



AVG Anti-Virus 2011

Manual Pengguna

Semakan dokumen 2011.21 (16.5.2011)

Hak cipta AVG Technologies CZ, s.r.o. Semua hak terpelihara.
Semua tanda dagangan lain adalah hak milik pemilik masing-masing.

Produk ini menggunakan RSA Data Security, Inc. MD5 Message-Digest Algorithm, Hak cipta(C) 1991-2, RSA Data Security, Inc. Dicipta pada 1991.

Produk ini menggunakan kod dari perpustakaan C-SaCzech, Hak cipta (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz).

Produk ini menggunakan zlib perpustakaan penekanan, Hak cipta (c) 1995-2002 Jean-loup Gailly dan Mark Adler.

Produk ini menggunakan perpustakaan pemampatan libzip2, Hak Cipta (c) 1996-2002 Julian R. Seward.



Kandungan

1. Pengenalan	7
2. Keperluan Pemasangan AVG	8
2.1 Sistem Pengendalian yang Disokong	8
2.2 Keperluan Minimum & Disyorkan HW	8
3. Opsyen Pemasangan AVG	9
4. Proses Pemasangan AVG	10
4.1 Selamat datang	10
4.2 Aktifkan lesen AVG anda	11
4.3 Pilih jenis pemasangan	12
4.4 Opsyen tersuai	13
4.5 Pasang AVG Security Toolbar	14
4.6 Perkembangan pemasangan	15
4.7 Pemasangan berjaya	15
5. Selepas Pemasangan	17
5.1 Pendaftaran produk	17
5.2 Akses ke antara muka pengguna	17
5.3 Mengimbas seluruh komputer	17
5.4 Ujian Eicar	17
5.5 Konfigurasi lalai AVG	18
6. Antara Muka Pengguna AVG	19
6.1 Menu Sistem	20
6.1.1 Fail	20
6.1.2 Komponen	20
6.1.3 Sejarah	20
6.1.4 Alat	20
6.1.5 Bantuan	20
6.2 Maklumat Status Keselamatan	22
6.3 Pautan Pantas	23
6.4 Gambaran keseluruhan Komponen	24
6.5 Statistik	25
6.6 Ikon Dulang Sistem	26
6.7 Alat AVG	27



7. Komponen AVG	29
7.1 AntiVirus	29
7.1.1 Prinsip AntiVirus	29
7.1.2 Antara Muka AntiVirus	29
7.2 AntiPerisian Pengintip	30
7.2.1 Prinsip AntiPerisian Pengintip	30
7.2.2 Antara Muka AntiPerisian Pengintip	30
7.3 Pengimbas Pautan	32
7.3.1 Prinsip Pengimbas Pautan	32
7.3.2 Antara Muka Pengimbas Pautan	32
7.3.3 Search-Shield	32
7.3.4 Perisai Layar	32
7.4 Perisai Residen	35
7.4.1 Prinsip Perisai Residen	35
7.4.2 Antara Muka Perisai Residen	35
7.4.3 Pengesanan Perisai Residen	35
7.5 Family Safety	40
7.6 AVG LiveKive	40
7.7 Pengimbas E-mel	40
7.7.1 Prinsip Pengimbas E-mel	40
7.7.2 Antara Muka Pengimbas E-mel	40
7.7.3 Pengesanan Pengimbas E-mel	40
7.8 Pengurus Kemas Kini	45
7.8.1 Kemas Kini Prinsip Pengurus	45
7.8.2 Kemas Kini Antara Muka Pengurus	45
7.9 Lesen	47
7.10 Pentadbiran Jauh	48
7.11 Perisai Dalam Talian	49
7.11.1 Prinsip Perisai Dalam Talian	49
7.11.2 Antara Muka Perisai Dalam Talian	49
7.11.3 Pengesanan Perisai Dalam Talian	49
7.12 AntiRootkit	52
7.12.1 Prinsip AntiRootkit	52
7.12.2 Antara Muka AntiRootkit	52
7.13 Penganalisis PC	54
7.14 Perlindungan ID	56
7.14.1 Prinsip Perlindungan ID	56



7.14.2 Antara Muka Perlindungan ID	56
7.15 Bar Alat Keselamatan	58
8. AVG Security Toolbar	60
8.1 Antara Muka AVG Security Toolbar	60
8.1.1 Butang logo AVG	60
8.1.2 kotak carian yang dikuasakan AVG Secure Search (powered by Google)	60
8.1.3 Status Halaman	60
8.1.4 Berita AVG	60
8.1.5 Berita	60
8.1.6 Hapuskan Sejarah	60
8.1.7 Pemberitahu E-mel	60
8.1.8 Maklumat Cuaca	60
8.1.9 Facebook	60
8.2 Opsyen AVG Security Toolbar	67
8.2.1 Tab Umum	67
8.2.2 Tab Butang Berguna	67
8.2.3 Tab Keselamatan	67
8.2.4 Tab Pilihan Lanjutan	67
9. Tetapan Lanjutan AVG	72
9.1 Penampilan	72
9.2 Bunyi	74
9.3 Abaikan Keadaan Rosak	76
9.4 Bilik Kebal Virus	77
9.5 Pengecualian PUP	78
9.6 Online Shield	80
9.6.1 Perlindungan Web	80
9.6.2 Pemesejan Segera	80
9.7 Pengimbas Pautan	84
9.8 Imbasan	85
9.8.1 Imbas Seluruh Komputer	85
9.8.2 Imbasan Sambungan Kerangka	85
9.8.3 Imbas Fail atau Folder Tertentu	85
9.8.4 Imbasan Peranti Boleh Dialih	85
9.9 Jadual	90
9.9.1 Imbasan yang Dijadualkan	90
9.9.2 Jadual Kemas Kini Pangkalan Data Virus	90
9.9.3 Jadual Kemas Kini Atur Cara	90



9.10 Pengimbas E-mel	100
9.10.1 Perakuan	100
9.10.2 Penapisan Mel	100
9.10.3 Pelayan	100
9.11 Perisai Residen	109
9.11.1 Tetap Lanjutan	109
9.11.2 Item yang dikecualikan	109
9.12 Pelayan Cache	113
9.13 AntiRootkit	114
9.14 Kemas kini	115
9.14.1 Proksi	115
9.14.2 Dailan	115
9.14.3 URL	115
9.14.4 Uruskan	115
9.15 Menyahdaya perlindungan AVG buat sementara waktu	122
9.16 Program Pembaikan Produk	123
10. Pengimbasan AVG	126
10.1 Antara Muka Pengimbasan	126
10.2 Imbasan Pratakrif	127
10.2.1 Imbasan Seluruh Komputer	127
10.2.2 Imbas Fail atau Folder Tertentu	127
10.2.3 Imbasan AntiRootkit	127
10.3 Pengimbasan dalam Windows Explorer	137
10.4 Pengimbasan Garis Perintah	138
10.4.1 Parameter Imbasan CMD	138
10.5 Penjadualan Imbasan	140
10.5.1 Tetap Jadual	140
10.5.2 Bagaimana untuk Mengimbas	140
10.5.3 Apa untuk Diimbas	140
10.6 Gambaran Keseluruhan Keputusan Imbasan	150
10.7 Butiran Keputusan Imbasan	151
10.7.1 Tab Gambaran Keseluruhan Keputusan	151
10.7.2 Tab Jangkitan	151
10.7.3 Tab Perisian Pengintip	151
10.7.4 Tab Amaran	151
10.7.5 Tab Rootkit	151
10.7.6 Tab Maklumat	151



10.8 Bilik Kebal Virus	159
11. Kemas kini AVG	161
11.1 Tahap Kemas kini	161
11.2 Jenis Kemas Kini	161
11.3 Kemas Kini Proses	161
12. Sejarah Acara	163
13. Soalan Lazim dan Sokongan Teknikal	165



1. Pengenalan

Manual pengguna ini memberikan dokumentasi menyeluruh untuk **AVG Anti-Virus 2011**.

Tahniah bagi pembelian AVG Anti-Virus 2011 anda!

AVG Anti-Virus 2011 adalah salah satu rangkaian produk AVG yang memenangi anugerah yang direka bentuk untuk memberikan anda ketenangan minda dan keselamatan menyeluruh untuk PC anda. Sama seperti semua produk AVG **AVG Anti-Virus 2011** telah direka bentuk semula sepenuhnya, daripada asas, untuk memberikan perlindungan keselamatan AVG yang terkenal dan diiktiraf dengan cara yang baru, lebih mesra pengguna dan berkesan. Produk **AVG Anti-Virus 2011** baru anda mempunyai antara muka yang diperkemas digabungkan dengan pengimbasan yang lebih agresif dan cepat. Lebih banyak ciri keselamatan yang telah diautomasi untuk kesenangan anda dan opsyen pengguna 'bijak' yang baru telah dimasukkan supaya anda boleh menyesuaikan ciri keselamatan kami dengan gaya hidup anda. Tiada lagi penggunaan yang menimbulkan curiga untuk keselamatan!

AVG telah direka dan dibangunkan untuk melindungi aktiviti pengkomputeran dan perangkaan anda. Nikmati pengalaman perlindungan penuh dari AVG.

Semua tawaran produk AVG

- Perlindungan yang berkaitan dengan cara anda menggunakan komputer anda dan Internet: perbankan dan membeli-belah, melayari dan mencari, bersembang dan menghantar e-mel, atau memuat turun fail dan membina rangkaian sosial – AVG mempunyai produk perlindungan yang sesuai untuk anda
- Perlindungan bebas gangguan yang dipercayai oleh lebih 110 juta orang di seluruh dunia dan digerakkan oleh rangkaian global penyelidik yang amat berpengalaman
- Perlindungan yang disokong oleh sokongan pakar 24 jam



2. Keperluan Pemasangan AVG

2.1. Sistem Pengendalian yang Disokong

AVG Anti-Virus 2011 adalah bertujuan untuk melindungi stesen kerja dengan sistem pengendalian berikut:

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

(dan berkemungkinan pek perkhidmatan lebih tinggi untuk sistem pengendalian khusus)

Nota: Komponen [Perlindungan ID](#) tidak disokong pada Windows XP x64. Pada sistem pengendalian ini, anda boleh memasang AVG Anti-Virus 2011 tetapi hanya tanpa komponen IDP.

2.2. Keperluan Minimum & Disyorkan HW

Keperluan perkakasan minimum untuk **AVG Anti-Virus 2011**:

- Intel Pentium CPU 1,5 GHz
- 512 MB memori RAM
- 750 MB ruang pemacu keras yang kosong (untuk tujuan pemasangan)

Keperluan perkakasan disyorkan untuk **AVG Anti-Virus 2011**:

- Intel Pentium CPU 1,8 GHz
- 512 MB memori RAM
- 1400 MB ruang pemacu keras yang kosong (untuk tujuan pemasangan)



3. Opsyen Pemasangan AVG

AVG boleh dipasang sama ada dari fail pemasangan yang tersedia pada CD pemasangan anda atau anda boleh memuat turun fail pemasangan terkini dari tapak web AVG (<http://www.avg.com/>).

Sebelum anda mula memasang AVG, kami amat menyarankan anda mengunjungi tapak web AVG (<http://www.avg.com/>) untuk menyemak fail pemasangan baru. Dengan cara ini, anda boleh memastikan untuk memasang versi tersedia terkini bagi AVG Anti-Virus 2011.

Sewaktu proses pemasangan, anda akan diminta nombor lesen/jualan. Sila pastikan anda mempunyainya sebelum memulakan pemasangan. Nombor jualan boleh ditemui pada pembungkusan CD. Jika anda sudah membeli salinan AVG dalam talian, nombor lesen anda akan dihantar kepada anda melalui e-mel.



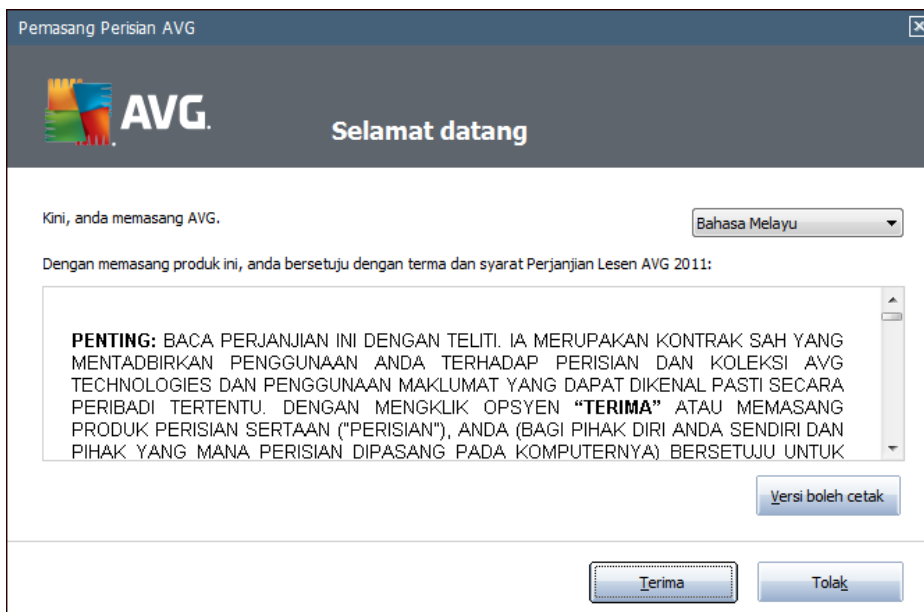
4. Proses Pemasangan AVG

Untuk memasang **AVG Anti-Virus 2011** pada komputer anda, anda perlu mendapatkan fail pemasangan terkini. Anda boleh menggunakan fail pemasangan dari CD yang merupakan sebahagian daripada edisi kotak anda tetapi fail ini mungkin telah tamat tempoh. Oleh itu, kami menyarankan untuk mendapatkan fail pemasangan terkini dalam talian. Anda boleh memuat turun fail dari tapak web AVG (<http://www.avg.com/>), bahagian **Pusat Sokongan / Muat Turun**.

Pemasangan adalah jujukan tettingkap dialog dengan penerangan ringkas mengenai apa yang perlu dilakukan pada setiap langkah. Dalam yang berikut, kami menawarkan penerangan untuk setiap tettingkap dialog.

4.1. Selamat datang

Proses pemasangan bermula dengan tettingkap dialog **Selamat datang**. Di sini anda memilih bahasa yang digunakan untuk proses pemasangan, dan bahasa lalai antara muka pengguna AVG. Di bahagian atas tettingkap dialog ditemui menu jatuh ke bawah dengan senarai bahasa yang anda boleh pilih:



Perhatian: Di sini, anda memilih bahasa untuk proses pemasangan. Bahasa yang anda pilih akan dipasang sebagai bahasa lalai bagi antara muka pengguna AVG, bersama-sama Bahasa Inggeris yang dipasang secara automatik. Jika anda mahu memasang bahasa tambahan lain untuk antara muka pengguna, sila tentukannya dalam salah satu dialog persediaan berikut yang dinamakan **Pilihan Tersuai**.

Selain itu, dialog ini menyediakan pernyataan penuh perjanjian lesen AVG. Sila baca dengan teliti. Untuk mengesahkan bahawa anda telah membaca, memahami dan menerima perjanjian ini tekan butang **Terima**. Jika anda tidak bersetuju dengan perjanjian lesen ini, tekan butang **Tolak**, dan proses pemasangan akan ditamatkan serta-merta.



4.2. Aktifkan lesen AVG anda

Dalam dialog **Aktifkan Lesen Anda** anda dijemput untuk mengisi nombor lesen anda ke dalam medan teks yang disediakan.

Nombor jualan boleh ditemui pada pembungkusan CD dalam kotak **AVG Anti-Virus 2011** anda. Nombor lesen akan berada dalam e-mel pengesahan yang anda terima selepas membeli **AVG Anti-Virus 2011** anda dalam talian. Anda mesti menaip nombor betul-betul seperti yang ditunjukkan. Jika bentuk digital nombor lesen tersedia (*dalam e-mel*), ia disyorkan untuk menggunakan kaedah salin dan tampal untuk memasukkannya.

Pemasang Perisian AVG

AVG. Aktifkan Lesen Anda

Nombor Lesen:

Contoh: 9FULL-NSDRS-KUL4L-UKSFR-L96M9-B2ALT-XWMX3

Jika anda membeli perisian AVG 2011 dalam talian anda, nombor lesen anda telah dihantar melalui e-mel. Untuk mengelakkan menaip ralat, kami mengesyorkan pemetongan dan penampalan nombor daripada e-mel kepada skrin ini.

Jika anda telah membeli perisian tersebut dalam kedai peruncitan, anda akan menemui nombor lesen pada kad pendaftaran produk yang termasuk dalam pakej tersebut. Sila pastikan anda menyalin nombor dengan betul.

< Kembali **Berikutnya >** Batalkan

Tekan butang **Berikutnya** untuk meneruskan proses pemasangan.



4.3. Pilih jenis pemasangan



Dialog **Pilih jenis pemasangan** menawarkan pilihan dua opsi pemasangan: **Pemasangan Cepat** dan **Pemasangan Tersuai**.

Untuk kebanyakan pengguna, adalah sangat disyorkan untuk mengekalkan **Pemasangan Pantas standard** yang memasang AVG dalam mod automatik sepenuhnya dengan tetapan yang dipraktikkan oleh vendor atur cara. Konfigurasi ini memberikan keselamatan maksimum yang digabungkan dengan penggunaan optimum sumber. Di masa hadapan, jika perlu untuk mengubah konfigurasi, anda sentiasa mempunyai kemungkinan untuk melakukannya secara terus dalam aplikasi AVG. Jika anda telah memilih opsi **Pemasangan Pantas**, tekan butang **Seterusnya** untuk meneruskan ke dialog [Pasang AVG Security Toolbar](#) berikut.

Pemasangan Tersuai sepatutnya hanya digunakan oleh pengguna berpengalaman yang mempunyai alasan yang sah untuk memasang AVG menggunakan tetapan bukan standard, cth. untuk disesuaikan dengan keperluan sistem khusus. Selepas memilih opsi ini, tekan butang **Seterusnya** untuk meneruskan ke dialog [Opsyen Tersuai](#).

Dalam seksyen kanan dialog anda boleh temui kotak semak berkaitan [alat AVG](#) (yang disokong dalam Windows Vista/Windows 7). Jika anda ingin memasang alat ini, tandakan kotak semak yang berkaitan. [Alat AVG](#) akan boleh diakses dari Bar Sisi Windows memberikan anda akses segera ke kebanyakan ciri paling penting **AVG Anti-Virus 2011** anda, iaitu [pengimbasan](#) dan [pengemaskinian](#).



4.4. Opsyen tersuai

Dialog **Opsyen Tersuai** membenarkan anda untuk menetapkan dua parameter bagi pemasangan:



Folder Destinasi

Di dalam seksyen **Folder Destinasi** dialog ini anda perlu menetapkan lokasi di mana **AVG Anti-Virus 2011** perlu dipasang. Secara lalai, AVG akan dipasang ke folder fail atur cara yang terletak pada pemacu C:. Jika anda hendak mengubah lokasi ini, gunakan butang **Semak Imbas** untuk memaparkan struktur pemacu dan pilih folder berkaitan.

Pemilihan Komponen

Seksyen **Pemilihan Komponen** menyediakan gambaran keseluruhan bagi semua komponen **AVG Anti-Virus 2011** yang boleh dipasang. Jika tetapan lalai tidak sesuai dengan anda, anda boleh membuang/menambah komponen tertentu.

Walau bagaimanapun, anda hanya boleh memilih dari komponen yang termasuk dalam edisi AVG yang anda beli!

Serlahkan mana-mana item dalam senarai **Pemilihan Komponen**, dan penerangan ringkas komponen berkaitan akan dipaparkan di sebelah kanan seksyen ini. Untuk maklumat terperinci mengenai kefungsiannya setiap komponen sila rujuk bab [Gambaran Keseluruhan Komponen](#) dokumentasi ini. Untuk kembali semula ke konfigurasi lalai yang dipratetap oleh vendor perisian gunakan butang **Lalai**.

Tekan butang **Berikutnya** untuk meneruskan.

4.5. Pasang AVG Security Toolbar



Dalam dialog **Pasang AVG Security Toolbar**, tentukan sama ada anda hendak memasang **AVG Security Toolbar**. Jika anda tidak mengubah tetapan lalai, komponen ini akan dipasang secara automatik ke dalam penyemak imbas Internet anda (*penyemak imbas yang disokong buat masa ini adalah Microsoft Internet Explorer v. 6.0 atau lebih tinggi, dan Mozilla Firefox v. 3.0 atau lebih tinggi*) dan untuk memberikan anda perlindungan dalam talian menyeluruh semasa melayari Internet.

Serta, anda mempunyai opsyen untuk menentukan sama ada anda hendak memilih **AVG Secure Search (powered by Google)** sebagai pembekal carian lalai anda. Jika benar, biarkan kotak semak berkaitan bertanda.



4.6. Perkembangan pemasangan

Dialog **Perkembangan Pemasangan** menunjukkan perkembangan proses pemasangan dan tidak memerlukan sebarang campur tangan:



Selepas proses pemasangan selesai, anda akan diarah semula ke dialog seterusnya.

4.7. Pemasangan berjaya





Dialog **Pemasangan berjaya** mengesahkan bahawa **AVG Anti-Virus 2011** anda telah dipasang dan dikonfigurasi sepenuhnya.

Dalam dialog ini sila berikan maklumat hubungan anda supaya anda boleh menerima semua maklumat dan berita berkaitan produk. Di bawah borang pendaftaran anda akan menemui dua opsiyen berikut:

- **Ya, maklumkan saya mengenai berita keselamatan dan tawaran istimewa AVG 2011 melalui e-mel** - tandakan kotak semak ini untuk menyatakan anda ingin dimaklumkan mengenai apa yang baru dalam lingkungan keselamatan Internet, dan ingin menerima maklumat mengenai tawaran istimewa, peningkatan dan naik taraf produk AVG dll.
- **Saya bersetuju untuk menyertai keselamatan web AVG 2011 dan Program Pembaikan Produk ...** - tandakan kotak semak ini untuk bersetuju anda ingin menyertai Program Pembaikan Produk (untuk butiran lihat bab [Tetapan Lanjut AVG / Program Pembaikan Produk](#)) yang mengumpulkan maklumat tanpa nama mengenai ancaman yang dikesan untuk meningkatkan tahap keselamatan Internet secara keseluruhan.

Untuk memuktamadkan proses pemasangan anda perlu memulakan semula komputer anda: pilih sama ada anda ingin **Mula Semula Sekarang**, atau anda ingin menangguhkan tindakan ini - **Mula Semula Kemudian**.

Nota: Jika menggunakan mana-mana lesen perniagaan AVG, dan jika anda telah memilih item Pentadbiran jauh sebelum ini untuk dipasang (lihat [Opsyen Tersuai](#)), dialog Pemasangan berjaya muncul dengan antara muka berikut:

Anda perlu menetapkan parameter AVG DataCenter - sila berikan rentetan sambungan ke AVG DataCenter dalam bentuk pelayan:port. Jika maklumat ini tidak tersedia buat sementara waktu, biarkan medan kosong dan anda boleh menetapkan konfigurasi kemudian dalam dialog **Tetapan Lanjutan / Pentadbiran Jauh**. Untuk maklumat terperinci mengenai pentadbiran Jauh AVG, sila rujuk manual pengguna AVG Business Edition; untuk dimuat turun dari laman web AVG (<http://www.avg.com/>).



5. Selepas Pemasangan

5.1. Pendaftaran produk

Menyelesaikan pemasangan **AVG Anti-Virus 2011**, sila daftarkan produk anda dalam talian pada tapak web AVG (<http://www.avg.com/>), halaman **Pendaftaran** (*diikuti arahan yang diberikan secara terus dalam halaman*). Selepas pendaftaran, anda boleh mendapatkan akses penuh ke akaun Pengguna AVG anda, surat berita Kemas Kini AVG dan perkhidmatan lain yang disediakan secara eksklusif untuk pengguna yang berdaftar.

5.2. Akses ke antara muka pengguna

[Antara Muka Pengguna AVG](#) boleh diakses dalam beberapa cara:

- klik dua kali [ikon dulang sistem AVG](#)
- klik dua kali ikon AVG pada desktop
- klik dua kali baris status di seksyen bawah [gajet AVG](#) (*jika dipasang; disokong pada Windows Vista/ Windows 7*)
- dari menu **Start/ Programs/AVG 2011/AVG User Interface**
- dari [AVG Security Toolbar](#) melalui opsyen **Lancarkan AVG**

5.3. Mengimbas seluruh komputer

Terdapat kemungkinan risiko bahawa virus komputer telah dihantar ke komputer anda sebelum pemasangan **AVG Anti-Virus 2011**. Atas sebab itu, anda harus menjalankan [Imbas seluruh komputer](#) untuk memastikan tiada jangkitan pada PC anda.

Untuk arahan bagi menjalankan [Imbas seluruh komputer](#) sila rujuk bab [Pengimbasan AVG](#).

5.4. Ujian Eicar

Untuk mengesahkan bahawa **AVG Anti-Virus 2011** telah dipasang dengan betul, anda boleh melakukan ujian EICAR.

Ujian EICAR adalah kaedah yang sememangnya selamat digunakan untuk menguji kefungsi sistem antivirus. Ia selamat untuk diagihkan kerana ia bukan virus sebenar dan tidak termasuk sebarang pecahan kod virus. Kebanyakan produk bertindak balas kepadanya seperti ia adalah virus (*walaupun biasanya ia melaporkannya dengan nama yang biasa seperti "EICAR-AV-Test"*). Anda boleh memuat turun virus EICAR dari tapak web EICAR di www.eicar.com, dan anda juga boleh menemui semula maklumat ujian EICAR di situ.

Cuba muat turun fail **eicar.com** dan simpannya pada cakera tempatan anda. Serta-merta selepas anda mengesahkan muat turun fail ujian, [Perisai Dalam Talian](#) akan bertindak balas kepadanya dengan amaran. Notis ini menunjukkan bahawa AVG dipasang dengan betul pada komputer anda.



Dari tapak web <http://www.eicar.com>, anda juga boleh memuat turun versi yang dimampatkan bagi 'virus' EICAR (cth. dalam bentuk *ecar_com.zip*). [Perisai Dalam Talian](#) membenarkan anda untuk memuat turun fail ini dan menyimpannya pada cakera tempatan anda tetapi, kemudian, [Perisai Residen](#) mengesan 'virus' apabila anda cuba mengeluarkannya. **Jika AVG gagal mengenal pasti fail ujian EICAR sebagai virus, anda harus menyemak konfigurasi atur cara semula!**

5.5. Konfigurasi lalai AVG

Konfigurasi lalai (*iaitu bagaimana aplikasi disediakan betul-betul selepas pemasangan*) bagi **AVG Anti-Virus 2011** disediakan oleh vendor perisian supaya semua komponen dan fungsi ditiun untuk mencapai prestasi optimum.

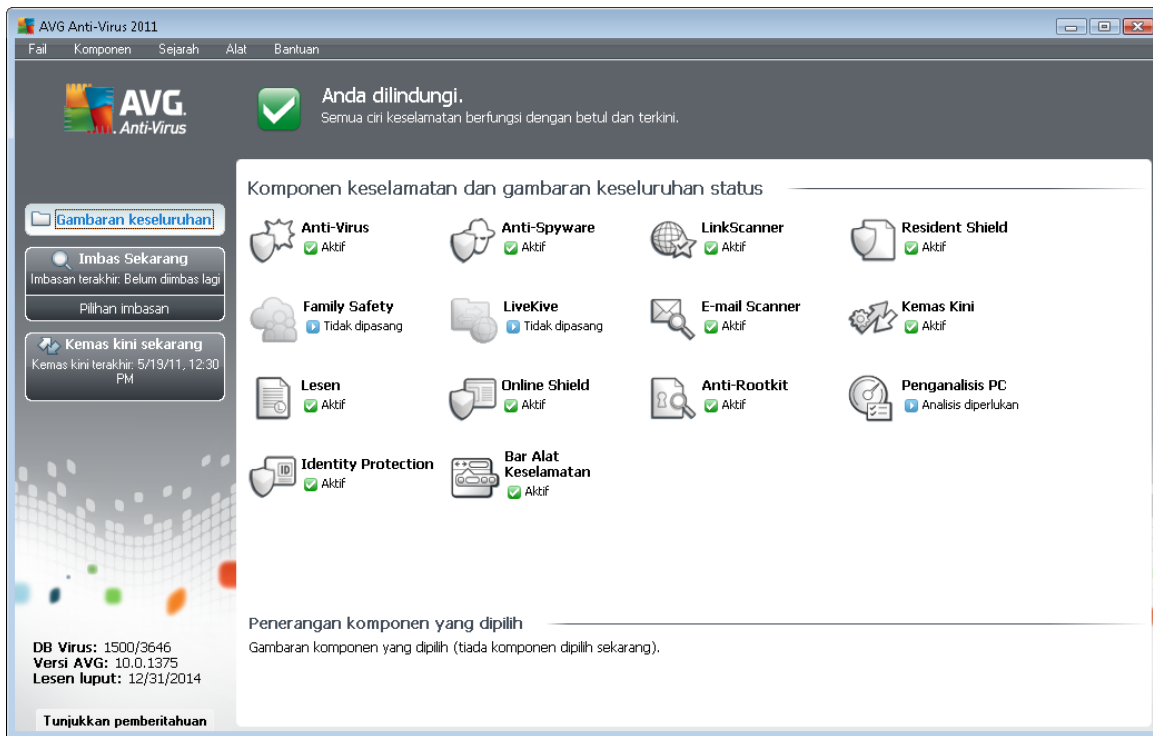
Melainkan anda mempunyai alasan penting untuk melakukannya, jangan ubah konfigurasi AVG! Perubahan kepada tetapan harus dilakukan oleh pengguna yang berpengalaman sahaja.

Beberapa pengeditan minor bagi tetapan [komponen AVG](#) boleh diakses secara terus daripada antara muka pengguna komponen khusus. Jika anda rasa anda perlu mengubah konfigurasi AVG untuk lebih sesuai dengan keperluan anda, pergi ke [Tetapan Lanjutan AVG](#): pilih item menu sistem **tetapan Alat/Lanjutan** dan edit konfigurasi AVG dalam dialog [Tetapan Lanjutan AVG](#) yang baru dibuka.



6. Antara Muka Pengguna AVG

AVG Anti-Virus 2011 terbuka dengan tettingkap utama:



Tettingkap utama dibahagikan kepada beberapa bahagian:

- **Menu Sistem** (*baris sistem atas dalam tettingkap*) adalah navigasi standard yang membenarkan anda mengakses semua komponen, perkhidmatan dan ciri AVG - [butiran >>](#)
- **Maklumat Status Keselamatan** (*bahagian atas tettingkap*) memberikan anda maklumat pada status semasa bagi atur cara AVG anda - [butiran >>](#)
- **Pautan Pantas** (*bahagian kiri tettingkap*) membenarkan anda untuk mengakses dengan pantas kepada tugas AVG yang paling penting dan paling kerap digunakan - [butiran >>](#)
- **Gambaran Keseluruhan Komponen** (*bahagian tengah tettingkap*) menawarkan gambaran keseluruhan komponen AVG yang dipasang - [butiran >>](#)
- **Statistik** (*bahagian bawah kiri tettingkap*) memberikan anda semua data statistik berkenaan operasi atur cara - [butiran >>](#)
- **Ikon Dulang Sistem** (*penjuru kanan bawah monitor, pada dulang sistem*) menunjukkan status semasa AVG - [butiran >>](#)
- **Alat AVG** (*bar sisi Windows, disokong dalam Windows Vista/7*) membolehkan akses pantas ke pengimbasan dan kemas kini AVG - [butiran >>](#)



6.1. Menu Sistem

Menu sistem adalah navigasi standard yang digunakan dalam semua aplikasi Windows. Ia terletak secara mendatar pada bahagian paling atas bagi tettingkap utama **AVG Anti-Virus 2011**. Gunakan menu sistem untuk mengakses komponen, ciri dan perkhidmatan AVG tertentu.

Menu sistem dibahagikan dalam lima bahagian utama:

6.1.1. Fail

- **Keluar** - menutup antara muka pengguna **AVG Anti-Virus 2011**. Walau bagaimanapun, aplikasi AVG akan terus dijalankan di latar belakang dan komputer anda masih akan dilindungi!

6.1.2. Komponen

Item **Komponen** bagi menu sistem memasukkan pautan kepada semua komponen AVG yang dipasang, membuka halaman dialog lalainya dalam antara muka pengguna:

- **Gambaran keseluruhan sistem** -beralih ke dialog antara muka pengguna lalai dengan [gambaran keseluruhan semua komponen yang dipasang dan statusnya](#)
- **AntiVirus** memastikan komputer anda dilindungi daripada virus yang cuba memasuki komputer anda- [butiran >>](#)
- **AntiPerisian Pengintip** memastikan bahawa komputer anda dilindungi daripada perisian pengintip dan adware - [butiran >>](#)
- **Pengimbas Pautan** memeriksa keputusan carian yang dipaparkan dalam pelayar internet anda - [butiran >>](#)
- **Pengimbas E-mel** memeriksa semua mel masuk dan keluar bagi virus - [butiran >>](#)
- **Keselamatan Keluarga** membantu mengawasi aktiviti dalam talian anak-anak anda, dan melindunginya daripada kandungan laman web yang tidak sesuai - [butiran>>](#)
- **LiveKive** memberikan sandaran automatik kepada data anda dalam talian - [butiran >>](#)
- **Perisai Residen** berjalan di latar belakang dan mengimbas fail semasa ia disalin, dibuka atau disimpan - [butiran >>](#)
- **Pengurus Kemas Kini** mengawal semua kemas kini AVG - [butiran >>](#)
- **Lesen** memaparkan nombor lesen, jenis dan tarikh tamat tempoh - [butiran >>](#)
- **Perisai Dalam Talian** mengimbas semua data yang dimuat turun oleh penyemak imbas web - [butiran >>](#)
- **AntiRootkit** mengesan atur cara dan teknologi yang cuba menyamarkan malware - [butiran >>](#)



- **Penganalisis PC** penganalisis menyediakan maklumat mengenai status komputer anda - [butiran >>](#)
- **Perlindungan Identiti** - komponen antimalware memberi fokus pada pencegahan pencuri identiti daripada mencuri barang digital peribadi anda yang bernilai - [butiran >>](#)
- **Bat Alat Keselamatan** membenarkan anda menggunakan kefungisian AVG yang dipilih secara terus daripada penyemak imbas Internet anda - [butiran >>](#)
- **Pentadbiran Jauh** hanya dipaparkan dalam AVG Business Edition jika anda telah menetapkan semasa [proses pemasangan](#) anda ingin komponen ini dipasang

6.1.3. Sejarah

- **[Imbas keputusan](#)** - beralih ke antara muka pengujian AVG, secara khusus kepada dialog **[Gambaran Keseluruhan Keputusan Imbasan](#)**
- **[Pengesanan Perisai Residen](#)** - membuka dialog dengan gambaran keseluruhan ancaman yang dikesan oleh **[Perisai Residen](#)**
- **[Pengesanan Pengimbas E-mel](#)** - membuka dialog dengan gambaran keseluruhan lampiran mesej mel yang dikesan sebagai berbahaya oleh komponen **[Pengimbas E-mel](#)**
- **[Penemuan Perisai Dalam Talian](#)** - membuka dialog dengan gambaran keseluruhan ancaman yang dikesan oleh **[Perisai Dalam Talian](#)**
- **[Bilik Kebal Virus](#)** - membuka antara muka ruang kuarantin (**[Bilik Kebal Virus](#)**) ke mana AVG membuang semua jangkitan yang dikesan yang tidak boleh dipulihkan secara automatik atas sebab tertentu. Di dalam kuarantin ini, fail yang dijangkiti dipencilkan dan keselamatan komputer dijamin dan pada masa yang sama, fail yang dijangkiti disimpan untuk kemungkinan pembaikan di masa hadapan
- **[Log sejarah acara](#)** - membuka antara muka log sejarah dengan gambaran keseluruhan semua tindakan **AVG Anti-Virus 2011** yang dilog

6.1.4. Alat

- **[Imbas komputer](#)** - mengalihkan ke [antara muka imbasan AVG](#) dan melancarkan imbasan seluruh komputer.
- **[Imbas folder yang dipilih](#)** - mengalihkan ke [antara muka pengimbasan AVG](#) dan membenarkan anda mentakrif dalam struktur pepohon komputer anda bagi fail dan folder masa yang harus diimbas.
- **[Imbas fail](#)** - membenarkan anda menjalankan ujian dengan permintaan pada fail tunggal yang dipilih daripada struktur pepohon bagi cakera anda.
- **[Kemas kini](#)** - melancarkan proses kemas kini secara automatik **AVG Anti-Virus 2011**.
- **[Kemas kini dari direktori](#)** - menjalankan proses kemas kini dari fail kemas kini yang terletak dalam folder tertentu pada cakera tempatan anda. Walau bagaimanapun, opsi ini hanya disyorkan sebagai kecemasan, cth. dalam situasi di mana tiada sambungan Internet



(contohnya, komputer anda dijangkiti dan dinyahsambung dari Internet; komputer anda disambungkan ke rangkaian dengan tiada akses kepada Internet, dll.). Dalam tettingkap yang baru dibuka, pilih folder di mana anda telah meletakkan fail kemas kini sebelum ini dan melancarkan proses kemas kini.

- **Tetapan lanjutan** - membuka dialog **tetapan lanjutan AVG** di mana anda boleh mengedit konfigurasi **AVG Anti-Virus 2011**. Secara umum, ia disyorkan untuk mengekalkan tetapan lalai bagi aplikasi seperti yang ditakrifkan oleh vendor perisian.

6.1.5. Bantuan

- **Kandungan** - membuka fail bantuan AVG
- **Dapatkan Bantuan Dalam Talian** - membuka tapak web AVG (<http://www.avg.com/>) di halaman pusat sokongan pelanggan
- **Web AVG anda** - membuka tapak web AVG (<http://www.avg.com/>)
- **Mengenai Virus dan Ancaman** - membuka **Ensiklopedia Virus** dalam talian di mana anda boleh mendapatkan maklumat terperinci mengenai virus yang dikenal pasti
- **Aktifkan semula** - membuka dialog **Aktifkan AVG** dengan data yang anda telah masukkan dalam dialog **Peribadikan AVG** bagi **proses pemasangan**. Dalam dialog ini, anda boleh memasukkan nombor lesen anda dengan sama ada menggantikan nombor jualan (*nombor yang anda telah pasangkan AVG*), atau untuk menggantikan nombor lesen lama (*cth. semasa menaik taraf ke produk AVG baru*).
- **Daftar sekarang** - menyambung kepada halaman pendaftaran bagi tapak web AVG (<http://www.avg.com/>). Sila isikan data pendaftaran anda; hanya pelanggan yang mendaftarkan produk AVG mereka boleh menerima sokongan teknikal percuma.

Perhatian: Jika menggunakan versi percubaan **AVG Anti-Virus 2011**, dua item kedua muncul sebagai **Beli sekarang** dan **Aktifkan**, membenarkan anda membeli versi penuh atur cara dengan serta-merta. Untuk **AVG Anti-Virus 2011** yang dipasang dengan nombor jualan, item dipaparkan sebagai **Daftar** dan **Aktifkan**. Untuk maklumat lanjut, sila rujuk bahagian **Lesen** bagi dokumentasi ini.

- **Mengenai AVG** - membuka dialog **Maklumat** dengan lima tab memberikan data pada nama atur cara, atur cara dan versi pangkalan data virus, maklumat sistem, perjanjian lesen dan maklumat hubungan bagi **AVG Technologies CZ**.

6.2. Maklumat Status Keselamatan

Bahagian **Maklumat Status Keselamatan** terletak di bahagian atas tettingkap utama AVG. Dalam bahagian ini, anda akan sentiasa mendapatkan maklumat mengenai status keselamatan terkini bagi **AVG Anti-Virus 2011** anda. Sila lihat gambaran keseluruhan ikon yang berkemungkinan bertindih dalam bahagian ini dan maksudnya:



- Ikon hijau menunjukkan bahawa AVG anda berfungsi sepenuhnya. Komputer anda



dilindungi sepenuhnya, terkini dan semua komponen dipasang berfungsi dengan betul.



- Ikon jingga memberi amaran bahawa satu atau lebih banyak komponen dikonfigurasi dengan salah dan anda harus memberikan perhatian kepada sifat/tetapannya. Tiada masalah kritikal dalam AVG dan anda berkemungkinan telah memutuskan untuk mematikan beberapa komponen atas sebab tertentu. Anda masih dilindungi oleh AVG. Walau bagaimanapun, sila berikan perhatian kepada masalah tetapan komponen! Namanya akan diberikan dalam bahagian **Maklumat Status Keselamatan**.

Ikon ini juga muncul jika atas beberapa sebab anda telah memutuskan untuk [mengabaikan status ralat komponen](#) (pilihan "Abaikan keadaan komponen" tersedia dari menu konteks yang dibuka dengan mengklik kanan pada ikon komponen masing-masing dalam gambaran keseluruhan komponen bagi tettingkap utama AVG). Anda mungkin perlu menggunakan opsyen ini dalam situasi tertentu tetapi amat disyorkan untuk mematikan opsyen "**Abaikan keadaan komponen**" secepat mungkin.



- Ikon merah menunjukkan bahawa AVG berada dalam status kritikal! Satu atau lebih komponen tidak berfungsi dengan betul dan AVG tidak dapat melindungi komputer anda. Sila berikan perhatian serta-merta untuk menyelesaikan masalah yang dilaporkan. Jika anda tidak dapat membetulkan ralat dengan sendiri, hubungi pasukan [sokongan teknikal AVG](#).

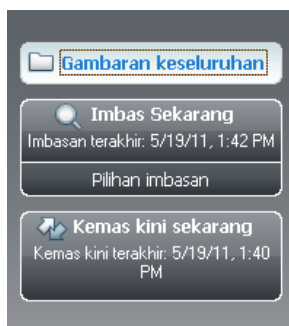
Jika AVG tidak ditetapkan ke prestasi optimum, butang baru dinamakan Betulkan (secara alternatif Betulkan semua jika masalah berkenaan melibat lebih daripada satu komponen) muncul di sebelah maklumat status keselamatan. Tekan butang ini untuk melancarkan proses automatik pemeriksaan dan konfigurasi atur cara. Ini cara mudah untuk menerapkan AVG ke prestasi optimum dan mencapai tahap keselamatan maksimum!

Adalah amat disyorkan supaya anda memberikan perhatian kepada Maklumat Status Keselamatan dan jika laporan menunjukkan sebarang masalah, teruskan dan cuba menyelesaikannya dengan serta-merta. Jika tidak, komputer anda berisiko!

Nota: maklumat status AVG boleh diperolehi pada bila-bila masa dari [ikon dulang sistem](#).

6.3. Pautan Pantas

Pautan pantas (dalam bahagian sebelah kiri [Antara Muka Pengguna AVG](#)) membenarkan anda untuk mengakses ciri AVG yang paling penting dan paling kerap digunakan:





- **Gambaran keseluruhan** - gunakan pautan ini untuk beralih dari sebarang antara muka AVG yang sedang terbuka ke lalai dengan gambaran keseluruhan semua komponen yang dipasang - lihat bab [Gambaran Keseluruhan Komponen >>](#)
- **Imbas sekarang** - secara lalai, butang ini menyediakan maklumat (*jenis imbasan, tarikh pelancaran terakhir*) bagi imbasan terakhir yang dilancarkan. Anda boleh sama ada melaksanakan arahan **Imbas sekarang** untuk melancarkan imbasan yang sama semula, atau mengikuti pautan **Pilihan imbasan** untuk membuka antara muka pengimbasan AVG di mana anda boleh menjalankan imbasan, menjadualkan imbasan atau mengedit parameternya - lihat bab [Pengimbasan AVG >>](#)
- **Kemas kini sekarang** - pautan ini menyediakan tarikh pelancaran yang terakhir bagi proses kemas kini. Tekan butang ini untuk membuka antara muka pengemaskinian, dan jalankan proses kemas kini AVG serta-merta - lihat bab [Kemas Kini AVG >>](#)

Pautan ini boleh diakses dari antara muka pengguna pada setiap masa. Apabila anda menggunakan pautan pantas untuk menjalankan proses tertentu, GUI akan beralih ke dialog baru tetapi pautan pantas masih tersedia. Tambahan pula, proses yang sedang dijalankan selanjutnya digambarkan secara grafik.

6.4. Gambaran keseluruhan Komponen

Bahagian **Gambaran Keseluruhan Komponen** terletak di bahagian tengah [Antara Muka Pengguna AVG](#). Bahagian tersebut dibahagikan kepada dua bahagian:

- Gambaran keseluruhan bagi komponen yang dipasang terdiri daripada panel dengan ikon komponen dan maklumat sama ada komponen masing-masing adalah aktif atau tidak aktif
- Penerangan bagi komponen yang dipilih

Dalam **AVG Anti-Virus 2011** bahagian **Gambaran Keseluruhan Komponen** mengandungi maklumat mengenai komponen berikut:

- **AntiVirus** memastikan komputer anda dilindungi daripada virus yang cuba memasuki komputer anda - [butiran >>](#)
- **AntiPerisian Pengintip** memastikan komputer anda dilindungi daripada perisian pengintip dan adware - [butiran >>](#)
- **Pengimbas Pautan** memeriksa keputusan carian yang dipaparkan dalam pelayar internet anda - [butiran >>](#)
- **Pengimbas E-mel** memeriksa semua mel masuk dan keluar bagi virus - [butiran >>](#)
- **Perisai Residen** berjalan di latar belakang dan mengimbas fail semasa ia disalin, dibuka atau disimpan - [butiran >>](#)
- **Keselamatan Keluarga** membantu mengawasi aktiviti dalam talian anak-anak anda, dan melindunginya daripada kandungan laman web yang tidak sesuai - [butiran >>](#)
- **LiveKive** memberikan sandaran automatik kepada data anda dalam talian - [butiran >>](#)



- **Pengurus Kemas Kini** mengawal semua kemas kini AVG - [butiran >>](#)
- **Lesen** memaparkan nombor lesen, jenis dan tarikh tamat tempoh - [butiran >>](#)
- **Perisai Dalam Talian** mengimbas semua data yang dimuat turun oleh penyemak imbas web - [butiran >>](#)
- **AntiRootkit** mengesan atur cara dan teknologi yang cuba menyamarkan malware - [butiran >>](#)
- **Penganalisis PC** menyediakan maklumat mengenai status komputer anda - [butiran >>](#)
- **Perlindungan Identiti** - komponen antimalware memberi fokus pada pencegahan pencuri identiti daripada mencuri barang digital peribadi anda yang bernilai - [butiran >>](#)
- **Bat Alat Keselamatan** membenarkan anda menggunakan kefungsiian AVG yang dipilih secara terus daripada penyemak imbas Internet anda - [butiran >>](#)
- **Pentadbiran Jauh** hanya dipaparkan dalam AVG Business Edition jika anda telah menetapkan semasa [proses pemasangan](#) anda ingin komponen ini dipasang

Klik sekali pada mana-mana ikon komponen untuk menyerlahkannya dalam gambaran keseluruhan komponen. Dalam masa yang sama, penerangan kefungsiian asas komponen muncul di bahagian bawah antara muka pengguna. Klik dua kali pada ikon untuk membuka antara muka komponen itu sendiri dengan senarai data statistik asas.

Klik kanan tetikus anda pada ikon komponen untuk mengembangkan menu konteks: selain daripada membuka antara muka grafik komponen, anda juga boleh memilih untuk **Abai keadaan komponen**. Pilih pilihan ini untuk menyatakan bahawa anda menyedari [keadaan ralat komponen](#) tetapi atas sebab tertentu anda hendak mengekalkan AVG anda seperti itu dan tidak mahu diberi amaran oleh [ikon dulang sistem](#).

