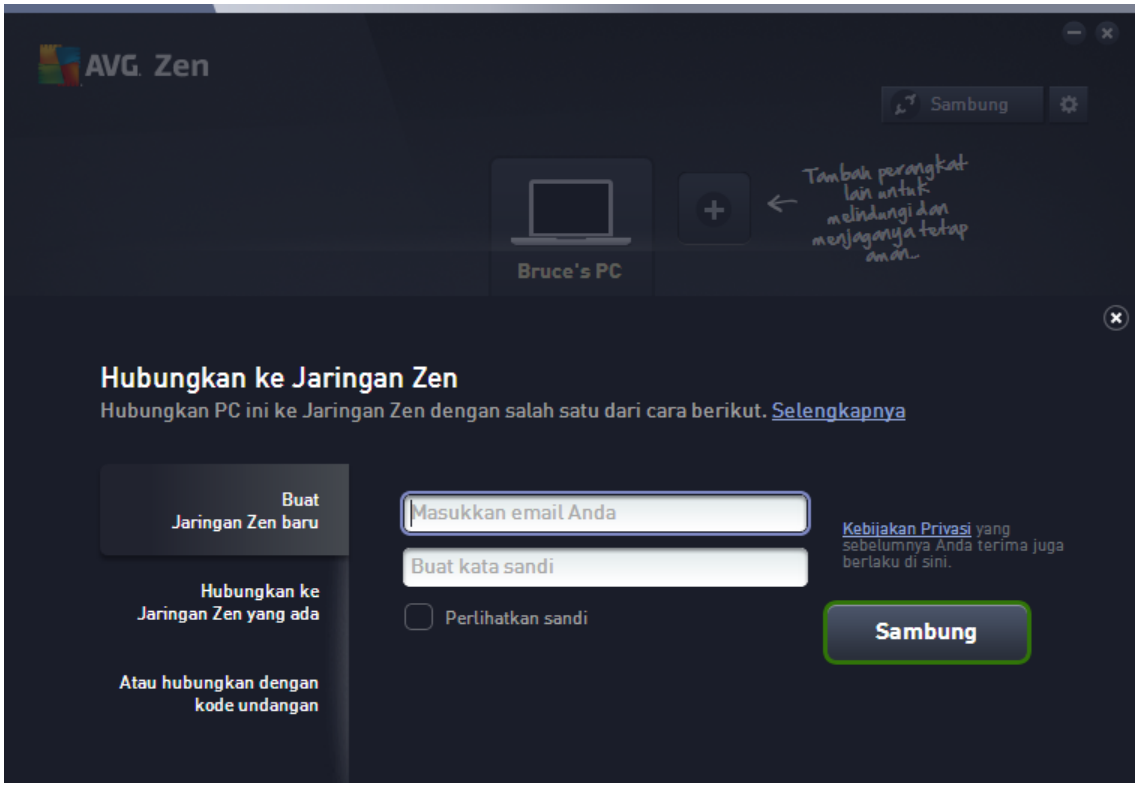
4. Tautan untuk mengaktifkan AVG MyAccount Anda akan dikirimkan kepada Anda (ke alamat email yang Anda gunakan di langkah 3). Anda perlu mengeklik tautan ini untuk menyelesaikan pembuatan MyAccount. Jika Anda tidak melihat email ini di kotak masuk Anda, email tersebut mungkin masuk ke folder spam.

Dari AVG Zen:

1. Jika Anda saat ini tidak login ke AVG MyAccount, klik tombol Status (dengan teks yang bertuliskan ***Sambung***) dan konfirmasikan dengan mengeklik tombol **Lanjutkan** di dialog pop-up kecil.

Jika sudah tersambung ke beberapa AVG MyAccount, Anda perlu keluar terlebih dahulu agar tersambung ke MyAccount yang berbeda. Klik tombol Status (dengan nama AVG MyAccount Anda padanya) dan konfirmasikan dengan mengeklik tombol **Keluar** di dialog pop-up kecil.

2. Pastikan panel ***Buat jaringan Zen baru*** pada sisi kiri subdialog yang baru terbuka dipilih.



3. Masukkan email yang Anda gunakan untuk login dan atur sandi (centang kotak ***Perlihatkan sandi*** di bawah jika Anda ingin melihat karakter tersembunyi), lalu klik tombol **Sambung**.

4. Setelah beberapa detik, Anda akan tersambung ke jaringan yang baru dibuat dengan hak administrator. Ini berarti bahwa Anda dapat menambah perangkat ke jaringan Anda, melihat dari jauh produk AVG yang terinstal pada perangkat tersebut dan, bila perlu, menghapusnya dari jaringan Anda.

2.3.6. Bagaimana cara menginstal produk AVG?

1. Produk AVG dapat diinstal dengan mudah lewat Zen. Untuk melakukannya, klik ubin Kategori pilihan Anda (ubin tersebut akan berwarna abu-abu menandakan bahwa Anda belum memiliki produk dari kategori ini, atau mungkin separuh hijau, yang berarti bahwa Anda sudah memiliki produk dari kategori ini, tetapi tidak ada sisa produk untuk diinstal).

2. Jika ingin segera memulai instalasi produk, yang Anda perlukan hanyalah mengeklik tombol **Dapatkan GRATIS**. Produk akan diinstal secara otomatis dengan pengaturan default.

   Jika ingin mengendalikan proses instalasi, klik tombol panah kecil (di sebelah kanan tombol **Dapatkan GRATIS**) dan klik **Instalasi khusus**. Dengan cara ini, Anda akan melihat instalasi sebagai rangkaian dialog, memungkinkan Anda mengubah folder tujuan, komponen yang terinstal, dll.

Proses instalasi beragam produk AVG secara detail dijelaskan di the bagian lain dari dokumentasi ini, atau bahkan panduan pengguna yang terpisah. Panduan ini dapat diunduh dengan mudah dari Situs web AVG.

3. Saat instalasi berlangsung, Anda akan melihat lingkaran hijau muncul di dalam ubin Kategori yang dipilih. Setelah instalasi berhasil, lingkaran hijau di dalam ubin menjadi penuh (di beberapa kategori mungkin hanya menjadi semi lingkaran, menandakan bahwa ada produk lain dalam kategori ini yang dapat diinstal). Harap dicatat bahwa lingkaran (atau semi lingkaran tersebut) dapat berubah ke warna berbeda (kuning atau merah) segera setelah instalasi; hal ini berarti bahwa ada beberapa masalah di dalam produk yang memerlukan perhatian Anda.

4. Anda akan mendapatkan pesan konfirmasi (muncul tepat di bawah ubin Kategori) bahwa instalasi telah berhasil diakhiri.

2.3.7. Bagaimana cara meninggalkan jaringan?

Perangkat PC:

1. Jika Anda merupakan bagian dari beberapa jaringan Zen dan ingin meninggalkannya, hal ini mudah untuk dilakukan. Pertama, klik tombol Status (dengan teks yang bertuliskan ***Tersambung***) dan klik tombol **Tinggalkan Jaringan Ini** di dialog pop-up kecil untuk melanjutkan.

2. Sekarang Anda perlu mengkonfirmasi bahwa Anda benar-benar ingin meninggalkan jaringan Zen. Untuk melakukannya, klik tombol **Tinggalkan**.

3. Setelah beberapa detik, Anda akan diputus sambungannya secara permanen. Administrator jaringan Anda sebelumnya tidak akan dapat mengatur produk AVG pada PC Anda. Teks pada tombol Status Anda akan berubah ke ***Sambung*** (yaitu kondisi awalnya).

Perangkat bergerak Android:

Tidak seperti perangkat PC, koneksi jaringan pada perangkat bergerak Android dilakukan langsung di dalam aplikasi itu sendiri:

1. Buka aplikasi AVG Anda dan ketuk ***ikon menu*** (yang merupakan logo aplikasi) yang berada di sudut kiri atas layar utama.

2. Pada bagian paling atas menu, Anda akan melihat teks ***Anda tersambung sebagai:***, bersama dengan nama AVG MyAccount Anda saat ini. Di sebelahnya, ada ikon pintu kecil dengan panah mengarah ke kanan. Klik ikon tersebut.

3. Konfirmasikan bahwa Anda benar-benar ingin meninggalkan jaringan Zen dengan mengkik tombol **OK**.

4. Setelah beberapa detik, Anda akan diputus sambungannya secara permanen. Administrator jaringan Anda sebelumnya tidak akan dapat mengatur produk AVG pada perangkat bergerak Android™ Anda. Namun, Anda dapat menyambung jaringan Zen ini (atau jaringan lain) kembali – baik langsung, maupun dengan menerima undangan.

Perangkat Mac:

Tidak seperti perangkat PC, koneksi jaringan pada perangkat Mac dilakukan langsung di dalam aplikasi itu sendiri:

1. Buka aplikasi AVG Anda dan klik tombol oblong di ujung kanan atas layar aplikasi Anda (kini bertuliskan “Tersambung”).

2. Pada bagian paling atas menu, Anda akan melihat teks ***Anda tersambung ke Jaringan Zen berikut: teks***, bersama dengan nama AVG MyAccount Anda.

3. Tepat di bawah info jaringan Zen, terdapat sebuah opsi **Tinggalkan Jaringan Ini**. Klik ikon tersebut.

4. Setelah beberapa detik, Anda akan diputus sambungannya secara permanen. Administrator jaringan Anda sebelumnya tidak akan dapat mengatur produk AVG pada PC Anda. Namun, Anda dapat menyambung jaringan Zen ini (atau jaringan lain) kembali – baik langsung, maupun dengan menerima undangan.

2.3.8. Bagaimana cara menghapus perangkat dari jaringan Anda?

1. Jika tidak ingin beberapa perangkat menjadi bagian dari jaringan Zen lagi, Anda dapat menghapusnya dengan mudah. Klik tombol Pengaturan, lalu pilih ***Pengaturan Perangkat*** di dialog pop-up.

2. Pada sisi kiri dialog Pengaturan Perangkat, terdapat daftar perangkat yang saat ini tersedia di jaringan Anda ditampilkan dalam kolom ubin. Alihkan ke perangkat yang ingin Anda hapus dengan mengeklik ubin dengan nama perangkat.

3. Anda akan melihat tautan ***Hapus dari Jaringan*** di samping sudut bawah dialog. Klik tautan tersebut.

Ingat bahwa tidak ada tautan seperti itu di pengaturan untuk perangkat yang saat ini Anda gunakan. Perangkat dianggap inti dari jaringan Anda dan oleh karenanya tidak dapat dihapus.

4. Sekarang Anda perlu mengkonfirmasi bahwa Anda benar-benar ingin menghapus perangkat ini dari jaringan Zen. Untuk melakukannya, klik tombol **Hapus**.

5. Perangkat akan dihapus secara permanen setelah beberapa detik. Anda tidak akan dapat mengatur produk AVG pada perangkat tersebut lagi; perangkat yang dihapus juga akan hilang dari pita Perangkat di Antarmuka Pengguna Anda.

2.3.9. Bagaimana cara melihat dan/atau mengatur produk AVG?

Jika Anda ingin melihat dan mengatur perangkat Anda sendiri

Pada kenyataannya, yang perlu Anda lakukan hanyalah mengeklik ubin Kategori yang sesuai. Hal ini membuka antarmuka pengguna produk AVG, memungkinkan Anda menjelajahi dan mengkonfigurasi sebanyak yang Anda inginkan. Sebagai contoh, mengeklik ubin ***PROTECTION*** membuka antarmuka pengguna AVG Internet Security, dll. Jika sebuah kategori terdiri dari lebih dari satu produk, Anda perlu mengeklik ubin lalu memilih sub ubin yang sesuai (seperti AVG PrivacyFix di bawah kategori ***PRIVASI & IDENTITAS***).

Produk AVG dapat dilihat dan dikelola lewat Zen secara detail dijelaskan di bagian lain dokumentasi ini, atau bahkan di panduan pengguna yang terpisah. Silakan mengunduh panduan ini dari situs web AVG.

Apabila ada masalah mendesak yang memerlukan perhatian Anda, Anda juga dapat mengeklik tombol Pesan. Dialog yang baru terbuka berisi daftar masalah dan kesulitan; beberapa di antaranya bahkan dapat ditangani langsung dari dialog ini - seperti masalah yang muncul dengan tombol tindakan khusus di sampingnya.

Jika Anda ingin melihat dan mengatur perangkat jauh (hanya administrator)

Hal ini juga cukup mudah. Pilih perangkat yang ingin Anda lihat dari pita Perangkat dan klik ubin Kategori yang sesuai. Kemudian, dialog baru terbuka, berisi gambaran umum singkat dari status produk AVG dalam kategori ini.

Sebagai administrator, Anda dapat menggunakan beberapa tombol untuk melakukan berbagai tindakan jarak jauh pada produk AVG dalam jaringan Zen Anda. Tindakan yang tersedia tergantung pada tipe perangkat (PC, Android atau Mac) dan ubin Kategori yang sedang Anda lihat saat ini. Perhatikan bahwa beberapa tindakan (seperti pemindaian atau pembaruan) mungkin tidak dapat diakses jika telah dilakukan baru-baru ini. Yang terdaftar di bawah ini merupakan semua tindakan jarak jauh yang tersedia untuk produk AVG:

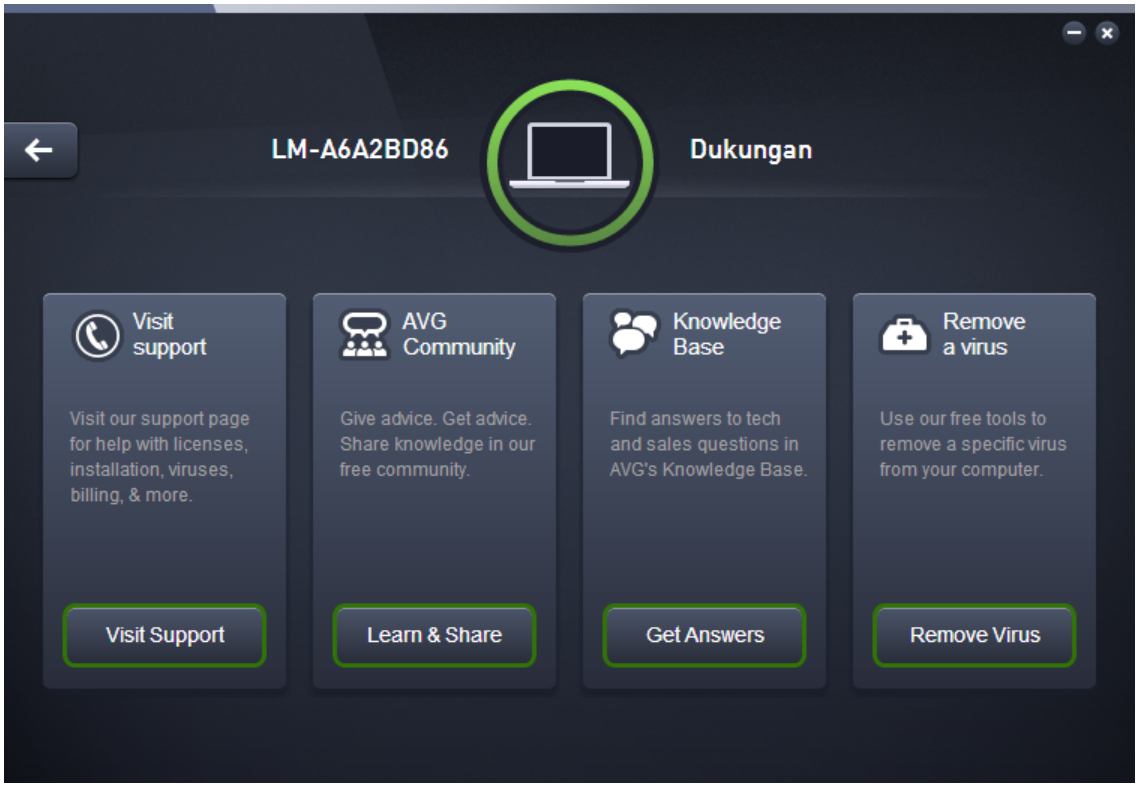
DEVICE TYPE	UBIN Kategori	TINDAKAN JAUH YANG TERSEDIA
PC	***PROTECTION (AVG Internet Security)***	• Tombol **Pindai Sekarang Juga** – segera klik untuk mulai memindai, memeriksa virus dan perangkat lunak berbahaya lainnya di perangkat jauh. Setelah pemindaian selesai, Anda akan segera diberi tahu tentang hasilnya. Klik di sini untuk mempelajari lebih lanjut tentang pemindaian di AVG Internet Security. • Tombol **Perbarui** – klik untuk mulai proses pembaruan AVG Internet Security pada perangkat jauh. Semua aplikasi antivirus harus selalu diperbarui untuk memastikan tingkat perlindungan yang maksimum. Klik di sini untuk mempelajari lebih lanjut tentang pentingnya pembaruan di AVG Internet Security. • Tombol **Tampilkan perincian** – tombol ini hanya tersedia jika ada masalah mendesak yang memerlukan perhatian Anda. Klik untuk membuka dialog Pesan di perangkat yang dipilih saat ini. Dialog ini

DEVICE TYPE	UBIN Kategori	TINDAKAN JAUH YANG TERSEDIA
		menampilkan daftar masalah yang diurutkan berdasarkan kategori produk. Beberapa di antaranya dapat langsung diatasi dengan mengeklik tombol **Fix Now**. Di AVG Internet Security, Anda dapat mis. mengaktifkan komponen perlindungan yang sebelumnya nonaktif.
PC	***PERFORMANCE (AVG PC TuneUp)***	• Tombol **Jalankan Pemeliharaan** – klik untuk memulai pemeliharaan sistem – serangkaian tugas didesain untuk membersihkan sistem pada perangkat jauh, mempercepatnya dan mengoptimalkan kinerjanya. • Tombol **Perbarui** – klik untuk memulai proses pembaruan AVG PC TuneUp pada perangkat jauh. Sangat penting untuk selalu memperbarui AVG PC TuneUp, karena fitur individualnya terus dikembangkan atau diselaraskan untuk menyesuaikan teknologi terbaru dan kesalahan yang diperbaiki. • Tombol **Tampilkan perincian** – tombol ini hanya tersedia jika ada masalah mendesak yang memerlukan perhatian Anda. Klik untuk membuka dialog Pesan di perangkat yang dipilih saat ini. Dialog ini menampilkan daftar masalah yang diurutkan berdasarkan kategori produk. Beberapa di antaranya dapat langsung diatasi dengan mengeklik tombol **Fix Now**.
Android	***PROTECTION (AVG AntiVirus)***	• Tombol **Pindai Sekarang Juga** – segera klik untuk mulai memindai, memeriksa virus dan konten berbahaya lainnya di perangkat Android jarak jauh. Setelah pemindaian selesai, Anda akan segera diberi tahu tentang hasilnya. • Tombol **Perbarui** – klik untuk mulai proses pembaruan AVG AntiVirus pada perangkat Android jarak jauh. Semua aplikasi antivirus harus selalu diperbarui untuk memastikan tingkat perlindungan yang maksimum. • Tombol **Tampilkan perincian** – tombol ini hanya tersedia jika ada masalah mendesak yang memerlukan perhatian Anda. Klik untuk membuka dialog Pesan di perangkat yang dipilih saat ini. Dialog ini menampilkan daftar masalah yang diurutkan berdasarkan kategori produk. Namun, untuk AVG AntiVirus untuk Android dialog ini murni informatif dan Anda tidak dapat mengubah apa pun.
Mac	***PROTECTION (AVG AntiVirus)***	• Tombol **Perbarui** – klik untuk mulai proses pembaruan AVG AntiVirus pada perangkat Mac jarak jauh. Semua aplikasi antivirus harus selalu diperbarui untuk memastikan tingkat perlindungan yang maksimum. • Tombol **Tampilkan perincian** – tombol ini hanya tersedia jika ada masalah mendesak yang memerlukan perhatian Anda. Klik untuk membuka dialog Pesan di perangkat yang dipilih saat ini. Dialog ini

DEVICE TYPE	UBIN Kategori	TINDAKAN JAUH YANG TERSEDIA
		menampilkan daftar masalah yang diurutkan berdasarkan kategori produk. Untuk AVG AntiVirus untuk Mac, Anda dapat menggunakan tombol **Fix Now** untuk mengaktifkan perlindungan nyata yang sebelumnya nonaktif.

2.4. Tanya-Jawab dan Dukungan

Dukungan pengguna untuk AVG Zen mudah diakses kapan saja lewat ubin kategori ***DUKUNGAN***.



Dialog baru yang Anda buka berisi tautan browser ke sumber daya dukungan paling umum.

NAMA KATEGORI	TEKS TOMBOL	KETERANGAN
Kunjungi dukungan	***Kunjungi Dukungan***	Halaman ini memberi Anda akses ke dukungan pengguna AVG profesional. Anda dapat mengajukan pertanyaan terkait lisensi, instalasi, virus, dan fitur produk tertentu.
Komunitas AVG	***Belajar & Berbagi***	Forum AVG merupakan cara hebat untuk mendapatkan saran dari pengguna AVG lainnya (tetapi Anda

NAMA KATEGORI	TEKS TOMBOL	KETERANGAN
		juga bisa memberikan bagian dengan saran Anda sendiri). Silakan berbagi pengetahuan Anda dalam komunitas pelanggan AVG ini.
Basis Pengetahuan	***Dapatkan Jawaban***	Beberapa pertanyaan tentang produk AVG lebih sering ditanyakan daripada yang lain. Pada halaman ini, Anda akan menemukan jawaban atas pertanyaan yang paling umum. Silakan mencobanya - mungkin solusi masalah Anda sudah menunggu di sana.
Hapus virus	***Hapus virus***	AVG menawarkan sejumlah alat perangkat lunak gratis yang mampu menghapus virus tertentu dari komputer Anda. Anda dapat mengunduhnya dari halaman ini.

3. AVG Internet Security

Bagian manual pengguna ini menyediakan dokumentasi pengguna yang komprehensif untuk **AVG Internet Security 2015**.

Namun, Anda mungkin juga ingin menggunakan sumber informasi lainnya:

- ***File Bantuan***: Bagian *Pemecahan masalah* tersedia langsung di file bantuan yang telah disertakan **AVG Internet Security 2015** *(untuk membuka file bantuan, tekan tombol F1 di setiap dialog pada aplikasi)*. Bagian ini menyediakan daftar situasi yang paling sering terjadi bila pengguna ingin mencari bantuan profesional untuk masalah teknis. Harap pilih situasi yang paling mirip dengan masalah Anda, dan klik untuk membuka petunjuk terperinci yang mengarahkan pada solusi masalah.

- ***Pusat Dukungan Situs Web AVG***: Atau, Anda dapat mencari solusi bagi masalah Anda pada situs Web AVG (*http://www.avg.com/*). Di bagian ***Pusat Dukungan*** Anda dapat menemukan tinjauan umum terstruktur atas grup tema yang menyangkut masalah penjualan dan teknis.

- ***Pertanyaan yang sering diajukan***: Pada situs Web AVG (*http://www.avg.com/*) Anda juga dapat menemukan bagian terstruktur terpisah dan menyatu atas pertanyaan yang sering diajukan. Bagian ini dapat diakses melalui opsi menu ***Pusat Dukungan / Tanya-Jawab dan Tutorial***. Sekali lagi, semua pertanyaan terbagi dengan rapi dalam kategori penjualan, teknis, dan virus.

- ***AVG ThreatLabs***: Situs web terkait AVG khusus (*http://www.avgthreatlabs.com/website-safety-reports/*) yang didedikasikan untuk masalah virus dengan menyediakan gambaran umum terstruktur mengenai informasi terkait ancaman online. Anda juga dapat menemukan petunjuk tentang cara menghapus virus, spyware, dan nasihat mengenai cara agar tetap terlindungi.

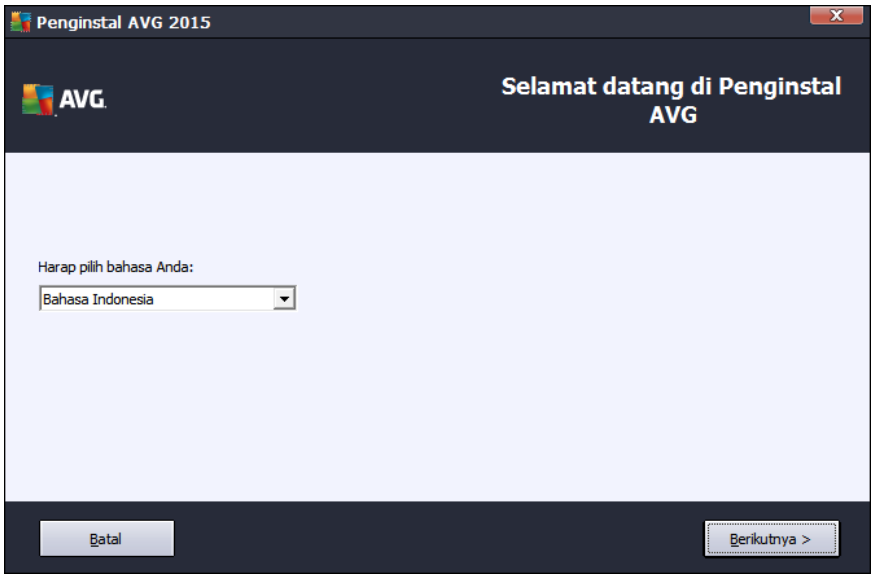
- ***Forum diskusi***: Anda juga dapat menggunakan forum diskusi pengguna AVG di http://forums.avg.com.

3.1. Proses Instalasi AVG

Untuk menginstal **AVG Internet Security 2015** pada komputer Anda, Anda perlu mendapatkan file instalasi terbaru. Untuk memastikan Anda menginstal versi **AVG Internet Security 2015** terbaru, Anda sebaiknya mengunduh file instalasi dari situs web AVG (http://www.avg.com/). Bagian ***Dukungan*** menyediakan gambaran umum terstruktur atas file instalasi bagi setiap edisi AVG. Setelah Anda mengunduh dan menyimpan file instalasi pada hard disk, Anda dapat meluncurkan proses instalasi. Instalasi adalah serentetan dialog sederhana dan mudah dipahami. Setiap dialog secara ringkas menerangkan apa yang dilakukan setiap langkah pada proses instalasi. Kami menawarkan penjelasan terperinci atas setiap jendela dialog berikut ini:

3.1.1. Selamat Datang: Pemilihan Bahasa

Proses instalasi dimulai dengan dialog ***Selamat datang di AVG Installer***:

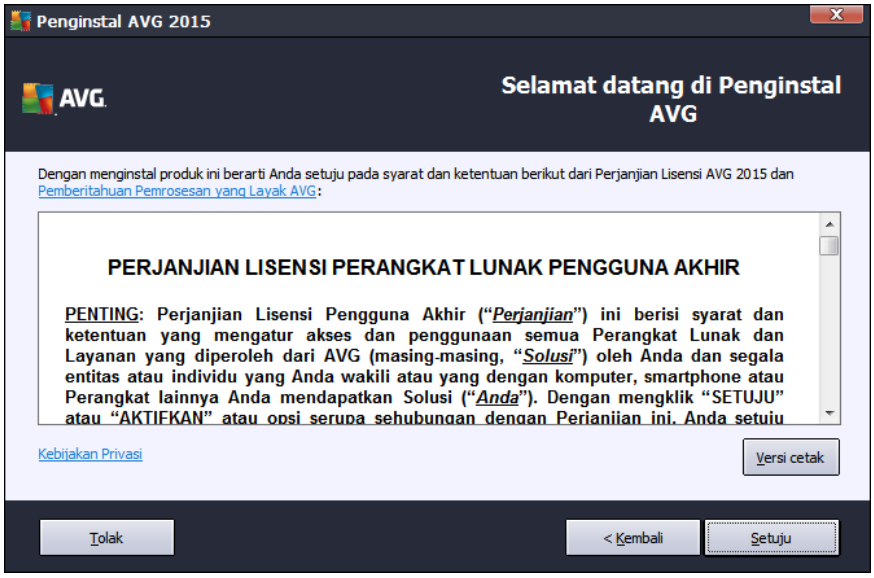


Di dialog ini, Anda dapat memilih bahasa yang digunakan untuk proses instalasi. Klik tombol kombinasi untuk bergulir ke bawah dalam menu bahasa. Pilih bahasa yang diinginkan, dan proses instalasi akan dilanjutkan dalam bahasa yang Anda pilih.

Perhatian: Di saat ini, Anda hanya memilih bahasa untuk proses instalasi. Aplikasi AVG Internet Security 2015 akan diinstal dalam bahasa yang dipilih, dan dalam bahasa Inggris yang selalu diinstal secara otomatis. Walau demikian, bisa saja menginstal bahasa lainnya dan menggunakan AVG Internet Security 2015 dalam salah satu bahasa ini. Anda akan diminta mengkonfirmasi pilihan bahasa alternatif dalam salah satu dialog pengaturan berikut bernama Opsi Khusus.

3.1.2. Selamat Datang: Perjanjian Lisensi

Dialog ***Selamat datang di AVG Installer*** menyediakan teks lengkap perjanjian lisensi AVG:



Silakan baca keseluruhan teks dengan seksama. Untuk mengkonfirmasi bahwa Anda telah membaca, memahami, dan menerima perjanjian, tekan tombol ***Terima***. Jika Anda tidak setuju dengan perjanjian lisensi tersebut, tekan tombol ***Tolak***, maka proses instalasi akan segera diakhiri.

Kebijakan Privasi dan Pemberitahuan Pemrosesan Adil AVG

Di samping perjanjian lisensi, dialog pengaturan ini juga menawarkan opsi untuk selengkapnya mempelajari ***Pemberitahuan Pemrosesan Adil AVG***, dan ***kebijakan privasi AVG***. Fungsi yang disebutkan ditampilkan di dialog dalam bentuk hyperlink aktif yang membawa Anda ke situs web khusus di mana Anda dapat menemukan informasi yang lebih mendetail. Klik tautan yang Anda inginkan agar diarahkan ke situs web AVG (http://www.avg.com/) di mana Anda dapat menemukan teks lengkap pernyataan tersebut.

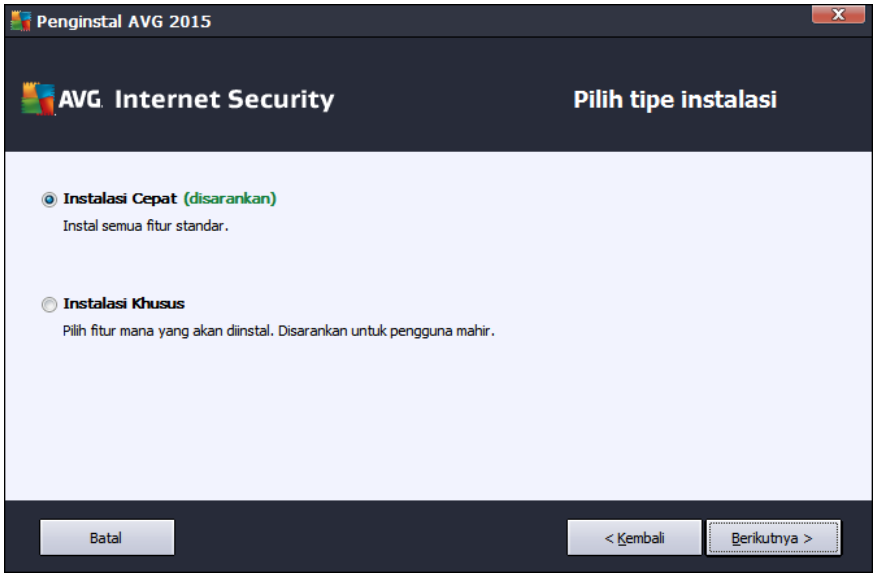
Tombol kontrol

Mulai dari dialog penyiapan pertama, tombol kontrol berikut tersedia:

- ***Versi cetak*** – Klik tombol untuk menampilkan teks lengkap perjanjian lisensi AVG dalam antarmuka web dan telah diatur dengan rapi untuk dicetak.
- ***Tolak*** – Klik untuk menolak perjanjian lisensi. Proses pengaturan akan segera ditutup. **AVG Internet Security 2015** tidak akan diinstal!
- ***Kembali*** – Klik untuk mundur satu langkah ke dialog pengaturan sebelumnya.
- ***Terima*** – Klik untuk mengkonfirmasi bahwa Anda telah membaca, memahami, dan menerima perjanjian lisensi. Instalasi akan dilanjutkan, dan Anda akan maju satu langkah ke dialog pengaturan berikut.

3.1.3. Pilih tipe instalasi

Dialog ***Pilih tipe instalasi*** menawarkan dua pilihan opsi instalasi: ***Cepat*** dan ***Instalasi Khusus***:



Instalasi cepat

Untuk sebagian besar pengguna, sangatlah disarankan untuk tetap menggunakan instalasi ***Cepat*** standar. Dengan cara ini Anda menginstal **AVG Internet Security 2015** dalam mode otomatis penuh dengan pengaturan yang sudah ditentukan oleh vendor program. Konfigurasi ini menyediakan keamanan maksimum yang dikombinasikan dengan penggunaan sumber daya yang optimal. Di masa mendatang, jika perlu mengubah konfigurasi, Anda akan selalu memiliki opsi untuk melakukannya secara langsung dalam aplikasi **AVG Internet Security 2015**.

Tekan tombol ***Berikutnya*** untuk melanjutkan ke dialog proses instalasi berikut ini.

Instalasi khusus

Instalasi Khusus hanya boleh digunakan oleh pengguna berpengalaman dengan alasan yang kuat untuk menginstal **AVG Internet Security 2015** dengan pengaturan non-standar, misalnya, agar pas dengan persyaratan sistem tertentu. Jika Anda memutuskan untuk menggunakan cara ini, opsi baru dari ***Folder tujuan*** akan diaktifkan dalam dialog. Di sini, Anda harus menentukan lokasi di mana **AVG Internet Security 2015** harus diinstal. Secara default, **AVG Internet Security 2015** akan diinstal ke folder file program di drive C:, sebagaimana dinyatakan di bidang teks pada dialog. Jika Anda ingin mengubah lokasi ini, gunakan tombol ***Jelajah*** untuk menampilkan struktur drive dan pilih folder yang diinginkan. Untuk kembali ke tujuan default yang ditentukan sebelumnya oleh vendor perangkat lunak, gunakan tombol ***Default***.

Setelah itu, tekan tombol ***Berikutnya*** untuk melanjutkan ke dialog Opsi Khusus.

Tombol kontrol

Sebagaimana dalam dialog pengaturan pada umumnya, ada tiga tombol kontrol yang tersedia:

- ***Batalkan*** – klik untuk keluar dari proses pengaturan dengan segera; **AVG Internet Security 2015** tidak akan diinstal!

- ***Kembali*** – klik untuk kembali satu langkah ke dialog pengaturan sebelumnya.
- ***Berikutnya*** – klik untuk melanjutkan instalasi dan maju satu langkah.

3.1.4. Opsi Khusus

Dialog ***Opsi Khusus*** memungkinkan Anda menentukan parameter terperinci pada instalasi:

Bagian ***Pemilihan Komponen*** menampilkan gambaran umum mengenai semua komponen **AVG Internet Security 2015** yang dapat diinstal. Jika pengaturan default tidak cocok untuk Anda, Anda dapat menghapus/menambah komponen tertentu. ***Walau demikian, Anda hanya dapat memilih dari komponen yang telah disertakan dalam edisi AVG yang dibeli!*** Sorot pilihan apa pun dalam daftar ***Pilihan Komponen***, dan keterangan singkat tentang komponen tersebut akan ditampilkan pada sisi kanan bagian ini. Untuk informasi terperinci tentang fungsionalitas masing-masing komponen, harap lihat bab Gambaran Umum Komponen dalam dokumentasi ini. Untuk kembali ke konfigurasi default yang ditentukan sebelumnya oleh vendor perangkat lunak, gunakan tombol ***Default***.

Pada langkah ini, Anda juga dapat memutuskan untuk menginstal variasi bahasa lainnya untuk produk tersebut *(secara default, aplikasi akan diinstal dalam bahasa yang telah Anda pilih saat Anda menyetel bahasa komunikasi, dan dalam Bahasa Inggris)*.

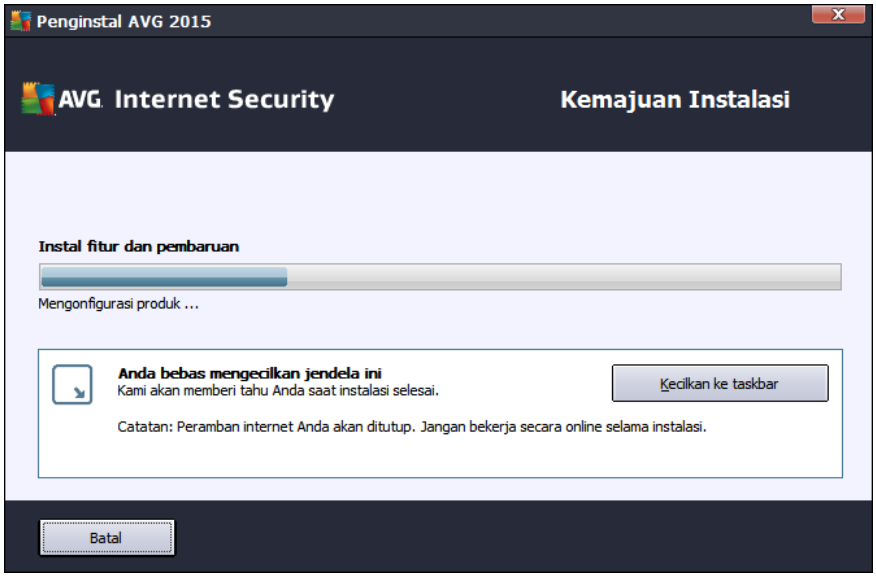
Tombol kontrol

Sebagaimana dalam dialog pengaturan pada umumnya, ada tiga tombol kontrol yang tersedia:

- ***Batalkan*** – klik untuk keluar dari proses pengaturan dengan segera; **AVG Internet Security 2015** tidak akan diinstal!
- ***Kembali*** – klik untuk kembali satu langkah ke dialog pengaturan sebelumnya.
- ***Berikutnya*** – klik untuk melanjutkan instalasi dan maju satu langkah.

3.1.5. Kemajuan Instalasi

Dialog ***Kemajuan Instalasi*** menampilkan kemajuan proses instalasi, dan tidak memerlukan campur-tangan apapun:



Setelah proses instalasi selesai, Anda akan dialihkan ke dialog berikutnya secara otomatis.

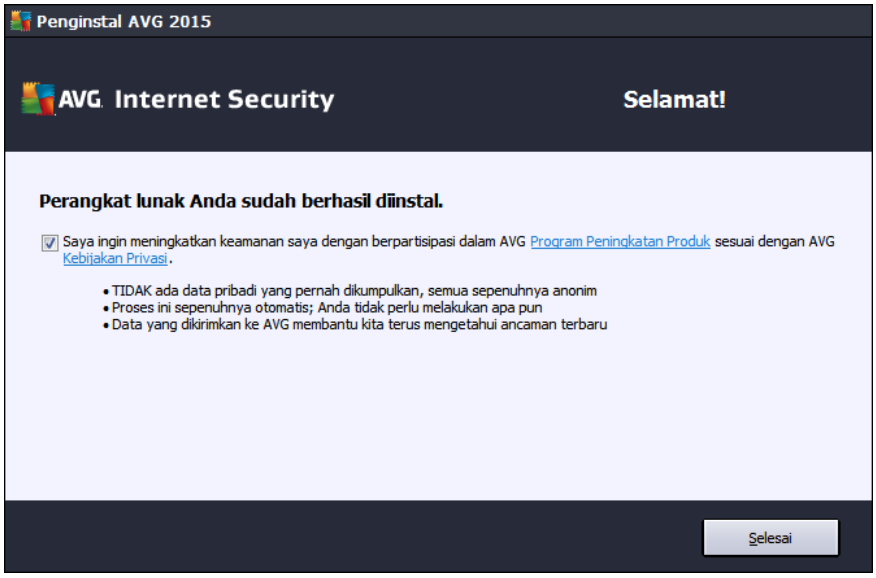
Tombol kontrol

Ada dua tombol kontrol yang tersedia dalam dialog ini:

- ***Minimalkan*** – Proses instalasi mungkin memerlukan waktu beberapa menit. Klik tombol untuk meminimalkan jendela dialog menjadi ikon yang terlihat di bilah sistem. Dialog akan muncul lagi setelah instalasi selesai.
- ***Batal*** – Tombol ini seharusnya hanya digunakan jika Anda ingin menghentikan proses instalasi yang sedang dijalankan. Harap diingat jika Anda memilih batal, **AVG Internet Security 2015** tidak akan diinstal!

3.1.6. Selamat!

Dialog ***Selamat*** mengonfirmasi bahwa **AVG Internet Security 2015** Anda telah terinstal lengkap dan dikonfigurasi:



Program Peningkatan Produk dan Kebijakan Privasi

Di sini Anda dapat memutuskan apakah Anda ingin berpartisipasi dalam ***Program Peningkatan Produk*** (*untuk perinciannya, lihat bab Pengaturan Lanjutan AVG/Program Peningkatan Produk*) yang mengumpulkan informasi anonim mengenai ancaman yang terdeteksi guna meningkatkan tingkatan keamanan Internet secara keseluruhan. Semua data diperlakukan secara rahasia dan tunduk terhadap Kebijakan Privasi AVG, klik tautan ***Kebijakan Privasi*** agar diarahkan ke situs web AVG (http://www.avg.com/) di mana Anda dapat menemukan teks lengkap Kebijakan Privasi AVG. Jika Anda setuju, biarkan opsi ini tetap dicentang *(opsi ini dikonfirmasi, secara default)*.

Untuk mengakhiri proses instalasi, tekan tombol ***Selesaikan***.

3.2. Setelah Instalasi

3.2.1. Pendaftaran produk

Setelah menyelesaikan instalasi **AVG Internet Security 2015**, daftarkan produk Anda secara online pada situs web AVG (*http://www.avg.com/*). Setelah pendaftaran, Anda akan mendapatkan akses penuh ke akun pengguna AVG, Berita pembaruan AVG, dan layanan lain yang disediakan khusus untuk pengguna terdaftar. Cara termudah untuk mendaftar adalah langsung dari antarmuka pengguna **AVG Internet Security 2015**. Silakan pilih item navigasi baris atas / Opsi / Daftarkan sekarang. Anda akan dialihkan ke halaman ***Pendaftaran*** pada situs web AVG (*http://www.avg.com/*). Harap ikuti petunjuk yang diberikan di halaman tersebut.

3.2.2. Akses ke antarmuka pengguna

Dialog utama AVG dapat diakses dengan beberapa cara:

- klik dua kali ikon baki sistem AVG

- klik dua kali ikon AVG di desktop
- dari menu ***Start/All Programs/AVG/AVG 2015***

3.2.3. Pemindaian seluruh komputer

Ada kemungkinan risiko bahwa virus komputer telah terkirim ke komputer Anda sebelum instalasi **AVG Internet Security 2015**. Karena alasan ini, Anda harus menjalankan Pemindaian seisi komputer untuk memastikan tidak ada infeksi pada PC Anda. Pemindaian pertama mungkin membutuhkan beberapa waktu *(sekitar satu jam)* tetapi disarankan untuk memulainya untuk memastikan komputer Anda tidak terganggu oleh ancaman. Untuk petunjuk mengenai menjalankan Pemindaian seisi komputer bacalah bab Pemindaian AVG.

3.2.4. Tes Eicar

Untuk mengkonfirmasi bahwa **AVG Internet Security 2015** telah diinstal dengan benar, Anda dapat menjalankan tes EICAR.

Tes EICAR adalah metode standar dan benar-benar aman untuk menguji operasi sistem antivirus. Ini aman diedarkan, karena ia bukan virus sungguhan, dan tidak berisi potongan kode virus. Kebanyakan produk bereaksi seolah-olah ia virus (*tetapi produk-produk tersebut biasanya melaporkannya dengan nama yang jelas, seperti "EICAR-AV-Test"*). Anda dapat mengunduh virus EICAR dari situs Web EICAR di www.eicar.com, dan di sana Anda juga akan menemukan semua informasi tes EICAR yang diperlukan.

Cobalah mengunduh file *eicar.com*, dan simpan di disk lokal Anda. Segera setelah Anda mengonfirmasi mengunduh file uji coba, **AVG Internet Security 2015** Anda akan memberikan reaksi dengan sebuah peringatan. Pemberitahuan ini menunjukkan bahwa AVG telah terinstal pada komputer Anda dengan benar.

Jika AVG gagal mengenali file tes EICAR sebagai virus, Anda harus memeriksa lagi konfigurasi program!

3.2.5. Konfigurasi default AVG

Konfigurasi default (*yakni cara aplikasi diatur tepat setelah instalasi*) **AVG Internet Security 2015** telah diatur oleh vendor perangkat lunak sehingga semua komponen dan fungsi telah disesuaikan untuk mencapai kinerja optimal. ***Jika Anda tidak memiliki alasan kuat untuk itu, jangan ubah konfigurasi AVG! Perubahan pengaturan hanya boleh dilakukan oleh pengguna berpengalaman.*** Jika Anda ingin mengubah konfigurasi AVG agar lebih sesuai dengan kebutuhan Anda, masuk ke Pengaturan Lanjut AVG: pilih *Opsi/Pengaturan Lanjut* item menu utama, lalu edit konfigurasi AVG dalam dialog Pengaturan Lanjut AVG yang baru dibuka.

3.3. Antarmuka Pengguna AVG

AVG Internet Security 2015 dibuka dengan jendela utama:

Jendela utama dibagi ke dalam beberapa bagian:

- ***Navigasi baris atas*** terdiri dari empat tautan aktif yang berjejer di bagian atas jendela utama *(Suka AVG, Laporan, Dukungan, Opsi).* Perincian >>
- ***Info Status Keamanan*** memberikan informasi dasar tentang status saat ini **AVG Internet Security 2015** Anda. Perincian >>
- ***Gambaran umum komponen terinstal*** dapat ditemukan pada garis balok mendatar di bagian tengah jendela utama. Komponen-komponen ini ditampilkan sebagai balok berwarna hijau terang yang diberi nama sesuai ikon komponen yang dimaksud, dan memberikan informasi tentang status komponen. Perincian >>
- ***Pindai/Perbarui tautan cepat*** diletakkan di baris balok bagian bawah pada jendela utama. Tombol-tombol ini memberikan akses cepat ke fungsi-fungsi AVG yang paling penting dan paling sering digunakan. Perincian >>

Di bagian luar jendela utama **AVG Internet Security 2015**, terdapat satu lagi elemen pengontrol yang bisa Anda gunakan untuk mengakses aplikasi:

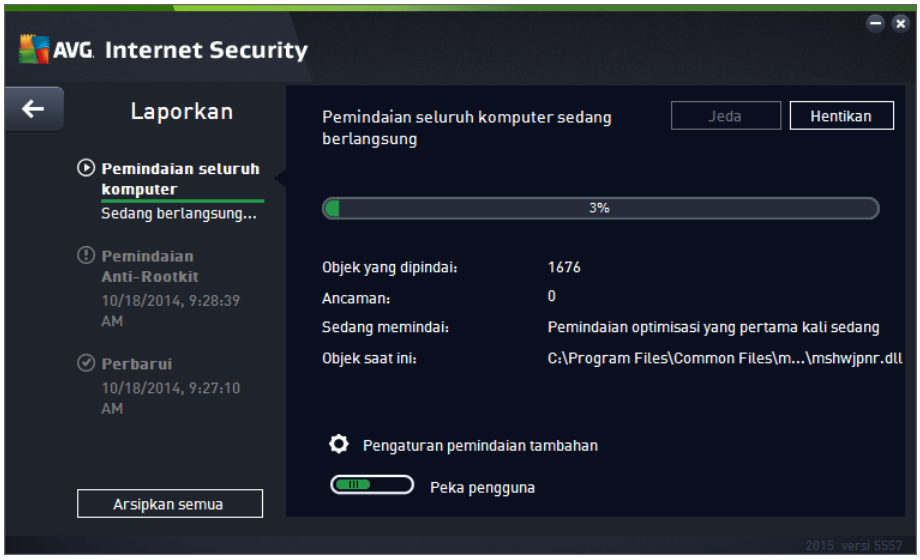
- ***Ikon baki sistem*** terletak di sudut kanan bawah layar *(pada baki sistem)* dan menunjukkan status terkini dari **AVG Internet Security 2015**. Perincian >>

3.3.1. Navigasi Baris Atas

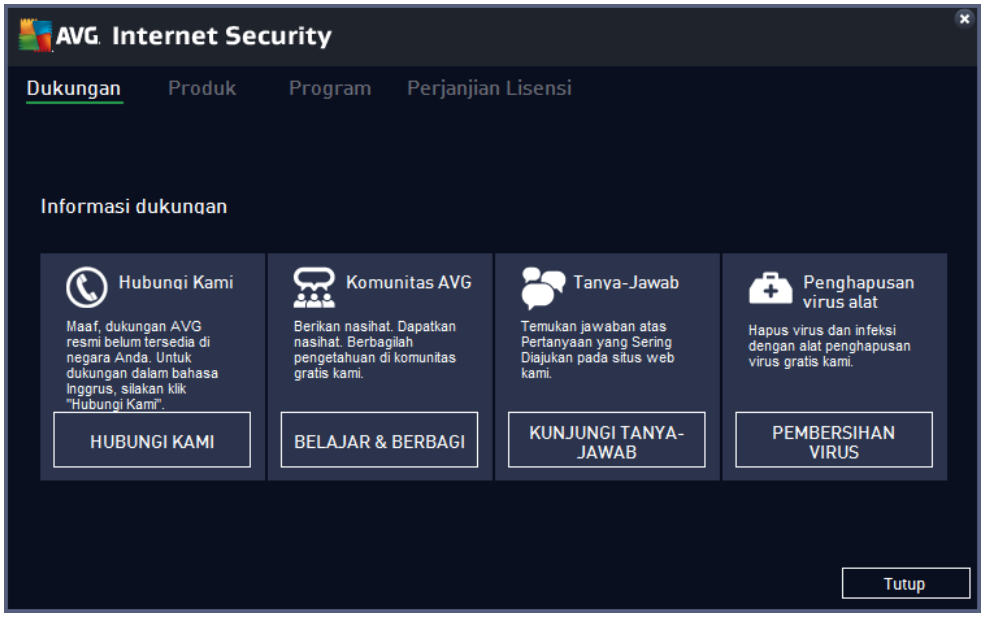
Navigasi baris atas terdiri dari beberapa tautan aktif yang berjajar di bagian atas jendela utama. Navigasi ini mencakup tombol-tombol berikut:

Klik tautan satu kali agar terhubung ke komunitas Facebook AVG dan untuk berbagi informasi, berita, tips, dan trik terbaru dari AVG demi keamanan maksimal internet Anda.

Membuka dialog ***Laporan*** baru yang berisi gambaran umum semua laporan terkait pada proses pemindaian dan pembaruan yang dijalankan sebelumnya. Jika pemindaian atau pembaruan sedang berjalan, ikon lingkaran yang berputar akan ditampilkan di samping teks ***Laporan*** pada navigasi atas antarmuka pengguna utama. Klik lingkaran ini agar dialog menggambarkan kemajuan proses yang sedang berjalan:



Membuka dialog baru yang terstruktur dalam empat tab di mana Anda dapat menemukan semua informasi terkait tentang **AVG Internet Security 2015**:



- ***Dukungan*** – Tab ini memberikan gambaran umum yang disusun dengan jelas mengenai semua kontak yang tersedia untuk dukungan pelanggan.
- ***Produk*** – Tab ini memberikan gambaran umum data teknis **AVG Internet Security 2015** yang paling penting yang mengacu pada informasi produk, komponen yang terinstal, perlindungan email yang diinstal, dan informasi sistem.
- ***Program*** – Pada tab ini Anda dapat menemukan informasi mengenai versi file program, dan mengenai kode pihak ketiga yang digunakan dalam produk.
- ***Perjanjian Lisensi*** – Tab ini memberikan teks lengkap perjanjian lisensi antara Anda dengan AVG Technologies.

Pemeliharaan **AVG Internet Security 2015** dapat diakses melalui item ***Opsi***. Klik tanda panah untuk membuka menu gulir-bawah:

- ***Pindai komputer*** menjalankan pemindaian seisi komputer.
- ***Pindai folder yang dipilih...*** – Beralih ke antarmuka pemindaian AVG dan memungkinkan Anda menentukan dalam struktur komputer; file dan folder mana yang harus dipindai.
- ***Pindai file...*** – Memungkinkan Anda untuk menjalankan tes atas permintaan untuk satu file tertentu. Klik opsi ini untuk membuka jendela baru dengan struktur disk Anda. Pilih file yang diinginkan, dan konfimasikan peluncuran pemindaian.
- ***Perbarui*** – Secara otomatis meluncurkan proses pembaruan pada **AVG Internet Security 2015**.

- ***Perbarui dari direktori...*** – Menjalankan proses pembaruan dari file pembaruan yang berada dalam folder tertentu pada disk lokal Anda. Walau demikian, opsi ini hanya disarankan saat darurat, misalnya situasi di mana tidak koneksi ke Internet (misalnya, komputer Anda terinfeksi dan terputus dari Internet; komputer Anda terhubung ke jaringan tanpa akses ke Internet, dll.). Dalam jendela yang baru dibuka, pilih folder di mana sebelumnya Anda meletakkan file pembaruan, dan luncurkan proses pembaruan.

- ***Gudang Virus*** – Membuka antarmuka ke tempat karantina, Gudang Virus, ke tempat AVG menghapus sepua infeksi yang terdeteksi. Di dalam karantina ini, file terinfeksi diisolasi, keamanan komputer Anda terjamin, dan file terinfeksi tersebut sekaligus disimpan seandainya nanti bisa diperbaiki.

- ***Riwayat*** – Menawarkan opsi submenu tertentu secara lebih lengkap:

  - *Hasil pemindaian* – Membuka dialog yang memberikan gambaran umum hasil pemindaian.