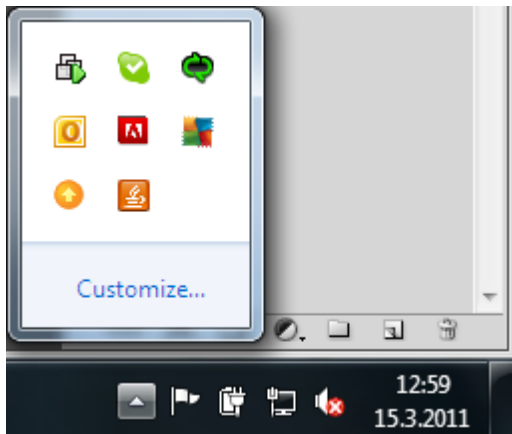
6.5. Statistik



Bahagian **Statistik** terletak di bahagian bawah [Antara Muka Pengguna AVG](#). Ia menawarkan senarai maklumat berkenaan operasi atur cara:

- **Virus DB** - memberitahu anda mengenai versi yang baru dipasang bagi pangkalan data virus
- **Versi AVG** - memberitahu anda mengenai versi AVG yang dipasang (*nombor adalah dalam bentuk 10.0.xx, di mana 10.0 adalah versi baris produk dan xxx adalah untuk nombor binaan*)
- **Lesen tamat tempoh** - memberikan tarikh tamat tempoh lesen AVG anda

6.6. Ikon Dulang Sistem

Ikon Dulang Sistem (pada bar tugas Windows anda) menunjukkan status terkini bagi **AVG Anti-Virus 2011** anda. Ia boleh dilihat setiap masa ada dulang sistem anda, tidak kira sama ada tettingkap utama AVG anda dibuka atau ditutup:



Jika dalam warna penuh , **Ikon Dulang Sistem** menunjukkan bahawa semua komponen AVG adalah aktif dan berfungsi sepenuhnya. Serta, ikon dulang sistem boleh dipaparkan dalam warna penuh jika AVG berada dalam keadaan ralat tetapi anda betul-betul menyedari mengenai situasi ini dan memutuskan dengan segera untuk [Abaikan keadaan komponen](#). Ikon dengan tanda seruan  menunjukkan masalah (*komponen tidak aktif, status ralat, dll.*). Klik dua kali pada **Ikon Dulang Sistem** untuk membuka tettingkap utama dan mengedit komponen.

Ikon dulang sistem seterusnya memberitahu mengenai aktiviti AVG dan kemungkinan perubahan status dalam atur cara (*cth, pelancaran automatik bagi imbasan atau kemas kini yang dijadualkan, perubahan status komponen, perulangan status ralat, ...*) melalui tettingkap pop timbul yang dibuka dari ikon dulang sistem AVG:



Ikon Dulang Sistem juga boleh digunakan sebagai pautan pantas untuk mengakses tettingkap utama AVG pada bila-bila masa - klik dua kali pada ikon. Dengan mengklik kanan pada **Ikon Dulang Sistem** anda membuka menu konteks ringkas dengan opsiyen berikut:

- **Buka Antara Muka Pengguna AVG** - klik untuk membuka [Antara Muka Pengguna AVG](#)
- **Mengimbas** - klik untuk membuka menu konteks bagi
- **Jalankan Penganalisis PC** - klik untuk melancarkan komponen [Penganalisis PC](#)
- **Imbasan yang berjalan** - item ini dipaparkan hanya jika imbasan sedang berjalan pada komputer anda. Untuk imbasan ini anda boleh menetapkan prioritinya, secara alternatif menghentikan atau menjeda imbasan yang sedang berjalan. Selain itu, tindakan berikut



boleh diakses: *Tetap prioriti bagi semua imbasan, Jeda semua imbasan atau Hentikan semua imbasan.*



- **Kemas kini sekarang** - melancarkan kemas kini [segera](#)
- **Bantuan** - membuka fail bantuan pada halaman mula

6.7. Alat AVG

Alat AVG dipaparkan pada desktop Windows (*Bar Sisi Windows*). Aplikasi ini hanya disokong dalam sistem pengendalian Windows Vista dan Windows 7. **Alat AVG** menawarkan akses segera kepada kefungsiian **AVG Anti-Virus 2011** yang paling penting, iaitu [pengimbasan](#) dan [pengemaskinian](#):



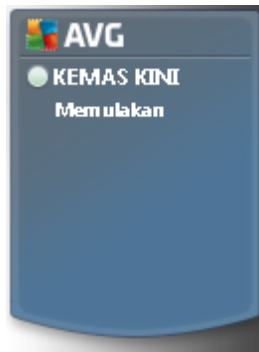
Alat AVG menyediakan opsyen akses pantas berikut:


- **Imbas sekarang** - klik pautan **Imbas sekarang** untuk memulakan [imbasan seluruh komputer](#) terus. Anda boleh melihat kemajuan proses pengimbasan dalam antara muka pengguna berganti alat ini. Gambaran keseluruhan statistik ringkas menyediakan maklumat mengenai bilangan objek yang diimbas, ancaman yang dikesan, dan ancaman yang dipulihkan. Semasa imbasan anda sentiasa boleh menjeda , atau menghentikan  proses pengimbasan. Untuk data terperinci berkaitan keputusan imbasan, sila rujuk dialog [Gambaran keseluruhan keputusan imbasan](#) yang boleh dibuka secara terus dari alat tersebut melalui pilihan **Tunjukkan butiran** (keputusan imbasan masing-masing akan disenaraikan di bawah **Imbasan alat bar sisi**).






- **Kemas kini sekarang** - klik pautan **Kemas kini sekarang** untuk melancarkan kemas kini

AVG terus dari dalam alat:



- **Pautan Twitter**  - membuka antara muka **alat AVG** baru memberikan gambaran keseluruhan suapan AVG terkini yang dipos di Twitter. Ikuti pautan **Lihat semua suapan AVG Twitter** untuk membuka penyemak imbas Internet anda dalam tettingkap baru, dan anda akan diarahkan semula terus ke laman web Twitter, khusus ke halaman yang dikhususkan bagi berita berkaitan AVG:



- **Pautan Facebook**  - membuka penyemak imbas Internet anda di laman web Facebook, khusus di halaman **komuniti AVG**
- **LinkedIn**  - pilihan ini hanya tersedia dalam pemasangan rangkaian (*iaitu sekiranya anda telah memasang AVG menggunakan salah satu lesen edisi AVG Business Edition*), dan ia membuka penyemak imbas internet anda pada laman web **AVG SMB Community** dalam rangkaian sosial LinkedIn
- **Penganalisis PC**  - membuka antara muka pengguna di dalam komponen **Penganalisis PC**
- **Kotak carian** - taipkan kata kunci dan dapatkan keputusan carian dengan serta-merta dalam tettingkap yang baru dibuka dengan penyemak imbas web lalai anda



7. Komponen AVG

7.1. AntiVirus

7.1.1. Prinsip AntiVirus

Enjin pengimbasan perisian antivirus mengimbas semua fail dan aktiviti fail (membuka/menutup fail, dll.) bagi virus yang diketahui. Sebarang virus yang dikesan akan disekat daripada melakukan sebarang tindakan dan kemudian, akan dibersihkan atau dikuarantin. Kebanyakan perisian antivirus juga menggunakan pengimbasan heuristik di mana fail diimbas untuk ciri virus biasa yang dipanggil tandatangan virus. Ini bermaksud bahawa pengimbas antivirus boleh mengesan virus yang baru dan tidak diketahui jika virus baru yang mengandungi beberapa ciri biasa bagi virus sedia ada.

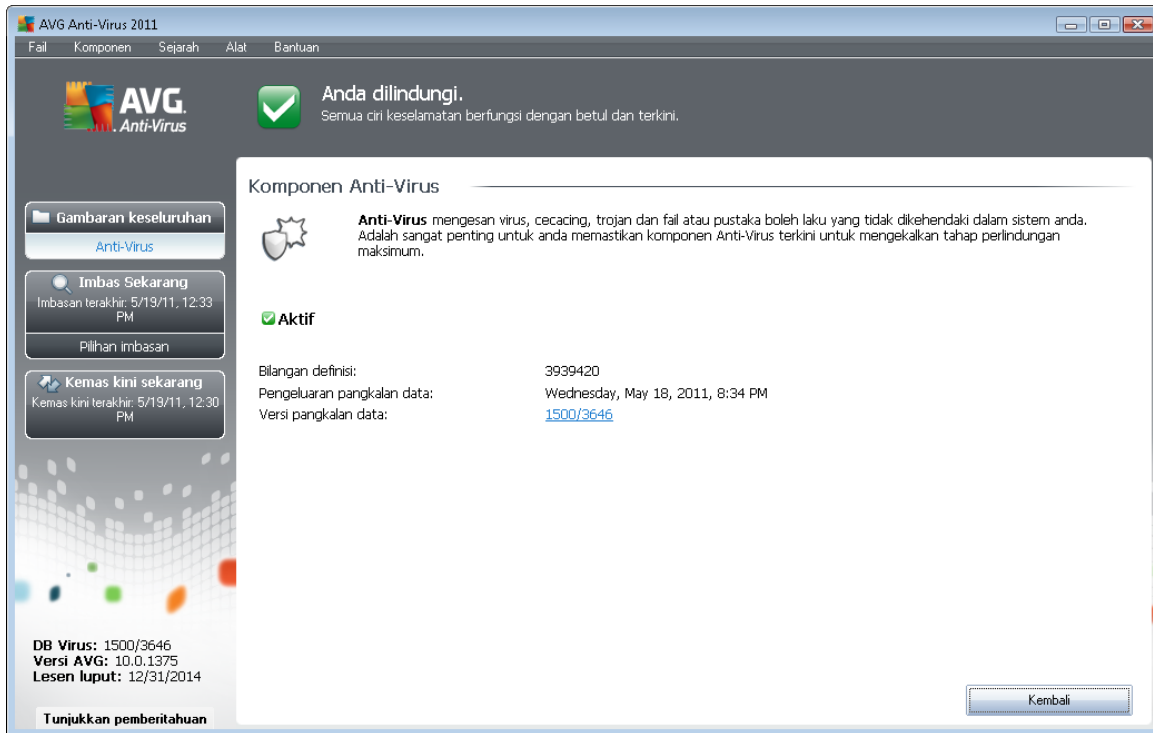
Ciri penting bagi perlindungan antivirus adalah tiada virus yang diketahui boleh dijalankan pada komputer!

Di mana hanya satu teknologi tunggal boleh kekurangan pengesanan atau pengenalpastian virus, **AntiVirus** menggabungkan beberapa teknologi untuk memastikan komputer anda dilindungi daripada virus:

- Pengimbasan - mencari rentetan aksara yang merupakan ciri bagi virus tertentu
- Analisis Heuristik - perlagakan dinamik objek yang diimbas' arahan dalam persekitaran komputer maya
- Pengesanan generik - pengesanan arahan ciri bagi virus/kumpulan virus yang ditetapkan

AVG juga boleh menganalisis dan mengesan aplikasi boleh laku atau pustaka DLL yang berpotensi tidak dikehendaki dalam sistem. Kami memanggil ancaman seperti ini sebagai Atur Cara Yang Berkemungkinan Tidak Diperlukan (pelbagai jenis perisian pengintip, adware, dsb.). Tambahan pula, AVG mengimbas pendaftaran sistem anda bagi entri yang mencurigakan, fail Internet sementara dan kuki penjejakan dan membolehkan anda memperlakukan semua item berpotensi berbahaya dengan cara yang sama seperti sebarang jangkitan lain.

7.1.2. Antara Muka AntiVirus



Antara muka komponen **AntiVirus** memberikan beberapa maklumat asas mengenai kefungsiian komponen, maklumat pada status semasa komponen (*komponen AntiVirus adalah aktif.*), dan gambaran keseluruhan ringkas statistik **AntiVirus** :

- **Bilangan definisi** - nombor memberikan kiraan virus yang ditakrifkan dalam versi terkini pangkalan data virus
- **Keluaran pangkalan data** - menentukan bila dan pukul berapa pangkalan data kali terakhir dikemas kini
- **Versi pangkalan data** - mentakrifkan bilangan versi pangkalan data virus yang sedang terpasang; dan nombor ini meningkat dengan setiap kemas kini asas virus

Terdapat hanya satu butang operasi yang tersedia dalam antara muka komponen ini (**Undur**) - tekan butang untuk kembali ke [antara muka pengguna AVG](#) lalai (*gambaran keseluruhan komponen*).

7.2. AntiPerisian Pengintip

7.2.1. Prinsip AntiPerisian Pengintip

Perisian pengintip biasanya ditakrifkan sebagai sejenis malware, cth. perisian yang mengumpulkan maklumat dari komputer pengguna tanpa pengetahuan atau persetujuan pengguna. Sesetengah aplikasi perisian pengintip juga boleh dipasang secara tidak sengaja dan biasanya mengandungi

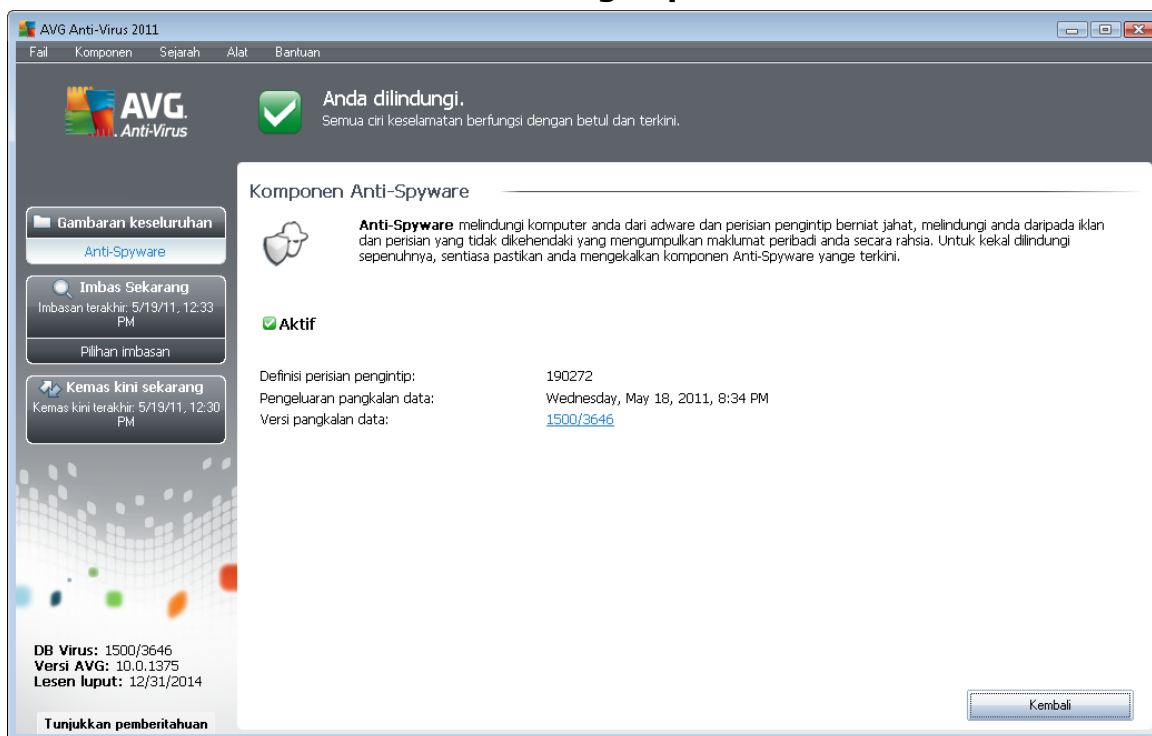


iklan, pop muncul tettingkap atau perisian berlainan jenis yang tidak disenangi.

Pada masa ini, sumber jangkitan yang paling lazim adalah laman web yang mempunyai kandungan yang mungkin berbahaya. Kaedah pemindahan lain seperti melalui e-mel atau pemindahan melalui cecacing dan virus juga tersebar luas. Perlindungan paling penting adalah untuk menggunakan pengimbas di latar belakang yang sentiasa dipasang, **AntiPerisian Pengintip**, yang berfungsi seperti perisai residen dan mengimbas aplikasi anda di latar belakang apabila anda menjalankannya.

Terdapat juga kemungkinan risiko yang malware telah dihantar ke komputer anda sebelum pemasangan AVG atau anda telah mengabaikan untuk memastikan **AVG Anti-Virus 2011** anda terkini dengan [pangkalan data dan kemas kini atur cara terkini](#). Atas sebab ini, AVG membolehkan anda mengimbas komputer anda sepenuhnya untuk menapis malware/perisian pengintip dengan menggunakan ciri pengimbasan. Ia juga mengesan malware yang tidur dan tidak aktif, cth. malware yang telah dimuat turun tetapi belum lagi diaktifkan.

7.2.2. Antara Muka AntiPerisian Pengintip



Antara muka komponen **AntiPerisian Pengintip** memberikan gambaran keseluruhan yang ringkas mengenai kefungsian komponen, maklumat mengenai status terkini komponen, dan beberapa (**statistik**AntiPerisian Pengintip:

- **Definisi perisian pengintip** - bilangan memberikan kiraan sampel perisian pengintip yang ditakrifkan dalam versi pangkalan data perisian pengintip terkini
- **Kemas kini pangkalan data** - menentukan bila dan pada pukul berapa pangkalan data perisian pengintip dikemas kini



- **Versi pangkalan data** - menentukan bilangan versi pangkalan data perisian pengintip terkini; dan nombor ini meningkat dengan setiap kemas kini pangkalan virus

Terdapat hanya satu butang operasi yang tersedia dalam antara muka komponen ini (**Undur**) - tekan butang untuk kembali ke [antara muka pengguna AVG](#) lalai (*gambaran keseluruhan komponen*).

7.3. Pengimbas Pautan

7.3.1. Prinsip Pengimbas Pautan

LinkScanner melindungi anda daripada bilangan ancaman 'hari ini ada, esok tiada' yang semakin meningkat di web. Ancaman ini boleh disembunyikan pada sebarang jenis laman web, daripada kerajaan kepada jenama yang besar dan terkenal kepada perniagaan kecil, dan ia jarang kekal di tapak berkenaan lebih daripada 24 jam. **LinkScanner** melindungi anda dengan menganalisis halaman web di sebalik semua pautan di mana-mana halaman web yang anda lihat dan memastikan ia selamat pada satu-satunya masa yang paling penting – semasa anda ingin mengklik pautan berkenaan.

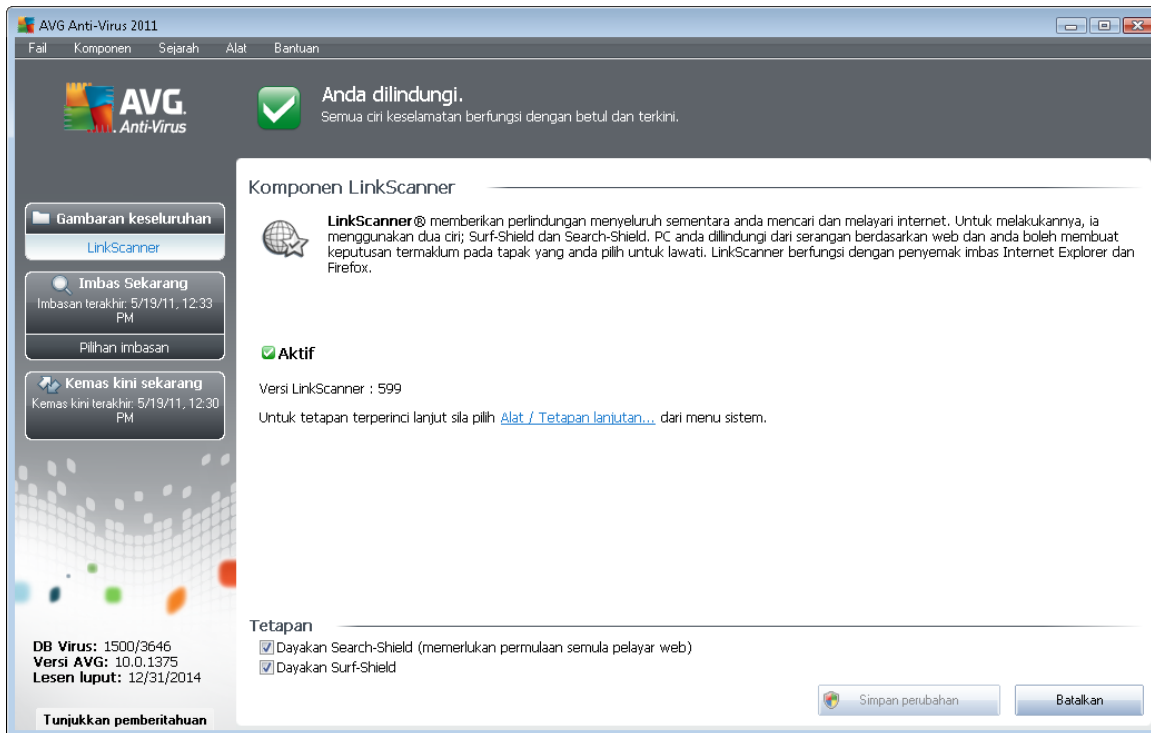
Teknologi **LinkScanner** terdiri daripada dua ciri, [Search-Shield](#) dan [Surf-Shield](#):

- **Search-Shield** mengandungi senarai laman web (*alamat URL*) yang diketahui berbahaya. Semasa membuat carian di Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, atau SlashDot, semua keputusan carian ditanda mengikut senarai ini dan ikon keputusan ditunjukkan (*untuk keputusan carian Yahoo hanya ikon keputusan "laman web dieksploitasi" ditunjukkan*).
- **Surf-Shield** mengimbas kandungan laman web yang anda lawati, tidak kira alamat laman web berkenaan. Walaupun sesetengah tapak web tidak dikesan oleh [Search-Shield](#) (*cth. apabila laman web berniat jahat yang baru dibuat atau apabila laman web yang dahulu bersih kini mengandungi beberapa malware*), ia akan dikesan dan disekat oleh [Surf-Shield](#) sebaik sahaja anda cuba melawatinya.

Nota: *LinkScanner* bukan bertujuan untuk platform pelayan!

7.3.2. Antara Muka Pengimbas Pautan

Antara muka komponen [LinkScanner](#) memberikan penerangan ringkas kefungsiannya dan maklumat komponen mengenai status semasanya. Seterusnya, anda boleh mencari maklumat mengenai nombor versi terkini pangkalan data [LinkScanner](#) (*versi LinkScanner*).



Tetapan LinkScanner

Di bahagian bawah dialog anda boleh mengedit beberapa opsiyen:

- **Dayakan Search-Shield** - (*dihidupkan secara lalai*): ikon pemberitahuan penasihat mengenai carian dilakukan dengan Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg atau SlashDot: diperiksa kandungan tapak yang dikembalikan oleh enjin carian.
- **Dayakan Surf-Shield** - (*dibuka secara lalai*): perlindungan (*masa nyata*) aktif daripada tapak yang boleh mengeksploitasi apabila ia diakses. Sambungan tapak yang diketahui berniat jahat dan kandungannya yang boleh mengeksploitasi apabila ia diakses oleh pengguna melalui penyemak imbas web (*atau sebarang aplikasi lain yang menggunakan HTTP*).

7.3.3. Search-Shield

Semasa membuat carian di Internet dengan **Search-Shield** dihidupkan, semua keputusan carian dikembalikan daripada enjin pencarian paling popular (*Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg dan SlashDot*) dinilai untuk pautan berbahaya atau mencurigakan. Dengan menanda pautan ini dan menandakan pautan jahat, **AVG Link Scanner** memberi amaran kepada anda sebelum anda mengklik pada pautan berbahaya atau mencurigakan, supaya anda boleh memastikan anda hanya pergi ke laman web selamat.

Semasa pautan dinilai pada halaman keputusan carian, anda akan melihat tanda grafik di sebelah



pautan yang memberitahu bahawa pengesahan pautan sedang dijalankan. Apabila penilaian selesai, ikon maklumat masing-masing akan dipaparkan.

Halaman yang dipautkan selamat (*ikon ini tidak akan dipaparkan untuk Yahoo! yang selamat Keputusan carian JP*).

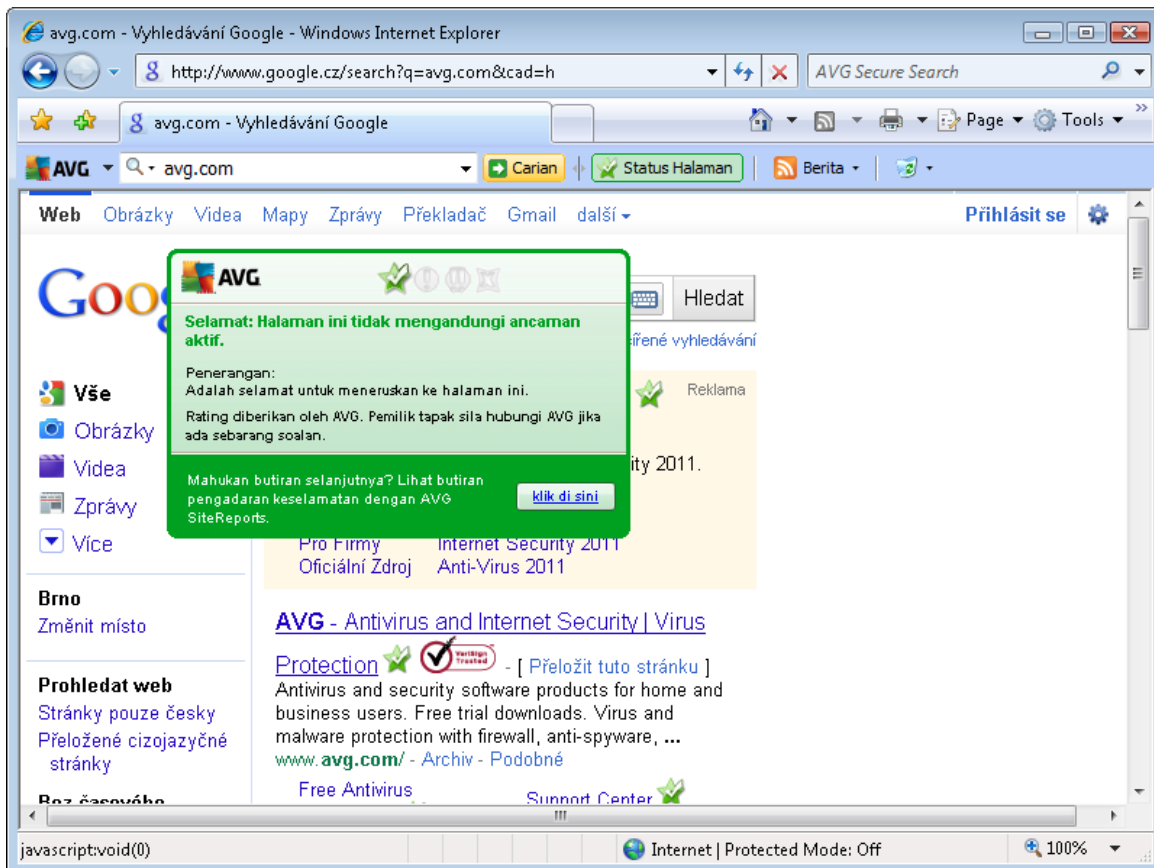
Halaman yang dipautkan tidak mengandungi ancaman tetapi agak mencurigakan (*dipersoalkan bagi asal atau motif, oleh itu, ia tidak disarankan untuk e-shopping dll.*).

Halaman yang boleh dipautkan boleh menjadi sama ada selamat sendiri tetapi mengandungi pautan selanjutnya ke halaman berbahaya secara positif; atau kod yang mencurigakan, walaupun, tidak mempunyai sebarang ancaman secara terus buat masa ini.

Halaman berpaut mengandungi ancaman aktif! Untuk keselamatan anda sendiri, anda tidak akan dibenarkan untuk melawati halaman ini.

Hhalaman yang dipautkan tidak boleh diakses dan oleh itu, tidak boleh diimbas.

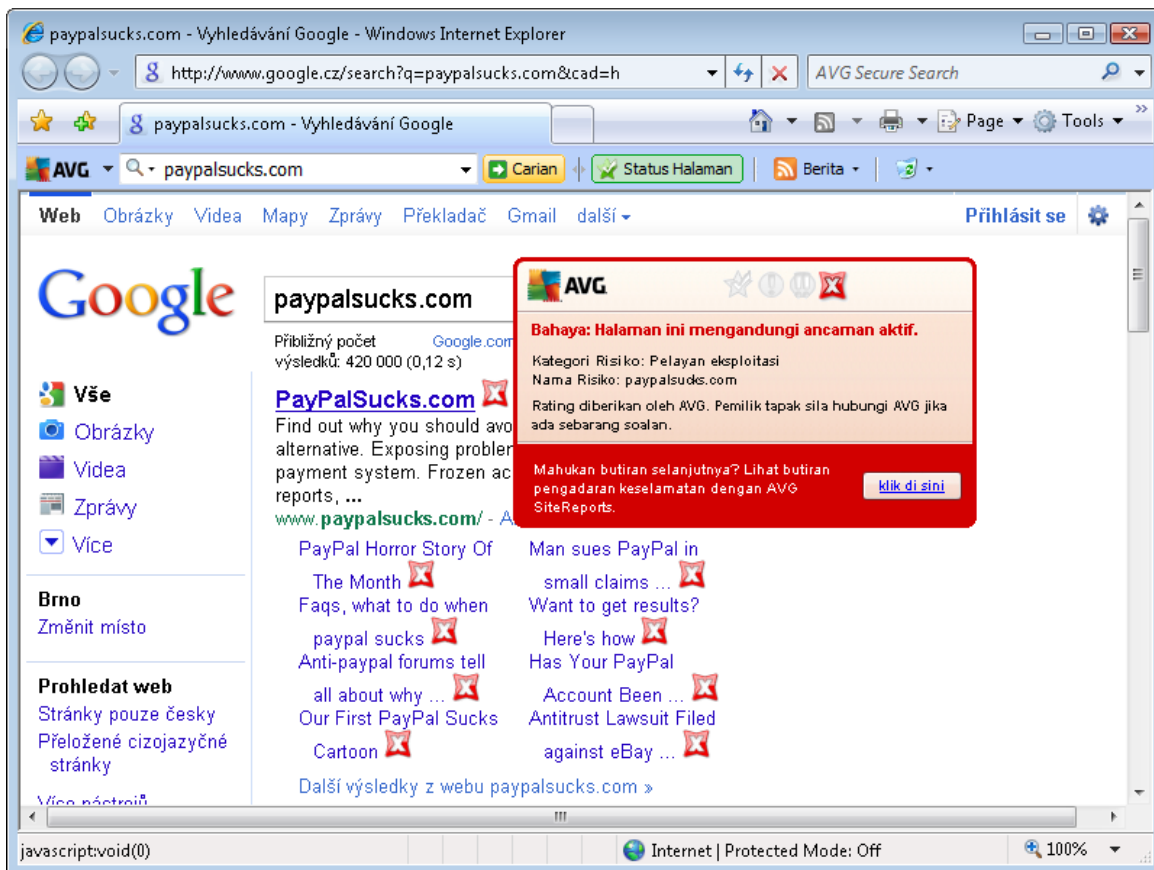
Menghalakan pada setiap ikon pengedaran akan memaparkan butiran mengenai pautan khusus yang dipersoalkan. Maklumat termasuk butiran tambahan mengenai ancaman (*jika ada*):



7.3.4. Perisai Layar

Perlindungan yang berkuasa ini menyekat kandungan sebarang laman web yang anda cuba untuk buka dan mengelaknya daripada dimuat turun ke komputer anda. Dengan ciri ini didayakan, mengklik pautan atau menaip dalam URL ke tapak berbahaya akan menghalang anda daripada membuka laman web secara automatik, dengan itu, melindungi anda daripada dijangkiti secara lalai. Adalah penting untuk mengingati bahawa halaman web dieksploitasi boleh menjangkiti komputer anda hanya dengan melawati tapak yang terlibat, untuk tujuan ini apabila anda meminta halaman web berbahaya mengandungi eksploitasi atau ancaman serius lain, [AVG Link Scanner](#) tidak akan membenarkan penyemak imbas anda memaparkannya.

Jika anda berhadapan dengan tapak web berniat jahat dalam pelayar web anda [AVG Link Scanner](#) akan memberi amaran kepada anda dengan skrin yang sama dengan:



Memasuki tapak web sangat berisiko dan ia tidak disyorkan!

7.4. Perisai Residen

7.4.1. Prinsip Perisai Residen

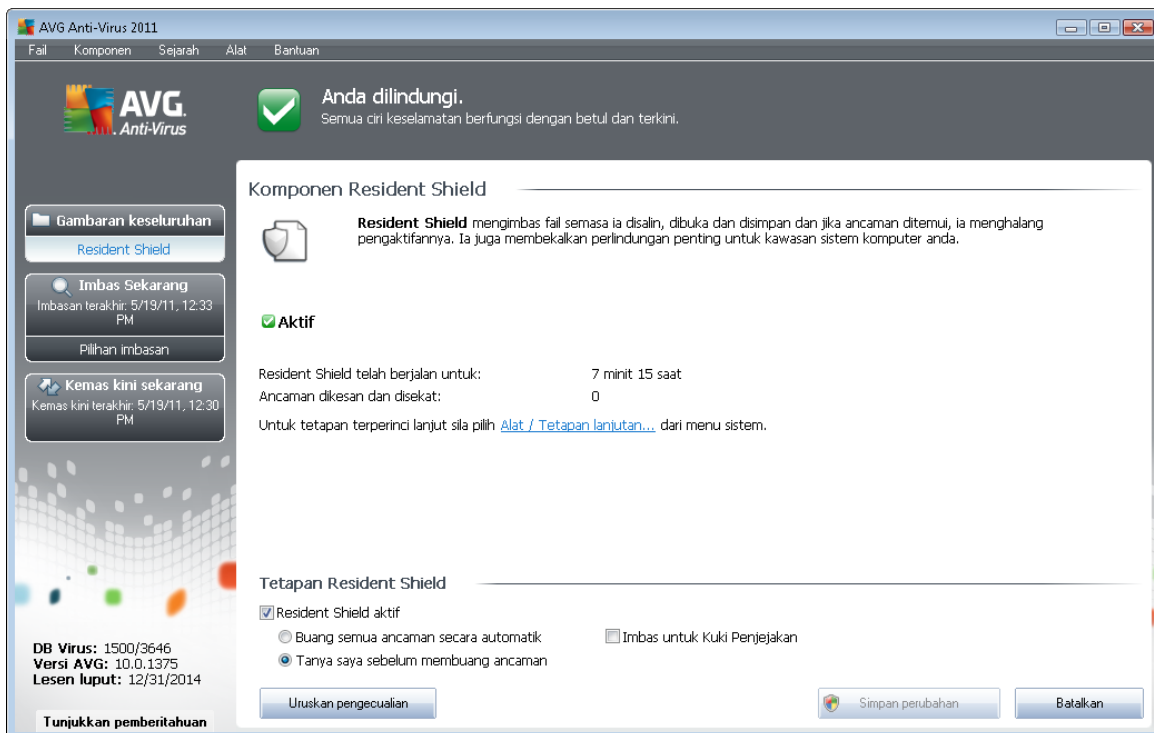
Komponen **Perisai Residen** memberikan komputer anda perlindungan berterusan. Ia mengimbas setiap fail yang dibuka, disimpan, atau disalin, dan mengawal kawasan sistem komputer. Apabila **Perisai Residen** menemui virus dalam fail yang diakses, ia menghentikan operasi yang sedang dijalankan dan tidak membenarkan virus untuk diaktifkan dengan sendiri. Biasanya, anda langsung tidak perasan proses itu, memandangkan ia berjalan "di belakang", dan anda hanya akan diberitahu apabila ancaman ditemui; dalam masa yang sama, **Perisai Residen** menyekat pengaktifan ancaman dan membuangnya. **Perisai Residen** sedang dimuatkan dalam memori komputer anda sewaktu permulaan sistem.

Apa yang boleh **Perisai Residen** lakukan?

- Imbas untuk jenis kemungkinan ancaman khusus
- Imbas media boleh ditanggalkan (*cakera denyar dll.*)
- Imbas fail dengan sambungan khusus atau tiada sambungan langsung
- Benarkan pengecualian dari imbasan - fail atau folder khusus yang tidak perlu diimbas

Amaran: Perisai Residen dimuatkan dalam memori komputer anda semasa permulaan, dan adalah penting anda memastikannya hidup sepanjang masa!

7.4.2. Antara Muka Perisai Residen



Di samping gambaran keseluruhan kefungsiian **Perisai Residen**, dan maklumat mengenai status komponen, antara muka **Perisai Residen** turut menawarkan beberapa data statistik:



- **Perisai Residen telah dijalankan untuk** - memberikan masa sejak komponen terkini dilancarkan
- **Ancaman dikesan dan disekat** - bilangan jangkitan yang dikesan yang dielakkan daripada dijalankan/dibuka (*jika perlu, nilai ini boleh ditetapkan semula; cth. untuk tujuan statistik - Tetapkan semula nilai*)

Tetapan Resident Shield

Dalam bahagian bawah tettingkap dialog, anda akan menemui bahagian yang dipanggil **tetapan Perisai Residen** di mana anda boleh mengedit beberapa tetapan asas bagi kefungsiian komponen (konfigurasi terperinci dengan semua komponen lain tersedia melalui item tetapan Alat/Lanjutan bagi menu sistem).

Opsyen **Perisai Residen adalah aktif** membenarkan anda menghidupkan/mematikan perlindungan residen dengan mudah. Secara lalai, fungsi dihidupkan. Dengan perlindungan residen dihidupkan, anda seterusnya boleh menentukan cara kemungkinan jangkitan yang dikesan harus dirawat (dibuang).

- sama ada secara automatik (**Buang semua ancaman secara automatik**)
- atau hanya selepas kelulusan pengguna (**Tanya saya sebelum membuang ancaman**)

Pilihan ini tidak memberi kesan kepada tahap keselamatan dan ia hanya menjejaskan keutamaan anda.

Dalam kedua-dua kes, anda masih boleh memilih sama ada anda hendak **Mengimbas untuk kuki penjejakan**. Dalam kes tertentu, anda boleh mengalihkan opsyen ini kepada mendapatkan tahap keselamatan maksimum, walau bagaimanapun, ia dimatikan secara lalai. (*kuki = bungkusan teks dihantar oleh pelayan ke pelayar web dan kemudian, dihantar semula tanpa diubah oleh pelayar setiap kali ia mengakses pelayan tersebut. Kuki HTTP digunakan untuk mengesahkan, menjejaki dan mengekalkan maklumat khusus mengenai pengguna seperti keutamaan tapak atau kandungan kart beli-belah elektronik mereka*).

Sila ambil perhatian: Vendor perisian telah menyediakan semua komponen AVG untuk memberikan prestasi optimum. Melainkan anda mempunyai alasan penting untuk melakukannya, jangan ubah konfigurasi AVG. Sebarang pertukaran kepada tetapan sepatutnya dilakukan oleh pengguna berpengalaman sahaja. Jika anda perlu mengubah konfigurasi AVG, pilih item menu sistem **Alat / Tetapan lanjutan** dan edit konfigurasi AVG dalam dialog [Tetapan Lanjutan AVG](#) yang baru dibuka.

Butang kawalan

Butang kawalan tersedia dalam antara muka **Perisai Residen** seperti berikut:

- **Uruskan pengecualian** - membuka dialog [Perisai Residen - Item Dikecualikan](#) di mana anda boleh menentukan folder dan fail yang harus ditinggalkan daripada pengimbasan [Perisai Residen](#)



- **Simpan perubahan** - tekan butang ini untuk menyimpan dan menggunakan sebarang perubahan yang dibuat dalam dialog ini
- **Batal** - tekan butang ini untuk kembali ke [antara muka pengguna AVG lalai](#) (gambaran keseluruhan komponen)

7.4.3. Pengesanan Perisai Residen

Perisai Residen mengimbas fail semasa ia disalin, dibuka atau disimpan. Apabila virus atau sebarang jenis ancaman dikesan, anda akan diberi amaran serta-merta melalui dialog berikut:



Dalam dialog amaran ini anda akan menemui data mengenai fail yang dikesan dan ditentukan sebagai dijangkiti (*Nama fail*), nama jangkitan yang dikenal pasti (*Nama ancaman*), dan pautan ke [Ensiklopedia Virus](#) di mana anda boleh menemui maklumat terperinci mengenai jangkitan yang dikesan, jika diketahui (*Maklumat lanjut*).

Selain itu, anda perlu membuat keputusan apa tindakan yang harus diambil sekarang - opsyen berikut tersedia:

Sila maklum bahawa, pada keadaan tertentu (apa jenis fail yang dijangkiti, dan di mana ia terletak), tidak semua opsyen sentiasa tersedia!

- **Alih keluar ancaman sebagai Pengguna Kuasa** – tandakan kotak jika anda rasa anda mungkin tidak mempunyai hak yang mencukupi untuk mengalih keluar ancaman sebagai pengguna biasa. Pengguna Kuasa mempunyai hak akses menyeluruh, dan jika ancaman terletak dalam folder sistem yang tertentu, anda mungkin perlu menggunakan kotak semakan ini untuk mengalih keluarnya dengan jaya.
- **Rawat** - butang ini hanya muncul jika jangkitan yang dikesan boleh dirawat. Kemudian, ia mengalihnya keluar dari fail, dan memulihkan fail ke keadaan asal. Jika fail itu sendiri merupakan virus, gunakan fungsi ini untuk memadamnya (*iaitu dialih keluar ke [Bilik Kebal Virus](#)*)

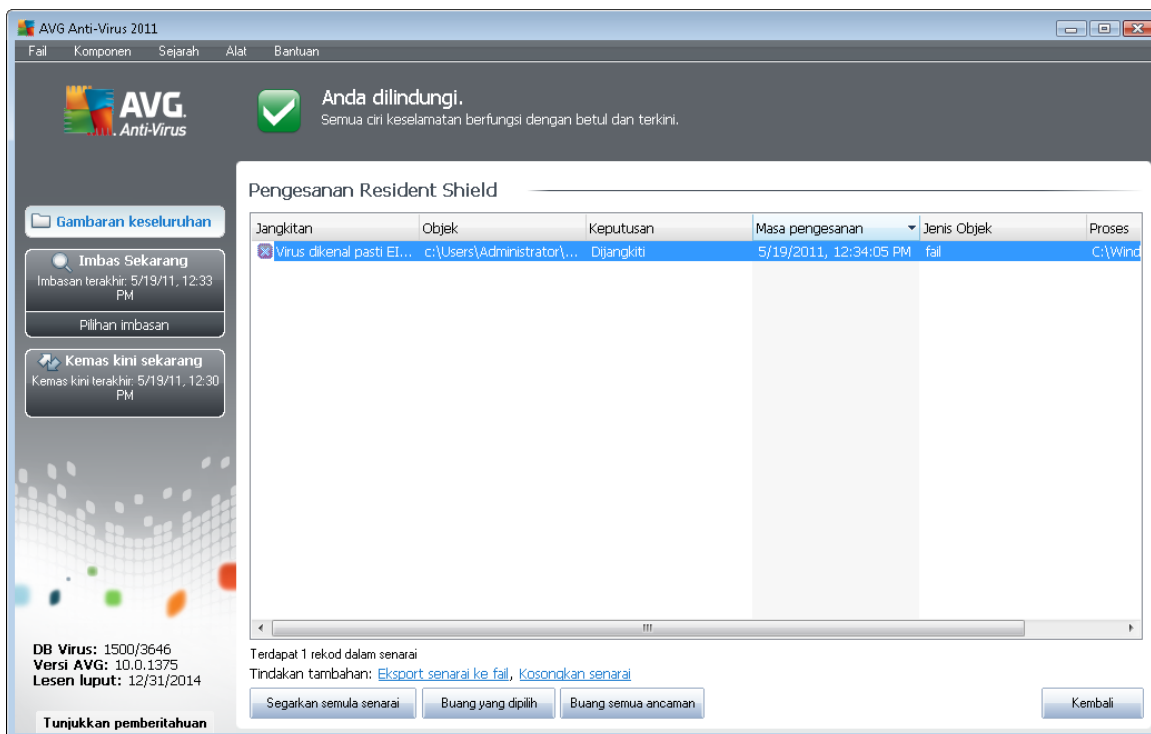


- **Alih ke Bilik Kebal** - virus tersebut akan dialihkan ke Bilik Kebal [AVG](#)
- **Pergi ke fail** - opsyen ini mengarahkan anda semula ke lokasi sebenar bagi objek yang mencurigakan (*membuka tettingkap Windows Explorer baru*)
- **Abaikan** - kami amat menyarankan UNTUK TIDAK menggunakan opsyen ini melainkan anda mempunyai alasan yang sangat kukuh untuk melakukannya!

Nota: Mungkin berlaku saiz objek yang dikesan melebihi had ruang bebas dalam Bilik Kebal Virus. Jika yang demikian, pop timbul mesej amaran memaklumkan anda mengenai isu apabila anda cuba mengalihkan objek yang dijangkiti ke Bilik Kebal Virus. Walau bagaimanapun, saiz Bilik Kebal Virus boleh diedit. Adalah ditentukan sebagai peratus boleh diubah suai bagi saiz sebenar cakera keras anda. Untuk meningkatkan saiz Bilik Kebal Virus anda, pergi ke dialog [Bilik Kebal Virus](#) dalam [Tetapan Lanjutan AVG](#), melalui opsyen 'Had saiz Bilik Kebal Virus'.

Di bahagian bawah dialog ini anda boleh menemui pautan **Tunjuk butiran** - klik untuk membuka tettingkap pop timbul dengan maklumat terperinci mengenai proses yang berjalan semasa jangkitan dikesan, dan pengenalan proses berkenaan.

Gambaran keseluruhan bagi semua ancaman yang dikesan oleh [Perisai Residen](#) boleh ditemui dalam dialog **pengesanan Perisai Residen** yang boleh diakses dari opsyen menu sistem [pengesanan Sejarah / Perisai Residen](#):



Pengesanan Perisai Residen menawarkan gambaran keseluruhan objek yang dikesan oleh [Perisai Residen](#), dinilai sebagai berbahaya dan sama ada dipulihkan atau dialihkan ke [Bilik Kebal Virus](#). Untuk setiap objek yang dikesan, maklumat berikut disediakan:



- **Jangkitan**- penerangan (malahan juga nama) bagi objek yang dikesan
- **Objek** - lokasi objek
- **Keputusan** - tindakan dilakukan dengan objek yang dikesan
- **Masa pengesanan** - tarikh dan masa objek dikesan
- **Jenis Objek** - jenis objek yang dikesan
- **Proses** - tindakan apa yang dilakukan untuk memanggil objek berpotensi berbahaya supaya ia boleh dikesan

Di bahagian bawah dialog, di bawah senarai, anda akan menemui maklumat mengenai jumlah bilangan objek dikesan yang disenaraikan di atas. Seterusnya, anda boleh mengeksport keseluruhan senarai objek yang dikesan dalam fail (**Eksport senarai ke fail**) dan padam semua entri pada objek dikesan (**Kosongkan senarai**). Butang **Muat semula senarai** akan mengemas kini senarai penemuan yang dikesan oleh **Perisai Residen**. Butang **Undur** mengalihkan anda semula ke [antara muka pengguna AVG](#) (gambaran keseluruhan komponen).

7.5. Family Safety

AVG Family Safety membantu anda melindungi anak anda daripada laman web, kandungan media dan carian dalam talian yang tidak sesuai, dan memberikan anda laporan berkenaan aktiviti dalam talian mereka. Anda boleh menetapkan tahap perlindungan yang sesuai untuk setiap anak anda dan memantaunya secara berasingan melalui log masuk unik.

Komponen aktif hanya semasa produk **AVG Family Safety** dipasang pada mesin anda. Jika anda tidak mempunyai produk **AVG Family Safety** dipasangkan, klik ikon masing-masing dalam antara muka pengguna **AVG Anti-Virus 2011** dan anda akan diarahkan semula kepada laman web produk yang mana anda akan mendapati semua butiran yang diperlukan.

7.6. AVG LiveKive

AVG LiveKive secara automatik membuat sandaran semua fail, foto dan muzik anda di satu tempat yang selamat, membolehkan anda berkongsi dengan keluarga dan rakan dan mengaksesnya dari sebarang peranti didayakan web, termasuk peranti iPhones dan Android.