  - *Hasil Resident Shield* – Membuka dialog berisi gambaran umum mengenai ancaman yang terdeteksi oleh Resident Shield.

  - *Hasil Identity Protection* – Membuka dialog dengan gambaran umum ancaman yang terdeteksi berdasarkan komponen Identitas.

  - *Hasil Perlindungan Email* – Membuka dialog berisi gambaran umum mengenai lampiran pesan e-mail yang terdeteksi sebagai ancaman oleh komponen Perlindungan Email.

  - *Hasil Online Shield* – Membuka dialog berisi gambaran umum mengenai ancaman yang terdeteksi oleh Online Shield.

  - *Log riwayat kejadian* – Membuka antarmuka log riwayat yang berisi gambaran umum semua **AVG Internet Security 2015** tindakan

  - *Log Firewall* – Membuka dialog yang berisi gambaran umum terperinci mengenai semua tindakan Firewall.

- ***Pengaturan lanjut...*** – Membuka dialog pengaturan lanjut AVG tempat Anda dapat mengedit **AVG Internet Security 2015** konfigurasi. Umumnya, disarankan untuk tetap menggunakan pengaturan default aplikasi sebagaimana ditentukan oleh vendor perangkat lunak.

- ***Pengaturan Firewall...*** – Membuka dialog mandiri untuk konfigurasi lanjut pada komponen Firewall.

- ***Daftar isi Bantuan*** – Membuka file bantuan AVG.

- ***Dapatkan dukungan*** – Buka dialog dukungan yang memberikan semua informasi kontak dan dukungan yang dapat diakses.

- ***Web AVG Anda*** – Membuka situs web AVG (*http://www.avg.com/*).

- ***Tentang Virus dan Ancaman*** – Membuka ensiklopedia virus online situs web AVG (*http://www.avg.com/*) di mana Anda dapat melihat informasi terperinci mengenai virus yang telah dikenali.

- ***MyAccount*** – Sambungkan ke halaman pendaftaran situs web ***AVG MyAccount***(*http://www.avg.com/*). Buat akun AVG Anda supaya Anda dapat memelihara produk dan lisesnsi AVG yang terdaftar, mengunduh produk baru, memantau status pesanan, atau mengatur data pribadi dan kata sandi Anda. Harap isikan data pendaftaran Anda ; hanya pelanggan yang mendaftarkan produk AVG mereka yang dapat menerima dukungan teknis gratis.

- ***Tentang AVG*** – Membuka dialog baru dengan empat tab yang menyediakan data mengenai lisensi yang Anda beli dan dukungan yang dapat diakses, informasi produk dan program, dan isi lengkap perjanjian lisensi. *(Dialog yang sama dapat dibuka melalui tautan Dukungan dari navigasi utama.)*

3.3.2. Info Status Keamanan

Bagian ***Info Status Keamanan*** berada di bagian atas jendela utama **AVG Internet Security 2015**. Di bagian ini akan selalu Anda temukan informasi mengenai status keamanan saat ini atas **AVG Internet Security 2015** Anda. Lihat gambaran umum mengenai berbagai ikon yang ditampilkan di bagian ini beserta artinya:

 – ikon hijau menunjukkan bahwa ***AVG Internet Security 2015 Anda berfungsi penuh***. Komputer Anda terlindungi sepenuhnya, mutakhir dan semua komponen yang terinstal bekerja dengan benar.

 – ikon kuning memperingatkan bahwa ***satu atau beberapa komponen salah konfigurasi*** dan Anda harus memeriksa properti/ pengaturannya. Tidak ada masalah kritis dalam **AVG Internet Security 2015** dan Anda barangkali telah memutuskan untuk menonaktifkan satu komponen karena suatu alasan. Anda tetap terlindungi! Walau demikian, perhatikanlah masalah pengaturan komponen! Komponen yang salah konfigurasi akan ditampilkan dengan garis oranye peringatan dalam antarmuka pengguna utama.

Ikon kuning juga muncul jika karena suatu alasan Anda memutuskan untuk mengabaikan status kesalahan komponen. Opsi ***Abaikan status kesalahan*** dapat diakses dalam cabang Pengaturan lanjut / Abaikan status kesalahan. Di sana Anda mempunyai opsi untuk menyatakan Anda mengetahui status kesalahan komponen namun karena suatu alasan Anda ingin membiarkan **AVG Internet Security 2015** begitu dan Anda tidak ingin diperingatkan. Anda mungkin perlu menggunakan opsi ini dalam situasi tertentu namun sangat disarankan untuk menonaktifkan opsi ***Abaikan status kesalahan*** secepatnya!

Atau ikon kuning juga akan ditampilkan jika **AVG Internet Security 2015** Anda meminta komputer dihidupkan ulang (***Hidupkan ulang diperlukan***). Perhatikan peringatan ini dan hidupkan ulang PC Anda.

 – ikon oranye menunjukkan bahwa ***AVG Internet Security 2015 dalam status kritis***! Satu atau beberapa komponen tidak berfungsi dengan benar dan **AVG Internet Security 2015** tidak dapat melindungi komputer Anda. Perhatikan segera untuk memperbaiki masalah yang dilaporkan! Jika Anda tidak dapat memperbaiki sendiri kesalahan tersebut, hubungi tim Dukungan teknis AVG.

Jika AVG Internet Security 2015 tidak diatur pada kinerja optimal, tombol baru bernama Klik untuk perbaiki (atau Klik untuk perbaiki semua jika masalah melibatkan lebih dari satu komponen) akan muncul di sebelah informasi status keamanan. Tekan tombol untuk meluncurkan proses otomatis pemeriksaan dan konfigurasi program. Inilah cara mudah untuk mengatur AVG Internet Security 2015 ke kinerja optimal dan mencapai tingkat keamanan maksimum!

Sangatlah disarankan agar Anda memperhatikan ***Info Status Keamanan*** dan jika laporan menunjukkan adanya masalah, teruskan dan cobalah mengatasinya dengan segera. Jika tidak, komputer Anda berisiko!

Catatan: *informasi status AVG Internet Security 2015 juga dapat diperoleh kapan saja dari ikon baki sistem.*

3.3.3. Gambaran Umum Komponen

Gambaran umum komponen terinstal dapat ditemukan pada garis balok mendatar di bagian tengah jendela utama. Komponen-komponen ini ditampilkan sebagai balok berwarna hijau terang yang diberi nama sesuai ikon komponen yang dimaksud. Setiap balok memberikan informasi tentang status terkini perlindungan. Jika komponen dikonfigurasi dengan tepat dan benar-benar berfungsi, informasi akan tertera dalam huruf berwarna hijau. Jika komponen berhenti, fungsionalitasnya akan terbatas, atau komponen berada dalam kondisi galat, Anda akan

diberitahu dengan teks peringatan yang ditampilkan dalam kolom teks oranye. ***Sangat disarankan untuk memperhatikan pengaturan komponen masing-masing!***

Gerakkan mouse ke komponen untuk menampilkan teks singkat di bagian bawah jendela utama. Teks ini memberikan pendahuluan dasar mengenai fungsionalitas komponen. Selain itu, teks ini juga memberikan informasi tentang status terkini komponen, dan menyebutkan layanan komponen yang tidak dikonfigurasi dengan benar.

Daftar komponen terinstal

Di bagian **AVG Internet Security 2015** ***Gambaran Umum Komponen*** berisi informasi mengenai komponen berikut:

- ***Komputer*** – Komponen ini mencakup dua layanan: ***AntiVirus Shield*** mendeteksi virus, spyware, worm, troya, file yang dapat dijalankan yang tidak diinginkan, atau pustaka dalam sistem Anda, serta melindungi Anda dari adware jahat/ perusak, dan pemindaian ***Anti-Rootkit*** untuk rootkit berbahaya yang bersembunyi di dalam aplikasi, driver, atau pustaka. Perincian >>
- ***Penjelajahan Web*** – Melindungi Anda dari serangan berbasis web saat Anda menelusuri atau menjelajahi Internet. Perincian >>
- ***Identitas*** – Komponen ini menjalankan layanan ***Identity Shield*** yang terus melindungi aset digital Anda dari ancaman baru dan tak dikenal di Internet. Perincian >>
- ***Email*** – Periksa pesan email masuk Anda dari SPAM, dan blok virus, serangan pishing, atau ancaman lainnya. Perincian >>
- ***Firewall*** – Mengontrol semua komunikasi di setiap port jaringan, yang melindungi Anda dari serangan jahat dan memblokir semua upaya penyusupan. Perincian >>

Tindakan yang dapat diakses

- ***Gerakkan mouse di atas ikon komponen*** untuk menyorotnya dalam gambaran umum komponen. Pada saat yang sama, keterangan fungsionalitas dasar komponen akan muncul di bagian bawah antarmuka pengguna.
- ***Klik sekali ikon komponen*** untuk membuka antarmuka komponen yang berisi informasi status terkini komponen, akses menuju konfigurasinya serta data statistik.

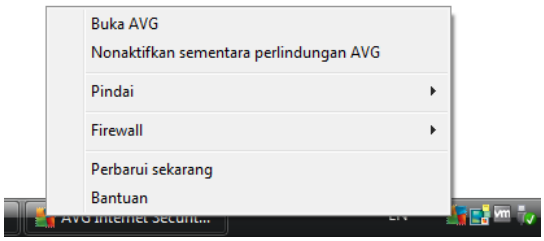
3.3.4. Pindai/ Perbarui Tautan Cepat

Tautan cepat terletak di baris tombol yang lebih rendah **AVG Internet Security 2015** dalam antarmuka pengguna. Tautan ini memungkinkan Anda mengakses fitur aplikasi yang paling penting dan paling sering digunakan secara cepat, misalnya pemindaian dan pembaruan. Tautan cepat dapat diakses dari semua dialog antarmuka pengguna:

- ***Pindai sekarang*** – Tombol ini secara grafis dibagi menjadi dua bagian. Ikuti tautan ***Pindai sekarang*** untuk menjalankan Pemindaian Seisi Komputer dengan segera, dan melihat kemajuan serta hasilnya pada jendela Laporan yang terbuka secara otomatis. Tombol ***Opsi*** membuka dialog ***Opsi Pemindaian*** di mana Anda dapat memilih atur pemindaian terjadwal dan mengedit parameter Pemindaian Seisi Komputer / Pindai File atau Folder Tertentu. *(Untuk perinciannya, lihat bab Pemindaian AVG)*
- ***Perbarui sekarang*** – Tekan tombol untuk menjalankan pembaruan produk dengan segera. Anda akan diberi tahu mengenai hasil pembaruan di slide dialog pada Ikon Baki Sistem AVG. *(Untuk perinciannya, lihat bab Pembaruan AVG)*

3.3.5. Ikon Baki Sistem

Ikon Baki Sistem AVG (pada Windows taskbar, sudut kanan bawah layar) *menunjukkan status terkini dari* **AVG Internet Security 2015** Anda. Ini selalu terlihat pada baki sistem Anda, baik antarmuka pengguna **AVG Internet Security 2015** sedang dibuka atau ditutup:



Tampilan Ikon Baki Sistem AVG

- Jika warnanya penuh tanpa elemen tambahan berarti ikon menunjukkan bahwa semua komponen **AVG Internet Security 2015** aktif dan berfungsi penuh. Walau demikian, ikon tersebut juga dapat ditampilkan seperti ini bila salah satu komponen tidak berfungsi penuh namun pengguna memutuskan untuk mengabaikan status komponen. *(Setelah mengkonfirmasi opsi pengabaian status komponen, Anda menyatakan bahwa Anda mengetahui status kesalahan komponen namun karena suatu alasan Anda ingin membiarkannya begitu, dan Anda tidak ingin diperingatkan tentang situasi tersebut.)*

- Ikon dengan tanda seru menunjukkan bahwa komponen *(atau bahkan lebih banyak komponen)* dalam status kesalahan. Selalu perhatikan peringatan demikian dan cobalah menghilangkan masalah konfigurasi komponen yang tidak diatur dengan benar. Agar dapat menerapkan perubahan dalam konfigurasi komponen, klik dua kali pada ikon baki sistem untuk membuka antarmuka pengguna aplikasi. Untuk informasi terperinci mengenai komponen apa saja yang berada dalam status kesalahan harap lihat bagian info status keamanan.

- Ikon baki sistem dapat ditampilkan dalam warna penuh dengan sinar lampu berkedip dan berputar. Versi grafik ini memberi sinyal atas proses pembaruan yang saat ini diluncurkan.

- Tampilan ikon yang berubah-ubah warna dengan panah menunjukkan **AVG Internet Security 2015** pemindaian sedang berjalan.

Informasi Ikon Baki Sistem AVG

Ikon Baki Sistem AVG juga memberikan informasi tentang berbagai aktivitas terkini dalam **AVG Internet Security 2015**, dan kemungkinan perubahan status dalam program (*misalnya peluncuran otomatis untuk pemindaian atau pembaruan terjadwal, pengalihan profil Firewall, perubahan status komponen, kejadian status kesalahan, ...*) melalui jendela pop-up yang terbuka dari ikon baki sistem.

Tindakan dapat diakses dari Ikon Baki Sistem AVG

Ikon Baki Sistem AVG juga dapat digunakan sebagai tautan cepat untuk mengakses antarmuka pengguna **AVG Internet Security 2015**; cukup klik dua kali ikon. Dengan mengeklik kanan ikon Anda akan membuka menu konteks singkat berisi opsi-opsi berikut:

- ***Buka AVG*** – klik untuk membuka antarmuka pengguna **AVG Internet Security 2015**.

- ***Nonaktifkan perlindungan AVG untuk sementara*** – Anda mempunyai opsi untuk menonaktifkan seluruh perlindungan yang diberikan oleh **AVG Internet Security 2015** sekaligus. Ingatlah bahwa Anda tidak boleh menggunakan opsi ini kecuali jika sangat diperlukan! Dalam kebanyakan kasus, tidak diperlukan untuk menonaktifkan **AVG Internet Security 2015** sebelum menginstal perangkat lunak atau memasang driver baru, meskipun installer atau wizard perangkat lunak menyarankan bahwa program dan aplikasi yang berjalan ditutup terlebih dahulu untuk memastikan tidak ada gangguan yang tidak diinginkan selama proses instalasi. Jika Anda menonaktifkan **AVG Internet Security 2015** untuk sementara, Anda harus mengaktifkannya lagi begitu Anda selesai. Jika Anda terhubung dengan Internet atau jaringan selama perangkat lunak antivirus Anda dinonaktifkan, komputer Anda rentan terhadap serangan.

- ***Pemindaian*** – klik untuk membuka menu konteks pemindaian yang telah ditetapkan (*Pemindaian Seisi Komputer, dan Pindai File atau Folder Tertentu*) lalu pilih pemindaian yang diinginkan; pemindaian akan segera diluncurkan.

- ***Firewall*** – klik untuk membuka menu konteks dengan akses cepat ke semua mode Firewall yang tersedia. Pilih dari gambaran umum dan klik untuk mengonfirmasi bahwa Anda ingin mengubah mode Firewall yang saat ini telah disiapkan.

- ***Menjalankan pemindaian ...*** – item ini ditampilkan hanya jika ada pemindaian yang sedang berjalan di komputer Anda. Untuk pemindaian ini, Anda dapat menentukan prioritasnya, selain menghentikan atau memberi jeda pada pemindaian yang sedang berjalan. Tindakan-tindakan berikut juga dapat diakses: *Tentukan prioritas semua pemindaian, Jeda semua pemindaian* atau *Hentikan semua pemindaian*.

- ***Jalankan Quick Tune*** – klik untuk meluncurkan komponen Quick Tune.

- ***Login ke AVG MyAccount*** – Membuka halaman awal MyAccount di mana Anda dapat mengatur produk langganan Anda, membeli perlindungan tambahan, mengunduh file instalasi, memeriksa pesanan dan invoice sebelumnya, dan mengatur informasi pribadi Anda.

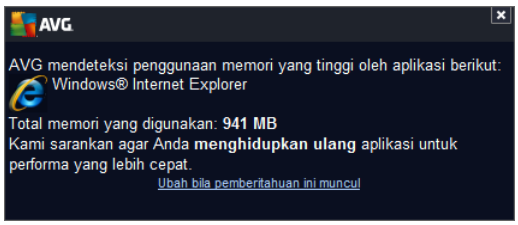
- ***Perbarui sekarang*** – meluncurkan pembaruan dengan segera.

- ***Bantuan*** – membuka file bantuan pada halaman awal.

3.3.6. Penasihat AVG

Penasihat AVG telah dirancang untuk mendeteksi masalah yang mungkin memperlambat komputer Anda, atau membahayakannya, dan menyarankan suatu tindakan untuk mengatasi situasi tersebut. Jika komputer Anda tiba-tiba berjalan lambat *(Menjelajah Internet, kinerja keseluruhan)*, biasanya tidak jelas apa penyebab sebenarnya, dan selanjutnya, bagaimana mengatasi masalah tersebut. Saat itulah ***Penasihat AVG*** digunakan: Penasihat AVG akan menampilkan pemberitahuan pada baki sistem yang memberitahu Anda kemungkinan masalahnya dan memberi saran bagaimana cara mengatasinya. ***Penasihat AVG*** tetap memonitor semua proses yang berjalan dalam PC Anda untuk mendeteksi kemungkinan masalah dan menawarkan tips bagaimana menghindari masalah tersebut.

Penasihat AVG dapat dilihat berupa pop-up geser melalui baki sistem:



Terutama, ***Penasihat AVG***akan memonitor hal-hal berikut ini:

- ***Kondisi browser Web yang sedang dibuka***. Browser Web mungkin membebani memori, terutama jika beberapa tab atau jendela telah dibuka selama beberapa waktu, dan menghabiskan terlalu banyak sumber daya sistem, mis. memperlambat komputer Anda. Dalam situasi demikian, menghidupkan ulang browser Web biasanya membantu.

- ***Menjalankan koneksi Peer-To-Peer***. Setelah menggunakan protokol P2P untuk berbagi file, koneksi terkadang dapat tetap aktif, dengan menggunakan jumlah tertentu dari bandwidth Anda. Akibatnya, penjelajahan web Anda berjalan lambat.

- ***Jaringan tak dikenal dengan nama yang dikenal***. Hal ini biasanya hanya terjadi kepada pengguna yang tersambung ke berbagai jaringan, biasanya dengan komputer portabel: Jika jaringan baru tak dikenal memiliki nama yang sama sebagai jaringan dikenal yang sering digunakan *(misalnya Home atau MyWifi)*, kekacauan dapat terjadi, dan Anda dapat dengan tidak sengaja terhubung ke jaringan yang benar-benar tidak dikenal dan berpotensi tidak aman. ***Penasihat AVG*** dapat mencegah hal ini dengan memperingatkan Anda bahwa nama yang dikenal sebenarnya merupakan jaringan yang baru. Tentu saja, jika Anda memutuskan bahwa jaringan yang tidak dikenal tersebut aman, Anda dapat menyimpannya ke daftar jaringan yang dikenal ***Penasihat AVG*** sehingga tidak akan dilaporkan lagi di kemudian hari.

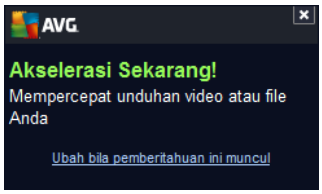
Di setiap situasi ini, ***Penasihat AVG*** memperingatkan Anda tentang kemungkinan masalah yang mungkin terjadi serta memberikan nama dan ikon proses atau aplikasi yang bertentangan. ***Penasihat AVG*** juga menyarankan langkah apa yang harus diambil untuk menghindari kemungkinan masalah tersebut.

Browser web yang didukung

Fitur ini dapat bekerja dengan browser web berikut: Internet Explorer, Chrome, Firefox, Opera, Safari.

3.3.7. Akselerator AVG

Akselerator AVG memungkinkan pemutaran video online lebih lancar dan membuat pengunduhan tambahan lebih mudah. Bila proses akselerasi video sedang berlangsung, Anda akan diberi tahu melalui jendela yang muncul di baki sistem.



3.4. Komponen AVG

3.4.1. Perlindungan Komputer

Komponen ***Komputer*** mencakup dua layanan keamanan utama: ***AntiVirus*** dan ***Data Safe***:

- ***AntiVirus*** terdiri dari mesin pemindaian yang melindungi semua file, area sistem pada komputer, dan media eksternal *(flash disk, dll.)* serta memindai virus yang dikenal. Semua virus yang terdeteksi akan diblokir agar tidak dapat berbuat apa pun, kemudian dibersihkan atau dikarantina di Gudang virus. Anda bahkan tidak melihat prosesnya, karena perlindungan tetap ini berjalan "di latar belakang". AntiVirus juga menggunakan pemindaian heuristik, di mana file dipindai berdasarkan karakteristik khas virus. Ini berarti pemindai AntiVirus dapat mendeteksi virus tak dikenal yang baru, jika virus baru tersebut memiliki

karakteristik khas dari virus yang telah ada. **AVG Internet Security 2015** juga dapat menganalisis dan mendeteksi aplikasi atau pustaka DLL yang dapat dijalankan yang mungkin tidak diinginkan dalam sistem *(berbagai jenis spyware, adware, dll.)*. Lagi pula, AntiVirus memindai registri sistem untuk mencari entri mencurigakan, file Internet sementara, dan cookie pelacak, serta memungkinkan Anda memperlakukan semua item yang mungkin merusak dengan cara yang sama dengan infeksi lainnya.

- ***Layanan Data Safe*** memudahan Anda membuat brankas virtual aman untuk menyimpan data berharga dan sensitif. daftar isi Data Safe dienkripsi dan diproteksi dengan kata sandi pilihan Anda agar tidak ada orang dapat mengaksesnya tanpa otorisasi.

Kontrol dialog

Untuk beralih antar dua bagian dialog, Anda cukup mengeklik bagian mana saja dari panel layanan terkait. Panel kemudian akan disorot dengan warna biru yang lebih muda. Di kedua bagian dialog, Anda dapat menemukan kontrol-kontrol berikut ini. Fungsionalitasnya tetap sama meskipun mereka adalah milik layanan keamanan yang satu atau lainnya *(AntiVirus atau Data Safe)*:

Aktif/ Tidak Aktif – Tombol ini mungkin mengingatkan Anda akan lampu lalu lintas, baik tampilannya ataupun fungsinya. Klik satu kali untuk beralih antar dua posisi. Warna hijau berarti ***Aktif***, yang berarti bahwa layanan keamanan AntiVirus aktif dan berfungsi penuh. Warna merah menunjukkan status ***Tidak Aktif***, yaitu layanan dinonaktifkan. Jika Anda tidak memiliki alasan yang tepat untuk menonaktifkan layanan, kami sangat menyarankan untuk membiarkan pengaturan default untuk semua konfigurasi keamanan. Pengaturan default menjamin kinerja aplikasi yang optimal dan keamanan maksimal. Jika karena alasan tertentu Anda ingin menonaktifkan layanan, Anda akan segera diperingatkan tentang risiko yang mungkin terjadi oleh tanda ***Peringatan*** berwarna merah dan informasi bahwa Anda tidak benar-benar terlindung pada saat itu. ***Harap diingat bahwa Anda harus mengaktifkan layanan lagi secepat mungkin!***

Pengaturan – Klik tombol agar diarahkan ke antarmuka pengaturan lanjut. Tepatnya, dialog tersebut akan terbuka dan Anda akan dapat mengkonfigurasi layanan yang dipilih, yaitu AntiVirus. Pada antarmuka pengaturan lanjut, Anda dapat mengedit semua konfigurasi setiap layanan keamanan dalam **AVG Internet Security 2015** tetapi konfigurasi tersebut hanya disarankan untuk pengguna yang berpengalaman!

Tanda panah – Gunakan tanda panah hijau di bagian kiri atas dialog untuk kembali ke antarmuka pengguna utama dengan gambaran umum komponen.

Cara membuat data safe Anda

Dalam bagian ***Data Safe*** dari dialog ***Perlindungan Komputer***, Anda dapat menemukan tombol ***Buat Data Safe Anda***. Klik tombol tersebut untuk membuka dialog baru dengan nama yang sama tempat Anda dapat menentukan parameter data safe yang Anda rencanakan. Harap isikan semua informasi yang diperlukan, dan ikuti petunjuk di dalam aplikasi tersebut:

Pertama, Anda harus menentukan nama data safe, dan membuat kata sandi yang kuat:

- ***Nama Data Safe*** – Untuk membuat data safe baru, Anda perlu memilih nama data safe yang cocok terlebih dahulu untuk menandainya. Jika Anda menggunakan komputer bersama anggota keluarga yang lain, Anda mungkin perlu mencantuman nama Anda berikut tanda daftar isi data safe, misalnya *Email ayah*.

- ***Buat kata sandi/ Ketik ulang kata sandi*** – Buat kata sandi untuk data safe Anda dan ketikkan ke dalam masing-masing bidang teks. Indikator gambar di sebelah kanan akan memberi tahu jika kata sandi Anda lemah *(relatif mudah dipecahkan dengan alat perangkat lunak khusus)* atau kuat; kami sarankan memilih kata sandi dengan setidaknya berkekuatan menengah. Anda dapat membuat kata sandi Anda lebih kuat dengan memasukkan huruf besar, angka, dan karakter lain seperti, tanda titik, tanda hubung, dll. Jika Anda ingin memastikan Anda mengetik kata sandi sesuai keinginan, Anda dapat mencentang kotak ***Tampilkan kata sandi*** *(tentu saja, orang lain tidak boleh melihat layar Anda)*.

- ***Petunjuk kata sandi*** – Kami sangat menyarankan Anda membuat petunjuk kata sandi bantuan yang akan mengingatkan Anda apa kata sandi Anda jika Anda lupa. Harap diingat bahwa Data Safe didesain untuk menyimpan file Anda dengan aman dengan hanya mengizinkan akses dengan kata sandi; tidak ada jalan lain untuk ini, dan jika Anda lupa kata sandi, Anda tidak dapat mengakses data safe Anda!

Setelah memasukkan semua data yang diperlukan ke dalam bidang teks, klik tombol ***Berikutnya*** untuk melanjutkan ke langkah berikutnya:

Dialog ini menampilkan opsi konfigurasi berikut:

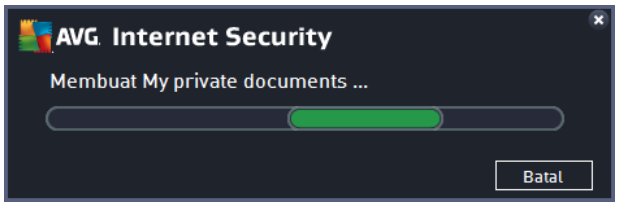
- ***Lokasi*** menyatakan tempat data safe akan ditempatkan secara fisik. Jelajahi tujuan yang cocok di hard drive, atau Anda dapat memilih lokasi yang sudah ditentukan, yaitu folder *Documents* Anda. Harap diingat bahwa setelah membuat data safe, Anda tidak dapat mengubah lokasinya.

- ***Ukuran*** – Anda dapat menentukan ukuran data safe terlebih dulu, yang akan mengambil ruang yang diperlukan pada disk. Nilai harus diatur jangan terlalu kecil *(tidak sesuai kebutuhan)*, atau terlalu besar *(terlalu banyak mengambil ruang disk yang tidak dipakai)*. Jika sudah tahu apa yang ingin Anda masukkan di data safe, Anda dapat meletakkan semua file di satu folder lalu menggunakan tautan ***Pilih folder*** untuk otomatis menghitung total ukurannya. Namun, ukuran dapat diubah nanti sesuai kebutuhan Anda.

- ***Akses*** – kotak centang di bagian ini memudahkan Anda membuat pintasan yang nyaman ke data safe Anda.

Cara menggunakan data safe Anda

Setelah Anda menyukai pengaturannya, klik tombol ***Buat Data Safe***. Dialog baru ***Data Safe Anda sekarang siap*** muncul memberitahukan bahwa data safe tersedia untuk menyimpan file Anda di dalamnya. Kini data safe dibuka dan Anda bisa segera mengaksesnya. Dengan tiap percobaan berikutnya untuk mengakses data safe, Anda akan diminta untuk membuka kunci data safe dengan kata sandi yang sudah Anda tentukan:

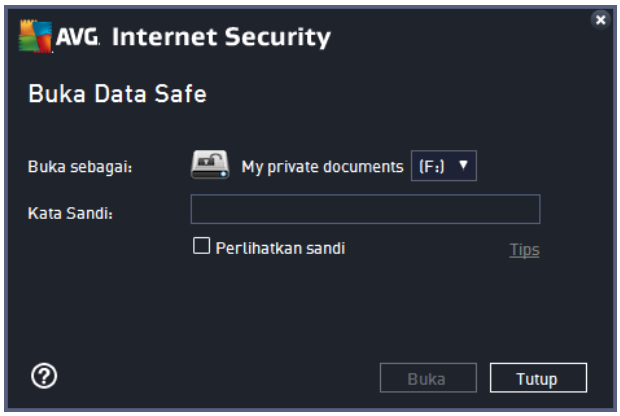


Untuk menggunakan data safe baru, Anda perlu membukanya terlebih dulu – klik tombol ***Buka Sekarang***. Saat membuka, data safe tampak di komputer Anda sebagai disk virtual baru. Harap tetapkan huruf pilihan Anda dari menu buka turun (*Anda hanya akan diizinkan untuk memilih disk yang saat ini tidak dipakai*). Biasanya, Anda

tidak dizinkan memilih C *(biasanya diterapkan untuk hard drive Anda)*, A *(floppy disk drive)*, atau D *(drive DVD)*. Harap diingat bahwa setiap kali Anda membuka kunci data safe, Anda dapat memilih huruf drive berbeda yang tersedia.

Cara membuka kunci data safe Anda

Dengan tiap percobaan berikutnya untuk mengakses data safe, Anda akan diminta untuk membuka kunci data safe dengan kata sandi yang sudah Anda tentukan:



Di dalam bidang teks, harap ketikkan kata sandi Anda untuk mengotorisasi diri Anda, dan klik tombol ***Buka kunci***. Jika Anda perlu bantuan mengingat kata sandi, klik ***Petunjuk*** untuk menampilkan petunjuk kata sandi yang Anda tentukan saat membuat data safe. Data safe baru kan muncul di gambaran umum data safe Anda sebagai TERBUKA, dan Anda akan dapat menambahkan/ menghapus file di dalamnya jika diperlukan.

3.4.2. Perlindungan Penjelajahan Web

Komponen ***Perlindungan Penjelajahan Web*** terdiri dari dua layanan: ***LinkScanner Surf-Shield*** dan ***Online Shield***:

- ***LinkScanner Surf-Shield*** melindungi Anda dari ancaman yang 'hari ini muncul dan besok menghilang' yang semakin meningkat jumlahnya di web. Ancaman ini dapat disembunyikan di berbagai jenis situs Web, mulai situs pemerintah hingga perusahaan besar dan terkenal, hingga bisnis kecil; dan biasanya ancaman ini jarang berada pada situs tersebut lebih dari 24 jam. LinkScanner melindungi Anda dengan menganalisis halaman web di balik semua tautan pada halaman situs yang Anda lihat dan memastikan bahwa tautan itu aman pada saat yang paling penting – yaitu saat Anda akan mengklik tautan tersebut. ***LinkScanner Surf-Shield tidak ditujukan untuk perlindungan platform server!***

- ***Online Shield*** adalah sebuah tipe perlindungan tetap secara waktu nyata yang memindai isi halaman web yang dikunjungi (dan file yang mungkin termasuk di dalamnya) bahkan sebelum halaman ditampilkan di browser web Anda atau diunduh ke komputer. Online Shield mendeteksi apakah halaman yang akan Anda kunjungi berisi javascript berbahaya dan mencegah halaman tersebut untuk ditampilkan. Selain itu, ia akan mengenali malware yang dimasukkan dalam sebuah laman dan segera menghentikan unduhannya agar jangan sampai masuk ke komputer Anda. Perlindungan tangguh ini akan memblokir berbagai konten jahat/ perusak dari halaman web apa pun yang coba Anda buka, dan mencegahnya agar tidak diunduh ke komputer Anda. Bila fitur ini diaktifkan, mengklik tautan atau mengetikkan URL ke situs berbahaya akan mencegah Anda secara otomatis dari membuka halaman Web tersebut, dengan demikian akan melindungi Anda dari terinfeksi secara tidak sengaja. Harap diingat bahwa halaman web yang terkena exploit dapat menginfeksi komputer Anda cukup dengan mengunjungi situs yang terpengaruh. ***Online Shield tidak ditujukan untuk perlindungan platform server!***

Kontrol dialog

Untuk beralih antar dua bagian dialog, Anda cukup mengeklik bagian mana saja dari panel layanan terkait. Panel kemudian akan disorot dengan warna biru yang lebih muda. Di kedua bagian dialog, Anda dapat menemukan kontrol-kontrol berikut ini. Fungsionalitasnya tetap sama meskipun mereka adalah milik layanan keamanan yang satu atau lainnya *(LinkScanner Surf-Shield atau Online Shield)*:

Aktif/ Tidak Aktif – Tombol ini mungkin mengingatkan Anda akan lampu lalu lintas, baik tampilannya ataupun fungsinya. Klik satu kali untuk beralih antar dua posisi. Warna hijau berarti ***Aktif***, yang berarti bahwa layanan keamanan LinkScanner Surf-Shield / Online Shield aktif dan berfungsi penuh. Warna merah menunjukkan status ***Tidak Aktif***, yaitu layanan dinonaktifkan. Jika Anda tidak memiliki alasan yang tepat untuk menonaktifkan layanan, kami sangat menyarankan untuk membiarkan pengaturan default untuk semua konfigurasi keamanan. Pengaturan default menjamin kinerja aplikasi yang optimal dan keamanan maksimal. Jika karena alasan tertentu Anda ingin menonaktifkan layanan, Anda akan segera diperingatkan tentang risiko yang mungkin terjadi oleh tanda ***Peringatan*** berwarna merah dan informasi bahwa Anda tidak benar-benar terlindung pada saat itu. ***Harap diingat bahwa Anda harus mengaktifkan layanan lagi secepat mungkin!***

Pengaturan – Klik tombol agar diarahkan ke antarmuka pengaturan lanjut. Secara tepat dialog tersebut akan terbuka dan Anda akan dapat mengkonfigurasi layanan yang dipilih, yaitu LinkScanner Surf-Shield atau Online Shield. Pada antarmuka pengaturan lanjut, Anda dapat mengedit semua konfigurasi setiap layanan keamanan dalam **AVG Internet Security 2015** tetapi konfigurasi tersebut hanya disarankan untuk pengguna yang berpengalaman!

Tanda panah – Gunakan tanda panah hijau di bagian kiri atas dialog untuk kembali ke antarmuka pengguna utama dengan gambaran umum komponen.

3.4.3. Perlindungan Identitas

Komponen ***Identity Protection*** menjalankan layanan ***Identity Shield*** yang terus melindungi aset digital Anda dari ancaman baru dan tak dikenal di Internet:

- ***Identity Protection*** merupakan layanan anti-malware yang melindungi Anda dari semua jenis malware (*spyware, bot, pencuri identitas, ...*) menggunakan teknologi perilaku dan memberikan perlindungan setiap hari dari virus baru.. Identity Protection difokuskan untuk mencegah agar pencuri identitas tidak mencuri sandi, perincian rekening bank, nomor kartu kredit dan data digital Anda yang bernilai lainnya dengan menggunakan semua jenis perangkat lunak jahat *(malware)* yang menarget PC Anda. Ini memastikan bahwa semua program yang dijalankan pada PC Anda atau di jaringan berbagi Anda beroperasi dengan benar. Identity Protection menemukan dan memblokir perilaku mencurigakan secara terus-menerus dan melindungi komputer Anda dari semua malware baru. Identity Protection memberikan perlindungan seketika bagi komputer Anda terhadap berbagai ancaman baru, bahkan yang tidak dikenal. Ia memantau semua proses *(termasuk yang tersembunyi)* dan lebih dari 285 macam pola perilaku, dan dapat menentukan apakah sesuatu yang membahayakan terjadi dalam sistem Anda. Oleh karena itu, ia dapat mengetahui ancaman yang bahkan belum diterangkan dalam basis data virus. Bila sebuah kode yang tidak dikenal masuk ke komputer Anda, kode tersebut segera diamati dan dipantau apakah menunjukkan perilaku jahat. Jika ternyata file tersebut jahat, Identity Protection akan memindahkan kode tersebut ke Gudang Virus dan membatalkan semua perubahan pada sistem yang telah dilakukannya *(injeksi kode, perubahan register, pembukaan port, dsb.)*. Anda tidak perlu memulai pemindaian untuk tetap terlindungi. Teknologi ini sangat proaktif, jarang memerlukan pembaruan, dan selalu siaga.

Kontrol dialog

Dalam dialog ini, Anda dapat menemukan kontrol berikut:

Aktif/ Tidak Aktif – Tombol ini mungkin mengingatkan Anda akan lampu lalu lintas, baik tampilannya ataupun fungsinya. Klik satu kali untuk beralih antar dua posisi. Warna hijau berarti ***Aktif***, yang berarti bahwa layanan keamanan Identity Protection aktif dan berfungsi penuh. Warna merah menunjukkan status ***Tidak Aktif***, yaitu layanan dinonaktifkan. Jika Anda tidak memiliki alasan yang tepat untuk menonaktifkan layanan, kami sangat menyarankan untuk membiarkan pengaturan default untuk semua konfigurasi keamanan. Pengaturan default menjamin kinerja aplikasi yang optimal dan keamanan maksimal. Jika karena

alasan tertentu Anda ingin menonaktifkan layanan, Anda akan segera diperingatkan tentang risiko yang mungkin terjadi oleh tanda ***Peringatan*** berwarna merah dan informasi bahwa Anda tidak benar-benar terlindung pada saat itu. ***Harap diingat bahwa Anda harus mengaktifkan layanan lagi secepat mungkin!***

 ***Pengaturan*** – Klik tombol agar diarahkan ke antarmuka pengaturan lanjut. Secara tepat dialog tersebut akan terbuka dan Anda akan dapat mengkonfigurasi layanan yang dipilih, yaitu Identity Protection. Pada antarmuka pengaturan lanjut, Anda dapat mengedit semua konfigurasi setiap layanan keamanan dalam **AVG Internet Security 2015** tetapi konfigurasi tersebut hanya disarankan untuk pengguna yang berpengalaman!

 ***Tanda panah*** – Gunakan tanda panah hijau di bagian kiri atas dialog untuk kembali ke antarmuka pengguna utama dengan gambaran umum komponen.

Sayangnya, dalam **AVG Internet Security 2015** layanan Identity Alert tidak disertakan. Jika Anda ingin menggunakan perlindungan semacam ini, ikuti tombol ***Tingkatkan untuk Mengaktifkan*** agar diarahkan ke halaman web khusus di mana Anda dapat membeli lisensi Identity Alert.

Harap diingat bahwa bahkan dengan edisi AVG Premium Security, layanan Identity Alert saat ini hanya tersedia di wilayah tertentu: AS, Inggris, Kanada, dan Irlandia.

3.4.4. Perlindungan Email

Komponen ***Perlindungan Email*** mencakup dua layanan keamanan berikut: ***Pemindai Email*** dan ***Anti-Spam*** *(layanan Anti-Spam hanya dapat diakses di Internet / edisi Premium Security)*.

- ***Pemindai Email***: Salah satu sumber paling umum dari virus dan troya adalah melalui email. Phishing dan spam membuat email menjadi sumber risiko yang jauh lebih besar. Akun email gratis hampir bisa dipastikan akan menerima email jahat semacam itu (*karena akun tersebut jarang memasang teknologi anti-spam*), dan pengguna di rumah sangat mengandalkan email semacam itu. Juga pengguna di rumah, yang menjelajahi situs tak dikenal dan mengisi formulir online dengan data pribadi (*misalnya alamat email mereka*), akan menambah kemungkinan terkena serangan melalui email. Perusahaan biasanya menggunakan akun email perusahaan dan menggunakan filter anti-spam, dll, untuk mengurangi risiko tersebut. Komponen Perlindungan Email bertanggung jawab untuk memindai setiap pesan email yang dikirim atau diterima; kapan saja virus terdeteksi dalam email, virus akan segera dipindahkan ke Gudang Virus. Komponen ini juga dapat memfilter jenis lampiran email tertentu, dan menambahkan teks sertifikasi ke pesan bebas infeksi. ***Pemindai Email tidak ditujukan untuk platform server!***

- ***Anti-Spam*** memeriksa semua pesan email masuk dan menandai email yang tidak diinginkan sebagai spam *(Spam merupakan email yang tidak diundang, hampir semuanya mengiklankan produk atau layanan yang dikirimkan massal ke sejumlah besar alamat email sekaligus, sehingga memenuhi kotak surat penerima. Email komersial resmi yang telah disetujui oleh konsumen tidak termasuk spam.)*. Anti-Spam dapat memodifikasi isi perihal email *(yang telah diidentifikasi sebagai spam)* dengan menambahkan string teks khusus. Sehingga Anda dengan mudah dapat menyaring email dalam klien email. Komponen Anti-Spam menggunakan beberapa metode analisis untuk memproses setiap pesan email, menawarkan perlindungan maksimum yang dapat diberikan dari pesan email yang tidak diinginkan. Anti-Spam menggunakan basis data yang diperbarui secara rutin untuk deteksi spam. Dapat juga menggunakan basis data umum server RBL *(dari alamat email "spammer yang dikenal")* dan secara manual menambahkan alamat email ke Daftar Putih Anda *(jangan tandai sebagai spam)* dan Daftar Hitam *(selalu tandai sebagai spam)*.

Kontrol dialog

Untuk beralih antar dua bagian dialog, Anda cukup mengeklik bagian mana saja dari panel layanan terkait. Panel kemudian akan disorot dengan warna biru yang lebih muda. Di kedua bagian dialog, Anda dapat menemukan kontrol-kontrol berikut ini. Fungsionalitasnya tetap sama meskipun mereka adalah milik layanan keamanan yang satu atau lainnya *(Pemindai Email atau Anti-Spam)*:

Aktif/ Tidak Aktif – Tombol ini mungkin mengingatkan Anda akan lampu lalu lintas, baik tampilannya ataupun fungsinya. Klik satu kali untuk beralih antar dua posisi. Warna hijau berarti ***Aktif***, yang berarti bahwa layanan keamanan aktif dan berfungsi penuh. Warna merah menunjukkan status ***Tidak Aktif***, yaitu layanan dinonaktifkan. Jika Anda tidak memiliki alasan yang tepat untuk menonaktifkan layanan, kami sangat menyarankan untuk membiarkan pengaturan default untuk semua konfigurasi keamanan. Pengaturan default menjamin kinerja aplikasi yang optimal dan keamanan maksimal. Jika karena alasan tertentu Anda ingin menonaktifkan layanan, Anda akan segera diperingatkan tentang risiko yang mungkin terjadi oleh tanda ***Peringatan*** berwarna merah dan informasi bahwa Anda tidak benar-benar terlindung pada saat itu. ***Harap diingat bahwa Anda harus mengaktifkan layanan lagi secepat mungkin!***

Pengaturan – Klik tombol agar diarahkan ke antarmuka pengaturan lanjut. Secara tepat dialog tersebut akan terbuka dan Anda akan dapat mengkonfigurasi layanan yang dipilih, yaitu Pemindai Email atau Anti-Spam. Pada antarmuka pengaturan lanjut, Anda dapat mengedit semua konfigurasi setiap layanan keamanan dalam **AVG Internet Security 2015** tetapi konfigurasi tersebut hanya disarankan untuk pengguna yang berpengalaman!

Tanda panah – Gunakan tanda panah hijau di bagian kiri atas dialog untuk kembali ke antarmuka pengguna utama dengan gambaran umum komponen.

3.4.5. Firewall

Firewall merupakan sebuah sistem yang memberlakukan kebijakan kontrol akses antara dua atau beberapa jaringan dengan cara memblokir/ memperbolehkan lalu lintas. Firewall berisi sekumpulan aturan yang melindungi jaringan internal dari serangan yang berasal *dari luar (biasanya dari Internet)* dan mengontrol semua komunikasi pada setiap port jaringan tunggal. Komunikasi dievaluasi sesuai dengan aturan yang ditentukan, kemudian akan

diperbolehkan atau dilarang. Jika Firewall mengenali adanya upaya penyusupan, ia akan "memblokir" upaya tersebut dan tidak memperbolehkan penyusup mengakses komputer. Firewall dikonfigurasi untuk memperbolehkan atau menolak komunikasi internal/ eksternal *(dua arah, masuk atau keluar)* melalui port yang ditentukan, dan bagi aplikasi perangkat lunak yang ditentukan. Misalnya, firewall dapat dikonfigurasi agar hanya memperbolehkan data Web mengalir masuk dan keluar dengan menggunakan Microsoft Explorer. Segala upaya untuk mentransmisikan data Web melalui browser lain akan diblokir. Firewall melindungi informasi yang dapat membuat orang mengenali Anda secara pribadi, agar tidak bisa dikirimkan dari komputer tanpa seizin Anda. Firewall mengontrol cara komputer Anda bertukar data dengan komputer lain di Internet atau jaringan lokal. Dalam sebuah organisasi, Firewall juga melindungi satu komputer dari serangan yang dilakukan pengguna internal pada komputer lain dalam jaringan.

Di **AVG Internet Security 2015**, ***Firewall*** mengontrol semua lalu lintas di setiap port jaringan pada komputer Anda. Berdasarkan pada aturan yang ditetapkan, Firewall mengevaluasi aplikasi yang sedang dijalankan pada komputer *(dan ingin menghubungkan ke Internet/ jaringan lokal)*, atau aplikasi yang mengakses komputer dari luar mencoba untuk menghubungkan ke PC Anda. Firewall kemudian akan memperbolehkan atau melarang komunikasi untuk masing-masing aplikasi ini pada port jaringan. Secara default, jika aplikasi tidak dikenal *(yakni tidak memiliki aturan Firewall yang ditentukan)*, Firewall akan menanyakan apakah Anda ingin memperbolehkan atau memblokir upaya komunikasi tersebut.

AVG Firewall tidak ditujukan untuk perlindungan platform server!

Saran: *Biasanya tidak disarankan untuk menggunakan lebih dari satu firewall pada satu komputer. Keamanan komputer tidak akan disempurnakan jika Anda menginstal lebih banyak firewall. Kemungkinan besar malah akan terjadi beberapa konflik antara kedua aplikasi ini. Karena itu, kami sarankan Anda menggunakan hanya satu firewall pada komputer Anda dan menonaktifkan semua firewall lain, sehingga meniadakan risiko kemungkinan konflik dan masalah apa pun yang berkaitan dengan hal ini.*

Note: *Setelah instalasi AVG Internet Security 2015 Anda, komponen Firewall mungkin meminta menghidupkan ulang komputer. Bila hal ini terjadi, dialog komponen muncul dengan informasi bahwa perlu menghidupkan ulang. Pada dialog tersebut, Anda akan langsung menemukan tombol* ***Hidupkan Ulang sekarang****. Sampai akhirnya dihidupkan ulang, komponen Firewall tidak benar-benar diaktifkan. Selain itu, semua opsi editing di dalam dialog akan tidak aktif. Harap perhatikan peringatan dan hidupkan ulang PC Anda sesegera mungkin*

Mode Firewall yang tersedia

Firewall memungkinkan Anda untuk menentukan aturan keamanan spesifik berdasarkan pada apakah komputer Anda terletak di suatu domain, sebuah komputer tunggal, atau bahkan notebook. Setiap opsi ini memerlukan tingkat perlindungan yang berbeda, dan level tersebut dicakup oleh mode masing-masing. Singkatnya, mode Firewall merupakan konfigurasi spesifik dari komponen Firewall, dan Anda dapat menggunakan beberapa konfigurasi yang telah ditentukan.

- ***Otomatis*** – Dalam mode ini, Firewall menangani semua lalu lintas jaringan secara otomatis. Anda akan diundang untuk mengambil keputusan. Firewall akan memungkinkan koneksi untuk setiap aplikasi yang dikenal, dan pada saat yang sama aturan aplikasi akan dibuat yang menentukan bahwa aplikasi tersebut selanjutnya dapat selalu terhubung. Untuk aplikasi lain, Firewall akan memutuskan apakah koneksi akan diperbolehkan atau diblokir berdasarkan perilaku aplikasi. Namun, pada situasi semacam itu, aturan tidak akan dibuat dan aplikasi akan diperiksa lagi setiap kali mencoba terhubung. Mode otomatis ini cukup sederhana dan direkomendasikan untuk sebagian besar pengguna.

- ***Interaktif*** – mode ini bermanfaat jika Anda ingin mengendalikan secara penuh semua lalu lintas jaringan ke dan dari komputer Anda. Firewall akan memantaunya dan memberitahu Anda setiap kali ada upaya untuk berkomunikasi atau mentransfer data, yang memungkinkan Anda untuk memperbolehkan atau memblokir upaya yang Anda rasa sesuai. Disarankan untuk pengguna mahir saja.

- ***Blokir akses ke Internet*** – Koneksi Internet benar-benar diblokir, Anda tidak dapat mengakses Internet dan tidak ada orang luar yang dapat mengakses komputer Anda. Hanya untuk penggunaan khusus dan dalam jangka waktu pendek.

- ***Nonaktifkan perlindungan Firewall (tidak disarankan)*** – menonaktifkan Firewall akan mengaktifkan semua lalu lintas jaringan ke dan dari komputer Anda. Akibatnya, pengaturan ini akan membuat rentan terhadap serangan peretas. Harap selalu pertimbangkan pilihan ini secara hati-hati.

Harap diingat bahwa ada mode otomatis khusus yang tersedia dalam Firewall. Mode ini akan diaktifkan dengan diam-diam jika komponen Komputer atau Identity Protection dinonaktifkan dan komputer Anda menjadi lebih rentan. Pada kasus tersebut, Firewall otomatis hanya akan memperbolehkan aplikasi yang dikenal dan benar-benar aman. Untuk aplikasi lainnya, Firewall akan bertanya pada Anda. Hal ini dilakukan untuk komponen perlindungan yang dinonaktifkan dan untuk mengamankan komputer Anda.

Kami sangat menyarankan untuk tidak menonaktifkan Firewall! Bagaimanapun juga, jika perlu dan Anda sungguh harus menonaktifkan komponen Firewall, Anda dapat melakukannya dengan memilih mode Nonaktifkan perlindungan Firewall dari daftar mode Firewall yang tersedia di atas.

Kontrol dialog

Dialog ini akan memberikan gambaran umum informasi dasar mengenai status komponen Firewall:

- ***Mode Firewall*** – Menyediakan informasi mengenai mode Firewall yang saat ini dipilih. Gunakan tombol ***Ubah*** yang terletak di sebelah informasi yang disediakan untuk beralih ke antarmuka Pengaturan Firewall jika Anda ingin mengubah mode saat ini ke mode lainnya *(untuk keterangan dan saran tentang penggunaan profil Firewall, silakan lihat paragraf sebelumnya)*.

- ***Berbagi file dan printer*** – Memberikan informasi apakah berbagi file dan printer *(untuk kedua arah)* diperbolehkan pada saat itu. Berbagi file dan printer artinya berbagi semua file atau folder yang Anda tandai sebagai "Digunakan Bersama" pada Windows, unit disk, printer, pemindai bersama dan semua perangkat sejenis. Berbagi item semacam itu hanya mungkin dilakukan dalam jaringan yang bisa dianggap aman *(misalnya di rumah, di kantor atau di sekolah)*. Namun, jika Anda tersambung ke jaringan

publik *(seperti Wi-Fi bandara atau kafe Internet)*, Anda mungkin tidak ingin berbagi apa pun.

- ***Terhubung ke*** – Memberikan informasi mengenai nama jaringan yang sedang terhubung dengan Anda. Dengan Windows XP, nama jaringan akan merespons nama yang Anda pilih untuk jaringan tertentu ketika pertama kali terhubung ke jaringan tersebut. Dengan Windows Vista dan versi di atasnya, nama jaringan akan diambil secara otomatis dari Network and Sharing Center.

- ***Atur ulang ke default*** – Tekan tombol ini untuk menimpa konfigurasi Firewall saat ini, dan untuk kembali ke konfigurasi default berdasarkan deteksi otomatis.

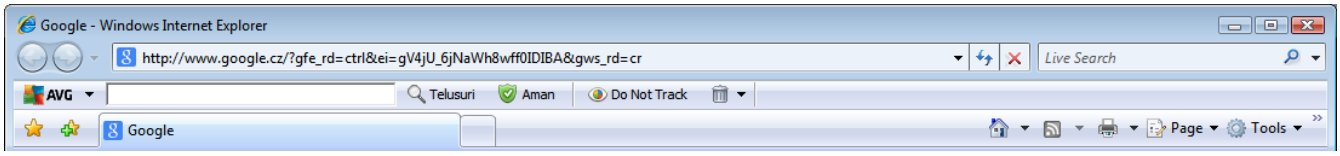
Dialog ini berisi kontrol-kontrol grafik berikut:

Pengaturan – Klik tombol untuk dialihkan ke antarmuka Pengaturan Firewall di mana Anda dapat mengedit semua konfigurasi Firewall. Semua konfigurasi hanya boleh dilakukan oleh pengguna berpengalaman!

Tanda panah – Gunakan tanda panah hijau di bagian kiri atas dialog untuk kembali ke antarmuka pengguna utama dengan gambaran umum komponen.