Komponen aktif hanya semasa produk **AVG LiveKive** dipasang pada mesin anda. Jika anda belum memasang produk **AVG LiveKive** dipasang, klik ikon masing-masing dalam antara muka pengguna **AVG Anti-Virus 2011** dan anda akan diarahkan semula ke laman web produk di mana anda boleh mendapatkan semua butiran yang diperlukan.

7.7. Pengimbas E-mel

Salah satu sumber virus dan trojan yang paling biasa adalah melalui e-mel. Pemalsuan dan spam membuatkan e-mel menjadi sumber risiko yang lebih hebat. Akaun e-mel percuma adalah lebih berkemungkinan menerima e-mel berniat jahat seperti itu (*kerana ia jarang menggunakan teknologi antispam*), dan pengguna rumah bergantung agak kuar pada e-mel seperti itu. Serta pengguna rumah yang melayari tapak yang tidak diketahui dan mengisi borang dalam talian dengan data



peribadi (*seperti alamat e-mel mereka*) meningkatkan pendedahan kepada serangan melalui e-mel. Syarikat biasanya menggunakan akaun e-mel korporat dan menggunakan penapis antispam dan lain-lain untuk mengurangkan risiko.

7.7.1. Prinsip Pengimbas E-mel

Pengimbas E-mel Peribadi mengimbas e-mel masuk/keluar secara automatik. Anda boleh menggunakannya bersama klien e-mel yang tidak mempunyai pasang masuknya sendiri di dalam AVG (*tetapi boleh turut digunakan untuk mengimbas mesej e-mel untuk klien e-mel yang disokong AVG menggunakan pasang masuk khusus, iaitu Microsoft Outlook, dan The Bat*). Ia perlu digunakan terutamanya bersama aplikasi e-mel seperti Outlook Express, Mozilla, Incredimail, dll.

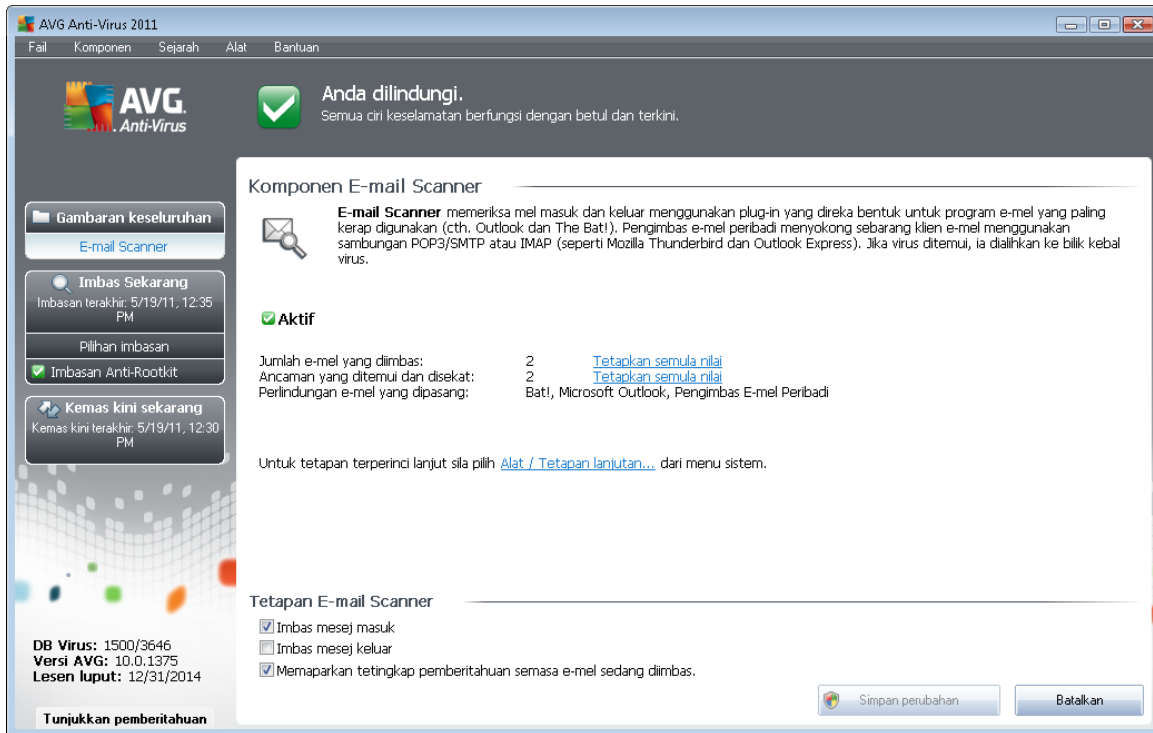
Sewaktu pemasangan [AVG](#) AVG terdapat pelayan automatik dibuat untuk kawalan e-mel: satu untuk memeriksa e-mel masuk dan yang kedua untuk memeriksa e-mel keluar. Menggunakan dua pelayan ini, e-mel diperiksa secara automatik pada port 110 dan 25 (*port standard untuk menghantar/menerima e-mel*).

Pengimbas E-mel berfungsi sebagai antara muka di antara klien e-mel dan pelayan e-mel pada Internet.

- **Mel masuk:** Apabila menerima mesej daripada pelayan, komponen **Pengimbas E-mel** mengujinya untuk virus, membuang lampiran yang dijangkiti dan menambah perakuan. Semasa dikesan, virus dikuarantin dalam [Bilik Kebal Virus](#) dengan serta-merta. Kemudian mesej itu diberikan kepada klien e-mel.
- **Mel Keluar:** Mesej dihantar dari klien e-mel ke Pengimbas E-mel; ia menguji mesej dan lampirannya untuk virus dan kemudian, menghantar mesej ke pelayan SMTP (*mengimbas e-mel keluar dinyahdayakan secara lalai dan boleh disediakan secara manual*).

Nota: Pengimbas E-mel AVG bukan bertujuan untuk platform pelayan!

7.7.2. Antara Muka Pengimbas E-mel



Dalam dialog komponen **Pengimbas E-mel** anda boleh menemui teks ringkas yang menerangkan kefungsiian komponen, maklumat mengenai status semasanya, dan (statistik berikut):

- **Jumlah e-mel yang diimbas** - berapa banyak mesej e-mel yang diimbas sejak **Pengimbas E-mel** dilancarkan kali terakhir (*jika perlu, nilai ini boleh ditetapkan semula; cth. untuk tujuan statistik - Tetapkan semula nilai*)
- **Ancaman ditemui dan disekat** - memberikan bilangan jangkitan yang dikesan dalam setiap mesej e-mel sejak kali terakhir **Pengimbas E-mel** dilancarkan
- **Perlindungan e-mel yang dipasang** - maklumat mengenai plug-in perlindungan e-mel khusus merujuk kepada klien e-mel lalai anda yang dipasang

Tetapan Pengimbas E-mel

Di bahagian bawah dialog, anda boleh menemui bahagian yang dinamakan **tetapan Pengimbas E-mel** di mana anda boleh mengedit beberapa ciri permulaan bagi kefungsiian komponen:

- **Imbas mesej masuk** - memeriksa item untuk menentukan bahawa semua e-mel yang dihantar ke akaun anda harus diimbas untuk virus. Secara lalai, item ini dihidupkan dan adalah disyorkan untuk tidak menukar tetapan ini!
- **Imbas mesej keluar** - memeriksa item untuk mengesahkan bahawa semua e-mel yang dihantar dari akaun anda harus diimbas untuk virus. Secara lalai, item ini dimatikan.



- **Paparkan tettingkap pemberitahuan semasa e-mel diimbis** - periksa item untuk mengesahkan anda hendak dimaklumkan melalui dialog pemberitahuan yang dipaparkan pada ikon AVG pada dulang sistem sewaktu pengimbasan mel anda melalui komponen [Pengimbas E-mel](#) . Secara lalai, item ini dihidupkan dan adalah disyorkan untuk tidak menukar tetapan ini!

Konfigurasi lanjutan bagi komponen **Pengimbas E-mel** boleh diakses melalui item **tetapan Alat/ Lanjutan** bagi menu sistem; walau bagaimanapun, konfigurasi lanjutan disarankan untuk pengguna berpengalaman sahaja!

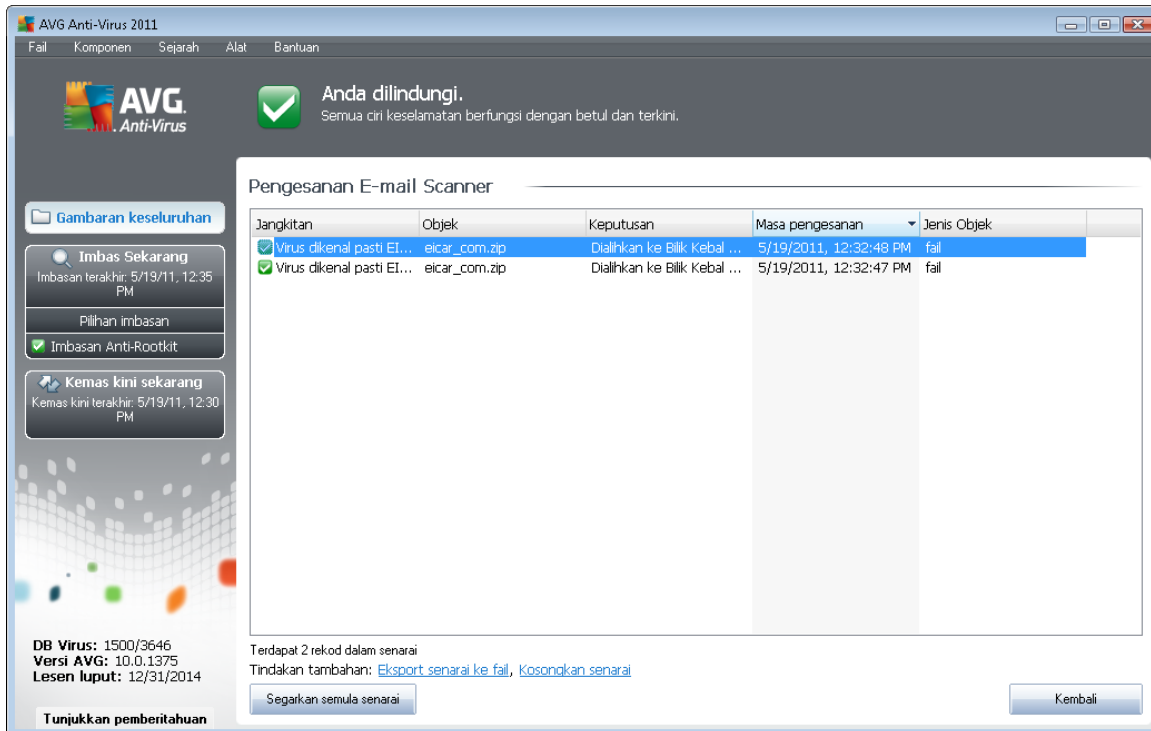
Sila ambil perhatian: Vendor perisian telah menyediakan semua komponen AVG untuk memberikan prestasi optimum. Melainkan anda mempunyai alasan penting untuk melakukannya, jangan ubah konfigurasi AVG. Sebarang pertukaran kepada tetapan sepatutnya dilakukan oleh pengguna berpengalaman sahaja. Jika anda perlu mengubah konfigurasi AVG, pilih item menu sistem **Alat / Tetapan lanjutan** dan edit konfigurasi AVG dalam dialog [Tetapan Lanjutan AVG](#) yang baru dibuka.

Butang kawalan

Butang kawalan dalam antara muka **Pengimbas E-mel** adalah seperti berikut:

- **Simpan perubahan** - tekan butang ini untuk menyimpan dan menggunakan sebarang perubahan yang dibuat dalam dialog ini
- **Batal** - tekan butang ini untuk kembali ke [antara muka pengguna AVG lalai](#) (gambaran keseluruhan komponen)

7.7.3. Pengesanan Pengimbas E-mel



Dalam dialog **pengesanan Pengimbas E-mel** (boleh diakses melalui menu sistem opsyen *Sejarah / pengesanan Pengimbas E-mel*) anda boleh melihat senarai semua penemuan yang dikesan oleh komponen **Pengimbas E-mel**. Untuk setiap objek yang dikesan, maklumat berikut disediakan:

- **Jangkitan**- penerangan (malahan juga nama) bagi objek yang dikesan
- **Objek** - lokasi objek
- **Keputusan** - tindakan dilakukan dengan objek yang dikesan
- **Masa pengesanan** - tarikh dan masa objek mencurigakan dikesan
- **Jenis Objek** - jenis objek yang dikesan

Di bahagian bawah dialog, di bawah senarai, anda akan menemui maklumat mengenai jumlah bilangan objek dikesan yang disenaraikan di atas. Seterusnya, anda boleh mengekspor keseluruhan senarai objek yang dikesan dalam fail (**Eksport senarai ke fail**) dan padam semua entri pada objek dikesan (**Kosongkan senarai**).

Butang kawalan

Butang kawalan tersedia dalam antara muka **pengesanan Pengimbas E-mel** adalah seperti berikut:

- **Muat semula senarai** - mengemas kini senarai ancaman yang dikesan



- **Kembali** - menukar anda kembali dialog yang dipaparkan sebelum ini

7.8. Pengurus Kemas Kini

7.8.1. Kemas Kini Prinsip Pengurus

Tiada perisian keselamatan yang boleh menjamin perlindungan sebenar dari pelbagai jenis ancaman melainkan ia dikemas kini secara tetap! Penulis virus sentiasa mencari kecelehan baru yang mereka boleh mengeksploitasi dalam perisian dan juga sistem pengendalian. Virus baru, malware baru, serangan penggadam baru muncul setiap hari. Oleh itu, vendor perisian berterusan mengeluarkan kemas kini dan tampalan keselamatan untuk membaiki sebarang lubang keselamatan yang didapati.

Adalah penting untuk mengemas kini AVG anda secara tetap!

Pengurus Kemas Kini membantu anda mengawal kemas kini tetap. Dalam komponen ini, anda boleh menjadualkan muat turun automatik bagi fail kemas kini sama ada dari Internet atau rangkaian tempatan. Kemas kini definisi virus penting patut dilakukan setiap hari, jika boleh. Kemas kini atur cara yang kurang penting boleh dilakukan setiap minggu.

Nota: Sila berikan perhatian kepada bab [Kemas Kini AVG](#) untuk maklumat lanjut mengenai jenis dan tahap kemas kini!

7.8.2. Kemas Kini Antara Muka Pengurus



Antara muka **Pengurus Kemas Kini** memaparkan maklumat mengenai kefungsiian komponen dan status semasanya, dan menyediakan data statistik relevan:

- **Kemas kini terkini** - menyatakan tarikh dan masa bagi kemas kini pangkalan data terakhir
- **Versi pangkalan data virus** - menentukan bilangan versi pangkalan data virus yang sedia dipasang; dan nombor ini meningkat dengan setiap kemas kini pangkalan data virus
- **Kemas kini yang dijadualkan seterusnya** - menyatakan tarikh dan masa bagi kemas kini pangkalan data seterusnya

tetapan Pengurus Kemas Kini

Di bahagian bawah dialog, anda boleh menemui bahagian **tetapan Pengurus Kemas Kini** di mana anda boleh melakukan beberapa perubahan kepada peraturan pelancaran proses kemas kini. Anda boleh mentakrifkan sama ada anda mahukan fail kemas kini dimuat turun secara automatik (**Mulakan kemas kini automatik**) atau hanya dalam permintaan. Secara lalai, opsiyen **Mulakan kemas kini automatik** dihidupkan dan kami mengesyorkan untuk mengekalkannya! Muat turun tetap bagi fail kemas kini terkini adalah penting untuk kefungsiian yang betul bagi sebarang perisian keselamatan!

Seterusnya, anda boleh menentukan bila kemas kini patut dilancarkan:

- **Secara berkala** - tentukan selang masa
- **Pada selang masa tertentu** - takrifkan masa hari yang tepat kemas kini perlu dilancarkan

Secara lalai, kemas kini ditetapkan pada setiap 4 jam. Ia amat disyorkan untuk mengekalkan tetapan ini melainkan anda mempunyai alasan yang betul untuk mengubahnya!

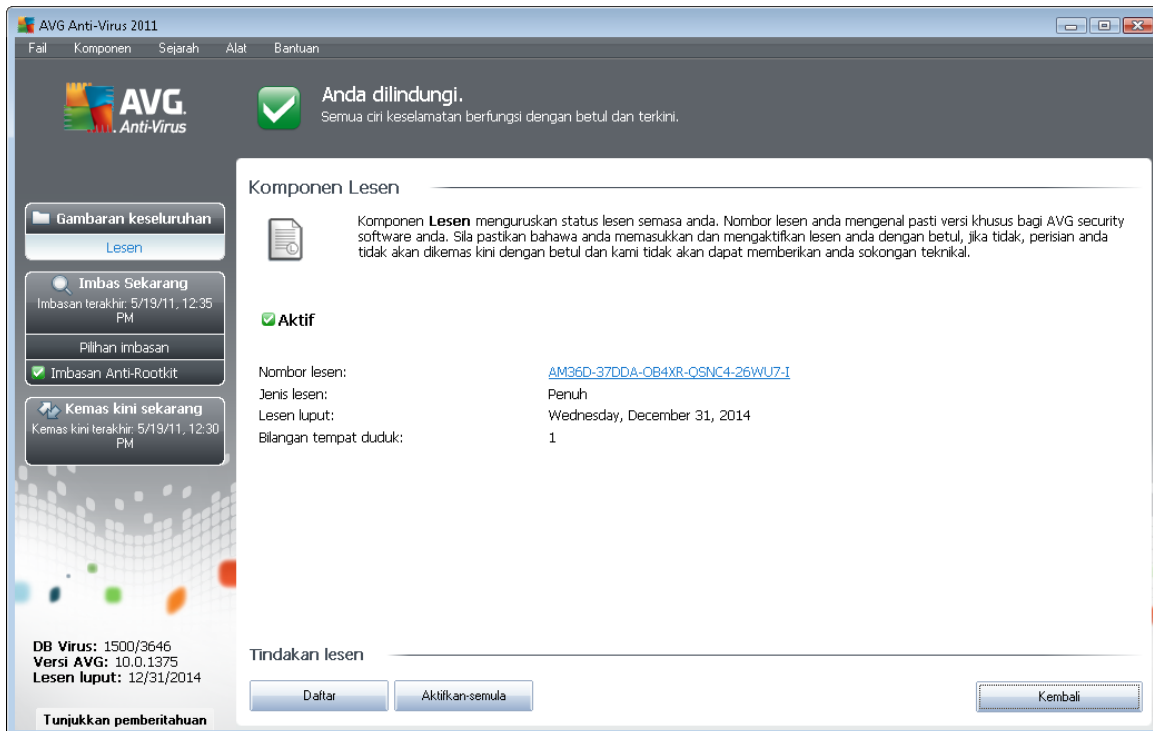
Sila ambil perhatian: Vendor perisian telah menyediakan semua komponen AVG untuk memberikan prestasi optimum. Melainkan anda mempunyai alasan penting untuk melakukannya, jangan ubah konfigurasi AVG. Sebarang pertukaran kepada tetapan sepatutnya dilakukan oleh pengguna berpengalaman sahaja. Jika anda perlu mengubah konfigurasi AVG, pilih item menu sistem **Alat / Tetapan lanjutan** dan edit konfigurasi AVG dalam dialog [Tetapan Lanjutan AVG](#) yang baru dibuka.

Butang kawalan

Butang kawalan yang tersedia dalam antara muka **Pengurus Kemas Kini** adalah seperti berikut:

- **Kemas kini sekarang** - melancarkan [kemas kini segera](#) dalam permintaan
- **Simpan perubahan** - tekan butang ini untuk menyimpan dan menggunakan sebarang perubahan yang dibuat dalam dialog ini
- **Batal** - tekan butang ini untuk kembali ke [antara muka pengguna AVG lalai](#) (gambaran keseluruhan komponen)

7.9. Lesen



Dalam antara muka komponen **Lesen** anda akan menemui teks ringkas menerangkan kegunaan komponen, maklumat mengenai status terkini, dan maklumat (berikut):

- **Nombor lesen** - menyediakan bentuk nombor lesen anda yang dipendekkan (*atas sebab keselamatan empat simbol akhir hilang*). Semasa memasukkan nombor lesen anda, anda perlu betul-betul tepat dan menaipnya betul-betul seperti yang ditunjukkan. Oleh itu, kami amat mengesyorkan untuk sentiasa menggunakan kaedah "salin & tampal" untuk sebarang manipulasi dengan nombor lesen.
- **Jenis lesen** - menentukan jenis produk yang dipasang.
- **Lesen tamat tempoh** - tarikh ini menentukan tempoh kesahan lesen anda. Jika anda hendak terus menggunakan **AVG Anti-Virus 2011** selepas tarikh ini, anda perlu memperbaharui lesen anda. Pembaharuan lesen boleh dilakukan dalam talian pada [laman web AVG](http://www.avg.com).
- **Bilangan tempat duduk** - berapa banyak stesen kerja pada mana anda tertakluk untuk memasang **AVG Anti-Virus 2011** anda.

Butang kawalan

- **Daftar** - menyambungkan ke halaman pendaftaran bagi tapak web AVG (<http://www.avg.com/>). Sila isikan data pendaftaran anda; hanya pelanggan yang mendaftarkan produk AVG mereka boleh menerima sokongan teknikal percuma.

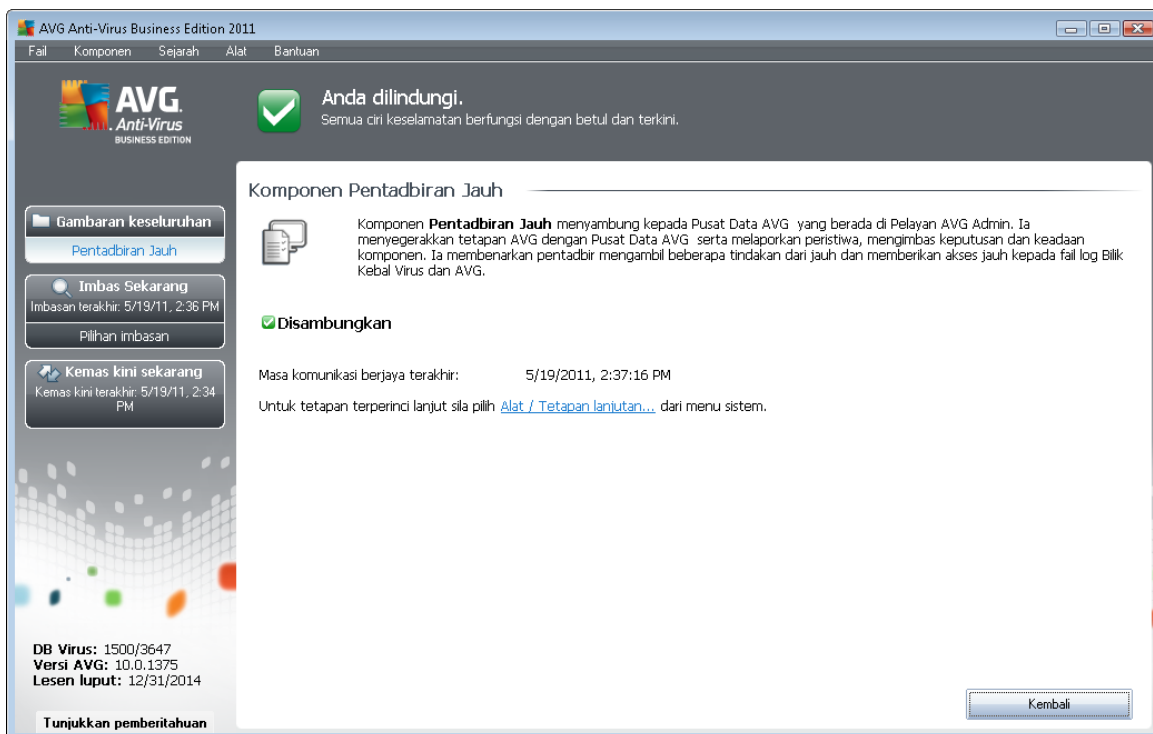


- **Aktifkan semula** - membuka dialog **Aktifkan AVG** dengan data yang anda telah masukkan dalam dialog **Peribadikan AVG** bagi [proses pemasangan](#). Dalam dialog ini, anda boleh memasukkan nombor lesen anda dengan sama ada menggantikan nombor jualan (*nombor yang anda telah pasangkan AVG*), atau untuk menggantikan nombor lesen lama (*cth. semasa menaik taraf ke produk AVG baru*).

Perhatian: Jika menggunakan versi percubaan bagi **AVG Anti-Virus 2011**, butang muncul sebagai **Beli sekarang** dan **Aktifkan**, membenarkan anda membeli versi penuh bagi atur cara dengan serta-merta. Untuk **AVG Anti-Virus 2011** yang dipasang dengan nombor jualan, butang dipaparkan sebagai **Daftar** dan **Aktifkan**.

- **Kembali** - tekan butang ini untuk kembali ke [antara muka AVG](#)alai (gambaran keseluruhan komponen).

7.10. Pentadbiran Jauh



Komponen **Pentadbiran Jauh** hanya memaparkan dalam antara muka pengguna **AVG Anti-Virus 2011** jika anda telah memasang Business Edition produk anda (*lihat komponen [Lesen](#)*). Dalam dialog **Pentadbiran Jauh** anda boleh menemui maklumat mengenai sama ada komponen ini aktif dan disambungkan ke pelayan. Semua tetapan komponen **Pentadbiran Jauh** perlu dilakukan dalam **Tetapan Lanjutan / Pentadbiran Jauh**.

Untuk penerangan terperinci mengenai opsyen dan kefungsiian komponen dalam sistem Pentadbiran Jauh AVG sila rujuk dokumentasi khusus yang ditetapkan untuk topik in secara eksklusif. Dokumentasi ini sedia untuk dimuat turun di [laman web AVG \(www.avg.com\)](http://www.avg.com), dalam bahagian **Pusat sokongan / Muat turun / Dokumentasi**.



Butang kawalan

- **Kembali** - tekan butang ini untuk kembali ke [antara muka AVG](#) lalai (*gambaran keseluruhan komponen*).

7.11. Perisai Dalam Talian

7.11.1. Prinsip Perisai Dalam Talian

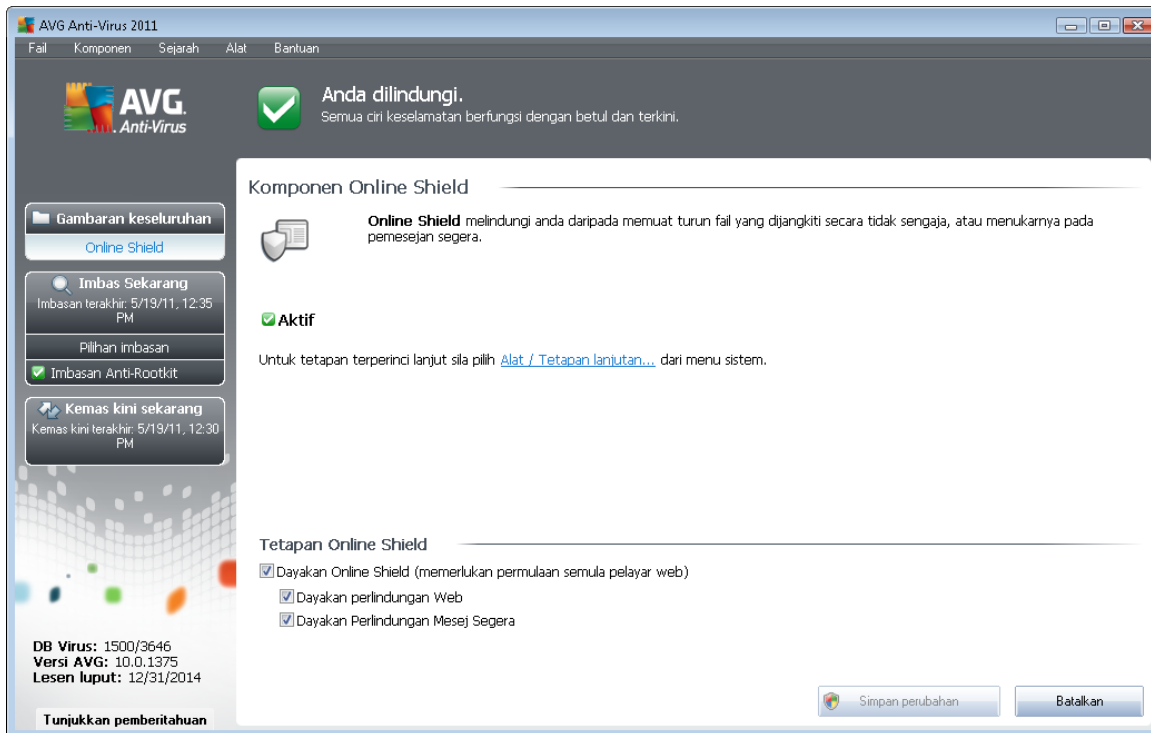
Online Shield adalah sejenis perlindungan residen masa nyata; ia mengimbas kandungan halaman web yang dilawati (*dan kemungkinan fail yang dimasukkan di dalamnya*) walaupun sebelum ini dipaparkan dalam pelayar web anda atau dimuat turun ke komputer anda.

Perisai Dalam Talian mengesan bahawa halaman yang anda akan lawati memasukkan beberapa javascript berbahaya dan mengelakkan halaman daripada dipaparkan. Serta, ia mengenal pasti malware yang terkandung dalam halaman dan menghentikan muat turunnya dengan serta-merta supaya ia tidak pergi ke komputer anda.

Perhatian: AVG Perisai Dalam Talian bukan bertujuan untuk platform pelayan!

7.11.2. Antara Muka Perisai Dalam Talian

Antara muka komponen **Perisai Dalam Talian** menerangkan kelakuan jenis perlindungan ini. Selain itu anda boleh menemui maklumat mengenai status semasa komponen. Di bahagian bawah dialog, kemudian, anda akan menemui opsyen pengeditan bagi kefungisian komponen ini:



Tetapan Online Shield

Pertama sekali, anda mempunyai pilihan untuk menghidupkan/mematikan **Perisai Dalam Talian** dengan segera dengan menandakan item **Dayakan Perisai Dalam Talian**. Pilihan ini didayakan secara lalai dan komponen **Perisai Dalam Talian** adalah aktif. Walau bagaimanapun, jika anda tidak mempunyai alasan yang baik untuk mengubah tetapan ini, kami mengesyorkan untuk memastikan komponen aktif. Jika item ini ditandakan, dan **Online Shield** berjalan, dua lagi opsi konfigurasi akan diaktifkan:

- **Dayakan perlindungan Web** - pilihan ini mengesahkan bahawa **Online Shield** harus menjalankan pengimbasan kandungan laman web.
- **Dayakan perlindungan Pemesejan Segera** - tandakan item ini jika anda mahukan **Perisai Dalam Talian** mengesahkan komunikasi pemesejan segera (*cth. ICQ, MSN Messenger, ...*) bebas virus.

Sila ambil perhatian: Vendor perisian telah menyediakan semua komponen AVG untuk memberikan prestasi optimum. Melainkan anda mempunyai alasan penting untuk melakukannya, jangan ubah konfigurasi AVG. Sebarang pertukaran kepada tetapan sepatutnya dilakukan oleh pengguna berpengalaman sahaja. Jika anda perlu mengubah konfigurasi AVG, pilih item menu sistem **Alat / Tetapan lanjutan** dan edit konfigurasi AVG dalam dialog [Tetapan Lanjutan AVG](#) yang baru dibuka.

Butang kawalan

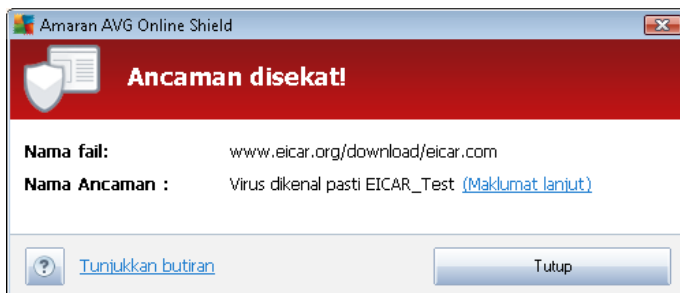


Butang kawalan tersedia dalam antara muka **Perisai Dalam Talian** adalah seperti berikut:

- **Simpan perubahan** - tekan butang ini untuk menyimpan dan menggunakan sebarang perubahan yang dibuat dalam dialog ini
- **Batal** - tekan butang ini untuk kembali ke [antara muka pengguna AVG](#) lalai (*gambaran keseluruhan komponen*)

7.11.3. Pengesanan Perisai Dalam Talian

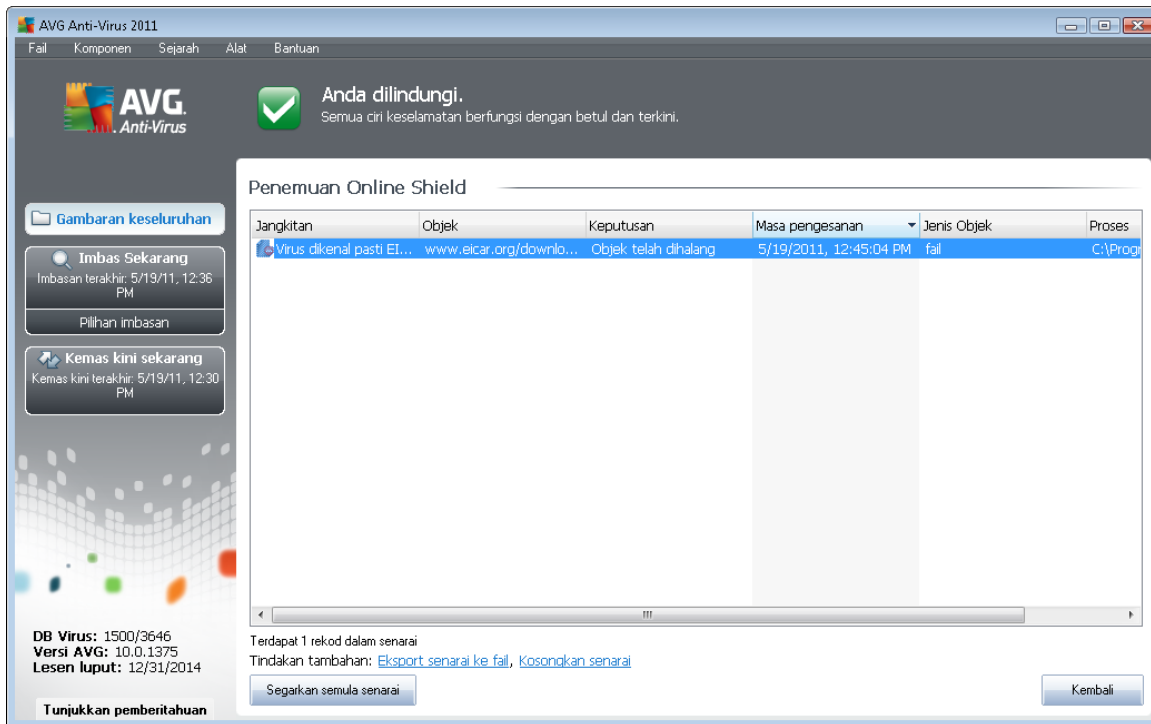
Perisai Dalam Talian mengimbas kandungan halaman web yang dilawati dan kemungkinan fail termasuk dalamnya walaupun sebelum ia dipaparkan dalam penyemak imbas web atau dimuat turun ke komputer anda. Jika ancaman dikesan, anda akan diberi amaran dengan serta-merta dengan dialog berikut:



Dalam dialog amaran ini anda akan menemui data mengenai fail yang dikesan dan ditentukan sebagai dijangkiti (*Nama fail*), nama jangkitan yang dikenal pasti (*Nama ancaman*), dan pautan ke [Ensiklopedia Virus](#) di mana anda boleh menemui maklumat terperinci mengenai jangkitan yang dikesan (*jika diketahui*). Dialog ini menyediakan butang berikut:

- **Tunjuk butiran** - klik butang **Tunjuk butiran** untuk membuka tettingkap pop-timbul baru di mana anda boleh menemui maklumat mengenai proses yang berjalan semasa jangkitan dikesan, dan pengenalan proses berkenaan.
- **Tutup** - klik butang ini untuk menutup dialog amaran.

Halaman web yang disyaki tidak akan dibuka dan pengesanan ancaman akan dilog dalam senarai **penemuan Perisai Dalam Talian** - gambaran keseluruhan ini bagi ancaman dikesan boleh diakses melalui menu sistem [penemuan Sejarah / Perisai Dalam Talian](#) .



Untuk setiap objek yang dikesan, maklumat berikut disediakan:

- **Jangkitan**- penerangan (*malahan juga nama*) bagi objek yang dikesan
- **Objek** - sumber objek (*halaman web*)
- **Keputusan** - tindakan dilakukan dengan objek yang dikesan
- **Pengesanan masa** - tarikh dan masa ancaman dikesan dan disekat
- **Jenis Objek** - jenis objek yang dikesan
- **Proses** - tindakan apa yang dilakukan untuk memanggil objek berpotensi berbahaya supaya ia boleh dikesan

Di bahagian bawah dialog, di bawah senarai, anda akan menemui maklumat mengenai jumlah bilangan objek dikesan yang disenaraikan di atas. Seterusnya, anda boleh mengeksport keseluruhan senarai objek yang dikesan dalam fail (**Eksport senarai ke fail**) dan padam semua entri pada objek dikesan (**Kosongkan senarai**). Butang **Muat semula senarai** akan mengemas kini senarai penemuan yang dikesan oleh **Perisai Dalam Talian**. Butang **Undur** mengalihkan anda semula ke [antara muka pengguna AVG](#) (*gambaran keseluruhan komponen*).

7.12. AntiRootkit

Rootkit adalah atur cara yang direka bentuk untuk melakukan kawalan asas sistem komputer tanpa kebenaran daripada pemilik sistem dan pengurus yang sah. Akses kepada perkakasan jarang diperlukan kerana rootkit bertujuan untuk menyita kawalan sistem pengendalian yang sedang

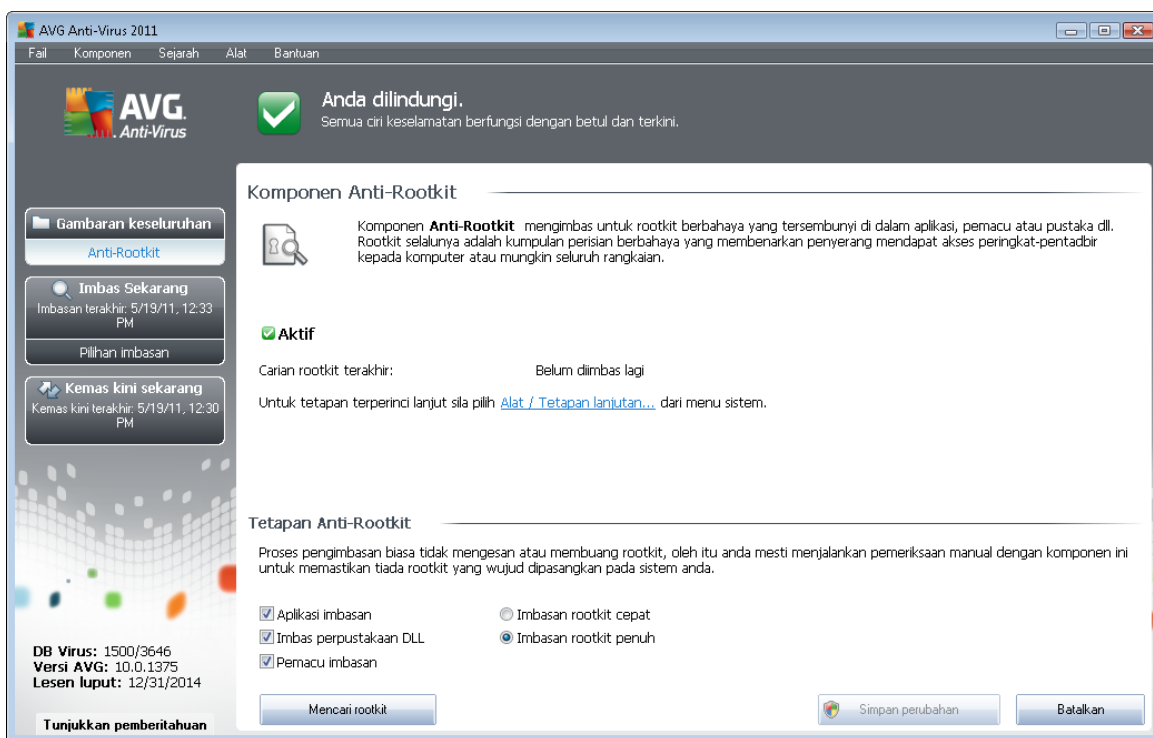


dijalankan pada perkakasan. Biasanya, rootkit bertindak untuk mengaburi kehadirannya pada sistem melalui subversi atau pengelakan daripada mekanisme keselamatan sistem pengendalian. Biasanya, ia juga adalah Trojan, dengan itu, menipu pengguna dengan mempercayai bahawa ia selamat untuk dijalankan pada sistemnya. Teknik yang digunakan untuk melaksanakan ini termasuk menyembunyikan proses yang sedang dijalankan daripada menyelia atur cara atau menyembunyikan fail atau data sistem daripada sistem pengendalian.

7.12.1. Prinsip AntiRootkit

AVG Anti-Rootkit adalah alat khusus untuk mengesan dan membuang rootkit yang berbahaya secara berkesan, cth. atur cara dan teknologi yang boleh menyamar kehadiran perisian berniat jahat pada komputer anda. **AVG Anti-Rootkit** boleh mengesan rootkit berdasarkan pada set peraturan yang dipraktikkan. Sila maklum bahawa semua rootkit dikesan (*bukan hanya* yang dijangkiti). Jika **AVG Anti-Rootkit** menemui rootkit, ia tidak semestinya bermaksud bahawa rootkit dijangkiti. Kadangkala, rootkit digunakan sebagai pemacu atau ia adalah sebahagian daripada aplikasi yang betul.

7.12.2. Antara Muka AntiRootkit



Antara muka pengguna **AntiRootkit** menyediakan penerangan ringkas mengenai kefungsiannya komponen, memaklumkan tentang status semasa komponen, dan juga membawa maklumat mengenai kali terakhir ujian **AntiRootkit** dilancarkan (**Carian rootkit terakhir**). Dialog **AntiRootkit** seterusnya menyediakan pautan [Tetapan Alat/Lanjutan](#). Gunakan pautan ini untuk diarahkan semula ke persekitaran konfigurasi lanjutan bagi komponen **AntiRootkit**.

Sila ambil perhatian: Vendor perisian telah menyediakan semua komponen AVG untuk memberikan prestasi optimum. Melainkan anda mempunyai alasan penting untuk melakukannya, jangan ubah konfigurasi AVG. Sebarang pertukaran kepada tetapan sepatutnya dilakukan oleh



pengguna berpengalaman sahaja.

Tetapan Anti-Rootkit

Pada bahagian bawah dialog, anda boleh dapati bahagian **tetapan AntiRootkit** di mana anda boleh menyediakan beberapa fungsi permulaan bagi pengimbasan kehadiran rootkit. Pertama sekali, tandakan kotak semak masing-masing untuk menentukan objek yang harus diimbas:

- **Aplikasi imbasan**
- **Imbas pustaka DLL**
- **Pemacu imbasan**

Seterusnya, anda boleh memilih mod pengimbasan rootkit:

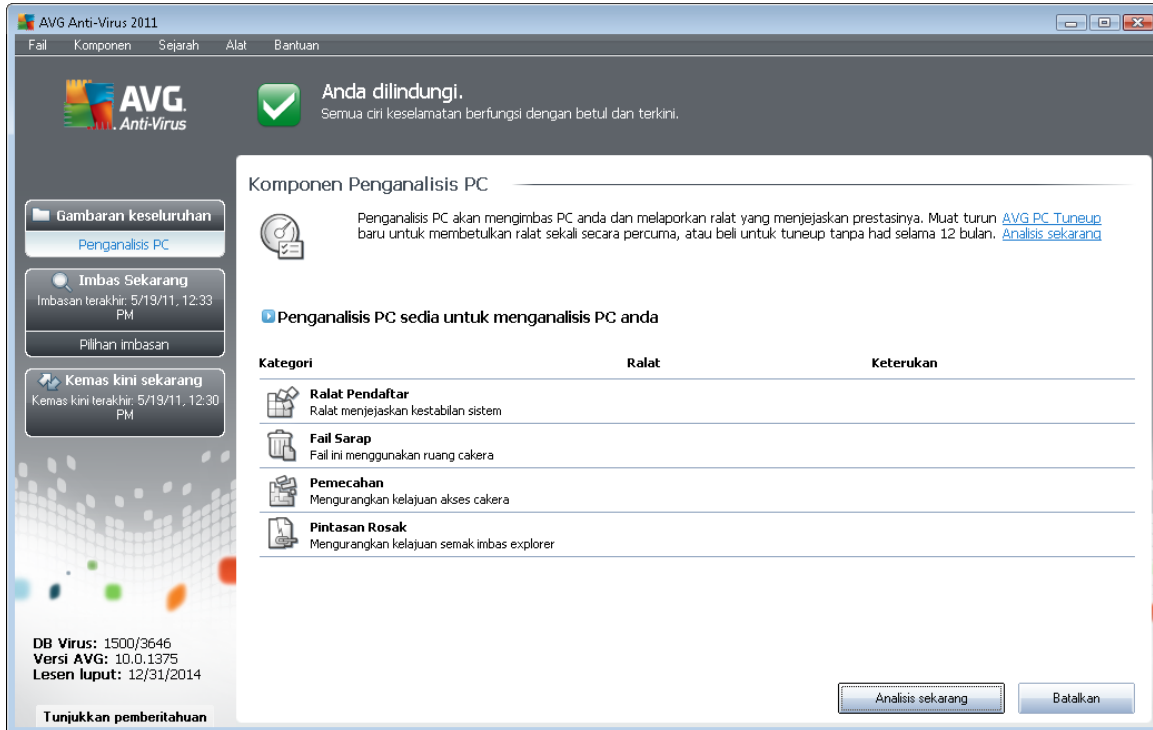
- **Imbasan rootkit cepat** - mengimbas semua proses berjalan, pemacu yang dimuatkan dan folder sistem (*biasanya, c:\Windows*)
- **Imbasan rootkit penuh** - mengimbas semua proses berjalan, pemacu yang dimuatkan, folder sistem (*biasanya, c:\Windows*), campur semua cakera tempatan (*termasuk cakera denyar tetapi tidak termasuk cakera liut/pemacu CD*)

Butang kawalan

- **Cari rootkit** - memandangkan imbasan rootkit bukan bahagian tersirat bagi **Imbasan seluruh komputer**, anda boleh menjalankan imbasan rootkit secara terus dari antara muka **AntiRootkit** menggunakan butang ini
- **Simpan perubahan** - tekan butang ini untuk menyimpan semua perubahan yang dibuat dalam antara muka ini dan untuk kembali ke **antara muka pengguna AVG lalai** (*gambaran keseluruhan komponen*)
- **Batal** - tekan butang ini untuk kembali ke **antara muka pengguna AVG** (*gambaran keseluruhan komponen*) tanpa menyimpan sebarang perubahan yang anda telah lakukan

7.13. Penganalisis PC

Komponen **Penganalisis PC** mampu mengimbas komputer anda bagi masalah sistem, dan memberikan anda gambaran keseluruhan telus mengenai apa yang menjejaskan prestasi keseluruhan komputer anda. Dalam antara muka pengguna komponen anda boleh melihat carta yang dibahagikan kepada empat baris yang merujuk kepada kategori tertentu: ralat pendaftar, fail sarap, errors, junk files, pemecahan, dan pintasan rosak:



- **Ralat Pendaftaran** Akan memberikan anda bilangan ralat dalam Pendaftaran Windows . Oleh sebab memperbaiki Pendaftaran memerlukan pengetahuan yang agak tinggi, kami tidak mengesyorkan anda mencuba dan membaikinya sendiri.
- **Fail Sarap** akan memberikan anda bilangan fail yang paling banyak berkemungkinan boleh dilakukan tanpa. Biasanya, ia adalah pelbagai jenis fail sementara, dan fail dalam Tong Kitar Semula.
- **Pemecahan** akan mengira peratusan cakera keras anda yang dipecahkan, iaitu digunakan untuk tempoh yang lama supaya kebanyakan fail, kini, terdapat pada bahagian berbeza bagi cakera fizikal. Anda boleh menggunakan beberapa alat penyahserpihan untuk membetulkan ini.
- **Pintasan Rosak** akan memberitahu anda mengenai pintasan yang tidak lagi berfungsi, membawa kepada lokasi tidak wujud dll.