3.5. AVG Security Toolbar

AVG Security Toolbar merupakan alat yang erat bekerja sama dengan layanan LinkScanner Surf-Shield, dan menjaga keamanan maksimum saat Anda menjelajah Internet. Dalam **AVG Internet Security 2015**, instalasi ***AVG Security Toolbar*** bersifat opsional; selama proses instalasi Anda diminta memutuskan apakah komponen tersebut harus diinstal. ***AVG Security Toolbar*** tersedia secara langsung dalam browser Internet Anda. Untuk saat ini, browser Internet yang didukung adalah Internet Explorer (*versi 6.0 dan yang lebih tinggi*), dan/atau Mozilla Firefox (*versi 3.0 dan yang lebih tinggi*). Tidak ada browser lain yang didukung *(jika Anda menggunakan browser Internet alternatif, misalnya Avant Browser, maka Anda mungkin mengalami cara kerja yang tidak diharapkan).*



AVG Security Toolbar terdiri dari item berikut:

- ***Logo AVG*** dengan menu buka-bawah:
  - ***Tingkat Ancaman Saat Ini*** – membuka halaman Web lab virus yang berisi tampilan grafis mengenai tingkat ancaman saat ini di Web.
  - ***Lab Ancaman AVG*** – membuka situs Web ***Lab Ancaman AVG*** tertentu *(pada http://www.avgthreatlabs.com)* tempat Anda dapat menemukan informasi mengenai berbagai keamanan situs web dan tingkat ancaman saat ini secara online.
  - ***Bantuan Toolbar*** – membuka bantuan online yang mencakup semua fungsionalitas ***AVG Security Toolbar***.
  - ***Kirim Masukan Produk*** – membuka halaman web berisi formulir yang dapat Anda isi dan memberi tahu kami pendapat Anda tentang ***AVG Security Toolbar***.

- ***Perjanjian Lisensi Pengguna Akhir*** – membuka situs web AVG yang berisi halaman keseluruhan teks persetujuan lisensi terkait penggunaan **AVG Internet Security 2015** Anda.
- ***Kebijakan Privasi*** – membuka situs web AVG yang berisi halaman tempat Anda dapat menemukan keseluruhan teks Kebijakan Privasi AVG.
- ***Hapus Instalasi AVG Security Toolbar*** – membuka halaman web yang memberikan keterangan terperinci tentang bagaimana cara menonaktifkan ***AVG Security Toolbar*** pada setiap browser web yang didukung.
- ***Tentang...*** – membuka jendela baru berisi informasi mengenai versi ***AVG Security Toolbar*** yang saat ini terinstal.

- ***Kolom penelusuran*** – menelusuri Internet menggunakan ***AVG Security Toolbar*** agar benar-benar aman dan nyaman karena semua hasil telusur yang ditampilkan seratus persen aman. Masukkan kata kunci atau kalimat ke dalam bidang penelusuran, dan tekan tombol ***Telusuri*** *(atau Enter)*.
- ***Site Safety*** – tombol ini membuka dialog baru yang menyediakan informasi tentang tingkat ancaman saat ini (*Aman*) dari halaman yang sedang Anda kunjungi. Gambaran umum singkat ini dapat diperluas, dan ditampilkan dengan perincian lengkap tentang semua kegiatan keamanan yang berkaitan dengan halaman, tepat dalam jendela browser (*Lihat Laporan Situs Web*):

- ***Do Not Track*** – layanan DNT membantu Anda mengidentifikasi berbagai situs web yang mengumpulkan data tentang berbagai aktivitas online Anda serta memberikan Anda pilihan untuk mengizinkannya atau melarangnya. Perincian >>
- ***Hapus*** – tombol 'bak sampah' menghadirkan menu turunan tempat Anda dapat memilih apakah ingin

menghapus informasi di formulir online penelusuran internet, pengunduhan, atau menghapus semua riwayat pencarian Anda sekaligus.

- ***Cuaca*** – tombol ini membuka dialog baru yang memberikan informasi mengenai cuaca saat ini di lokasi Anda, serta prakiraan cuaca untuk dua hari mendatang. Informasi ini rutin diperbarui setiap 3-6 jam. Dalam dialog, Anda dapat mengubah lokasi yang diinginkan secara manual, menentukan apakah Anda ingin melihat info suhu dalam Celsius atau Fahrenheit.

- ***Facebook*** – Tombol ini memungkinkan Anda menghubungkan ke jaringan sosial Facebook langsung dari dalam ***AVG Security Toolbar***.

- Tombol pintasan untuk akses cepat ke aplikasi ini: ***Calculator***, ***Notepad***, ***Windows Explorer***.

3.6. AVG Do Not Track

AVG Do Not Track membantu Anda mengidentifikasi situs web yang sedang mengumpulkan data tentang aktivitas online Anda. ***AVG Do Not Track*** yang merupakan bagian dari AVG Security Toolbar menampilkan berbagai situs web dan pengiklan yang mengumpulkan data tentang aktivitas Anda serta memberi Anda pilihan untuk mengizinkannya atau melarangnya.

- ***AVG Do Not Track*** memberikan informasi tambahan untuk Anda tentang kebijakan privasi layanan terkait, begitu juga tautan langsung untuk Keluar dari layanan, jika tersedia.

- Selain itu, ***AVG Do Not Track*** mendukung protokol W3C DNT untuk secara otomatis memberitahu situs yang tidak ingin dilacak. Pemberitahuan ini diaktifkan secara default, tetapi dapat diubah kapan pun.

- ***AVG Do Not Track*** diberikan berdasarkan syarat dan ketentuan ini.

- ***AVG Do Not Track*** diaktifkan secara default, tetapi dapat dengan mudah dinonaktifkan kapan pun. Petunjuknya dapat ditemukan di artikel Tanya-Jawab Menonaktifkan fitur AVG Do Not Track.

- Untuk informasi selanjutnya tentang ***AVG Do Not Track***, silakan kunjungi situs web kami.

Saat ini, fungsionalitas ***AVG Do Not Track*** hanya didukung di peramban Mozilla Firefox, Chrome, dan Internet Explorer.

3.6.1. Antarmuka AVG Do Not Track

Ketika online, ***AVG Do Not Track*** segera memperingatkan Anda bila ada aktivitas pengumpulan data yang terdeteksi. Dalam kasus yang demikian, ikon ***AVG Do Not Track*** yang terletak di AVG Security Toolbar mengubah tampilannya; satu angka kecil muncul di samping ikon yang memberikan informasi tentang layanan pengumpulan data yang terdeteksi:  Klik ikon itu untuk melihat dialog berikut:

Semua layanan pengumpulan data yang terdeteksi terdaftar di ***Pelacak di gambaran umum*** halaman ini. Ada tiga tipe aktivitas pengumpulan data yang dikenali oleh ***AVG Do Not Track***:

- ***Web Analytics*** *(diperbolehkan secara default):* Layanan yang digunakan untuk meningkatkan kinerja dan pengalaman situs web terkait. Dalam kategori ini Anda dapat menemukan layanan seperti Google Analytics, Omniture, atau Yahoo Analytics. Kami menyarankan untuk tidak memblokir layanan web analytics, karena situs web mungkin tidak bekerja sesuai yang dimaksudkan.

- ***Ad Networks*** *(beberapa diblokir secara default):* Layanan yang mengumpulkan atau membagikan data tentang aktivitas online Anda ke banyak situs, baik secara langsung maupun tidak langsung, untuk menawari Anda Iklan yang dipersonalisasi dan tidak seperti Iklan yang berbasis daftar isi. Layanan ini ditentukan berdasarkan kebijakan privasi masing-masing jaringan Iklan sebagaimana tersedia di situs web jaringan Iklan tersebut. Beberapa jaringan iklan diblokir secara default.

- ***Social Buttons*** *(diperbolehkan secara default):* Elemen yang didesain untuk meningkatkan pengalaman berjejaring sosial. Tombol sosial dijalankan dari jejaring sosial ke situs yang sedang Anda kunjungi. Tombol tersebut dapat mengumpulkan data tentang aktivitas online Anda jika Anda masuk. Contoh-contoh tombol Sosial antara lain: Plugin Sosial Facebook, Tombol Twitter, dan Google +1.

Catatan: *Tergantung pada layanan yang berjalan di latar belakang situs web, tiga bagian yang diterangkan di atas mungkin tidak muncul pada dialog AVG Do Not Track.*

Kontrol dialog

- ***Apa itu pelacakan?*** – Klik tautan ini di bagian atas dialog agar Anda diarahkan kembali ke halaman web khusus yang menyediakan penjelasan terperinci tentang prinsip-prinsip pelacakan, dan keterangan tipe-tipe pelacakan spesifik.

- ***Blokir Semua*** – Klik tombol ini yang terletak di bagian bawah dialog untuk menyatakan Anda tidak menginginkan aktivitas pengumpulan data sama sekali*(untuk detail lihat bab Proses pelacakan pemblokiran*

- ***Pengaturan AVG Do Not Track*** – klik tautan di bagian bawah dialog agar Anda diarahkan kembali ke halaman web khusus, agar Anda dapat menetapkan konfigurasi spesifik berbagai parameter ***AVG Do Not Track*** *(lihat bab pengaturan AVG Do Not Track untuk informasi lengkap)*

3.6.2. Informasi tentang proses pelacakan

Daftar layanan pengumpulan data yang terdeteksi hanya menyediakan nama layanan tertentu. Untuk membuat keputusan cepat tentang apakah masing-masing layanan harus diblokir atau diizinkan, Anda mungkin perlu tahu lebih banyak. Gerakkan mouse Anda ke masing-masing item daftar. Sebuah gelembung informasi muncul dengan memberikan data terperinci tentang layanan. Anda akan mengetahui apakah layanan pelacakannya mengumpulkan data pribadi Anda atau data lain yang tersedia; apakah data sedang dibagi dengan subjek pihak ketiga lain, dan apakah data yang dikumpulkan sedang disimpan untuk kemungkinan tujuan lebih lanjut:

Di bagian bawah gelembung informasi, Anda dapat melihat hyperlink ***Kebijakan Privasi*** yang mengarahkan Anda ke situs web khusus untuk kebijakan privasi dari masing-masing layanan yang terdeteksi.

3.6.3. Memblokir proses pelacakan

Dengan daftar semua Ad Networks / Social Buttons / Web Analytics, Anda sekarang memiliki opsi untuk mengontrol layanan mana yang harus diblokir. Anda dapat memakai dua cara:

- ***Blokir Semua*** – Klik tombol ini yang terletak di bagian bawah dialog untuk menyatakan Anda tidak menginginkan aktivitas pengumpulan data sama sekali. *(Namun, harap ingat bahwa tindakan ini mungkin merusak fungsionalitas di laman web terkait di mana layanan ini sedang berjalan!)*

- – Jika Anda tidak ingin memblokir semua sistem yang terdeteksi sekaligus, Anda dapat menentukan apakah layanan tersebut harus diizinkan atau diblokir satu per satu. Anda mungkin memperbolehkan untuk menjalankan beberapa sistem yang terdeteksi *(misalnya: Web Analytics):* sistem ini menggunakan data yang dikumpulkan untuk pengoptimalan situs web mereka sendiri, dan dengan cara ini mereka membantu meningkatkan lingkungan Internet secara umum bagi semua pengguna. Namun, pada saat yang sama Anda dapat memblokir aktivitas pengumpulan data semua proses yang diklasifikasikan sebagai Ad Networks. Cukup klik ikon di samping masing-masing layanan untuk memblokir pengumpulan data *(nama proses akan muncul sebagai dicoret)*, atau untuk memperbolehkan pengumpulan data kembali.

3.6.4. Pengaturan AVG Do Not Track

Dialog ***Do Not Track Options*** menawarkan opsi konfigurasi berikut:

- ***Do Not Track diaktifkan*** – Secara default, layanan DNT aktif *(HIDUPKAN)* Untuk menonaktifkan layanan ini, pindahkan posisi saklar ke ON.

- Di bagian tengah dialog ini Anda dapat melihat kotak berisi daftar layanan kumpulan data yang dikenal yang dapat digolongkan sebagai Ad Networks. Secara default, ***Do Not Track*** memblokir beberapa Ad Networks secara otomatis dan keputusan pemblokiran ini tetap bergantung Anda apakah sisanya harus diblokir juga, atau dibiarkan diizinkan. Untuk melakukannya, cukup klik tombol ***Blokir Semua*** di bawah daftar. Atau Anda dapat menggunakan tombol ***Default*** untuk membatalkan seluruh pengaturan perubahan yang telah berjalan, dan kembali ke konfigurasi semula.

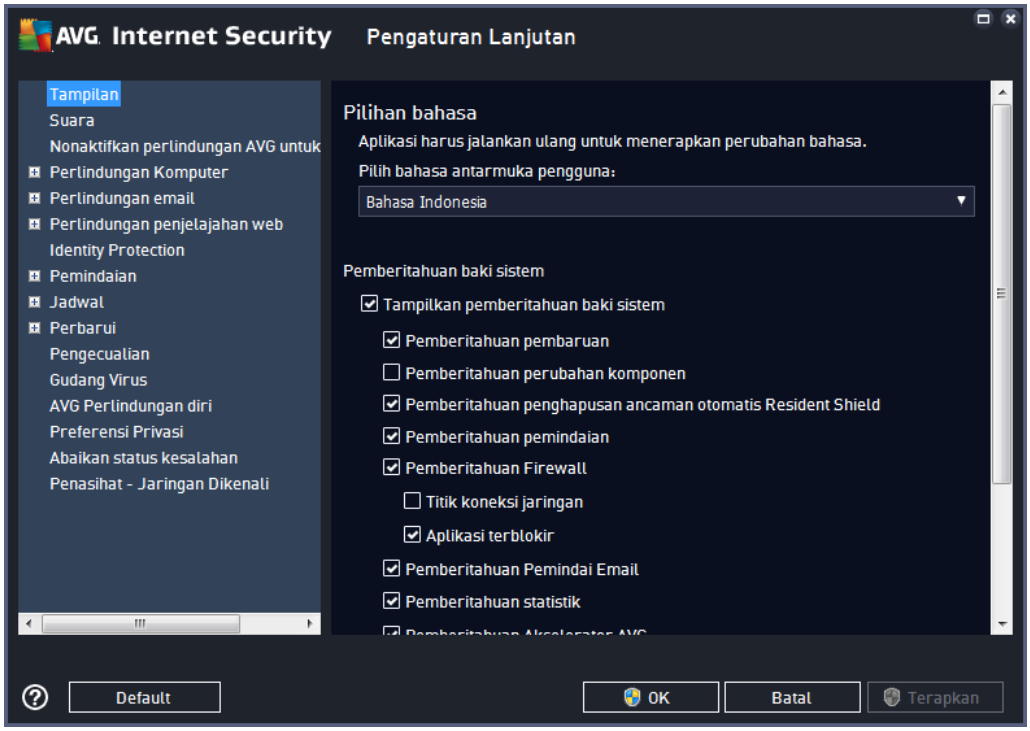
- ***Beri tahu situs web...*** – Di bagian ini, Anda dapat mengaktifkan/menonaktifkan opsi ***Beri tahu situs yang tidak boleh melacak saya*** *(diaktifkan secara default).* Biarkan opsi ini ditandai untuk mengonfirmasi bahwa Anda ingin agar ***Do Not Track*** memberi tahu penyedia layanan pengumpulan data bahwa Anda tidak mau dilacak.

3.7. Pengaturan Lanjut AVG

Dialog konfigurasi lanjut **AVG Internet Security 2015** akan membuka jendela baru bernama ***Pengaturan AVG Lanjut***. Jendela ini terbagi dua bagian: bagian kiri menawarkan navigasi dengan susunan terstruktur ke berbagai opsi konfigurasi program. Pilih komponen yang ingin Anda ubah konfigurasinya (*atau bagian spesifiknya*) untuk membuka dialog pengeditan di bagian sebelah kanan jendela.

3.7.1. Tampilan

Item pertama pada struktur navigasi, ***Tampilan***, mengacu pada pengaturan umum antarmuka pengguna **AVG Internet Security 2015**, dan menyediakan beberapa opsi mendasar pada cara kerja aplikasi:

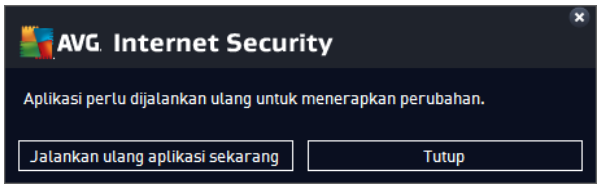


Pemilihan bahasa

Di bagian ***Pemilihan bahasa*** Anda dapat memilih bahasa yang diinginkan dari menu buka-bawah. Bahasa yang dipilih kemudian akan digunakan untuk seluruh antarmuka pengguna **AVG Internet Security 2015**. Menu buka-bawah hanya menawarkan bahasa yang sebelumnya telah Anda pilih untuk diinstal selama proses instalasi plus Bahasa Inggris (*Bahasa Inggris selalu diinstal secara otomatis, secara default*). Untuk menyelesaikan perpindahan **AVG Internet Security 2015** Anda ke bahasa lain, Anda harus menjalankan ulang aplikasi. Harap ikuti langkah-langkah ini:

- Dalam menu buka-bawah, pilih bahasa yang diinginkan pada aplikasi
- Konfirmasi pilihan Anda dengan menekan tombol ***Terapkan*** *(sudut kanan bawah dialog)*
- Tekan tombol ***OK*** untuk mengkonfirmasi
- Sebuah dialog baru akan muncul yang memberi tahu Anda bahwa untuk mengubah bahasa aplikasi, Anda perlu menjalankan ulang **AVG Internet Security 2015**

- Tekan tombol ***Jalankan ulang AVG sekarang*** untuk menyetujui menjalankan ulang program, dan tunggu sebentar hingga perubahan bahasa diberlakukan:



Pemberitahuan baki sistem

Dalam bagian ini Anda dapat menyembunyikan tampilan pemberitahuan baki sistem mengenai status aplikasi **AVG Internet Security 2015**. Secara default, pemberitahuan sistem diperbolehkan untuk ditampilkan. Sangat disarankan untuk membiarkan konfigurasi ini! Pemberitahuan sistem misalnya memberikan informasi diluncurkannya proses pemindaian atau pembaruan, atau mengenai perubahan status komponen **AVG Internet Security 2015**. Anda harus memperhatikan pemberitahuan ini!

Namun demikian, jika karena beberapa alasan Anda tidak ingin diberi tahu dengan cara ini, atau Anda hanya ingin melihat pemberitahuan tertentu *(berhubungan dengan komponen AVG Internet Security 2015 tertentu)*, Anda dapat menentukan dan menetapkan preferensi dengan mencentang/ mengosongkan kotak centang pada opsi berikut:

- ***Tampilkan pemberitahuan baki sistem*** *(diaktifkan, secara default)* – secara default, semua pemberitahuan ditampilkan. Jangan tandai item ini untuk menonaktifkan sama sekali tampilan semua pemberitahuan sistem. Bila diaktifkan, Anda dapat memilih lebih lanjut pemberitahuan spesifik yang akan ditampilkan:
  - ***Pemberitahuan pembaruan*** *(aktif, secara default)* – putuskan apakah informasi mengenai **AVG Internet Security 2015** peluncuran proses pembaruan, kemajuannya, dan finalisasinya harus ditampilkan.
  - ***Pemberitahuan perubahan komponen*** *(dinonaktifkan, secara default)* – putuskan apakah informasi mengenai aktivitas/ inaktivitas komponen, atau kemungkinan masalahnya harus ditampilkan. Saat melaporkan status kesalahan komponen, opsi ini sama dengan fungsi informatif ikon baki sistem yang melaporkan masalah dalam komponen **AVG Internet Security 2015**.
  - ***Pemberitahuan penghapusan ancaman otomatis Resident Shield*** *(diaktifkan, secara default)* – putuskan apakah informasi mengenai penyimpanan, penyalinan, dan proses pembukaan file harus ditampilkan atau disembunyikan (*konfigurasi ini hanya muncul saat opsi pulihkan otomatis pada Resident Shield telah diaktifkan*).
  - ***Pemberitahuan pemindaian*** *(aktif, secara default)* – putuskan apakah informasi saat peluncuran otomatis pemindaian terjadwal, kemajuan, dan hasilnya harus ditampilkan.
  - ***Pemberitahuan Firewall*** *(diaktifkan, secara default)* – putuskan apakah informasi yang berkaitan dengan status dan proses Firewall, mis. peringatan aktivasi/ deaktivasi, kemungkinan pemblokiran lalu lintas, dll. harus ditampilkan. Item ini menyediakan dua opsi pilihan yang lebih spesifik *(untuk penjelasan terperinci masing-masing, silakan baca bab Firewall pada dokumen ini)*:
    – ***Titik koneksi jaringan*** *(dinonaktifkan, secara default)* – ketika tersambung ke jaringan, Firewall menginformasikan apakah aplikasi ini mengetahui jaringan tersebut dan bagaimana berbagi file dan printer akan diatur.

– ***Aplikasi yang diblokir*** *(diaktifkan, secara default)* – ketika aplikasi yang tidak dikenal atau mencurigakan mencoba tersambung ke jaringan, Firewall memblokir usaha tersebut dan menampilkan sebuah pemberitahuan. Sangat penting uuntuk membuat Anda terus tahu, karena itu kami menyarankan Anda untuk selalu mengaktifkan fitur.

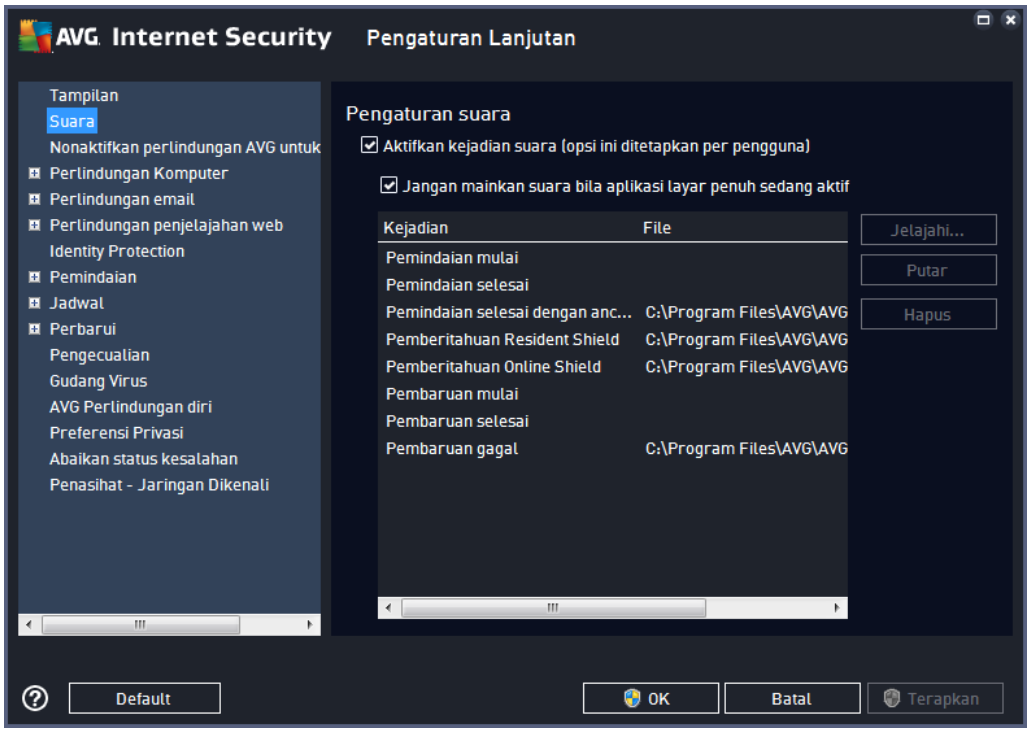
- ***Pemberitahuan Pemindai Email*** *(diaktifkan, secara default)* – putuskan apakah informasi mengenai pemindaian semua pesan email yang masuk dan keluar akan ditampilkan.
- ***Pemberitahuan statistik*** *(diaktifkan, secara default)* – biarkan opsi ini ditandai untuk memperbolehkan pemberitahuan peninjauan statistik secara rutin ditampilkan di baki sistem.
- ***Pemberitahuan Akselerator AVG*** *(diaktifkan, secara default)* – putuskan apakah informasi tentang aktivitas ***Akselerator AVG*** harus ditampilkan. Layanan ***Akselerator AVG*** memungkinkan pemutaran video online lebih lancar dan membuat pengunduhan tambahan lebih mudah.
- ***Pemberitahuan perbaikan waktu booting*** *(dinonaktifkan, secara default)* – putuskan apakah Anda ingin diberi tahu tentang akselerasi waktu booting komputer Anda.
- ***Pemberitahuan Penasihat AVG*** *(diaktifkan, secara default)* – putuskan apakah informasi tentang aktivitas Penasihat AVG harus ditampilkan di panel geser pada baki sistem.

Mode permainan

Fungsi AVG ini dirancang untuk aplikasi layar penuh bila balon informasi AVG (*misalnya saat dimulainya pemindaian terjadwal*) dirasa mengganggu (*hal ini dapat menyembunyikan aplikasi atau merusak grafiknya*). Untuk menghindari hal ini, biarkan kotak untuk opsi ***Aktifkan mode permainan bila aplikasi layar penuh dijalankan*** ditandai (*pengaturan default*).

3.7.2. Suara

Dalam dialog ***Pengaturan Suara*** Anda dapat menetapkan apakah Anda ingin diberi tahu tentang tindakan tertentu **AVG Internet Security 2015** dengan pemberitahuan suara:



Pengaturan ini hanya berlaku untuk akun pengguna aktif. Maksudnya, setiap pengguna dapat mengatur sendiri suaranya. Jika Anda ingin memperbolehkan pemberitahuan suara, biarkan opsi ***Aktifkan kejadian suara*** tetap ditandai (*opsi diaktifkan secara default*) untuk mengaktifkan daftar semua tindakan yang relevan. Anda mungkin juga perlu menandai opsi ***Jangan mainkan suara bila aplikasi layar penuh sedang aktif*** untuk membungkam pemberitahuan suara bila merasa terganggu *(lihat juga bagian mode Permainan pada bab Pengaturan lanjut/ Tampilan dalam dokumen ini)*.

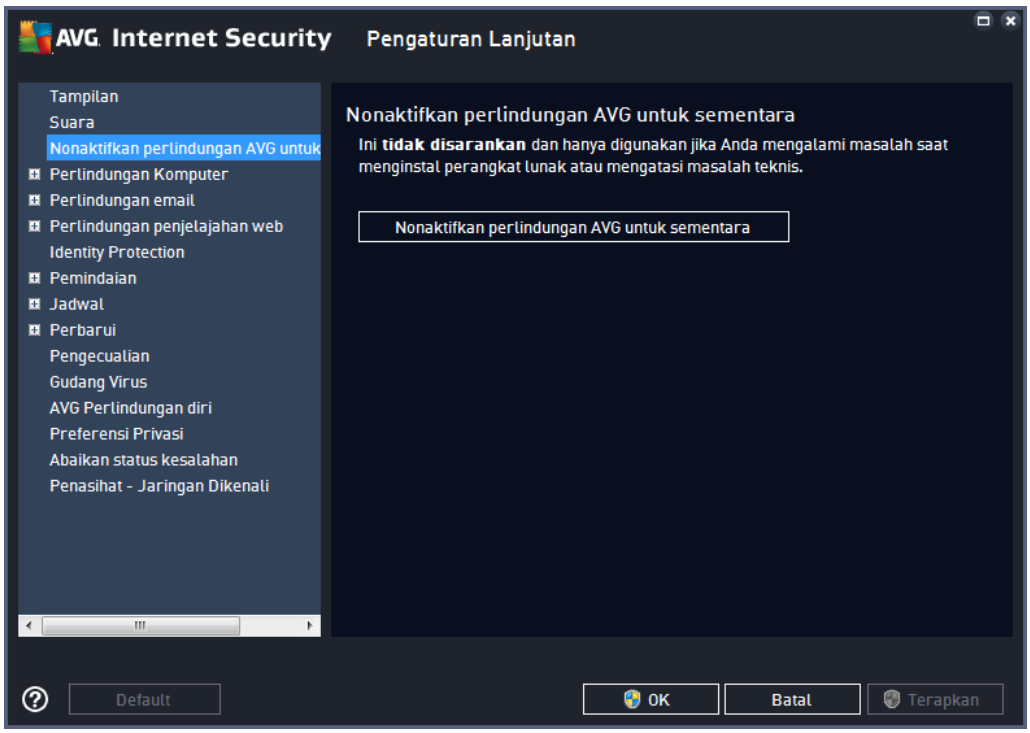
Tombol kontrol

- ***Jelajah...*** – setelah memilih kejadian yang bersangkutan dari daftar, gunakan tombol ***Jelajah*** untuk mencari file suara yang diinginkan di disk Anda, yang akan digunakan. *(Perhatikan bahwa hanya file suara *.wav yang didukung untuk saat ini!)*
- ***Putar*** – untuk mendengarkan suara yang dipilih, sorot kejadian dalam daftar dan tekan tombol ***Putar***.
- ***Hapus*** – gunakan tombol ***Hapus*** untuk menghapus suara yang ditetapkan untuk kejadian tertentu.

3.7.3. Menonaktifkan perlindungan AVG untuk sementara

Dalam dialog ***Nonaktifkan perlindungan AVG untuk sementara*** Anda mempunyai opsi untuk menonaktifkan seluruh perlindungan yang diberikan oleh **AVG Internet Security 2015** sekaligus.

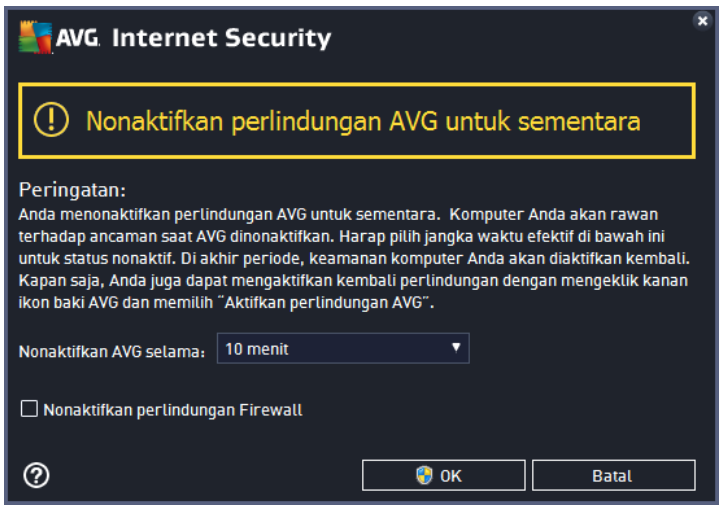
Ingatlah bahwa Anda tidak boleh menggunakan opsi ini kecuali jika sangat diperlukan!



Umumnya, ***tidak perlu*** menonaktifkan **AVG Internet Security 2015** sebelum menginstal perangkat lunak atau driver baru, meskipun penginstal atau wizard perangkat lunak menyarankan agar program dan aplikasi yang berjalan ditutup terlebih dahulu untuk memastikan tidak ada gangguan yang tidak diinginkan selama proses instalasi. Jika Anda mengalami masalah selama penginstalan, coba nonaktifkan perlindungan tetap *(di dialog yang tertaut, hapus centang item **Aktifkan Resident Shield**)* terlebih dahulu. Jika Anda menonaktifkan **AVG Internet Security 2015** untuk sementara, Anda harus mengaktifkannya lagi begitu Anda selesai. Jika Anda terhubung dengan Internet atau jaringan saat perangkat lunak antivirus Anda dinonaktifkan, komputer Anda rentan terhadap serangan.

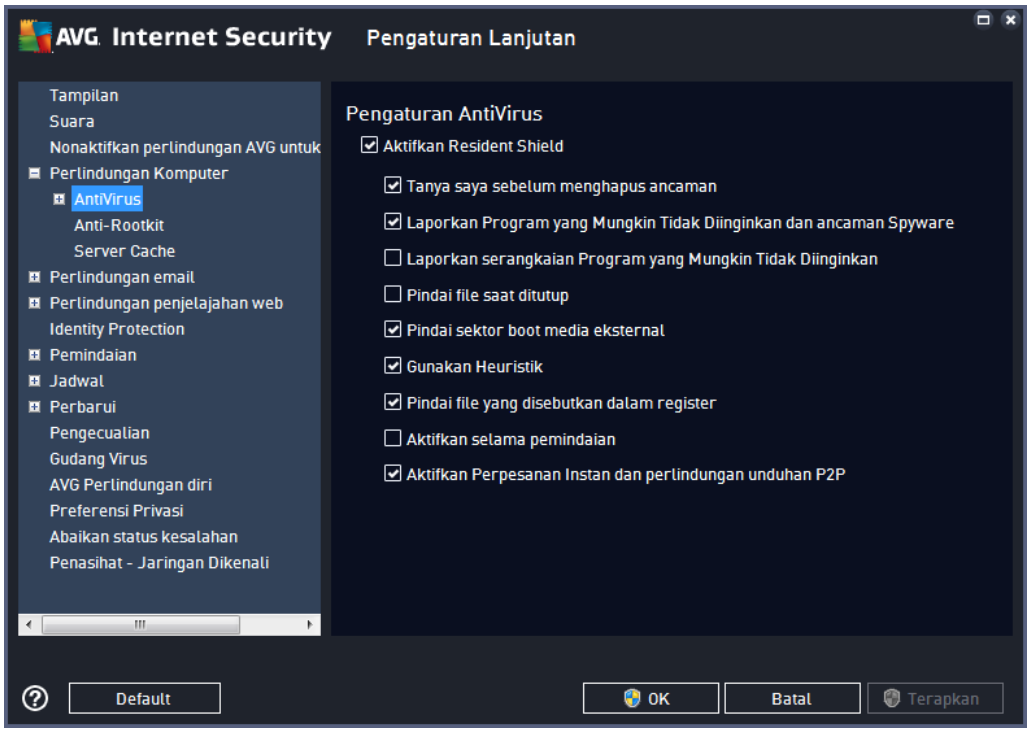
Cara menonaktifkan perlindungan AVG

Centang ***Nonaktifkan perlindungan AVG untuk sementara***, dan konfirmasi pilihan Anda dengan menekan tombol ***Terapkan.*** Dalam dialog ***Nonaktifkan perlindungan AVG untuk sementara*** yang baru dibuka, tetapkan berapa lama Anda ingin menonaktifkan **AVG Internet Security 2015**. Secara default, perlindungan akan dinonaktifkan selama 10 menit, yang seharusnya cukup untuk tugas umum seperti menginstal perangkat lunak baru, dsb. Anda dapat menetapkan jangka waktu yang lebih lama, tetapi opsi ini tidak disarankan jika tidak sepenuhnya perlu. Setelah itu, semua komponen yang dinonaktifkan akan diaktifkan lagi secara otomatis. Maksimal, Anda dapat menonaktifkan perlindungan AVG sampai komputer dihidupkan ulang. Opsi terpisah untuk menonaktifkan komponen ***Firewall*** disajikan dalam dialog ***Nonaktifkan perlindungan AVG untuk sementara***. Centang ***Nonaktifkan perlindungan Firewall*** untuk melakukannya.



3.7.4. Perlindungan Komputer

AntiVirus bersama dengan ***Resident Shield*** melindungi komputer Anda secara terus-menerus dari semua jenis virus, spyware, dan malware yang dikenal *(termasuk malware nonaktif dan tidur, yakni malware yang telah terunduh namun belum diaktifkan)*.



Dalam dialog ***Pengaturan Resident Shield***, Anda dapat mengaktifkan atau menonaktifkan sepenuhnya perlindungan tetap dengan menandai atau tidak menandai item ***Aktifkan Resident Shield*** (*opsi ini telah diaktifkan secara default*). Selain itu, Anda dapat memilih fitur perlindungan tetap apa yang harus diaktifkan:

- ***Tanya saya sebelum menghapus ancaman*** (*diaktifkan secara default*) – centang untuk memastikan bahwa Resident Shield tidak akan melakukan tindakan apapun secara otomatis; melainkan akan menampilkan dialog yang menjelaskan ancaman yang terdeteksi, yang memungkinkan Anda memutuskan apa yang harus dilakukan. Jika Anda membiarkan kotak ini tidak dicentang, **AVG Internet Security 2015** otomatis akan memulihkan infeksi; dan jika tidak memungkinkan, objek tersebut akan dipindahkan ke Gudang Virus.

- ***Laporkan Program yang Mungkin Tidak Diinginkan dan ancaman Spyware*** (*diaktifkan secara default*) – centang untuk mengaktifkan pemindaian spyware serta virus. Spyware merupakan kategori malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang terinstal secara tidak disengaja. Kami sarankan untuk tetap mengaktifkan fitur ini karena akan meningkatkan keamanan komputer Anda.

- ***Laporkan serangkaian Program yang Mungkin Tidak Diinginkan*** (*dinonaktifkan secara default*) – tandai untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, tetapi dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, meskipun hal ini dapat memblokir program yang legal, dan karenanya dinonaktifkan secara default.

- ***Pindai file saat ditutup*** (*dinonaktifkan secara default*) – pemindaian saat ditutup memastikan bahwa AVG akan memindai berbagai objek aktif (misalnya aplikasi, dokumen, ...) saat sedang dibuka, dan saat sedang ditutup; fitur ini membantu Anda melindungi komputer terhadap beberapa tipe virus canggih.

- ***Pindai sektor boot media eksternal*** (*aktif secara default*) – centang untuk memindai sektor boot USB flashdisk, disk drive eksternal dan media eksternal laiinya dari ancaman.

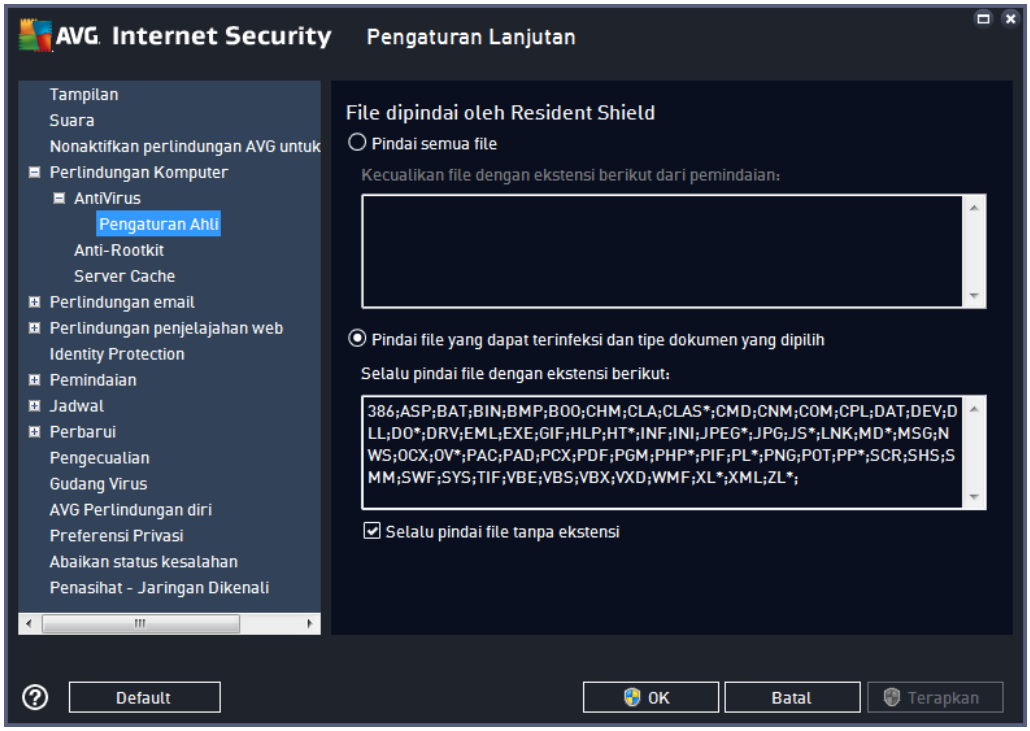
- ***Gunakan Heuristik*** (*diaktifkan secara default*) – analisis heuristik akan digunakan untuk deteksi (*emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual*).

- ***Pindai file yang disebutkan dalam register*** (*diaktifkan secara default*) – parameter ini menentukan apakah AVG akan memindai semua file yang dapat dijalankan yang ditambahkan ke register startup agar infeksi yang dikenal tidak dijalankan saat komputer dihidupkan berikutnya.

- ***Aktifkan selama pemindaian*** (*dinonaktifkan secara default*) – dalam kondisi tertentu (*dalam keadaan sangat darurat*) Anda dapat mencentang opsi ini untuk mengaktifkan algoritma paling menyeluruh yang akan memeriksa semua objek yang mungkin mengancam, secara mendalam. Tetapi harap diingat bahwa metode ini memakan waktu lama.

- ***Aktifkan perlindungan Pesan Instan dan perlindungan unduhan P2P*** (*diaktifkan secara default*) – centang pilihan ini jika Anda ingin memastikan bahwa komunikasi pesanInappropriate style instan (*misalnya AIM, Yahoo!, ICQ, Skype, MSN Messenger, ...*) dan data yang diunduh dalam jaringan Peer-to-Peer *(jaringan yang mengizinkan koneksi langsung antar klien, tanpa server, yang berpotensi membahayakan, biasanya digunakan untuk berbagi file musik)* bebas virus.

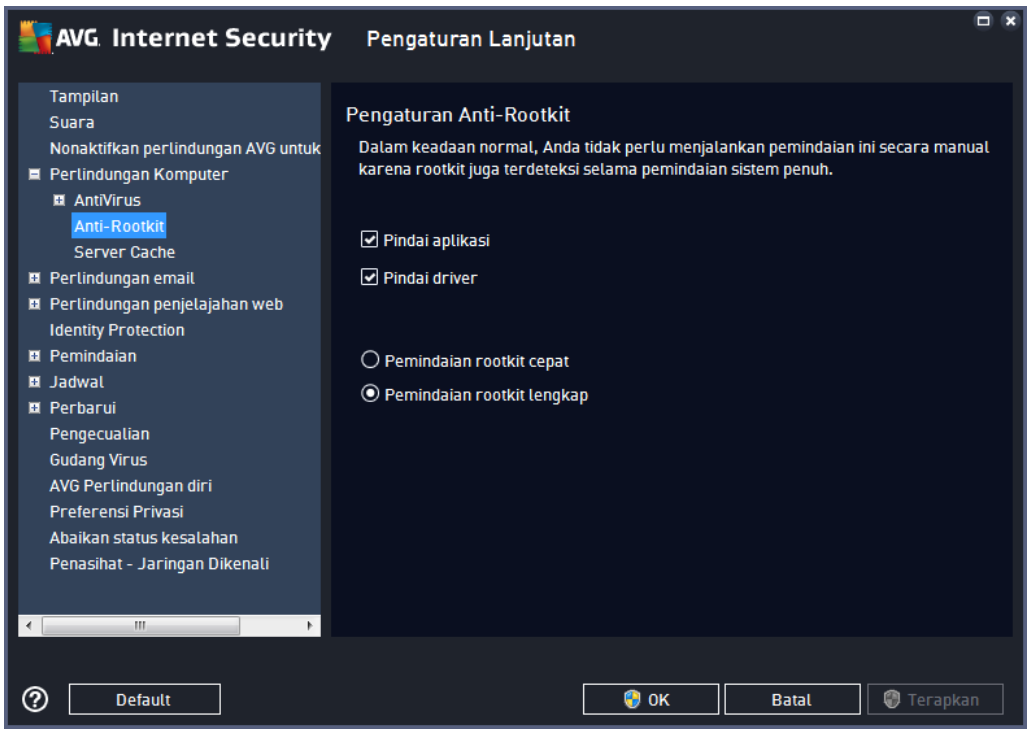
Dalam dialog ***File Dipindai oleh Resident Shield*** Anda dapat mengkonfigurasi file yang akan dipindai (*menurut ekstensi tertentu*):



Tandai kotak yang bersangkutan untuk memutuskan apakah Anda ingin ***Pindai semua file*** atau ***Pindai file yang dapat terinfeksi dan tipe dokumen yang dipilih*** saja. Untuk mempercepat pemindaian dan memberikan tingkat perlindungan secara maksimum pada saat bersamaan, kami menyarankan Anda untuk menggunakan pengaturan default. Dengan cara ini, hanya file yang terinfeksilah yang akan dipindai. Pada bagian dialog yang bersangkutan, Anda juga dapat menemukan daftar ekstensi yang dapat diedit yang menentukan file-file yang dimasukkan pada pemindaian.

Tandai ***Selalu pindai file tanpa ekstensi*** (*secara default*) untuk memastikan bahwa bahkan file tanpa ekstensi dan format yang tidak dikenal akan dipindai oleh Resident Shield. Kami sarankan untuk tetap mengaktifkan fitur ini, karena file tanpa ekstensi dianggap mencurigakan.

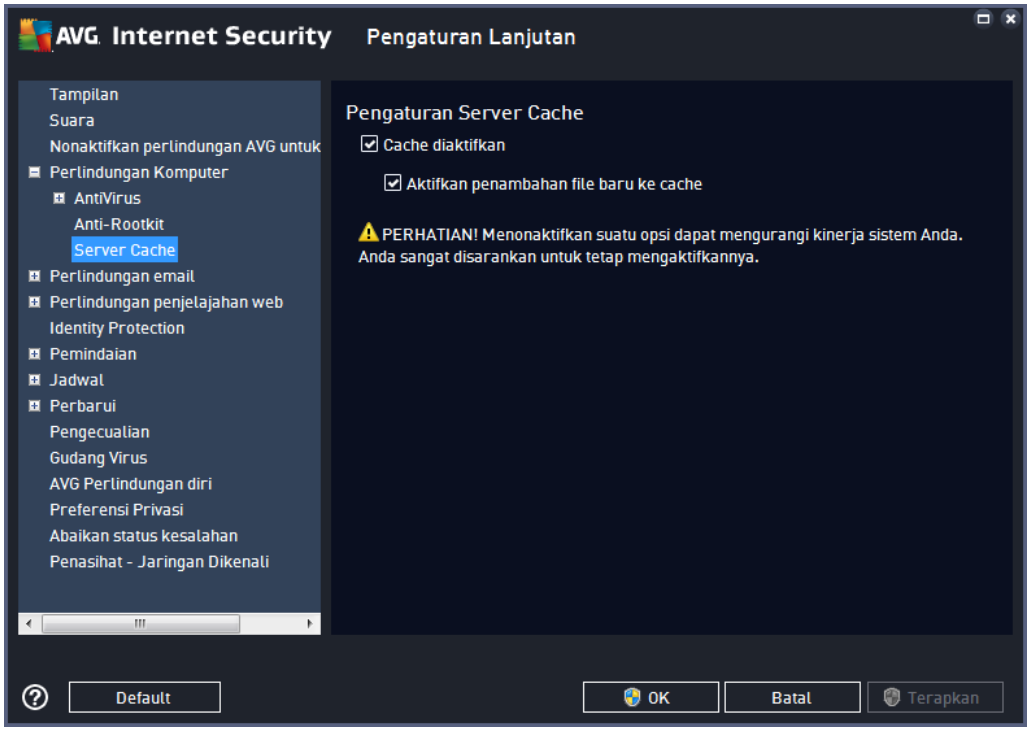
Dalam dialog ***Pengaturan Anti-Rootkit*** Anda dapat mengedit parameter khusus dan konfigurasi layanan ***Anti-Rootkit*** pada pemindaian anti-rootkit. Pemindaian anti-rootkit adalah proses default yang telah disertakan dalam Pemindaian Seisi Komputer:



Pindai aplikasi dan ***Pindai driver*** memungkinkan Anda menetapkan secara terperinci apa yang harus disertakan dalam pemindaian anti-rootkit. Pengaturan ini ditujukan untuk pengguna mahir; kami sarankan untuk tetap mengaktifkan semua opsi. Anda juga dapat memilih mode pemindaian rootkit:

- ***Pemindaian rootkit cepat*** – memindai semua proses yang berjalan, driver yang dimuat dan folder sistem (*biasanya c:\Windows*)
- ***Pemindaian rootkit lengkap*** – memindai semua proses yang berjalan, driver yang dimuat, folder sistem (*biasanya c:\Windows*), ditambah semua disk lokal (*termasuk flash-disk, namun tidak termasuk floppy-disk/drive CD*)

Dialog ***Pengaturan Server Cache*** merujuk pada proses server cache yang dirancang untuk mempercepat semua tipe pemindaian **AVG Internet Security 2015**:



Server cache ini mengumpulkan dan menyimpan informasi file terpercaya (*file dianggap terpercaya jika ditandai dengan tanda tangan digital dari sumber terpercaya*). File ini kemudian secara otomatis dianggap aman, dan tidak perlu dipindai kembali; karena itu file ini akan dilompati selama pemindaian.

Dialog ***Pengaturan Server Cache*** menawarkan opsi konfigurasi berikut:

- ***Cache diaktifkan*** (*diaktifkan secara default*) – kosongkan kotaknya untuk menonaktifkan ***Server Cache*** dan mengosongkan memori cache. Perhatikan, pemindaian mungkin melambat, dan kinerja komputer Anda secara keseluruhan akan menurun, karena setiap file yang sedang digunakan akan dipindai untuk mencari virus dan spyware terlebih dahulu.

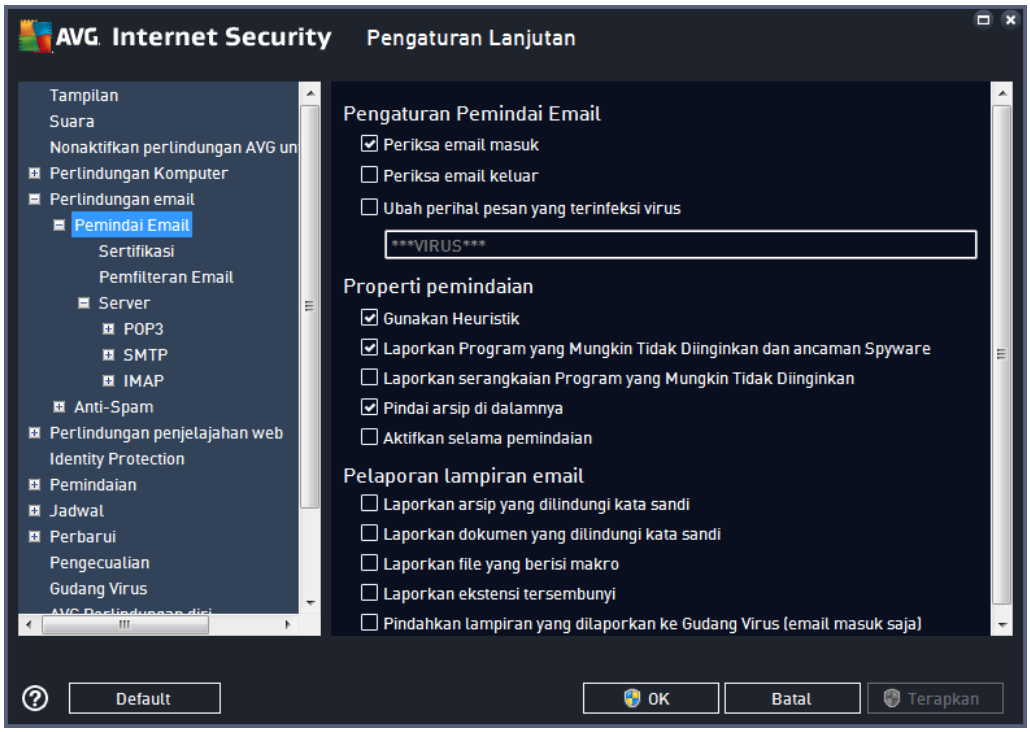
- ***Aktifkan penambahan file baru ke cache*** (*diaktifkan secara default*) – hapus centang pada kotak untuk menghentikan penambahan file lainnya ke memori cache. File yang sudah ditambahkan ke cache akan disimpan dan digunakan hingga aktivitas cache dinonaktifkan sama sekali, atau hingga pembaruan basis data virus berikutnya.

Kecuali jika Anda mempunyai alasan kuat untuk menonaktifkan server cache, kami sangat menyarankan agar Anda membiarkan pengaturan default dan tetap mengaktifkan kedua opsi! Jika tidak, Anda mungkin mengalami penurunan yang signifikan pada kecepatan sistem dan kinerja.

3.7.5. Pemindai Email

Di bagian ini, Anda dapat mengedit konfigurasi terperinci dari Email Scanner dan Anti-Spam:

Dialog ***Pemindai Email*** dibagi menjadi tiga bagian:



Pemindaian email

Di bagian ini, Anda dapat menetapkan pengaturan dasar ini untuk pesan email masuk dan/atau keluar:

- ***Periksa email masuk*** (*diaktifkan secara default*) – tandai untuk mengaktifkan/ menonaktifkan opsi pemindaian semua pesan email yang dikirim ke klien email Anda
- ***Periksa email keluar*** (*dinonaktifkan secara default*) – tandai untuk mengaktifkan/ menonaktifkan opsi pemindaian semua pesan email yang dikirim dari akun Anda
- ***Ubah perihal pesan yang terinfeksi virus*** (*dinonaktifkan secara default*) – jika Anda ingin diberi peringatan bahwa pesan email yang dipindai terdeteksi sebagai terinfeksi, tandai item ini dan isi teks yang diinginkan ke dalam kolom teks. Teks ini kemudian ditambahkan ke bidang "Perihal" untuk setiap pesan email terinfeksi untuk lebih memudahkan identifikasi dan pemfilteran. Nilai defaultnya adalah ***VIRUS*** yang kami sarankan untuk tetap digunakan.

Properti pemindaian

Di bagian ini, Anda dapat menetapkan bagaimana pesan email akan dipindai:

- ***Gunakan Heuristik*** (*diaktifkan secara default*) – tandai untuk menggunakan metode deteksi heuristik saat memindai pesan email. Bila opsi ini aktif, Anda dapat memfilter lampiran email tidak hanya berdasarkan ekstensinya tetapi juga isi sebenarnya dari lampiran tersebut akan dipertimbangkan. Pemfilteran dapat diatur dalam dialog Pemfilteran Email.
- ***Laporkan Program yang Mungkin Tidak Diinginkan dan ancaman Spyware*** (*diaktifkan secara default*) – centang untuk mengaktifkan pemindaian spyware serta virus. Spyware merupakan kategori

malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang terinstal secara tidak disengaja. Kami sarankan untuk tetap mengaktifkan fitur ini karena akan meningkatkan keamanan komputer Anda.

- ***Laporkan serangkaian Program yang Mungkin Tidak Diinginkan*** (*dinonaktifkan secara default*) – tandai untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, tetapi dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, walaupun hal ini dapat memblokir program yang legal, dan karenanya dinonaktifkan secara default.

- ***Pindai arsip di dalamnya*** (*diaktifkan secara default*) – tandai untuk memindai isi arsip yang terlampir ke pesan email.

- ***Aktifkan selama pemindaian*** (*dinonaktifkan secara default*) – dalam kondisi khusus (*misalnya jika dicurigai bahwa komputer Anda terinfeksi virus atau serangan*) Anda dapat mencentang opsi ini untuk mengaktifkan algoritma pemindaian paling menyeluruh yang akan memindai bahkan area yang paling sulit terinfeksi di komputer Anda, agar benar-benar merasa yakin. Tetapi harap diingat bahwa metode ini memakan waktu lama.

Pelaporan lampiran email

Di bagian ini, Anda dapat mengatur laporan tambahan tentang file yang mungkin membahayakan atau mencurigakan. Perhatikan bahwa tidak ada dialog peringatan yang ditampilkan, hanya teks sertifikasi yang akan ditambahkan di akhir pesan email, dan semua laporan tersebut akan terdaftar dalam dialog deteksi Perlindungan Email:

- ***Laporkan arsip yang dilindungi kata sandi*** – arsip (*ZIP, RAR, dll.*) yang dilindungi kata sandi tidak dapat dipindai dari virus; centang kotak ini untuk melaporkannya sebagai berpotensi berbahaya.

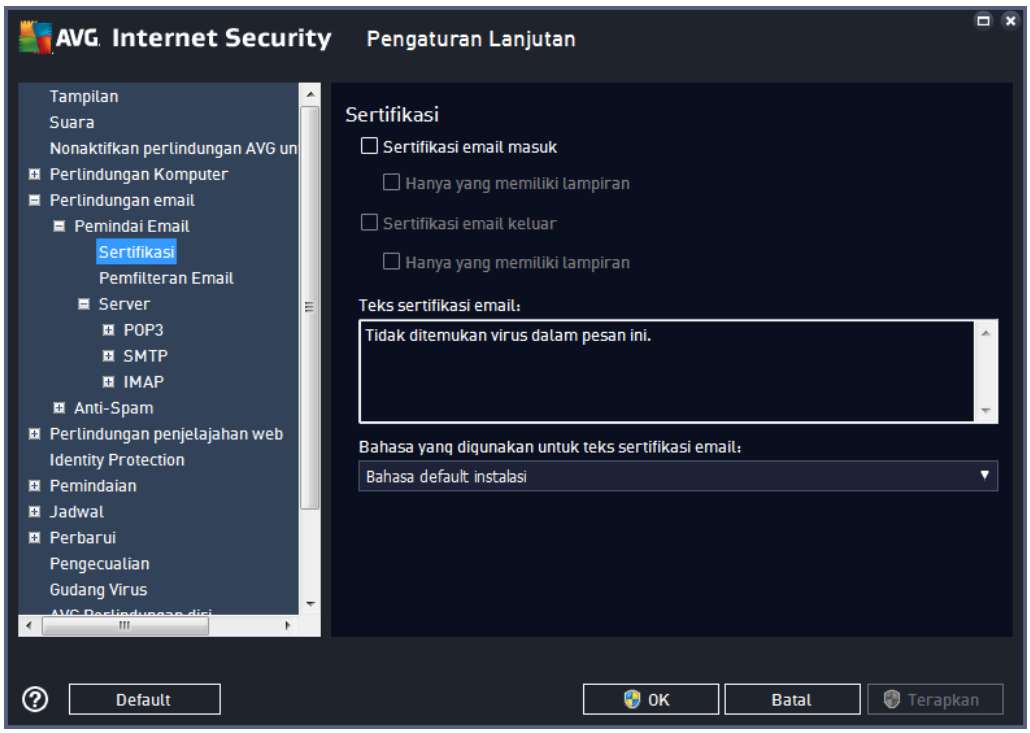
- ***Laporkan dokumen yang dilindungi kata sandi*** – dokumen yang dilindungi kata sandi tidak dapat dipindai dari virus; centang kotak ini untuk melaporkannya sebagai berpotensi berbahaya.

- ***Laporkan file yang berisi makro*** – makro merupakan urutan langkah yang telah ditetapkan untuk mempermudah tugas pengguna (*makro MS Word sudah dikenal luas*). Oleh karena itu, makro dapat berisi petunjuk yang mungkin berbahaya, dan Anda mungkin ingin menandai kotak ini untuk memastikan file dengan makro akan dilaporkan sebagai mencurigakan.

- ***Laporkan ekstensi tersembunyi*** – ekstensi tersembunyi dapat membuat, misalnya file dapat dijalankan yang mencurigakan "sesuatu.txt.exe", tampak sebagai file teks biasa yang tidak berbahaya "sesuatu.txt"; tandai kotak ini untuk melaporkannya sebagai berpotensi membahayakan.

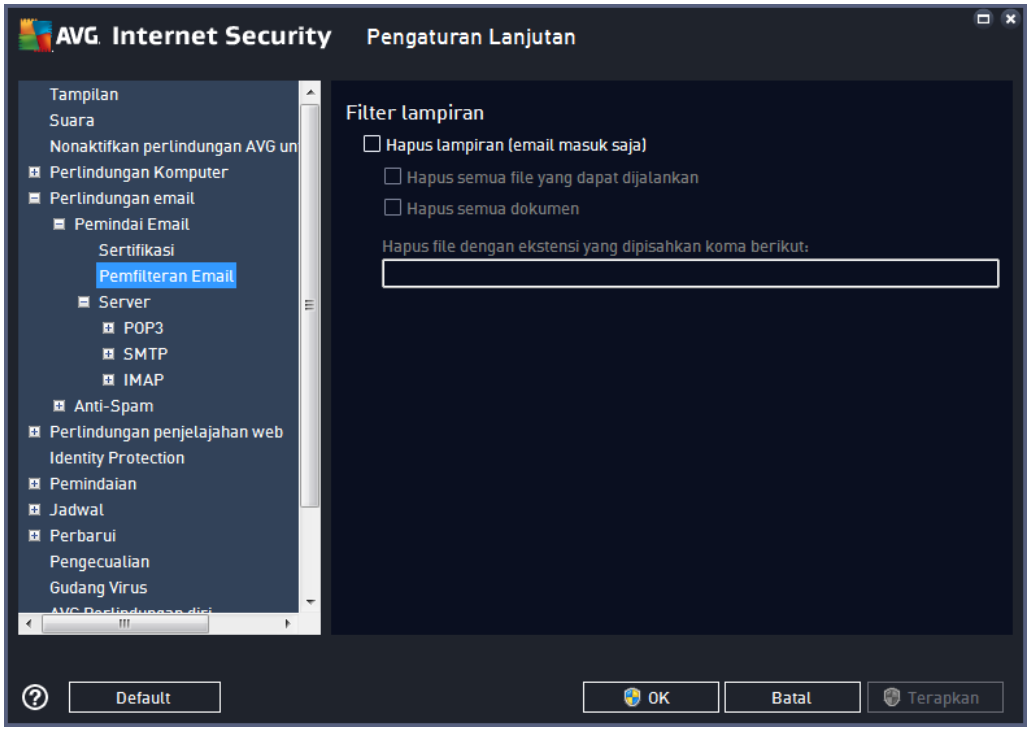
- ***Pindahkan lampiran yang dilaporkan ke Gudang Virus*** – tentukan apakah Anda ingin diberi tahu melalui email tentang arsip yang dilindungi sandi, dokumen yang dilindungi sandi, file berisi makro dan/ atau file dengan ekstensi tersembunyi yang terdeteksi sebagai lampiran pada pesan email yang dipindai. Jika pesan-pesan demikian teridentifikasi selama pemindaian, tetapkan apakah objek terinfeksi yang terdeteksi harus dipindah ke Gudang Virus.

Dalam dialog ***Sertifikasi*** Anda dapat menandai kotak tertentu untuk memutuskan apakah Anda ingin mengizinkan email masuk (***Sertifikasi email masuk***) dan/atau email keluar (***Sertifikasi email keluar***). Untuk setiap opsi ini Anda dapat menetapkan lebih jauh parameter ***Hanya yang memiliki lampiran*** sehingga sertifikasi hanya ditambahkan pada pesan email yang berisi lampiran:



Secara default, teks sertifikasi terdiri dari informasi dasar yang berbunyi *Tidak ditemukan virus dalam pesan ini.* Walau demikian, informasi ini dapat ditambah atau diubah menurut kebutuhan Anda: tuliskan teks sertifikasi yang diinginkan ke dalam bidang ***Teks sertifikasi email***. Di bagian ***Bahasa yang digunakan untuk teks sertifikasi email*** Anda dapat menentukan lebih jauh dalam bahasa apa bagian sertifikasi yang dibuat secara otomatis tersebut (*Tidak ditemukan virus dalam pesan ini*) harus ditampilkan.

Catatan: *Harap diingat bahwa teks default hanya akan ditampilkan dalam bahasa yang diminta, dan teks yang telah Anda sesuaikan tidak akan diterjemahkan secara otomatis!*



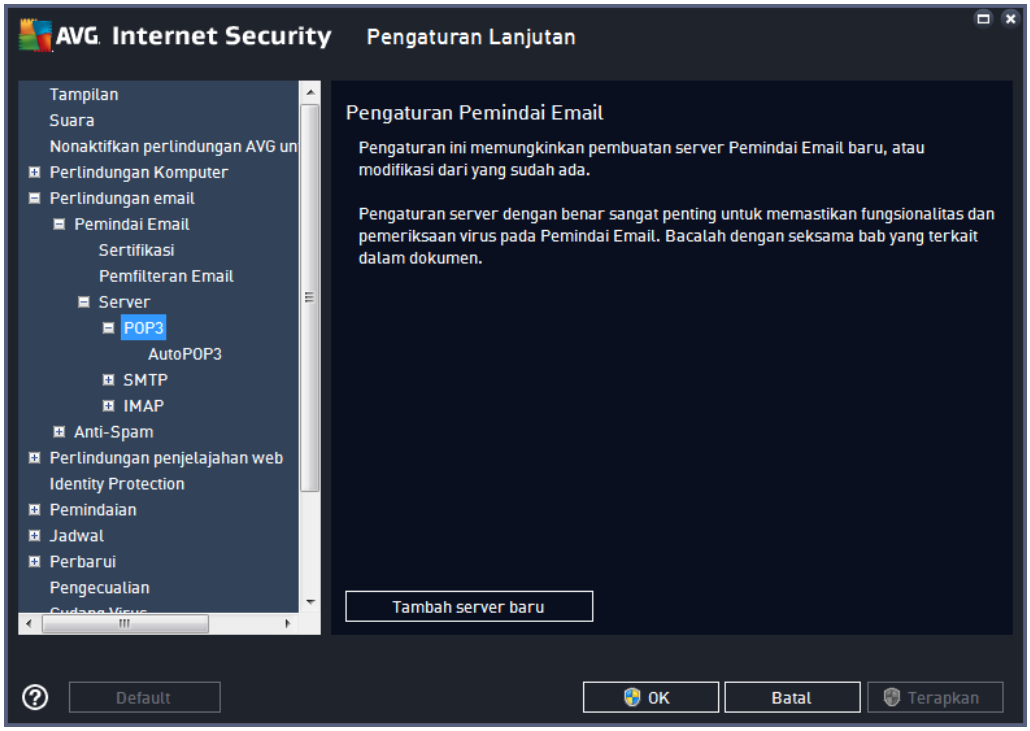
Dialog ***Filter lampiran*** memungkinkan Anda mengatur parameter untuk pemindaian lampiran pesan email. Secara default, opsi ***Hapus lampiran*** dinonaktifkan. Jika Anda memutuskan untuk mengaktifkannya, semua pesan email yang terdeteksi sebagai terinfeksi atau mungkin berbahaya akan dihapus secara otomatis. Jika Anda ingin menetapkan tipe lampiran tertentu yang harus dihapus, pilih opsi yang terkait:

- ***Hapus semua file yang dapat dijalankan*** – semua file *.exe akan dihapus
- ***Hapus semua dokumen*** – semua file *.doc, *.docx, *.xls, *.xlsx akan dihapus
- ***Hapus file dengan ekstensi yang dipisahkan koma ini*** – akan menghapus semua file dengan ekstensi yang ditetapkan

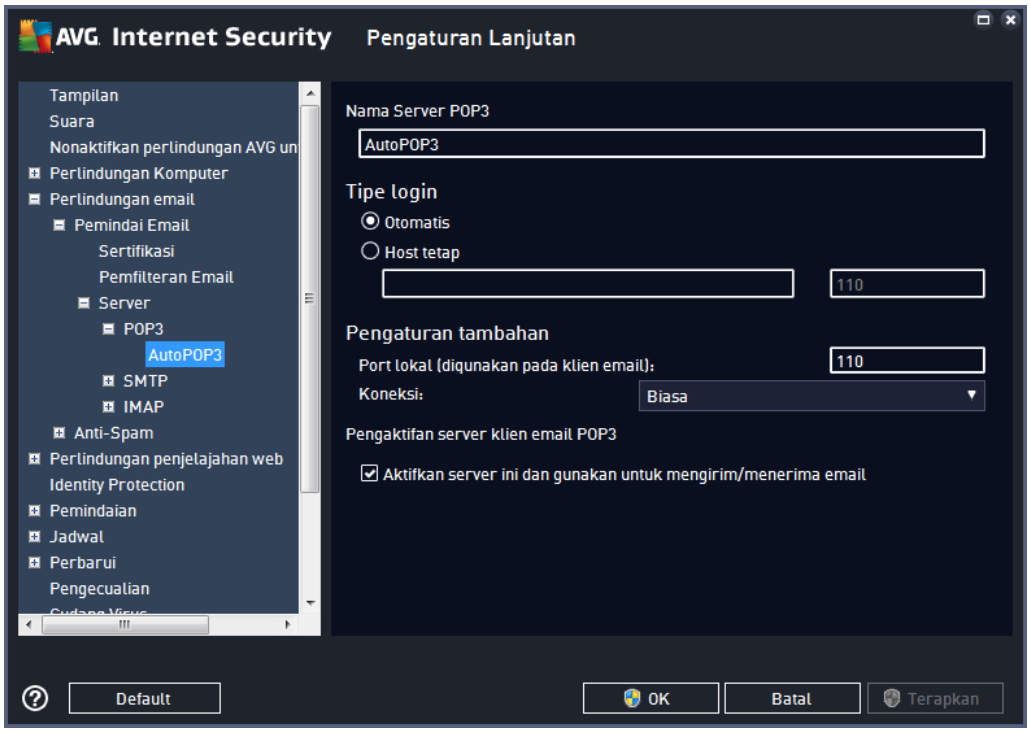
Di bagian ***Server***, Anda dapat mengedit parameter server Pemindai Email:

- Server POP3
- Server SMTP
- Server IMAP

Anda dapat menetapkan server baru untuk email masuk atau keluar, dengan tombol ***Tambah server baru***.



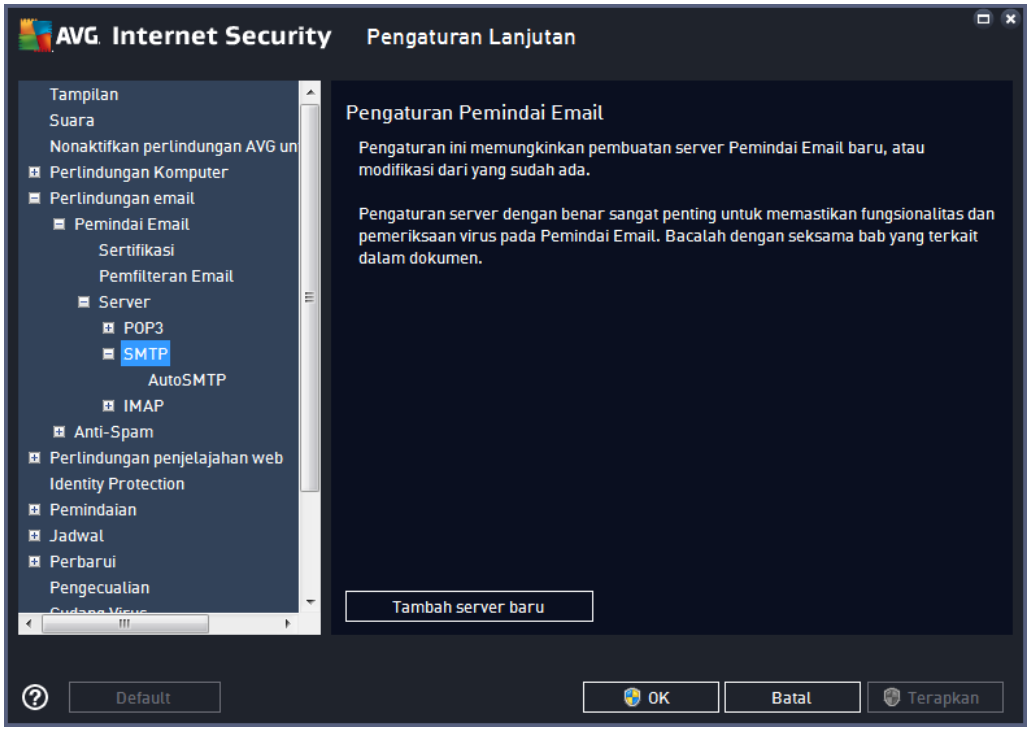
Dalam dialog ini, Anda dapat mengatur server Pemindai Email baru dengan menggunakan protokol POP3 untuk email masuk:



- ***Nama Server POP3*** – di bidang ini Anda dapat menentukan nama server yang baru ditambahkan (*untuk*

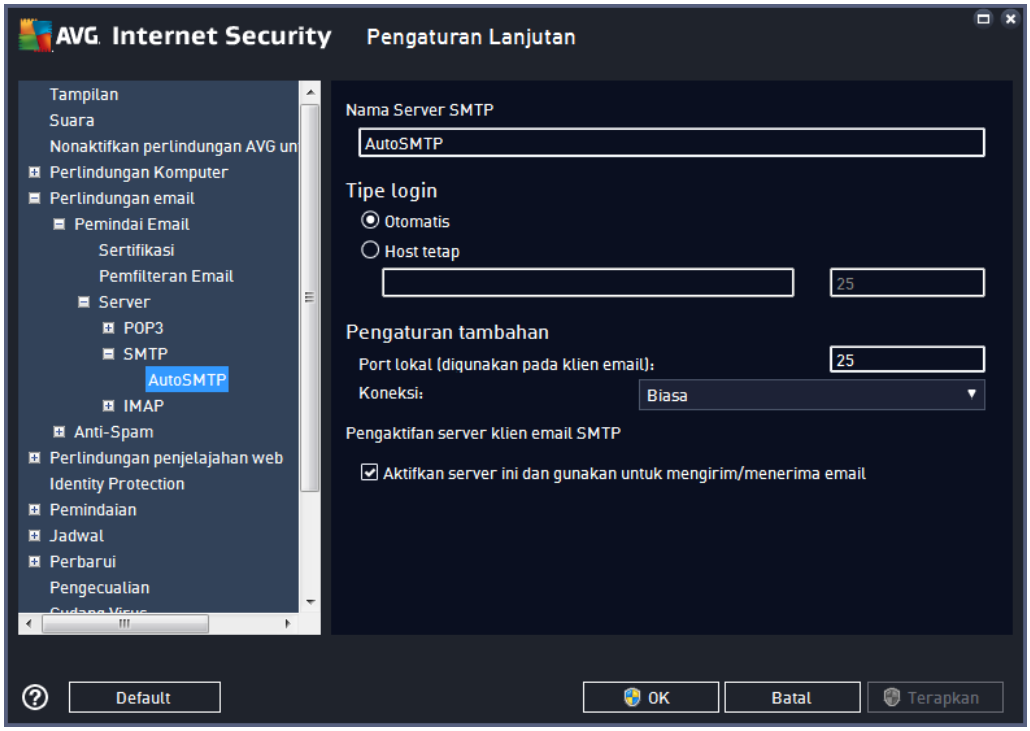
menambahkan server POP3, klik tombol kanan mouse di atas pilihan POP3 pada menu navigasi kiri).

- ***Tipe Login*** – menetapkan metode untuk menentukan server email yang digunakan untuk email masuk:
  - ***Otomatis*** – login akan dilakukan secara otomatis, sesuai pengaturan klien email Anda.
  - ***Host tetap*** – dalam kasus ini, program akan selalu menggunakan server yang ditentukan di sini. Tentukan alamat atau nama server email Anda. Nama login tetap tidak berubah. Untuk nama, Anda dapat menggunakan nama domain (*misalnya, pop.acme.com*) serta alamat IP (*misalnya, 123.45.67.89*). Jika server email menggunakan port non-standar, Anda dapat menentukan port ini setelah nama server dengan menggunakan titik dua sebagai pemisah (*misalnya, pop.acme.com:8200*). Port standar untuk komunikasi POP3 adalah 110.
- ***Pengaturan Tambahan*** – menetapkan parameter yang lebih terperinci:
  - ***Port lokal*** – menentukan port yang akan dicari oleh aplikasi email Anda untuk berkomunikasi. Anda kemudian harus menentukan port ini sebagai port untuk komunikasi POP3 dalam aplikasi email Anda.
  - ***Koneksi*** – dalam menu buka-bawah ini, Anda dapat menentukan jenis koneksi yang akan digunakan (*biasa/ SSL/ SSL default*). Jika Anda memilih koneksi SSL, data yang dikirim akan dienkripsi tanpa risiko dapat dilacak atau dipantau oleh pihak ketiga. Fitur ini juga hanya tersedia bila server email tujuan mendukungnya.
- ***Aktivasi Server POP3 Clien Email*** – tandai/ hapus tanda item ini untuk mengaktifkan atau menonaktifkan server POP3 yang ditentukan



Dalam dialog ini, Anda dapat mengatur server Pemindai Email baru dengan menggunakan protokol SMTP untuk

email keluar:



- ***Nama Server SMTP*** – pada bidang ini, Anda dapat menentukan nama server yang baru ditambahkan (*untuk menambahkan server SMTP, klik tombol kanan mouse di atas pilihan SMTP pada menu navigasi kiri*). Untuk membuat server "AutoSMTP" secara otomatis, bidang ini dinonaktifkan.

- ***Tipe Login*** – menetapkan metode untuk menentukan server email yang digunakan bagi email keluar:

  - ***Otomatis*** – login akan dilakukan secara otomatis, sesuai pengaturan klien email Anda

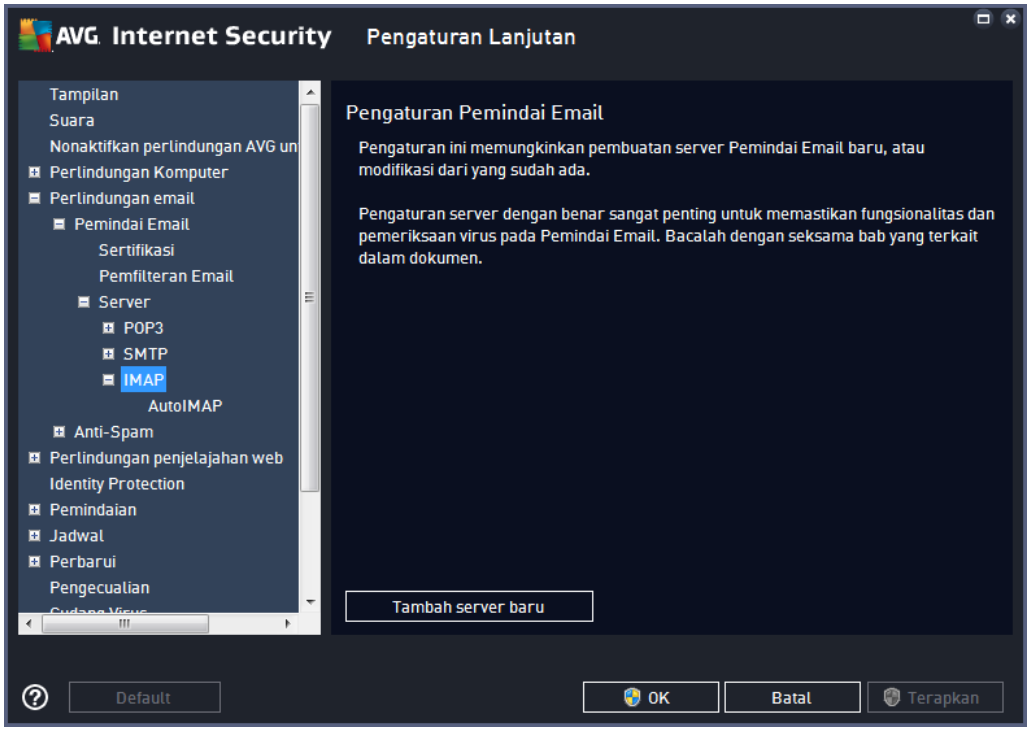
  - ***Host tetap*** – Dalam kasus ini, program akan selalu menggunakan server yang ditentukan di sini. Tentukan alamat atau nama server email Anda. Anda dapat menggunakan nama domain (*misalnya, smtp.acme.com*) ataupun alamat IP (*misalnya, 123.45.67.89*) untuk nama server. Jika server Email menggunakan port non-standar, Anda dapat menetapkan port ini setelah nama server dengan menggunakan titik dua sebagai pemisah (*misalnya, smtp.acme.com:8200*). Port standar untuk komunikasi SMTP adalah 25.

- ***Pengaturan Tambahan*** – menetapkan parameter yang lebih terperinci:

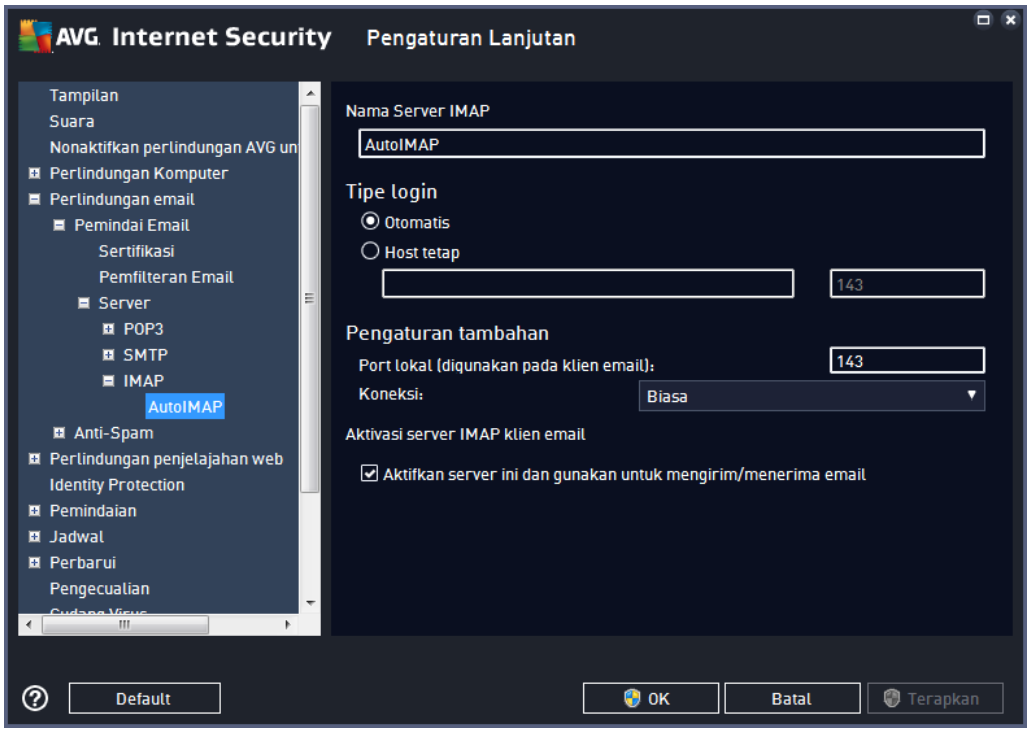
  - ***Port lokal*** – menentukan port yang akan dicari oleh aplikasi email Anda untuk berkomunikasi. Anda kemudian harus menentukan port ini sebagai port untuk komunikasi SMTP dalam aplikasi email Anda.

  - ***Koneksi*** – dalam menu buka-bawah ini, Anda dapat menentukan jenis koneksi yang akan digunakan (*biasa/ SSL/ SSL default*). Jika Anda memilih koneksi SSL, data yang dikirim akan dienkripsi tanpa risiko dapat dilacak atau dipantau oleh pihak ketiga. Fitur ini hanya tersedia bila server email tujuan mendukungnya.

- ***Aktivasi server SMTP klien email*** – centang/ hapus centang kotak ini untuk mengaktifkan/ menonaktifkan server SMTP yang ditentukan di atas



Dalam dialog ini, Anda dapat mengatur server Pemindai Email baru dengan menggunakan protokol IMAP untuk email keluar:



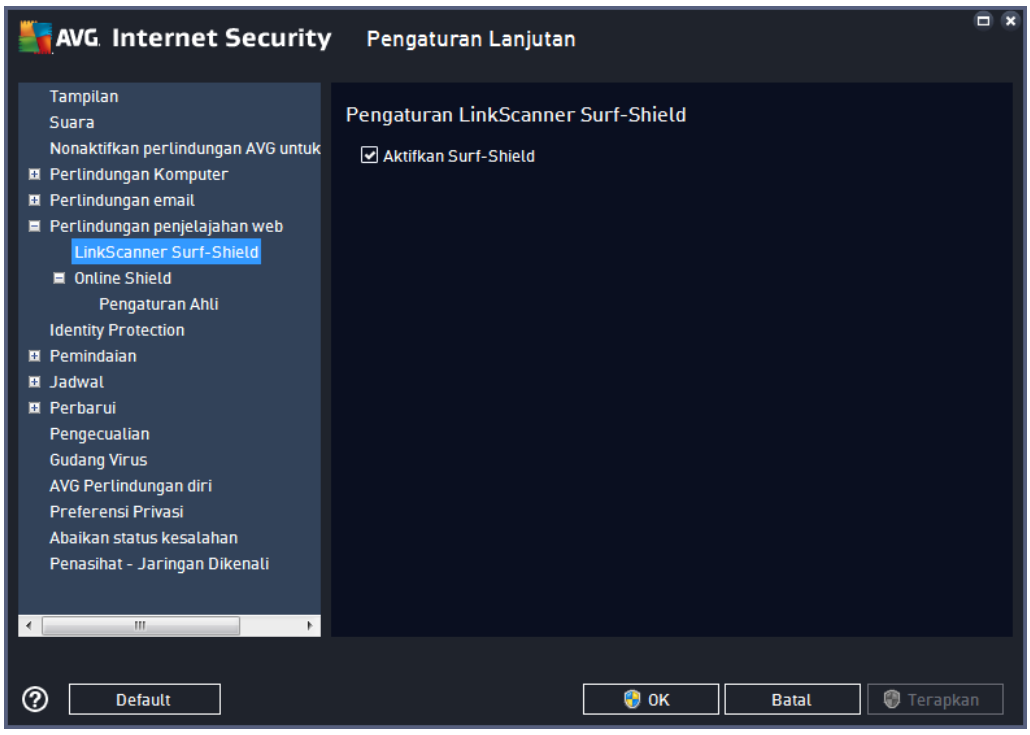
- ***Nama Server IMAP*** – di bidang ini Anda dapat menentukan nama server yang baru ditambahkan (*untuk*

menambah server IMAP, klik tombol kanan mouse di atas item IMAP pada menu navigasi kiri).

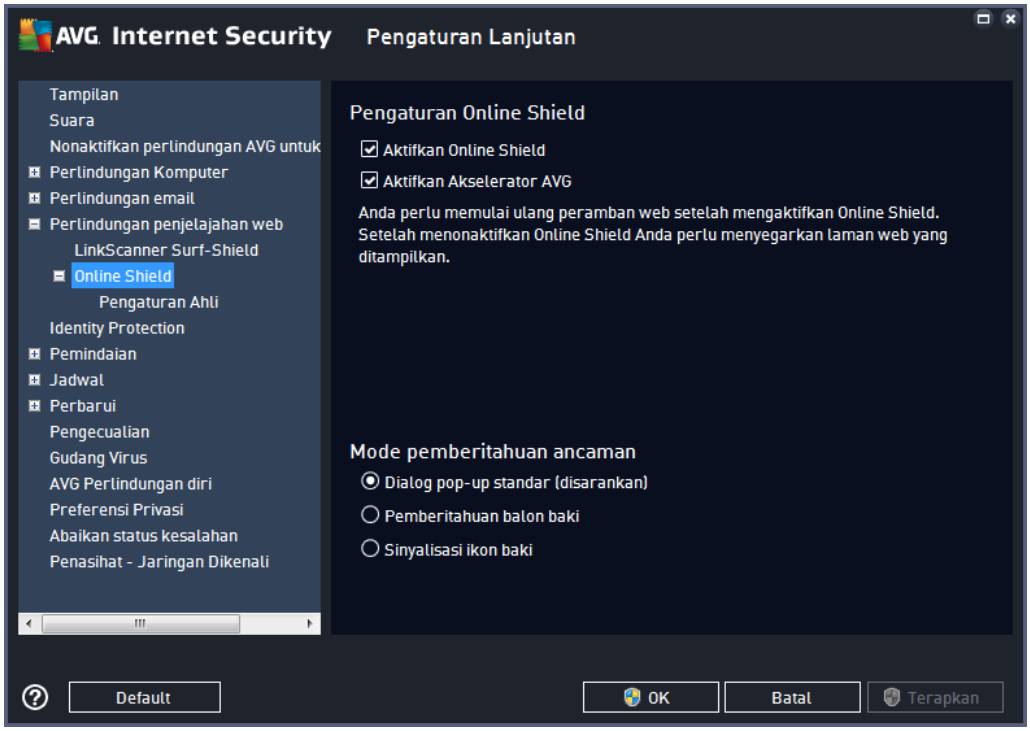
- ***Tipe Login*** – menetapkan metode untuk menentukan server email yang digunakan bagi email keluar:
  - ***Otomatis*** – login akan dilakukan secara otomatis, sesuai pengaturan klien email Anda
  - ***Host tetap*** – Dalam kasus ini, program akan selalu menggunakan server yang ditentukan di sini. Tentukan alamat atau nama server email Anda. Anda dapat menggunakan nama domain (*misalnya, smtp.acme.com*) ataupun alamat IP (*misalnya, 123.45.67.89*) untuk nama server. Jika server Email menggunakan port non-standar, Anda dapat menetapkan port ini setelah nama server dengan menggunakan titik dua sebagai pemisah (*misalnya, imap.acme.com:8200*). Port standar untuk komunikasi IMAP adalah 143.
- ***Pengaturan Tambahan*** – menetapkan parameter yang lebih terperinci:
  - ***Port lokal yang digunakan*** – menentukan port yang akan dicari oleh aplikasi email Anda untuk berkomunikasi. Anda kemudian harus menentukan port ini sebagai port untuk komunikasi IMAP dalam aplikasi email Anda.
  - ***Koneksi*** – dalam menu buka-bawah ini, Anda dapat menentukan jenis koneksi yang akan digunakan (*biasa/ SSL/ SSL default*). Jika Anda memilih koneksi SSL, data yang dikirim akan dienkripsi tanpa risiko dapat dilacak atau dipantau oleh pihak ketiga. Fitur ini hanya tersedia bila server email tujuan mendukungnya.
- ***Aktivasi Server IMAP klien email*** – centang/ hapus centang kotak ini untuk mengaktifkan/ menonaktifkan server IMAP yang ditetapkan di atas.

3.7.6. Perlindungan Penjelajahan Web

Dialog ***Pengaturan LinkScanner*** memungkinkan Anda untuk memilih/ tidak memilih fitur-fitur berikut:



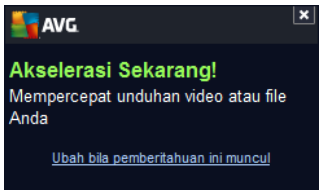
- ***Aktifkan Surf-Shield*** – (*diaktifkan secara default*): perlindungan aktif (*waktu nyata*) terhadap situs-situs yang bersifat eksploitatif selama situs tersebut diakses. Koneksi situs jahat yang telah dikenal dan konten eksploitatif diblokir begitu diakses oleh pengguna melalui browser web (*atau aplikasi lain yang menggunakan HTTP*).



Dialog ***Online Shield*** menyediakan opsi berikut:

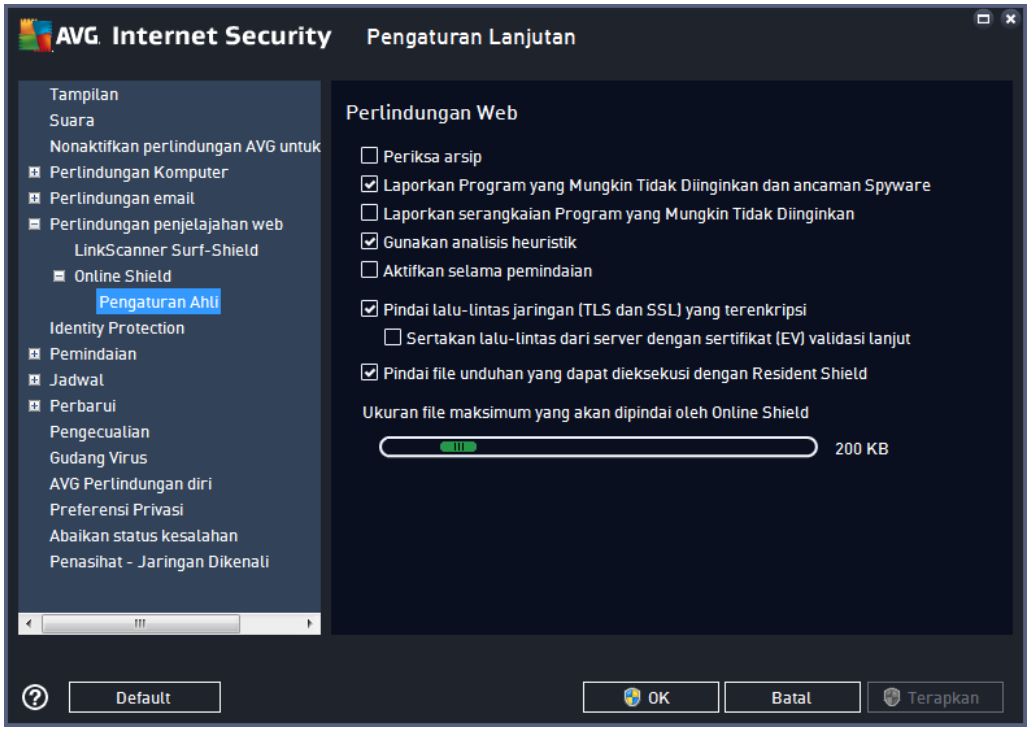
- ***Aktifkan Online Shield*** *(diaktifkan secara default)* – Mengaktifkan/menonaktifkan seluruh layanan ***Online Shield***. Untuk pengaturan lanjutan selebihnya pada ***Online Shield*** harap lanjutkan ke dialog berikutnya bernama Perlindungan Web.

- ***Aktifkan Akselerator AVG*** *(diaktifkan, secara default)* – Aktifkan/nonaktifkan layanan Akselerator AVG. AVG Accelerator memungkinkan pemutaran video online lebih lancar dan membuat pengunduhan tambahan lebih mudah. Bila proses akselerasi video sedang berlangsung, Anda akan diberi tahu melalui jendela yang muncul di baki sistem:



Mode pemberitahuan ancaman

Di bagian bawah dialog, pilih dengan metode apa Anda ingin diberitahu tentang potensi ancaman yang terdeteksi: lewat dialog pop-up standar, lewat pemberitahuan balon baki, atau lewat info ikon baki.



Dalam dialog ***Perlindungan Web***, Anda dapat mengedit konfigurasi komponen yang menyangkut pemindaian konten situs Web. Antarmuka pengeditan memungkinkan Anda untuk mengkonfigurasi beberapa opsi dasar berikut:

- ***Periksa arsip*** – (*dinonaktifkan secara default*): memindai isi arsip yang mungkin telah dimasukkan di halaman www yang akan ditampilkan.
- ***Laporkan Program yang Mungkin Tidak Diinginkan dan ancaman Spyware*** – (*diaktifkan secara default*): centang untuk mengaktifkan pemindaian untuk spyware serta virus. Spyware merupakan kategori malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang terinstal secara tidak disengaja. Kami sarankan untuk tetap mengaktifkan fitur ini karena akan meningkatkan keamanan komputer Anda.
- ***Laporkan serangkaian Program yang Mungkin Tidak Diinginkan*** – (*dinonaktifkan secara default*): tandai untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, tetapi dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, walaupun hal ini dapat memblokir program yang legal, dan karenanya dinonaktifkan secara default.
- ***Gunakan heuristik*** – (*diaktifkan secara default*): memindai isi halaman yang akan ditampilkan, menggunakan metode analisis heuristik (*emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual*).
- ***Aktifkan selama pemindaian*** – (*dinonaktifkan secara default*): dalam kondisi khusus (*dicurigai bahwa komputer Anda terinfeksi*) Anda dapat mencentang opsi ini untuk mengaktifkan algoritma pemindaian paling menyeluruh yang akan memindai area yang jarang terinfeksi sekalipun, agar benar-benar merasa yakin. Tetapi harap diingat bahwa metode ini memakan waktu lama.

- ***Pindai lalu lintas jaringan (TSL dan SSL) yang dienkripsi*** – (*diaktifkan secara default*): biarkan ditandai untuk memperbolehkan AVG memindai juga semua jaringan komunikasi yang dienkripsi, yaitu koneksi terhadap protokol keamanan (SSL dan versi terbarunya, TLS). Ini berlaku untuk situs web yang menggunakan HTTPS, dan koneksi klien email yang menggunakan TLS/SSL. Lalu-lintas aman didekripsi, dipindari dari malware, dan dienkripsi lagi untuk dikirim dengan aman ke komputer Anda. Dalam opsi ini Anda dapat memutuskan untuk ***menyertakan lalu lintas dari server dengan sertifikat validasi yang diperpanjang (EV)*** dan juga memindai komunikasi jaringan yang dienkripsi dari server yang disertifikasi dengan Sertifikat Validasi yang Diperpanjang. Pengeluaran sertifikat EV membutuhkan validasi ekstensif oleh otoritas sertifikat, dan situs web yang dioperasikan di bawah sertifikat tersebut karenanya jauh lebih terpercaya *(kecil kemungkinannya menyebarkan malware)*. Untuk alasan ini, Anda dapat memutuskan untuk tidak memindai lalu-lintas dari server bersertifikasi EV, yang akan membuat komunikasi terenkripsi lebih cepat.

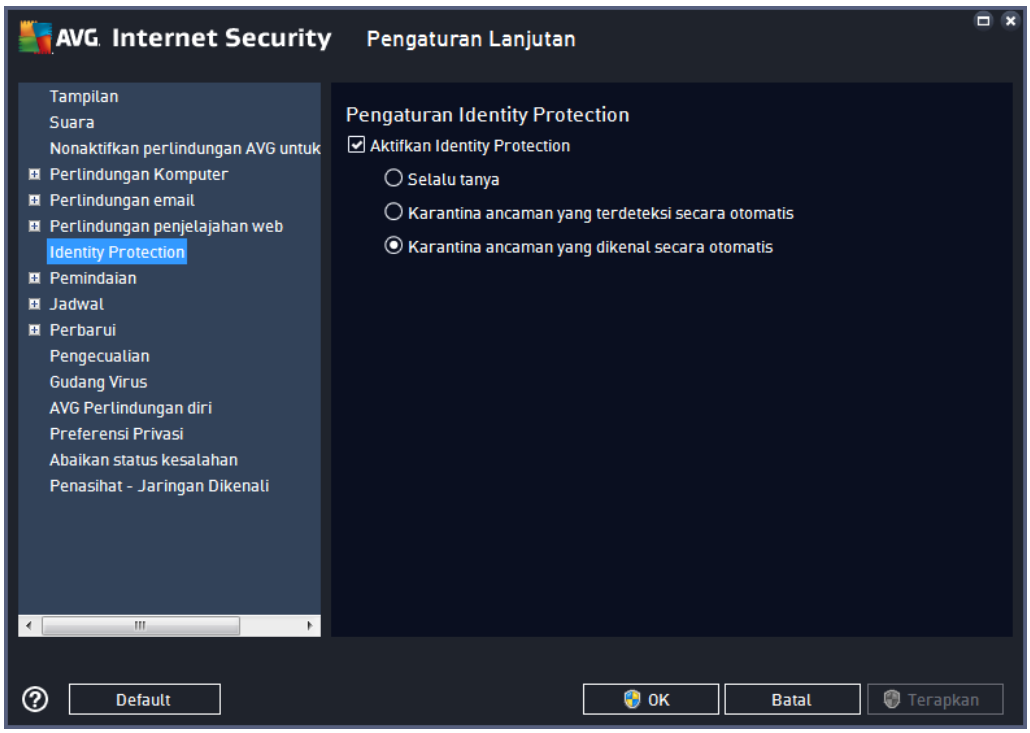
- ***Pindai file unduhan yang dapat dieksekusi dengan Resident Shield*** – (*diaktifkan secara default*): memindai file yang dapat dieksekusi *(biasanya file dengan ekstensi exe, bat, com)* setelah file diunduh. Resident Shield memindai file sebelum mengunduh untuk memastikan tidak ada kode berbahaya yang masuk ke komputer Anda. Namun, pemindaian ini dibatasi oleh ***Ukuran bagian maksimum file yang akan dipindai*** – lihat item berikutnya di dialog ini. Oleh karena itu, file besar dipindai bagian per bagian, dan ini juga berlaku untuk sebagian besar file yang dapat dieksekusi. File yang dapat dieksekusi dapat menjalankan berbagai tugas di komputer Anda, dan penting agar semuanya 100% aman. Hal ini dapat dipastikan dengan memindai file bagian per bagian sebelum diunduh, dan tepat setelah unduhan file selesai. Kami sarankan agar Anda menjaga opsi ini tetap dicentang. Jika menonaktifkan opsi ini, Anda masih yakin bahwa AVG akan menenukan potensi kode berbahaya apa pun. Hanya saja, biasanya pemindaian ini tidak akan dapat mengevaluasi file secara kompleks, jadi pemindaian ini mungkin menghasilkan laporan salah.

Bilah geser di bawah dialog memungkinkan Anda untuk menentukan ***Ukuran bagian file maksimum yang akan dipindai*** – jika file yang disertakan ada di halaman yang ditampilkan, Anda juga dapat memindai isinya bahkan sebelum diunduh ke komputer Anda. Namun, pemindaian file besar akan memakan waktu lama dan halaman Web mungkin diunduh jauh lebih pelan. Anda dapat menggunakan bilah geser untuk menetapkan ukuran maksimum file yang masih akan dipindai dengan ***Online Shield***. Bahkan jika file unduhan lebih besar dari yang ditentukan, dan oleh karenanya tidak akan dipindai dengan Online Shield, Anda masih terlindung: jika file terinfeksi, ***Resident Shield*** akan segera mendeteksinya.

3.7.7. Perlindungan Identitas

Perlindungan Identitas adalah komponen anti-malware yang melindungi Anda dari semua jenis malware (*spyware, bot, pencurian identitas, ...*) menggunakan teknologi perilaku dan memberikan perlindungan setiap hari dari virus baru *(untuk penjelasan terperinci mengenai fungsionalitas komponen, lihat bab Identitas)*.

Dialog ***Pengaturan Perlindungan Identitas*** memungkinkan Anda mengaktifkan atau menonaktifkan fitur dasar komponen Perlindungan Identitas:



Aktifkan Perlindungan Identitas (*diaktifkan secara default*) – hilangkan centang untuk menonaktifkan komponen Identitas. ***Kami sangat menyarankan agar Anda tidak melakukannya jika tidak perlu!*** Bila Perlindungan Identitas diaktifkan, Anda dapat menetapkan apa yang dilakukan bila ancaman terdeteksi:

- ***Selalu tanya*** – saat ancaman terdeteksi, Anda akan ditanyai apakah ia harus dipindahkan ke karantina untuk memastikan tidak terhapusnya aplikasi yang ingin Anda jalankan.
- ***Karantina ancaman yang terdeteksi secara otomatis*** – centang kotak ini untuk menetapkan bahwa Anda ingin semua ancaman yang mungkin terdeteksi segera dipindahkan ke ruang aman di Gudang Virus. Dengan menyimpan pengaturan default, saat ancaman terdeteksi, Anda akan ditanyai apakah ancaman harus dipindahkan ke karantina untuk memastikan tidak terhapusnya aplikasi yang ingin Anda jalankan.
- ***Karantina ancaman yang dikenal secara otomatis*** (*aktif secara default*) – biarkan item ini ditandai jika Anda ingin agar semua aplikasi yang terdeteksi sebagai kemungkinan malware untuk dipindah segera dan secara otomatis ke Gudang Virus.

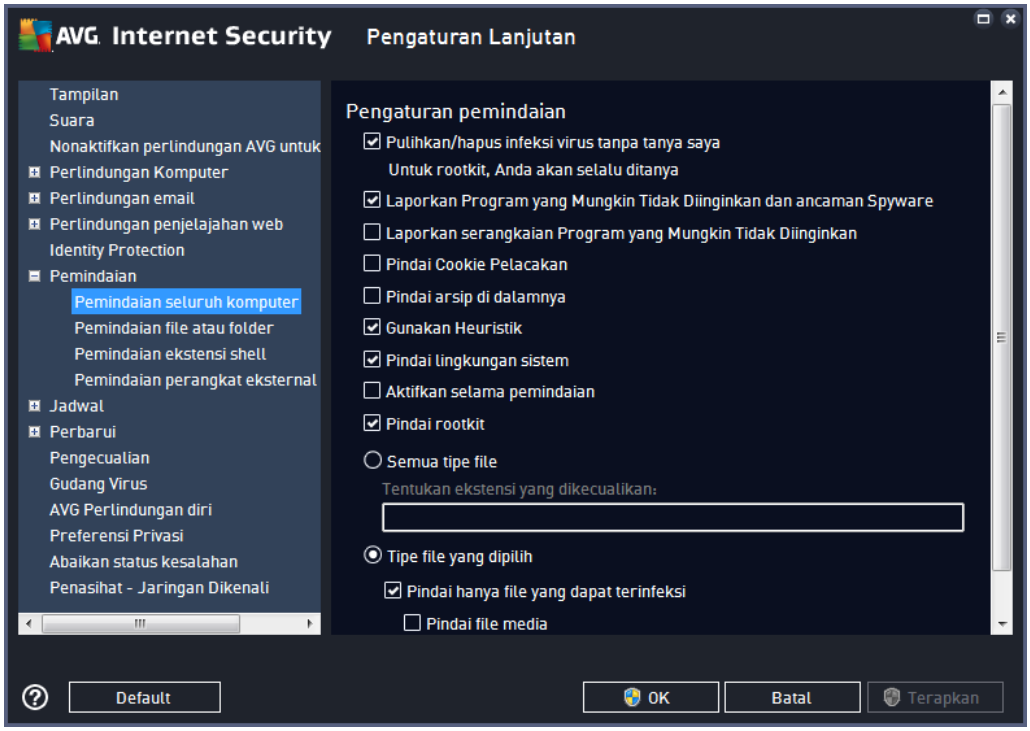
3.7.8. Pemindaian

Pengaturan pindai lanjutan terbagi ke dalam empat kategori yang merujuk pada tipe pemindaian tertentu sebagaimana ditentukan oleh vendor perangkat lunak:

- Pemindaian seluruh komputer – pemindaian standar yang ditentukan untuk seluruh komputer
- Pemindaian file atau folder tertentu – pemindaian standar yang ditentukan atas area yang dipilih pada komputer Anda
- Pemindaian ekstensi shell – pemindaian tertentu atas objek yang dipilih, langsung dari lingkungan Windows Explorer
- Pemindaian perangkat eksternal – pemindaian tertentu atas perangkat eksternal yang dipasang pada

komputer Anda

Opsi ***Pemindaian Seluruh Komputer*** memungkinkan Anda mengedit parameter salah satu pemindaian yang telah ditetapkan oleh vendor perangkat lunak, Pindai Seluruh Komputer:



Pengaturan pemindaian

Bagian ***Pengaturan pemindaian*** menyediakan daftar parameter pemindaian yang secara opsional dapat diaktifkan/ dinonaktifkan:

- ***Pulihkan/ hapus infeksi tanpa bertanya pada saya*** (*diaktifkan secara default*) – jika ada virus teridentifikasi selama pemindaian, maka dapat dipulihkan secara otomatis jika penawarnya tersedia. Jika file yang terinfeksi tidak dapat dipulihkan secara otomatis, objek yang terinfeksi akan dipindahkan ke Gudang Virus.

- ***Laporkan Program yang Mungkin Tidak Diinginkan dan ancaman Spyware*** (*diaktifkan secara default*) – centang untuk mengaktifkan pemindaian spyware serta virus. Spyware merupakan kategori malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang terinstal secara tidak disengaja. Kami sarankan untuk tetap mengaktifkan fitur ini karena akan meningkatkan keamanan komputer Anda.

- ***Laporkan serangkaian program yang mungkin tidak diinginkan*** (*dinonaktifkan secara default*) – tandai untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, tetapi dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, walaupun hal ini dapat memblokir program yang legal, dan karenanya dinonaktifkan secara default.

- ***Pindai cookie pelacakan*** (*dinonaktifkan secara default*) – parameter ni menetapkan bahwa cookie harus

dideteksi selama pemindaian; (*cookie HTTP digunakan untuk mengautentikasi, melacak, dan memelihara informasi tertentu tentang pengguna, seperti preferensi situs atau isi kereta belanja elektronik mereka*).