Untuk memulakan analisis sistem anda, tekan butang **Analisis sekarang**. Anda kemudiannya akan boleh melihat kemajuan analisis dan keputusannya terus di dalam carta:



The screenshot shows the AVG Anti-Virus 2011 interface. At the top, it says "Anda dilindungi." (You are protected). Below that, it displays "Komponen Penganalisis PC" (PC Analysis Components). A table lists the results of the analysis, categorized by type of error. The table has three columns: "Kategori" (Category), "Ralat" (Error), and "Keterangan" (Details). The results are as follows:

Kategori	Ralat	Keterangan
Ralat Pendaftaran Ralat menjejaskan kestabilan sistem	137 ralat ditemui Butiran...	[Progress bar]
Fail Sarap Fail ini menggunakan ruang cakera	132 ralat ditemui Butiran...	[Progress bar]
Pemecahan Mengurangkan kelajuan akses cakera	10% dipecahkan Butiran...	[Progress bar]
Pintasan Rosak Mengurangkan kelajuan semak imbas explorer	13 ralat ditemui Butiran...	[Progress bar]

At the bottom of the interface, there are two buttons: "Baiki sekarang" (Fix now) and "Batalkan" (Cancel). On the left side, there are several utility buttons: "Gambaran keseluruhan" (Overview), "Penganalisis PC" (PC Analyzer), "Imbas Sekarang" (Refresh now), "Kemas kini sekarang" (Update now), and "Tunjukkan pemberitahuan" (Show notifications).

Gambaran keseluruhan keputusan menyediakan bilangan masalah sistem yang dikesan (**Ralat**) dibahagikan mengikut kategori tertentu yang diuji. Keputusan analisis juga akan dipaparkan secara grafik pada paksi dalam lajur **Keterangan** .

Butang kawalan

- **Analisis sekarang** (dipaparkan sebelum analisis bermula) - tekan butang ini untuk melancarkan analisis segera komputer anda
- **Betulkan sekarang** (dipaparkan sebaik sahaja analisis selesai) - tekan butang untuk pergi ke laman web AVG (<http://www.avg.com/>) di halaman yang menyediakan maklumat terperinci dan terkini berkaitan dengan komponen **Penganalisis PC**
- **Batal** - tekan butang ini untuk berhenti menjalankan analisis, atau untuk kembali ke [antara muka pengguna AVG](#) lalai (gambaran keseluruhan komponen) sebaik sahaja analisis selesai

7.14. Perlindungan ID

AVG Identity Protection adalah produk antimalware yang memberi tumpuan kepada mengelakkan pencuri identiti daripada mencuri kata laluan anda, butiran akaun bank, nombor kad kredit dan barangan digital peribadi yang lain yang bernilai daripada semua jenis perisian berniat jahat (*malware*) yang mensasarkan PC anda. Ia memastikan semua atur cara yang dijalankan pada PC anda beroperasi dengan betul. **AVG Identity Protection** mengesan dan menyekat kelakuan yang mencurigakan pada asas berterusan dan melindungi komputer anda daripada semua malware baru.

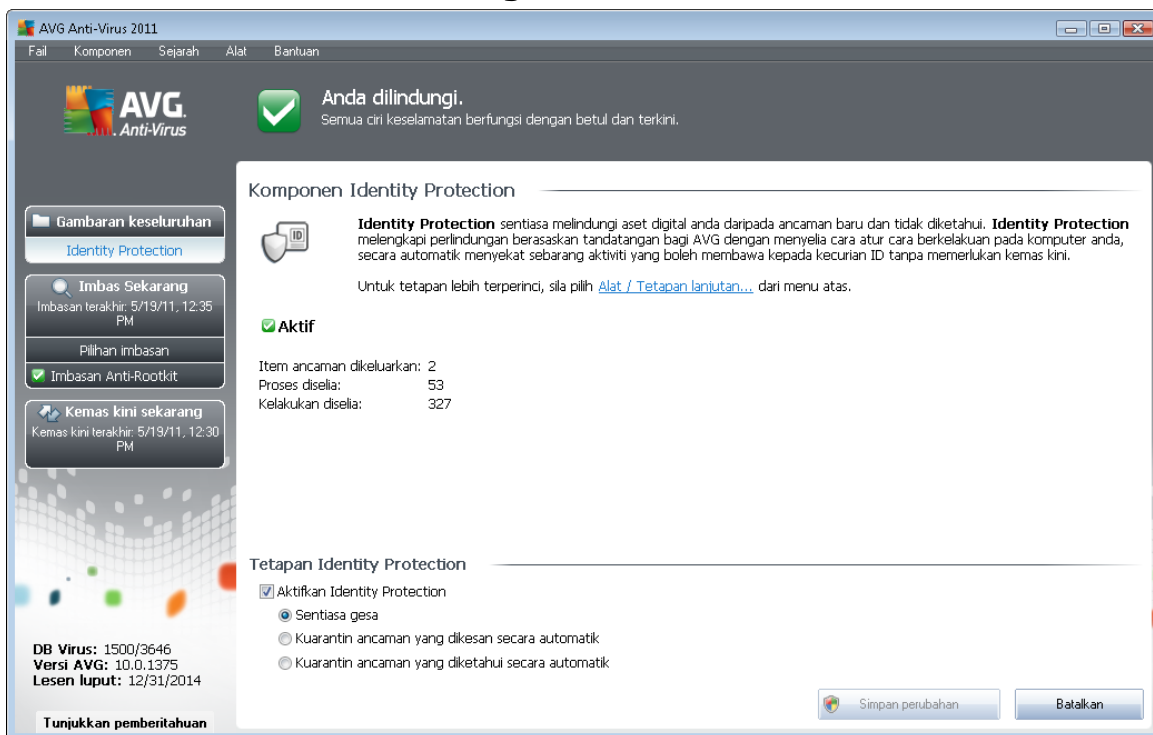


7.14.1. Prinsip Perlindungan ID

AVG Identity Protection adalah komponen antimalware yang melindungi anda daripada semua jenis malware (*perisian pengintip, bot, pencuri identiti, ...*) menggunakan teknologi kelakuan dan memberikan perlindungan hari sifar untuk virus baru. Apabila malware menjadi sofistikated dan datang dalam bentuk atur cara normal yang boleh mendedahkan PC anda kepada penyerang jauh bagi pencuri identiti, **AVG Identity Protection** melindungi anda daripada pelaksanaan baru ini yang berasaskan malware. Ia adalah perlindungan percuma kepada **AVG Anti-Virus** yang melindungi anda daripada fai berasaskan dan diketahui virus menggunakan mekanisme tandatangan dan pengimbasan.

Kami amat mengesyorkan anda mempunyai kedua-dua komponen **AVG Anti-Virus dan **AVG Identity Protection** dipasang, untuk mempunyai perlindungan lengkap untuk PC anda.**

7.14.2. Antara Muka Perlindungan ID



Antara muka komponen **Perlindungan Identiti** menyediakan penerangan ringkas tentang kefungsi asas komponen, statusnya, dan beberapa data statistik:

- **Item malware dibuang** - memberikan bilangan aplikasi yang dikesan sebagai malware dan dibuang
- **Proses diselia** - bilangan aplikasi yang sedang dijalankan yang diselia oleh IDP
- **Kelakuan diselia** - bilangan tindakan khusus yang sedang dijalankan dalam aplikasi yang diselia



Tetapan Perlindungan Identiti

Di bahagian bawah dialog, anda akan menemui bahagian **tetapan Perlindungan Identiti** di mana anda boleh mengedit beberapa ciri permulaan bagi kefungsiian komponen:

- **Aktifkan Perlindungan Identiti** - (*dibuka secara lalai*): tanda untuk mengaktifkan komponen IDP dan untuk membuka opsyen pengeditan selanjutnya.

Dalam sesetengah kes, **Perlindungan Identiti** mungkin melaporkan bahawa beberapa fail yang sah adalah mencurigakan atau berbahaya. Memandangkan **Perlindungan Identiti** mengesan ancaman berdasarkan pada kelakuan mereka, ini biasanya berlaku apabila beberapa atur cara cuba memantau penekanan kekunci, memasang atur cara lain atau pemacu baru yang dipasang pada komputer. Oleh itu, sila pilih salah satu opsyen berikut yang menentukan kelakuan komponen **Perlindungan Identiti** sekiranya mengesan aktiviti mencurigakan:

- **Sentiasa gesa** - jika aplikasi dikesan sebagai malware, anda akan ditanya sama ada ia harus disekat (*pilihan ini dihidupkan secara lalai dan disyorkan untuk tidak mengubahnya melainkan anda mempunyai sebab sebenar untuk melakukannya*)
- **Kuarantin ancaman yang dikesan secara automatik** - semua aplikasi dikesan sebagai malware akan disekat secara automatik
- **Kuarantin ancaman yang diketahui secara automatik** - hanya aplikasi dengan kepastian mutlak dikesan sebagai malware akan disekat

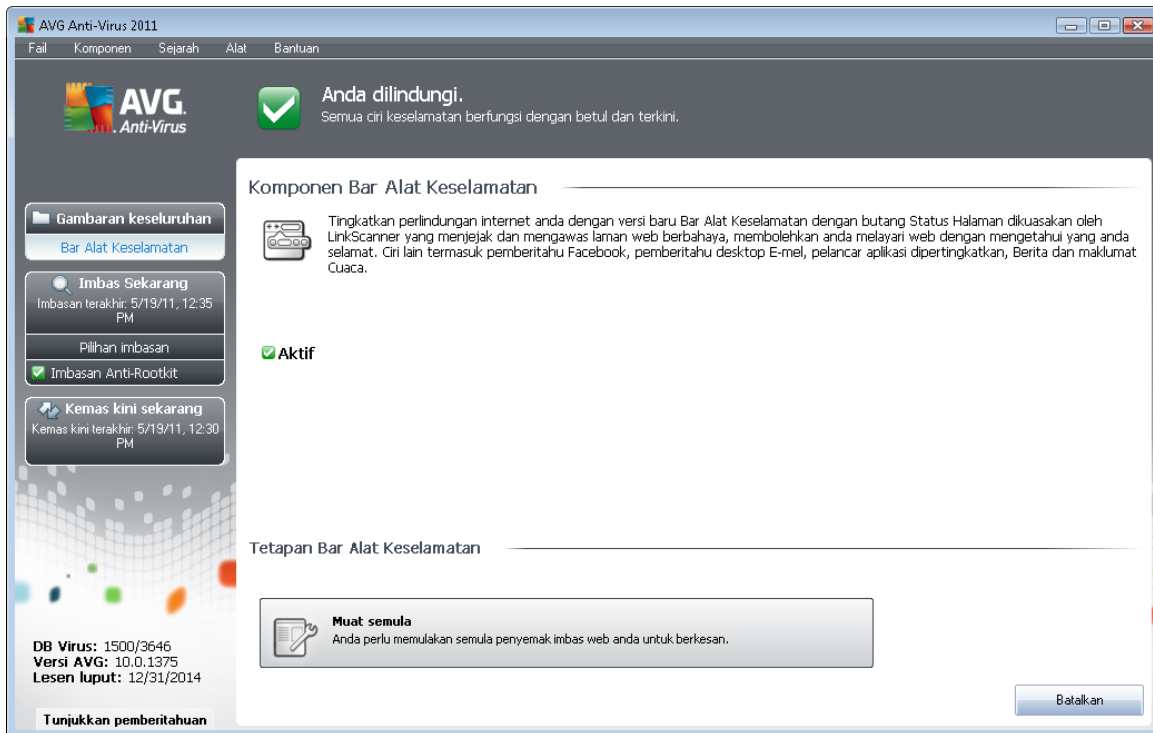
Butang kawalan

Butang kawalan yang tersedia dalam antara muka **Perlindungan Identiti** adalah seperti berikut:

- **Simpan perubahan** - tekan butang ini untuk menyimpan dan menggunakan sebarang perubahan yang dibuat dalam dialog ini
- **Batal** - tekan butang ini untuk kembali ke [antara muka pengguna AVG lalai](#) (*gambaran keseluruhan komponen*)

7.15. Bar Alat Keselamatan

Bar Alat Keselamatan adalah bar alat penyemak imbas web pilihan, menawarkan perlindungan AVG dipertingkatkan dan pelbagai ciri dan alat dengan mudah semasa melayari web. Buat masa ini, **Bar Alat Keselamatan** disokong oleh penyemak imbas Internet Explorer (*6.0 atau lebih tinggi*) dan Mozilla Firefox (*3.0 atau lebih tinggi*):



Semua tetapan komponen **Bar Alat Keselamatan** boleh diakses secara terus dalam [Bar Alat Keselamatan](#) dalam penyemak imbas web anda.



8. AVG Security Toolbar

AVG Security Toolbar adalah alat baru yang berfungsi bersama dengan komponen [LinkScanner](#). **AVG Security Toolbar** boleh digunakan untuk mengawal fungsi [LinkScanner](#) dan untuk mengubah suai kelakuannya.

Jika anda memilih untuk memasang bar alat sewaktu pemasangan bagi **AVG Anti-Virus 2011**, ia akan ditambah ke dalam penyemak imbas web anda (*Internet Explorer 6.0 atau lebih tinggi dan Mozilla Firefox 3.0 atau lebih tinggi*) secara automatik. Penyemak imbas internet lain tidak disokong buat masa ini.

Nota: Jika anda menggunakan beberapa penyemak imbas Internet alternatif (cth. Avant Browser) anda boleh menghadapi kelakuan yang tidak dijangka.

8.1. Antara Muka AVG Security Toolbar

AVG Security Toolbar direka bentuk untuk bekerja dengan **MS Internet Explorer** (versi 6.0 atau lebih tinggi) dan **Mozilla Firefox** (versi 3.0 atau lebih tinggi). Sebaik sahaja anda telah memutuskan anda hendak memasang **AVG Security Toolbar** (sewaktu [proses pemasangan AVG](#) anda diminta untuk memutuskan sama ada anda hendak memasang komponen ini atau tidak), komponen akan terletak dalam penyemak imbas web anda betul-betul di bawah bar alamat:



AVG Security Toolbar terdiri daripada yang berikut:

8.1.1. Butang logo AVG

Butang ini menyediakan akses ke item bar alat umum. Klik butang logo untuk diarahkan semula ke [laman web AVG](#). Dengan mengklik penuding di sebelah ikon AVG akan membuka yang berikut:

- **Maklumat Bar Alat** - pautan kepada halaman utama **AVG Security Toolbar** dengan maklumat terperinci mengenai perlindungan bar alat
- **Lancarkan AVG** - membuka **AVG Anti-Virus 2011** [antara muka pengguna](#)
- **Maklumat AVG** - membuka menu konteks dengan pautan berikut membawa maklumat keselamatan penting berkaitan **AVG Anti-Virus 2011**:
 - *Mengenai Ancaman* - membuka [laman web AVG](#) pada halaman yang menyediakan data paling penting mengenai ancaman utama, syor pembuangan virus, maklumat kemas kini AVG, akses ke [pangkalan data Virus](#) dan lebih banyak maklumat berkaitan
 - *Berita AVG* - membuka halaman web memberikan keluaran berita berkaitan AVG yang terkini

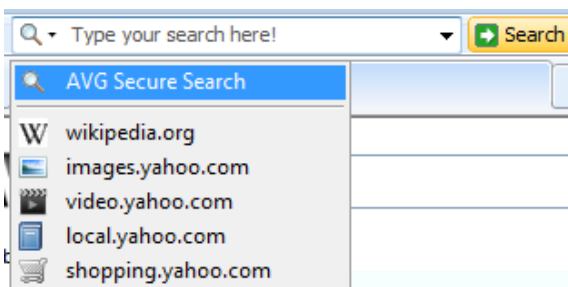


- *Tahap Ancaman Semasa* - membuka halaman web makmal virus dengan paparan grafik bagi tahap ancaman semasa pada web
- *AVG Threat Labs* - membuka laman web [Laporan Laman AVG](#) di mana anda boleh mencari ancaman khusus mengikut nama dan dapatkan maklumat terperinci mengenai setiap satu
- **Opsyen** - membuka dialog konfigurasi di mana anda boleh mengubah suai tetapan **AVG Security Toolbar** untuk disesuaikan dengan keperluan anda - lihat bab berikut [Opsyen AVG Security Toolbar](#)
- **Hapuskan Sejarah** - membenarkan anda di dalam **AVG Security Toolbar** menghapus sejarah sepenuhnya, atau secara berasingan menghapus sejarah carian, menghapus sejarah pelayar, menghapus sejarah muat turun dan menghapus kuki.
- **Kemas kini** - memeriksa untuk kemas kini baru untuk **AVG Security Toolbar anda**
- **Bantuan** - memberikan opsyen untuk membuka fail bantuan, hubungi [sokongan teknikal AVG](#), hantar maklum balas berkaitan produk anda, atau lihat butiran bagi versi terkini bar alat

8.1.2. kotak carian yang dikuasakan AVG Secure Search (powered by Google)

Kotak **AVG Secure Search (powered by Google)** adalah cara yang mudah dan selamat untuk mencari web menggunakan AVG Secure Search (powered by Google). Masukkan perkataan atau ungkapan dalam kotak carian, tekan butang **Carian**, atau kekunci **Enter**, untuk memulakan carian pada pelayan AVG Secure Search (powered by Google) secara terus, tidak kira halaman apa yang sedang dipaparkan. Kotak carian juga menyenaraikan sejarah carian anda. Carian dilakukan melalui kotak carian dianalisis menggunakan perlindungan [Search-Shield](#).

Secara alternatif, di dalam medan carian anda boleh bertukar ke Wikipedia, atau sebarang perkhidmatan carian khusus lain - lihat gambar:







8.1.3. Status Halaman

Terus di dalam bar alat, butang ini memaparkan penilaian halaman web yang sedang dipaparkan berdasarkan kriteria komponen [Surf-Shield](#) :

-  - Halaman yang dipautkan adalah selamat

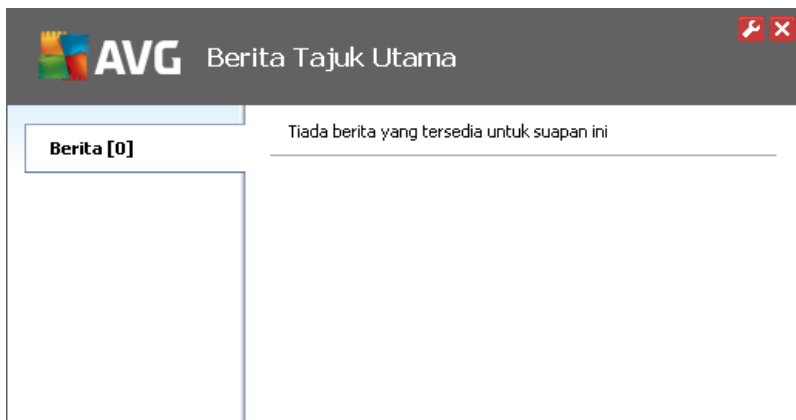


-  - Halaman agak mencurigakan.
-  - Halaman mengandungi pautan kepada halaman berbahaya secara positif.
-  - Halaman yang dipautkan mengandungi ancaman aktif! Untuk keselamatan anda sendiri, anda tidak akan dibenarkan untuk melawati halaman ini.
-  - Halaman ini tidak boleh diakses dan oleh itu, tidak boleh diimbas.


Klik butang untuk membuka panel maklumat dengan data terperinci mengenai halaman web khusus.

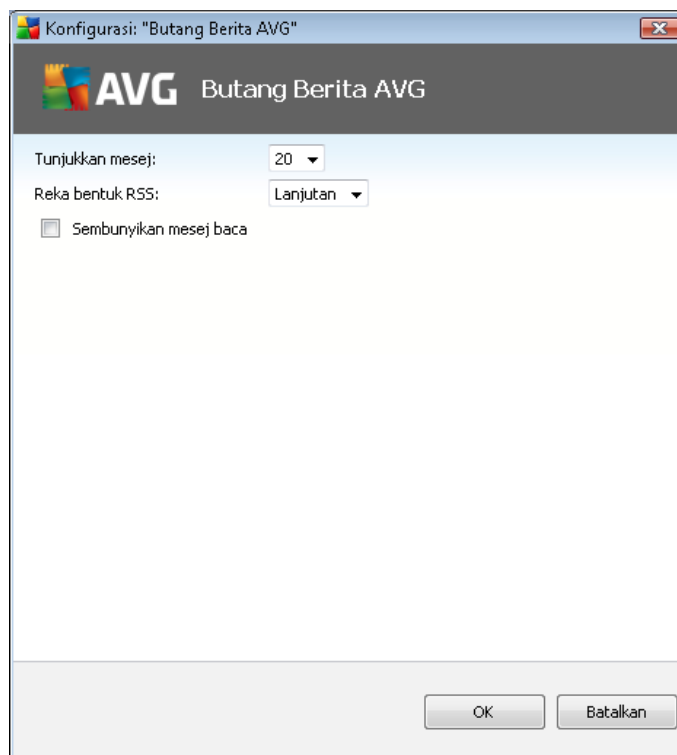
8.1.4. Berita AVG


Terus dari dalam **AVG Security Toolbar**, butang ini membuka gambaran keseluruhan mengenai **berita Tajuk Utama** berkaitan AVG, kedua-dua berita dari akhbar dan siaran akhbar syarikat:



Di sudut atas kanan anda boleh melihat dua butang kawalan merah:

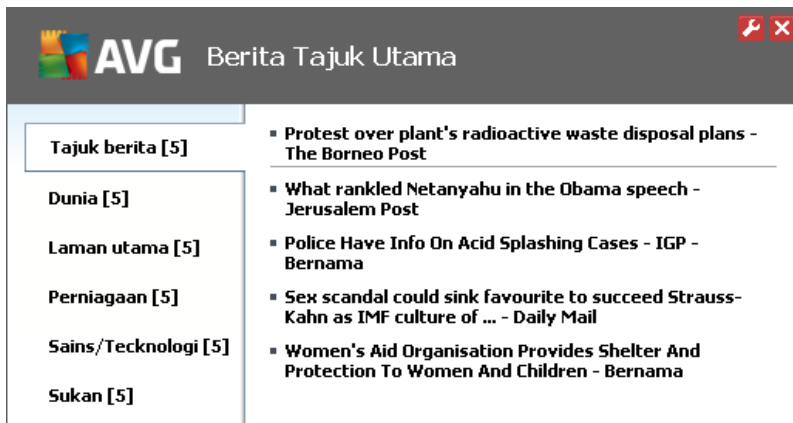
-  - butang ini membuka dialog pengeditan di mana anda boleh menentukan parameter butang **Berita AVG** yang dipaparkan di dalam **AVG Security Toolbar**.




- **Tunjuk mesej** - menukar bilangan halaman yang diinginkan yang dipaparkan pada satu masa
- **Reka bentuk RSS** - pilih antara mod Lanjut/Asas bagi paparan semasa gambaran keseluruhan berita (*secara lalai, mod Lanjut dipilih - lihat gambar di atas*)
- **Sembunyi mesej telah dibaca** - tanda item ini untuk mengesahkan bahawa setiap mesej yang telah dibaca tidak perlu dipaparkan lagi, supaya mesej baru boleh disalurkan
-  - klik butang ini untuk menutup gambaran keseluruhan berita yang sedang dibuka

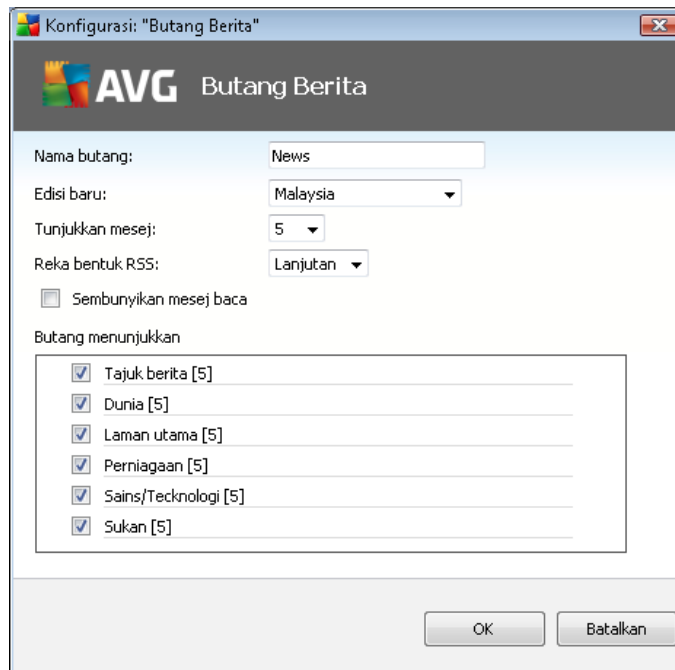
8.1.5. Berita

Begitu juga, terus dari dalam **AVG Security Toolbar**, butang ini membuka gambaran keseluruhan mengenai berita terkini dari media terpilih yang dibahagikan kepada beberapa bahagian:




Di sudut atas kanan anda boleh melihat dua butang kawalan berwarna merah:

-  - butang ini membuka dialog pengeditan di mana anda boleh menetapkan parameter butang **Berita** yang dipaparkan dalam **AVG Security Toolbar**.



- o **Nama butang** - anda mempunyai pilihan untuk menukar nama butang sambil ia dipaparkan dalam **AVG Security Toolbar**
- o **Edisi berita** - pilih negara dari senarai ini untuk mempunyai berita dipaparkan dari wilayah yang dipilih
- o **Tunjuk mesej** - tetapkan bilangan mesej yang diinginkan yang akan dipaparkan pada satu-satu

masa


- o **Reka bentuk RSS** - bertukar antara opsyen Asas/Lanjutan untuk memilih reka bentuk gambaran keseluruhan berita (**reka bentuk lanjutan ditetapkan secara lalai, lihat gambar di atas**)
- o **Sembunyikan mesej telah dibaca** - tandakan item ini untuk mengesahkan bahawa sebarang mesej telah dibaca tidak harus dipaparkan lagi dalam gambaran keseluruhan berita, dan perlu digantikan dengan tajuk berita baru
- o **Butang menunjukkan** - dalam medan ini anda boleh menentukan apa jenis berita yang harus dipaparkan dalam **gambaran keseluruhan berita** AVG Security Toolbar
 -  - klik butang ini untuk menutup gambaran keseluruhan berita yang sedang dibuka

8.1.6. Hapuskan Sejarah

Dengan menggunakan butang ini anda boleh menghapuskan sejarah penyemak imbas anda sama seperti melalui opsyen **logo AVG -> Hapuskan sejarah**.

8.1.7. Pemberitahu E-mel

Butang **Pemberitahu E-mel** membenarkan anda untuk mengaktifkan opsyen dimaklumkan mengenai mesej e-mel yang baru tiba terus di dalam antara muka **AVG Security Toolbar**. Butang ini membuka dialog pengeditan berikut di mana anda boleh mentakrifkan parameter bagi akaun e-mel anda dan peraturan paparan e-mel. Sila ikuti arahan di dalam dialog:



- **Jenis akaun** - Tetapkan jenis protokol yang digunakan oleh akaun e-mel anda. Anda boleh memilih alternatif berikut: *Gmail*, *POP3*, atau pilih nama pelayan dari menu jantai bawah di dalam *item Lain-lain* (*buat masa ini, anda boleh menggunakan opsyen ini jika akaun anda*



di Yahoo! Mail atau Hotmail JP). Jika anda tidak pasti jenis pelayan e-mel yang digunakan oleh akaun anda, cuba cari maklumat ini daripada penyedia e-mel anda, atau pembekal khidmat internet anda.

- **Log Masuk** - Dalam seksyen di bawah, berikan bentuk sebenar *alamat e-mel* anda, dan *kata laluan* masing-masing. Biarkan opsyen *Log Masuk Auto* ditandakan supaya anda tidak perlu mengisi data ini berulang kali.
- **Akaun ujian** - Gunakan butang ini untuk menguji butiran yang dimasukkan.
- **Tetapkan Semula Tetapan** - Mengeluarkan butiran alamat e-mel yang dimasukkan di atas dengan cepat.
- **Semak bagi e-mel baru setiap ... minit** - Takrifkan selang masa yang akan digunakan untuk menyemak mesej e-mel baru (*dalam julat 5-120 minit*), dan tetapkan sama ada dan bagaimana anda ingin dimaklumkan mengenai ketibaan mesej baru ini.
- **Benarkan amaran e-mel baharu** - Jangan tandakan ini untuk menyahdaya pemberitahuan visual bagi ketibaan mesej e-mel.
 - **Mainkan bunyi semasa e-mel baharu tiba** - Jangan tandakan ini untuk menyahdaya pemberitahuan bunyi bagi ketibaan mesej e-mel baru.
 - **Tutup tettingkap pemberitahuan selepas 5 saat** - Tandakan ini untuk menutup tettingkap pemberitahuan visual secara automatik bagi ketibaan mesej e-mel baharu selepas 5 saat.

8.1.8. Maklumat Cuaca

Butang **Cuaca** memaparkan maklumat mengenai suhu semasa (*dikemas kini setiap 3-6 jam*) di destinasi anda yang dipilih terus di dalam antara muka **AVG Security Toolbar**. Klik butang ini untuk membuka panel maklumat baru dengan gambaran keseluruhan cuaca yang terperinci:

Brno, CZ
[[tukar lokasi](#)]

26° C

Kelajuan angin: 19,31 km/j
Matahari Terbit: 05:04
Matahari Terbenam: 20:34

JUM Tgi: 24 °C Rdh: 14 °C	SAB Tgi: 25 °C Rdh: 14 °C
--	--

Dikemas Kini 05/20/2011 14:38:10 **YAHOO! NEWS** [Ramalan Penuh >](#)



Berikut adalah opsyen pengeditan:

- **Tukar lokasi** - klik teks **Tukar lokasi** untuk memaparkan dialog baru dinamakan **Cari lokasi anda**. Isikan nama lokasi yang anda inginkan ke dalam medan teks, dan sahkan dengan mengklik butang **Cari**. Seterusnya, di dalam senarai semua lokasi yang mempunyai nama yang sama pilih destinasi yang anda cari. Akhir sekali, panel maklumat akan dipaparkan sekali lagi menyediakan maklumat cuaca bagi lokasi yang dipilih.
- **Penukar Fahrenheit / Celsius** - di sudut atas kanan panel maklumat anda boleh memilih antara skala Fahrenheit dan Celsius. Berdasarkan pilihan anda, maklumat suhu akan seterusnya diberikan menggunakan skala yang diinginkan.
- **Ramalan Penuh** - jika berminat dengan ramalan penuh dan terperinci, gunakan pautan **Ramalan Penuh** untuk pergi ke laman web cuaca yang dikhususkan.

8.1.9. Facebook

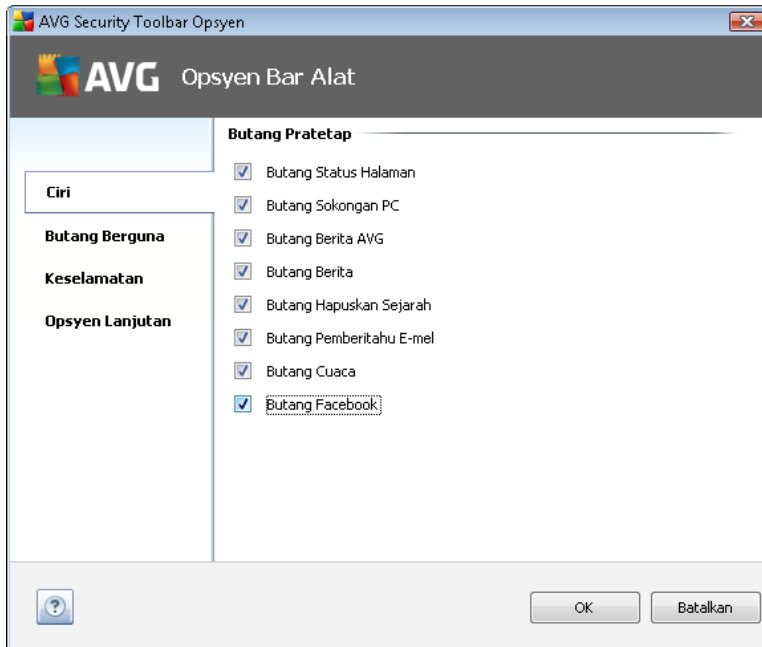
Butang **Facebook** membenarkan anda menyambung ke rangkaian sosial [Facebook](#) dari **AVG Security Toolbar** secara langsung. Klik butang ini, dan jemputan untuk log masuk muncul; klik sekali lagi untuk membuka dialog **log masuk Facebook**. Berikan data akses anda, dan tekan butang **Sambung**. Jika anda belum lagi mempunyai akaun [Facebook](#), anda boleh membuat satu terus menggunakan pautan **Daftar untuk Facebook**.

Sebaik sahaja anda melepasi proses pendaftaran [Facebook](#), anda akan dijemput untuk membenarkan aplikasi **Sambungan Sosial AVG**. Kefungsian aplikasi ini adalah penting bagi sambungan bar alat - [Facebook](#), oleh itu adalah disyorkan untuk membenarkan kefungsiannya, jadi pastikan anda membenarkannya. Selepas itu, sambungan [Facebook](#) akan diaktifkan, dan butang **Facebook** dalam **AVG Security Toolbar** kini menawarkan opsyen menu [Facebook](#) standard.

8.2. Opsyen AVG Security Toolbar

Semua konfigurasi parameter **AVG Security Toolbar** boleh diakses secara terus dalam panel **AVG Security Toolbar**. Antara muka pengeditan terbuka melalui item menu bar alat **AVG / Pilihan** dalam dialog baru yang dipanggil **Pilihan Bar Alat** yang dibahagikan ke dalam empat bahagian:

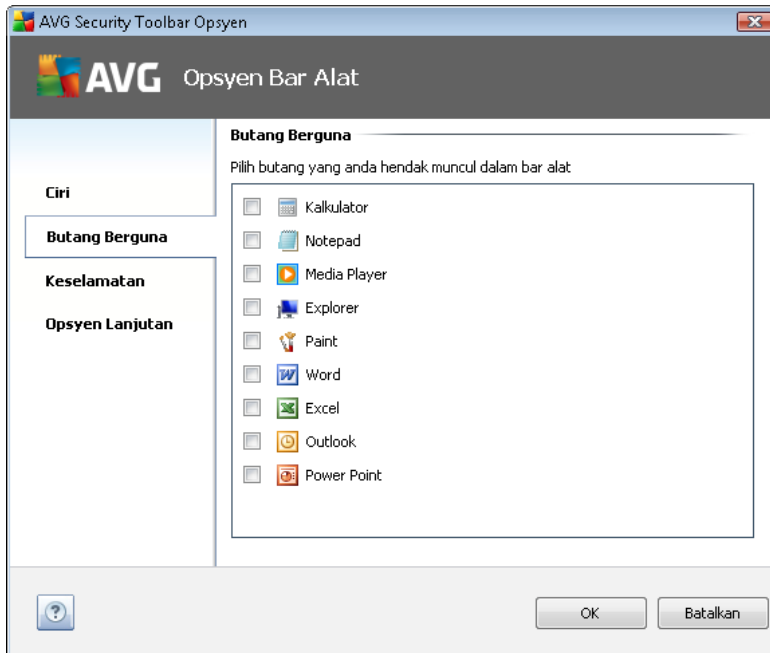
8.2.1. Tab Umum



Pada tab ini anda boleh menentukan butang yang harus dipaparkan / tersembunyi dalam panel **AVG Security Toolbar**. Tandakan sebarang pilihan jika anda mahukan butang masing-masing dipaparkan. Seterusnya, terangkan kefungsian setiap butang bar alat:

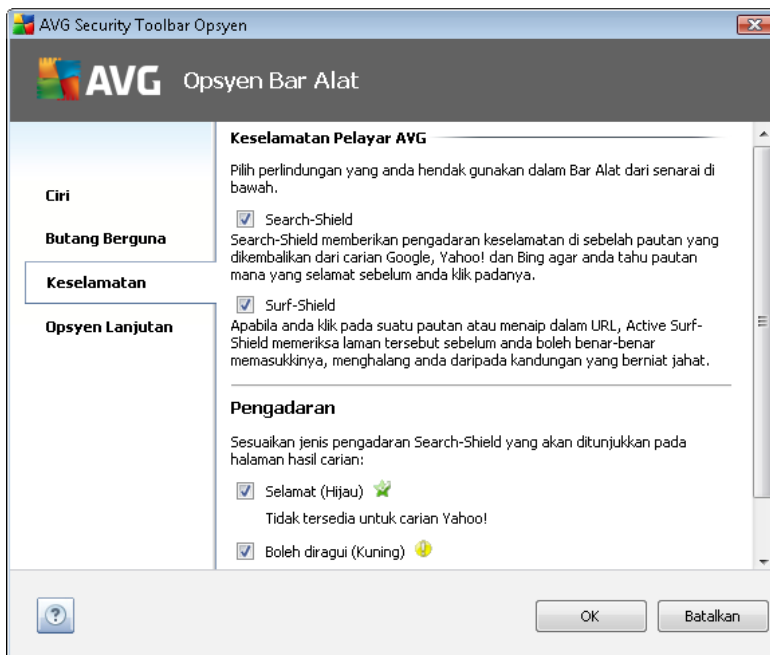
- **Butang Status Halaman** - butang ini menawarkan kemungkinan dipaparkan maklumat mengenai status keselamatan halaman yang sedang dibuka dalam **AVG Security Toolbar**
- **AVG News Button** - butang membuka halaman web memberikan keluaran berita berkaitan AVG yang terkini
- **News Button** - butang memberikan gambaran keseluruhan berita terkini daripada berita harian
- **Butang Hapuskan Sejarah** - butang ini membolehkan anda Memadam sejarah lengkap, atau Memadam sejarah carian, Memadam sejarah penyemak imbas, Memadam sejarah muat turun, atau Memadam kuki secara terus dari panel AVG Security Toolbar
- **Butang Makluman E-mel** - butang ini membolehkan anda dipaparkan mesej e-mel anda yang baru sampai dalam antara muka **AVG Security Toolbar**
- **Butang Cuaca** - butang ini menawarkan maklumat segera mengenai keadaan cuaca di lokasi yang dipilih
- **Butang Facebook** - butang ini menawarkan sambungan terus ke rangkaian sosial [Facebook](https://www.facebook.com/AVG)

8.2.2. Tab Butang Berguna



Tab **Butang Berguna** membenarkan anda memilih aplikasi daripada senarai dan memaparkan ikonnya dalam antara muka bar alat. Ikon tersebut kemudiannya bertindak sebagai pautan pantas membolehkan untuk melancarkan aplikasi masing-masing dengan segera.






8.2.3. Tab Keselamatan



Tab **Keselamatan** dibahagikan ke dalam dua bahagian, **AVG Browser Security** dan **Pengadaran**, di

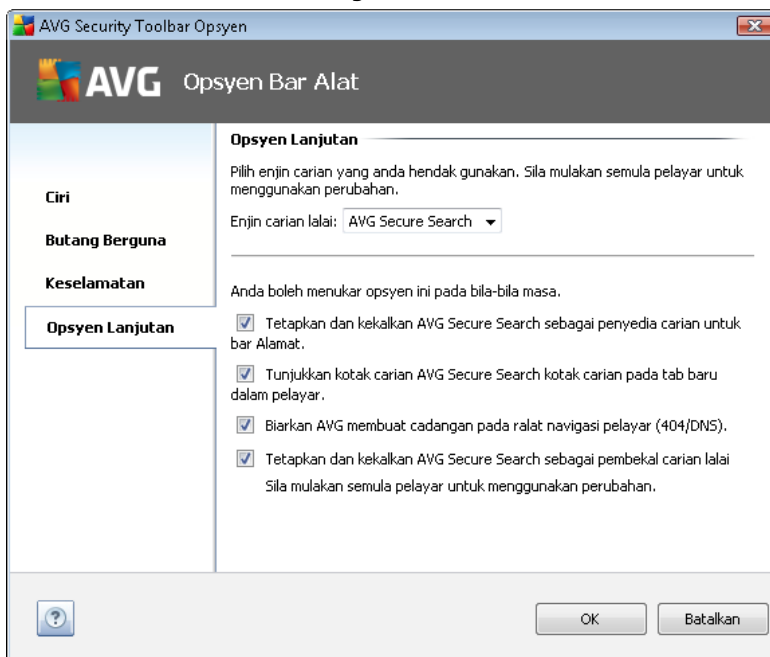


mana anda boleh menanda kotak semakan tertentu untuk menguntukkan kefungisian **AVG Security Toolbar** yang anda hendak gunakan:

- **Browser Security** - tandakan item ini untuk mengaktifkan atau mematikan perkhidmatan [AVG Search-Shield](#) dan/atau [Surf-Shield](#)
- **Rating** - pilih simbol grafik yang digunakan untuk rating hasil carian melalui komponen [Search-Shield](#) yang anda hendak gunakan:
 -  halaman adalah selamat
 -  halaman agak mencurigakan
 -  halaman mengandungi pautan kepada halaman berbahaya secara positif
 -  halaman mengandungi ancaman aktif
 -  halaman tidak boleh diakses, maka, tidak boleh diimbas

Tandakan opsyen masing-masing untuk mengesahkan anda mahu diberitahu mengenai tahap ancaman tertentu ini. Walau bagaimanapun, paparan tanda merah yang diperuntukkan kepada halaman yang mengandungi ancaman aktif dan berbahaya tidak boleh dimatikan. ***Sekali lagi, ia disyorkan untuk mengekalkan konfigurasi lalai yang ditetapkan oleh vendor atur cara melainkan anda mempunyai sebab sebenar untuk mengubahnya.***

8.2.4. Tab Pilihan Lanjutan





Pada tab **Pilihan Lanjutan** pertama sekali, pilih enjin carian yang anda hendak gunakan sebagai lalai. Anda mempunyai pilihan *AVG Secure Search (powered by Google)*, *Baidu*, *WebHledani*, *Yandex* dan *Yahoo! JP*. Setelah menukar enjin carian lalai, sila mulakan semula penyemak imbas internet anda untuk perubahan berkesan.

Seterusnya, anda boleh mengaktifkan atau mematikan tetapan **Bar Alat Keselamatan AVG** khusus selanjutnya (*kapsyen yang disenaraikan merujuk kepada tetapan AVG Secure Search (powered by Google) lalai*):

- **Tetapkan dan simpan AVG Secure Search (powered by Google) sebagai pembekal carian untuk bar Alamat** - jika ditanda, opsi ini membenarkan anda menaip kata kunci carian secara terus ke dalam bar alamat ke dalam penyemak imbas Internet dan perkhidmatan Google akan digunakan secara automatik untuk mencari laman web berkaitan.
- **Benarkan AVG membuat cadangan mengenai ralat navigasi penyemak imbas (404/DNS)** jika semasa mencari web, anda menemui halaman tidak wujud atau halaman tidak boleh dipaparkan (ralat 404), anda akan diarahkan semula secara automatik ke halaman web yang membenarkan anda memilih daripada gambaran keseluruhan halaman alternatif berkaitan topik.
- **Tetapkan dan simpan AVG Secure Search (powered by Google) sebagai pembekal carian lalai** - Google ialah enjin carian lalai untuk carian web dalam **Bar Alat Keselamatan AVG**, dan mengaktifkan opsi ini juga boleh menjadi enjin carian lalai penyemak imbas web anda.

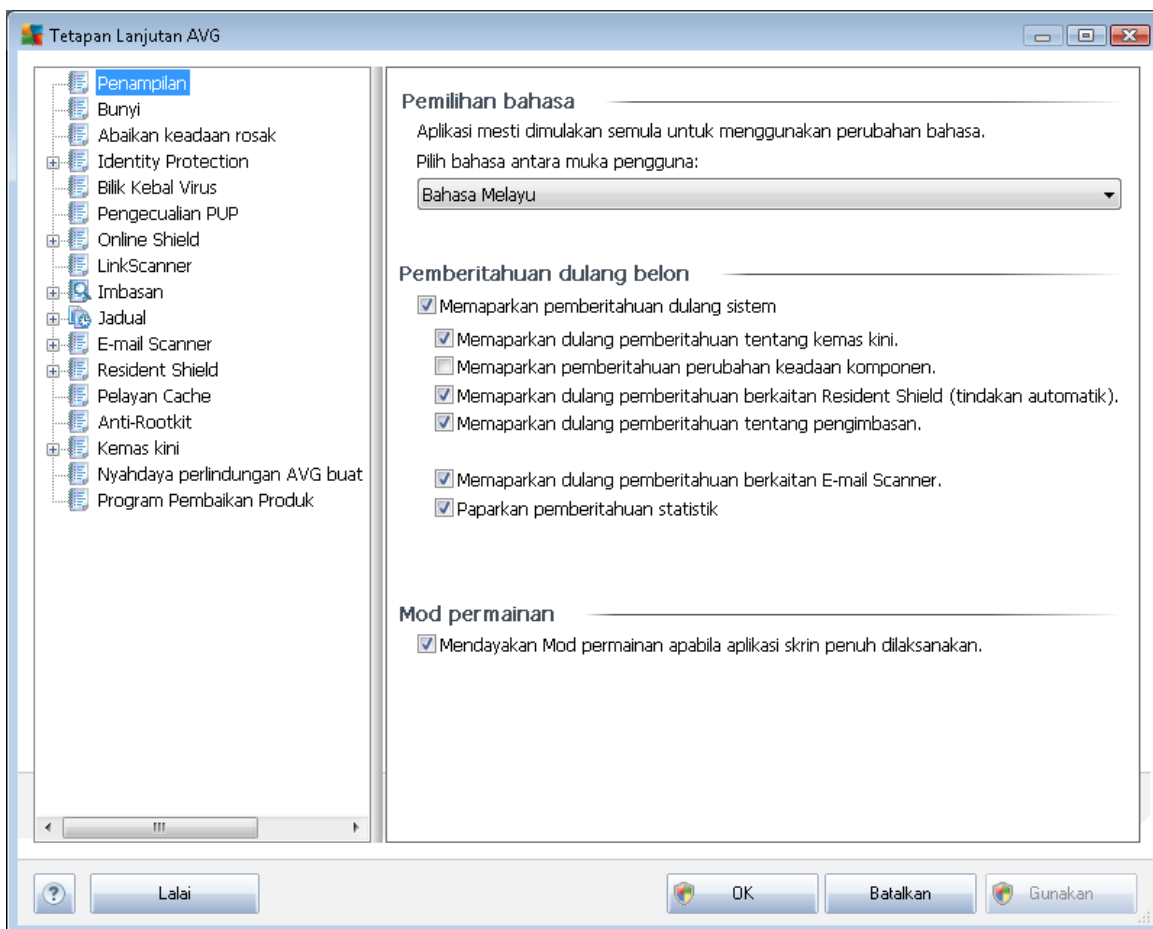


9. Tetapan Lanjutan AVG

Dialog konfigurasi lanjutan **AVG Anti-Virus 2011** terbuka dalam tettingkap baru yang dinamakan **Tetapan AVG Lanjutan**. Tetingkap dibahagikan kepada dua bahagian: bahagian kiri menawarkan navigasi pepohon yang diatur ke opsyen konfigurasi atur cara. Pilih komponen yang anda hendak ubah konfigurasi bagi (*atau bahagian tertentu*) untuk membuka dialog pengeditan dalam bahagian kanan tetingkap.

9.1. Penampilan

Item pertama bagi pepohon navigasi, **Penampilan**, merujuk kepada tetapan umum bagi [antara muka pengguna AVG](#) dan beberapa pilihan permulaan bagi kelakuan aplikasi:

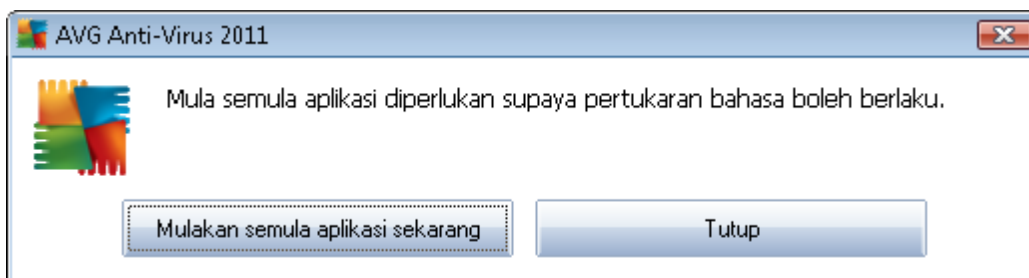


Pemilihan bahasa

Dalam bahagian **Pemilihan bahasa** anda boleh memilih bahasa yang anda kehendaki dari menu jatuh ke bawah; kemudian, bahasa tersebut akan digunakan untuk keseluruhan [antara muka pengguna AVG](#). Menu jatuh ke bawah menawarkan bahasa yang anda pilih sebelum ini untuk dipasang semasa [proses pemasangan](#) (*lihat bab [Opsyen Tersuai](#)*) dan Bahasa Inggeris (*yang dipasang secara lalai*). Walau bagaimanapun, untuk selesai menukar aplikasi ke bahasa lain, anda

perlu memulakan semula antara muka pengguna; ikuti langkah ini:

- Pilih bahasa aplikasi yang dikehendaki dan sahkan pemilihan anda dengan menekan butang **Guna** (penjuru bawah kanan)
- Tekan butang **OK** untuk mengesahkan
- Pop timbul tettingkap dialog baru memberitahu anda perubahan bahasa antara muka pengguna AVG memerlukan mula semula aplikasi:



Pemberitahuan dulang belon

Dalam bahagian ini, anda boleh menghimpit paparan pemberitahuan belon dulang sistem pada status aplikasi. Secara lalai, pemberitahuan belon boleh dipaparkan dan ia disarankan untuk mengekalkan konfigurasi ini! Pemberitahuan belon biasanya memberitahu mengenai beberapa perubahan status komponen AVG dan anda harus memberikan perhatian kepadanya!

Walau bagaimanapun, jika beberapa alasan yang anda tentukan untuk tidak dipaparkan pemberituannya atau anda hendak hanya pemberitahuan tertentu (berkaitan dengan komponen AVG khusus) dipaparkan, anda boleh mentakrifkan dan menentukan keutamaan anda dengan menanda/tidak menanda opsyen berikut:

- **Paparkan pemberitahuan dulang sistem** - secara lalai, item ini ditandakan (*dihidupkan*), dan pemberitahuan dipaparkan. Nyahtanda item ini untuk mematikan sepenuhnya semua paparan pemberitahuan belon. Semasa dihidupkan, anda seterusnya boleh memilih pemberitahuan khusus mana yang harus dipaparkan:
 - **Paparkan pemberitahuan dulang mengenai [kemas kini](#)** - tentukan sama ada maklumat berkenaan pelancaran proses, perkembangan dan penyelesaian kemas kini AVG harus dipaparkan;
 - **Paparkan pemberitahuan perubahan keadaan komponen** - tentukan sama ada maklumat berkenaan keaktifan/ketidaktifan komponen atau kemungkinan masalahnya harus dipaparkan. Semasa melaporkan status kerosakan komponen, opsyen ini sama dengan fungsi berguna bagi [ikon dulang sistem](#) (perubahan warna) melaporkan sebarang masalah dalam sebarang komponen AVG;
 - **Paparkan pemberitahuan dulang berkaitan [Perisai Residen](#) (*tindakan automatik*)** - putuskan sama ada maklumat mengenai proses penyimpanan, penyalinan dan pembukaan fail harus dipaparkan atau disekat (*konfigurasi ini hanya*



menunjukkan jika pilihan [Autopulih Perisai Residen](#) dihidupkan);

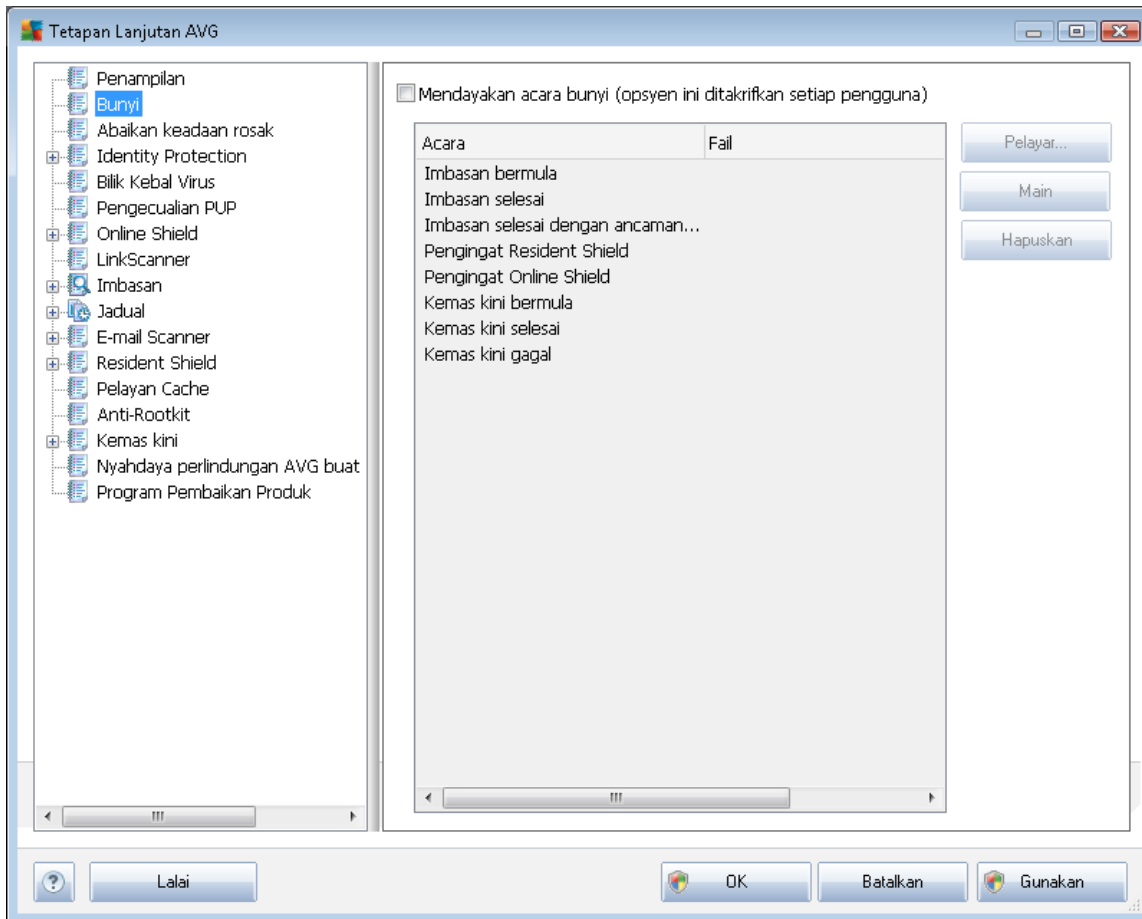
- o **Paparkan pemberitahuan dulang mengenai [pengimbasan](#)** - tentukan sama ada maklumat pada pelancaran automatik bagi imbasan yang dijadualkan, perkembangan dan keputusannya harus dipaparkan;
- o **Paparkan [Pengimbas E-mel](#) pemberitahuan dulang berkaitan** - tentukan sama ada maklumat mengenai pengimbasan semua mesej e-mel masuk dan keluar harus dipaparkan.
- o **Paparkan pemberitahuan statistik** - pastikan opsyen ditanda untuk membolehkan pemberitahuan semakan semula statistik dipaparkan dalam dulang sistem.

Mod permainan

Fungsi AVG ini direka bentuk untuk aplikasi skrin penuh di mana kemungkinan belon maklumat AVG (*dipaparkan cth. apabila imbasan yang dijadualkan dimulakan*) akan mengganggu (*ia boleh meminimumkan aplikasi atau merosakkan grafiknya*). Untuk mengelakkan situasi ini, pastikan kotak semakan untuk pilihan **Dayakan mod permainan semasa aplikasi skrin penuh dijalankan** ditandakan (*tetapan lalai*).

9.2. Bunyi

Dalam dialog **Bunyi** anda boleh menentukan sama ada anda hendak memberitahu mengenai tindakan AVG tertentu melalui pemberitahuan bunyi. Jika yang demikian, tandakan opsyen **Dayakan peristiwa bunyi** (*dimatikan secara lalai*) untuk mengaktifkan senarai tindakan AVG:

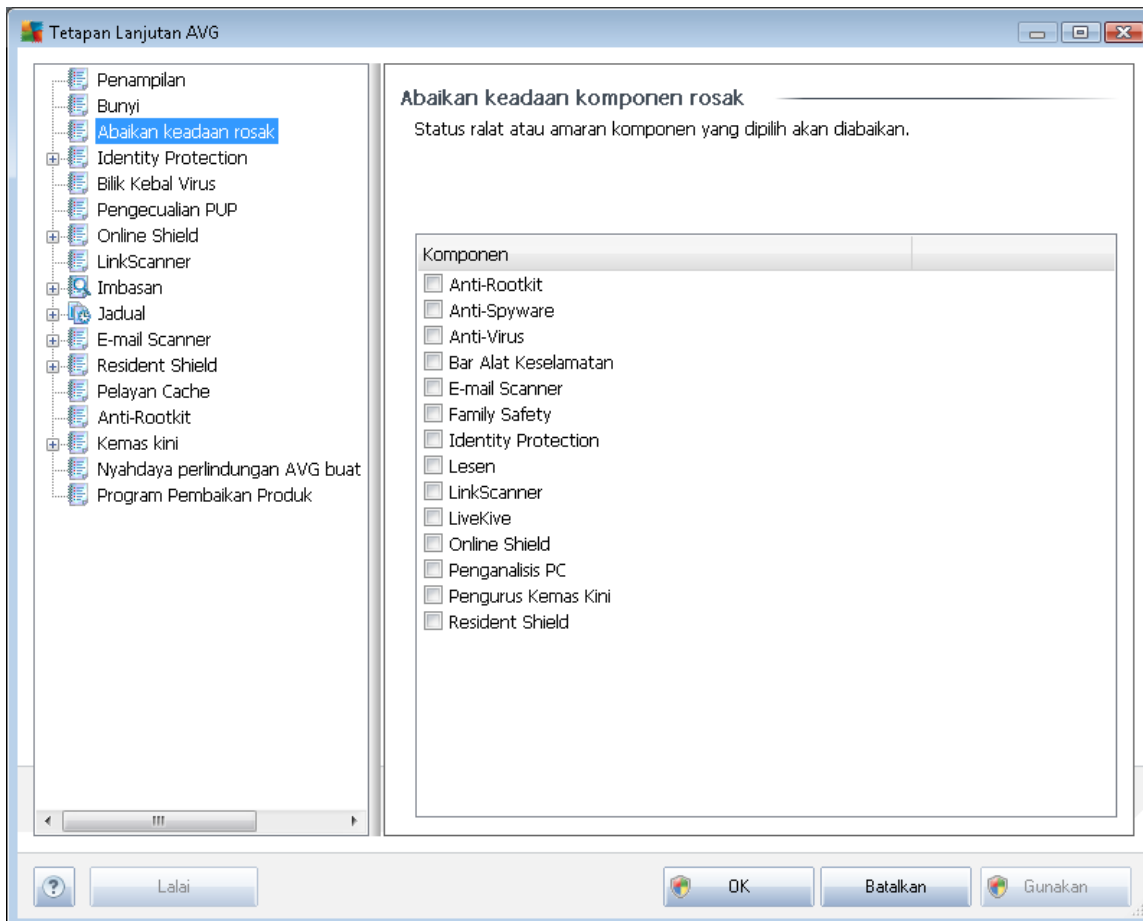


Kemudian, pilih peristiwa tersebut daripada senarai dan semak imbas (**Semak imbas**) cakera anda untuk bunyi yang sesuai yang anda hendak peruntukkan kepada peristiwa ini. Untuk mendengar bunyi yang dipilih, serlahkan peristiwa dalam senarai dan tekan butang **Main** . Gunakan butang **Padam** untuk membuang bunyi yang diperuntukkan kepada peristiwa tertentu.

Nota: Hanya bunyi *.wav yang disokong!

9.3. Abaikan Keadaan Rosak

Dalam dialog **Abaikan keadaan komponen rosak** anda boleh menanda rait komponen yang anda tidak mahu diberitahu:



Secara lalai, tiada komponen yang dipilih dalam senarai ini. Ia bermaksud bahawa jika sebarang komponen mendapat status ralat, anda akan diberitahu mengenainya dengan serta-merta melalui:

- **ikon dulang sistem** - semasa semua bahagian AVG bekerja dengan betul, ikon dipaparkan dalam empat warna; walau bagaimanapun, jika ralat berlaku, ikon muncul dengan tanda seruan berwarna kuning,
- penerangan teks bagi masalah sedia ada dalam bahagian **Maklumat Status Keselamatan** bagi tettingkap utama AVG

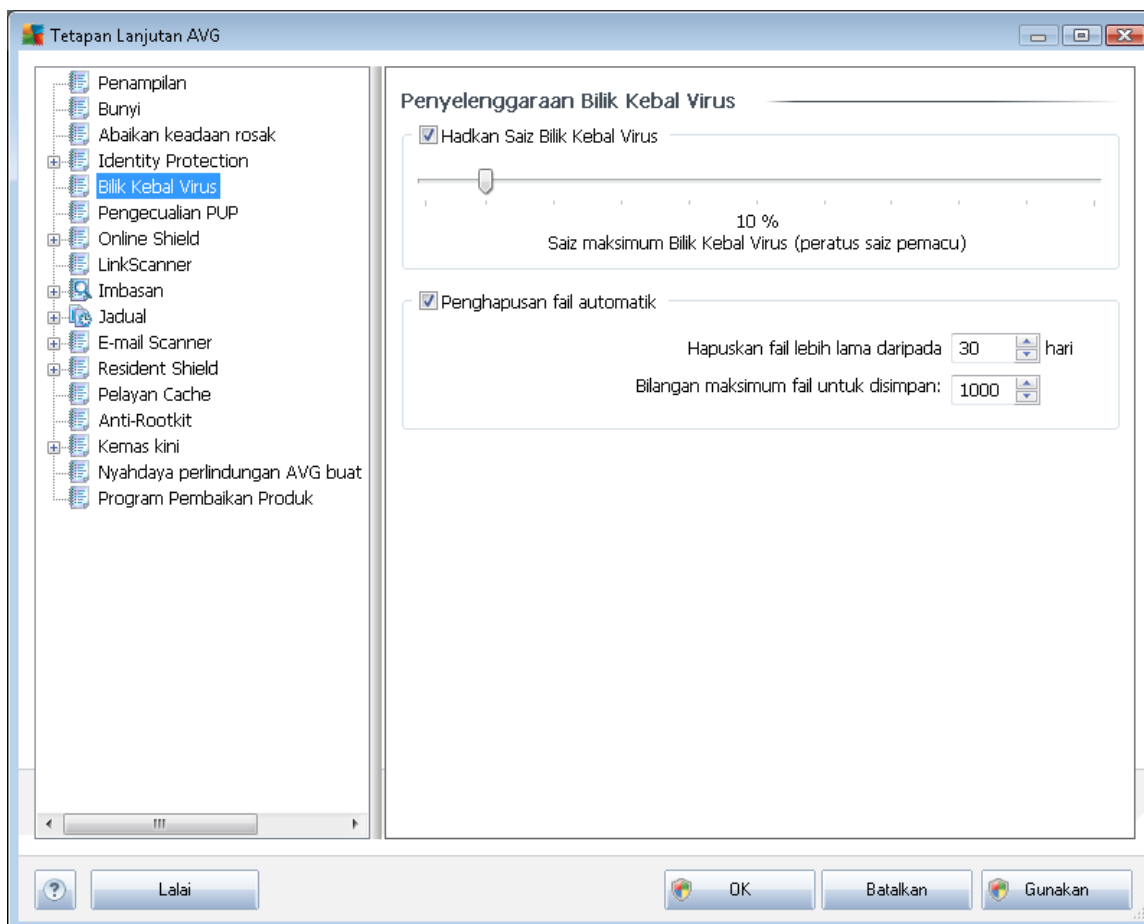
Mungkin terdapat situasi bagi sesetengah sebab anda perlu mematikan komponen secara sementara (*ini tidak disarankan, anda harus cuba memastikan semua komponen kekal dihidupkan dan dalam konfigurasi lalai, tetapi ia boleh berlaku*). Dalam kes itu, ikon dulang sistem secara automatik melaporkan status ralat komponen. Walau bagaimanapun, dalam kes ini, kita tidak dapat bercakap mengenai ralat sebenar memandangkan anda telah mencetuskannya dengan sengaja dan anda mengetahui kemungkinan risiko. Pada masa yang sama, apabila dipaparkan dalam warna



kelabu, ikon sebenarnya tidak boleh melaporkan sebarang kemungkinan ralat selanjutnya yang mungkin berlaku.

Untuk situasi ini, dalam dialog di atas, anda boleh memilih komponen yang mungkin berada dalam keadaan ralat (*atau dimatikan*) dan anda tidak mahu diberitahu mengenainya. Opsyen yang sama bagi **Mengabaikan keadaan komponen** juga tersedia untuk komponen tertentu secara terus dari gambaran keseluruhan [komponen dalam tettingkap utama AVG](#).

9.4. Bilik Kebal Virus



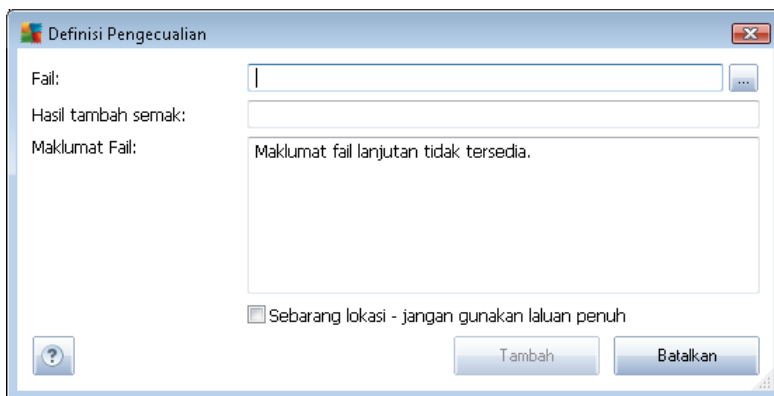
Dialog **penyelenggaraan Bilik Kebal Virus** membenarkan anda menentukan beberapa parameter berkenaan pentadbiran objek yang disimpan dalam [Bilik Kebal Virus](#):

- **Hadkan saiz Bilik Kebal Virus** - gunakan gelangsar untuk menyediakan saiz maksimum bagi [Bilik Kebal Virus](#). Saiz tersebut ditentukan mengikut perkadaran dibandingkan dengan saiz cakera setempat anda.
- **Pemadaman fail automatik** - dalam bahagian ini menentukan tempoh masa maksimum bagi objek yang patut disimpan dalam [Bilik Kebal Virus](#) (**Padam fail yang lebih lama daripada ... hari**), dan bilangan fail maksimum untuk disimpan dalam [Bilik Kebal Virus](#) (**Bilangan fail maksimum untuk disimpan**)

semak ini adalah rentetan aksara yang dijana secara automatik yang membenarkan AVG untuk membezakan fail yang dipilih daripada fail lain dengan jelas. Hasil tambah semak dijana dan dipaparkan selepas penambahan fail berjaya.

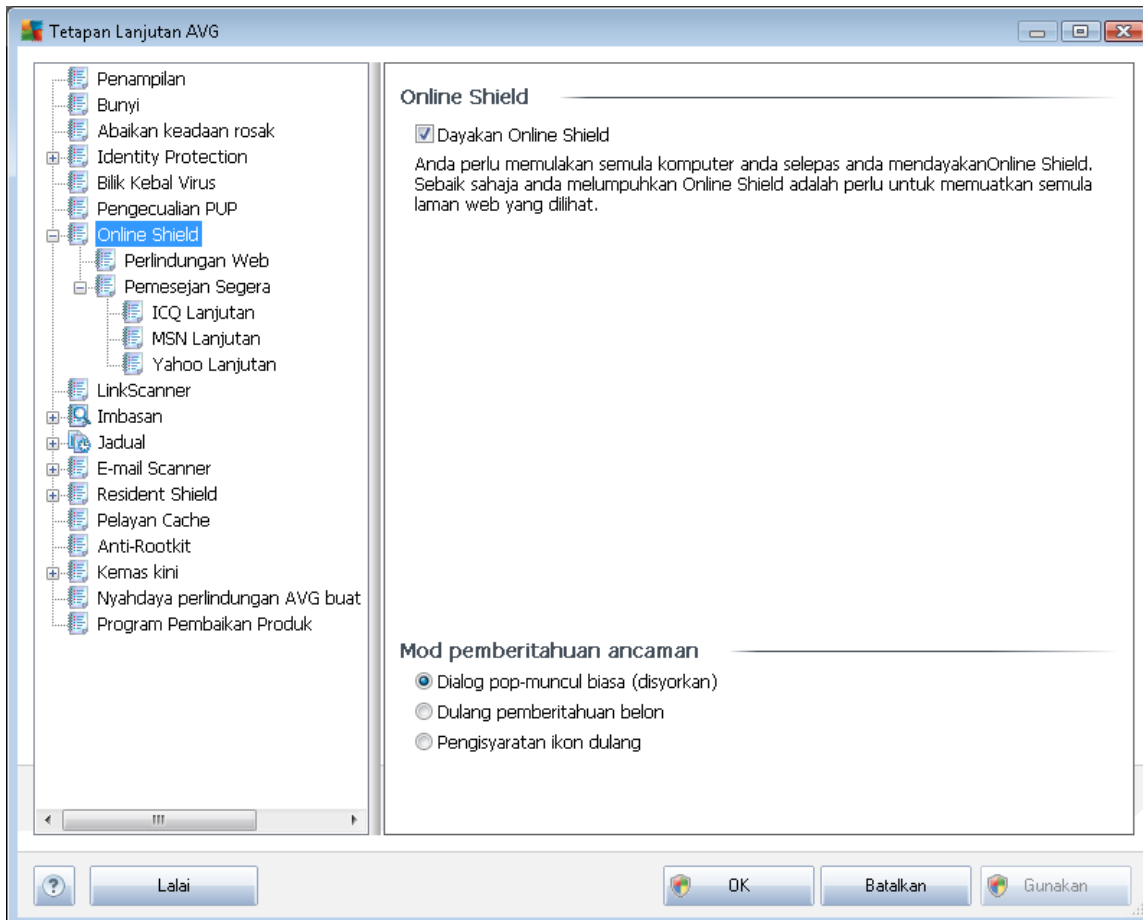
Butang kawalan

- **Edit** - membuka dialog pengeditan (*serupa dengan dialog untuk definisi pengecualian baru, lihat di bawah*) bagi pengecualian yang sudah ditakrifkan di mana anda boleh mengubah parameter pengecualian
- **Buang** - memadam item yang dipilih dari senarai pengecualian
- **Tambah pengecualian** - membuka dialog pengeditan di mana anda boleh mentakrifkan parameter bagi pengecualian baru untuk dicipta:



- **Fail** - taipkan laluan penuh ke fail yang anda ingin tandakan sebagai pengecualian
- **Hasil tambah semak** - memaparkan 'tandatangan' unik bagi fail yang dipilih. Hasil tambah semak ini adalah rentetan aksara yang dijana secara automatik yang membenarkan AVG untuk membezakan fail yang dipilih daripada fail lain dengan jelas. Hasil tambah semak dijana dan dipaparkan selepas penambahan fail berjaya.
- **Maklumat Fail** - memaparkan sebarang maklumat tambahan yang tersedia mengenai fail (*maklumat lesen/versi dll.*)
- **Sebarang lokasi - jangan gunakan laluan penuh** - jika anda mahu menentukan fail ini sebagai pengecualian hanya untuk lokasi tertentu, maka, biarkan kotak semak ini tidak bertanda. Jika kotak semak ini bertanda, fail yang ditetapkan ditakrifkan sebagai pengecualian walau di mana ia berada (*walau bagaimanapun, anda perlu mengisi laluan penuh ke fail ini juga; fail ini akan kemudiannya digunakan sebagai contoh unik bagi kemungkinan dua fail yang mempunyai nama yang sama muncul dalam sistem anda*).

9.6. Online Shield



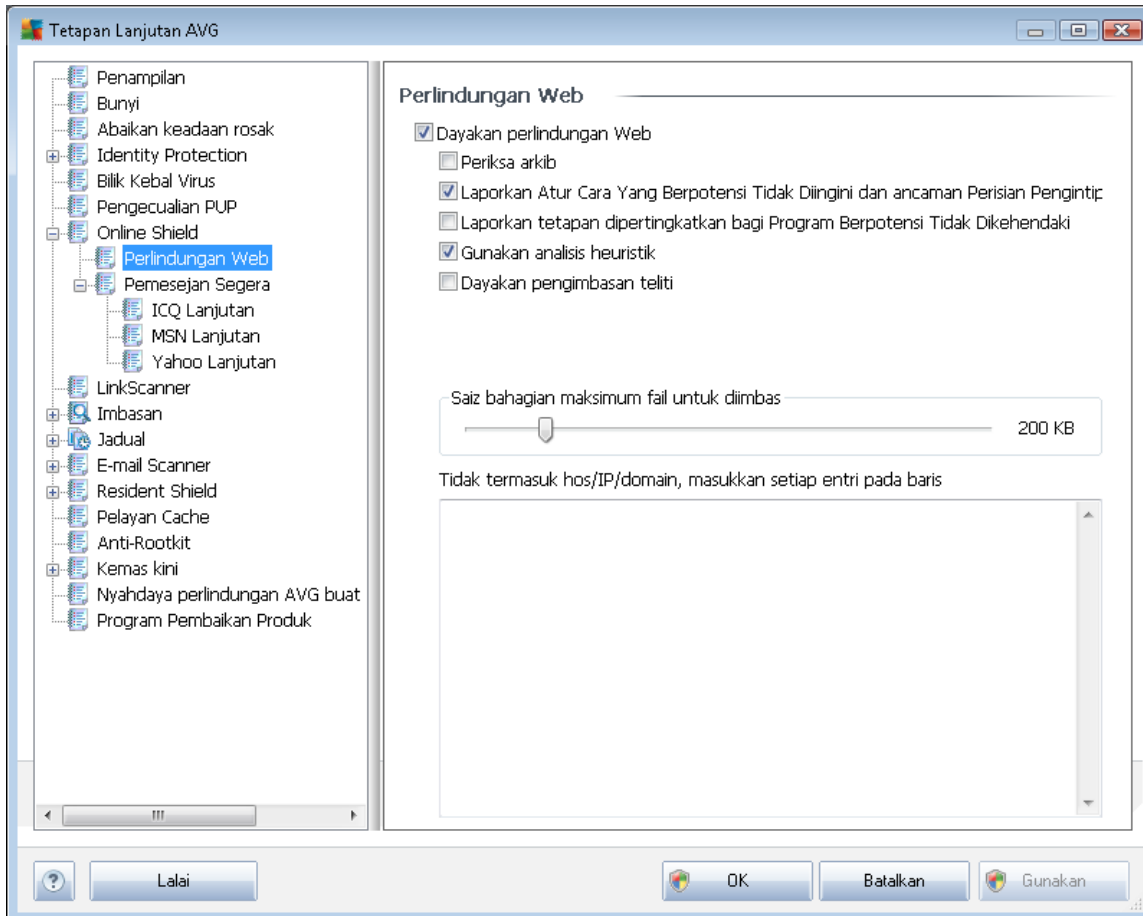
Dialog **Online Shield** membenarkan anda mengaktifkan/menyahaktifkan seluruh komponen **Online Shield** melalui opsyen **Dayakan Online Shield** (*diaktifkan secara lalai*). Untuk tetapan lanjutan seterusnya bagi komponen ini, sila teruskan ke dialog berikutnya seperti yang disenaraikan dalam navigasi pepohon:

- [Perlindungan Web](#)
- [Pemesejan Segera](#)

Mod pemberitahuan ancaman

Dalam bahagian bawah dialog, pilih dalam cara mana anda hendak diberitahu mengenai kemungkinan ancaman yang dikesan: melalui dialog pop timbul standard, melalui pemberitahuan belon dulang atau melalui maklumat ikon dulang.

9.6.1. Perlindungan Web



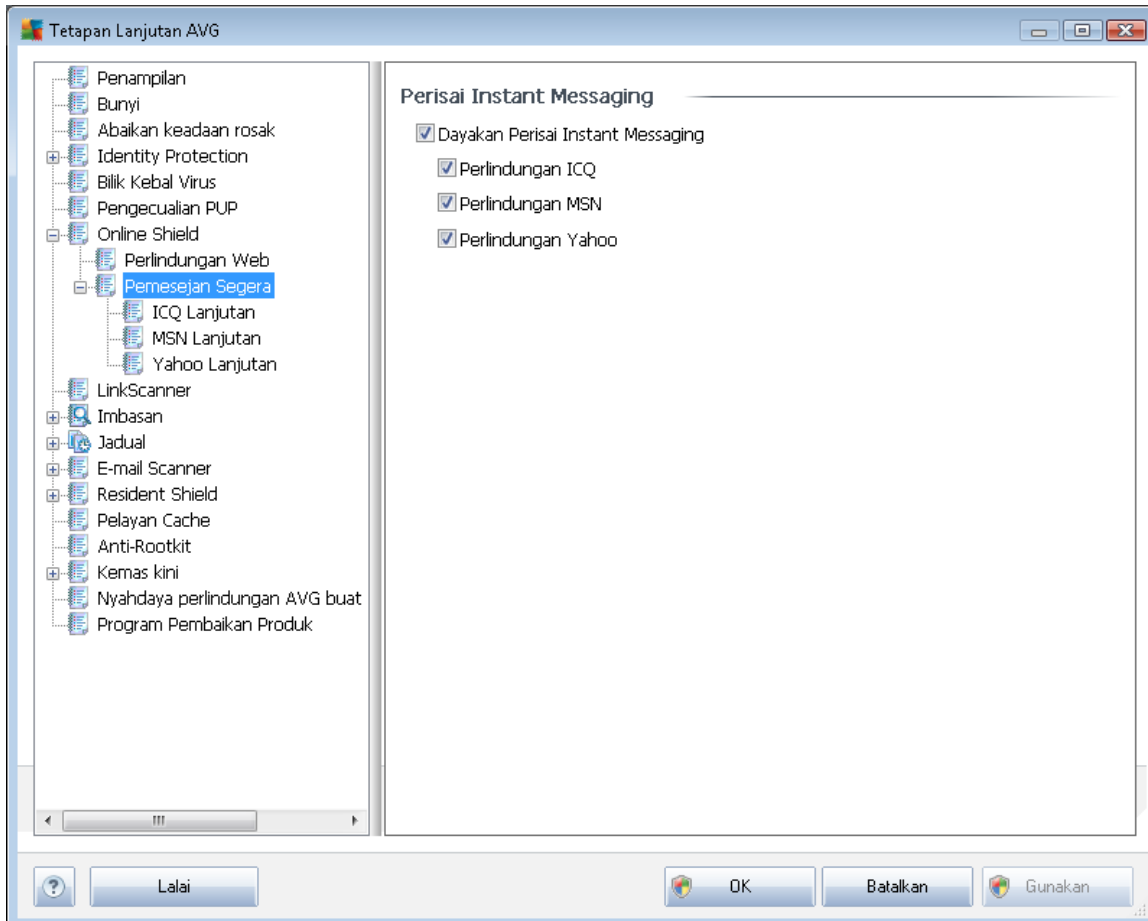
Dalam dialog **Perlindungan Web** anda boleh mengedit konfigurasi komponen berkenaan imbasan kandungan tapak web. Antara muka penyuntingan ini membenarkan anda untuk mengkonfigurasi opsyen permulaan berikut:

- **Dayakan perlindungan Web** - pilihan ini mengesahkan bahawa [Perisai Dalam Talian](#) harus menjalankan pengimbasan kandungan halaman www. Jika opsyen ini dihidupkan (*secara lalai*), seterusnya, anda boleh menghidupkan/mematikan item ini:
 - **Periksa arkib** - (*ditutup secara lalai*): imbas kandungan arkib yang berkemungkinan dimasukkan dalam halaman www untuk dipaparkan.
 - **Laporkan Atur Cara yang Berpotensi Tidak Diingini dan ancaman Perisian Pengintip** - (*dihidupkan secara lalai*): tandakan untuk mengaktifkan enjin [AntiPerisian Pengintip](#), dan imbas untuk perisian pengintip serta untuk virus. [Perisian pengintip mewakili kategori malware yang dipersoalkan, walaupun, ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat.](#) Kami mengesyorkan untuk mengekalkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.
 - **Laporkan set dipertingkatkan bagi Program Berpotensi Tidak Dikehendaki** -

ditutup secara lalai): tandakan untuk mengesan pakej yang diluaskan bagi [perisian pengintip](#): atur cara yang sangat ok dan tidak berbahaya apabila diperolehi dari pengilang secara terus, tetapi, boleh disalahgunakan untuk tujuan berniat jahat selepas itu. Ini adalah langkah tambahan yang meningkatkan keselamatan komputer anda dengan lebih lagi, walau bagaimanapun, ia boleh menyekat atur cara sah dan oleh itu, dimatikan secara lalai.

- **Gunakan analisis heuristik** - (*dibuka secara lalai*): imbas kandungan halaman yang akan dipaparkan menggunakan kaedah [analisis heuristik](#) (*perlagakan dinamik arahan objek yang diimbas dalam persekitaran komputer maya*).
- **Dayakan pengimbasan teliti** (*ditutup secara lalai*) - dalam situasi khusus (*mengesyaki komputer anda dijangkiti*) anda boleh menandakan opsi ini untuk mengaktifkan algoritma pengimbasan yang paling teliti yang akan turut mengimbas kawasan komputer anda yang sukar dijangkiti, sekadar untuk mendapatkan kepastian sepenuhnya. Namun ingat bahawa kaedah ini agak mengambil masa
- **Bahagian saiz fail maksimum untuk diimbas** - jika fail yang dimasukkan terdapat dalam halaman yang dipaparkan, anda juga boleh mengimbas kandungannya sebelum ia dimuat turun ke komputer anda. Walau bagaimanapun, pengimbasan fail besar mengambil sedikit masa dan muat turun laman web mungkin menjadi perlahan. Anda boleh menggunakan bar gelangsar untuk menentukan saiz maksimum bagi fail yang masih diimbas dengan [Perisai Dalam Talian](#). Walaupun jika fail yang dimuat turun adalah lebih besar daripada yang ditentukan, dan oleh itu, tidak akan diimbas dengan Perisai Dalam Talian, anda masih dilindungi: jika fail dijangkiti, [Resident Shield](#) akan mengesannya dengan serta-merta.
- **Keluarkan hos/IP/domain** - ke dalam medan teks, anda boleh menaip nama sebenar bagi pelayan (*hos, alamat IP, alamat IP dengan topeng, atau URL*) atau domain yang harus diimbas oleh [Perisai Dalam Talian](#). Oleh itu, hanya kecualikan hos yang anda betul-betul pasti tidak akan memberikan kandungan tapak web berbahaya.

9.6.2. Pemesejan Segera

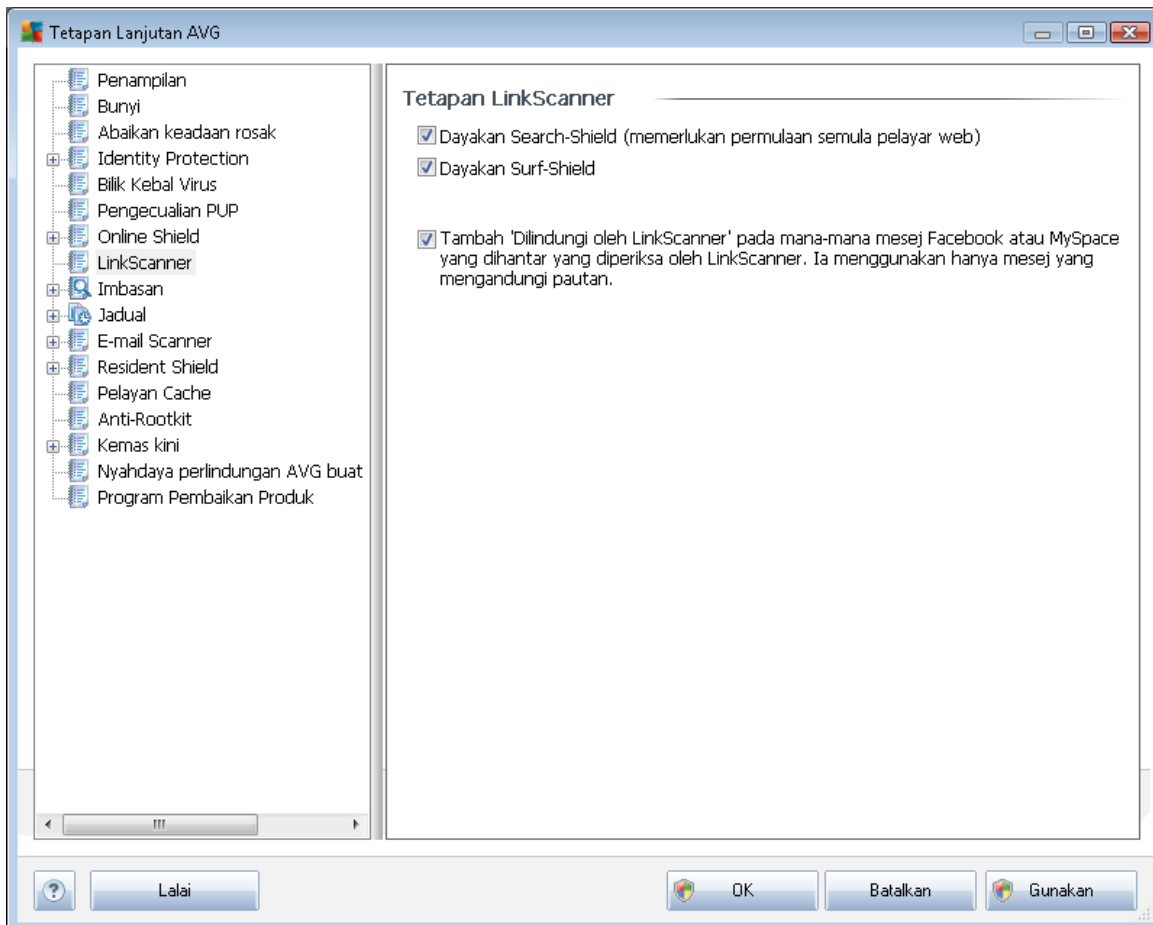


Dalam dialog **Perisai Pemesejan Segera** anda boleh mengedit tetapan komponen **Perisai Dalam Talian** yang merujuk kepada pengimbasan pemesejan segera. Buat masa ini, tiga atur cara pemesejan segera disokong: **ICQ**, **MSN**, dan **Yahoo** - tandakan rait item masing-masing untuk setiap satunya jika anda mahukan **Perisai Dalam Talian** mengesahkan komunikasi dalam talian adalah bebas virus.

Untuk spesifikasi selanjutnya mengenai pengguna dibenarkan/disekat, anda boleh melihat dan mengedit dialog masing-masing (**ICQ Lanjutan**, **MSN Lanjutan**, **Yahoo Lanjutan**) dan tentukan **Senarai Putih** (*senarai pengguna yang akan dibenarkan untuk berkomunikasi dengan anda*) dan pengguna **Senarai Hitam** (*yang harus disekat*).

9.7. Pengimbas Pautan

Dialog **tetapan LinkScanner** membenarkan anda menghidupkan/mematikan ciri permulaan bagi **LinkScanner**.



- **Dayakan Search-Shield** - (*dihidupkan secara lalai*): ikon pemberitahuan penasihat mengenai carian dilakukan dengan Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg atau SlashDot diperiksa kandungan tapak yang dikembalikan oleh enjin carian.
- **Dayakan Surf-Shield** - (*hidupkan secara lalai*): perlindungan (*masa nyata*) aktif daripada tapak yang boleh mengeksploitasi apabila ia diakses. Sambungan tapak yang diketahui berniat jahat dan kandungannya yang boleh mengeksploitasi apabila ia diakses oleh pengguna melalui penyemak imbas web (*atau sebarang aplikasi lain yang menggunakan HTTP*).
- **Tambah 'Dipastikan selamat oleh LinkScanner' ...** - tandakan item ini jika anda ingin memasukkan notis perakuan mengenai semakan **Link Scanner** ke dalam semua mesej yang mengandungi hiperpautan aktif, yang dihantar dari rangkaian sosial Facebook dan MySpace.



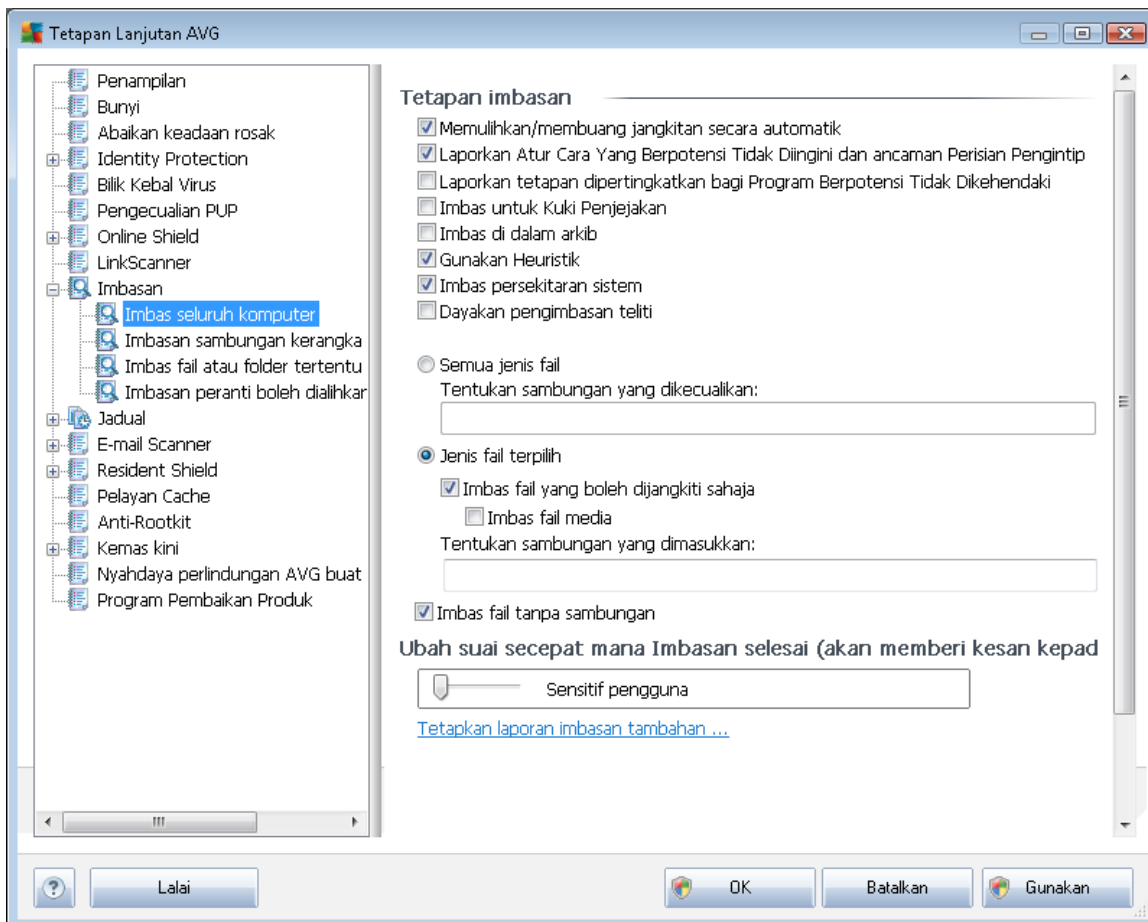
9.8. Imbasan

Tetapan imbasan lanjutan dibahagikan kepada empat kategori merujuk kepada jenis imbasan khusus seperti yang ditentukan oleh vendor perisian:

- [Imbasan Seluruh Komputer](#) - imbasan dipraktik standard bagi seluruh komputer
- [Imbasan Sambungan Kerangka](#) - imbasan khusus bagi objek yang dipilih dari persekitaran Windows Explorer
- [Imbas Fail atau Folder Khusus](#) - imbasan dipraktik khusus bagi kawasan yang dipilih pada komputer anda
- [Imbasan Peranti Boleh Dialihkan](#) - pengimbasan khusus bagi peranti boleh dialihkan yang dilampirkan ke komputer anda

9.8.1. Imbas Seluruh Komputer

Opsyen **Imbas Seluruh Komputer** membenarkan anda mengedit parameter bagi salah satu imbasan yang dipraktikkan oleh vendor perisian, [Imbasan seluruh komputer](#).





Tetapan imbasan

Bahagian **Tetapan imbasan** menawarkan senarai parameter imbasan yang boleh dihidupkan/dimatikan secara pilihan:

- **Pulih/buang jangkitan secara automatik** (*dibuka secara lalai*) - jika virus dikenal pasti sewaktu imbasan, ia boleh dipulihkan secara automatik jika cara mengatasinya tersedia. Jika fail yang dijangkiti tidak boleh dipulihkan secara automatik, objek yang dijangkiti akan dialih ke [Bilik Kebal Virus](#).
- **Laporkan Program Berpotensi Tidak Dikehendaki dan ancaman Perisian Pengintip** (*dibuka secara lalai*) - tandakan untuk mengaktifkan enjin [AntiPerisian Pengintip](#), dan imbas untuk perisian pengintip serta untuk virus. [Perisian pengintip mewakili kategori malware yang dipersoalkan, walaupun, ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat.](#) Kami mengesyorkan untuk mengekalkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.
- **Laporkan set dipertingkatkan bagi Program Berpotensi Tidak Dikehendaki**(*ditutup secara lalai*) -tandakan untuk mengesan pakej yang diluaskan bagi [perisian pengintip](#): atur cara yang sangat ok dan tidak berbahaya apabila diperoleh dari pengilang secara terus, tetapi, boleh disalahgunakan untuk tujuan berniat jahat selepas itu. Ini adalah langkah tambahan yang meningkatkan keselamatan komputer anda dengan lebih lagi, walau bagaimanapun, ia boleh menyekat atur cara sah dan oleh itu, dimatikan secara lalai.
- **Imbas untuk Kuki Penjejakan**(*ditutup secara lalai* - parameter ini bagi komponen [AntiPerisian Pengintip](#)mentakrifkan bahawa kuki harus dikesan;*kuki HTTP digunakan untuk mengesahkan, menjejaki dan mengekalkan maklumat tertentu mengenai pengguna seperti keutamaan tapak atau kandungan kart beli-belah elektroniknya*
- **Imbas dalam arkib**(*ditutup secara lalai*) - parameter ini menentukan bahawa imbasan harus memeriksa semua fail yang disimpan dalam arkib, cth. ZIP, RAR, ...
- **Gunakan Heuristik** - (*dibuka secara lalai*) - analisis heuristik (*perlagakan dinamik arahan objek yang diimbas dalam persekitaran komputer maya*) akan menjadi salah satu kaedah yang digunakan untuk pengesanan virus sewaktu imbasan;
- **Imbas persekitaran sistem** (*dibuka secara lalai*) - imbasan juga akan memeriksa kawasan sistem komputer anda.
- **Dayakan pengimbasan teliti**(*ditutup secara lalai*) - dalam situasi khusus (*mengesyaki komputer anda dijangkiti*) anda boleh menandakan opsyen ini untuk mengaktifkan algoritma pengimbasan yang paling teliti yang akan turut mengimbas kawasan komputer anda yang sukar dijangkiti, sekadar untuk mendapatkan kepastian sepenuhnya. Namun ingat bahawa kaedah ini agak mengambil masa.