- ***Pindai arsip di dalamnya*** (*dinonaktifkan secara default*) – parameter ini menetapkan bahwa pemindaian harus memeriksa semua file yang tersimpan dalam arsip, misalnya, ZIP, RAR, ...
- ***Gunakan heuristik*** (*diaktifkan secara default*) – analisis heuristik (*emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual*) akan menjadi salah satu metode yang digunakan untuk deteksi virus selama pemindaian.
- ***Pindai lingkungan sistem*** (*diaktifkan secara default*) – pemindaian juga akan memeriksa area sistem komputer Anda.
- ***Aktifkan selama pemindaian*** (*dinonaktifkan secara default*) – dalam kondisi khusus (*dicurigai bahwa komputer Anda terinfeksi*) Anda dapat mencentang opsi ini untuk mengaktifkan algoritma pemindaian paling menyeluruh yang akan memindai area yang jarang terinfeksi sekalipun, agar benar-benar merasa yakin. Tetapi harap diingat bahwa metode ini memakan waktu lama.
- ***Pindai rootkit*** (*aktif secara default*) – Pemindaian Anti-Rootkit menelusuri PC Anda dari kemungkinan rootkit, yaitu program dan teknologi yang dapat menutupi aktivitas malware di komputer Anda. Jika rootkit terdeteksi, tidak berarti komputer Anda terinfeksi. Di beberapa kasus, driver atau bagian tertentu dari aplikasi biasa mungkin salah terdeteksi sebagai rootkit.

Anda juga harus memutuskan apakah Anda ingin memindai

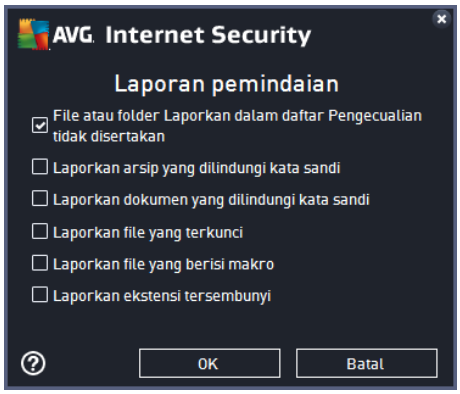
- ***Semua tipe file*** dengan opsi penentuan pengecualian dari pemindaian dengan memberikan daftar file ekstensi yang dipisah koma (*setelah disimpan, koma akan berganti menjadi titik koma*) untuk file yang tidak boleh dipindai.
- ***Tipe file yang dipilih*** – Anda dapat menentukan bahwa Anda hanya ingin memindai file yang dapat terinfeksi (*file yang tidak dapat terinfeksi tidak akan dipindai, misalnya beberapa file teks biasa, atau file yang tidak dapat dijalankan lainnya*), termasuk file media (*file video, audio – jika Anda membiarkan kotak ini tidak dicentang, maka hal ini akan lebih mengurangi waktu pemindaian, karena file ini seringkali terlalu besar dan sangat kecil kemungkinannya untuk terinfeksi virus*). Sekali lagi, Anda dapat menentukan ekstensi file yang harus selalu dipindai.
- Secara opsional, Anda dapat memutuskan apakah Anda ingin memilih opsi ***Pindai file tanpa ekstensi*** – opsi ini diaktifkan secara default, dan disarankan Anda membiarkannya kecuali Anda memiliki alasan kuat untuk mengubahnya. File tanpa ekstensi cukup mencurigakan dan harus selalu dipindai.

Sesuaikan secepat apa pemindaian selesai

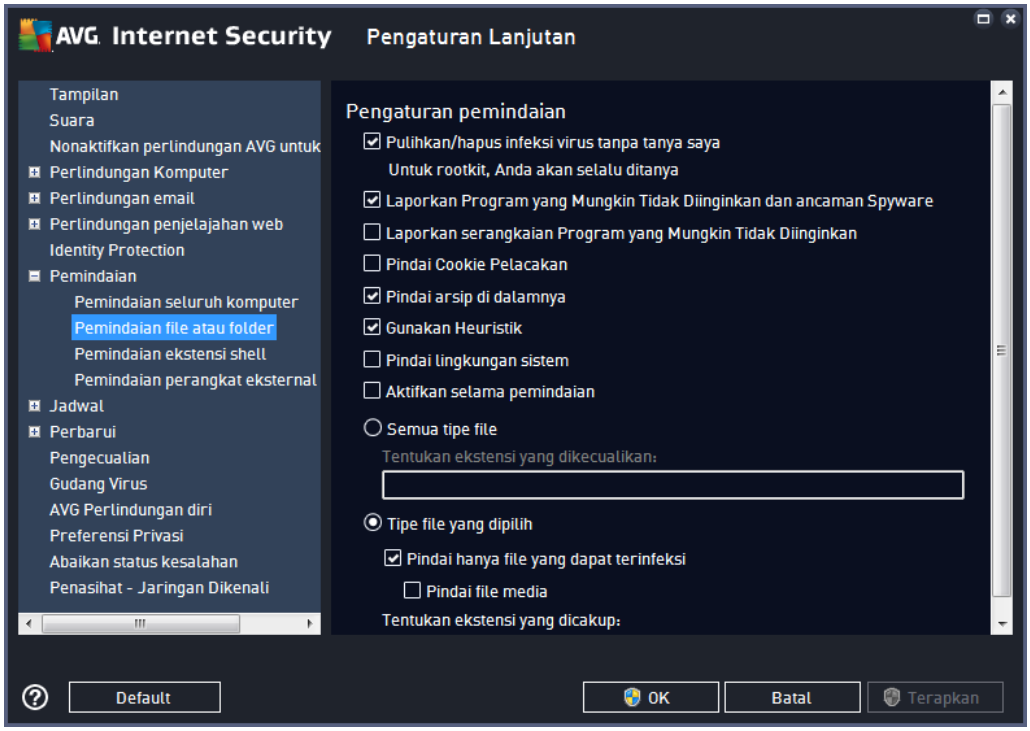
Di bagian ***Sesuaikan kecepatan melakukan pemindaian*** Anda dapat menentukan lebih jauh kecepatan pemindaian sesuai dengan penggunaan sumber daya sistem. Secara default, nilai opsi ini diatur ke tingkat penggunaan sumber daya otomatis yang *peka pengguna*. Jika Anda ingin pemindaian berjalan lebih cepat, ini akan menghemat waktu tetapi sumber daya sistem yang digunakan akan jauh meningkat selama pemindaian dan akan memperlambat aktivitas lain pada PC (*opsi ini dapat digunakan bila komputer hidup namun tidak ada orang yang saat itu menggunakannya*). Di sisi lain, Anda dapat menurunkan sumber daya sistem yang digunakan dengan memperpanjang waktu pemindaian.

Atur laporan pemindaian tambahan ...

Klik tautan ***Atur laporan pindai tambahan ...*** untuk membuka jendela dialog mandiri bernama ***Laporan pindai*** di mana Anda dapat menandai beberapa item untuk menetapkan temuan apa yang harus dilaporkan:



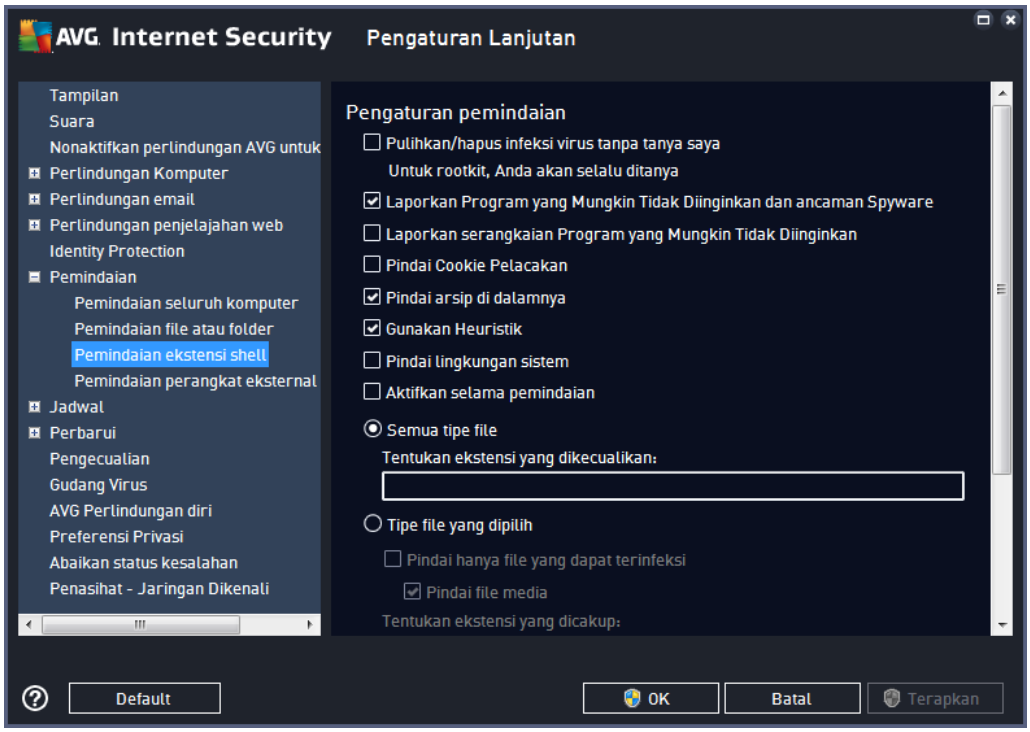
Antarmuka pengeditan untuk ***Pindai File atau Folder Tertentu*** identik dengan dialog pengeditan Pindai Seluruh Komputer. Semua opsi konfigurasinya sama; walau demikian, pengaturan default lebih ketat untuk Pindai Seluruh Komputer:



Semua parameter yang diatur dalam dialog konfigurasi ini hanya berlaku untuk area yang dipilih bagi pemindaian dengan Pindai File atau Folder Tertentu!

Catatan: *Untuk keterangan mengenai parameter tertentu, bacalah bab Pengaturan Lanjutan AVG/ Pemindaian/ Pindai Seluruh Komputer.*

Seperti pada fungsi Pindai Seluruh Komputer sebelumnya, fungsi yang dinamai ***Pemindaian Ekstensi Shell*** ini juga menawarkan beberapa opsi untuk mengedit pemindaian yang ditentukan oleh vendor perangkat lunak. Kali ini konfigurasi berhubungan dengan pemindaian objek tertentu yang diluncurkan langsung dari lingkungan Windows Explorer (*ekstensi shell*), lihat bab Pemindaian di Windows Explorer:

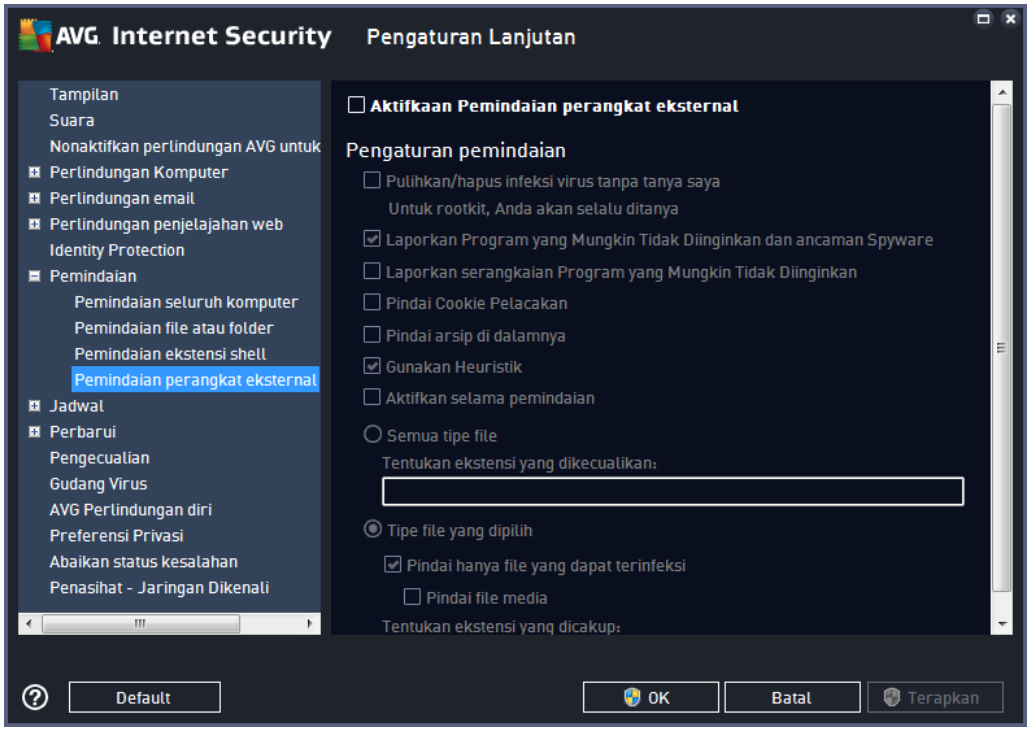


Daftar parameter identik dengan yang tersedia untuk Pindai Seluruh Komputer. Akan tetapi, pengaturan default berbeda (*misalnya, Pindai Seluruh Komputer secara default tidak memeriksa arsip tetapi memindai lingkungan sistem; sementara Pemindaian Ekstensi Shell melakukan sebaliknya.*).

Catatan: *Untuk keterangan mengenai parameter tertentu, bacalah bab Pengaturan Lanjutan AVG/ Pemindaian/ Pindai Seluruh Komputer.*

Dibandingkan dengan dialog Pindai Seluruh Komputer, dialog ***Pemindaian Ekstensi Shell*** juga berisi bagian bernama ***Pengaturan lainnya terkait dengan Antarmuka Pengguna AVG***, tempat Anda dapat menentukan apakah Anda ingin kemajuan dan hasil pemindaian dapat diakses dari antarmuka pengguna AVG. Anda juga dapat menentukan bahwa hasil pemindaian seharusnya hanya ditampilkan jika ada infeksi yang terdeteksi selama pemindaian.

Antarmuka pengeditan untuk ***Pemindaian Perangkat Eksternal*** juga sangat mirip dengan dialog pengeditan Pindai Seluruh Komputer:



Pemindaian Perangkat Eksternal dijalankan secara otomatis begitu Anda memasang perangkat eksternal ke komputer Anda. Secara default, pemindaian ini dinonaktifkan. Walau demikian, sangatlah penting memindai ancaman potensial pada perangkat eksternal karena merupakan sumber infeksi utama. Untuk menyiapkan pemindaian ini dan agar diluncurkan secara otomatis bila diperlukan, tandai opsi ***Aktifkan pemindaian perangkat eksternal***.

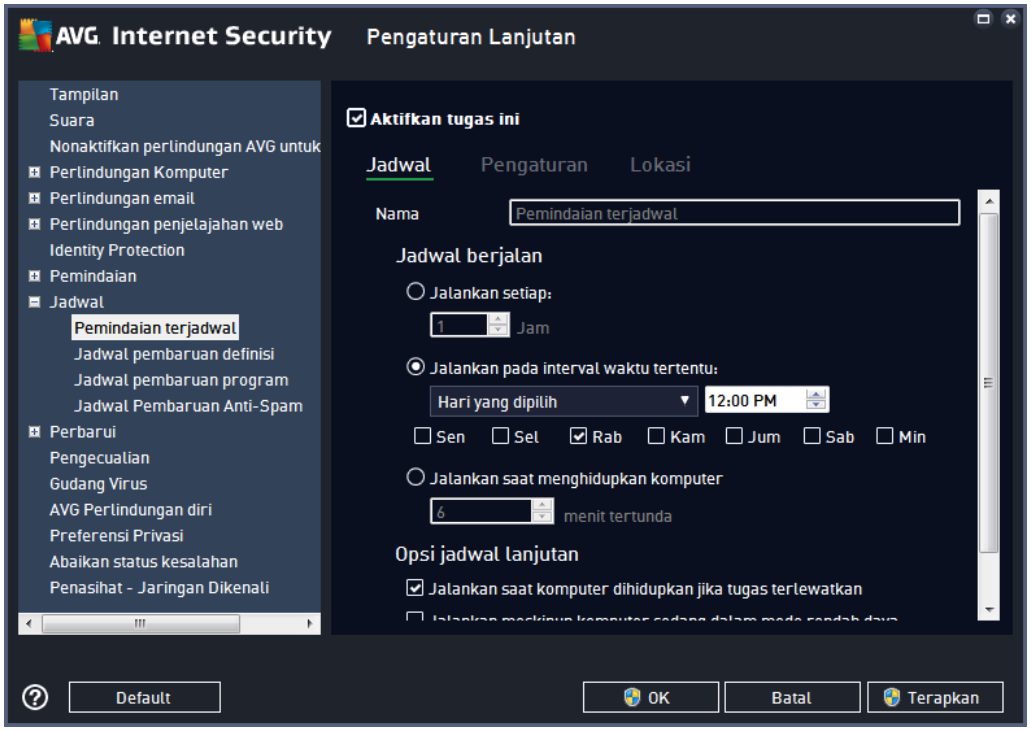
Catatan: *Untuk keterangan mengenai parameter tertentu, bacalah bab Pengaturan Lanjutan AVG/ Pemindaian/ Pindai Seluruh Komputer.*

3.7.9. Jadwal

Di bagian ***Jadwal*** Anda dapat mengedit pengaturan default:

- Pemindaian Terjadwal
- Jadwal Pembaruan Definisi
- Jadwal Pembaruan Program
- Jadwal Pembaruan Anti-Spam

Parameter pemindaian yang telah dijadwalkan dapat diedit (*atau jadwal baru yang telah diatur*) pada ketiga tab. Pada tiap tab, Anda dapat menandai/tidak menandai item ***Aktifkan tugas ini*** terlebih dahulu untuk menonaktifkan tes terjadwal untuk sementara, dan mengaktifkannya lagi saat diperlukan:



Berikutnya, kolom teks ***Nama*** (*dinonaktifkan untuk semua jadwal default*) menunjukkan nama yang ditetapkan ke jadwal ini oleh vendor program. Untuk jadwal yang baru ditambah (*Anda dapat menambahkan jadwal baru dengan mengklik kanan di atas item* ***Pemindaian terjadwal*** *dalam struktur navigasi di sebelah kiri*) Anda dapat menetapkan nama Anda sendiri, dan selanjutnya kolom teks akan terbuka untuk pengeditan. Cobalah selalu gunakan nama pemindaian yang singkat, deskriptif dan sesuai agar mudah membedakan pemindaian tersebut nanti dari jadwal lain.

Contoh: *Anda tidak disarankan untuk memberi nama pemindaian "Pindai baru" atau "Pindaianku" karena nama tersebut tidak menunjukkan apa yang diperiksa. Sebaliknya, sebuah contoh nama deskriptif yang baik misalnya "Pemindaian area sistem", dll. Yang juga tidak perlu ditetapkan dalam nama pemindaian adalah apakah pemindaian itu untuk seluruh komputer atau pun hanya untuk pemindaian atas file atau folder yang dipilih – pemindaian Anda akan selalu menjadi versi spesifik dari pindai file atau folder yang dipilih.*

Dalam dialog ini, Anda dapat menentukan lebih lanjut parameter pemindaian berikut:

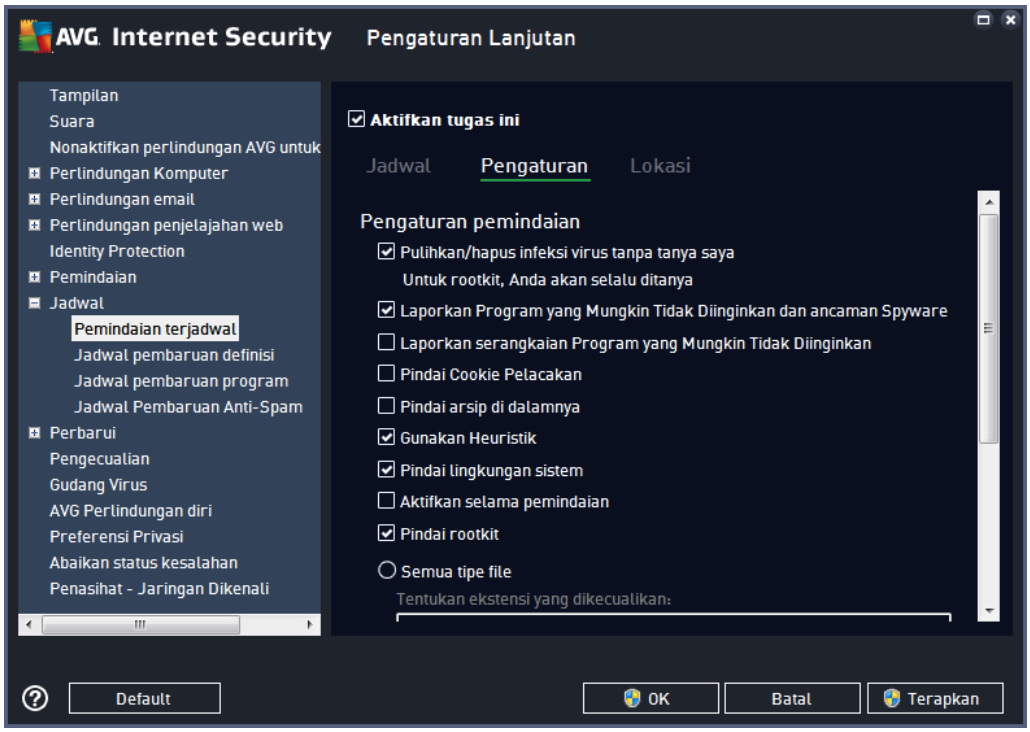
Jadwal berjalan

Di sini, Anda dapat menetapkan interval waktu untuk peluncuran pemindaian yang baru dijadwalkan. Penentuan waktu dapat ditentukan melalui peluncuran pembaruan yang berulang setelah periode waktu tertentu (***Jalankan setiap ...***) atau dengan menentukan tanggal dan waktu yang pasti (***Jalankan pada waktu tertentu***), atau mungkin dengan menentukan kejadian yang akan dikaitkan dengan peluncuran pembaruan (***Jalankan saat menghidupkan komputer***).

Opsi jadwal lanjutan

- ***Jalankan saat komputer dihidupkan jika tugas terlewatkan*** – jika pemindaian dijadwalkan pada waktu tertentu, opsi ini akan memastikan bahwa pemindaian akan dijalankan setelah itu seandainya pada waktu yang dijadwalkan komputer sedang mati.

- ***Jalankan meskipun komputer sedang dalam mode daya rendah*** – pemindaian harus dilakukan sekalipun komputer sedang menggunakan daya baterai pada waktu yang dijadwalkan.



Pada tab ***Pengaturan*** Anda akan menemukan daftar parameter pemindaian yang secara opsional dapat diaktifkan/ dinonaktifkan. Secara default, hampir semua parameter diaktifkan dan fungsionalitasnya diterapkan selama pemindaian. ***Kecuali Anda mempunyai alasan yang kuat untuk mengubah pengaturan ini, kami menyarankan untuk tetap menggunakan konfigurasi yang sudah ditetapkan***:

- ***Pulihkan/ hapus infeksi virus tanpa bertanya pada saya*** *(diaktifkan secara default):* jika virus teridentifikasi selama pemindaian, maka dapat dipulihkan secara otomatis jika penawarnya tersedia. Jika file yang terinfeksi tidak dapat dipulihkan secara otomatis, objek yang terinfeksi akan dipindahkan ke Gudang Virus.

- ***Laporkan program yang mungkin tidak diinginkan dan ancaman spyware*** *(diaktifkan secara default):* centang untuk mengaktifkan pemindaian spyware serta virus. Spyware merupakan kategori malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang terinstal secara tidak disengaja. Kami sarankan untuk tetap mengaktifkan fitur ini karena akan meningkatkan keamanan komputer Anda.

- ***Laporkan serangkaian program yang mungkin tidak diinginkan*** (*dinonaktifkan secara default*): tandai untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, tetapi dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, walaupun hal ini dapat memblokir program yang legal, dan karenanya dinonaktifkan secara default.

- ***Pindai cookie pelacakan*** (*dinonaktifkan secara default*): parameter ini menetapkan bahwa cookie harus dideteksi selama pemindaian; (*cookie HTTP digunakan untuk mengautentikasi, melacak, dan memelihara informasi tertentu tentang pengguna, seperti preferensi situs atau isi kereta belanja elektronik mereka*).

- ***Pindai arsip di dalamnya*** (*dinonaktifkan secara default*): parameter ini menetapkan bahwa pemindaian harus memeriksa semua file bahkan jika tersimpan di dalam arsip, misalnya ZIP, RAR, ...

- ***Gunakan heuristik*** (*diaktifkan secara default*): analisis heuristik (*emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual*) akan menjadi salah satu metode yang digunakan untuk deteksi virus selama pemindaian.

- ***Pindai lingkungan sistem*** (*diaktifkan secara default*): pemindaian juga akan memeriksa area sistem komputer Anda.

- ***Aktifkan selama pemindaian*** (*dinonaktifkan secara default):* dalam kondisi khusus (*misalnya jika dicurigai bahwa komputer Anda terinfeksi*) Anda dapat menandai opsi ini untuk mengaktifkan algoritma pemindaian paling menyeluruh yang akan memindai area paling sulit terinfeksi sekalipun di komputer Anda, agar benar-benar merasa yakin. Tetapi harap diingat bahwa metode ini memakan waktu lama.

- ***Pindai rootkit*** *(diaktifkan secara default): Pemindaian* Anti-Rootkit menelusuri komputer Anda dari kemungkinan rootkit, yaitu program dan teknologi yang dapat menutupi aktivitas malware di komputer Anda. Jika rootkit terdeteksi, tidak berarti komputer Anda terinfeksi. Di beberapa kasus, driver atau bagian tertentu dari aplikasi biasa mungkin salah terdeteksi sebagai rootkit.

Anda juga harus memutuskan apakah Anda ingin memindai

- ***Semua tipe file*** dengan opsi penentuan pengecualian dari pemindaian dengan memberikan daftar file ekstensi yang dipisah koma (*setelah disimpan, koma akan berganti menjadi titik koma*) untuk file yang tidak boleh dipindai.

- ***Tipe file yang dipilih*** – Anda dapat menentukan bahwa Anda hanya ingin memindai file yang dapat terinfeksi (*file yang tidak dapat terinfeksi tidak akan dipindai, misalnya beberapa file teks biasa, atau file yang tidak dapat dijalankan lainnya*), termasuk file media (*file video, audio – jika Anda membiarkan kotak ini tidak dicentang, maka hal ini akan lebih mengurangi waktu pemindaian, karena file ini seringkali terlalu besar dan sangat kecil kemungkinannya untuk terinfeksi virus*). Sekali lagi, Anda dapat menentukan ekstensi file yang harus selalu dipindai.

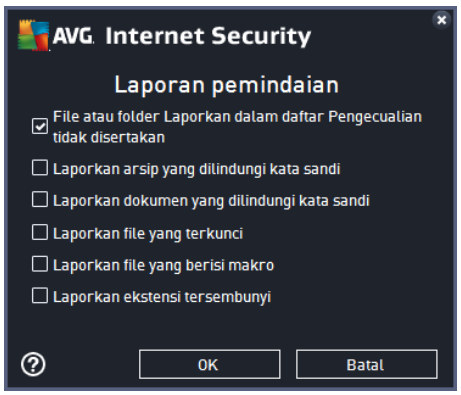
- Secara opsional, Anda dapat memutuskan apakah Anda ingin memilih opsi ***Pindai file tanpa ekstensi*** – opsi ini diaktifkan secara default, dan disarankan Anda membiarkannya kecuali Anda memiliki alasan kuat untuk mengubahnya. File tanpa ekstensi cukup mencurigakan dan harus selalu dipindai.

Sesuaikan secepat apa pemindaian selesai

Dalam bagian ini Anda dapat menentukan lebih lanjut kecepatan pemindaian yang diinginkan berdasarkan penggunaan sumber daya sistem. Secara default, nilai opsi ini diatur ke tingkat penggunaan sumber daya otomatis yang *peka pengguna*. Jika Anda ingin pemindaian berjalan lebih cepat, ini akan menghemat waktu tetapi sumber daya sistem yang digunakan akan jauh meningkat selama pemindaian dan akan memperlambat aktivitas lain pada PC (*opsi ini dapat digunakan bila komputer hidup namun tidak ada orang yang saat itu menggunakannya*). Di sisi lain, Anda dapat menurunkan sumber daya sistem yang digunakan dengan memperpanjang waktu pemindaian.

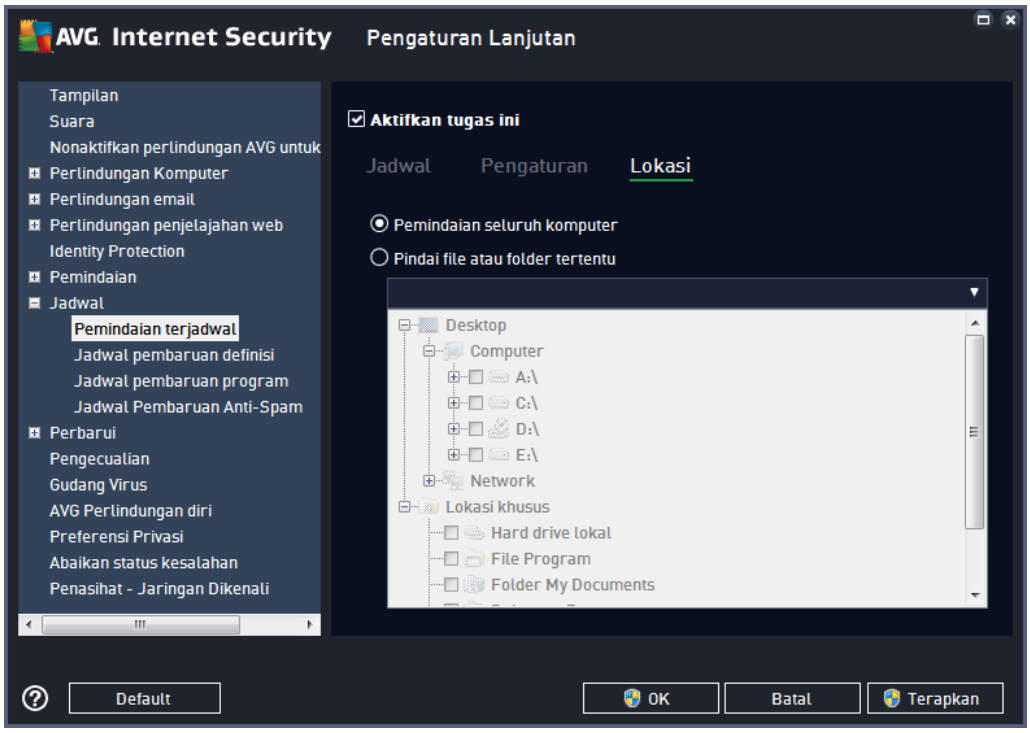
Atur laporan pemindaian tambahan

Klik tautan ***Atur laporan pindai tambahan ...*** untuk membuka jendela dialog mandiri bernama ***Laporan pindai*** di mana Anda dapat menandai beberapa item untuk menetapkan temuan apa yang harus dilaporkan:



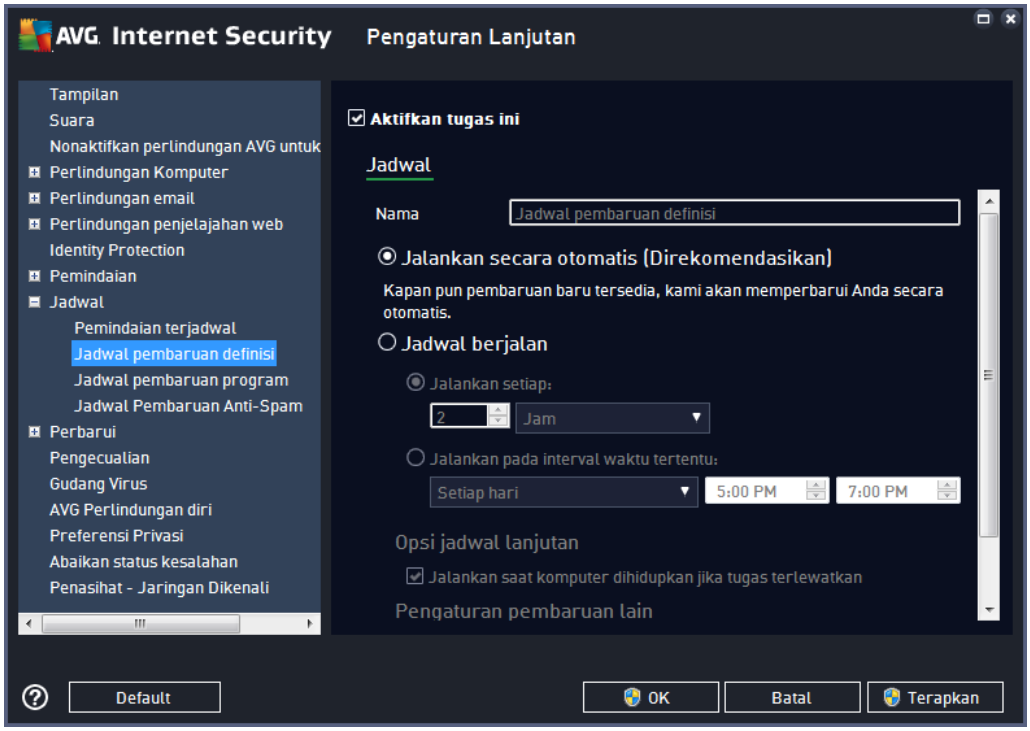
Opsi matikan komputer

Pada bagian ***Opsi matikan komputer***, Anda dapat memutuskan apakah komputer akan dimatikan secara otomatis setelah proses pemindaian yang berjalan selesai. Dengan mengkonfirmasi opsi ini (***Matikan komputer setelah pemindaian selesai***), sebuah opsi baru yang diaktifkan akan memungkinkan komputer dimatikan sekalipun saat itu sedang terkunci (***Matikan paksa jika komputer terkunci***).



Pada tab ***Lokasi*** Anda dapat menentukan apakah Anda ingin menjadwalkan pemindaian seluruh komputer atau pemindaian file atau folder tertentu. Jika Anda memilih pemindaian file atau folder, di bagian bawah dialog ini akan diaktifkan struktur yang ditampilkan dan Anda dapat menetapkan folder yang akan dipindai.

Jika ***benar-benar perlu***, Anda dapat mengosongkan item ***Aktifkan tugas ini*** untuk menonaktifkan pembaruan definisi yang terjadwal untuk sementara, dan mengaktifkannya lagi nanti:



Dalam dialog ini Anda dapat mengatur beberapa parameter terperinci untuk jadwal pembaruan definisi. Kolom teks ***Nama*** (*dinonaktifkan untuk semua jadwal default*) menampilkan nama yang ditetapkan ke jadwal ini oleh vendor program.

Jadwal berjalan

Secara default, tugas akan diluncurkan secara otomatis (***Jalankan secara otomatis***) segera setelah pembaruan definisi virus telah tersedia. Kami menyarankan agar Anda tetap menggunakan konfigurasi ini kecuali Anda memiliki alasan yang tepat untuk mengubahnya! Kemudian, Anda dapat mengatur peluncuran tugas secara manual dan menetapkan interval waktu untuk peluncuran pembaruan definisi terjadwal yang baru. Penentuan waktu dapat ditentukan melalui peluncuran pembaruan yang berulang setelah periode waktu tertentu(***Jalankan setiap ...***) atau dengan menentukan tanggal dan waktu yang pasti (***Jalankan pada waktu tertentu***).

Opsi jadwal lanjutan

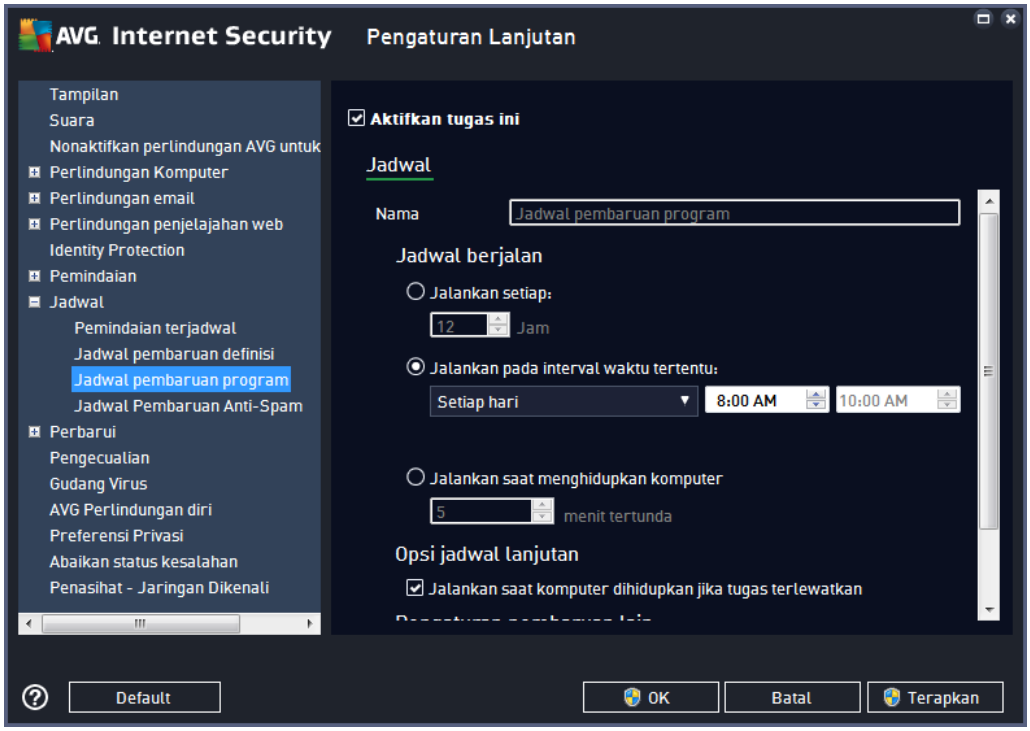
Bagian ini memungkinkan Anda menentukan dalam kondisi apa pembaruan definisi harus diluncurkan/ tidak diluncurkan jika komputer dalam mode daya rendah atau dimatikan sepenuhnya.

Pengaturan pembaruan lain

Akhirnya, centang opsi ***Jalankan lagi pembaruan begitu koneksi Internet tersedia*** untuk memastikan bahwa jika koneksi Internet terputus dan proses pembaruan gagal, pembaruan akan segera diluncurkan lagi setelah koneksi Internet pulih. Setelah pembaruan terjadwal diluncurkan pada waktu yang ditentukan, Anda akan diberi tahu mengenai hal ini melalui jendela yang muncul di atas ikon baki sistem AVG (*asalkan Anda telah membiarkan*

konfigurasi default pada dialog Pengaturan Lanjutan/ Tampilan).

Jika ***benar-benar perlu***, Anda dapat mengosongkan item ***Aktifkan tugas ini*** untuk menonaktifkan pembaruan program yang terjadwal untuk sementara, dan mengaktifkannya lagi nanti:



Kolom teks ***Nama*** (*dinonaktifkan untuk semua jadwal default*) menampilkan nama yang ditetapkan ke jadwal ini oleh vendor program.

Jadwal berjalan

Di sini, tetapkan interval waktu untuk peluncuran pembaruan program yang baru dijadwalkan. Penentuan waktu dapat ditentukan melalui peluncuran pembaruan yang berulang setelah periode waktu tertentu (***Jalankan setiap***) atau dengan menentukan tanggal dan waktu yang pasti (***Jalankan pada waktu tertentu***), atau mungkin dengan menentukan kejadian yang akan dikaitkan dengan peluncuran pembaruan (***Jalankan saat menghidupkan komputer***).

Opsi jadwal lanjutan

Bagian ini memungkinkan Anda menentukan dalam kondisi apa pembaruan program boleh/tidak boleh diluncurkan jika komputer dalam mode daya rendah atau dimatikan sepenuhnya.

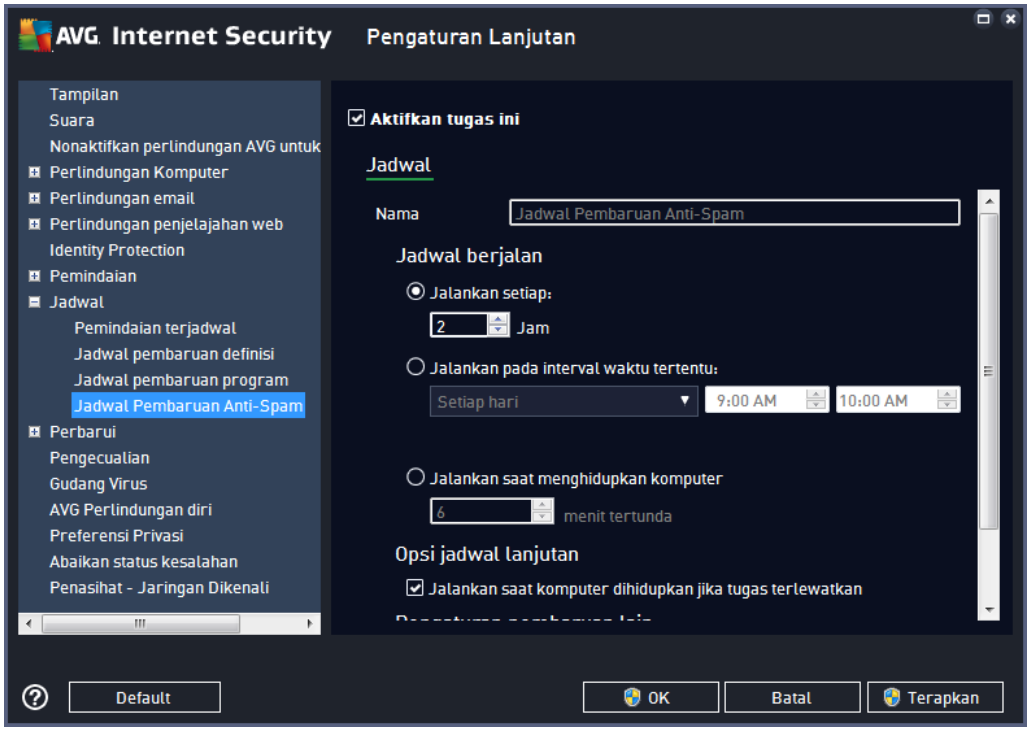
Pengaturan pembaruan lain

Centang opsi ***Jalankan lagi pembaruan begitu koneksi Internet tersedia*** untuk memastikan bahwa jika koneksi Internet terputus dan proses pembaruan gagal, pembaruan akan segera diluncurkan lagi segera setelah koneksi Internet pulih. Setelah pembaruan terjadwal diluncurkan pada waktu yang ditentukan, Anda akan diberi tahu mengenai hal ini melalui jendela yang muncul di atas ikon baki sistem AVG (*asalkan Anda telah membiarkan*

konfigurasi default pada dialog Pengaturan Lanjutan/Tampilan).

***Catatan:** Jika terjadi konflik waktu antara pembaruan program terjadwal dan pemindaian terjadwal, maka proses pembaruan akan lebih diprioritaskan dan pemindaian akan dihentikan sementara. Dalam hal ini, Anda akan diberi tahu tentang benturan tersebut*

Jika benar-benar perlu, Anda dapat mengosongkan item ***Aktifkan tugas ini*** untuk menonaktifkan pembaruan Anti-Spam yang terjadwal untuk sementara, dan mengaktifkannya lagi nanti:



Dalam dialog ini Anda dapat mengatur beberapa parameter terperinci untuk jadwal pembaruan. Kolom teks ***Nama*** (*dinonaktifkan untuk semua jadwal default*) berisi nama yang ditetapkan ke jadwal ini oleh vendor program.

Jadwal berjalan

Di sini, tetapkan interval waktu untuk jadwal baru peluncuran pembaruan Anti-Spam. Penentuan waktu dapat ditentukan melalui peluncuran pembaruan Anti-Spam yang berulang setelah periode waktu tertentu (***Jalankan setiap***) atau dengan menentukan tanggal dan waktu yang pasti (***Jalankan pada waktu tertentu***), atau mungkin dengan menentukan kejadian yang akan dikaitkan dengan peluncuran pembaruan (***Jalankan saat menghidupkan komputer***).

Opsi jadwal lanjutan

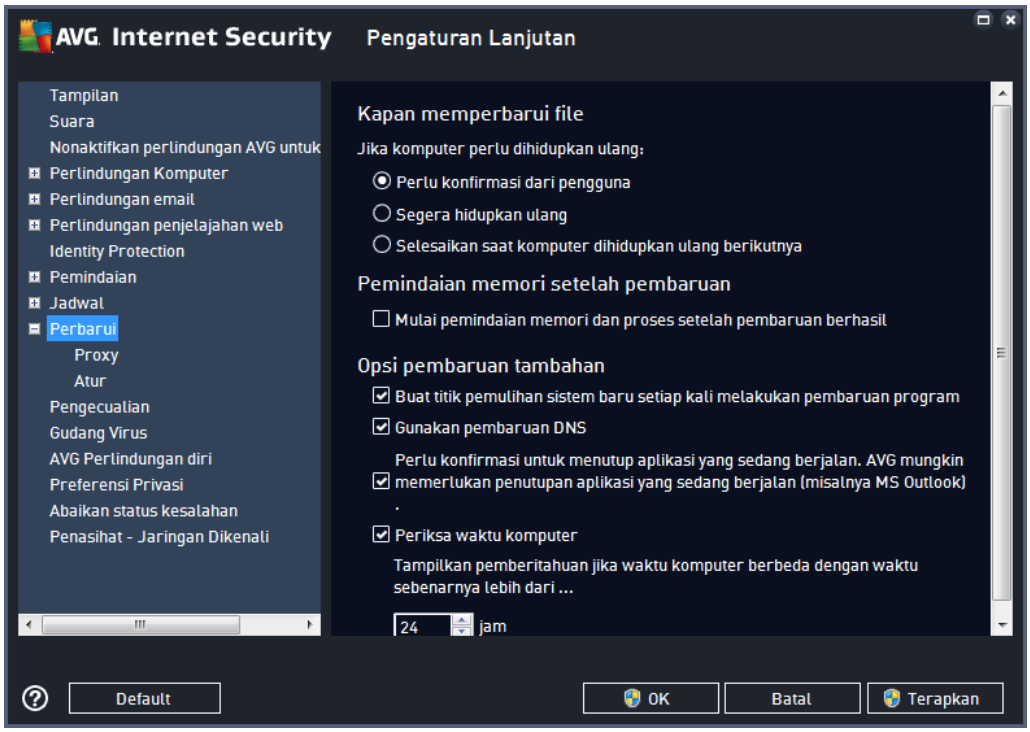
Bagian ini memungkinkan Anda menentukan dalam kondisi apa pembaruan Anti-Spam harus/tidak boleh diluncurkan jika komputer dalam mode daya rendah atau dimatikan sepenuhnya.

Pengaturan pembaruan lain

Tandai opsi ***Jalankan lagi pembaruan begitu koneksi Internet tersedia*** untuk memastikan bahwa jika koneksi Internet terputus dan proses pembaruan Anti-Spam gagal, pembaruan akan segera dijalankan lagi setelah koneksi Internet pulih. Setelah pemindaian terjadwal diluncurkan pada waktu yang ditentukan, Anda akan diberi tahu mengenai hal ini melalui jendela pop-up yang muncul di atas ikon baki sistem AVG (*asalkan Anda membiarkan konfigurasi default pada dialog Pengaturan Lanjutan/Tampilan*).

3.7.10. Perbarui

Item navigasi ***Perbarui*** membuka dialog baru di mana Anda dapat menetapkan parameter umum yang menyangkut Pembaruan AVG:



Kapan memperbarui file

Di bagian ini, Anda dapat memilih tiga opsi alternatif yang akan digunakan jika proses pembaruan mengharuskan PC dihidupkan ulang. Penuntasan pembaruan dapat dijadwalkan saat PC dihidupkan ulang berikutnya, atau Anda dapat menghidupkan ulang segera:

- ***Minta konfirmasi dari pengguna*** *(secara default)* – Anda akan dimintai persetujuan untuk menghidupkan ulang PC yang diperlukan buat menuntaskan proses pembaruan
- ***Hidupkan ulang segera*** – secara otomatis komputer akan dihidupkan ulang segera setelah proses pembaruan selesai, dan persetujuan Anda tidak akan diperlukan
- ***Selesaikan saat komputer dihidupkan ulang berikutnya*** – penuntasan proses pembaruan akan ditunda hingga saat berikutnya komputer dihidupkan ulang. Harap diingat bahwa opsi ini hanya disarankan jika Anda yakin komputer akan dihidupkan ulang secara rutin, setidaknya sekali sehari!

Pemindaian memori setelah pembaruan

Centang kotak ini untuk menentukan apakah Anda ingin meluncurkan pemindaian memori baru setelah setiap pembaruan yang berhasil selesai. Pembaruan yang terakhir diunduh dapat berisi definisi virus baru, dan definisi ini dapat segera diterapkan dalam pemindaian.

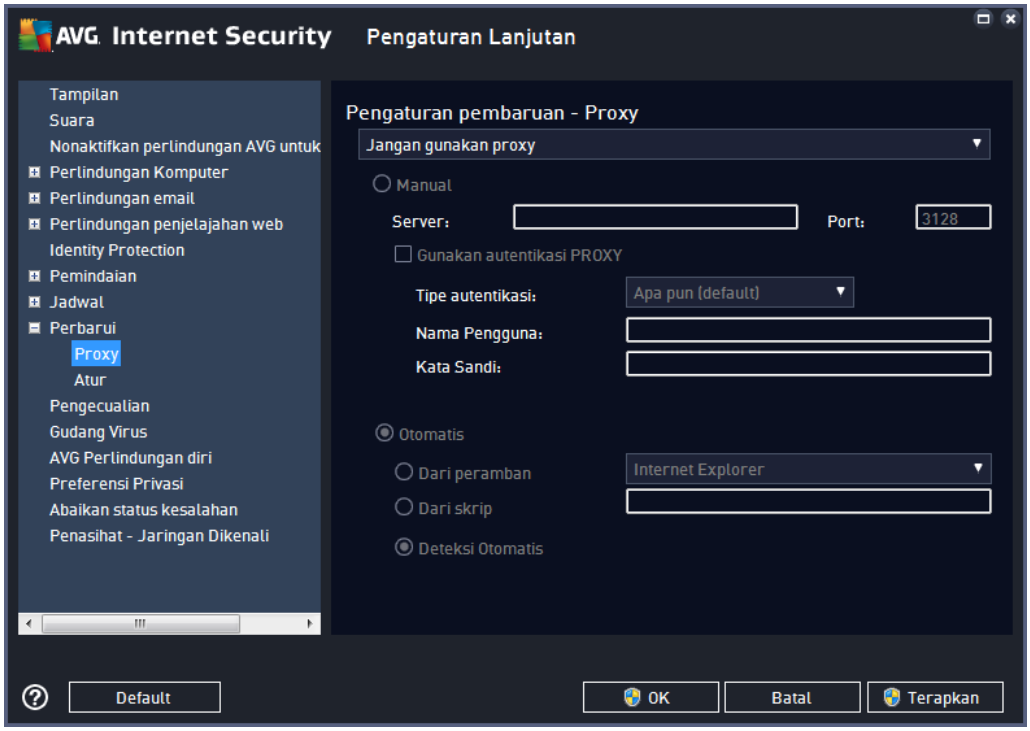
Opsi pembaruan tambahan

- ***Buat titik pemulihan sistem baru setiap kali melakukan pembaruan program*** (*diaktifkan secara default*) – sebelum setiap peluncuran pembaruan program AVG, akan dibuat titik pemulihan sistem. Seandainya proses pembaruan gagal dan sistem operasi crash, Anda dapat memulihkan OS ke konfigurasi aslinya dari titik ini. Opsi ini dapat diakses melalui Start / All Programs / Accessories / System tools / System Restore, tetapi segala perubahan hanya disarankan untuk pengguna yang berpengalaman! Biarkan kotak ini ditandai jika Anda ingin menggunakan fungsionalitas ini.

- ***Gunakan pembaruan DNS*** (*diaktifkan secara default*) – bila item ini ditandai, setelah pembaruan diluncurkan, **AVG Internet Security 2015** akan mencari informasi tentang versi basis data virus terbaru dan versi program terbaru pada server DNS. Kemudian, hanya file pembaruan yang benar-benar diperlukan saja yang akan diunduh dan diterapkan. Dengan cara ini, total jumlah data yang diunduh akan diminimalkan, dan proses pembaruan berjalan lebih cepat.

- ***Minta konfirmasi sebelum menutup aplikasi yang berjalan*** (*diaktifkan secara default*) – ini akan membantu Anda memastikan tidak ada penutupan aplikasi yang sedang berjalan tanpa seizin Anda – jika diperlukan untuk menuntaskan proses pembaruan.

- ***Periksa waktu komputer*** (*diaktifkan secara default) – tandai opsi ini untuk menyatakan Anda ingin pemberitahuan ditampilkan seandainya waktu komputer berbeda dengan waktu yang benar lebih dari jumlah jam yang ditetapkan.*



Server proxy adalah server mandiri atau layanan yang berjalan pada PC, yang menjamin koneksi ke Internet lebih

aman. Sesuai aturan jaringan yang ditentukan, Anda nanti dapat mengakses Internet baik secara langsung atau melalui server proxy; keduanya juga dapat diperbolehkan sekaligus. Kemudian, dalam item pertama pada dialog ***Pengaturan pembaruan – Proxy*** Anda harus memilih dari menu kotak kombo apakah Anda ingin:

- ***Jangan gunakan proxy*** – pengaturan default
- ***Gunakan proxy***
- ***Cobalah koneksi menggunakan poxy dan jika gagal, hubungkan langsung***

Jika Anda memilih suatu opsi menggunakan server proxy, Anda nanti harus menentukan beberapa data lebih lanjut. Pengaturan server dapat dikonfigurasi secara manual atau secara otomatis.