Seterusnya, anda harus menentukan sama ada anda mahu mengimbas

- **Semua jenis fail** dengan kemungkinan pengecualian yang ditakrifkan daripada imbasan dengan memberikan senarai yang pemanjangan fail yang dipisahkan oleh koma (*apabila*

disimpan, koma bertukar kepada koma bertitik) yang tidak harus diimbis;

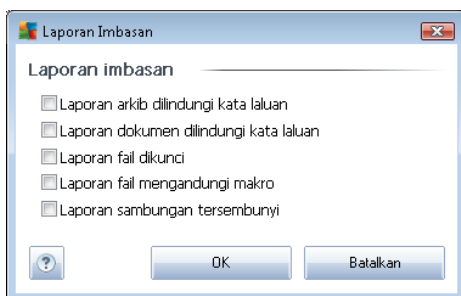
- **Jenis fail yang dipilih** - anda boleh menentukan bahawa anda hendak mengimbis hanya fail yang berkemungkinan dijangkiti (*fail yang tidak boleh dijangkiti tidak akan diimbis, contohnya sesetengah fail teks biasa atau sesetengah fail bukan boleh laku*), termasuk fail media (*video, fail audio - jika anda membiarkan kotak in tidak ditandakan, ia akan mengurangkan lebih banyak masa kerana fail ini biasanya agak besar dan agak tidak berkemungkinan dijangkiti virus*). Sekali lagi, anda boleh menentukan sambungan fail mana yang sepatutnya sentiasa diimbis.
- Secara pilihan, anda boleh menentukan anda hendak **Mengimbis fail tanpa sambungan** - opsyen ini dihidupkan secara lalai dan ia disyorkan untuk anda mengekalkannya melainkan anda mempunyai sebab sebenar untuk mengubahnya. Fail tanpa sambungan adalah lebih mencurigakan dan sepatutnya diimbis setiap masa.

Laraskan berapa cepat Imbasan selesai

Dalam bahagian **Laraskan berapa cepat imbasan selesai** anda boleh menentukan selanjutnya kelajuan pengimbasan yang dikehendaki bergantung kepada penggunaan sumber sistem. Secara lalai, nilai opsyen ini ditetapkan kepada tahap *sensitif pengguna* bagi penggunaan sumber automatik. Jika anda hendak imbasan dijalankan dengan pantas, ia akan mengambil masa yang kurang tetapi penggunaan sumber sistem akan meningkat dengan ketara sewaktu imbasan dan akan melambatkan aktiviti anda yang lain pada PC (*opsyen ini boleh digunakan semasa komputer anda dihidupkan tetapi tiada siapa yang menggunakannya*). Sebaliknya, anda boleh mengurangkan penggunaan sumber sistem dengan menambah tempoh pengimbasan.

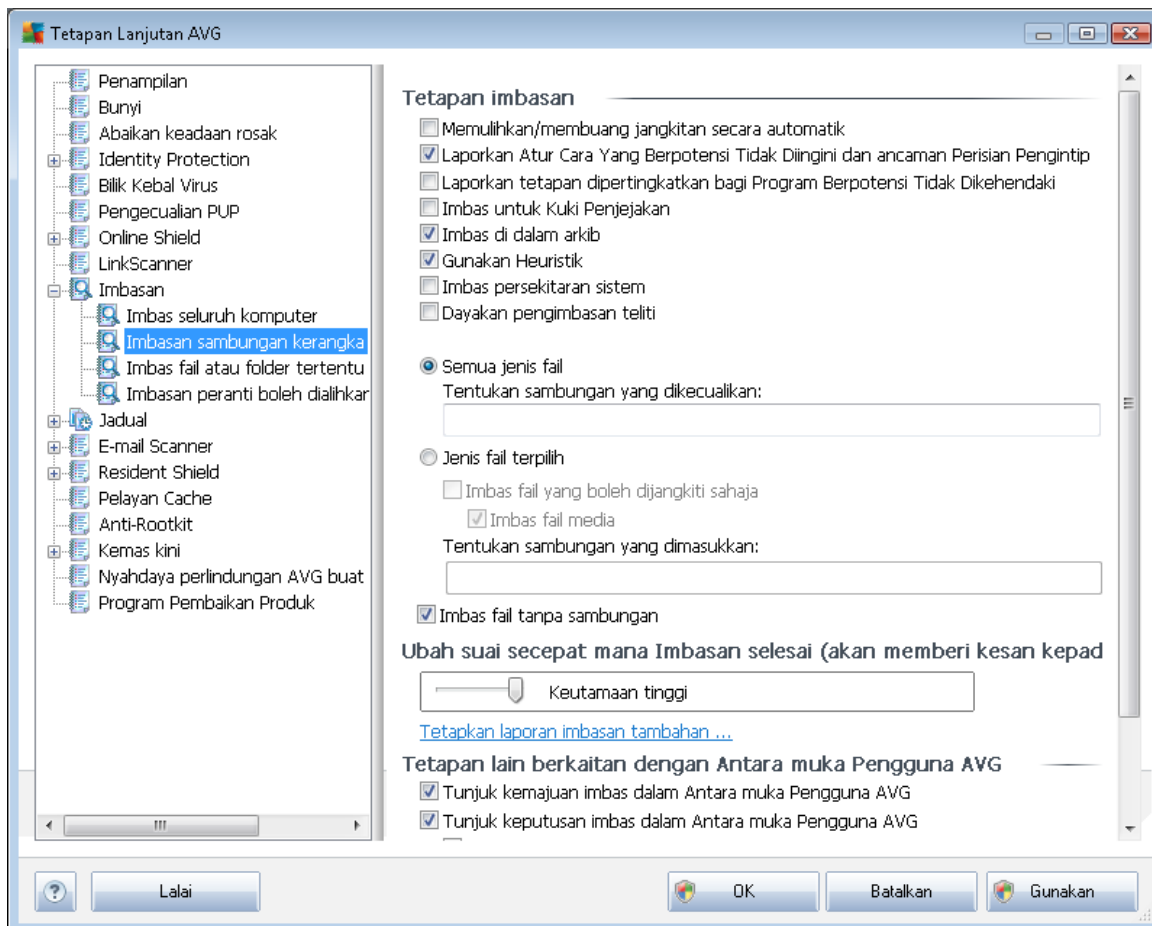
Tetapkan laporan imbasan tambahan ...

Klik pautan **Tetapkan laporan imbasan tambahan ...** untuk membuka tettingkap dialog tersendiri yang dipanggil **Laporan imbasan** di mana anda boleh menanda rait beberapa item untuk mentakrifkan penemuan imbasan yang harus dilaporkan:



9.8.2. Imbasan Sambungan Kerangka

Sama dengan item [Imbasan seluruh komputer](#) sebelumnya, item ini dinamakan **Imbasan sambungan kerangka** juga menawarkan beberapa opsyen untuk pengeditan imbasan yang dipraktikkan oleh vendor perisian. Kali ini, konfigurasi dikaitkan dengan [pengimbasan objek tertentu dilancarkan secara terus dari persekitaran Windows Explorer](#) (*sambungan kerangka*), lihat bab [Mengimbis dalam Windows Explorer](#).



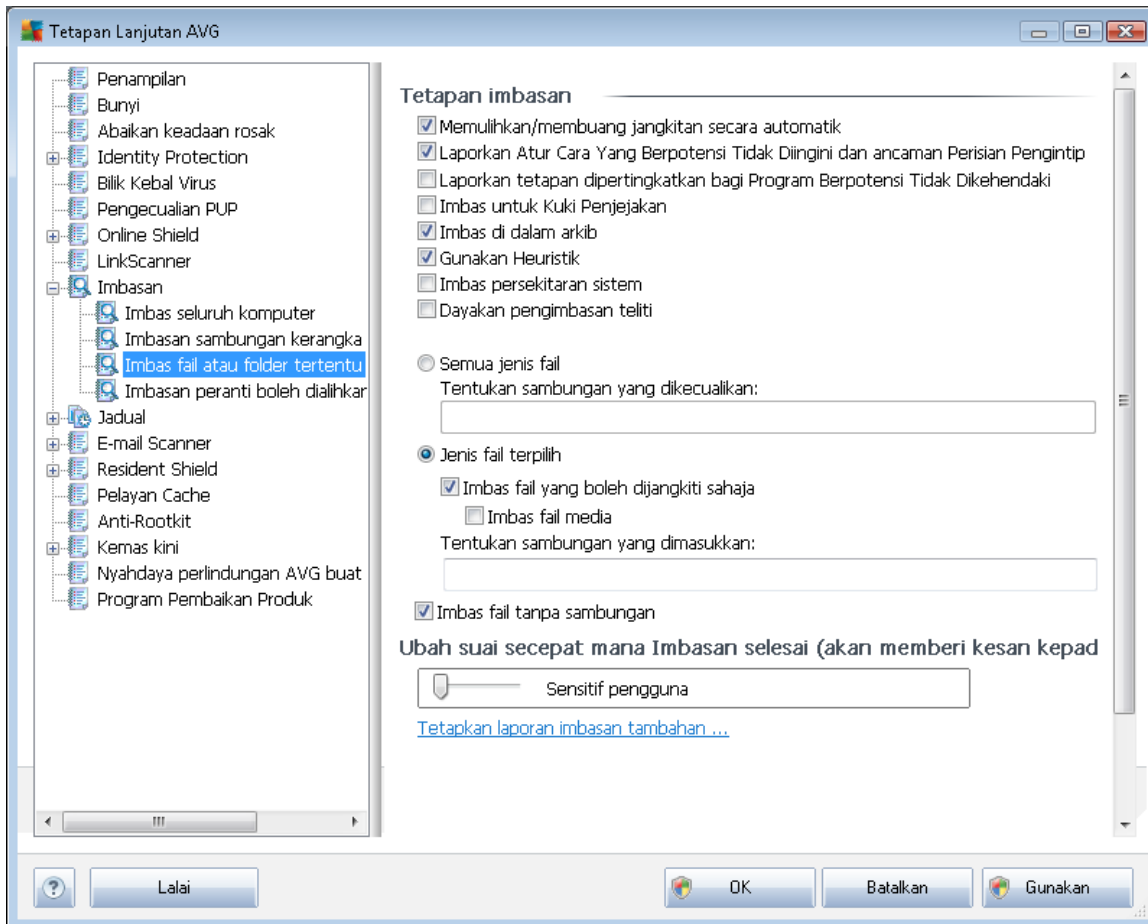
Senarai parameter adalah sama dengan yang tersedia untuk [Imbas seluruh komputer](#). Walau bagaimanapun, tetapan lalai berbeza (*contohnya, Imbasan Seluruh Komputer secara lalai tidak memeriksa arkib tetapi ia mengimbas persekitaran sistem, manakala dengan Imbasan Sambungan Kerangka ia adalah sebaliknya*).

Perhatian: Untuk penerangan mengenai parameter tertentu, sila rujuk bab [Tetapan Lanjutan AVG / Imbasan / Imbasan Seluruh Komputer](#).

Jika dibandingkan dengan dialog [Imbasan Seluruh Komputer](#), dialog **Imbasan sambungan kerangka** turut memasukkan bahagian yang dinamakan **Tetapan lain berkaitan Antara Muka Pengguna AVG**, di mana anda boleh menentukan sama ada anda mahu kemajuan imbasan dan keputusan imbasan boleh diakses dari antara muka pengguna AVG. Juga, anda boleh mentakrifkan bahawa keputusan imbasan hanya boleh dipaparkan jika jangkitan dikesan semasa pengimbasan.

9.8.3. Imbas Fail atau Folder Tertentu

Antara muka pengeditan untuk **Imbas fail atau folder tertentu** adalah sama dengan dialog pengeditan [Imbas Seluruh Komputer](#). Semua opsyen konfigurasi adalah sama; walau bagaimanapun, tetapan lalai adalah lebih tegas untuk [Imbas seluruh komputer](#).

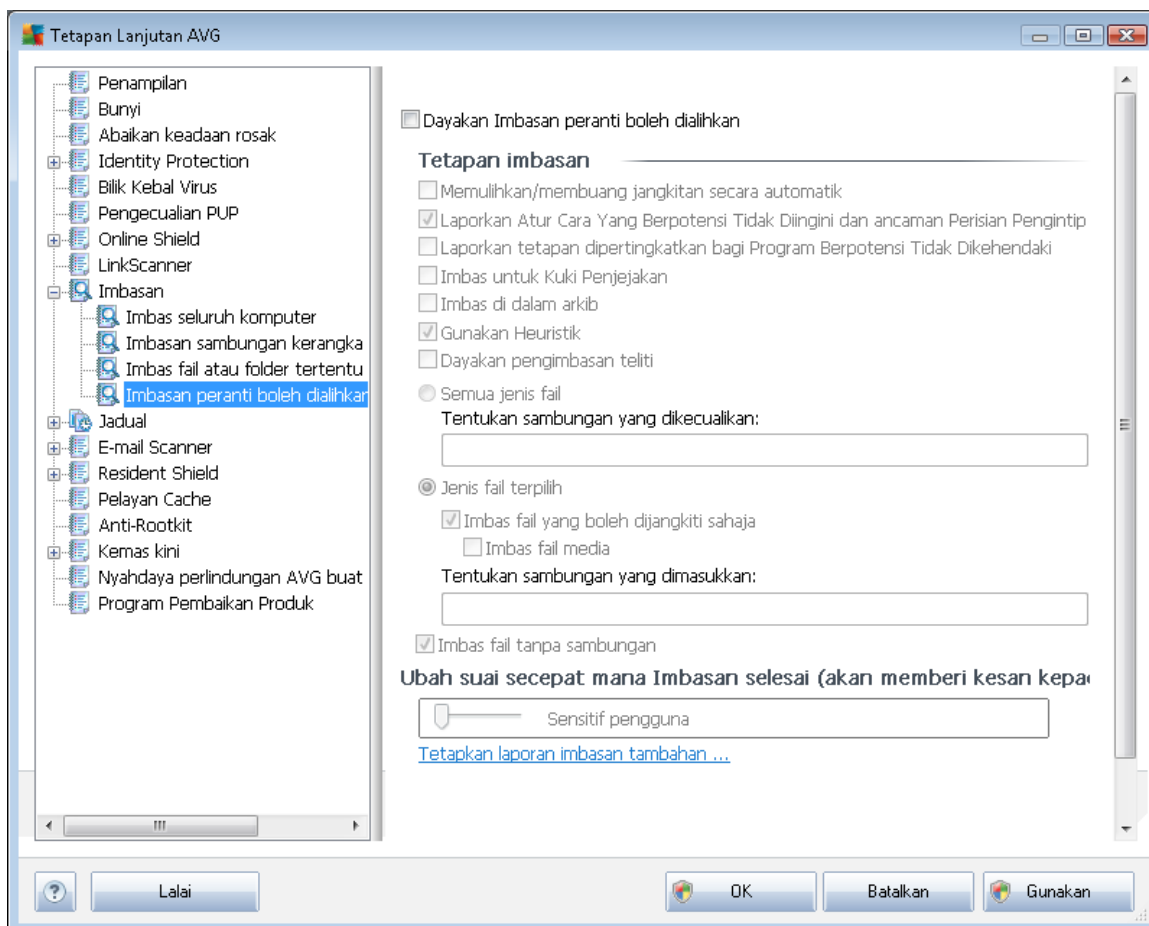


Semua parameter yang disediakan dalam dialog konfigurasi ini hanya digunakan pada kawasan yang dipilih untuk imbasan dengan **Imbas fail atau folder tertentu!**

Perhatian: Untuk penerangan mengenai parameter tertentu, sila rujuk bab **Tetapan Lanjutan AVG / Imbasan / Imbas Seluruh Komputer.**

9.8.4. Imbasan Peranti Boleh Dialih

Antara muka pengeditan untuk *Imbasan peranti boleh ditanggalkan* juga sama dengan dialog pengeditan [Imbas Seluruh Komputer](#).



Imbasan peranti boleh dialihkan dilancarkan secara automatik apabila anda melampirkan sebarang peranti boleh dialihkan ke komputer anda. Secara lalai, pengimbasan ini dimatikan. Walau bagaimanapun, ia adalah penting untuk mengimbas peranti boleh dialihkan untuk kemungkinan ancaman memandangkan ini adalah sumber jangkitan utama. Untuk membuatkan imbasan ini bersedia dan dilancarkan secara automatik apabila diperlukan, tanda opsyen **Dayakan imbasan peranti boleh dialihkan**.

Perhatian: Untuk penerangan mengenai parameter tertentu, sila rujuk bab [Tetapan Lanjutan AVG / Imbasan / Imbas Seluruh Komputer](#).

9.9. Jadual

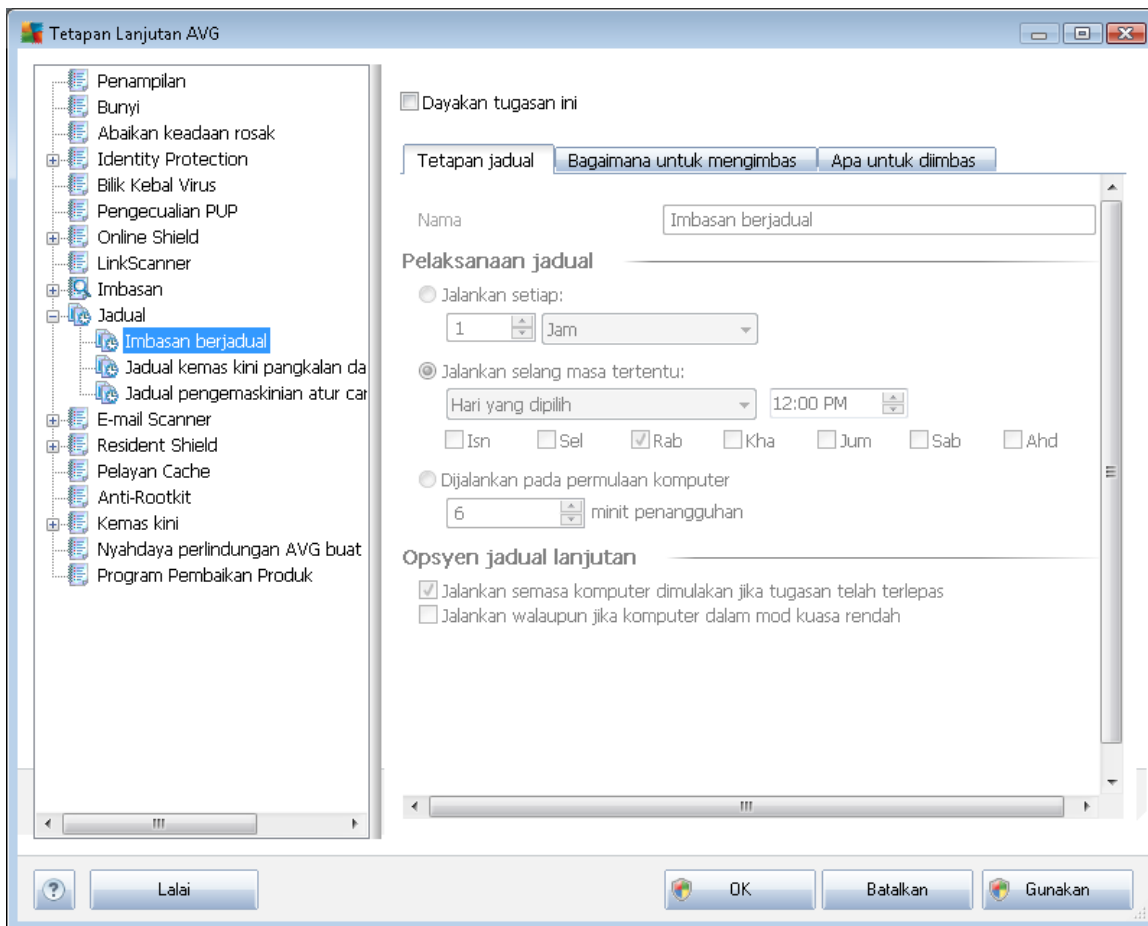
Dalam bahagian **Jadual** anda boleh mengedit tetapan lalai bagi:

- [Imbasan berjadual](#)

- [Jadual kemas kini pangkalan data virus](#)
- [Jadual kemas kini atur cara](#)

9.9.1. Imbasan yang Dijadualkan

Parameter bagi imbasan yang dijadualkan boleh diedit (*atau jadual baru disediakan*) pada tiga tab. Pada setiap tab, anda boleh menanda/tidak menanda dahulu item **Dayakan tugas ini** untuk menyahaktifkan ujian yang dijadualkan buat sementara waktu, dan menghidupkannya semula apabila perlu:



Seterusnya, dalam medan teks dipanggil **Nama** (*dinyahaktifkan untuk semua jadual lalai*) terdapat nama yang diperuntukkan kepada jadual ini oleh vendor atur cara. Untuk jadual yang baru ditambah (*anda boleh menambah jadual baru dengan mengklik kanan tetikus item **Imbasan yang dijadualkan** dalam pepohon navigasi kin*) anda boleh menentukan nama anda sendiri dan jika medan teks akan terbuka untuk pengeditan. Cuba selalu gunakan nama yang ringkas, deskriptif dan sesuai untuk imbasan untuk membuatkan ia mudah untuk kemudian, mengenal pasti imbasan dari yang lain.

Contoh: Ia tidak sesuai untuk memanggil imbasan dengan nama "Imbasan baru" atau "Imbasan



saya" memandangkan nama ini tidak merujuk kepada apa yang sebenarnya imbasan periksa. Sebaliknya, contoh nama deskriptif adalah "Imbasan kawasan sistem" dll. Serta, tidak perlu untuk menentukan jika nama imbasan sama ada ia adalah imbasan seluruh komputer atau hanya imbasan fail atau folder yang dipilih - imbasan anda sendiri yang akan sentiasa menjadi versi khusus bagi [imbasan bagi fail atau folder yang dipilih](#).

Di dalam dialog ini anda boleh menentukan lebih lanjut parameter imbasan yang berikut:

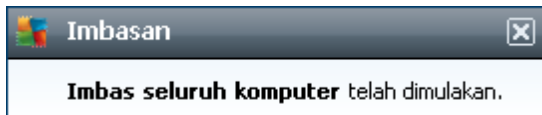
Pelaksanaan jadual

Di sini, anda boleh menentukan jarak waktu untuk pelancaran imbasan baru yang dijadualkan. Pemasaan boleh menjadi sama ada ditakrifkan oleh pelancaran imbasan berulang selepas satu tempoh masa tertentu (**Jalankan setiap ...**) atau dengan menentukan tarikh dan masa sebenar (**Jalankan pada jarak waktu khusus ...**), atau berkemungkinan dengan mentakrifkan peristiwa yang pelancaran imbasan harus dikaitkan dengan (**Tindakan berdasarkan permulaan komputer**).

Opsyen jadual lanjutan

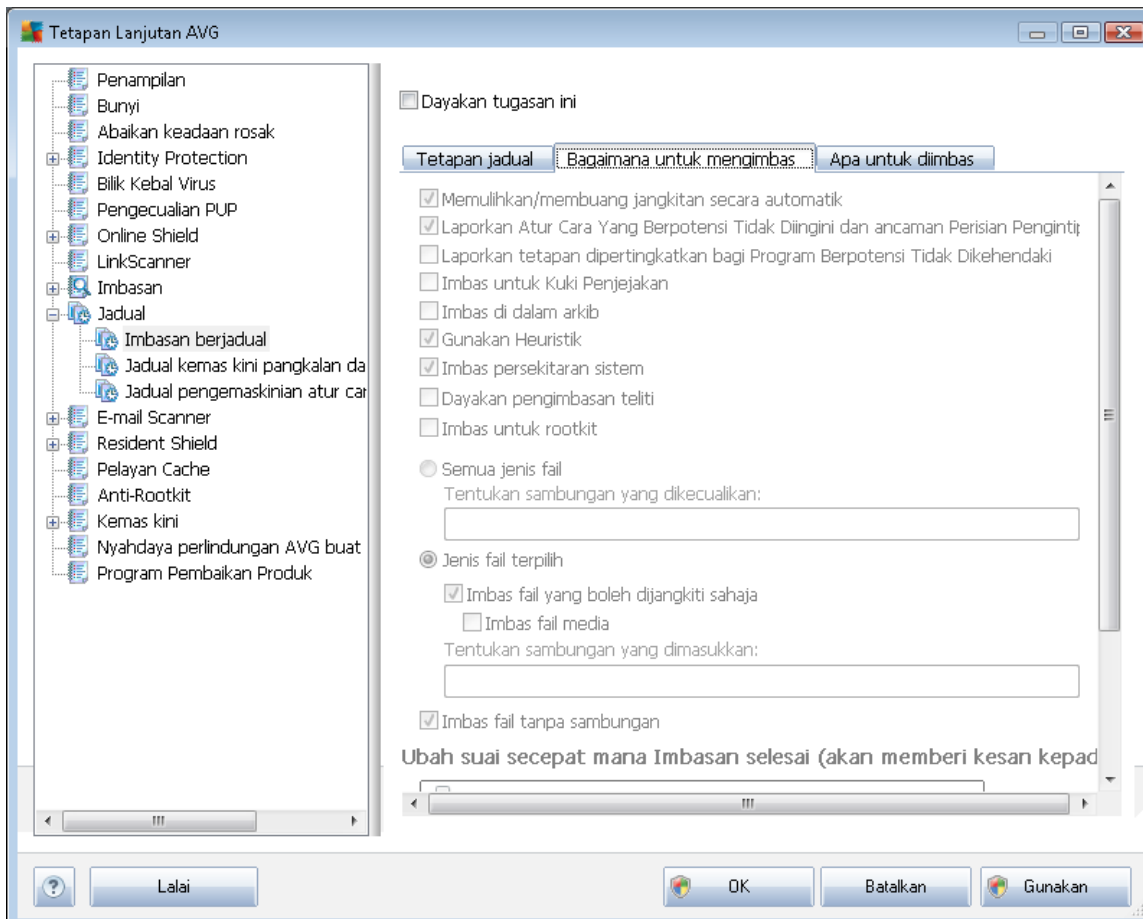
Bahagian ini membenarkan anda untuk mentakrifkan di bawah keadaan mana imbasan patut/tidak patut dilancarkan jika komputer di dalam mod kuasa rendah atau dimatikan sepenuhnya.

Apabila imbasan yang dijadualkan telah dilancarkan dalam masa yang telah ditentukan, anda akan diberitahu mengenai fakta ini melalui tettingkap pop muncul pada [ikon dulang sistem AVG](#):



Kemudian, [ikon dulang sistem AVG](#) yang baru muncul (*dalam warna penuh dengan lampu suluh*) memberitahu imbasan yang dijadualkan sedang dijalankan. Klik kanan pada ikon AVG imbasan berjalan untuk membuka menu konteks di mana anda boleh membuat keputusan untuk menjeda atau malah menghentikan imbasan yang sedang berjalan, dan juga menukar prioriti imbasan yang sedang berjalan:





Pada tab **Cara untuk mengimbas** anda akan menemui senarai parameter pengimbasan yang boleh dihidupkan/dimatikan secara pilihan. Secara lalai, kebanyakan parameter dibuka dan kefungsiannya akan dilaksanakan semasa pengimbasan. Melainkan anda mempunyai alasan yang sah untuk mengubah tetapan ini, kami mengesyorkan untuk mengekalkan konfigurasi yang dipratetap ini:

- **Pulihkan/buang jangkitan secara automatik** (*dibuka secara lalai*):jika virus dikenal pasti sewaktu imbasan, ia boleh dipulihkan secara automatik jika terdapat cara mengatasinya. Jika fail yang dijangkiti tidak boleh dipulihkan secara automatik, objek yang dijangkiti akan dialih ke [Bilik Kebal Virus](#).
- **Laporkan Program Berpotensi Tidak Dikehendaki dan ancaman Perisian Pengintip** (*dibuka secara lalai*):tandaan untuk mengaktifkan enjin [AntiPerisian Pengintip](#) , dan imbas untuk perisian pengintip serta untuk virus. [Perisian pengintip mewakili kategori malware yang dipersoalkan, walaupun, ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat.](#) Kami mengesyorkan untuk mengekalkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.
- **Laporkan set dipertingkatkan bagi Program Berpotensi Tidak Dikehendaki**(*ditutup secara lalai*):tandaan untuk mengesan pakej yang diluaskan bagi [perisian pengintip](#): atur cara yang sangat ok dan tidak berbahaya apabila diperoleh dari pengilang secara terus,



tetapi, boleh disalahgunakan untuk tujuan berniat jahat selepas itu. Ini adalah langkah tambahan yang meningkatkan keselamatan komputer anda dengan lebih lagi, walau bagaimanapun, ia boleh menyekat atur cara sah dan oleh itu, dimatikan secara lalai.

- **Imbas untuk Kuki Penjejakan** (*ditutup secara lalai*): parameter ini bagi komponen [AntiPerisian Pengintip](#) mentakrifkan bahawa kuki harus dikesan sewaktu imbasan; *nkuki HTTP digunakan untuk mengesahkan, menjejaki dan mengekalkan maklumat tertentu mengenai pengguna seperti keutamaan tapak atau kandungan kart beli-belah elektroniknya*
- **Imbas dalam arkib** (*ditutup secara lalai*): parameter ini mentakrifkan imbasan harus memeriksa semua fail walaupun jika ia disimpan dalam arkib, cth. ZIP, RAR, ...
- **Gunakan Heuristik** (*dibuka secara lalai*): analisis heuristik (*perlagakan dinamik arahan objek yang diimbas dalam persekitaran komputer maya*) akan menjadi salah satu kaedah yang digunakan untuk pengesanan virus sewaktu imbasan;
- **Imbas persekitaran sistem** (*dibuka secara lalai*): imbasan juga akan memeriksa kawasan sistem komputer anda;
- **Dayakan pengimbasan teliti** (*ditutup secara lalai*) - dalam situasi khusus (*mengesyaki komputer anda dijangkiti*) anda boleh menandakan opsyen ini untuk mengaktifkan algoritma pengimbasan yang paling teliti yang akan turut mengimbas kawasan komputer anda yang sukar dijangkiti, sekadar untuk mendapatkan kepastian sepenuhnya. Jangan lupa bahawa kaedah ini agak mengambil masa.
- **Imbas untuk rootkit** (*ditutup secara lalai*): - tandakan item ini jika anda mahu memasukkan pengesanan rootkit ke dalam pengimbasan seluruh komputer. Pengesanan rootkit juga tersedia dengan sendiri dalam komponen [AntiRootkit](#);

Seterusnya, anda harus menentukan sama ada anda mahu mengimbas

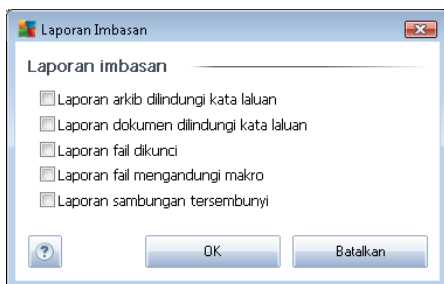
- **Semua jenis fail** dengan kemungkinan pengecualian yang ditakrifkan daripada imbasan dengan memberikan senarai yang pemanjangan fail yang dipisahkan oleh koma (*apabila disimpan, koma bertukar kepada koma bertitik*) yang tidak harus diimbas;
- **Jenis fail yang dipilih** - anda boleh menentukan bahawa anda hendak mengimbas hanya fail yang berkemungkinan dijangkiti (*fail yang tidak boleh dijangkiti tidak akan diimbas, contohnya sesetengah fail teks biasa atau sesetengah fail bukan boleh laku*), termasuk fail media (*video, fail audio - jika anda membiarkan kotak in tidak ditandakan, ia akan mengurangkan lebih banyak masa kerana fail ini biasanya agak besar dan agak tidak berkemungkinan dijangkiti virus*). Sekali lagi, anda boleh menentukan sambungan fail mana yang sepatutnya sentiasa diimbas.
- Secara pilihan, anda boleh menentukan anda hendak **Mengimbas fail tanpa sambungan** - opsyen ini dihidupkan secara lalai dan ia disyorkan untuk anda mengekalkannya melainkan anda mempunyai sebab sebenar untuk mengubahnya. Fail tanpa sambungan adalah lebih mencurigakan dan sepatutnya diimbas setiap masa.

Laraskan berapa cepat Imbasan selesai

Dalam bahagian **Laraskan berapa cepat Imbasan selesai** anda boleh menentukan selanjutnya kelajuan pengimbasan yang dikehendaki bergantung kepada penggunaan sumber sistem. Secara lalai, nilai opsyen ini ditetapkan kepada tahap *sensitif pengguna* bagi penggunaan sumber automatik. Jika anda mahu pengimbasan dijalankan dengan lebih cepat, ia akan mengambil masa yang kurang tetapi penggunaan sumber sistem akan meningkat secara signifikan sewaktu imbasan dan akan melambatkan aktiviti anda yang lain pada PC (*opsyen ini boleh digunakan semasa komputer anda dihidupkan tetapi tiada siapa yang sedang bekerja dengannya*). Sebaliknya, anda boleh mengurangkan penggunaan sumber sistem dengan menambah tempoh pengimbasan.

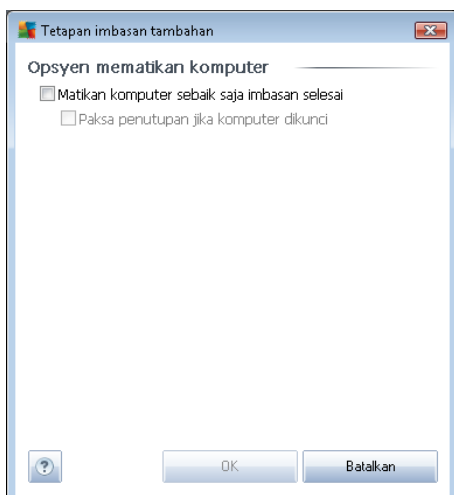
Tetapkan laporan imbasan tambahan

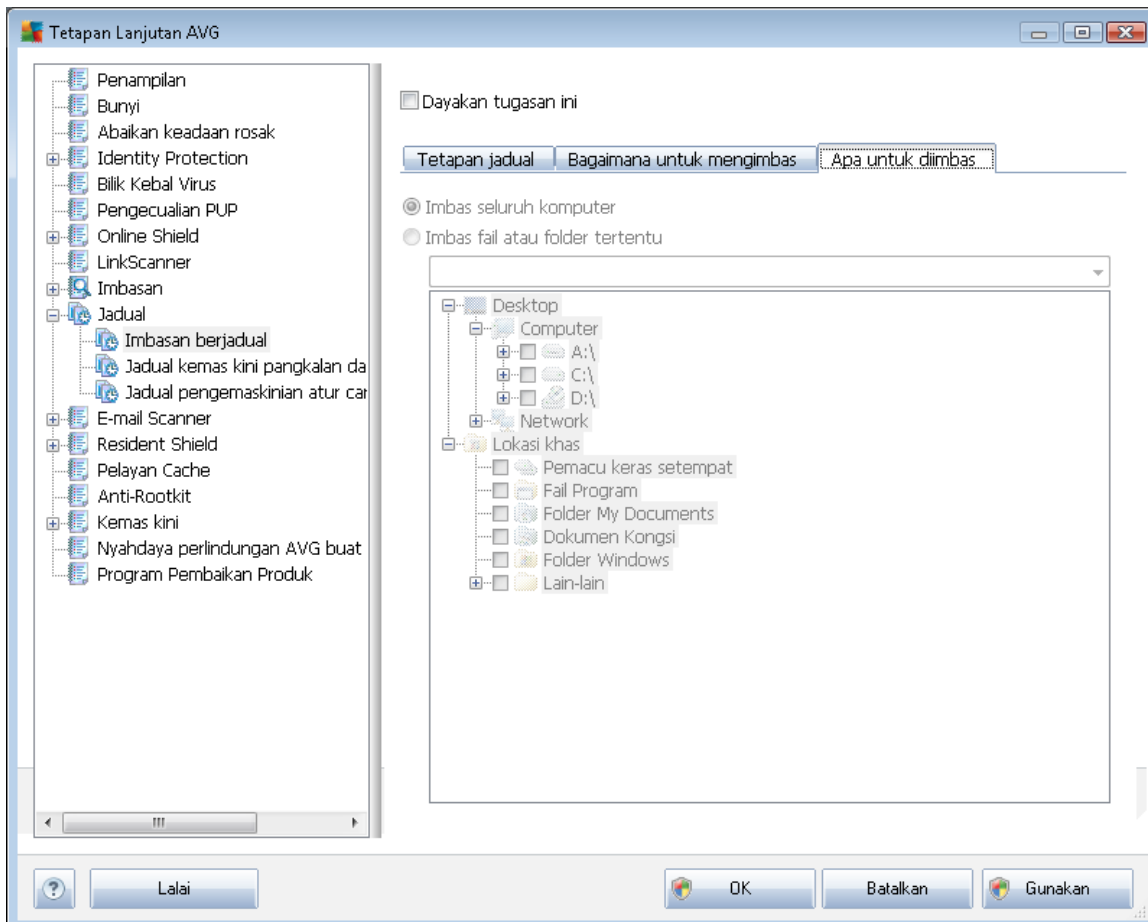
Klik pautan **Tetapkan laporan imbasan tambahan ...** untuk membuka tettingkap dialog tersendiri yang dipanggil **Laporan imbasan** di mana anda boleh menanda rait beberapa item untuk mentakrifkan penemuan imbasan yang harus dilaporkan:



Tetapan imbasan tambahan

Klik **Tetapan imbasan tambahan ...** untuk membuka dialog **Opsyen mematikan komputer** lain di mana anda boleh menentukan sama ada komputer harus dimatikan secara automatik sebaik sahaja proses pengimbasan yang berjalan tamat. Dengan mengesahkan opsyen ini (**Matikan komputer apabila imbasan selesai**), pengaktifan opsyen baru membenarkan komputer dimatikan walaupun jika ia sedang dikunci (**Paksa untuk dimatikan jika komputer dikunci**).

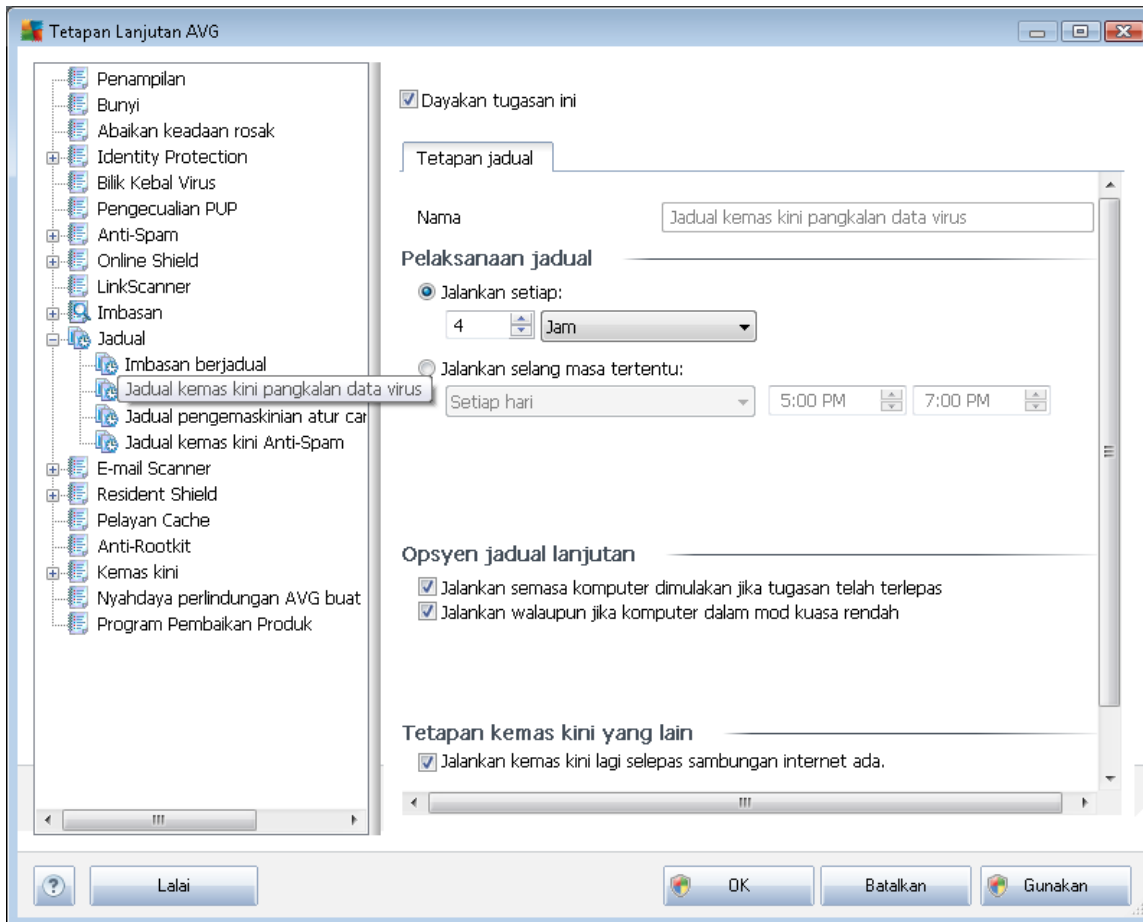




Pada tab ***Apa yang hendak diimbas*** anda boleh menentukan sama ada anda mahu menjadualkan [pengimbasan seluruh komputer](#) atau [pengimbasan fail atau folder tertentu](#). Jika anda memilih pengimbasan fail atau folder tertentu, dalam bahagian bawah dialog ini, struktur pepohonan yang dipaparkan diaktifkan dan anda boleh menentukan folder untuk diimbas.

9.9.2. Jadual Kemas Kini Pangkalan Data Virus

Jika ***benar-benar perlu***, anda boleh tidak menanda item ***Dayakan tugas ini*** untuk menyahaktifkan kemas kini pangkalan data virus yang dijadualkan buat sementara waktu, dan menghidupkannya semula pada waktu lain:



Penjadualan kemas kini pangkalan data virus asas diliputi dalam komponen [Pengurus Kemas Kini](#). Dalam dialog ini, anda boleh menyediakan beberapa parameter terperinci bagi jadual kemas kini pangkalan data virus. Dalam medan teks yang dipanggil **Nama** (*nyahaktifkan semua jadual lalai*) terdapat nama yang diperuntukkan kepada jadual ini oleh vendor atur cara.

Pelaksanaan jadual

Dalam bahagian ini, tentukan jarak waktu untuk pelancaran kemas kini pangkalan data virus yang baru dijadualkan. Pemasaan boleh sama ada, ditakrifkan oleh pelancaran kemas kini berulang selepas satu tempoh tertentu bagi masa (**Jalankan setiap ...**) atau dengan menentukan tarikh dan masa sebenar (**Jalankan pada waktu tertentu ...**).

Opsyen jadual lanjutan

Bahagian ini membenarkan anda mentakrifkan di bawah keadaan mana kemas kini pangkalan data virus harus/tidak harus dilancarkan jika komputer berada dalam mod kuasa rendah atau dimatikan sepenuhnya.



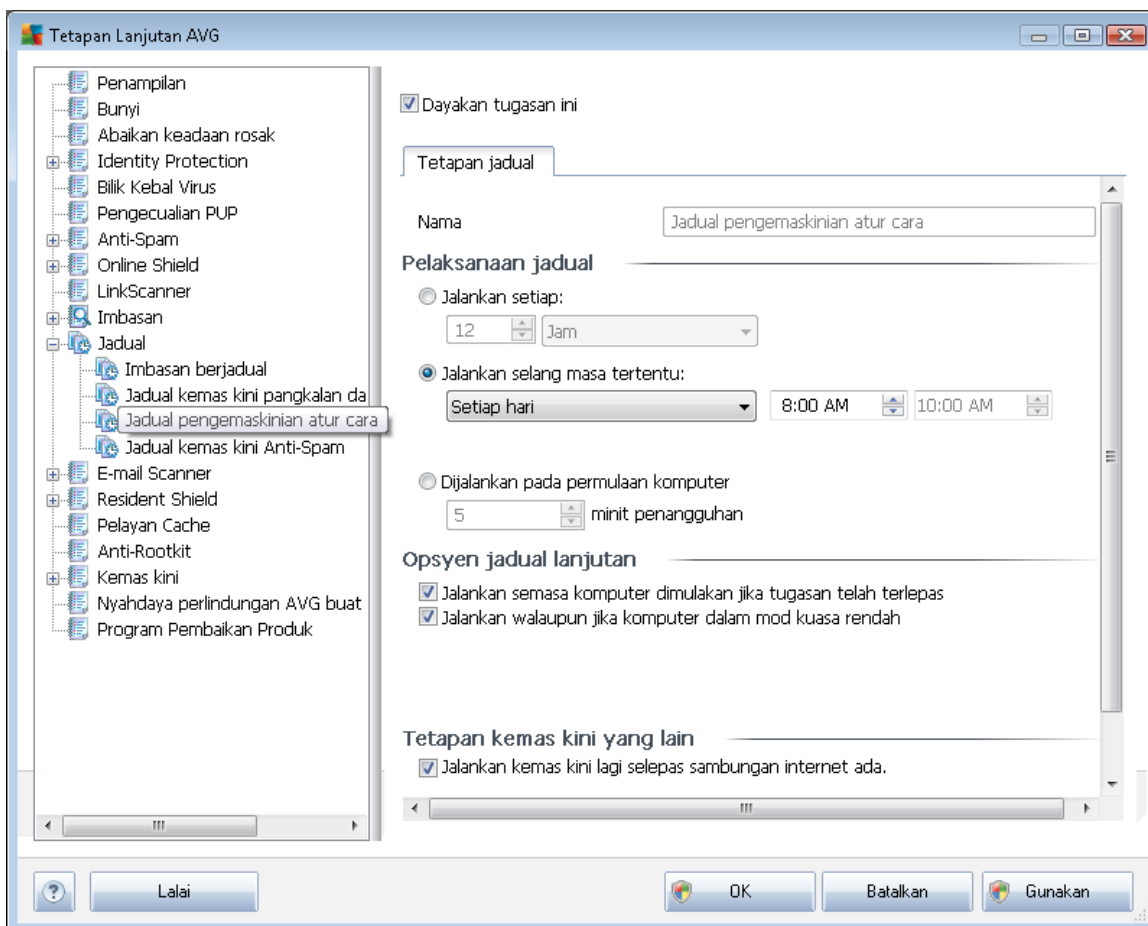
Tetapan kemas kini yang lain

Akhir sekali, tandakan opsyen **Jalankan sebaik sahaja sambungan Internet tersedia** untuk memastikan jika sambungan internet rosak dan proses kemas kini gagal, ia akan dilancarkan semula dengan serta-merta selepas sambungan internet disimpan semula.

Sebaik sahaja kemas kini yang dijadualkan dilancarkan tepat pada masa anda telah tentukan, anda akan diberitahu mengenai fakta ini melalui tettingkap pop timbul yang terbuka pada [ikon dulang sistem AVG](#) (diberikan bahawa anda telah menyimpan konfigurasi lalai bagi dialog [Tetapan/Rupa Lanjutan](#)).

9.9.3. Jadual Kemas Kini Atur Cara

Jika **benar-benar perlu**, anda boleh tidak menanda item **Dayakan tugas ini** untuk menyahaktifkan kemas kini atur cara buat sementara waktu, dan menghidupkannya semula pada waktu lain:



Dalam medan teks yang dipanggil **Nama** (nyahaktifkan semua jadual lalai) terdapat nama yang diperuntukkan kepada jadual ini oleh vendor atur cara.



Pelaksanaan jadual

Di sini, tentukan jarak waktu untuk kemas kini atur cara yang baru dilancarkan. Masa boleh sama ada ditentukan oleh pelancaran kemas kini berulang selepas tempoh masa tertentu (***Jalankan setiap ...***) atau dengan menentukan tarikh dan masa sebenar (***Jalankan dalam masa tertentu ...***), atau kemungkinan dengan menentukan acara yang pelancaran kemas kini harus dikaitkan dengan (***Tindakan berdasarkan pada permulaan komputer***).

Opsyen jadual lanjutan

Bahagian ini membenarkan anda menentukan dalam keadaan apa kemas kini atur cara harus/tidak harus dilancarkan jika komputer berada dalam mod kuasa rendah atau dimatikan sepenuhnya.