Konfigurasi manual

Jika Anda memilih konfigurasi manual (tandai opsi ***Manual*** *untuk mengaktifkan bagian dialognya*) Anda harus menentukan item berikut:

- ***Server*** – menetapkan alamat IP server atau nama server
- ***Port*** – menetapkan nomor port yang memungkinkan akses Internet (*secara default, nomor ini diatur ke 3128 namun dapat diatur berbeda – jika Anda tidak yakin, hubungi administrator jaringan Anda*)

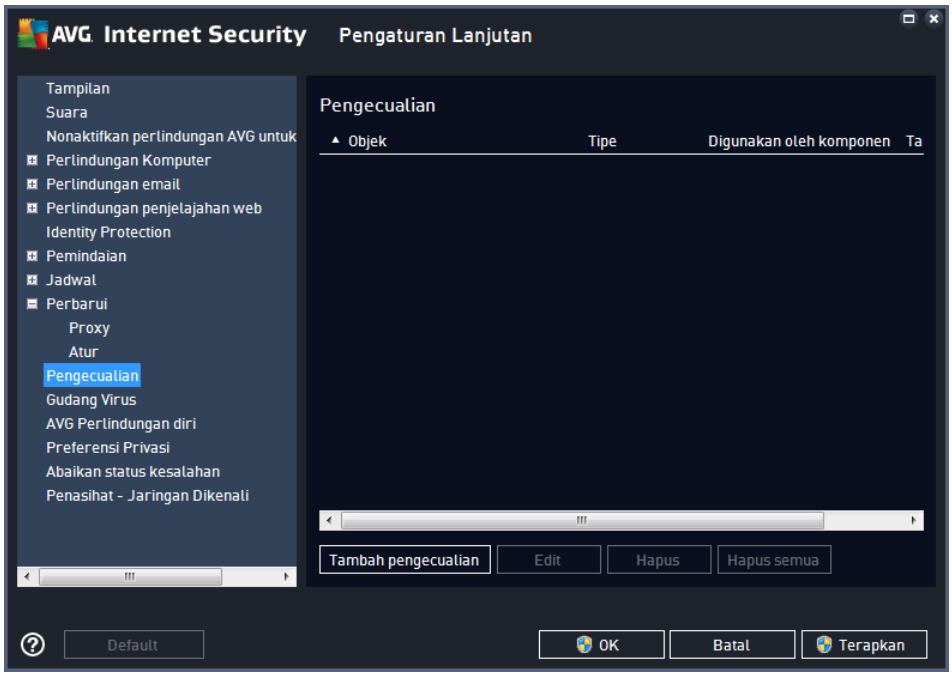
Server proxy juga dapat dikonfigurasi dengan aturan tertentu untuk setiap pengguna. Jika server proxy Anda telah diatur dengan cara ini, tandai opsi ***Gunakan autentikasi PROXY*** untuk memverifikasi bahwa nama pengguna dan kata sandi Anda sudah sah untuk menghubungkan ke Internet melalui server proxy.

Konfigurasi otomatis

Jika Anda memilih konfigurasi otomatis (*tandai opsi* ***Otomatis*** *untuk mengaktifkan bagian dialognya*) maka pilih dari mana konfigurasi proxy akan diambil:

- ***Dari browser*** – konfigurasi akan dibaca dari browser Internet default Anda
- ***Dari skrip*** – konfigurasi akan dibaca dari skrip yang telah diunduh dengan fungsi yang menghasilkan alamat proxy
- ***Deteksi otomatis*** – konfigurasi akan dideteksi secara otomatis, langsung dari server proxy

Dialog ***Manajemen Pembaruan*** menyediakan dua opsi yang dapat diakses melalui dua tombol:



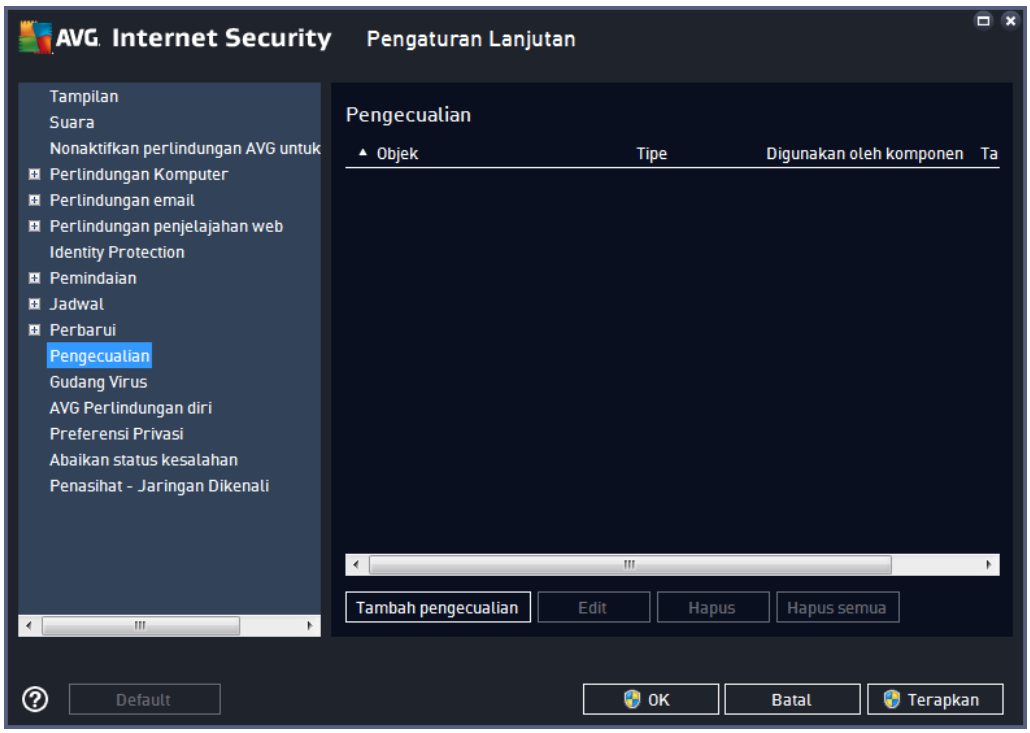
- ***Hapus file pembaruan sementara*** – tekan tombol ini untuk menghapus semua file pembaruan sementara dari hard disk Anda (*secara default, file ini akan disimpan selama 30 hari*)

- ***Kembalikan basis data virus ke versi sebelumnya*** – tekan tombol ini untuk menghapus versi basis data virus terbaru dari hard disk Anda, dan kembali ke versi yang telah disimpan sebelumnya (*versi basis data virus baru akan menjadi bagian dari pembaruan berikutnya*)

3.7.11. Pengecualian

Pada dialog ***Pengecualian*** Anda dapat menentukan pengecualian, yaitu item yang akan diabaikan oleh **AVG Internet Security 2015**. Biasanya, Anda harus menentukan pengecualian jika AVG terus mendeteksi program atau file sebagai ancaman, atau memblokir situs web yang aman sebagai berbahaya. Tambahkan file atau situs web semacam itu dalam daftar pengecualian ini, maka AVG tidak akan melaporkan atau memblokirnya lagi.

Selalu pastikan bahwa file, program atau situs web yang ditanyakan benar-benar aman!



Bagan dalam dialog menampilkan daftar pengecualian, jika sebelumnya telah ditentukan. Setiap item memiliki kotak centang di sampingnya. Jika kotak ini dicentang, maka pengecualiannya berlaku; jika tidak, maka pengecualiannya hanya ditetapkan tapi saat ini belum digunakan. Dengan mengeklik kepala kolom, Anda dapat mengurutkan item diperbolehkan sesuai dengan kriteria yang terkait.

Tombol kontrol

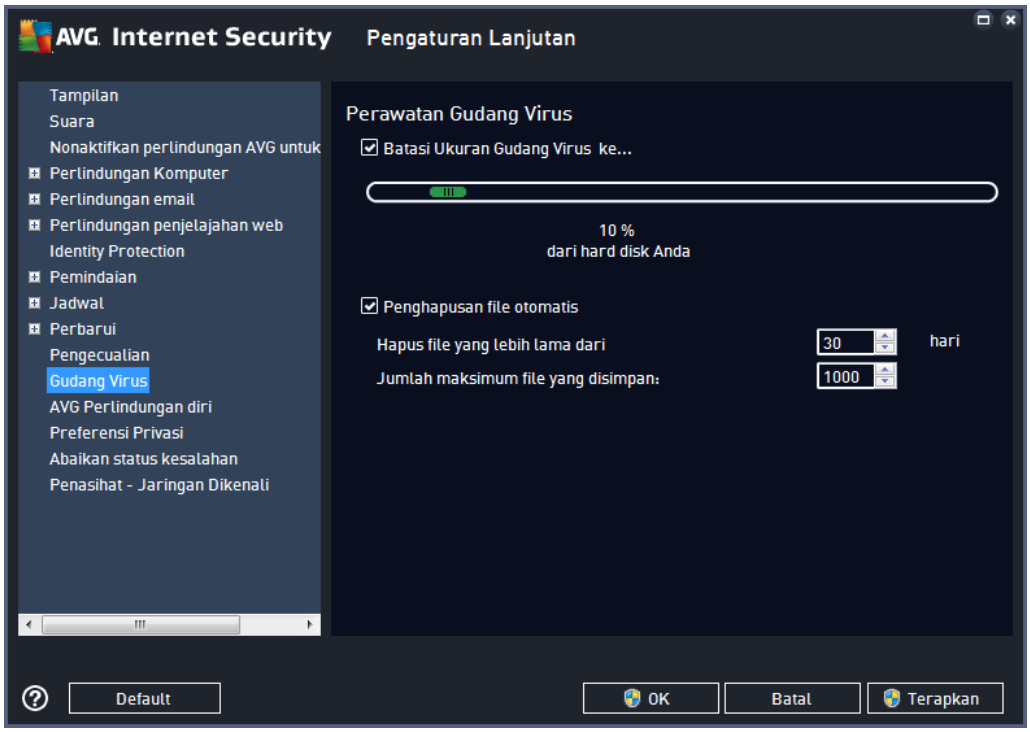
- ***Tambah pengecualian*** – Klik untuk membuka dialog baru di mana Anda dapat menentukan item yang harus dikecualikan dari pemindaian AVG. Pertama kali, Anda akan diminta untuk menentukan tipe objek, misalnya apakah sebuah file, folder, URL, atau sertifikat. Kemudian Anda harus menjelajahi disk Anda untuk memberikan jalur objek yang dimaksud, atau tipe URL. Terakhir, Anda dapat memilih fitur AVG apa yang harus mengabaikan objek yang dipilih *(Resident Shield, Identity Protection, Pemindaian)*.

- ***Edit*** – Tombol ini hanya aktif jika beberapa pengecualian telah ditentukan, dan tertera dalam bagan. Kemudian Anda dapat menggunakan tombol untuk membuka dialog edit untuk pengecualian yang dipilih, dan mengonfigurasi parameter pengecualian.

- ***Hapus*** – Gunakan tombol ini untuk membatalkan pengecualian yang sebelumnya telah ditentukan. Anda dapat menghapusnya satu per satu, atau menyorot balok pengecualian pada daftar lalu membatalkan pengecualian yang telah ditentukan. Setelah membatalkan pengecualian, file, folder atau URL tersebut akan diperiksa oleh AVG lagi. Perhatikan bahwa hanya pengecualiannya yang akan dihapus, bukan file atau folder itu sendiri!

- ***Hapus semua*** – Gunakan tombol ini untuk menghapus semuapengecualian yang ditentukan dalam daftar.

3.7.12. Gudang Virus

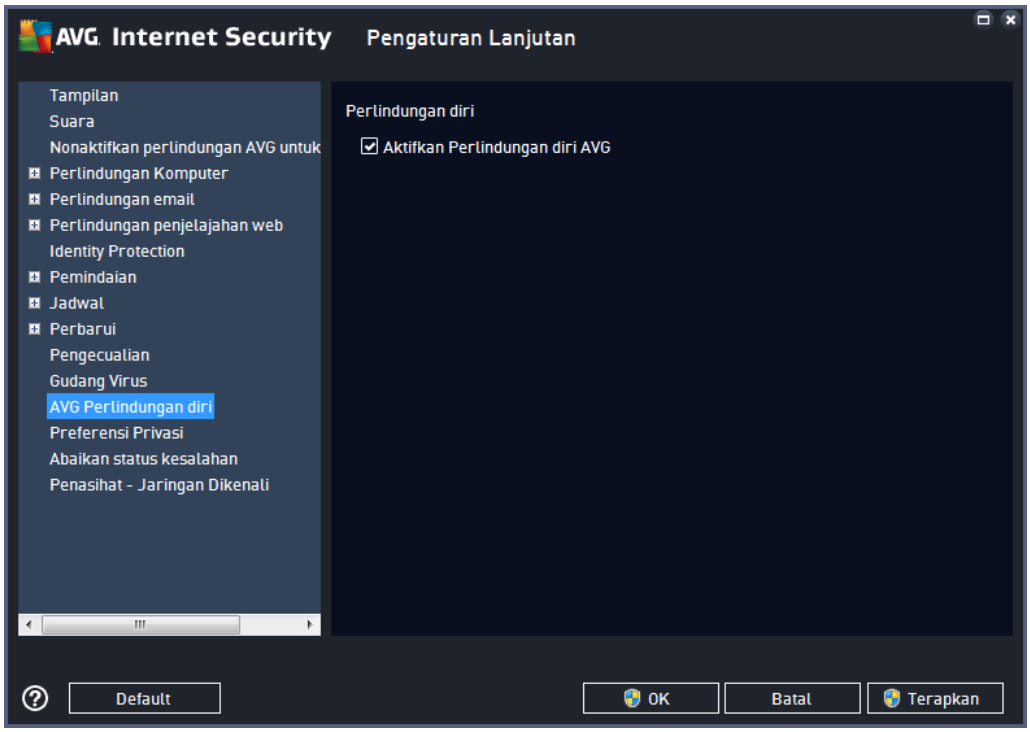


Dialog ***Perawatan Gudang Virus*** memungkinkan Anda menentukan beberapa parameter yang menyangkut administrasi berbagai objek yang tersimpan dalam Gudang Virus:

- ***Batasi Ukuran Gudang Virus*** – gunakan penggeser untuk mengatur ukuran maksimum Gudang Virus. Ukuran ditetapkan secara proporsional, dibandingkan dengan ukuran disk lokal Anda.

- ***Penghapusan file otomatis*** – di bagian ini, tentukan lama maksimum untuk menyimpan objek dalam Gudang Virus (***Hapus file yang lebih lama dari ... hari***), dan jumlah maksimum file yang disimpan dalam Gudang Virus (***Jumlah maksimum file yang disimpan***).

3.7.13. Perlindungan Diri AVG

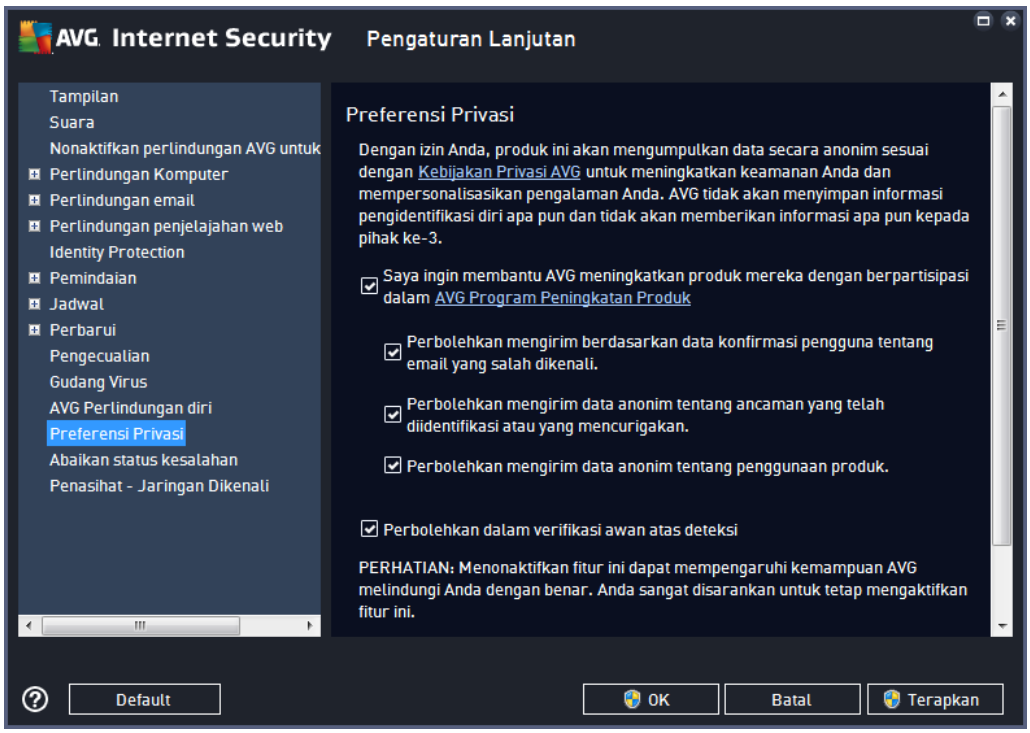


Perlindungan Diri AVG mengaktifkan **AVG Internet Security 2015** untuk melindungi prosesnya sendiri, file, kunci registri, dan driver agar tidak berubah atau dinonaktifkan. Alasan utama untuk perlindungan semacam ini karena beberapa ancaman canggih mencoba untuk melumpuhkan perlindungan anti virus, lalu menyebabkan kerusakan pada komputer Anda dengan bebas.

Kami menyarankan agar fiitur ini selalu diaktifkan!

3.7.14. Preferensi Privasi

Dialog ***Preferensi Privasi*** meminta Anda untuk berpartisipasi dalam peningkatan produk AVG dan membantu kami meningkatkan tingkat keamanan Internet. Laporan Anda membantu kami mengumpulkan informasi mutakhir mengenai ancaman terbaru dari semua peserta di seluruh dunia, dan sebagai timbal baliknya kami dapat menyempurnakan perlindungan bagi semua orang. Laporan ini dibuat secara otomatis, sehingga tidak mengganggu kenyamanan Anda. Tidak ada data pribadi yang disertakan dalam laporan tersebut. Pelaporan ancaman yang terdeteksi bersifat opsional, walau demikian, kami minta Anda membiarkan opsi ini diaktifkan. Ini akan membantu kami meningkatkan perlindungan untuk Anda dan pengguna AVG lainnya.



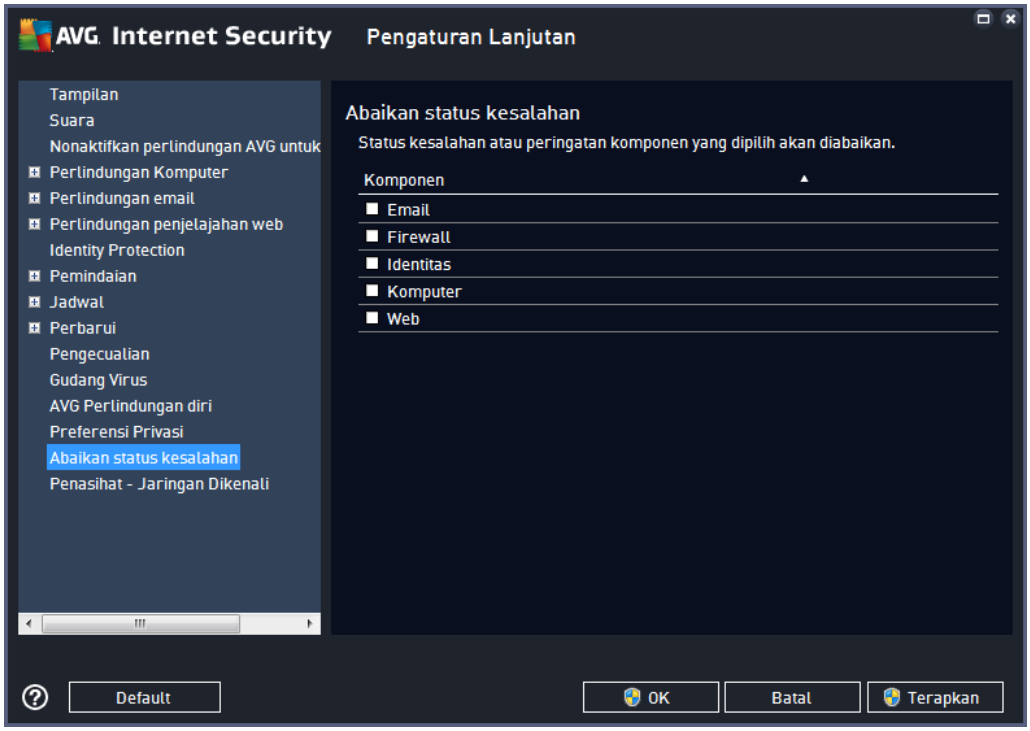
Dalam dialog, opsi pengaturan berikut ini tersedia:

- ***Saya ingin membantu AVG meningkatkan produk-produknya dengan berpartisipasi dalam Program Peningkatan Produk AVG*** *(diaktifkan secara default)* – Jika Anda ingin membantu kami meningkatkan **AVG Internet Security 2015** lebih lanjut, tetap centang kotak ini. Ini akan memungkinkan semua ancaman yang ditemukan untuk dilaporkan ke AVG, sehingga kami dapat mengumpulkan informasi terbaru mengenai malware dari semua peserta di seluruh dunia, dan dengan demikian dapat meningkatkan perlindungan bagi siapa saja. Laporan ini dibuat secara otomatis, sehingga tidak mengganggu kenyamanan Anda, dan tidak ada data pribadi yang disertakan dalam laporan tersebut.
    - ***Perbolehkan mengirim menurut data konfirmasi pengguna tentang email yang salah diidentifikasi*** *(diaktifkan secara default)* – mengirim informasi tentang pesan email yang salah diidentifikasi sebagai spam atau tentang pesan spam yang tidak terdeteksi oleh layanan Anti-Spam. Saat mengirim jenis informasi ini, Anda akan diminta konfirmasi.
    - ***Perbolehkan mengirim data anonim tentang ancaman yang dikenali atau dicurigai*** *(diaktifkan secara default)* – mengirim informasi tentang kode atau pola perilaku yang positif berbahaya atau mencurigakan *(boleh jadi berupa virus, spyware, atau halaman Web jahat yang coba Anda akses)* yang terdeteksi pada komputer Anda.
    - ***Perbolehkan mengirim data anonim tentang penggunaan produk*** *(diaktifkan secara default)* – mengirim statistik dasar tentang penggunaan aplikasi, seperti jumlah deteksi, pemindaian yang diluncurkan, pembaruan berhasil atau tidak berhasil, dsb.
- ***Perbolehkan di verifikasi awan atas deteksi*** *(diaktifkan secara default)* – ancaman yang terdeteksi akan diperiksa apakah benar-benar terinfeksi untuk memilah peringatan palsu.
- ***Saya ingin AVG untuk mempersonalisasi pengalaman saya dengan mengaktifkan Personalisasi AVG*** *(dinonaktifkan secara default)* – fitur ini secara anonim menganalisis perilaku program dan aplikasi

yang terinstal pada PC Anda. Berdasarkan analisis ini, AVG dapat menawarkan layanan yang ditargetkan secara langsung dengan kebutuhan Anda, untuk memastikan keamanan maksimum Anda.

3.7.15. Abaikan Status Kesalahan

Dalam dialog ***Abaikan status kesalahan***, Anda dapat menandai komponen-komponen yang tidak perlu diberitahukan kepada Anda:



Secara default, tidak ada komponen yang dipilih dalam daftar ini. Berarti jika ada komponen diberi status kesalahan, Anda akan segera diberitahu melalui:

- ikon baki sistem – saat semua bagian AVG bekerja dengan benar, ikon-ikonnya ditampilkan dalam empat warna; walau demikian, jika terjadi kesalahan, ikon akan tampak bersama tanda seru berwarna kuning,
- keterangan teks mengenai masalah yang ada di bagian Info Status Keamanan pada jendela utama AVG

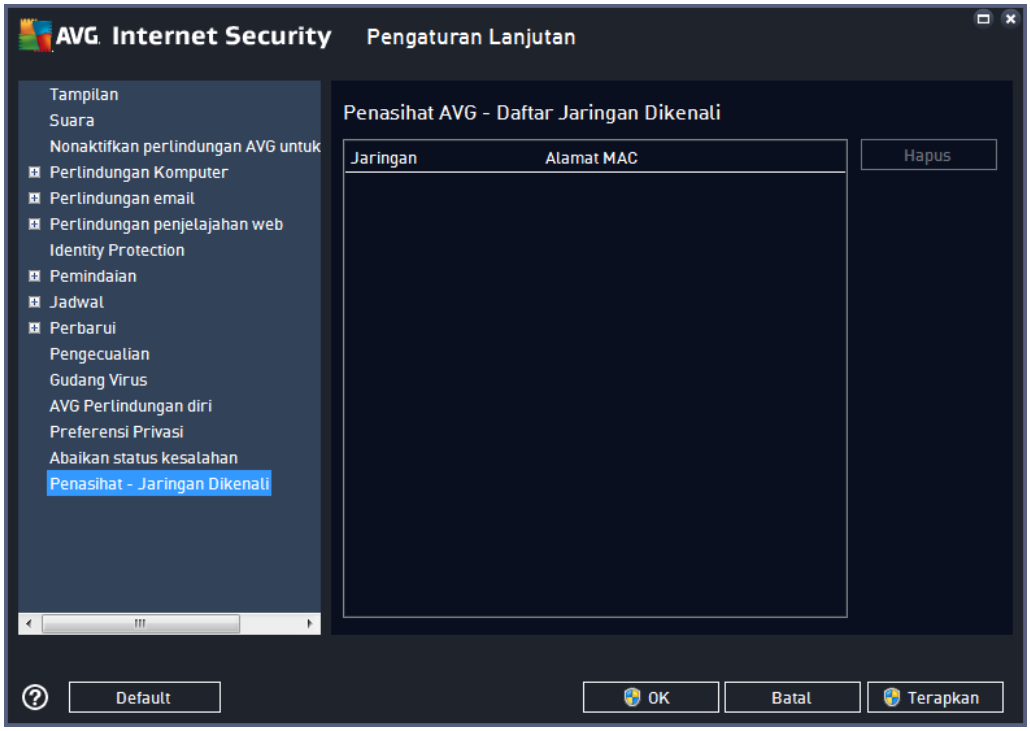
Mungkin akan ada situasi di mana karena suatu alasan, Anda harus menonaktifkan komponen untuk sementara. ***Ini tidak direkomendasikan Anda harus tetap mengaktifkan semua komponen selamanya dan dalam konfigurasi default***, tetapi hal ini mungkin saja terjadi. Dalam hal ini, ikon baki sistem secara otomatis melaporkan status kesalahan komponen tersebut. Walau demikian, dalam hal ini kita tidak dapat membicarakan tentang kesalahan sebenarnya karena Anda sengaja melakukannya, dan Anda mengetahui akan potensi risikonya. Di saat yang sama, saat ditampilkan dalam warna abu-abu, ikon tersebut tidak dapat melaporkan dengan sebenarnya segala kemungkinan kesalahan lebih lanjut yang mungkin muncul.

Untuk situasi ini, dalam dialog ***Abaikan status kesalahan*** Anda dapat memilih komponen yang mungkin sedang mengalami kesalahan (*atau dinonaktifkan*) dan Anda tidak ingin diberitahu mengenai hal tersebut. Tekan tombol ***OK*** untuk mengonfirmasi.

3.7.16. Advisor – Jaringan Dikenali

AVG Advisor memiliki fitur yang memantau jaringan yang terhubung dengan Anda, dan jika jaringan baru ditemukan *(dengan nama jaringan yang sudah digunakan, yang dapat menyebabkan kekacauan),* Anda akan diberi tahu dan disarankan untuk memeriksa keamanan jaringan. Jika Anda memutuskan bahwa jaringan baru yang akan terhubung sudah aman, Anda juga dapat menyimpannya ke daftar ini *(Melalui tautan yang disediakan di pemberitahuan baki AVG Advisor yang bergulir pada baki sistem apabila ada jaringan tak dikenal yang terdeteksi. Untuk keterangan selengkapnya, lihat bab AVG Advisor)*. AVG Advisor kemudian akan mengingat atribut unik dari jaringan tersebut *(terutama alamat MAC)*, dan tidak akan menampilkan pemberitahuan di lain waktu. Setiap jaringan yang tersambung dengan Anda otomatis akan dianggap sebagai jaringan yang dikenal dan ditambahkan pada daftar. Anda dapat menghapus masing-masing entri dengan menekan tombol ***Hapus***; masing-masing jaringan tersebut kemudian akan dianggap tidak dikenal dan berpotensi tidak aman lagi.

Pada jendela dialog ini, Anda dapat memeriksa jaringan mana yang dianggap akan dikenal:



Catatan: *Fitur jaringan yang dikenal dalam AVG Advisor tidak didukung pada Windows XP 64-bit.*

3.8. Pengaturan Firewall

Konfigurasi Firewall akan dibuka dalam jendela baru berisi sejumlah dialog di mana Anda dapat mengatur parameter lebih lanjut dari komponen tersebut. Konfigurasi Firewall akan dibuka dalam jendela baru di mana Anda dapat mengedit parameter lebih lanjut dari komponen tersebut pada sejumlah dialog konfigurasi. Konfigurasi ini dapat ditampilkan dalam mode dasar maupun mode ahli. Saat Anda pertama kali masuk ke jendela konfigurasi, jendela ini akan dibuka dalam versi dasar untuk mengedit parameter berikut ini:

- Umum
- Aplikasi

- Berbagi File dan Printer

Di bagian bawah dialog, Anda akan menemukan tombol ***Mode ahli***. Tekan tombol ini untuk menampilkan lebih banyak item dalam navigasi dialog untuk konfigurasi Firewall sangat lanjut:

- Pengaturan Lanjutan
- Jaringan Yang Ditentukan
- Layanan Sistem
- Log

3.8.1. Umum

Dialog ***Informasi umum*** memberikan gambaran umum semua mode Firewall yang tersedia. Pilihan mode Firewall saat ini dapat diubah dengan hanya memilih mode lain dari menu.

Walau demikian, vendor perangkat lunak telah mengatur semua komponen AVG Internet Security 2015 untuk memberikan kinerja optimal. Jika Anda tidak memiliki alasan kuat untuk melakukannya, jangan ubah konfigurasi default. Semua perubahan pengaturan hanya boleh dilakukan oleh pengguna berpengalaman!

Firewall memungkinkan Anda untuk menentukan aturan keamanan spesifik berdasarkan pada apakah komputer Anda terletak di suatu domain, sebuah komputer tunggal, atau bahkan notebook. Setiap opsi ini memerlukan tingkat perlindungan yang berbeda, dan level tersebut dicakup oleh mode masing-masing. Singkatnya, mode Firewall merupakan konfigurasi spesifik dari komponen Firewall, dan Anda dapat menggunakan beberapa konfigurasi yang telah ditentukan:

- ***Otomatis*** – Dalam mode ini, Firewall menangani semua lalu lintas jaringan secara otomatis. Anda akan diundang untuk mengambil keputusan. Firewall akan memungkinkan koneksi untuk setiap aplikasi yang dikenal, dan pada saat yang sama aturan aplikasi akan dibuat yang menentukan bahwa aplikasi tersebut

selanjutnya dapat selalu terhubung. Untuk aplikasi lain, Firewall akan memutuskan apakah koneksi akan diperbolehkan atau diblokir berdasarkan perilaku aplikasi. Namun, pada situasi semacam itu, aturan tidak akan dibuat dan aplikasi akan diperiksa lagi setiap kali mencoba terhubung. ***Mode otomatis ini cukup sederhana dan direkomendasikan untuk sebagian besar pengguna.***

- ***Interaktif*** – mode ini bermanfaat jika Anda ingin mengendalikan secara penuh semua lalu lintas jaringan ke dan dari komputer Anda. Firewall akan memantaunya dan memberitahu Anda setiap kali ada upaya untuk berkomunikasi atau mentransfer data, yang memungkinkan Anda untuk memperbolehkan atau memblokir upaya yang Anda rasa sesuai. Disarankan untuk pengguna mahir saja.

- ***Memblokir akses ke Internet*** – Koneksi Internet benar-benar diblokir, Anda tidak dapat mengakses Internet dan tidak ada orang luar yang dapat mengakses komputer Anda. Hanya untuk penggunaan khusus dan dalam jangka waktu pendek.

- ***Nonaktifkan perlindungan Firewall*** – menonaktifkan Firewall akan mengaktifkan semua lalu lintas jaringan ke dan dari komputer Anda. Akibatnya, pengaturan ini akan membuat rentan terhadap serangan peretas. Harap selalu pertimbangkan pilihan ini secara hati-hati.

Harap diingat bahwa ada mode otomatis khusus yang tersedia dalam Firewall. Mode ini akan diaktifkan dengan diam-diam jika komponen Komputer atau Perlindungan Identitas dinonaktifkan dan komputer Anda menjadi lebih rentan. Pada kasus tersebut, Firewall otomatis hanya akan memperbolehkan aplikasi yang dikenal dan benar-benar aman. Untuk aplikasi lainnya, Firewall akan bertanya pada Anda. Hal ini dilakukan untuk komponen perlindungan yang dinonaktifkan dan untuk mengamankan komputer Anda.

3.8.2. Aplikasi

Dialog ***Aplikasi*** berisi daftar semua aplikasi yang mencoba berkomunikasi melalui jaringan selama ini, dan ikon untuk tindakan yang ditetapkan:

Aplikasi dalam ***Daftar aplikasi*** adalah aplikasi yang terdeteksi pada komputer Anda (*dan telah ditetapkan dengan tindakan tertentu*). Tipe tindakan berikut dapat digunakan:

- – memungkinkan komunikasi untuk semua jaringan
- – blokir komunikasi
- – pengaturan lanjutan yang ditetapkan

Perhatikan bahwa hanya aplikasi yang telah diinstal yang akan dapat dideteksi. Secara default, bila aplikasi baru mencoba untuk terhubung melalui jaringan untuk yang pertama kali, Firewall akan membuat sebuah aturan baginya secara otomatis sesuai dengan basis data terpercaya, atau menanyakan apakah Anda ingin memperbolehkan atau memblokir komunikasi tersebut. Untuk selanjutnya, Anda akan dapat menyimpan jawaban sebagai aturan permanen (yang nanti akan dicantumkan dalam dialog ini).

Tentu saja, Anda juga dapat menentukan aturan untuk aplikasi baru saat itu juga – dalam dialog ini, tekan ***Tambah*** lalu masukkan perincian aplikasi.

Selain aplikasi, daftar ini juga berisi dua item khusus. ***Aturan Aplikasi Prioritas*** (*di bagian atas daftar*) bersifat pilihan, dan selalu diterapkan sebelum aturan untuk aplikasi masing-masing. ***Aturan Aplikasi Lainnya*** (*di bagian bawah daftar*) digunakan sebagai "jalan terakhir", bila tidak ada aturan aplikasi tertentu yang berlaku, mis. untuk aplikasi yang tidak dikenal dan tidak ditentukan. Pilih tindakan yang harus dijalankan bila aplikasi tersebut mencoba berkomunikasi lewat jaringan: Blokir *(komunikasi akan selalu diblokir)*, Perbolehkan *(komunikasi akan diperbolehkan lewat semua jaringan)*, Tanya *(Anda akan diminta untuk memutuskan apakah komunikasi harus diperbolehkan atau diblokir)*. ***Item ini memiliki opsi pengaturan yang berbeda dengan aplikasi umum dan hanya ditujukan bagi pengguna berpengalaman. Kami sangat menyarankan agar Anda tidak memodifikasi pengaturan!***

Tombol kontrol

Daftar ini dapat diedit menggunakan tombol kontrol berikut:

- ***Tambah*** – membuka dialog kosong untuk menetapkan aturan aplikasi baru.
- ***Edit*** – membuka dialog yang sama dengan data yang disediakan untuk mengedit kumpulan aturan aplikasi yang ada.
- ***Hapus*** – menghapus aplikasi yang dipilih dari daftar.

3.8.3. Berbagi file dan printer

Berbagi file dan printer artinya berbagi semua file atau folder yang Anda tandai sebagai "Dibagi" pada Windows, unit disk, printer, pemindai bersama dan semua perangkat sejenis. Berbagi item semacam itu hanya mungkin dilakukan dalam jaringan yang bisa dianggap aman *(misalnya di rumah, di kantor atau di sekolah)*. Namun, jika Anda tersambung ke jaringan publik *(seperti Wi-Fi bandara atau kafe Internet)*, Anda mungkin tidak ingin berbagi apa pun. AVG Firewall dapat dengan mudah memblokir atau memperbolehkan berbagi dan memungkinkan Anda untuk menyimpan pilihan Anda untuk jaringan yang telah dikunjungi.

Pada dialog ***Berbagi File dan Printer*** Anda Anda dapat mengedit konfigurasi berbagi file dan printer, serta jaringan yang tersambung saat ini. Dengan Windows XP, nama jaringan akan merespons nama yang Anda pilih untuk jaringan tertentu ketika pertama kali terhubung ke jaringan tersebut. Dengan Windows Vista dan versi di atasnya, nama jaringan akan diambil secara otomatis dari Network and Sharing Center.

3.8.4. Pengaturan lanjut

Editing yang ada pada dialog Pengaturan lanjut ditujukan untuk PENGGUNA YANG BERPENGALAMAN SAJA!

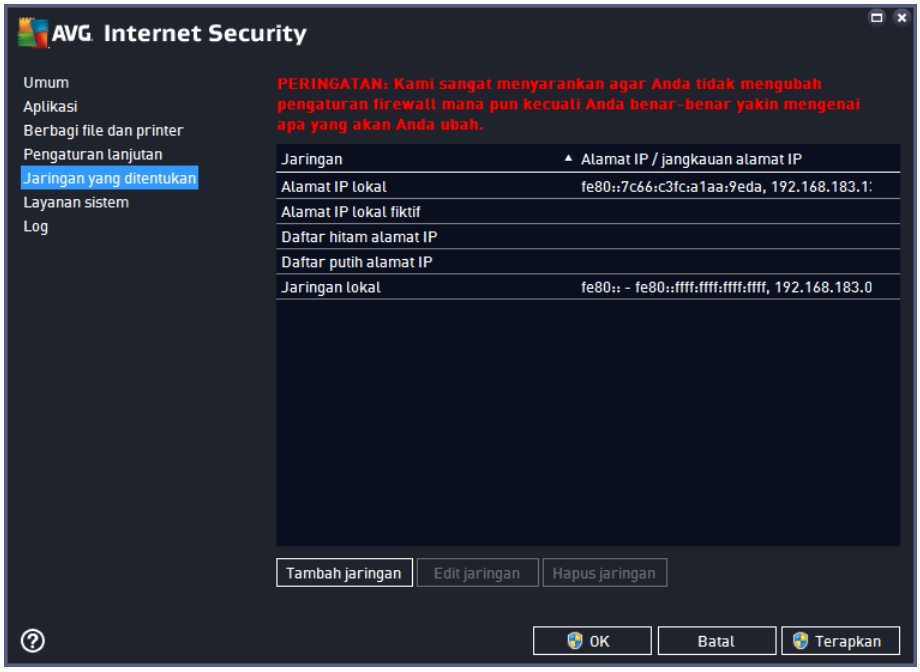
Dialog ***Pengaturan lanjut*** memungkinkan Anda untuk memilih/ menghapus parameter Firewall berikut ini:

- ***Mengizinkan lalu lintas dari/ke mesin virtual yang didukung oleh firewall*** – dukungan untuk koneksi jaringan pada mesin virtual seperti VMware.
- ***Mengizinkan semua lalu lintas ke jaringan pribadi virtual (Virtual Private Networks/VPN)*** – dukungan untuk koneksi VPN *(digunakan untuk tersambung ke komputer jarak jauh)*.
- ***Membuat log untuk lalu lintas masuk/ keluar tak dikenal*** – semua percobaan komunikasi *(masuk/ keluar)* oleh aplikasi tak dikenal akan dicatat pada log Firewall.
- ***Nonaktifkan verifikasi aturan untuk semua aturan aplikasi*** – Firewall terus-menerus memonitor semua file yang dicakup oleh tiap aturan aplikasi. Bila modifikasi pada file biner terjadi, Firewall sekali lagi akan mengkonfirmasi kredibilitas aplikasi dengan langkah-langkah standar, yaitu memverifikasi sertifikat, mencarinya di dalam database aplikasi terpercaya, dll. Jika aplikasi tidak dapat dianggap aman, Firewall selanjutnya akan memperlakukan aplikasi berdasarkan mode yang dipilih:
  - jika Firewall berjalan di ***mode Otomatis***, aplikasi akan diizinkan, secara default;
  - jika Firewall berjalan di ***mode Interaktif***, aplikasi akan diblokir, dan dialog pemberitahuan akan muncul meminta pengguna memutuskan cara aplikasi diperlakukan.

Prosedur yang diinginkan tentang cara memperlakukan aplikasi tertentu dapat ditentukan untuk tiap aplikasi secara terpisah di dalam dialog Aplikasi.

3.8.5. Jaringan yang ditentukan

Editing yang ada pada dialog jaringan yang Ditetapkan ditujukan untuk PENGGUNA YANG BERPENGALAMAN SAJA!



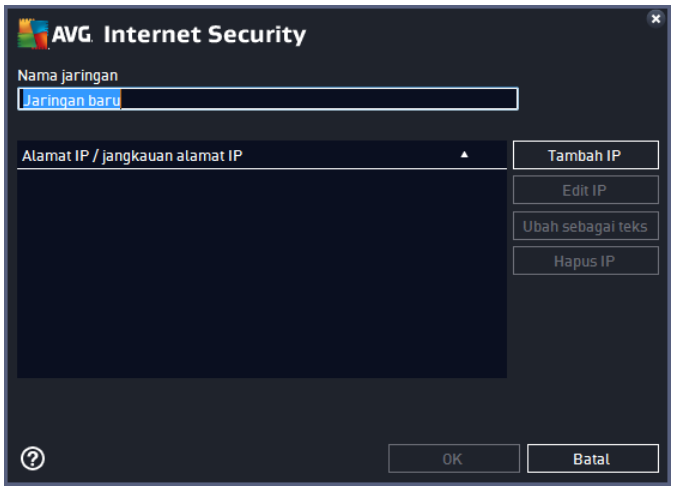
Dialog ***Jaringan yang ditetapkan*** menyediakan daftar semua jaringan yang terhubung ke komputer Anda. Daftar

ini memberikan informasi berikut mengenai setiap jaringan yang terdeteksi:

- ***Jaringan*** – menyediakan daftar nama semua jaringan ke mana komputer terhubung.
- ***Kisaran alamat IP*** – setiap jaringan akan dideteksi secara otomatis dan ditetapkan dalam bentuk kisaran alamat IP.

Tombol kontrol

- ***Tambah jaringan*** – membuka jendela dialog baru di mana Anda dapat mengedit parameter untuk jaringan yang baru saja ditetapkan, yaitu memberikan ***nama Jaringan*** dan menetapkan ***kisaran alamat IP***:



- ***Edit jaringan*** – membuka jendela dialog ***Properti jaringan*** (*lihat di atas*) di mana Anda dapat mengedit berbagai parameter jaringan yang sudah ditetapkan (*dialognya sama dengan dialog untuk menambah jaringan baru, lihat keterangan dalam paragraf sebelumnya*).
- ***Hapus jaringan*** – menghapus referensi jaringan yang dipilih dari daftar jaringan.

3.8.6. Layanan sistem

Segala pengeditan dalam dialog Layanan sistem dan protokol ditujukan untuk PENGGUNA BERPENGALAMAN SAJA!

Dialog ***Layanan sistem dan protokol*** menampilkan daftar layanan sistem dan protokol standar Windows yang mungkin perlu berkomunikasi melalui jaringan. Bagan ini berisi kolom berikut:

- ***Layanan sistem dan protokol*** – Kolom ini menampilkan nama masing-masing layanan sistem.
- ***Tindakan*** – Kolom ini menampilkan ikon untuk tindakan yang ditetapkan:
  - o Memungkinkan komunikasi untuk semua jaringan
  - o Blokir komunikasi

Untuk mengedit pengaturan suatu item dalam daftar ini (*termasuk tindakan yang ditetapkan*), klik kanan pada item tersebut dan pilih ***Edit***. ***Akan tetapi, pengeditan aturan sistem hanya boleh dilakukan oleh pengguna mahir; sangat tidak disarankan mengedit aturan sistem!***

Aturan sistem yang ditentukan pengguna

Untuk membuka dialog baru bagi penentuan aturan layanan sistem Anda (*lihat gambar di bawah*), tekan tombol ***Atur aturan sistem pengguna***. Dialog yang sama akan terbuka jika Anda memutuskan untuk mengedit konfigurasi item yang telah ada dalam layanan sistem dan daftar protokol. Bagian atas dari dialog ini menampilkan gambaran umum semua perincian aturan sistem yang saat ini diedit, sedangkan bagian bawah menampilkan perincian yang dipilih. Perincian aturan dapat diedit, ditambahkan, atau dihapus oleh tombol terkait:

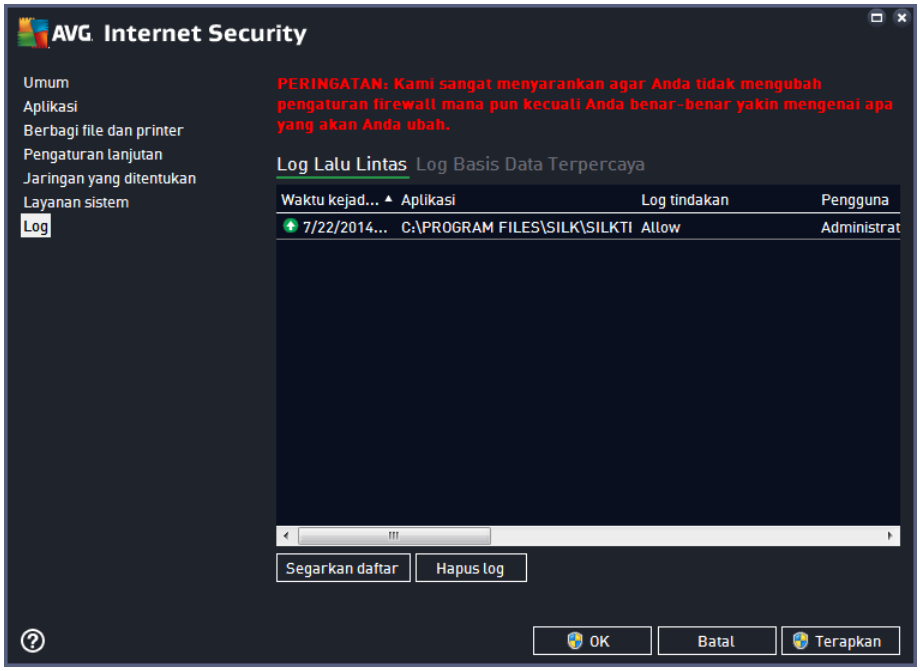
Perhatikan bahwa pengaturan aturan terperinci ini sifatnya tingkat lanjut dan ditujukan terutama bagi administrator jaringan yang memerlukan kontrol penuh atas konfigurasi Firewall. Jika Anda tidak mengerti mengenai tipe protokol komunikasi, nomor port jaringan, definisi alamat IP, dll., jangan memodifikasi pengaturan ini! Jika Anda benar-benar perlu mengubah konfigurasi, harap lihat file dialog bantuan terkait untuk perincian spesifik.

3.8.7. Log

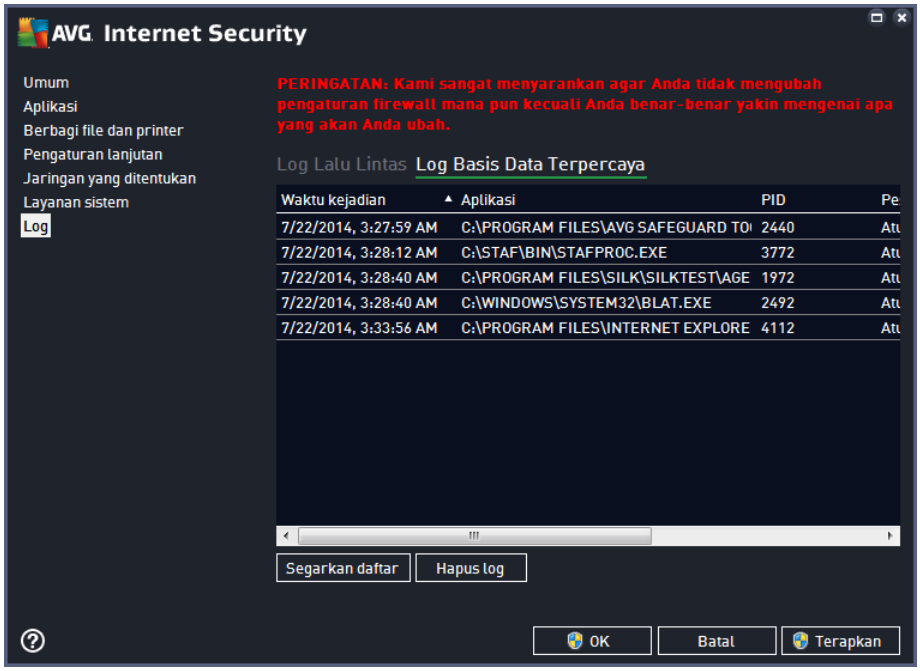
Editing yang ada pada dialog Log ditujukan untuk PENGGUNA YANG BERPENGALAMAN SAJA!

Dialog ***Log*** memungkinkan Anda meninjau daftar semua tindakan dan kejadian di Firewall yang terekam dalam log bersama keterangan terperinci mengenai parameter yang relevan yang ditampilkan dalam dua tab:

- ***Log Lalu Lintas*** – Tab ini memberikan informasi mengenai aktivitas dari semua aplikasi yang telah mencoba terhubung ke jaringan. Untuk setiap item, Anda akan menemukan informasi tentang waktu kejadian, nama aplikasi, tindakan log terkait, nama pengguna, PID, arah lalu lintas, tipe protokol, jumlah port lokal dan jauh, serta informasi mengenai alamat IP lokal dan jauh.



- ***Log Basis Data Terpercaya*** – *Basis data terpercaya* adalah basis data internal AVG untuk mengumpulkan informasi mengenai aplikasi yang disertifikasi dan dipercaya yang selalu diperbolehkan untuk berkomunikasi secara online. Saat suatu aplikasi baru pertama kali mencoba menghubungkan ke jaringan (*yakni pada saat belum ada aturan firewall yang ditetapkan untuk aplikasi ini*), perlu dicari tahu apakah komunikasi jaringan diperbolehkan untuk aplikasi tersebut. Pertama, AVG menelusuri *Basis data terpercaya*, dan jika aplikasi tersebut terdaftar, maka ia akan diberi akses ke jaringan secara otomatis. Hanya setelah itulah, bila tidak ada informasi mengenai aplikasi ini yang tersedia dalam basis data, Anda akan ditanyai dalam dialog mandiri apakah Anda mau memperbolehkan aplikasi tersebut mengakses jaringan.



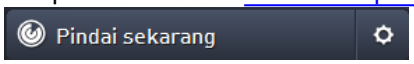
Tombol kontrol

- ***Segarkan daftar*** – semua parameter yang terekam dalam log dapat disusun menurut atribut yang dipilih: secara kronologis (*tanggal*) atau menurut abjad (*kolom lainnya*) – tinggal klik judul kolomnya. Gunakan tombol ***Segarkan daftar*** untuk memperbarui informasi yang ditampilkan saat ini.

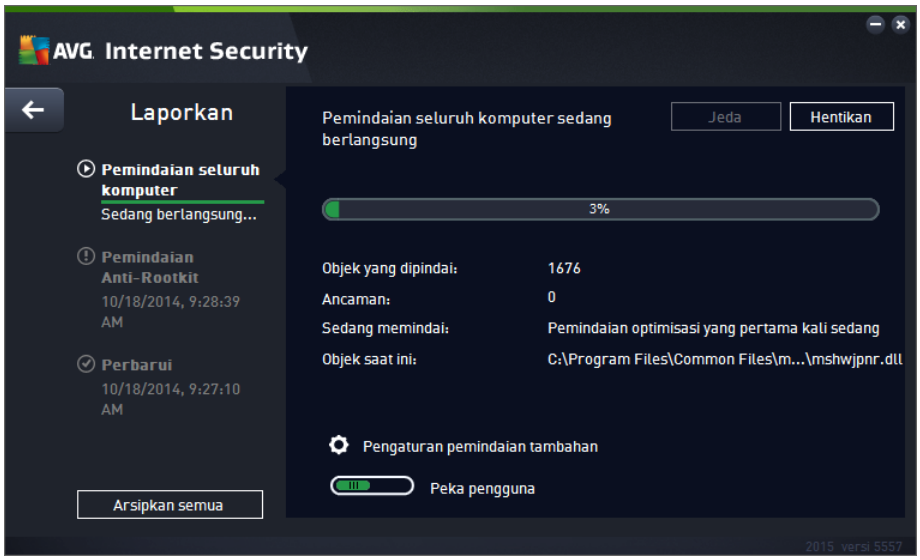
- ***Hapus log*** – tekan untuk menghapus semua entri dalam diagram.

3.9. Pemindaian AVG

Secara default, **AVG Internet Security 2015** tidak menjalankan pemindaian, karena setelah pemindaian awal *(Anda akan ditanya untuk menjalankannya*), Anda harus terlindungi sepenuhnya oleh komponen tetap dari **AVG Internet Security 2015** yang akan selalu menjaga, dan tidak akan membiarkan kode jahat apa pun memasuki komputer Anda. Tentu saja, Anda dapat menjadwalkan pemindaian untuk dijalankan pada interval rutin, atau secara manual menjalankan pemindaian sesuai dengan kebutuhan Anda kapan saja.