Tetapan kemas kini yang lain

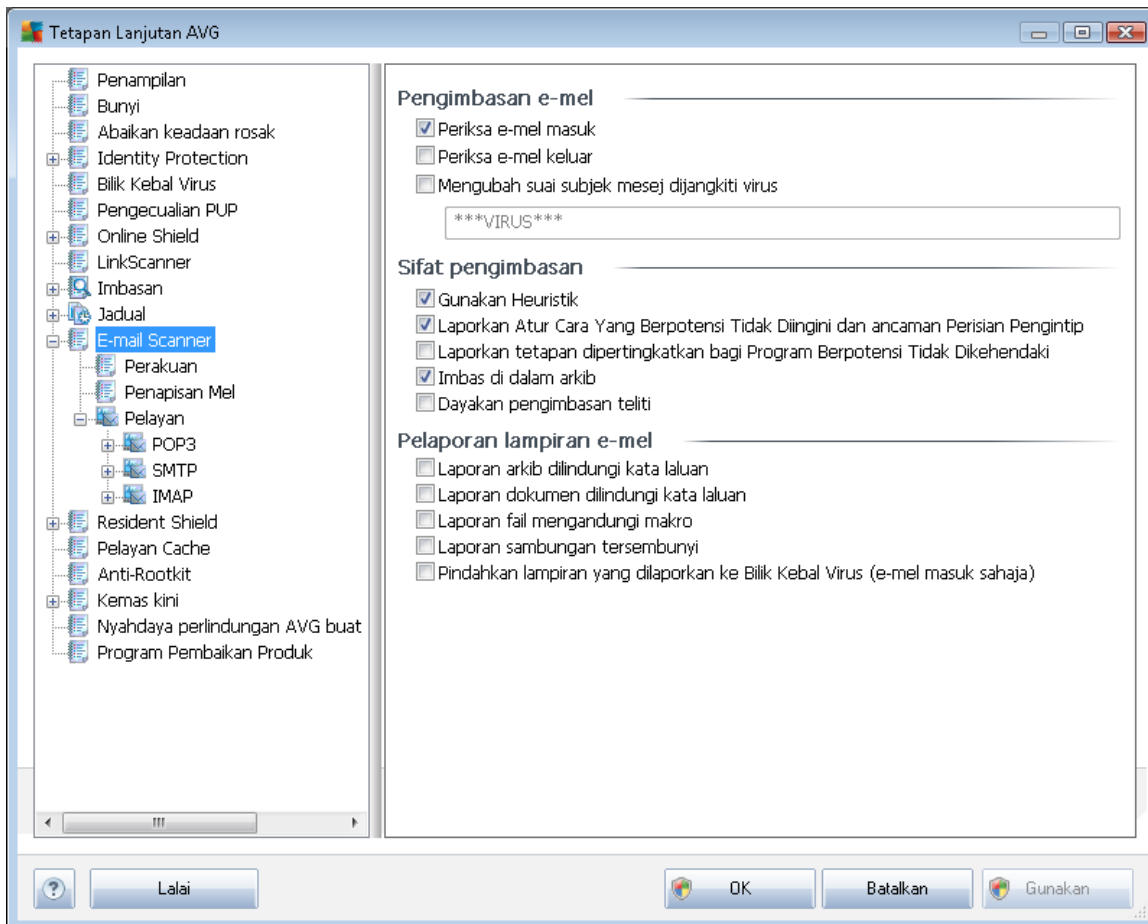
Tandakan opsyen ***Jalankan kemas kini semula sebaik sahaja sambungan Internet tersedia*** untuk memastikan jika sambungan internet rosak dan proses kemas kini gagal, ia akan dilancarkan semula dengan serta-merta selepas sambungan internet disimpan semula.

Sebaik sahaja kemas kini yang dijadualkan dilancarkan tepat pada masa anda telah tentukan, anda akan diberitahu mengenai fakta ini melalui tettingkap pop timbul yang terbuka pada [ikon dulang sistem AVG](#) (diberikan bahawa anda telah menyimpan konfigurasi lalai bagi dialog [Tetapan/Rupa Lanjutan](#)).

Perhatian: Jika persamaan masa bagi kemas kini atur cara yang dijadualkan dan imbasan yang dijadualkan berlaku, proses kemas kini adalah lebih utama dan imbasan akan diganggu.

9.10. Pengimbas E-mel

Dialog *Pengimbas E-mel* dibahagikan ke dalam tiga bahagian:



Pengimbasan e-mel

Dalam bahagian ini, anda boleh menetapkan asas ini untuk mesej e-mel masuk dan/atau keluar:

- **Semak e-mel masuk** (*buka secara lalai*) - tanda untuk buka/tutup opsiyen bagi mengimbas semua mesej e-mel yang dihantar ke klien e-mel anda
- **Semak e-mel keluar** (*tutup secara lalai*) - tanda untuk buka/tutup opsiyen bagi mengimbas semua mesej e-mel yang dihantar dari klien e-mel anda
- **Ubah suai subjek mesej dijangkiti virus** (*tutup secara lalai*) - jika anda ingin diberi amaran mesej e-mel yang diimbas dikesan sebagai boleh berjangkit, tandakan item ini dan isikan teks yang diinginkan ke dalam medan teks. Teks ini kemudiannya akan ditambahkan ke medan "Subjek" setiap mesej e-mel yang dikesan untuk pengenalan dan penapisan yang lebih mudah. Nilai lalai ialah *****VIRUS***** yang kami syorkan untuk disimpan.



Sifat pengimbasan

Dalam bahagian ini, anda boleh menentukan cara mesej e-mel akan diimbas:

- **Gunakan Heuristik buka secara lalai** – tandakan untuk menggunakan [kaedah pengesanan heuristik](#) semasa mengimbas mesej e-mel. Apabila opsyen ini hidup, anda boleh menapis lampiran e-mel bukan sahaja dengan sambungan tetapi juga kandungan sebenar lampiran boleh dipertimbangkan. Penapisan boleh ditetapkan dalam dialog [Penapisan Mel](#).
- **Laporkan Program Berpotensi Tidak Dikehendaki dan ancaman Perisian Pengintip (dibuka secara lalai)** - tandakan untuk mengaktifkan enjin [AntiPerisian Pengintip](#), dan imbas untuk perisian pengintip serta untuk virus. [Perisian pengintip mewakili kategori malware yang dipersoalkan, walaupun, ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat.](#) Kami mengesyorkan untuk mengekalkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.
- **Laporkan set dipertingkatkan bagi Atur Cara yang Berpotensi Tidak Diingini tutup secara lalai**– tandakan untuk mengesan pakej yang diluaskan bagi [perisian pengintip](#): atur cara yang sangat ok dan tidak berbahaya apabila diperoleh dari pengilang secara terus, tetapi, boleh disalahgunakan untuk tujuan berniat jahat selepas itu. Ini adalah langkah tambahan yang meningkatkan keselamatan komputer anda dengan lebih lagi, walau bagaimanapun, ia boleh menyekat atur cara sah dan oleh itu, dimatikan secara lalai.
- **Imbas dalam arkib buka secara lalai** – tandakan untuk mengimbas kandungan arkib yang dilampirkan kepada mesej e-mel.
- **Dayakan pengimbasan menyeluruh (tutup secara lalai)** - dalam situasi khusus (*cth. syak komputer anda dijangkiti oleh virus atau eksploitasi*) anda boleh menandakan opsyen ini untuk mengaktifkan algoritma pengimbasan menyeluruh yang akan turut mengimbas kawasan komputer anda yang sukar untuk dijangkiti, sekadar untuk mendapatkan kepastian sepenuhnya. Namun ingat bahawa kaedah ini agak mengambil masa.

Pelaporan lampiran e-mel

Dalam seksyen ini, anda boleh menetapkan laporan tambahan mengenai fail yang berpotensi berbahaya atau mencurigakan. Sila maklum bahawa tiada dialog amaran yang akan dipaparkan, hanya teks perakuan akan ditambah ke penghujung mesej e-mel, dan semua laporan seumpamanya akan disenaraikan dalam dialog [pengesanan Pengimbas E-mel](#):

- **Laporkan arkib yang dilindungi kata laluan** - arkib (*JZIP, RAR dll.*) yang dilindungi oleh kata laluan adalah tidak mungkin diimbas untuk virus; tandakan kotak untuk melaporkan ini sebagai berpotensi berbahaya.
- **Laporkan dokumen yang dilindungi kata laluan** – dokumen dilindungi kata laluan tidak mungkin diimbas untuk virus; tandakan kotak untuk melaporkannya sebagai berpotensi berbahaya.
- **Laporkan fail mengandungi makro** – makro adalah urutan langkah yang dipratakrifkan untuk menjadikan tugas tertentu lebih mudah untuk pengguna (*makro MS Word dikenali*

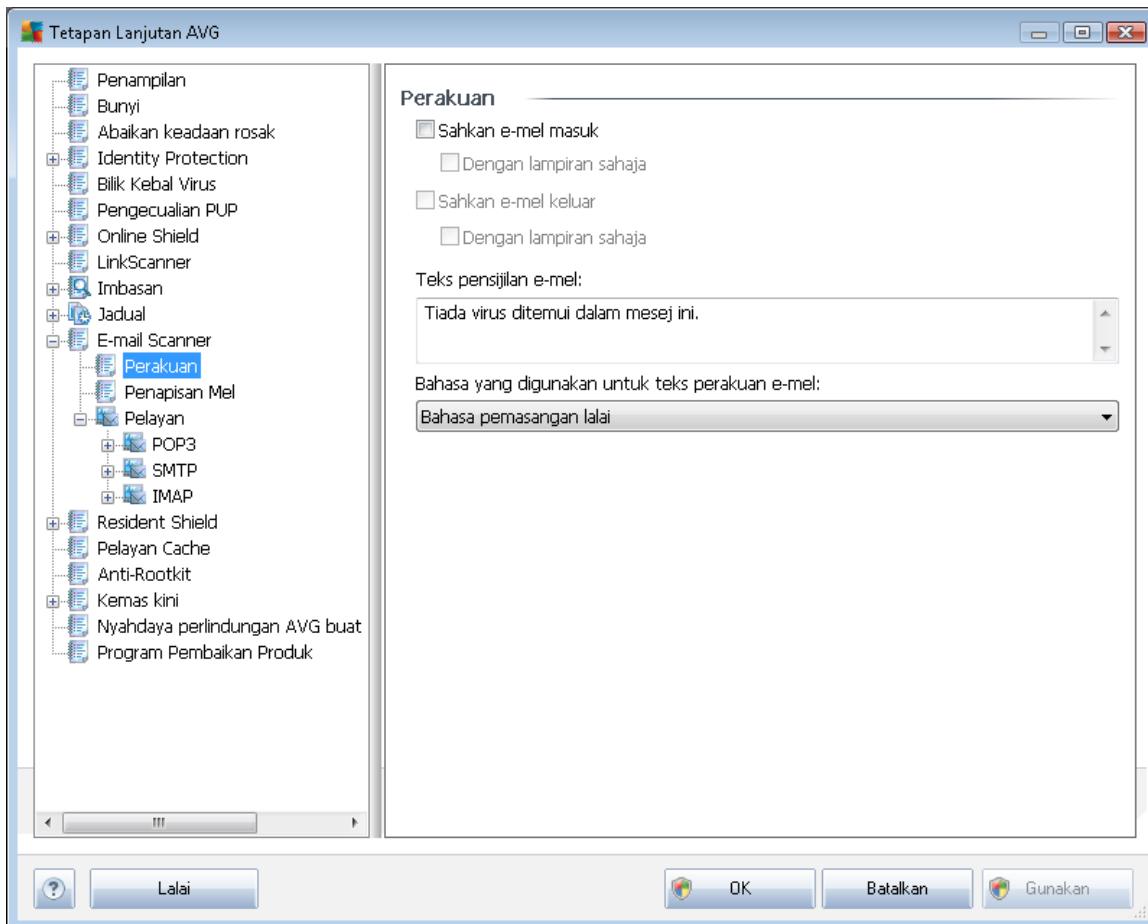


rama). Dengan itu, makro boleh mengandungi arahan berpotensi berbahaya, dan anda mungkin ingin menandakan kotak untuk memastikan fail dengan makro akan dilaporkan sebagai mencurigakan.

- **Laporkan sambungan tersembunyi** - sambungan tersembunyi boleh menjadikan cthnya. fail boleh laku mencurigakan "sesuatu.txt.exe" kelihatan seperti fail teks biasa yang tidak berbahaya "sesuatu.txt"; tandakan kotak untuk melaporkan ini sebagai berpotensi berbahaya.
- **Alihkan lampiran yang dilaporkan ke Bilik Kebal Virus** - tentukan sama ada anda hendak diberitahu melalui e-mel mengenai arkib yang dilindungi kata laluan, dokumen yang dilindungi kata laluan, makro mengandungi fail dan/atau fail dengan sambungan tersembunyi dikesan sebagai lampiran bagi mesej e-mel yang diimbis. Jika mesej seperti itu dikenal pasti sewaktu pengimbasan, tentukan sama ada objek berjangkit yang dikesan harus dialih ke [Bilik Kebal Virus](#).

9.10.1. Perakuan

Dalam dialog **Perakuan** anda boleh menetapkan teks dan bahasa perakuan bagi kedua-dua mel masuk dan mel keluar:



Teks perakuan ini terdiri daripada dua bahagian, bahagian pengguna dan bahagian sistem - lihat



contoh berikut: baris pertama mewakili bahagian pengguna, yang lain dijana secara automatik:

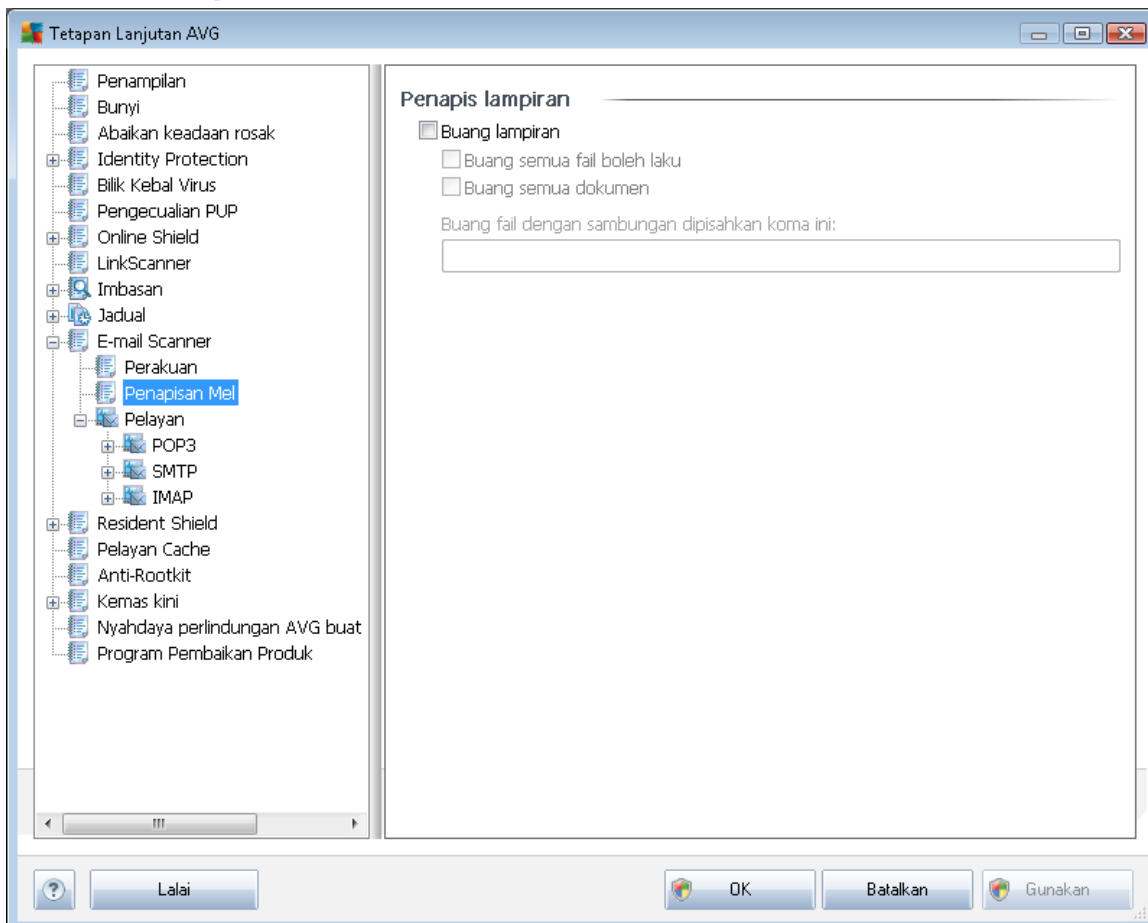
Tiada virus ditemui dalam mesej ini.

Diperiksa oleh AVG.

Versi: x.y.zz / Pangkalan Data Virus: xx.y.z - Tarikh Keluaran: 12/9/2010

Jika anda membuat keputusan untuk menggunakan perakuan bagi sama ada mesej e-mel masuk atau keluar, di dalam dialog ini anda boleh menetapkan perkataan sebenar bagi bahagian pengguna teks perakuan (**Teks perakuan e-mel**), dan memilih bahasa yang mana perlu digunakan untuk bahagian sistem perakuan yang dijana secara automatik (**Bahasa yang digunakan bagi teks perakuan e-mel**).

9.10.2. Penapisan Mel

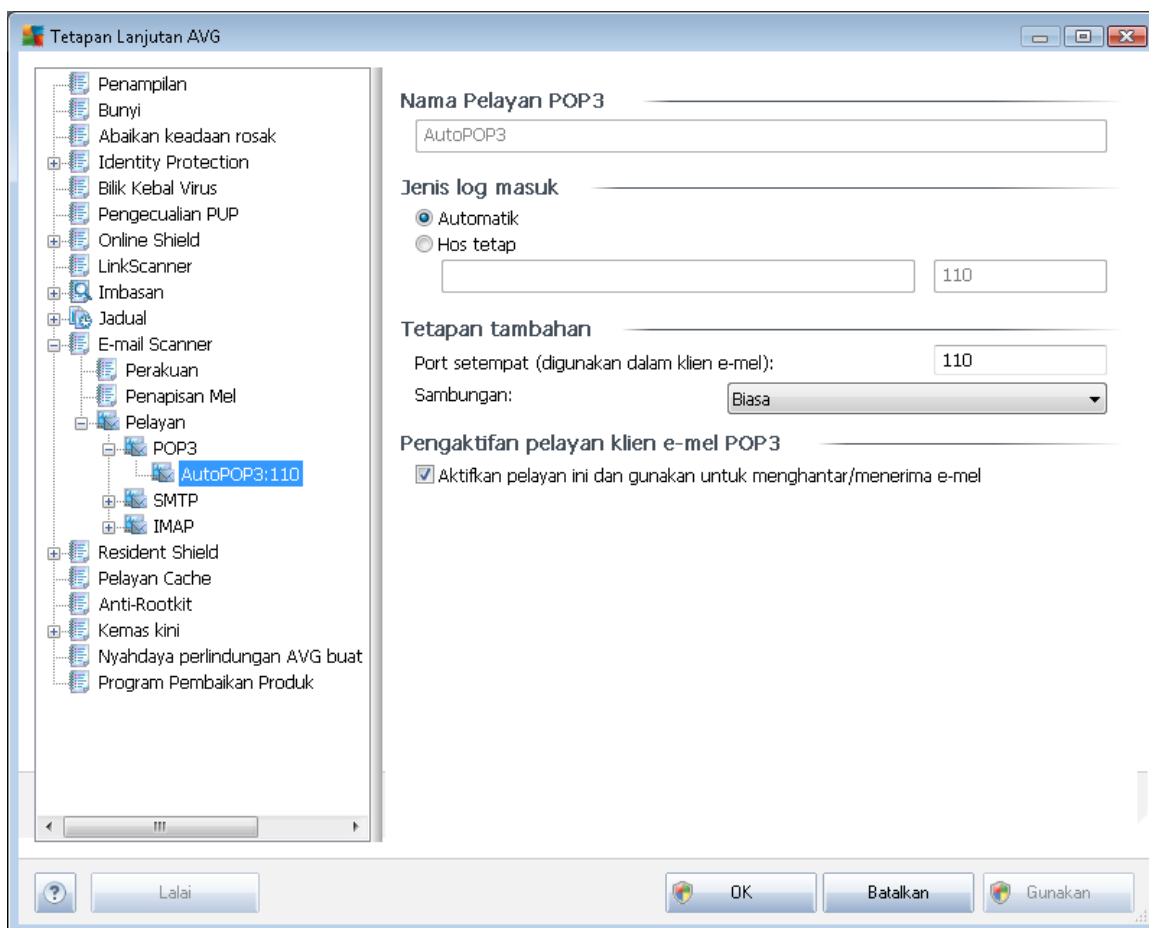


Dialog **Penapis lampiran** membenarkan anda menyediakan parameter untuk pengimbasan lampiran mesej e-mel. Secara lalai, opsiyen **Buang lampiran** dimatikan. Jika anda memutuskan untuk mengaktifkannya, semua lampiran mesej e-mel yang dikesan sebagai berjangkit atau berpotensi berbahaya akan dibuang secara automatik. Jika anda mahu menentukan jenis lampiran khusus yang harus dibuang, pilih opsiyen berikut:

- **Buang semua fail boleh laku** - semua fail *.exe akan dipadamkan
- **Buang semua dokumen** - semua fail *.doc, *.docx, *.xls, *.xlsx akan dipadam
- **Buang fail dengan sambungan yang dipisahkan oleh koma** - akan membuang semua fail dengan sambungan yang ditentukan

9.10.3. Pelayan

Dalam bahagian **Pelayan** anda boleh mengedit parameter bagi pelayan komponen [Pengimbas E-mel](#), atau menyediakan pelayan baru menggunakan butang **Tambah pelayan baru**.

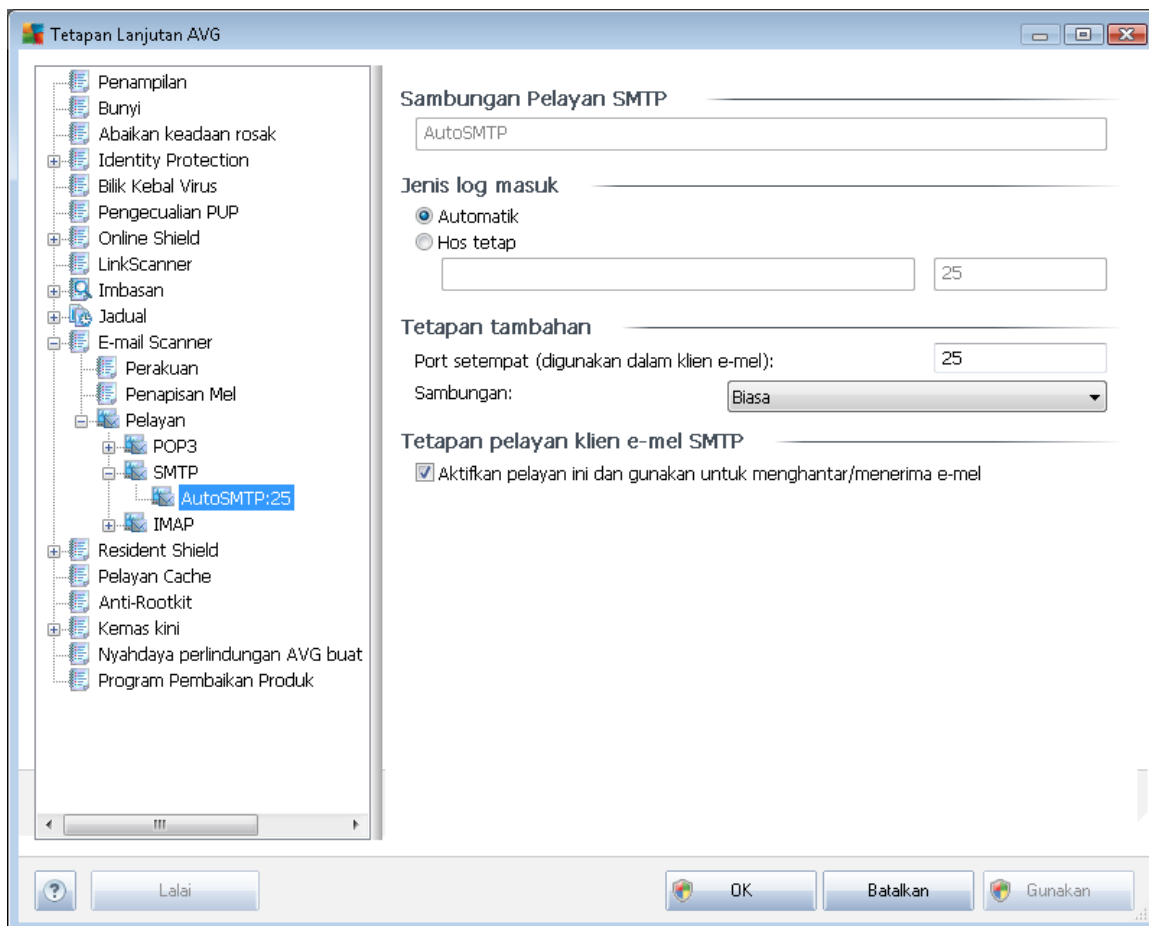


Dalam dialog ini (*dibuka melalui Pelayan / POP3*) anda boleh menyediakan pelayan [Pengimbas E-mel](#) baru menggunakan protokol POP3 untuk mel masuk:

- **Nama Pelayan POP3** - dalam medan ini anda boleh menentukan nama pelayan yang baru ditambah (*untuk menambah pelayan POP3, klik butang tetikus kanan di atas item POP3 di sebelah kiri menu navigasi*). Bagi pelayan "AutoPOP3" yang dibuat secara automatik medan ini dinyahaktifkan.



- **Jenis log masuk** - menentukan kaedah untuk menentukan pelayan mel yang digunakan untuk mel masuk:
 - **Automatik** – Log masuk akan dijalankan secara automatik, mengikut tetapan klien e-mel anda.
 - **Hos tetap** – Dalam kes ini, atur cara akan sentiasa menggunakan pelayan yang dinyatakan di sini. Sila nyatakan alamat atau nama pelayan mel anda. Nama log masuk kekal tidak berubah. Untuk nama, anda boleh menggunakan nama domain (*contohnya, pop.acme.com*) dan juga alamat IP *contohnya, 123.45.67.89*). Jika pelayan mel menggunakan port bukan standard, anda boleh menentukan port ini selepas nama pelayan menggunakan tanda titik bertindih sebagai penentu had (*contohnya, pop.acme.com:8200*). Port standard untuk komunikasi POP3 ialah 110.
- **Tetapan tambahan** - menentukan parameter yang lebih terperinci:
 - **Port tempatan** - menentukan port di mana komunikasi dari aplikasi mel anda harus dijangka. Anda kemudiannya mesti menentukan dalam aplikasi mel anda port ini sebagai port untuk komunikasi POP3.
 - **Sambungan** - dalam menu jatuh bawah, anda boleh menentukan jenis sambungan apa untuk digunakan (*biasa/SSL/SSL lalai*). Jika anda memilih sambungan SSL, data yang dihantar disulitkan tanpa risiko dijejaki atau diselia oleh pihak ketiga. Ciri ini juga tersedia hanya apabila pelayan mel destinasi menyokongnya.
- **Pengaktifan pelayan POP3 klien e-mel** - tanda/buang tanda item ini untuk mengaktifkan atau menyahaktifkan pelayan POP3 yang ditentukan

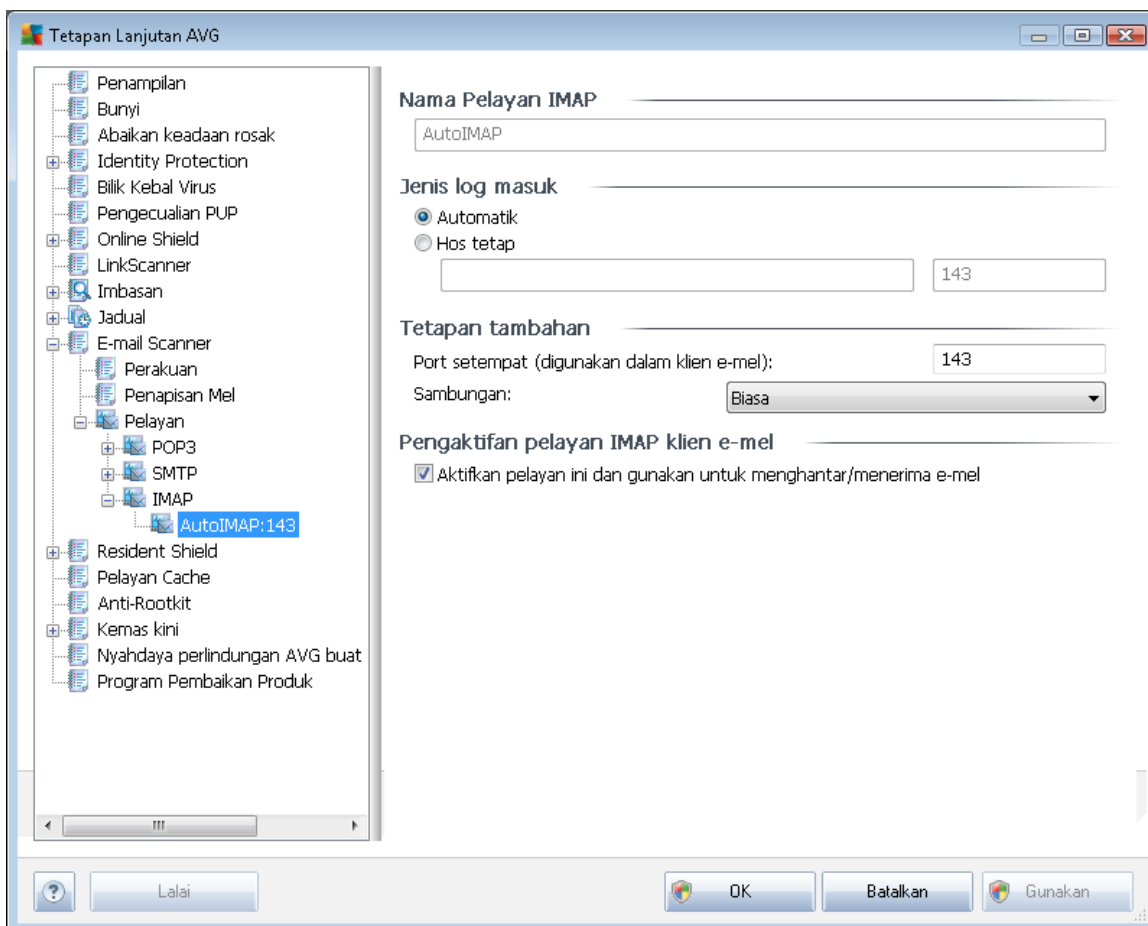


Dalam dialog ini (*dibuka melalui **Pelayan / SMTP***) anda boleh menyediakan pelayan [Pengimbas E-mel](#) baru menggunakan protokol SMTP untuk mel keluar:

- **Nama Pelayan SMTP** - dalam medan ini anda boleh menentukan nama pelayan yang baru ditambah (*untuk menambah pelayan SMTP, klik butang tetikus kanan di atas item SMTP di sebelah kiri menu navigasi*). Untuk pelayan "AutoSMTP" yang dibuat secara automatik medan ini dinyahaktifkan.
- **Jenis log masuk** - mentakrifkan kaedah untuk menentukan pelayan mel yang digunakan untuk mel keluar:
 - **Automatik** - log masuk akan dijalankan secara automatik mengikut tetapan klien e-mel anda
 - **Hos tetap** - dalam kes ini, atur cara akan sentiasa menggunakan pelayar yang ditentukan di sini. Sila nyatakan alamat atau nama pelayan mel anda. Anda boleh menggunakan nama domain (sebagai contoh, smtp.acme.com) dan juga alamat IP (*sebagai contoh, 123.45.67.89*) sebagai nama. Jika pelayan mel menggunakan port tidak standard, anda boleh menaip port ini di belakang nama pelayan menggunakan noktah bertindih sebagai penentu hadnya (*sebagai contoh, smtp.acme.com:8200*).

Port standard untuk komunikasi SMTP ialah 25.

- **Tetapan tambahan** - menentukan parameter yang lebih terperinci:
 - **Port tempatan** - menentukan port di mana komunikasi dari aplikasi mel anda harus dijangka. Kemudian, anda mesti menentukan port ini sebagai port untuk komunikasi SMTP dalam aplikasi mel anda.
 - **Sambungan** - dalam menu jatuh ke bawah ini, anda boleh menentukan jenis sambungan mana untuk digunakan (*biasa/SSL/SSL lalai*). Jika anda memilih sambungan SSL, data yang dihantar disulitkan tanpa risiko dijejaki atau diselia oleh pihak ketiga. Ciri ini tersedia hanya apabila pelayan mel destinasi menyokongnya.
- **Pengaktifan pelayan SMTP klien e-mel** - tandakan/jangan tandakan kotak ini untuk mengaktifkan/menyahaktifkan pelayan SMTP yang ditentukan di atas



Dalam dialog ini (dibuka melalui **Pelayan / IMAP**) anda boleh menetapkan pelayan **Pengimbas E-mel** menggunakan protokol IMAP untuk mel keluar:

- **Nama Pelayan IMAP** - dalam medan ini anda boleh menentukan nama pelayan yang baru ditambah (*untuk menambah pelayan IMAP, klik butang tetikus kanan di atas item IMAP*)

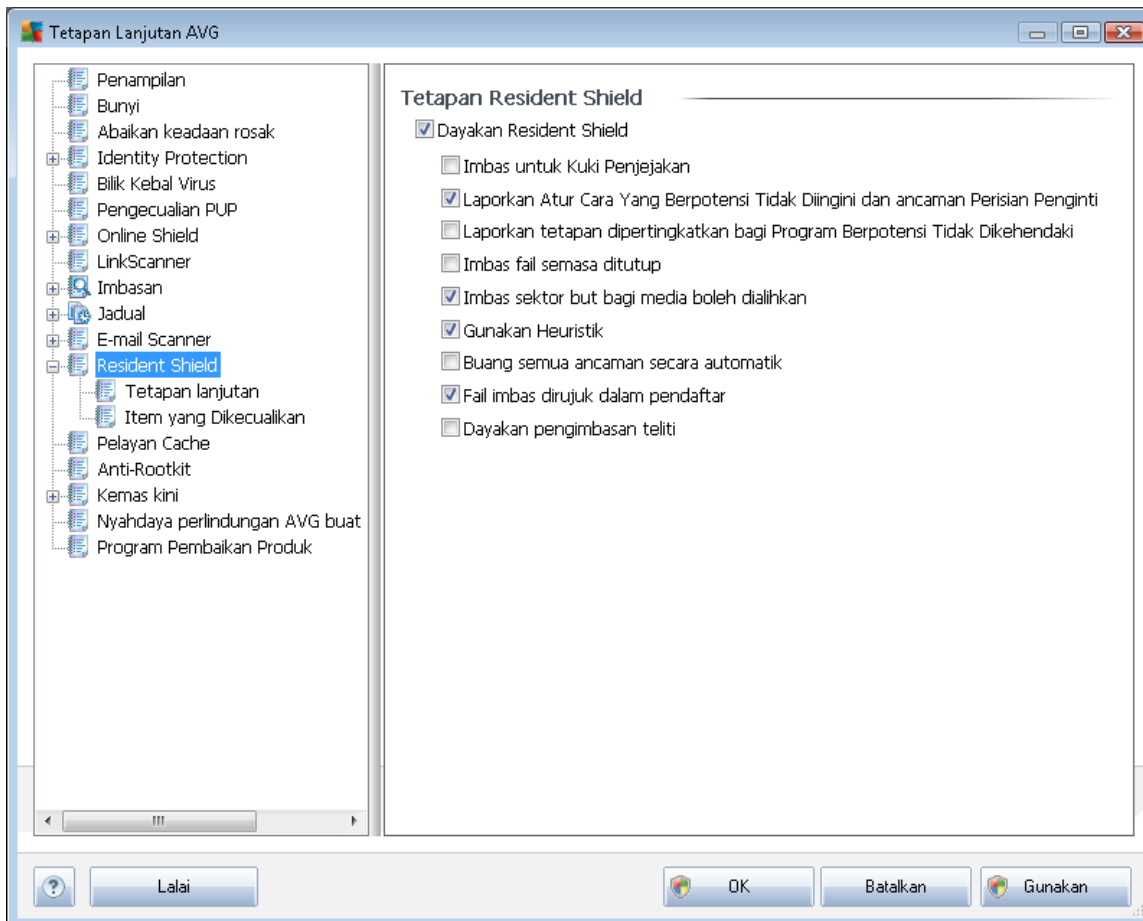


bagi menu navigasi kiri). Bagi pelayan "AutoIMAP" yang dibuat secara automatik medan ini dinyahaktifkan.

- **Jenis log masuk** - mentakrifkan kaedah untuk menentukan pelayan mel yang digunakan untuk mel keluar:
 - **Automatik** - log masuk akan dijalankan secara automatik mengikut tetapan klien e-mel anda
 - **Hos tetap** - dalam kes ini, atur cara akan sentiasa menggunakan pelayar yang ditentukan di sini. Sila nyatakan alamat atau nama pelayan mel anda. Anda boleh menggunakan nama domain (*sebagai contoh, smtp.acme.com*) dan juga alamat IP (*sebagai contoh, 123.45.67.89*) sebagai nama. Jika pelayan mel menggunakan port tidak standard, anda boleh menaip port ini di belakang nama pelayan menggunakan noktah bertindih sebagai pengehad (*sebagai contoh, imap.acme.com:8200*). Port standard untuk komunikasi IMAP ialah 143.
- **Tetapan tambahan** - menentukan parameter yang lebih terperinci:
 - **Port tempatan** - menentukan port di mana komunikasi dari aplikasi mel anda harus dijangka. Anda kemudiannya mesti menentukan dalam aplikasi mel anda port ini sebagai port untuk IMAP.
 - **Sambungan** - dalam menu jatuh ke bawah ini, anda boleh menentukan jenis sambungan mana untuk digunakan (*biasa/SSL/SSL lalai*). Jika anda memilih sambungan SSL, data yang dihantar disulitkan tanpa risiko dijejaki atau diselia oleh pihak ketiga. Ciri ini tersedia hanya apabila pelayan mel destinasi menyokongnya.
- **Pengaktifan pelayan IMAP klien e-mel** - tandakan/jangan tandakan kotak ini untuk mengaktifkan/menyahaktifkan pelayan IMAP yang ditentukan di atas

9.1.1. Perisai Residen

Komponen [Perisai Residen](#) memberikan perlindungan langsung bagi fail dan folder daripada virus, perisian pengintip dan malware lain.



Dalam dialog **Tetapan Perisai Residen** anda boleh mengaktifkan atau menyahaktifkan perlindungan [Perisai Residen](#) sepenuhnya dengan menanda/menyahtanda item **Dayakan Perisai Residen** (*opsyen ini dihidupkan secara lalai*). Selain daripada itu, anda boleh memilih ciri [Perisai Residen](#) harus diaktifkan:

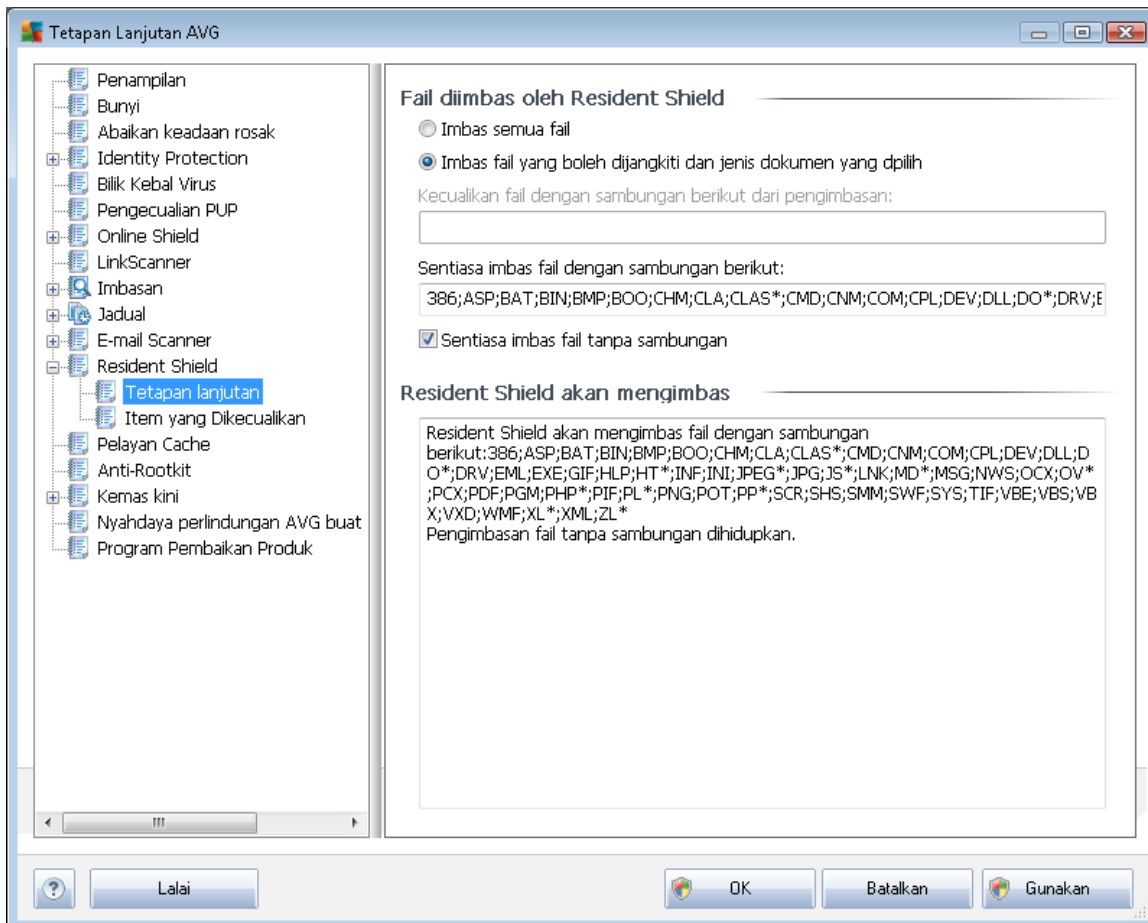
- **Imbas untuk Kuki penjejakan** (*ditutup secara lalai*) - parameter ini menentukan bahawa kuki harus dikesan sewaktu pengimbasan. (*Kuki HTTP digunakan untuk mengesahkan, menjejaki dan mengekalkan maklumat tertentu mengenai pengguna seperti keutamaan tapak atau kandungan kart beli-belah elektronik*)
- **Laporkan Atur Cara yang Berpotensi Tidak Diingini dan ancaman Perisian Pengintip** - (*dihidupkan secara lalai*): tandakan untuk mengaktifkan enjin [AntiPerisian Pengintip](#), dan imbas untuk perisian pengintip serta untuk virus. [Perisian pengintip mewakili kategori malware yang dipersoalkan, walaupun, ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat.](#) Kami mengesyorkan untuk mengekalkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.



- **Laporkan set dipertingkatkan bagi Program Berpotensi Tidak Dikehendaki** (*ditutup secara lalai*) - tandakan untuk mengesan pakej yang diluaskan bagi [perisian pengintip](#): atur cara yang sangat sesuai dan tidak berbahaya apabila diperoleh dari pengilang secara terus, tetapi, boleh disalahgunakan untuk tujuan berniat jahat selepas itu. Ini adalah ukuran tambahan yang meningkatkan keselamatan komputer anda dengan lebih lagi, walau bagaimanapun, ia boleh menyekat atur cara sah dan oleh itu, dimatikan secara lalai.
- **Imbas fail semasa tutup** (*ditutup secara lalai*) - pengimbasan semasa tutup memastikan AVG mengimbas objek aktif (cth. aplikasi, dokumen ...) semasa ia dibuka dan juga semasa ia ditutup; ciri ini membantu anda melindungi komputer anda daripada beberapa jenis virus sofistikated
- **Imbas sektor but bagi media boleh ditanggalkan** (*dibuka secara lalai*)
- **Gunakan Heuristik** - (*dibuka secara lalai*) [analisis heuristik](#) akan digunakan untuk pengesanan (*perlagakan dinamik arahan objek yang diimbas dalam persekitaran komputer maya*)
- **Keluarkan semua ancaman secara automatik** (*dimatikan secara lalai*) - sebarang jangkitan yang dikesan akan dirawat secara automatik jika terdapat cara menyembuhkannya, dan semua jangkitan yang tidak boleh diperbaiki akan dialih keluar.
- **Imbas fail yang dirujuk dalam pendaftar** (*dibuka secara lalai*) - parameter ini mentakrifkan bahawa AVG akan mengimbas semua fail boleh laku yang ditambah ke pendaftar permulaan untuk mengelakkan jangkitan yang diketahui dilakukan pada permulaan komputer yang seterusnya.
- **Dayakan pengimbasan teliti** (*ditutup secara lalai*) - dalam situasi khusus (*dalam keadaan kecemasan ekstrem*) anda boleh menandakan opsi ini untuk mengaktifkan algoritma yang paling teliti yang akan memeriksa semua objek yang berkemungkinan mengancam di bahagian dalam. Namun jangan lupa bahawa kaedah ini agak mengambil masa.

9.11.1. Tetap Lanjut

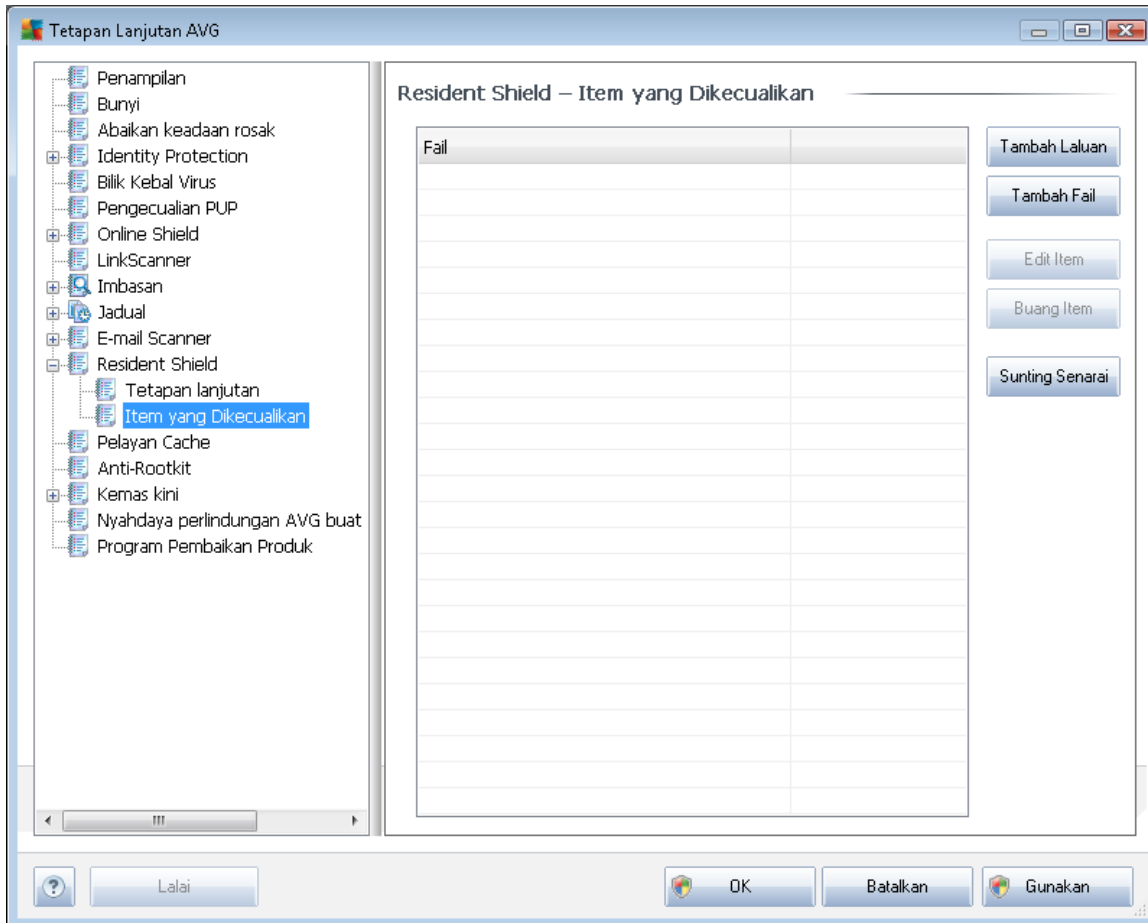
Dalam dialog **Fail yang diimbas oleh Perisai Residen** dialog anda boleh mengkonfigurasi fail mana yang akan diimbas (oleh sambungan tertentu):



Tentukan sama ada anda mahu semua fail diimbas atau hanya fail yang boleh dijangkiti - jika sedemikian, anda boleh seterusnya menentukan senarai sambungan yang mentakrifkan fail yang harus dikecualikan daripada pengimbasan dan juga senarai sambungan fail yang menentukan fail yang mesti diimbas dalam apa jua keadaan.