Antarmuka pemindaian AVG dapat diakses dari antarmuka pengguna utama melalui tombol yang secara grafis dibagi menjadi dua bagian: 

- ***Pindai sekarang*** – Tekan tombol agar tertaut untuk segera menjalankan Pemindaian seluruh komputer, dan lihat kemajuan serta hasilnya pada jendela Laporan yang terbuka secara otomatis:



- ***Opsi*** – Pilih tombol ini *(secara grafis ditampilkan sebagai tiga garis mendatar dalam kolom hijau)* untuk membuka dialog ***Opsi Pemindaian*** di mana Anda dapat mengatur pemindaian terjadwal dan mengedit parameter Pemindaian seluruh komputer/Pindai file atau folder tertentu.

Dalam dialog ***Opsi Pemindaian***, Anda dapat melihat tiga bagian konfigurasi pemindaian utama:

- ***Atur pemindaian terjadwal*** – Klik opsi ini untuk membuka dialog baru dengan gambaran umum semua jadwal pemindaian. Sebelum Anda menentukan pemindaian Anda sendiri, Anda hanya bisa melihat satu pemindaian terjadwal yang telah ditetapkan oleh vendor perangkat lunak yang tertera dalam diagram. Pemindaian dinonaktifkan, secara default. Untuk mengaktifkannya, klik kanan lalu pilih opsi *Aktifkan tugas* dari menu konteks. Setelah pemindaian terjadwal diaktifkan, Anda bisa mengedit konfigurasinya melalui tombol *Edit jadwal pemindaian*. Anda juga dapat mengeklik tombol *Tambahkan jadwal pemindaian* untuk membuat jadwal pemindaian baru Anda sendiri.

- ***Pemindaian seluruh komputer/Pengaturan*** – Tombol dibagi menjadi dua bagian. Klik opsi *Pemindaian seluruh komputer* untuk segera menjalankan pemindaian seluruh komputer Anda *(untuk perincian tentang pemindaian seluruh komputer, silakan lihat bab yang dimaksud bernama Pemindaian yang ditetapkan/Pemindaian seluruh komputer)*. Mengklik bagian *Pengaturan* akan membawa Anda ke dialog konfigurasi pemindaian seluruh komputer.

- ***Pemindaian seluruh komputer/Pengaturan*** – Lagi, tombol dibagi menjadi dua bagian. Klik opsi *Pindai file atau folder tertentu* untuk segera menjalankan pemindaian bagian tertentu komputer Anda *(untuk perincian tentang pemindaian file atau folder tertentu, silakan lihat bab yang dimaksud yaitu Pemindaian yang ditetapkan/Pindai file atau folder tertentu)*. Mengeklik bagian *Pengaturan* akan membawa Anda ke dialog konfigurasi pemindaian file atau folder tertentu.

- ***Pindai komputer untuk rootkit / Pengaturan*** – Bagian kiri tombol yang bertuliskan *Pindai komputer untuk rootkit* segera menjalankan pemindai anti-rootkit *(untuk rincian tentang pemindaian rootkit, harap baca bab terkait berjudul Pemindaian yang ditentukan sebelumnya / Pindai komputer untuk rootkit).* Mengklik bagian *Pengaturan* kan membawa Anda ke dialog konfigurasi pemindaian rootkit.

3.9.1. Pemindaian Yang Ditetapkan

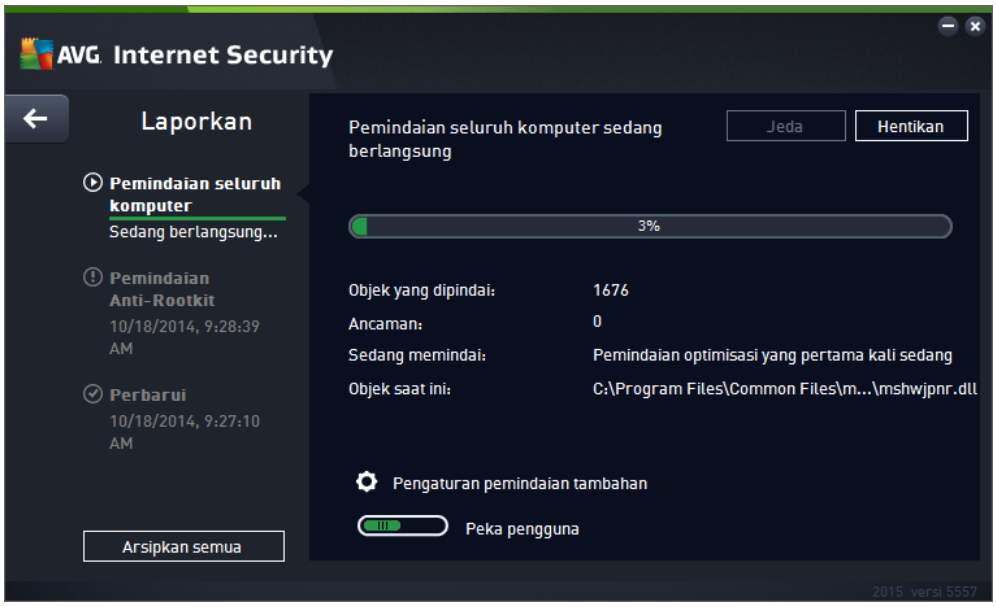
Salah satu fitur utama **AVG Internet Security 2015** adalah pemindaian saat diperlukan. Tes atas permintaan dirancang untuk memindai berbagai bagian komputer Anda bila muncul kecurigaan mengenai kemungkinan infeksi virus. Namun, sangat disarankan untuk melakukan tes demikian secara rutin sekalipun menurut Anda tidak ada virus yang dapat ditemukan pada komputer Anda.

Dalam **AVG Internet Security 2015** Anda akan menemukan tipe pemindaian yang sudah ditentukan oleh vendor perangkat lunak berikut in:

Pemindaian seluruh komputer memindai seluruh komputer Anda untuk mencari kemungkinan infeksi dan/atau program yang mungkin tidak diinginkan. Tes ini akan memindai semua hard drive di komputer Anda, akan mendeteksi dan memulihkan virus yang ditemukan, atau memindahkan infeksi yang terdeteksi ke Gudang Virus. Pemindaian seluruh komputer Anda harus dijadwalkan pada komputer Anda sedikitnya sekali seminggu.

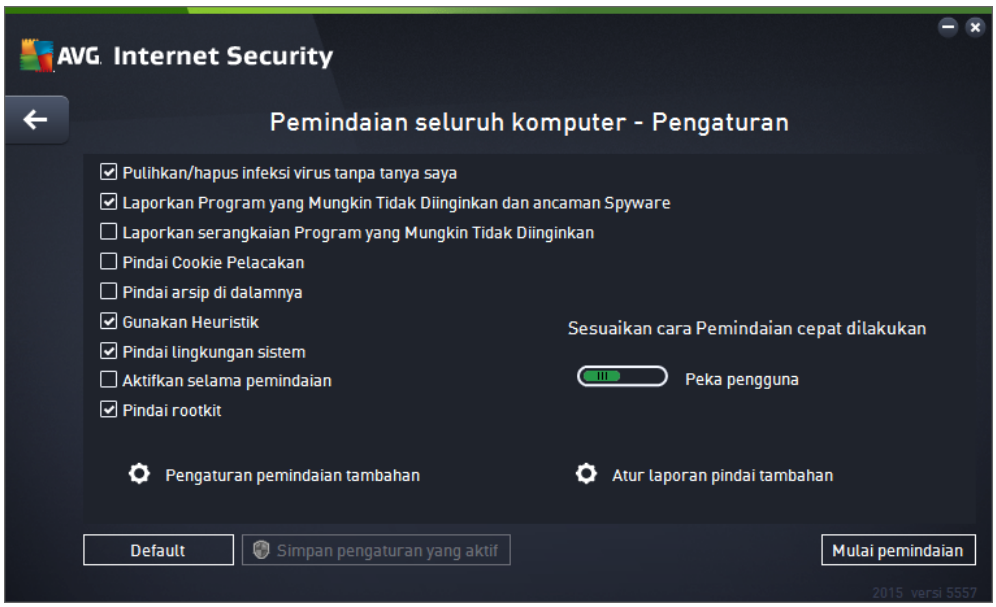
Peluncuran pemindaian

Pemindaian seluruh komputer dapat langsung diluncurkan dari antarmuka pengguna utama dengan mengeklik tombol ***Pindai sekarang***. Tidak ada pengaturan tertentu lainnya yang harus dikonfigurasi untuk tipe pemindaian ini, pemindaian akan segera dimulai. Dalam dialog ***Pemindaian seluruh komputer sedang dijalankan*** (*lihat cuplikan layar*) Anda dapat melihat kemajuan dan hasilnya. Pemindaian dapat dihentikan untuk sementara (***Jeda***) atau dibatalkan (***Hentikan***) jika perlu.



Mengedit konfigurasi pindai

Anda dapat mengedit konfigurasi ***Pemindaian seluruh komputer*** dalam dialog ***Pemindaian seluruh komputer – Pengaturan*** *(dialog ini dapat diakses melalui tautan Pengaturan untuk Pindai seluruh komputer dalam dialog Opsi pemindaian).* ***Anda disarankan untuk tetap menggunakan pengaturan default kecuali ada alasan yang kuat untuk mengubahnya!***



Dalam daftar parameter pemindaian, Anda dapat mengaktifkan/ menonaktifkan parameter tertentu bila diperlukan:

- ***Pulihkan / hapus infeksi virus tanpa bertanya pada saya*** *(diaktifkan secara default)* – Jika ada virus teridentifikasi selama pemindaian, maka virus dapat dipulihkan secara otomatis jika penawarnya tersedia. Jika file yang terinfeksi tidak dapat dipulihkan secara otomatis, objek yang terinfeksi akan dipindahkan ke Gudang Virus.

- ***Laporkan Program yang Mungkin Tidak Diinginkan dan ancaman Spyware*** *(diaktifkan secara default)* – Centang untuk mengaktifkan pemindaian untuk spyware serta virus. Spyware merupakan kategori malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang terinstal secara tidak disengaja. Kami sarankan untuk tetap mengaktifkan fitur ini karena akan meningkatkan keamanan komputer Anda.

- ***Laporkan serangkaian Program yang Mungkin Tidak Diinginkan*** *(dinonaktifkan secara default)* – Tandai untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, tetapi dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, walaupun hal ini dapat memblokir program yang legal, dan karenanya dinonaktifkan secara default.

- ***Pindai Cookie Pelacak*** *(nonaktif secara default)* – Parameter ini menetapkan bahwa cookie harus dideteksi *(cookie HTTP digunakan untuk mengautentikasi, melacak, dan memelihara informasi tertentu tentang pengguna, seperti preferensi situs atau isi kereta belanja elektronik mereka)*.

- ***Pindai arsip di dalamnya*** *(dinonaktifkan secara default)* – Parameter ini menentukan bahwa pemindaian harus memeriksa semua file yang tersimpan dalam arsip, misalnya, ZIP, RAR, ...

- ***Gunakan Heuristik*** *(diaktifkan secara default)* – Analisis heuristik (*emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual*) akan menjadi salah satu metode yang digunakan untuk mendeteksi virus selama pemindaian.

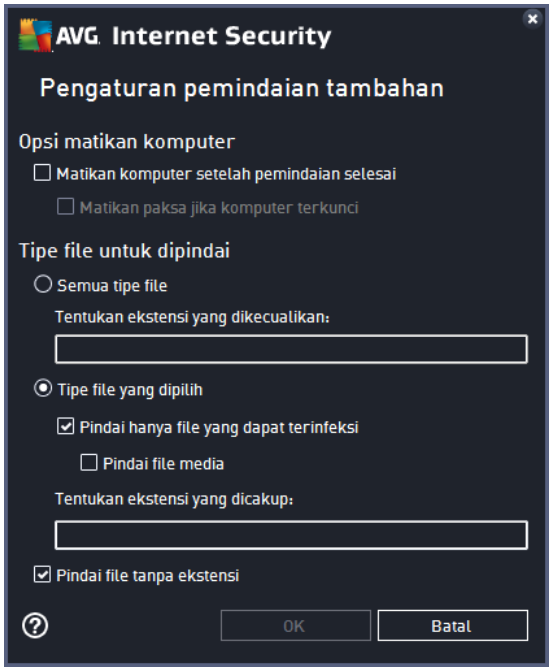
- ***Pindai lingkungan sistem*** *(diaktifkan secara default)* – Pemindaian juga akan memeriksa area sistem komputer Anda.

- ***Aktifkan selama pemindaian*** *(dinonaktifkan secara default)* – Dalam kondisi khusus *(dicurigai bahwa*

komputer Anda terinfeksi) Anda dapat mencentang opsi ini untuk mengaktifkan algoritma pemindaian paling menyeluruh yang akan memindai area yang jarang terinfeksi sekalipun, agar benar-benar merasa yakin. Tetapi harap diingat bahwa metode ini memakan waktu lama.

- ***Pindai rootkit*** *(aktif secara default)* – menyertakan pemindaian anti-rootkit ke dalam pemindaian keseluruhan komputer. The pemindaian anti-rootkit dapat dijalankan secara terpisah.

- ***Pengaturan pindai tambahan*** – tautan ini akan membuka dialog Pengaturan pemindaian tambahan di mana Anda dapat menetapkan parameter berikut:



  - ***Opsi matikan komputer*** – memutuskan apakah komputer akan dimatikan secara otomatis setelah proses pemindaian yang berjalan selesai. Dengan mengkonfirmasi opsi ini (***Matikan komputer setelah pemindaian selesai***), sebuah opsi baru yang diaktifkan akan memungkinkan komputer dimatikan sekalipun saat itu sedang terkunci (***Matikan paksa jika komputer terkunci***).

  - ***Tipe file untuk pemindaian*** – selanjutnya Anda harus memutuskan apakah Anda ingin memindai:

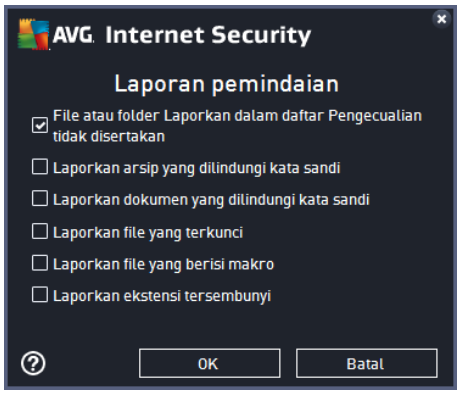
    - ***Semua tipe file*** dengan opsi penentuan pengecualian dari pemindaian dengan memberikan daftar ekstensi file yang dipisah koma, untuk file yang tidak boleh dipindai;

    - ***Tipe file yang dipilih*** – Anda dapat menentukan bahwa Anda hanya ingin memindai file yang dapat terinfeksi (*file yang tidak dapat terinfeksi tidak akan dipindai, misalnya beberapa file teks biasa, atau file yang tidak dapat dijalankan lainnya*), termasuk file media (*file video, audio – jika Anda membiarkan kotak ini tidak dicentang, maka hal ini akan lebih mengurangi waktu pemindaian, karena file ini seringkali terlalu besar dan sangat kecil kemungkinannya untuk terinfeksi virus*). Sekali lagi, Anda dapat menentukan ekstensi file yang harus selalu dipindai.

    - Secara opsional, Anda dapat memutuskan untuk memilih opsi ***Pindai file tanpa ekstensi*** – opsi ini diaktifkan secara default, dan disarankan Anda membiarkannya kecuali Anda memiliki alasan kuat untuk mengubahnya. File tanpa ekstensi cukup mencurigakan dan harus selalu dipindai.

- ***Sesuaikan secepat apa pemindaian selesai*** – Anda dapat menggunakan penggeser untuk mengganti prioritas proses pemindaian. Secara default, nilai opsi ini diatur ke tingkat penggunaan sumber daya otomatis yang *peka pengguna*. Sebagai alternatif, Anda dapat menjalankan proses pemindaian lebih lambat yang berarti beban sumber daya sistem akan diminimumkan (*berguna saat Anda perlu menggunakan komputer tersebut namun Anda tidak peduli berapa lama pemindaian akan berlangsung*), atau lebih cepat dengan kebutuhan sumber daya sistem yang bertambah (*misalnya saat komputer ditinggalkan untuk sementara*).

- ***Atur laporan pindai tambahan*** – tautan ini akan membuka dialog baru ***Laporan pindai*** di mana Anda dapat memilih kemungkinan tipe temuan apa saja yang harus dilaporkan:



Peringatan: *Pengaturan pindai ini sama dengan parameter pemindaian yang baru ditetapkan – seperti diterangkan dalam bab Pemindaian AVG / Menjadwalkan pemindaian/ Cara Memindai. Seandainya Anda harus memutuskan untuk mengubah konfigurasi default* ***Pemindaian seluruh komputer*** *maka Anda dapat menyimpan pengaturan baru sebagai konfigurasi default untuk digunakan bagi semua pemindaian seluruh komputer selanjutnya.*

Pindai File atau Folder Tertentu – hanya memindai area komputer Anda yang telah dipilih untuk dipindai (*folder, hard disk, disket floppy, atau CD yang dipilih, dll.*). Kemajuan pemindaian jika terdeteksi virus dan penyembuhannya sama dengan pemindaian seluruh komputer: virus yang ditemukan akan dipulihkan atau dipindahkan ke Gudang Virus. Pemindaian file atau folder dapat digunakan untuk mengatur tes Anda sendiri dan menjadwalkannya berdasarkan kebutuhan.

Peluncuran pemindaian

Pindai file atau folder tertentu dapat diluncurkan langsung dari dialog Opsi pemindaian dengan mengeklik tombol **Pindai file atau folder tertentu**. Sebuah dialog baru bernama ***Pilih file atau folder tertentu untuk pemindaian*** akan dibuka. Dalam struktur komputer Anda, pilih folder yang ingin Anda pindai. Jalur ke setiap folder yang dipilih akan dibuat secara otomatis dan muncul dalam kotak teks di bagian atas dialog ini. Juga ada opsi pada folder tertentu yang dipindai sementara semua sub foldernya telah dikecualikan dari pemindaian ini; untuk melakukannya ketikkan tanda kurang "**-**" di depan jalur yang telah dibuat secara otomatis (*lihat cuplikan layar*). Untuk mengecualikan seluruh folder dari pemindaian, gunakan tanda "!" parameter. Terakhir, untuk meluncurkan pemindaian, tekan tombol ***Mulai pindai*** ; proses pemindaiannya sendiri pada dasarnya sama dengan Pemindaian seluruh komputer.

Mengedit konfigurasi pindai

Anda dapat mengedit konfigurasi ***Pindai File atau Folder Tertentu*** dalam dialog ***Pindai File atau Folder Tertentu – Pengaturan*** *(dialog ini dapat diakses melalui tautan Pengaturan untuk Pindai file atau folder tertentu di dalam dialog Opsi pemindaian).* ***Anda disarankan untuk tetap menggunakan pengaturan default kecuali ada alasan yang kuat untuk mengubahnya!***

Dalam daftar parameter pemindaian, Anda dapat mengaktifkan/menonaktifkan parameter tertentu bila diperlukan:

- ***Pulihkan / hapus infeksi virus tanpa bertanya pada saya*** *(diaktifkan secara default)*: Jika ada virus terdeteksi selama pemindaian, virus dapat dipulihkan otomatis jika penawarnya tersedia. Jika file yang terinfeksi tidak dapat dipulihkan secara otomatis, objek yang terinfeksi akan dipindahkan ke Gudang Virus.

- ***Laporkan Program yang Mungkin Tidak Diinginkan dan ancaman Spyware*** *(diaktifkan secara default)*: Centang untuk mengaktifkan pemindaian spyware serta virus. Spyware merupakan kategori

malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang terinstal secara tidak sengaja. Kami sarankan untuk tetap mengaktifkan fitur ini karena akan meningkatkan keamanan komputer Anda.

- ***Laporkan serangkaian Program yang Mungkin Tidak Diinginkan*** *(dinonaktifkan secara default)*: Tandai untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, tetapi dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, walaupun hal ini dapat memblokir program yang legal, dan karenanya dinonaktifkan secara default.

- ***Pindai Cookie Pelacak*** *(nonaktif secara default)*: Parameter ini menetapkan bahwa cookie harus dideteksi *(cookie HTTP digunakan untuk mengautentikasi, melacak, dan memelihara informasi tertentu tentang pengguna, seperti preferensi situs atau isi kereta belanja elektronik mereka)*.

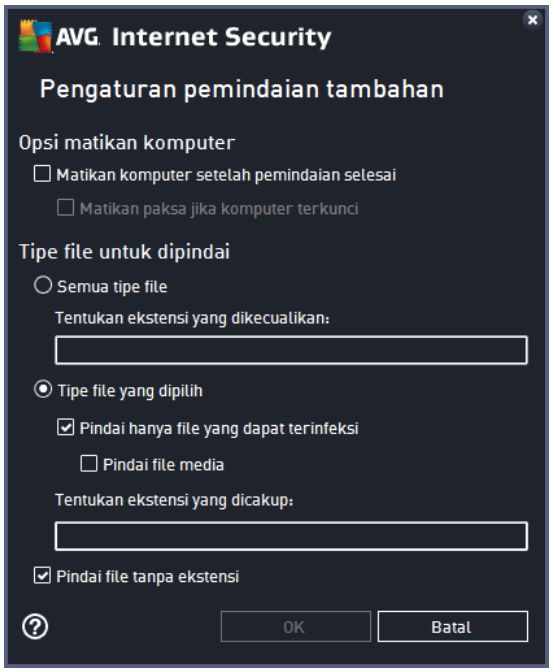
- ***Pindai arsip di dalamnya*** *(diaktifkan secara default)*: Parameter ini menetapkan bahwa pemindaian harus memeriksa semua file sekalipun file tersebut tersimpan dalam arsip, misalnya ZIP, RAR, ...

- ***Gunakan Heuristik*** *(diaktifkan secara default)*: Analisis heuristik *(emulasi dinamis dari petunjuk objek yang dipindaidi lingkungan komputer virtual)* akan menjadi salah satu metode yang digunakan untuk deteksi virus selama pemindaian.

- ***Pindai lingkungan sistem*** *(dinonaktifkan secara default)*: Pemindaian juga akan memeriksa area sistem komputer Anda.

- ***Aktifkan pemindaian menyeluruh*** *(dinonaktifkan secara default)*: Dalam kondisi khusus *(misalnya jika dicurigai bahwa komputer Anda terinfeksi)* Anda dapat menandai opsi ini untuk mengaktifkan algoritma pemindaian paling menyeluruh yang akan memindai area paling sulit terinfeksi sekalipun di komputer Anda, agar benar-benar merasa yakin. Tetapi harap diingat bahwa metode ini memakan waktu lama.

- ***Pengaturan pindai tambahan*** – Tautan ini akan membuka dialog ***Pengaturan pindai tambahan*** di mana Anda dapat menentukan parameter berikut:



- ***Opsi matikan komputer*** – memutuskan apakah komputer akan dimatikan secara otomatis setelah proses pemindaian yang berjalan selesai. Dengan mengkonfirmasi opsi ini (***Matikan komputer setelah pemindaian selesai***), sebuah opsi baru yang diaktifkan akan memungkinkan komputer dimatikan sekalipun saat itu sedang terkunci (***Matikan paksa jika komputer terkunci***).

- ***Tipe file untuk pemindaian*** – selanjutnya Anda harus memutuskan apakah Anda ingin memindai:

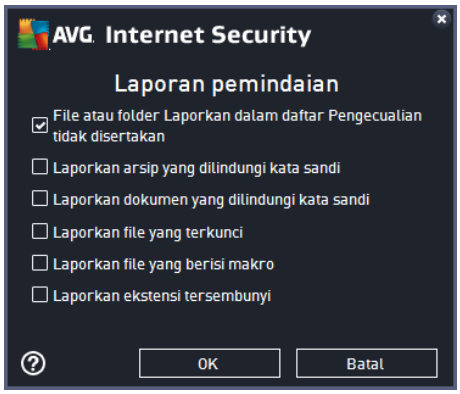
  - ***Semua tipe file*** dengan opsi penentuan pengecualian dari pemindaian dengan memberikan daftar ekstensi file yang dipisah koma, untuk file yang tidak boleh dipindai;

  - ***Tipe file yang dipilih*** – Anda dapat menentukan bahwa Anda hanya ingin memindai file yang dapat terinfeksi (*file yang tidak dapat terinfeksi tidak akan dipindai, misalnya beberapa file teks biasa, atau file yang tidak dapat dijalankan lainnya*), termasuk file media (*file video, audio – jika Anda membiarkan kotak ini tidak dicentang, maka hal ini akan lebih mengurangi waktu pemindaian, karena file ini seringkali terlalu besar dan sangat kecil kemungkinannya untuk terinfeksi virus*). Sekali lagi, Anda dapat menentukan ekstensi file yang harus selalu dipindai.

  - Secara opsional, Anda dapat memutuskan untuk memilih opsi ***Pindai file tanpa ekstensi*** – opsi ini diaktifkan secara default, dan disarankan Anda membiarkannya kecuali Anda memiliki alasan kuat untuk mengubahnya. File tanpa ekstensi cukup mencurigakan dan harus selalu dipindai.

- ***Sesuaikan secepat apa pemindaian selesai*** – Anda dapat menggunakan penggeser untuk mengganti prioritas proses pemindaian. Secara default, nilai opsi ini diatur ke tingkat penggunaan sumber daya otomatis yang *peka pengguna*. Sebagai alternatif, Anda dapat menjalankan proses pemindaian lebih lambat yang berarti beban sumber daya sistem akan diminimumkan (*berguna saat Anda perlu menggunakan komputer tersebut namun Anda tidak peduli berapa lama pemindaian akan berlangsung*), atau lebih cepat dengan kebutuhan sumber daya sistem yang bertambah (*misalnya saat komputer ditinggalkan untuk sementara*).

- ***Atur laporan pindai tambahan*** – tautan ini akan membuka dialog baru ***Laporan Pindai*** di mana Anda dapat memilih tipe temuan yang berpotensi untuk dilaporkan:

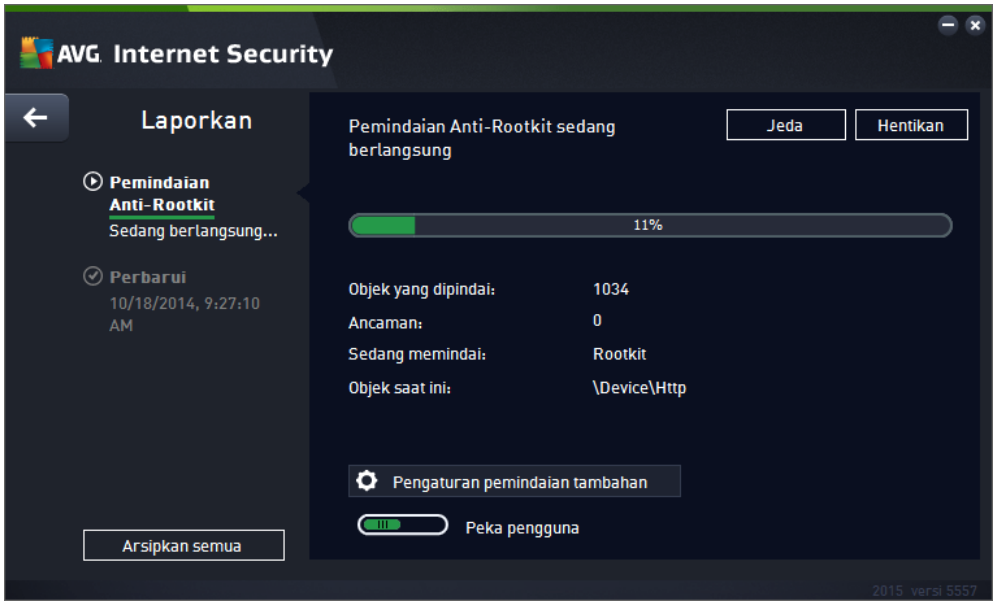


Peringatan: *Pengaturan pindai ini sama dengan parameter pemindaian yang baru ditetapkan – seperti diterangkan dalam bab Pemindaian AVG / Menjadwalkan pemindaian/ Cara Memindai. Seandainya Anda harus memutuskan untuk mengubah konfigurasi default* ***Pindai file atau folder tertentu*** *maka Anda dapat menyimpan pengaturan baru sebagai konfigurasi default untuk digunakan bagi semua pemindaian file atau folder selanjutnya. Selain itu, konfigurasi ini akan digunakan sebagai template bagi semua pemindaian yang baru Anda jadwalkan (semua pemindaian khusus berdasarkan pada konfigurasi saat ini pada Pindai file atau folder yang dipilih).*

Pindai komputer untuk rootkit mendeteksi dan menghilangkan rootkit berbahaya secara efektif, misalnya program dan teknologi yang dapat menyamarkan kehadiran perangkat lunak jahat pada komputer Anda. Rootkit dirancang untuk mengambil alih kontrol utama pada sistem komputer, tanpa seizin pemilik sistem dan manajer yang berwenang. Pemindaian ini mampu mendeteksi rootkit berdasarkan seperangkat aturan yang ditentukan. Jika rootkit ditemukn, bukan berarti rootkit terinfeksi. Kadang, rootkit digunakan sebagai driver atau bagian dari aplikasi yang benar.

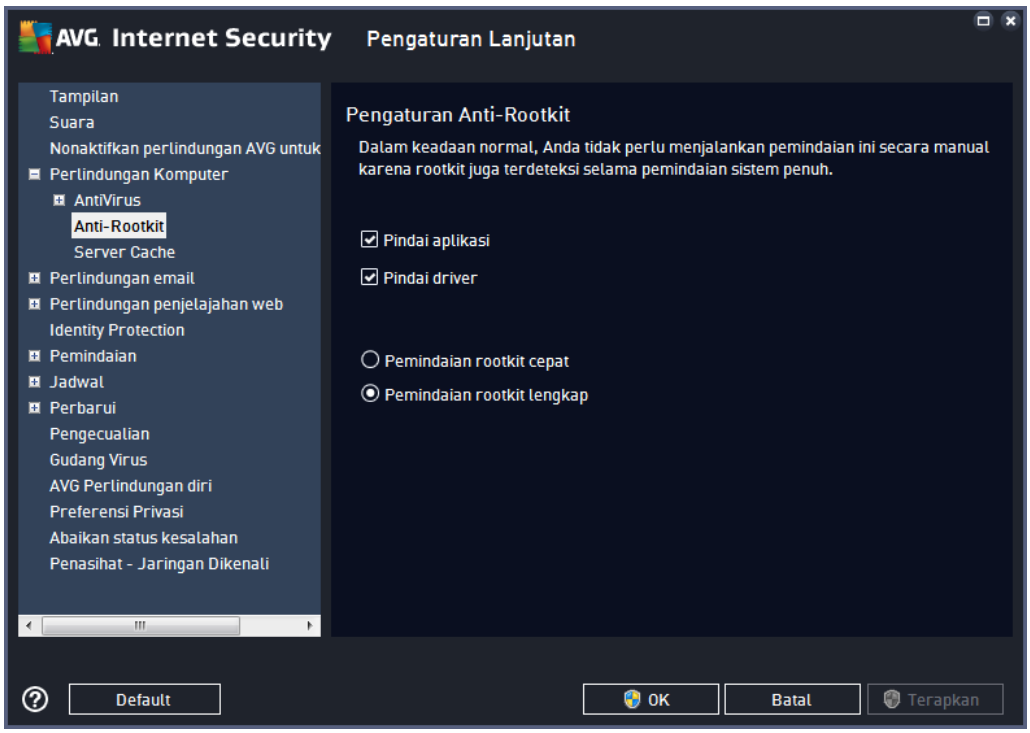
Peluncuran pemindaian

Pindai komputer untuk rootkit dapat dijalankan dari dialog Opsi pemindaian dengan mengklik tombol ***Pindai komputer untuk rootkit***. Dialog baru berjudul ***Pemindaian anti-rootkit sedang berlangsung*** terbuka menunjukkan progres pemindaian yang dijalankan:



Mengedit konfigurasi pindai

Anda dapat mengedit konfigurasi pemindaian Anti-Rootkit di dalam dialog ***Pengaturan Anti-Rootkit*** *(dialog ini dapat diakses melalui tautan Pengaturan untuk Pemindaian Anti-Rootkit di dalam dialog Opsi pemindaian).* ***Anda disarankan untuk tetap menggunakan pengaturan default kecuali ada alasan yang kuat untuk mengubahnya!***

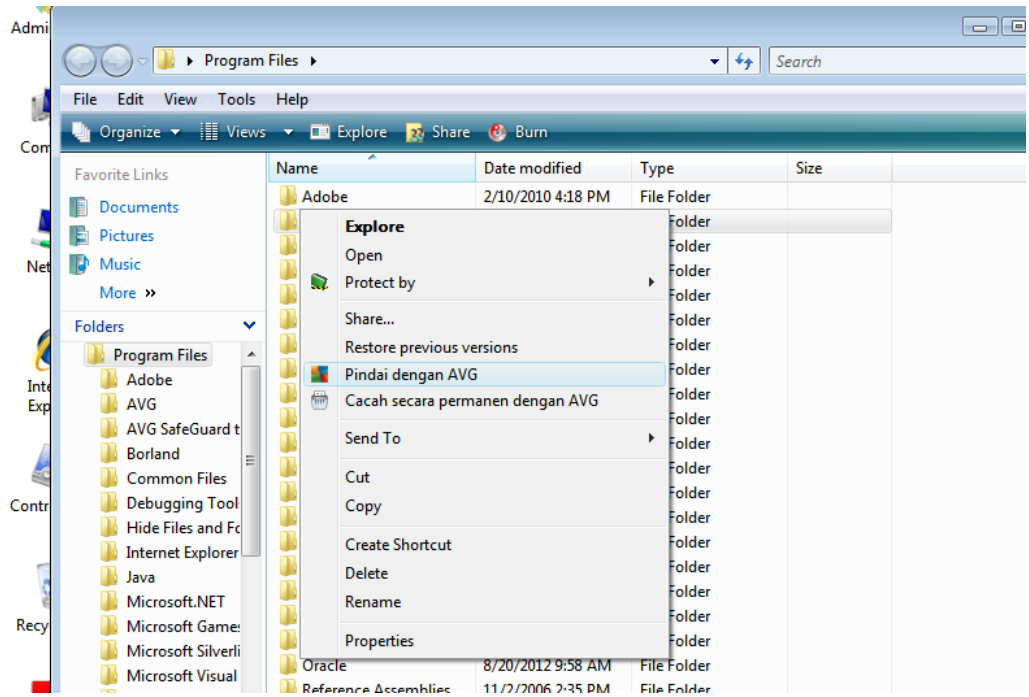


Pindai aplikasi dan ***Pindai driver*** memungkinkan Anda menetapkan secara terperinci apa yang harus disertakan dalam pemindaian anti-rootkit. Pengaturan ini ditujukan untuk pengguna mahir; kami sarankan untuk tetap mengaktifkan semua opsi. Anda juga dapat memilih mode pemindaian rootkit:

- ***Pemindaian rootkit cepat*** – memindai semua proses yang berjalan, driver yang dimuat dan folder sistem (*biasanya c:\Windows*)
- ***Pemindaian rootkit lengkap*** – memindai semua proses yang berjalan, driver yang dimuat, folder sistem (*biasanya c:\Windows*), ditambah semua disk lokal (*flash-disk, namun tidak termasuk floppy-disk/drive CD*)

3.9.2. Memindai dalam Windows Explorer

Di samping pemindaian yang telah ditetapkan, yang diluncurkan untuk seisi komputer atau area yang dipilih, **AVG Internet Security 2015** juga menyediakan opsi untuk pemindaian cepat atas objek tertentu secara langsung di lingkungan Windows Explorer. Jika Anda ingin membuka file tidak dikenal dan Anda tidak bisa memastikan isinya, Anda mungkin perlu memeriksanya bila diperlukan. Ikuti langkah-langkah ini:



- Dalam Windows Explorer, sorot file *(atau folder)* yang ingin Anda periksa
- Klik kanan mouse Anda di atas objek untuk membuka menu konteks
- Pilih opsi ***Pindai dengan AVG*** agar file dipindai dengan **AVG Internet Security 2015**

3.9.3. Pemindaian Baris Perintah

Dalam **AVG Internet Security 2015** ada opsi untuk menjalankan pemindaian dari baris perintah. Anda dapat menggunakan opsi ini untuk kejadian di server, atau saat membuat skrip batch yang akan diluncurkan secara otomatis setelah komputer melakukan boot. Dari baris perintah, Anda dapat meluncurkan pemindaian bersama sebagian besar parameter yang ditawarkan dalam antarmuka pengguna grafis AVG.

Untuk meluncurkan pemindaian AVG dari baris perintah, jalankan perintah berikut dalam folder di mana AVG terinstal:

- ***avgscanx*** untuk OS 32 bit
- ***avgscana*** untuk OS 64 bit

Sintaksis perintah

Sintaksis perintah mengikuti:

- ***avgscanx /parameter*** ... misalnya, ***avgscanx /comp*** untuk memindai seisi komputer
- ***avgscanx /parameter /parameter*** ... dengan beberapa parameter sekaligus, ini harus ditempatkan dalam satu baris dan dipisahkan dengan spasi serta karakter garis miring
- jika parameter mengharuskan diberikannya nilai tertentu (seperti ***/scan*** yang memerlukan informasi mengenai pemilihan area pada komputer yang akan dipindai, maka Anda harus memberikan jalur yang

persis ke bagian yang dipilih tersebut), nilai-nilainya dipisahkan dengan titik koma, sebagai contoh: ***avgscanx /scan=C:\;D:***

Parameter pemindaian

Untuk menampilkan tinjauan umum seluruh parameter yang tersedia, ketikkan perintah tersebut dengan parameter /? atau /HELP (mis. ***avgscanx /?***). Satu-satunya parameter wajib adalah /SCAN untuk menentukan area komputer yang harus dipindai. Untuk penjelasan lebih lanjut mengenai opsi ini, lihat tinjauan umum parameter baris perintah.

Untuk menjalankan pemindaian, tekan ***Enter***. Selama pemindaian, Anda dapat menghentikan proses dengan menggunakan ***Ctrl+C*** atau ***Ctrl+Pause***.

Pemindaian CMD diluncurkan dari antarmuka grafis

Bila Anda menjalankan komputer dalam Safe Mode di Windows, ada juga opsi untuk meluncurkan pemindaian baris perintah dari antarmuka pengguna grafis. Pemindaiannya sendiri akan diluncurkan dari baris perintah, dialog ***Penyusun Baris Perintah*** hanya memungkinkan Anda menentukan sebagian besar parameter pemindaian dalam antarmuka grafis yang mudah.

Berhubung dialog ini hanya dapat diakses dalam Safe Mode di Windows, untuk melihat keterangan terperinci mengenai dialog ini bacalah file bantuan yang dibuka langsung dari dialog.

Kemudian diikuti daftar semua parameter yang tersedia untuk pemindaian baris perintah:

- /SCAN Pindai file atau folder tertentu */SCAN=path;path (misalnya /SCAN=C:\;D:\)*
- /COMP Pemindaian seluruh Komputer
- /HEUR Gunakan analisis heuristik
- /EXCLUDE Kecualikan jalur atau file dari pemindaian
- /@ File perintah /nama file/
- /EXT Pindai ekstensi ini /misalnya EXT=EXE,DLL/
- /NOEXT Jangan pindai ekstensi ini /misalnya NOEXT=JPG/
- /ARC Pindai arsip
- /CLEAN Bersihkan secara otomatis
- /TRASH Pindahkan file terinfeksi ke Gudang Virus
- /QT Pengujian cepat
- /LOG Buat file hasil pemindaian
- /MACROW Laporkan makro

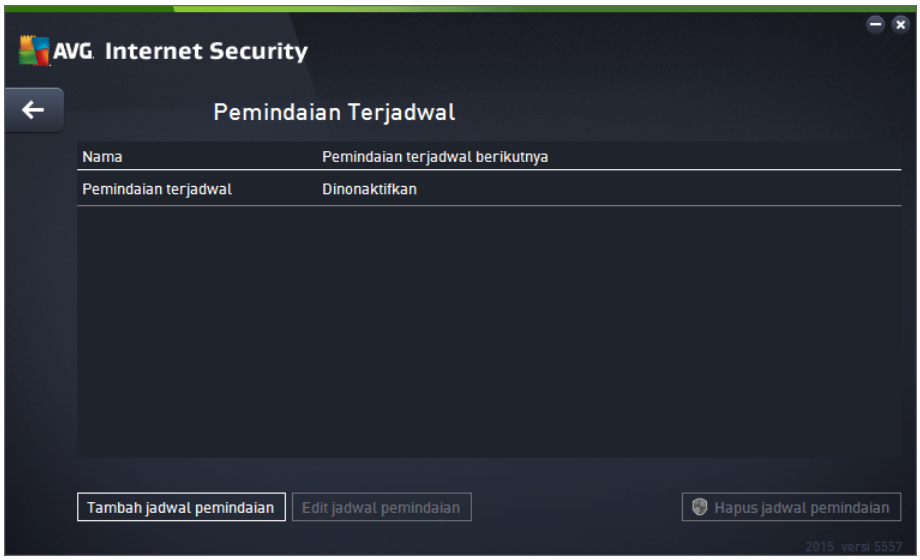
- /PWDW Laporkan file yang dilindungi kata sandi
- /ARCBOMBSW Laporkan bom arsip *(arsip yang dikompresi secara berulang kali)*
- /IGNLOCKED Abaikan file terkunci
- /REPORT Laporkan ke file /nama file/
- /REPAPPEND Tambahkan ke file laporan
- /REPOK Laporkan file yang tidak terinfeksi sebagai OK
- /NOBREAK Jangan perbolehkan CTRL-BREAK untuk menggugurkan
- /BOOT Aktifkan pemeriksaan MBR/BOOT
- /PROC Pindai proses aktif
- /PUP Laporkan Program yang mungkin tidak diinginkan
- /PUPEXT Laporkan serangkaian Program yang mungkin tidak diinginkan
- /REG Pindai register
- /COO Pindai cookie
- /? Tampilkan bantuan untuk topik ini
- /HELP Tampilkan bantuan untuk topik ini
- /PRIORITY Atur prioritas pindai /Low, Auto, High/ *(lihat Pengaturan lanjutan/Pemindaian)*
- /SHUTDOWN Matikan komputer setelah pemindaian selesai
- /FORCESHUTDOWN Matikan paksa komputer setelah pemindaian selesai
- /ADS Pindai Aliran Data Alternatif *(hanya NTFS)*
- /HIDDEN Laporkan file dengan ekstensi tersembunyi
- /INFECTABLEONLY Pindai file dengan ekstensi terinfeksi saja
- /THOROUGHSCAN Aktifkan pemindaian menyeluruh
- /CLOUDCHECK Periksa positif palsu
- /ARCBOMBSW Laporkan file arsip yang dikompresi ulang

3.9.4. Penjadwalan Pemindaian

Dengan **AVG Internet Security 2015** Anda dapat menjalankan pemindaian saat diperlukan *(misalnya saat Anda mencurigai adanya infeksi yang terbawa ke komputer Anda)* atau berdasarkan rencana yang telah dijadwalkan. Sangat disarankan untuk menjalankan pemindaian berdasarkan jadwal: dengan cara ini Anda dapat memastikan

komputer terlindung dari segala kemungkinan terinfeksi, dan Anda tidak perlu memikirkan apakah telah meluncurkan dan kapan meluncurkan pemindaian. Anda harus meluncurkan Pemindaian Seisi Komputer secara rutin, sedikitnya sekali seminggu. Walau demikian, jika memungkinkan, luncurkan pemindaian seisi komputer Anda setiap hari – sebagaimana diatur dalam konfigurasi default jadwal pemindaian. Jika komputer "selalu dihidupkan" maka Anda dapat menjadwalkan pemindaian di luar jam kerja. Jika komputer kadang dimatikan, maka pemindaian jadwal akan terjadi saat komputer dihidupkan bila tugas tersebut telah lewat.

Jadwal pemindaian dapat dibuat/diedit pada dialog ***Pemindaian terjadwal*** yang dapat diakses melalui tombol ***Atur pemindaian terjadwal*** di dalam dialog Opsi pemindaian. Pada dialog ***Pemindaian Terjadwal*** yang baru, Anda dapat melihat gambaran umum lengkap mengenai semua pemindaian terjadwal saat ini:



Pada dialog ini Anda dapat menentukan pemindaian Anda sendiri. Gunakan tombol ***Tambah jadwal pemindaian*** untuk membuat jadwal pemindaian baru Anda sendiri. Parameter pemindaian yang telah dijadwalkan dapat diedit (*atau jadwal baru yang telah diatur*) pada ketiga tab:

- Jadwal
- Pengaturan
- Lokasi

Pada setiap tab Anda cukup dapat beralih ke tombol "lalu lintas" untuk menonaktifkan sementara tes terjadwal, dan diaktifkan kembali bila diperlukan.

Di bagian atas tab ***Jadwal*** Anda akan menemukan kolom teks tempat Anda dapat menetapkan nama jadwal pemindaian yang saat ini sedang ditentukan. Cobalah selalu gunakan nama pemindaian yang singkat, deskriptif dan sesuai agar mudah membedakan pemindaian tersebut nanti dari jadwal lain. Misalnya, tidaklah tepat untuk memberi nama pemindaian dengan "Pemindaian baru" atau "Pindaianku" karena nama tersebut tidak menunjukkan apa yang sebenarnya diperiksa oleh pemindaian tersebut. Sebaliknya, sebuah contoh nama deskriptif yang baik misalnya "Pemindaian area sistem", dll.

Dalam dialog ini, Anda dapat menentukan lebih lanjut parameter pemindaian berikut:

- ***Jadwal berjalan*** – Di sini, Anda dapat menetapkan interval waktu untuk peluncuran pemindaian yang baru dijadwalkan. Penentuan waktu dapat ditentukan melalui peluncuran pembaruan yang berulang setelah periode waktu tertentu *(Jalankan setiap ...)* atau dengan menentukan tanggal dan waktu yang pasti *(Jalankan pada waktu tertentu)*, atau mungkin dengan menentukan kejadian yang akan dikaitkan dengan peluncuran pembaruan *(Jalankan saat menghidupkan komputer)*.

- ***Opsi jadwal lanjutan*** – Di bagian ini Anda dapat menentukan dalam kondisi apa pemindaian harus/tidak boleh diluncurkan jika komputer dalam mode daya rendah atau dimatikan sama sekali. Setelah pemindaian terjadwal diluncurkan pada waktu yang ditetapkan, Anda akan diberi tahu mengenai hal ini melalui jendela sembul yang dibuka lewat ikon baki sistem AVG. Sebuah ikon baki sistem AVG yang beru kemudian muncul (dengan penuh warna bersama sinar berkedip) yang memberi tahu adanya pemindaian terjadwal yang sedang dijalankan. Klik kanan pada ikon pemindaian AVG yang sedang berjalan untuk membuka konteks menu yang dapat Anda gunakan untuk memutuskan akan melakukan jeda atau bahkan menghentikan pemindaian yang sedang berjalan, dan juga mengubah prioritas pemindaian yang sedang berjalan saat itu.

Kontrol pada dialog

- ***Simpan*** – Menyimpan semua perubahan yang telah dilakukan pada tab ini atau tab lain pada dialog ini, dan kembali ke gambaran umum Pemindaian terjadwal. Dengan demikian, jika Anda ingin mengkonfigurasi parameter tes pada semua tab, tekan tombol untuk menyimpannya hanya setelah Anda menentukan semua persyaratan.

- – Gunakan tanda panah hijau di bagian kiri atas dialog untuk kembali ke gambaran umum Pemindaian terjadwal.

Di bagian atas tab ***Pengaturan*** Anda akan menemukan kolom teks tempat Anda dapat menetapkan nama jadwal pemindaian yang saat ini sedang ditentukan. Cobalah selalu gunakan nama pemindaian yang singkat, deskriptif dan sesuai agar mudah membedakan pemindaian tersebut nanti dari jadwal lain. Misalnya, tidaklah tepat untuk memberi nama pemindaian dengan "Pemindaian baru" atau "Pindaianku" karena nama tersebut tidak menunjukkan apa yang sebenarnya diperiksa oleh pemindaian tersebut. Sebaliknya, sebuah contoh nama deskriptif yang baik misalnya "Pemindaian area sistem", dll.

Pada tab ***Pengaturan*** Anda akan menemukan daftar parameter pemindaian yang secara opsional dapat diaktifkan/dinonaktifkan. ***Kecuali Anda mempunyai alasan yang kuat untuk mengubah pengaturan ini, kami menyarankan untuk tetap menggunakan konfigurasi yang sudah ditetapkan***:

- ***Pulihkan/ hapus infeksi virus tanpa bertanya pada saya*** *(diaktifkan secara default):* jika virus teridentifikasi selama pemindaian, maka dapat dipulihkan secara otomatis jika penawarnya tersedia. Jika file yang terinfeksi tidak dapat dipulihkan secara otomatis, objek yang terinfeksi akan dipindahkan ke Gudang Virus.

- ***Laporkan program yang mungkin tidak diinginkan dan ancaman spyware*** *(diaktifkan secara default):* centang untuk mengaktifkan pemindaian spyware serta virus. Spyware merupakan kategori malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang terinstal secara tidak disengaja. Kami sarankan untuk tetap mengaktifkan fitur ini karena akan meningkatkan keamanan komputer Anda.

- ***Laporkan serangkaian program yang mungkin tidak diinginkan*** (*dinonaktifkan secara default*): tandai untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, tetapi dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, walaupun hal ini dapat memblokir program yang legal, dan karenanya dinonaktifkan secara default.

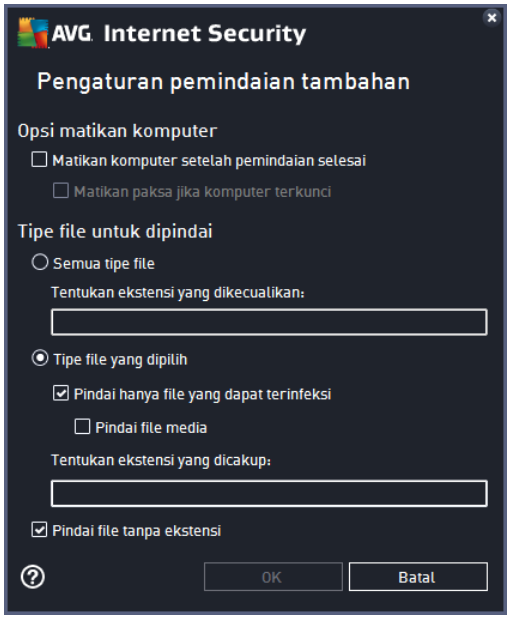
- ***Pindai cookie pelacakan*** (*dinonaktifkan secara default*): parameter ini menetapkan bahwa cookie harus

dideteksi selama pemindaian; (*cookie HTTP digunakan untuk mengautentikasi, melacak, dan memelihara informasi tertentu tentang pengguna, seperti preferensi situs atau isi kereta belanja elektronik mereka*).

- ***Pindai arsip di dalamnya*** (*dinonaktifkan secara default*): parameter ini menetapkan bahwa pemindaian harus memeriksa semua file bahkan jika tersimpan di dalam arsip, misalnya ZIP, RAR, ...
- ***Gunakan heuristik*** (*diaktifkan secara default*): analisis heuristik (*emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual*) akan menjadi salah satu metode yang digunakan untuk deteksi virus selama pemindaian.
- ***Pindai lingkungan sistem*** (*diaktifkan secara default*): pemindaian juga akan memeriksa area sistem komputer Anda.
- ***Aktifkan selama pemindaian*** (*dinonaktifkan secara default):* dalam kondisi khusus (*misalnya jika dicurigai bahwa komputer Anda terinfeksi*) Anda dapat menandai opsi ini untuk mengaktifkan algoritma pemindaian paling menyeluruh yang akan memindai area paling sulit terinfeksi sekalipun di komputer Anda, agar benar-benar merasa yakin. Tetapi harap diingat bahwa metode ini memakan waktu lama.
- ***Pindai rootkit*** *(diaktifkan secara default): Pemindaian* Anti-Rootkit menelusuri komputer Anda dari kemungkinan rootkit, yaitu program dan teknologi yang dapat menutupi aktivitas malware di komputer Anda. Jika rootkit terdeteksi, tidak berarti komputer Anda terinfeksi. Di beberapa kasus, driver atau bagian tertentu dari aplikasi biasa mungkin salah terdeteksi sebagai rootkit.

Pengaturan pindai tambahan

Tautan ini akan membuka dialog baru ***Pengaturan Pindai Tambahan*** di mana Anda dapat menetapkan parameter berikut:



- ***Opsi matikan komputer*** – memutuskan apakah komputer akan dimatikan secara otomatis setelah proses pemindaian yang berjalan selesai. Dengan mengkonfirmasi opsi ini *(Matikan komputer setelah pemindaian selesai)*, sebuah opsi baru yang diaktifkan akan memungkinkan komputer dimatikan sekalipun saat itu sedang terkunci (*Matikan paksa jika komputer terkunci)*.

- ***Tipe file untuk pemindaian*** – selanjutnya Anda harus memutuskan apakah Anda ingin memindai:

  - ***Semua tipe file*** dengan opsi penentuan pengecualian dari pemindaian dengan memberikan daftar ekstensi file yang dipisah koma, untuk file yang tidak boleh dipindai.

  - ***Tipe file yang dipilih*** – Anda dapat menentukan bahwa Anda hanya ingin memindai file yang dapat terinfeksi *(file yang tidak dapat terinfeksi tidak akan dipindai, misalnya beberapa file teks biasa, atau file yang tidak dapat dijalankan lainnya)*, termasuk file media *(file video, audio – jika Anda membiarkan kotak ini tidak ditandai, maka hal ini akan lebih mengurangi waktu pemindaian, karena file ini seringkali terlalu besar dan sangat kecil kemungkinannya untuk terinfeksi virus)*. Sekali lagi, Anda dapat menentukan ekstensi file yang harus selalu dipindai.

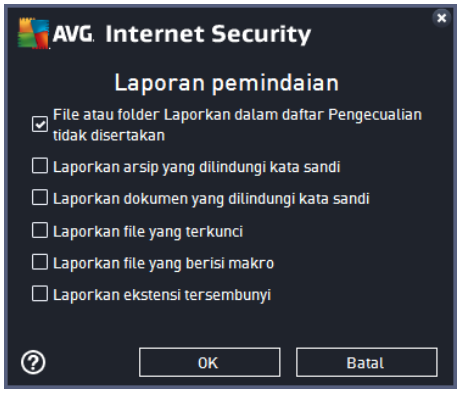
  - Secara opsional, Anda dapat memutuskan apakah Anda ingin memilih opsi ***Pindai file tanpa ekstensi*** – opsi ini diaktifkan secara default, dan disarankan Anda membiarkannya kecuali Anda memiliki alasan kuat untuk mengubahnya. File tanpa ekstensi cukup mencurigakan dan harus selalu dipindai.

Sesuaikan secepat apa pemindaian selesai

Dalam bagian ini Anda dapat menentukan lebih lanjut kecepatan pemindaian yang diinginkan berdasarkan penggunaan sumber daya sistem. Secara default, nilai opsi ini diatur ke tingkat penggunaan sumber daya otomatis yang *peka pengguna*. Jika Anda ingin pemindaian berjalan lebih cepat, ini akan menghemat waktu tetapi sumber daya sistem yang digunakan akan jauh meningkat selama pemindaian dan akan memperlambat aktivitas lain pada PC (*opsi ini dapat digunakan bila komputer hidup namun tidak ada orang yang saat itu menggunakannya*). Di sisi lain, Anda dapat menurunkan sumber daya sistem yang digunakan dengan memperpanjang waktu pemindaian.

Atur laporan pemindaian tambahan

Klik tautan ***Atur laporan pindai tambahan ...*** untuk membuka jendela dialog mandiri bernama ***Laporan pindai*** di mana Anda dapat menandai beberapa item untuk menetapkan temuan apa yang harus dilaporkan:

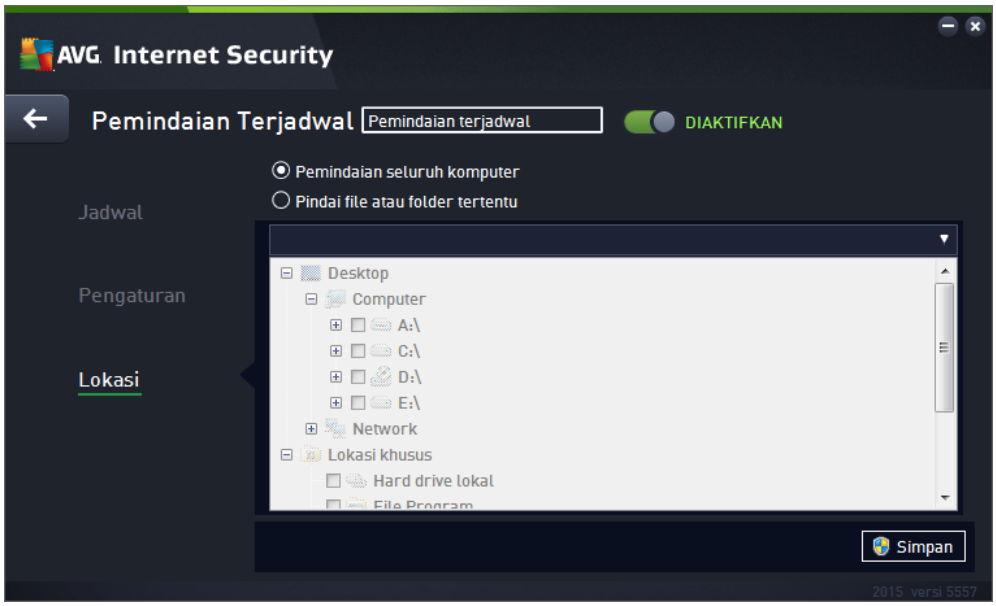


Kontrol pada dialog

- ***Simpan*** – Menyimpan semua perubahan yang telah dilakukan pada tab ini atau tab lain pada dialog ini, dan kembali ke gambaran umum Pemindaian terjadwal. Dengan demikian, jika Anda ingin mengkonfigurasi parameter tes pada semua tab, tekan tombol untuk menyimpannya hanya setelah Anda menentukan semua persyaratan.

- – Gunakan tanda panah hijau di bagian kiri atas dialog untuk kembali ke gambaran umum Pemindaian

terjadwal.



Pada tab ***Lokasi*** Anda dapat menentukan apakah Anda ingin menjadwalkan pemindaian seluruh komputer atau pemindaian file atau folder tertentu. Jika Anda memilih untuk memindai file atau folder tertentu, maka struktur yang ditampilkan di bagian bawah dialog ini akan diaktifkan dan Anda dapat menentukan folder yang akan dipindai (*perluas item dengan mengeklik tanda plus hingga Anda menemukan folder yang ingin Anda pindai*). Anda dapat memilih beberapa folder dengan menandai kotaknya masing-masing. Folder yang dipilih akan ditampilkan dalam bidang teks di bagian atas dialog, dan menu turun-bawah akan menyimpan riwayat pemindaian yang Anda pilih untuk digunakan kemudian. Atau, masukkan jalur lengkap ke folder yang diinginkan secara manual (*jika memasukkan beberapa jalur, pisahkan dengan titik koma tanpa menambah spasi*).

Dalam struktur, Anda juga dapat melihat cabang ***Lokasi khusus***. Di bawah ini adalah daftar lokasi yang akan dipindai setelah kotak centang yang dimaksud ditandai:

- ***Hard drive lokal*** – semua hard drive komputer Anda
- ***File program***
    - C:\Program Files\
    - *dalam versi 64-bit* C:\Program Files (x86)
- ***Folder My Documents***
    - *untuk Win XP:* C:\Documents and Settings\Default User\My Documents\
    - *untuk Windows Vista/7*: C:\Users\user\Documents\
- ***Dokumen Bersama***
    - *untuk Win XP*: C:\Documents and Settings\All Users\Documents\

- *untuk Windows Vista/7*: C:\Users\Public\Documents\

- ***Folder Windows*** – C:\Windows\

- ***Lainnya***

  - *Drive sistem* – hard drive tempat menginstal sistem operasi Anda (biasanya C:)

  - *Folder sistem* – C:\Windows\System32\

  - *Folder File Sementara* – C:\Documents and Settings\User\Local\ (*Windows XP*); atau C:\Users\user\AppData\Local\Temp\ (*Windows Vista/7*)

  - *File Internet Sementara* – C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (*Windows XP*); atau C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

Kontrol pada dialog

- ***Simpan*** – Menyimpan semua perubahan yang telah dilakukan pada tab ini atau tab lain pada dialog ini, dan kembali ke gambaran umum Pemindaian terjadwal. Dengan demikian, jika Anda ingin mengkonfigurasi parameter tes pada semua tab, tekan tombol untuk menyimpannya hanya setelah Anda menentukan semua persyaratan.

- ← – Gunakan tanda panah hijau di bagian kiri atas dialog untuk kembali ke gambaran umum Pemindaian terjadwal.

3.9.5. Hasil Pemindaian

Dialog ***Gambaran umum hasil pemindaian*** memberikan daftar hasil semua pemindaian yang telah dilakukan. Diagram ini memberikan informasi berikut mengenai masing-masing hasil pemindaian:

- ***Ikon*** – Kolom pertama menampilkan ikon informasi yang menjelaskan status pemindaian:

- Tidak ditemukan infeksi, pemindaian selesai
- Tidak ditemukan infeksi, pemindaian tersela sebelum selesai
- Infeksi ditemukan dan tidak dipulihkan, pemindaian selesai
- Infeksi ditemukan dan tidak dipulihkan, pemindaian tersela sebelum selesai
- Infeksi ditemukan dan semua dipulihkan atau dihapus, pemindaian selesai
- Infeksi ditemukan dan semua dipulihkan atau dihapus, pemindaian tersela sebelum selesai

- ***Nama*** – Kolom ini memberikan nama pemindaian yang dimaksud. Baik salah satu dari pemindaian yang ditentukan, atau pemindaian terjadwal Anda sendiri.
- ***Waktu mulai*** – Memberikan tanggal dan waktu yang tepat saat pemindaian diluncurkan.
- ***Waktu selesai*** – Memberikan tanggal dan waktu yang tepat saat pemindaian selesai, dihentikan sementara, atau terganggu.
- ***Objek yang diuji*** – Memberikan jumlah semua objek yang telah dipindai.
- ***Infeksi*** – Menunjukkan jumlah infeksi yang dihapus/total yang ditemukan.
- ***Tinggi /Sedang / Rendah*** – Tiga kolom berurutan yang memberitahukan jumlah infeksi yang ditemukan menurut tingkat keseriusannya yaitu tinggi, sedang dan rendah.
- ***Rootkit*** – Menunjukkan jumlah rootkit yang ditemukan selama pemindaian.

Kontrol dialog

Lihat perincian – Klik tombol ini untuk melihat informasi terperinci mengenai pemindaian yang dipilih *(disorot dalam diagram di atas)*.

Hapus hasil – Klik tombol ini untuk menghapus informasi hasil pemindaian yang dipilih dari diagram.

– Gunakan tanda panah hijau di bagian kiri atas dialog untuk kembali ke antarmuka pengguna utama dengan gambaran umum komponen.

3.9.6. Perincian hasil pemindaian

Untuk membuka gambaran umum informasi terperinci tentang hasil pemindaian yang dipilih, klik tombol ***Lihat perincian*** yang dapat diakses pada dialog Gambaran umum hasil pemindaian. Anda akan diarahkan ke antarmuka dialog yang sama yang menerangkan informasi tentang hasil pemindaian secara terperinci. Informasi tersebut dibagi menjadi tiga tab:

- ***Ringkasan*** – Tab ini memberikan informasi dasar tentang pemindaian: Apakah pemindaian berhasil diselesaikan, apakah ada ancaman yang ditemukan dan apa yang terjadi pada ancaman itu.
- ***Perincian*** – Tab ini menampilkan semua informasi tentang pemindaian, termasuk perincian tentang ancaman yang terdeteksi. Ekspor gambaran umum ke file memungkinkan Anda menyimpan hasil pemindaian sebagai file .csv.

- ***Deteksi*** – Tab ini hanya ditampilkan jika ada ancaman yang terdeteksi selama pemindaian, dan memberikan informasi terperinci tentang ancaman tersebut:

  Tingkat keparahan informasi: informasi atau peringatan, bukan ancaman sesungguhnya. Biasanya dokumen yang berisi makro, dokumen atau arsip yang dilindungi oleh kata sandi, file terkunci, dll.

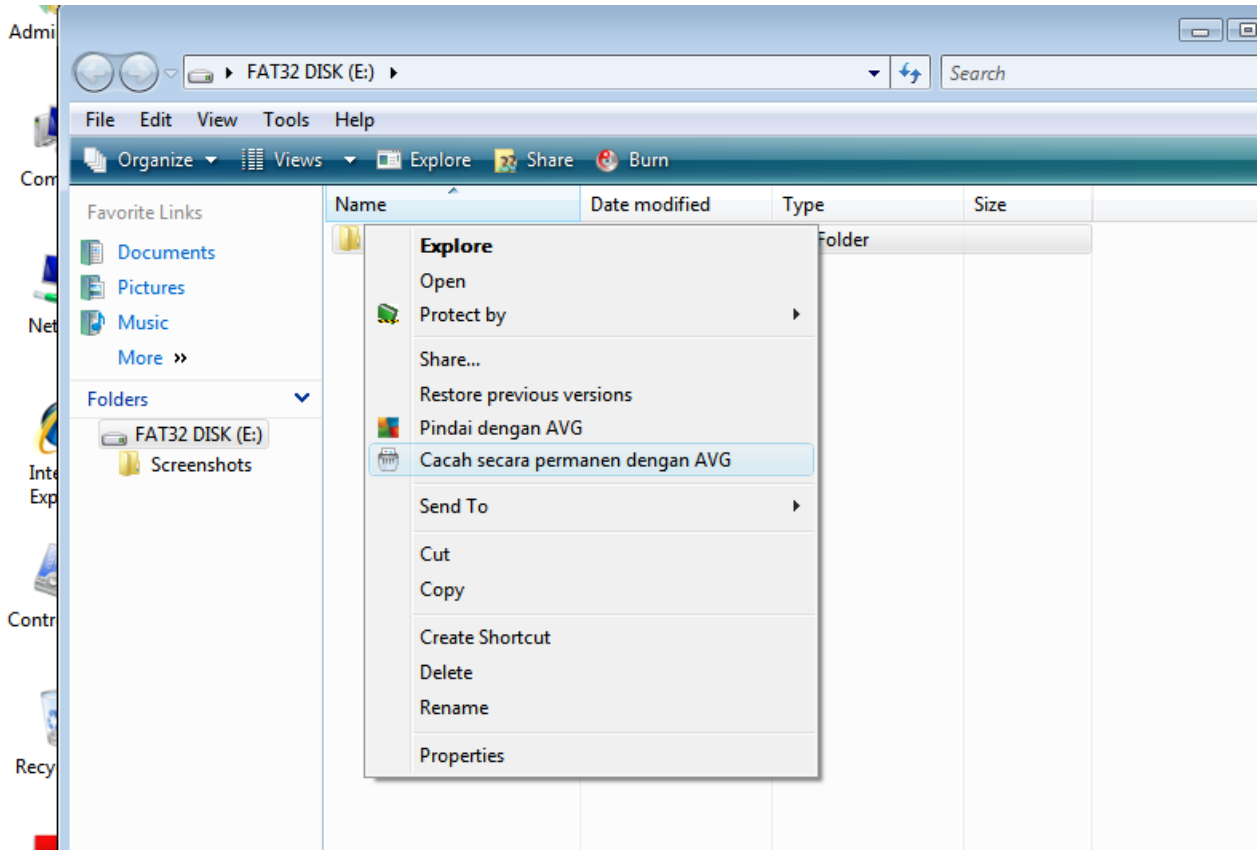
  Keseriusan sedang: biasanya berupa PUP *(potentially unwanted programs/program yang mungkin tidak diinginkan, misalnya adware)* atau cookie pelacak

  Keseriusan tinggi: ancaman serius seperti virus, Troya, eksploit, dll. Dan juga objek-objek yang terdeteksi oleh metode deteksi Heuristik, yaitu ancaman yang belum diterangkan dalam basis data virus.

3.10. AVG File Shredder

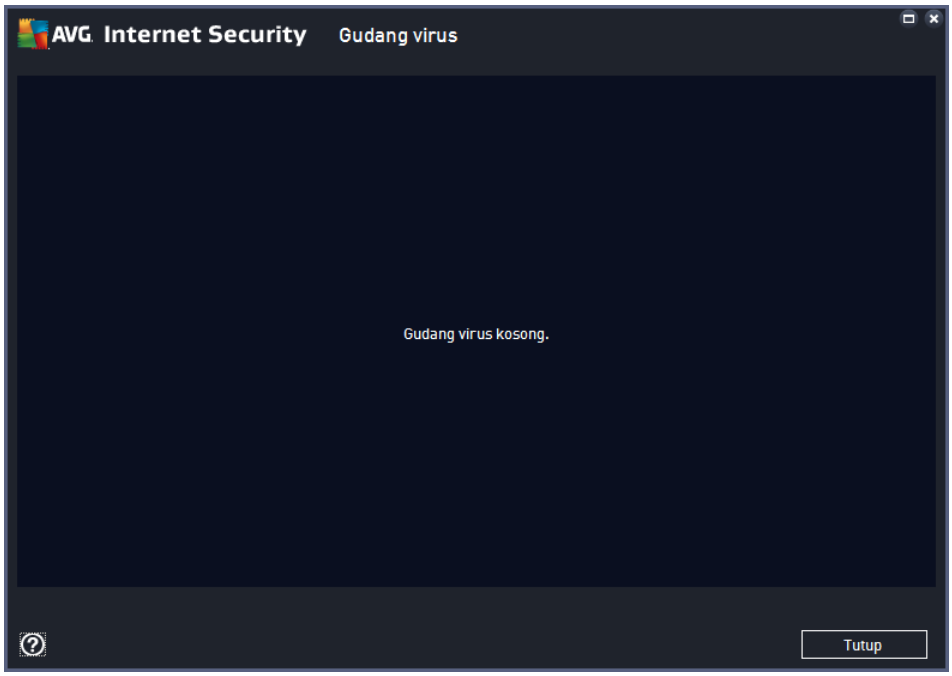
AVG File Shredder telah didesain untuk menghapus file dengan sangat aman, sehingga, tidak ada kemungkinan memulihkannya, bahkan dengan alat perangkat lunak canggih untuk tujuan ini.

Untuk mencacah file atau folder, klik kanan kanan file atau folder di file manager *(Windows Explorer, Total Commander, ...)* dan pilih ***Cacah secara permanen dengan AVG*** di menu konteks. File di Tempat Sampah juga dapat dicacah. Jika file khusus di lokasi khusus *(misalkan CD-ROM)* tidak dapat dicacah dengan baik, Anda akan diberi tahu, atau opsi di menu konteks tidak akan tersedia sama sekali.



Harap selalu diingat: Sekali Anda mencacah file, file akan hilang selamanya.

3.11. Gudang Virus



Gudang Virus merupakan lingkungan aman untuk manajemen objek yang dicurigai/terinfeksi, yang terdeteksi selama tes AVG. Begitu objek yang terinfeksi telah terdeteksi selama pemindaian, dan AVG tidak dapat memulihkannya secara otomatis, Anda akan diminta untuk memutuskan apa yang harus dilakukan dengan objek yang dicurigai tersebut. Solusi yang disarankan adalah memindah objek tersebut ke ***Gudang Virus*** untuk penanganan lebih lanjut. Kegunaan utama ***Gudang Virus*** adalah menyimpan setiap file yang dihapus selama jangka waktu tertentu, sampai Anda benar-benar yakin tidak memerlukannya lagi di lokasi aslinya. Jika Anda menyadari bahwa hilangnya file menyebabkan masalah, Anda dapat mengirim file tersebut untuk dianalisis, atau mengembalikannya ke lokasi asli.

Antarmuka ***Gudang Virus*** membuka jendela tersendiri dan menyediakan gambaran umum informasi mengenai objek terinfeksi yang telah dikarantina:

- ***Tanggal Ditambahkan*** – Memberikan tanggal dan waktu file yang dicurigai terdeteksi dan dipindahkan ke Gudang Virus.
- ***Ancaman*** – Jika Anda menginstal komponen Identitas dalam **AVG Internet Security 2015**, identifikasi grafis keparahan yang ditemukan akan diberikan di bagian ini: dari yang ringan *(tiga titik hijau)* hingga yang sangat berbahaya *(tiga titik merah)*. Anda juga akan menemukan informasi mengenai jenis infeksi dan lokasi asalnya. Tautan *Info Selebihnya* membawa Anda ke halaman yang memberikan informasi rinci mengenai ancaman terdeteksi dalam ensiklopedia virus online.
- ***Sumber*** – Menentukan komponen **AVG Internet Security 2015** mana yang telah mendeteksi masing-masing ancaman.
- ***Pemberitahuan*** – Dalam situasi yang sangat jarang, beberapa catatan dapat terjadi dalam kolom ini yang memberikan keterangan terperinci tentang masing-masing ancaman yang terdeteksi.

Tombol kontrol

Tombol kontrol berikut dapat diakses dari antarmuka ***Gudang Virus***:

- ***Pulihkan*** – mengembalikan file yang terinfeksi ke lokasi aslinya pada disk Anda.
- ***Pulihkan Sebagai*** – memindai file yang terinfeksi ke folder yang dipilih.
- ***Kirim untuk analisa*** – tombol ini hanya aktif saat Anda menyorot objek di daftar deteksi di atas. Dalam kasus tersebut, Anda memiliki opsi untuk mengirim deteksi pilihan ke lab virus AVG untuk dianalisa lebih jauh dan terperinci. Perhatikan bahwa fitur ini hanya berfungsi untuk mengirim file positif palsu, yaitu file yang telah dideteksi oleh AVG sebagai sesuatu yang terinfeksi atau mencurigakan, tetapi Anda yakin tidak berbahaya.
- ***Perincian*** – untuk informasi terperinci tentang virus tertentu yang dikarantina dalam ***Gudang Virus*** sorot item yang dipilih pada daftar lalu klik tombol ***Perincian*** untuk memanggil dialog baru dengan keterangan ancaman yang terdeteksi.
- ***Hapus*** – menghapus sama sekali file yang terinfeksi dari ***Gudang Virus*** dan tidak akan dapat dikembalikan.
- ***Kosongkan Gudang*** – menghapus sama sekali semua isi ***Gudang Virus***. Dengan menghapus file dari ***Gudang Virus***, maka file tersebut akan dihapus dari disk dan tidak akan dapat dikembalikan (*tidak dipindahkan ke Recycle Bin*).

3.12. Riwayat

Riwayat mencakup semua kejadian di masa lampau *(seperti pembaruan, pemindaian, deteksi, dll.)* dan laporan tentang kejadian-kejadian tersebut. Bagian ini dapat diakses dari antarmuka pengguna utama melalui item ***Opsi/ Riwayat***. Selanjutnya, riwayat semua kejadian yang tercatat dibagi menjadi bagian-bagian berikut:

- Hasil Pemindaian
- Hasil Resident Shield
- Hasil Perlindungan Email
- Hasil Online Shield
- Riwayat Kejadian
- Log Firewall

3.12.1. Hasil pemindaian

Dialog ***Gambaran umum hasil pemindaian*** dapat diakses melalui item menu ***Opsi / Riwayat / Hasil pemindaian*** di navigasi baris atas dari jendela utama **AVG Internet Security 2015** . Dialog ini memberikan daftar semua pemindaian yang sebelumnya telah dijalankan dan informasi mengenai hasilnya:

- ***Nama*** – tujuan pemindaian; bisa berupa nama salah satu pemindaian yang ditentukan, atau nama yang Anda berikan pada pemindaian yang dijadwalkan sendiri. Setiap nama berisi ikon yang menunjukkan hasil pemindaian:

  – ikon hijau memberitahu ada infeksi terdeteksi selama pemindaian

  – ikon biru memberitahu ada infeksi terdeteksi selama pemindaian namun objek yang terinfeksi telah dihapus secara otomatis

  – ikon merah memberitahu ada infeksi terdeteksi selama pemindaian dan tidak dapat dihapus!

  Setiap ikon mungkin penuh atau terpotong separuh – ikon penuh menyatakan pemindaian telah dilakukan dan selesai dengan benar; ikon terpotong separuh berarti pemindaian dibatalkan atau terputus.

  Catatan: *Untuk informasi terperinci mengenai setiap pemindaian, lihat dialog Hasil Pemindaian yang dapat diakses melalui tombol Lihat perincian (di bagian bawah dialog ini).*

- ***Waktu mulai*** – tanggal dan waktu pemindaian diluncurkan
- ***Waktu selesai*** – tanggal dan waktu pemindaian selesai
- ***Objek yang diuji*** – jumlah objek yang telah diperiksa selama pemindaian
- ***Infeksi*** – jumlah infeksi virus yang terdeteksi/dihapus
- ***Tinggi / Sedang*** – kolom ini menunjukkan jumlah infeksi yang dihapus/total yang ditemukan yaitu tingkat

keparahan tinggi, sedang, dan rendah

- ***Info*** – informasi terkait proses dan hasil pemindaian *(biasanya setelah selesai atau jika terhenti)*
- ***Rootkit*** – jumlah rootkit

Tombol kontrol

Tombol kontrol untuk dialog ***Gambaran umum hasil pemindaian*** adalah:

- ***Lihat perincian*** – tekan tombol ini untuk berpindah ke dialog Hasil pemindaian untuk melihat data terperinci mengenai pemindaian yang dipilih
- ***Hapus hasil*** – tekan untuk menghapus item yang dipilih dari tinjauan umum hasil pemindaian
- ← – untuk beralih kembali ke dialog utama AVG default *(gambaran umum komponen),* gunakan tanda panah di sudut kiri atas dialog ini

3.12.2. Hasil Resident Shield

Layanan ***Resident Shield*** adalah bagian dari komponen ***Komputer*** dan memindai file selagi file disalin, dibuka, atau disimpan. Bila ada virus atau semacam ancaman yang terdeteksi, Anda akan segera diperingatkan melalui dialog berikut:

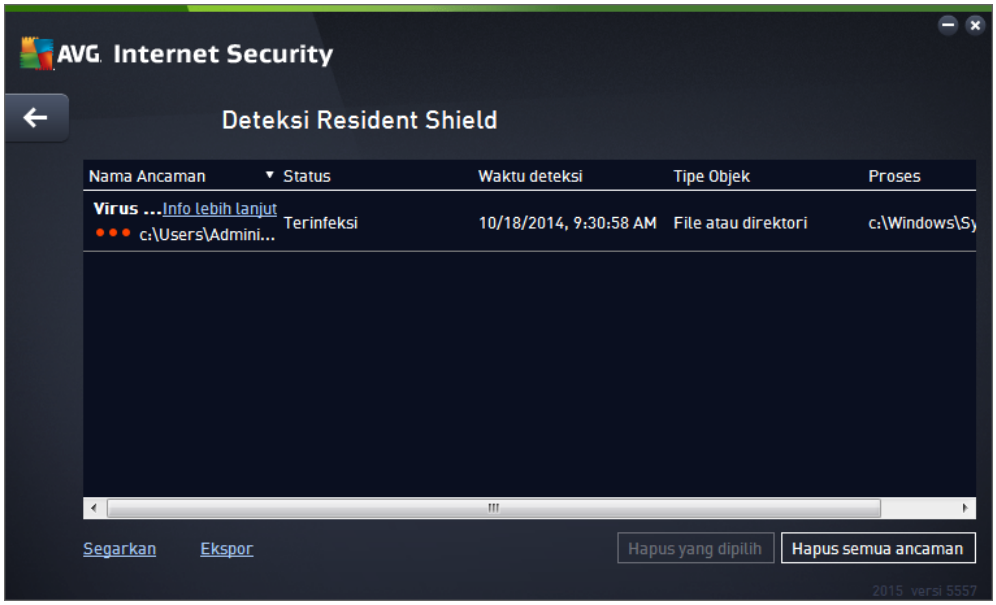
Di dalam dialog peringatan ini, Anda akan menemukan informasi tentang objek yang dideteksi dan ditetapkan sebagai terinfeksi (*Ancaman*), dan beberapa fakta penjelasan tentang infeksi yang dikenali (*Deskripsi*). Tautan *Info selebihnya* membawa Anda ke halaman yang memberikan informasi rinci mengenai ancaman terdeteksi dalam ensiklopedia virus online, bila informasi ini diketahui. Dalam dialog ini, Anda juga akan melihat gambaran umum solusi yang tersedia untuk menangani ancaman yang terdeteksi. Salah satu alternatif akan ditandai sebagai disarankan: ***Lindungi Saya (disarankan). Bila memungkinkan, Anda harus selalu mencentang opsi ini!***

Catatan: *Ini mungkin terjadi karena ukuran objek yang terdeteksi melebihi batas kapasitas kosong dalam Gudang Virus. Jika demikian, sebuah pesan peringatan akan muncul memberi tahu Anda tentang masalah saat Anda mencoba memindah objek yang terinfeksi ke Gudang Virus. Namun demikian, ukuran Gudang Virus tidak dapat diubah. Ini telah ditetapkan berupa persentase ukuran nyata dari hard disk Anda yang dapat disesuaikan. Untuk*

menambah ukuran Gudang Virus Anda, masuk ke dialog Gudang Virus dalam Pengaturan Lanjutan AVG, melalui opsi 'Batasi ukuran Gudang Virus'.

Di bagian bawah dialog Anda dapat menemukan tautan ***Tampilkan perincian***. Klik tautan ini untuk membuka jendela baru dengan informasi terperinci tentang proses yang berjalan ketika infeksi terdeteksi, dan identifikasi proses.

Daftar semua deteksi Resident Shield tersedia sebagai gambaran umum dalam dialog ***deteksi Resident Shield***. Dialog ini dapat diakses melalui item menu ***Opsi / Riwayat / Deteksi Resident Shield*** di navigasi baris atas jendela utama **AVG Internet Security 2015** . Dialog ini memberikan gambaran umum mengenai berbagai objek yang terdeteksi oleh resident shield, yang telah dievaluasi sebagai berbahaya dan telah dipulihkan atau dipindahkan ke Gudang Virus.



Untuk setiap objek yang terdeteksi, tersedia informasi berikut:

- ***Nama ncaman*** – deskripsi (*bahkan mungkin nama*) objek yang terdeteksi dan lokasinya. Tautan *Info Selebihnya* membawa Anda ke halaman yang memberikan informasi rinci mengenai ancaman terdeteksi dalam ensiklopedia virus online.
- ***Status*** – tindakan yang dilakukan pada objek yang terdeteksi
- ***Waktu Deteksi*** – tanggal dan waktu ancaman telah terdeteksi dan terblokir
- ***Tipe Objek*** – tipe objek yang terdeteksi
- ***Proses*** – tindakan yang telah dilakukan untuk memanggil objek yang mungkin berbahaya agar dapat dideteksi

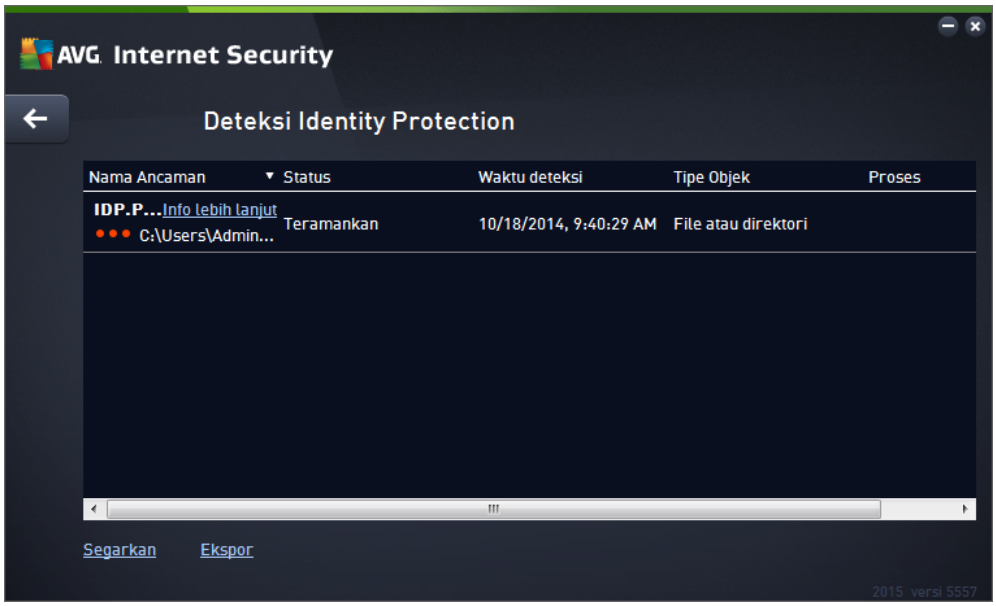
Tombol kontrol

- ***Segarkan*** – memperbarui daftar temuan yang terdeteksi oleh ***Online Shield***
- ***Ekspor*** – mengekspor seluruh daftar objek yang terdeteksi ke dalam file

- ***Hapus yang dipilih*** – Anda dapat menyorot catatan yang dipilih dalam daftar, dan menggunakan tombol ini untuk menghapus item yang dipilih saja
- ***Hapus semua ancaman*** – gunakan tombol ini untuk menghapus semua catatan yang tertera dalam dialog ini
- ← – untuk beralih kembali ke dialog utama AVG default *(gambaran umum komponen),* gunakan tanda panah di sudut kiri atas dialog ini

3.12.3. Hasil Perlindungan Identitas

Dialog ***Hasil Perlindungan Identitas*** dapat diakses melalui item menu ***Opsi / Riwayat/Hasil Perlindungan Identitas*** di navigasi baris atas dari jendela utama **AVG Internet Security 2015** .



Dialog ini memberikan daftar semua temuan yang terdeteksi oleh komponen Perlindungan Identitas. Untuk setiap objek yang terdeteksi, tersedia informasi berikut:

- ***Nama Ancaman*** – deskripsi *(bahkan mungkin nama)* objek yang terdeteksi dan lokasinya. Tautan *Info Selebihnya* membawa Anda ke halaman yang memberikan informasi rinci mengenai ancaman terdeteksi dalam ensiklopedia virus online.
- ***Status*** – tindakan yang dilakukan pada objek yang terdeteksi
- ***Waktu Deteksi*** – tanggal dan waktu ancaman telah terdeteksi dan terblokir
- ***Tipe Objek*** – tipe objek yang terdeteksi
- ***Proses*** – tindakan yang telah dilakukan untuk memanggil objek yang mungkin berbahaya agar dapat dideteksi

Di bagian bawah dialog, di bawah daftar, Anda akan menemukan informasi mengenai jumlah total objek terdeteksi yang dicantumkan di atas. Anda juga dapat mengekspor seluruh daftar objek yang terdeteksi dalam sebuah file (***Ekspor daftar ke file***) dan menghapus semua entri pada objek yang terdeteksi (***Kosongkan daftar***).

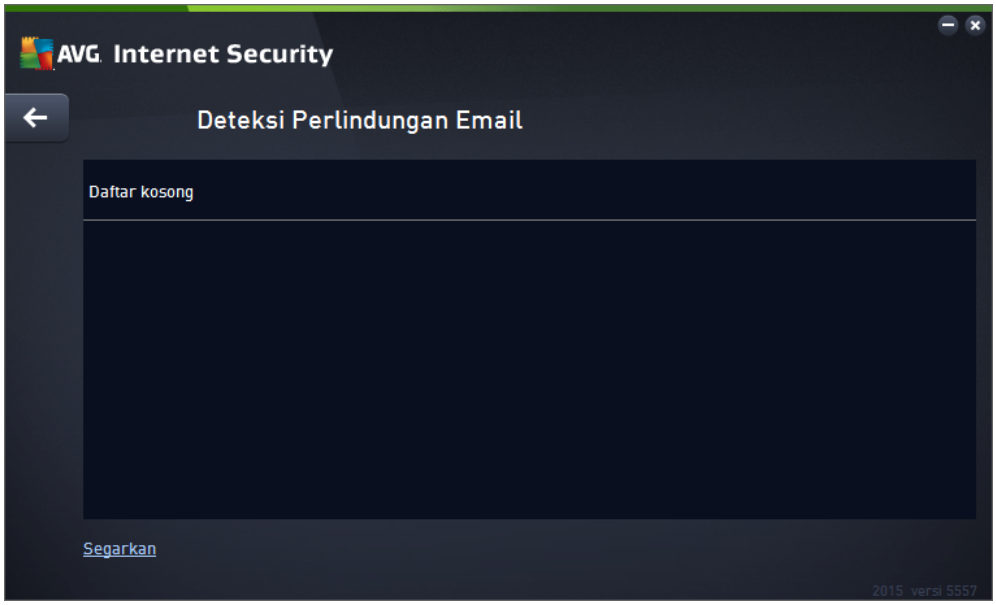
Tombol kontrol

Tombol kontrol yang tersedia dalam antarmuka ***Hasil Perlindungan Identitas*** adalah sebagai berikut:

- ***Segarkan daftar*** – memperbarui daftar ancaman yang terdeteksi
- ← – untuk beralih kembali ke dialog utama AVG default *(gambaran umum komponen),* gunakan tanda panah di sudut kiri atas dialog ini

3.12.4. Hasil Perlindungan Email

Dialog ***Hasil Perlindungan Emil*** dapat diakses melalui item menu ***Opsi / Riwayat / Hasil Perlindungan Email*** di navigasi baris atas dari jendela utama **AVG Internet Security 2015** .



Dialog ini memberikan daftar semua temuan yang terdeteksi oleh komponen Pemindai Email. Untuk setiap objek yang terdeteksi, tersedia informasi berikut:

- ***Nama deteksi*** – keterangan *(bahkan mungkin nama)* objek yang terdeteksi dan lokasinya
- ***Hasil*** – tindakan yang dilakukan pada objek yang terdeteksi
- ***Waktu Deteksi*** – tanggal dan waktu objek yang mencurigakan terdeteksi
- ***Tipe Objek*** – tipe objek yang terdeteksi
- ***Proses*** – tindakan yang telah dilakukan untuk memanggil objek yang mungkin berbahaya agar dapat dideteksi

Di bagian bawah dialog, di bawah daftar, Anda akan menemukan informasi mengenai jumlah total objek terdeteksi yang dicantumkan di atas. Anda juga dapat mengekspor seluruh daftar objek yang terdeteksi dalam sebuah file (***Ekspor daftar ke file***) dan menghapus semua entri pada objek yang terdeteksi (***Kosongkan daftar***).

Tombol kontrol

Tombol kontrol yang tersedia dalam antarmuka ***deteksi Pemindai E-mail*** adalah:

- ***Segarkan daftar*** – memperbarui daftar ancaman yang terdeteksi
- ← – untuk beralih kembali ke dialog utama AVG default *(gambaran umum komponen),* gunakan tanda panah di sudut kiri atas dialog ini

3.12.5. Hasil Online Shield

Online Shield memindai isi halaman Web yang dikunjungi dan mungkin file yang dimasukkan di dalamnya bahkan sebelum halaman ditampilkan di peramban Web Anda atau diunduh ke komputer. Bila ada ancaman yang terdeteksi, Anda akan segera diperingatkan dengan dialog berikut:

Dalam dialog peringatan ini Anda akan menemukan informasi tentang objek yang terdeteksi dan dinyatakan sebagai terinfeksi (*Ancaman*), dan beberapa fakta deskriptif tentang infeksi yang dikenali (*Nama objek*). Tautan *Info lainnya* akan mengarahkan Anda ke ensiklopedia virus online tempat Anda dapat memperoleh informasi terperinci mengenai infeksi yang terdeteksi, bila informasi ini diketahui. Dialog ini menyediakan elemen-elemen kontrol berikut:

- ***Tampilkan perincian*** – klik tautan untuk membuka jendela pop-up baru tempat Anda dapat menemukan informasi tentang proses yang sedang berjalan ketika infeksi terdeteksi, dan proses identifikasi.
- ***Tutup*** – klik tombol untuk menutup dialog peringatan.

Halaman web yang dicurigai tidak akan dibuka, dan deteksi ancaman tidak akan dilog dalam daftar ***Temuan Online Shield***. Gambaran umum ancaman yang terdeteksi ini dapat diakses melalui ***Opsi / Riwayat / Temuan Online Shield*** item menu di navigasi baris atas jendela utama **AVG Internet Security 2015**.

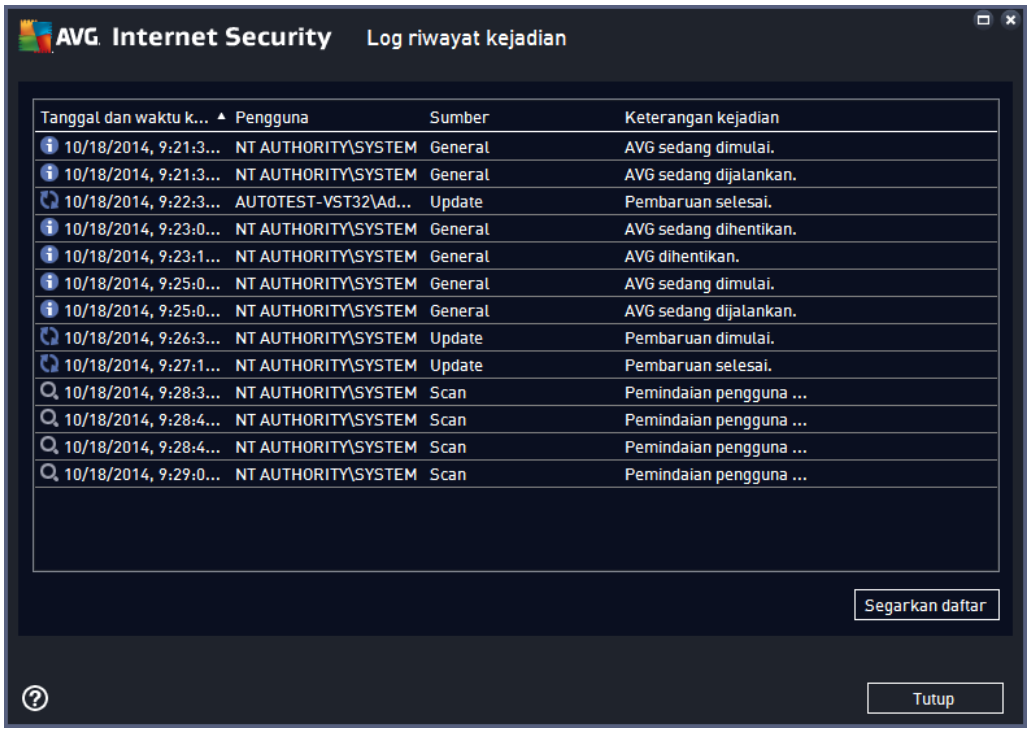
Untuk setiap objek yang terdeteksi, tersedia informasi berikut:

- ***Nama Ancaman*** – deskripsi (*mungkin bahkan nama*) objek yang terdeteksi, dan sumbernya (*halaman web*); tautan *Info selebihnya* membawa Anda ke halaman yang menyediakan informasi rinci mengenai ancaman yang terdeteksi dalam ensiklopedia virus online.
- ***Status*** – tindakan yang dilakukan pada objek yang terdeteksi
- ***Waktu Deteksi*** – tanggal dan waktu ancaman telah terdeteksi dan terblokir
- ***Tipe Objek*** – tipe objek yang terdeteksi

Tombol kontrol

- ***Segarkan*** – memperbarui daftar temuan yang terdeteksi oleh ***Online Shield***
- ***Ekspor*** – mengekspor seluruh daftar objek yang terdeteksi ke dalam file
- ← – untuk beralih kembali ke dialog utama AVG default *(gambaran umum komponen),* gunakan tanda panah di sudut kiri atas dialog ini

3.12.6. Riwayat Kejadian



Dialog ***Riwayat kejadian*** dapat diakses melalui menu ***Opsi / Riwayat / Riwayat Kejadian*** di navigasi baris atas dari jendela utama **AVG Internet Security 2015**. Dalam dialog ini Anda dapat menemukan ringkasan kejadian penting yang terjadi selama operasi **AVG Internet Security 2015**. Dialog ini memberikan catatan mengenai tipe kejadian berikut ini: informasi mengenai pembaruan aplikasi AVG, informasi pemindaian mulai, selesai atau berhenti (*termasuk tes yang dilakukan secara otomatis*); informasi mengenai kejadian yang berhubungan dengan deteksi virus (*oleh resident shield atau pemindaian*) termasuk lokasi kejadian, dan kejadian penting lainnya.

Untuk setiap kejadian, tercantum informasi berikut:

- ***Tanggal dan Waktu Kejadian*** menunjukkan tanggal dan waktu persis kejadian berlangsung.
- ***Pengguna*** menampilkan nama pengguna yang saat itu login pada saat kejadian.
- ***Sumber*** memberikan informasi mengenai komponen sumber atau bagian lain dari sistem AVG yang memicu kejadian tersebut
- ***Keterangan Kejadian*** berisi ringkasan singkat apa yang sebenarnya terjadi.

Tombol kontrol

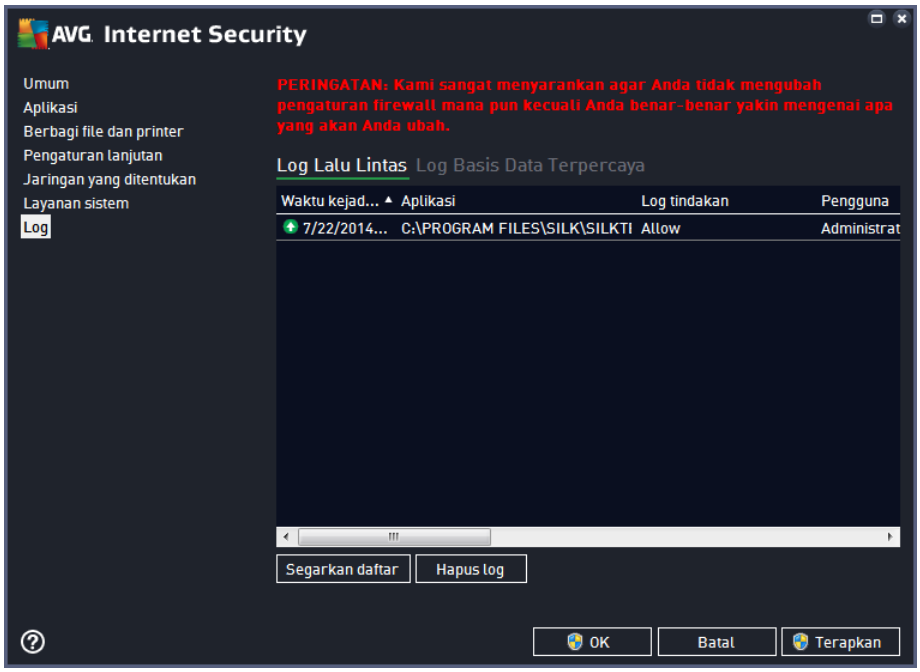
- ***Segarkan daftar*** – tekan tombol untuk memperbarui semua entri dalam daftar kejadian
- ***Tutup*** – tekan tombol untuk kembali ke **AVG Internet Security 2015** jendela utama

3.12.7. Log Firewall

Dialog ini dimaksudkan untuk konfigurasi yang lebih sulit, dan kami menyarankan Anda untuk tidak merubah seluruh pengaturan tersebut kecuali Anda sangat yakin mengenai perubahan tersebut!

Dialog ***Log*** memungkinkan Anda meninjau daftar semua tindakan dan kejadian di Firewall yang terekam dalam log bersama keterangan terperinci mengenai parameter yang relevan yang ditampilkan dalam dua tab:

- ***Log Lalu Lintas*** – Tab ini memberikan informasi mengenai aktivitas dari semua aplikasi yang telah mencoba terhubung ke jaringan. Untuk setiap item, Anda akan menemukan informasi tentang waktu kejadian, nama aplikasi, tindakan log terkait, nama pengguna, PID, arah lalu lintas, tipe protokol, jumlah port lokal dan jauh, serta informasi mengenai alamat IP lokal dan jauh.



- ***Log Basis Data Terpercaya*** – *Basis data terpercaya* adalah basis data internal AVG untuk mengumpulkan informasi mengenai aplikasi yang disertifikasi dan dipercaya yang selalu diperbolehkan untuk berkomunikasi secara online. Saat suatu aplikasi baru pertama kali mencoba menghubungkan ke jaringan (*yakni pada saat belum ada aturan firewall yang ditetapkan untuk aplikasi ini*), perlu dicari tahu apakah komunikasi jaringan diperbolehkan untuk aplikasi tersebut. Pertama, AVG menelusuri *Basis data terpercaya*, dan jika aplikasi tersebut terdaftar, maka ia akan diberi akses ke jaringan secara otomatis. Hanya setelah itulah, bila tidak ada informasi mengenai aplikasi ini yang tersedia dalam basis data, Anda akan ditanyai dalam dialog mandiri apakah Anda mau memperbolehkan aplikasi tersebut mengakses jaringan.

Tombol kontrol

- ***Segarkan daftar*** – semua parameter yang terekam dalam log dapat disusun menurut atribut yang dipilih: secara kronologis (*tanggal*) atau menurut abjad (*kolom lainnya*) – tinggal klik judul kolomnya. Gunakan tombol ***Segarkan daftar*** untuk memperbarui informasi yang ditampilkan saat ini.

- ***Hapus log*** – tekan untuk menghapus semua entri dalam diagram.

3.13. Pembaruan AVG

Tidak ada perangkat lunak keamanan yang dapat menjamin perlindungan sesungguhnya dari berbagai tipe ancaman, kecuali jika rutin diperbarui! Penulis virus selalu mencari kelemahan baru yang dapat mereka eksploitasi dalam perangkat lunak maupun sistem operasi. Virus baru, malware baru, serangan peretas baru muncul setiap hari. Karena alasan ini, vendor perangkat lunak terus mengeluarkan pembaruan dan penambal keamanan, untuk memperbaiki berbagai lubang keamanan yang ditemukan.

Mengingat semua ancaman komputer baru yang merebak, dan kecepatan penyebarannya, sangatlah penting untuk memperbarui **AVG Internet Security 2015** Anda secara rutin. Solusi terbaik adalah membiarkan pengaturan default program di mana pembaruan otomatis telah dikonfigurasi. Harap diingat bahwa jika basis data virus **AVG Internet Security 2015** Anda tidak diperbarui, program tidak akan dapat mendeteksi ancaman terbaru!

Sangatlah penting memperbarui AVG Anda secara rutin! Pembaruan definisi virus penting harus dilakukan setiap hari jika memungkinkan. Pembaruan program yang kurang penting bisa dilakukan setiap minggu.

3.13.1. Peluncuran pembaruan

Untuk memberikan keamanan maksimum, **AVG Internet Security 2015** secara default dijadwalkan untuk mencari pembaruan basis data virus baru setiap empat jam. Karena pembaruan AVG tidak dirilis berdasarkan jadwal tetap, tapi disesuaikan dengan respons terhadap jumlah dan keseriusan ancaman baru, pemeriksaan ini sangat penting untuk memastikan basis data virus AVG selalu terbarui.

Jika Anda ingin memeriksa file pembaruan baru dengan segera, gunakan tautan cepat Perbarui sekarang dalam antarmuka pengguna utama. Tautan ini selalu tersedia dari dialog antarmuka pengguna mana saja. Begitu Anda memulai pembaruan, AVG akan memverifikasi terlebih dahulu apakah ada file pembaruan baru yang tersedia. Jika ya, **AVG Internet Security 2015** akan mulai mengunduhnya dan meluncurkan proses pembaruannya. Anda akan diberi tahu mengenai hasil pembaruan di slide dialog pada Ikon Baki Sistem AVG.

Jika ingin mengurangi jumlah peluncuran pembaruan, Anda dapat mengatur sendiri parameter peluncuran pembaruan. Namun demikian, Anda sangat disarankan untuk meluncurkan pembaruan setidaknya sekali sehari! Konfigurasi dapat diedit di bagian Pengaturan lanjut/Jadwal, khususnya dalam dialog berikut:

- Jadwal pembaruan definisi
- Jadwal pembaruan program
- Jadwal pembaruan Anti-Spam

3.13.2. Tingkat pembaruan

AVG Internet Security 2015 menyediakan dua tingkat pembaruan untuk dipilih:

- ***Pembaruan definisi*** berisi perubahan yang diperlukan agar perlindungan antivirus, anti-spam dan anti-malware tetap bisa diandalkan. Biasanya, ini tidak termasuk segala perubahan pada kode dan hanya memperbarui basis data definisi. Pembaruan ini akan diterapkan begitu tersedia.
- ***Pembaruan program*** berisi beragam perubahan program, perbaikan dan peningkatan.

Saat menjadwalkan pembaruan, Anda dapat menetapkan parameter tertentu bagi kedua tingkat pembaruan:

- Jadwal pembaruan definisi

- Jadwal pembaruan program

Catatan: *Jika pembaruan program terjadwal dan pemindaian terjadwal terjadi bersamaan, proses pembaruan didahulukan dan pemindaian akan dihentikan. Dalam hal ini Anda akan diberi tahu tentang benturan ini.*

3.14. Tanya-Jawab dan Dukungan Teknis

Seandainya Anda mempunyai kesulitan dalam hal penjualan atau teknis dengan aplikasi **AVG Internet Security 2015** Anda, ada sejumlah cara untuk memperoleh bantuan. Harap pilih dari opsi berikut ini:

- ***Dapatkan Dukungan***: Tepat dalam aplikasi AVG, Anda dapat mengunjungi halaman dukungan pelanggan khusus pada situs web AVG (*http://www.avg.com/*). Pilih item menu utama ***Bantuan / Dapatkan Dukungan*** untuk dialihkan ke situs Web AVG dengan fasilitas dukungan yang tersedia. Untuk melanjutkan, harap ikuti petunjuk di halaman web.

- ***Dukungan*** *(tautan menu utama)*: Menu aplikasi AVG (*di bagian atas antarmuka pengguna utama*) berisi tautan ***Dukungan*** yang akan membuka dialog baru berisi semua jenis informasi yang mungkin Anda perlukan saat mencoba menemukan bantuan. Dialog ini berisi data dasar mengenai program AVG yang telah Anda instal (*program / versi basis data*), perincian lisensi, dan daftar tautan dukungan cepat.

- ***Pemecahan masalah dalam file bantuan***: Bagian ***Pemecahan masalah*** baru tersedia langsung di file bantuan yang telah disertakan dalam **AVG Internet Security 2015** *(untuk membuka file bantuan, tekan tombol F1 di setiap dialog pada aplikasi)*. Bagian ini menyediakan daftar situasi yang paling sering terjadi bila pengguna ingin mencari bantuan profesional untuk masalah teknis. Harap pilih situasi yang paling mirip dengan masalah Anda, dan klik untuk membuka petunjuk terperinci yang mengarahkan pada solusi masalah.

- ***Pusat Dukungan Situs Web AVG***: Atau, Anda dapat mencari solusi bagi masalah Anda pada situs web AVG (*http://www.avg.com/*). Di bagian ***Dukungan*** Anda dapat menemukan Gambaran Umum grup tematis yang mengatasi masalah penjualan dan teknis, bagian yang telah disusun tentang tanya-jawab, dan semua kontak yang tersedia.

- ***AVG ThreatLabs***: Situs web terkait AVG khusus (*http://www.avgthreatlabs.com/website-safety-reports/*) yang didedikasikan untuk masalah virus dengan menyediakan gambaran umum terstruktur mengenai informasi terkait ancaman online. Anda juga dapat menemukan petunjuk tentang cara menghapus virus, spyware, dan nasihat mengenai cara agar tetap terlindungi.

- ***Forum diskusi***: Anda juga dapat menggunakan forum diskusi pengguna AVG di http://community.avg.com/.