Seksyen di bawah yang dinamakan **Resident Shield akan mengimbas** meringkaskan lagi tetapan semasa, memaparkan gambaran keseluruhan terperinci tentang apa yang akan diimbas oleh **Resident Shield** sebenarnya.

9.11.2. Item yang dikecualikan



Dialog **Perisai Residen - Item Yang Dikecualikan** menawarkan kemungkinan mentakrifkan fail dan/ atau folder yang harus dikecualikan dari [imbasan](#) Perisai Residen.

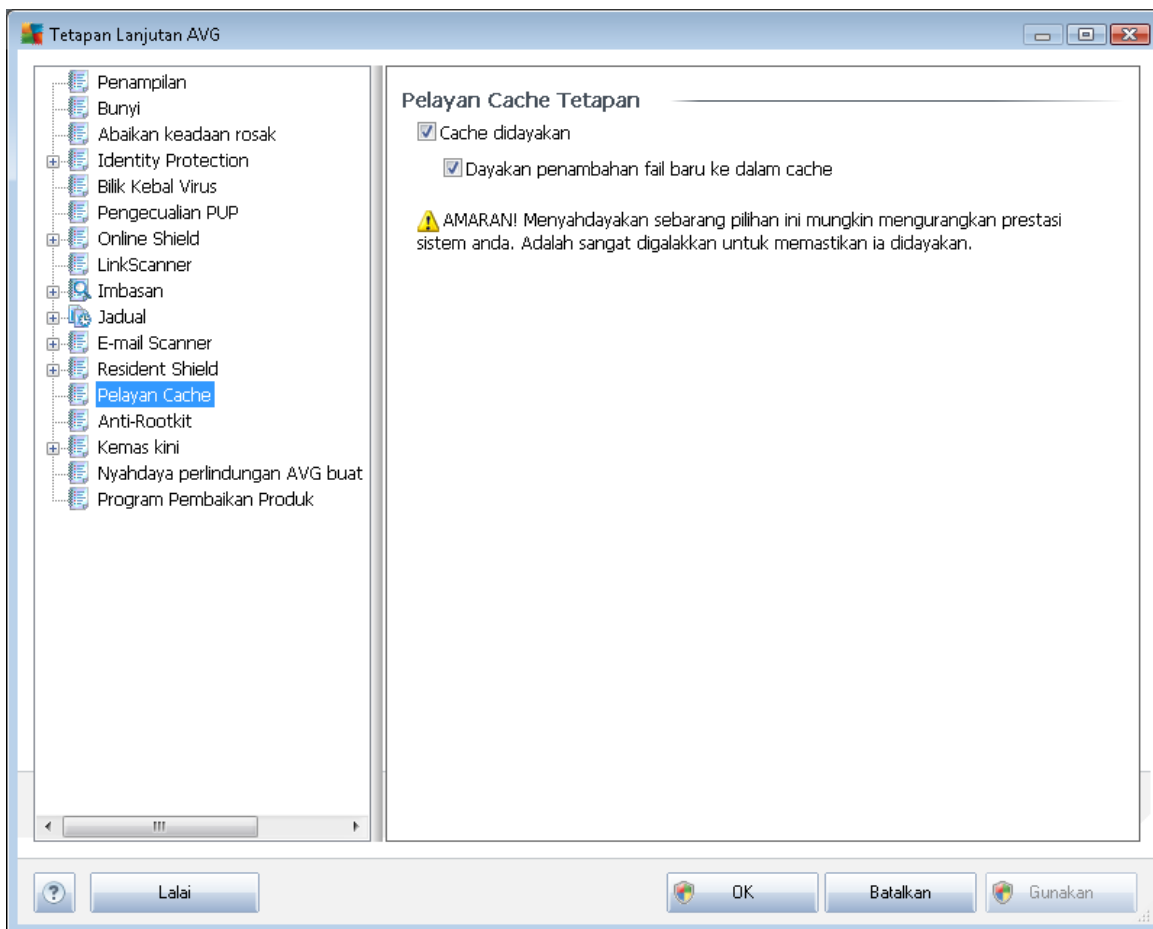
Jika ini tidak penting, kami sangat mengesyorkan untuk tidak mengecualikan sebarang item!

Dialog menyediakan butang kawalan berikut:

- **Tambah Laluan**– tentukan direktori untuk dikecualikan daripada imbasan dengan memilihnya satu persatu dari pohon navigasi cakera tempatan
- **Tambah Fail** – tentukan fail untuk dikecualikan daripada pengimbasan dengan memilihnya satu persatu daripada pohon navigasi cakera tempatan
- **Edit Item**– membenarkan anda mengedit laluan yang ditentukan kepada fail atau folder yang dipilih
- **Buang Item** – membenarkan anda memadam laluan ke item yang dipilih daripada senarai

9.12. Pelayan Cache

Pelayan Cache adalah proses untuk mempercepatkan sebarang imbasan (*imbasan dengan permintaan, seluruh imbasan komputer yang dijadualkan, imbasan [Perisai Residen](#)*). Ia mengumpul dan memastikan maklumat bagi fail yang boleh dipercayai (*fail sistem dengan tandatangan digital dll.*): Fail-fail ini kemudian, dikira selamat dan ia dilangkau sewaktu imbasan.

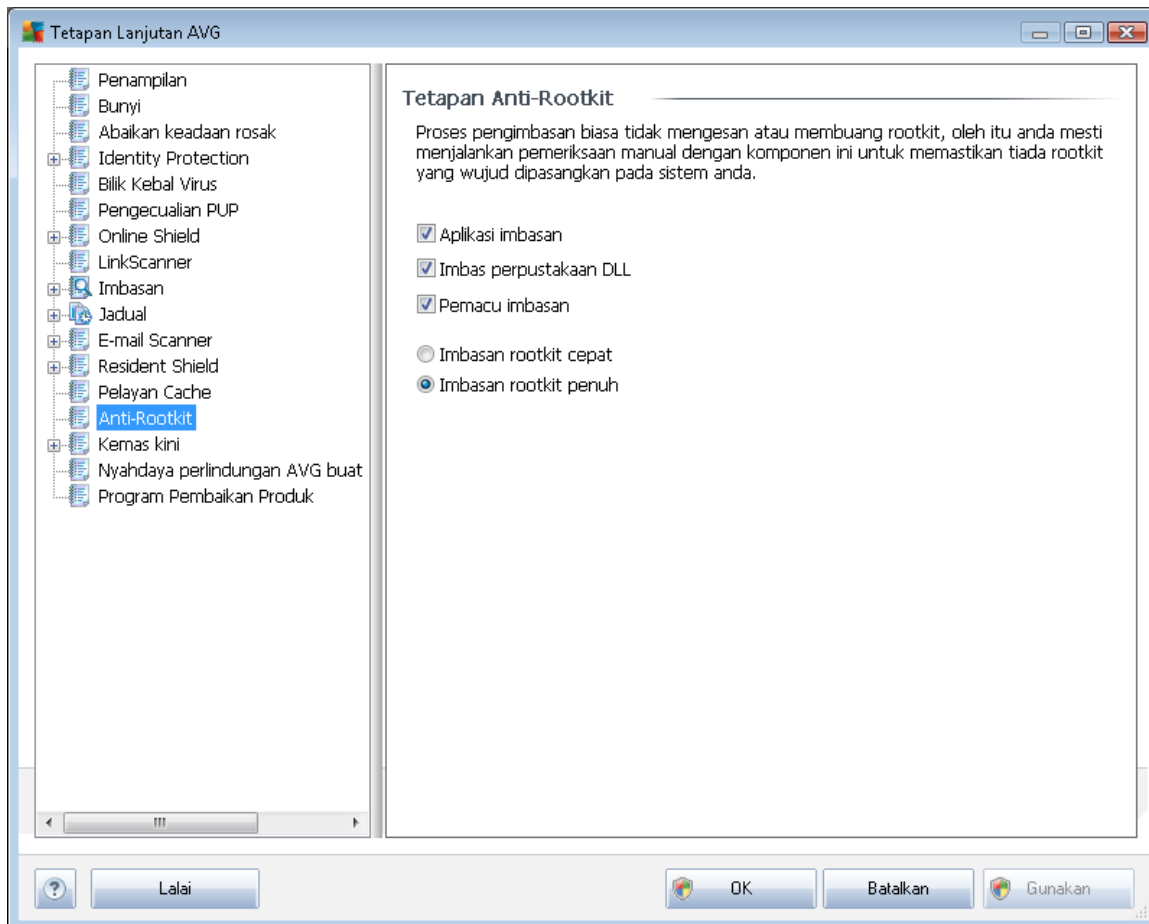


Dialog tetapan menawarkan dua pilihan:

- **Cache didayakan** (*dihidupkan secara lalai*) - jangan tanda kotak untuk mematikan **Pelayan Cache**, dan mengosongkan memori cache. Sila maklum bahawa pengimbasan mungkin memperlahankan, dan seluruh prestasi komputer anda berkurangan kerana setiap fail tunggal yang digunakan akan diimbas untuk virus dan perisian pengintip dahulu.
- **Dayakan penambahan fail baru ke dalam cache** (*dihidupkan secara lalai*) - jangan tanda kotak untuk berhenti menambah lebih banyak fail ke dalam memori cache. Sebarang fail yang telah dibuat cache akan disimpan dan digunakan sehingga cache dimatikan sepenuhnya atau sehingga kemas kini seterusnya bagi pangkalan data virus.

9.13. AntiRootkit

Dalam dialog ini, anda boleh mengedit konfigurasi komponen [AntiRootkit](#).



Mengedit semua fungsi komponen [AntiRootkit](#) seperti yang diberikan dalam dialog ini juga boleh diakses secara terus daripada [antara muka komponen AntiRootkit](#).

Tandakan kotak semakan masing-masing untuk menentukan objek khusus yang harus diimbas:

- **Aplikasi imbasan**
- **Imbas pustaka DLL**
- **Pemacu imbasan**

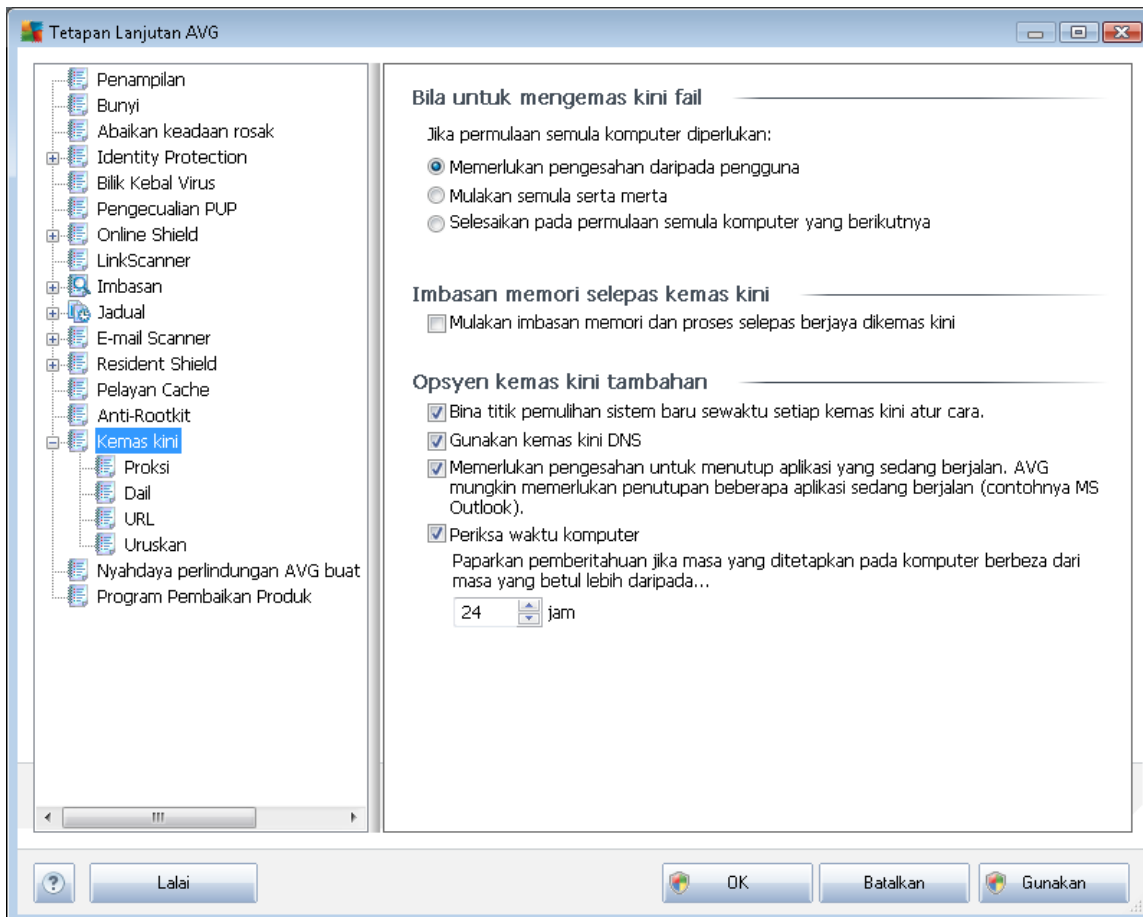
Seterusnya, anda boleh memilih mod pengimbasan rootkit:

- **Imbasan rootkit cepat** - mengimbas semua proses berjalan, pemacu yang dimuatkan dan folder sistem (*biasanya, c:\Windows*)
- **Imbasan rootkit penuh** - mengimbas semua proses berjalan, pemacu yang dimuatkan,



folder sistem (*biasanya, c:\Windows*), campur semua cakera tempatan (*termasuk cakera denyar tetapi tidak termasuk cakera liut/pemacu CD*)

9.14. Kemas kini



Item navigasi **Kemas Kini** membuka dialog baru di mana anda boleh menentukan parameter umum berkenaan [kemas kini AVG](#):

Bila untuk mengemas kini fail

Dalam seksyen ini, anda boleh memilih daripada tiga pilihan alternatif untuk digunakan jika proses kemas kini memerlukan anda memulakan semula PC. Penyelesaian kemas kini boleh dijadualkan untuk mula semula PC seterusnya, atau anda boleh melancarkan mula semula dengan segera:

- **Memerlukan pengesahan dari pengguna** (*secara lalai*)- anda akan diminta untuk meluluskan mula semula PC yang diperlukan untuk menyelesaikan [proses kemas kini](#)
- **Mula semula serta-merta** - komputer akan dimulakan semula secara automatik selepas [proses kemas kini](#) telah selesai dan kelulusan anda tidak diperlukan



- **Lengkapkan mula semula komputer seterusnya** - penyelesaian [proses kemas kini](#) akan ditangguh sehingga mula semula komputer seterusnya. Sila ingat bahawa pilihan ini hanya disyorkan jika anda pasti bahawa komputer dimulakan semula dengan kerap, sekurang-kurangnya sekali sehari!

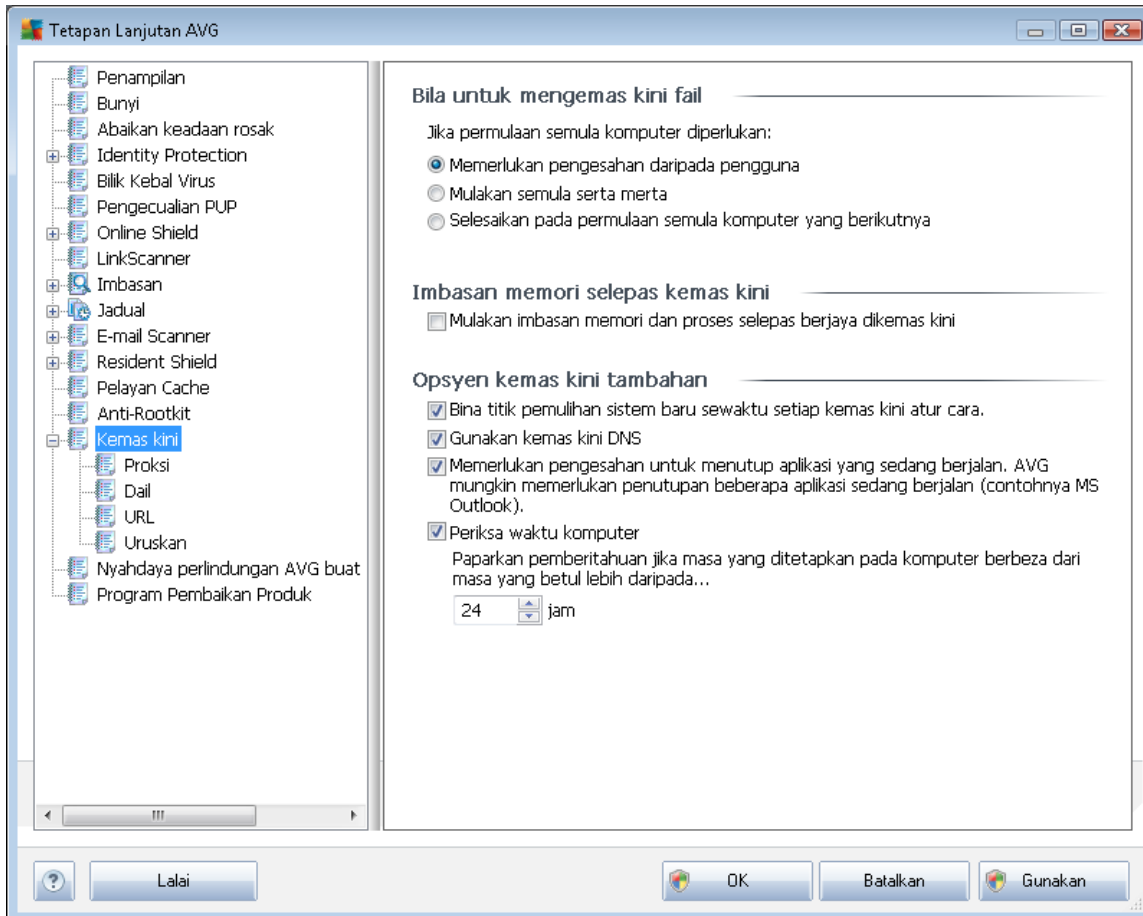
Imbasan memori selepas kemas kini

Tandakan kotak semakan ini untuk mentakrifkan bahawa anda hendak melancarkan imbasan memori baru selepas setiap kemas kini yang berjaya dilengkapkan. Kemas kini yang terkini dimuat turun mungkin telah mengandungi definisi virus baru dan ini boleh digunakan dalam pengimbasan dengan serta-merta.

Opsyen kemas kini tambahan

- **Bina titik pemulihan sistem selepas setiap kemas kini atur cara** - sebelum setiap pelancaran kemas kini atur cara AVG, titik pemulihan sistem dibuat. Jika proses kemas kini gagal dan sistem pengendalian anda hancur, anda sentiasa boleh memulihkan OS anda dalam konfigurasi asal dari titik ini. Opsyen ini boleh diakses melalui Start / All Programs / Accessories / System tools / System Restore, tetapi sebarang perubahan hanya boleh disarankan kepada pengguna berpengalaman sahaja! Pastikan kotak semakan ini ditandakan jika anda hendak menggunakan kefungsiannya ini.
- **Gunakan kemas kini DNS (dihidupkan secara lalai)** - dengan item ini ditanda, sebaik sahaja kemas kini dilancarkan, **AVG Anti-Virus 2011** anda mencari maklumat mengenai versi pangkalan data virus terkini dan versi atur cara terkini pada pelayan DNS. Kemas kini fail terkecil yang amat diperlukan dimuat turun, dan digunakan. Dengan cara ini, jumlah amaun data yang dimuat turun diminimumkan, dan proses kemas kini berjalan dengan lebih cepat.
- **Memerlukan pengesahan untuk menutup aplikasi yang sedang dijalankan (dihidupkan secara lalai)** akan membantu anda memastikan tiada aplikasi yang sedang dijalankan yang akan ditutup tanpa kebenaran anda - jika diperlukan untuk proses kemas kini diselesaikan;
- **Periksa masa komputer** - tandakan opsyen ini untuk mengesahkan bahawa anda mahu pemberitahuan ini dipaparkan jika masa komputer berbeza dari masa yang betul lebih daripada bilangan jam yang ditetapkan.

9.14.1. Proksi



Pelayan proksi adalah pelayan atau perkhidmatan tersendiri yang dijalankan pada PC yang memberi jaminan sambungan lebih selamat kepada Internet. Menurut peraturan rangkaian yang ditentukan, kemudian, anda boleh mengakses Internet sama ada secara terus atau melalui pelayan proksi; kedua-dua kemungkinan juga boleh dibenarkan dalam masa yang sama. Kemudian, dalam item pertama bagi dialog **Tetapan kemas kini - Proksi** anda perlu memilih dari menu kotak kombo sama ada anda mahu:

- **Gunakan proksi**
- **Jangan gunakan pelayan proksi - tetapan lalai**
- **Cuba penyambungan menggunakan proksi dan jika ia gagal, sambungkan secara langsung**

Jika anda memilih sebarang opsyen menggunakan pelayan proksi, anda perlu menentukan beberapa data selanjutnya. Tetapan pelayan boleh dikonfigurasi sama ada secara manual atau secara automatik.



Konfigurasi manual

Jika anda memilih konfigurasi manual (semak *opsyen Manual* untuk mengaktifkan bahagian dialog *masing-masing*) anda perlu menentukan item berikut:

- **Pelayan**– menentukan alamat IP pelayan atau nama pelayan
- **Port**– menentukan bilangan port yang mendayakan akses Internet (*secara lalai, nombor ini ditetapkan kepada 3128 tetapi boleh ditetapkan secara berbeza – jika anda tidak pasti, hubungi pentadbir rangkaian anda*)

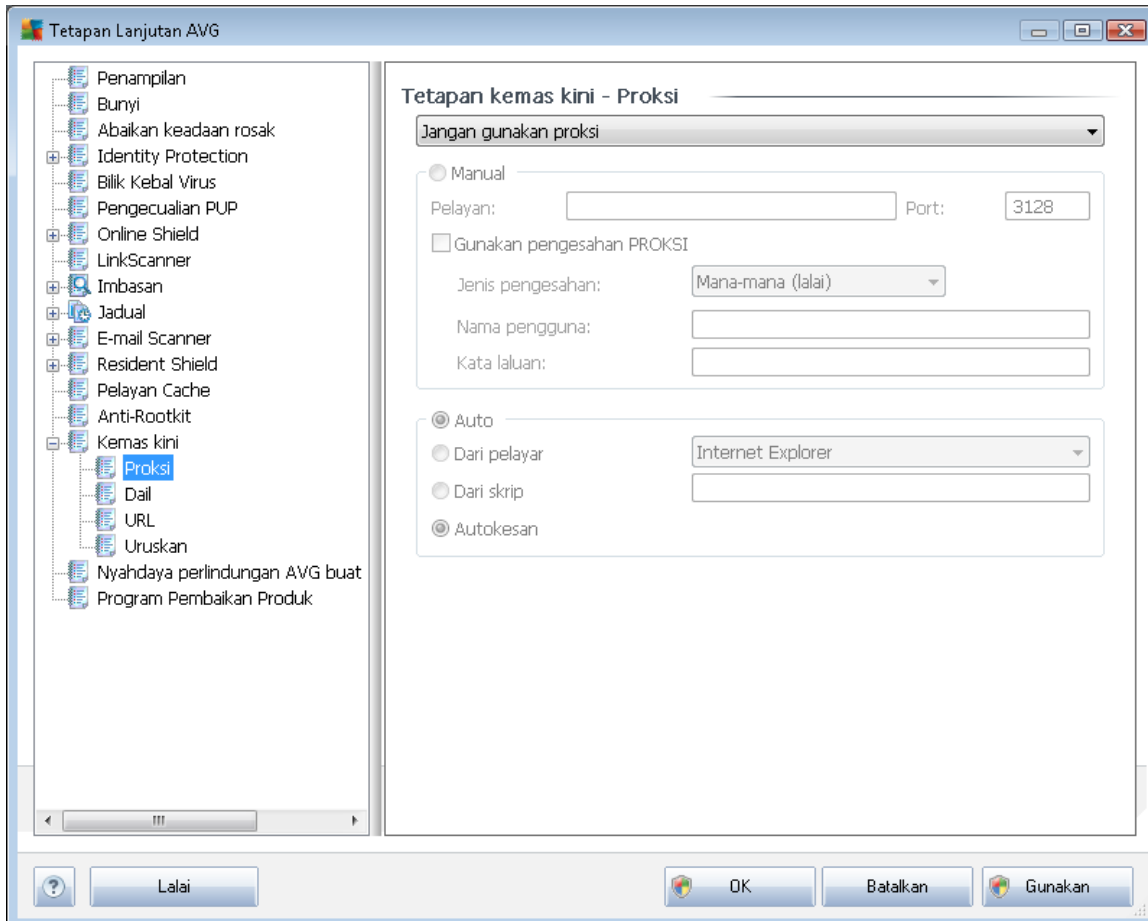
Pelayan proksi juga boleh mengkonfigurasi peraturan tertentu untuk setiap pengguna. Jika pelayan proksi anda disediakan dengan cara ini, tandakan opsyen **Guna pengesahan PROKSI** untuk mengesahkan bahawa nama pengguna dan kata laluan anda sah untuk menyambung kepada Internet melalui pelayan proksi.

Konfigurasi automatik

Jika anda memilih konfigurasi automatik (*tandakan pilihan Auto* untuk mengaktifkan bahagian dialog *masing-masing*) kemudian, sila pilih dari mana konfigurasi proksi akan dilakukan:

- **Dari pelayar** - konfigurasi akan dibaca dari pelayar internet lalai anda
- **Dari skrip** - konfigurasi akan dibaca dari skrip yang dimuat turun dengan fungsi yang mengembalikan alamat proksi
- **Autokesan** - konfigurasi akan dikesan secara automatik secara terus dari pelayan proksi

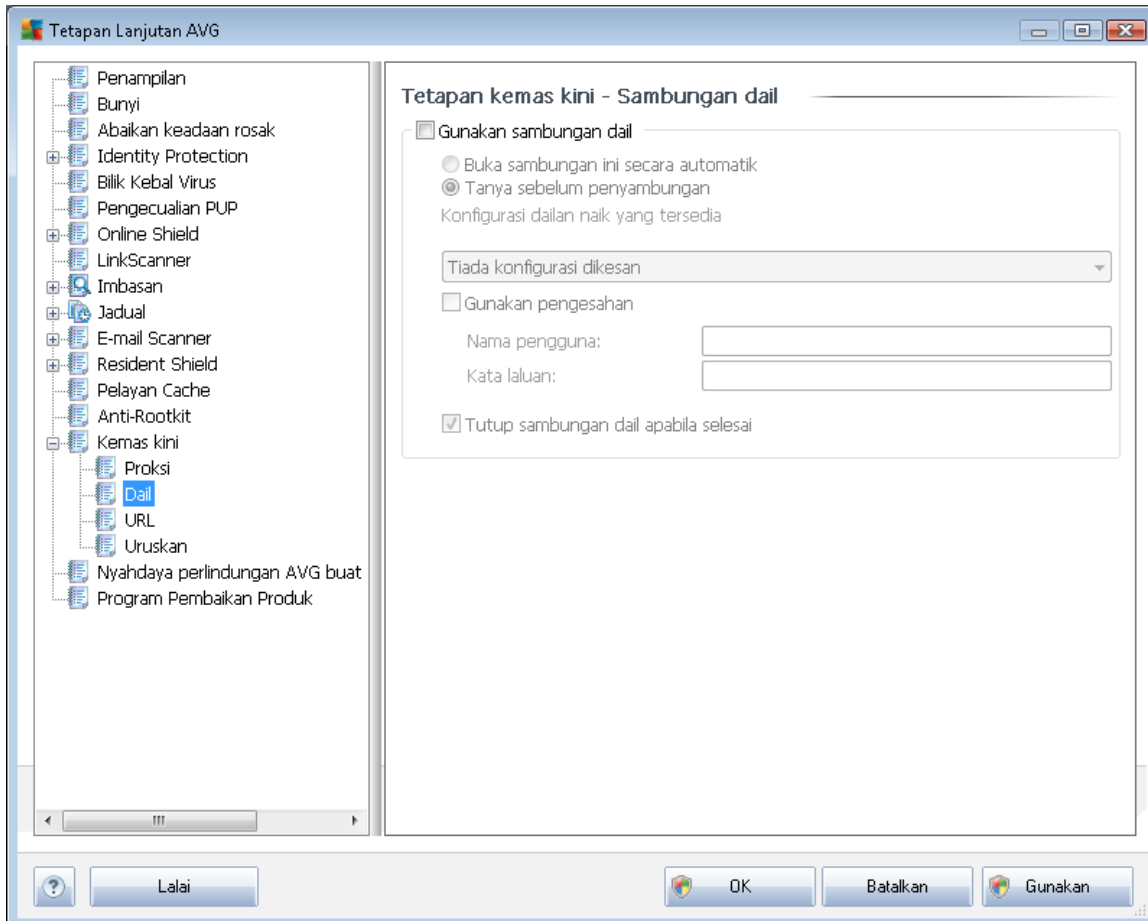
9.14.2. Dailan



Semua parameter yang ditakrifkan secara pilihan dalam dialog **Kemas kini tetapan - sambungan Dailan** merujuk kepada sambungan dailan kepada Internet. Medan dialog adalah tidak aktif sehingga anda menandakan opsiyen **Gunakan sambungan dailan** yang mengaktifkan medan.

Tentukan sama ada anda hendak bersambung kepada Internet secara automatik (**Buka sambungan ini secara automatik**) atau anda mahu mengesahkan sambungan secara manual setiap kali (**Tanya sebelum sambungan**). Untuk sambungan automatik, anda harus seterusnya memilih sama ada sambungan harus ditutup selepas kemas kini selesai (**Tutup sambungan dailan apabila selesai**).

9.14.3. URL

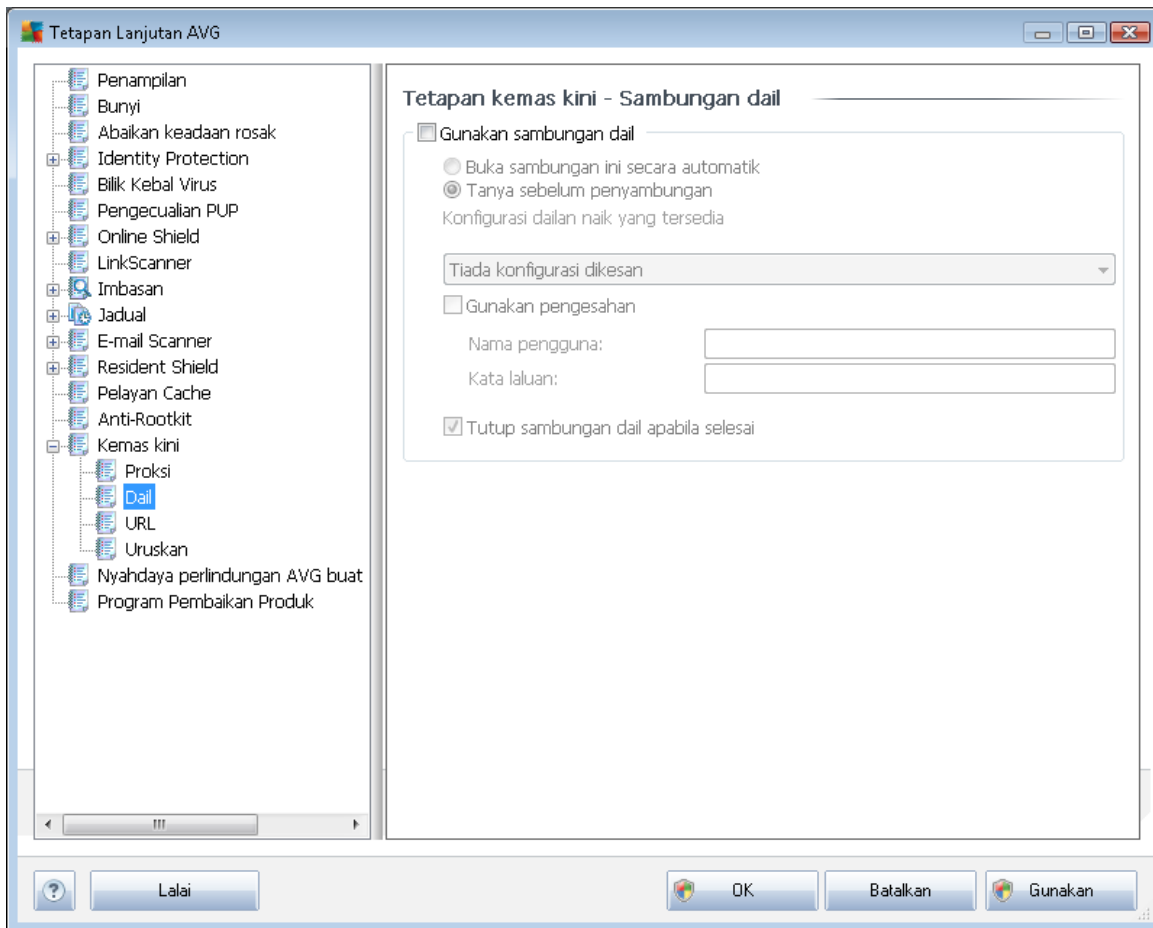


Dialog **URL** menawarkan senarai alamat Internet dari mana fail kemas kini dimuat turun. Senarai dan itemnya boleh diubah suai menggunakan butang kawalan berikut:

- **Tambah**– membuka dialog di mana anda boleh menentukan URL baru untuk ditambah ke senarai
- **Edit** - membuka dialog di mana anda boleh mengedit parameter URL yang dipilih
- **Padam**– memadam URL yang dipilih dari senarai
- **Alih ke Atas**– mengalihkan URL yang dipilih ke satu kedudukan atas dalam senarai
- **Alih ke Bawah** – mengalihkan URL yang dipilih ke satu kedudukan ke bawah dalam senarai

9.14.4. Uruskan

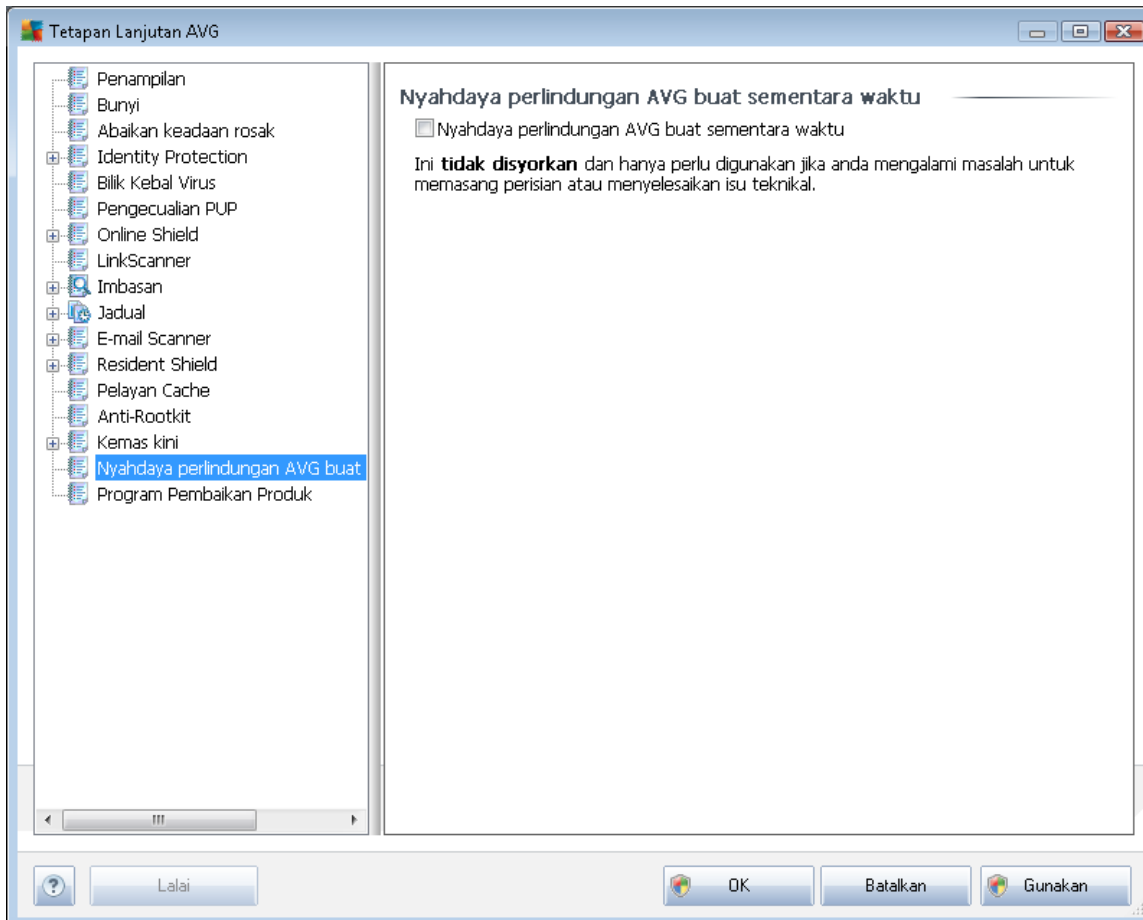
Dialog **Uruskan** menawarkan dua opsi yang boleh diakses melalui dua butang:



- **Padam fail kemas kini sementara** - tekan butang ini untuk memadam semua fail kemas kini berlebihan dari cakera keras anda (*secara lalai, fail ini disimpan selama 30 hari*)
- **Kembalikan semula pangkalan data virus ke versi sebelumnya** – tekan butang ini untuk memadam versi pangkalan virus terkini daripada cakera keras anda, dan untuk kembali ke versi yang disimpan sebelum ini (*versi pangkalan virus baru akan menjadi sebahagian daripada kemas kini berikut*)



9.15. Menyahdaya perlindungan AVG buat sementara waktu



Dalam dialog ***Menyahdaya perlindungan AVG buat sementara waktu*** anda mempunyai pilihan untuk mematikan keseluruhan perlindungan yang dikawal oleh **AVG Anti-Virus 2011** anda sekaligus.

Jangan lupa bahawa anda tidak seharusnya menggunakan opsi ini melainkan ia adalah benar-benar perlu!

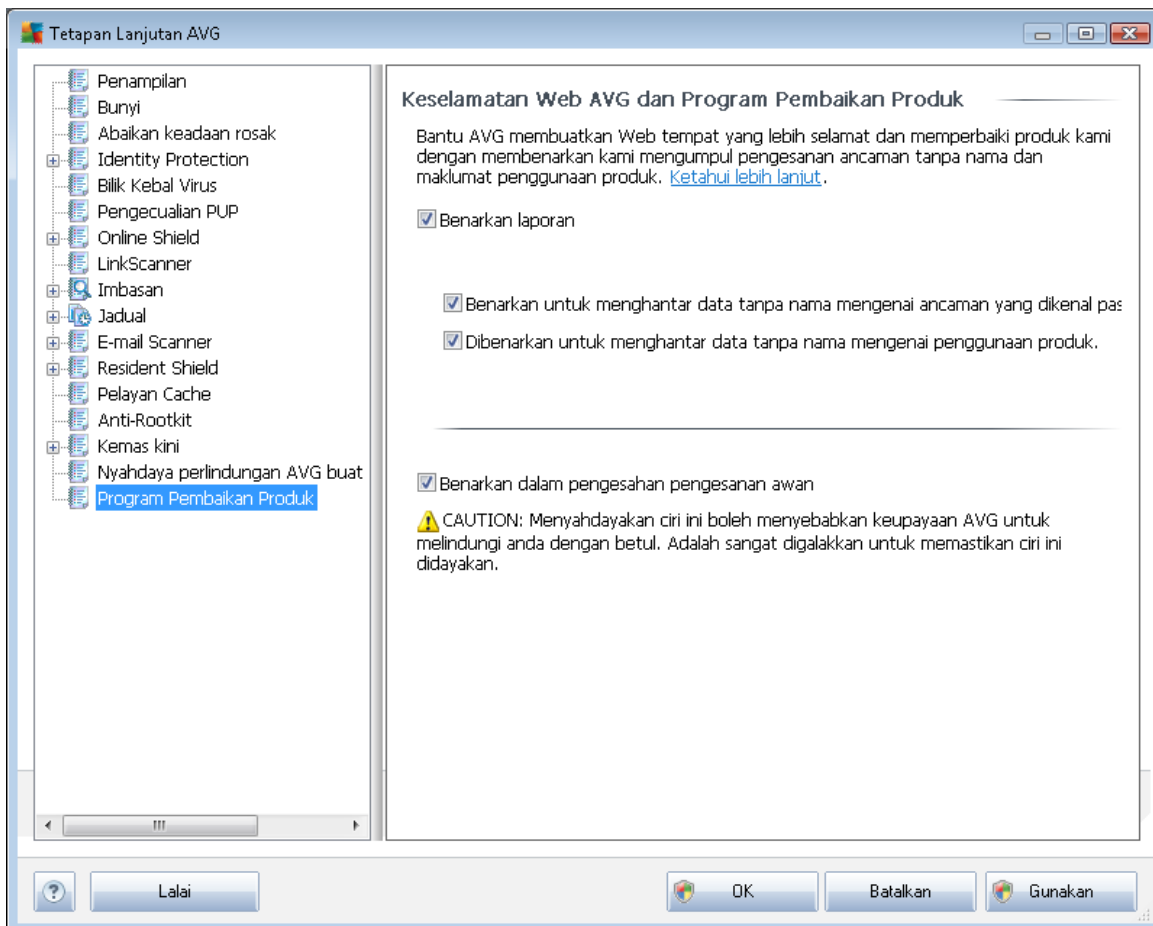
Dalam kebanyakan kes, adalah ***tidak perlu*** menyahdayakan AVG sebelum memasang perisian atau pemacu baru, walaupun jika pemasangan atau wizard perisian mencadangkan bahawa atur cara dan aplikasi yang dijalankan dimatikan dahulu untuk memastikan tiada gangguan yang tidak dikehendaki sewaktu proses pemasangan. Sekiranya anda benar-benar menghadapi masalah semasa pemasangan, cuba menyahaktifkan komponen ***Perisai Residen*** terlebih dahulu. Jika anda perlu menyahdayakan AG buat sementara waktu, anda perlu mendayakannya semula sebaik sahaja anda selesai. Jika anda bersambung ke Internet atau rangkaian semasa perisian antivirus anda dinyahdayakan, komputer anda terdedah kepada serangan.



9.16. Program Pembaikan Produk

Dialog **Keselamatan Web dan Program Pembaikan Produk AVG** menjemput anda untuk menyertai pembaikan produk AVG, dan membantu kami meningkatkan tahap keselamatan Internet secara keseluruhan. Tandakan opsyen **Benarkan pelaporan** untuk mendayakan pelaporan ancaman yang dikesan kepada AVG. Ini membantu kami mengumpulkan maklumat terbaru tentang ancaman terkini dari semua peserta di seluruh dunia, dan kami boleh sebagai balasan membaiki perlindungan untuk semua orang.

Pelaporan diuruskan secara automatik, oleh itu tidak akan memberikan anda sebarang masalah dan tiada data peribadi disertakan dalam laporan. Pelaporan ancaman yang dikesan adalah pilihan, walau bagaimanapun, kami meminta anda menghidupkan juga ciri ini, kerana ia membantu kami membaiki perlindungan untuk anda dan pengguna AVG lain.



Hari ini, terdapat lebih banyak ancaman di luar sana selain virus biasa. Penulis kod berniat jahat dan laman web merbahaya sangat berinovasi, dan ancaman jenis baru muncul dengan kerap, dan sebahagian besarnya di Internet. Ini adalah beberapa yang paling biasa:

- **Virus ialah kod berniat jahat yang menyalin dan menyebarkan dirinya sendiri, selalunya tidak disedari sehingga berlaku kerosakan.** Sesetengah virus adalah ancaman serius, memadam atau sengaja mengubah fail dalam laluan mereka, manakala



sesetengah virus melakukan sesuatu yang kelihatan tidak berbahaya, seperti memainkan muzik. Bagaimanapun, semua virus adalah berbahaya kerana keupayaan asasnya untuk berkembang - malah satu virus ringkas boleh memenuhi memori komputer sekelip mata, dan menyebabkan kerosakan.

- **Cecacing** ialah satu subkategori virus yang mana, tidak seperti virus normal, tidak memerlukan objek "pembawa" untuk melampirkannya; ia menghantar dirinya sendiri kepada komputer lain sendiri, selalunya melalui e-mel, dan hasilnya selalu melebihi bebas pelayan e-mel dan sistem rangkaian.
- **Perisian Pengintip** selalunya ditakrifkan sebagai kategori malware (*malware = sebarang perisian berniat jahat, termasuk virus*) atur cara melingkungi – biasanya kuda Trojan – disasarkan untuk mencuri maklumat peribadi, kata laluan, nombor kad kredit, atau mencerobohi komputer dan membenarkan penyerang mengawalnya dari jauh; sudah pasti, semuanya tanpa pengetahuan atau kebenaran pemilik komputer.
- **Program berpotensi tidak dikehendaki** adalah sejenis perisian pengintip yang boleh tetapi tidak semestinya merbahaya kepada komputer anda. Contoh khusus PUP adalah adware, perisian yang direka untuk mengedarkan pengiklanan, biasanya dengan memaparkan pop muncul iklan; mengganggu, tetapi tidak benar-benar berbahaya.
- **Kuki penjejakan** boleh dianggap sebagai sejenis perisian pengintip, memandangkan fail kecil ini, disimpan dalam pelayan web dan dihantar secara automatik kepada laman web "induk" apabila anda melawatnya lagi, boleh mengandungi data seperti sejarah pelayaran anda dan maklumat serupa yang lain.
- **Eksplit** adalah kod berniat jahat yang cuba mengambil kesempatan dari kekurangan atau kelemahan dalam sistem pengendalian, pelayan Internet, atau atur cara penting lain.
- **Pemancingan data** adalah percubaan untuk mendapatkan data peribadi sensitif dengan menyamar sebagai organisasi yang dipercayai dan terkenal. Biasanya, mangsa berpotensi dihubungi melalui e-mel pukal meminta mereka untuk cthnya. mengemas kini butiran akaun bank mereka. Untuk melakukan itu, mereka dijemput mengikuti pautan yang diberikan yang kemudiannya membawa kepada laman web palsu bank itu.
- **Penipuan adalah e-mel besar mengandungi maklumat berbahaya, merisaukan atau cuma mengganggu dan tidak berguna.** Kebanyakan daripada ancaman di atas menggunakan mesej e-mel palsu untuk disebarkan.
- **Laman web berniat jahat** adalah yang akan dengan sengaja memasang perisian berniat jahat pada komputer anda, dan laman yang digodam juga berbuat begitu, cuma ini adalah laman web sah yang telah dikompromi untuk menjangkiti pelawat.

Untuk melindungi anda dari semua jenis ancaman ini, AVG memasukkan komponen khusus ini:

- **[AntiVirus](#)** untuk melindungi komputer anda dari virus,
- **[AntiPerisian Pengintip](#)** untuk melindungi komputer anda dari perisian pengintip,
- **[Online Shield](#)** untuk melindungi anda daripada virus dan perisian pengintip semasa



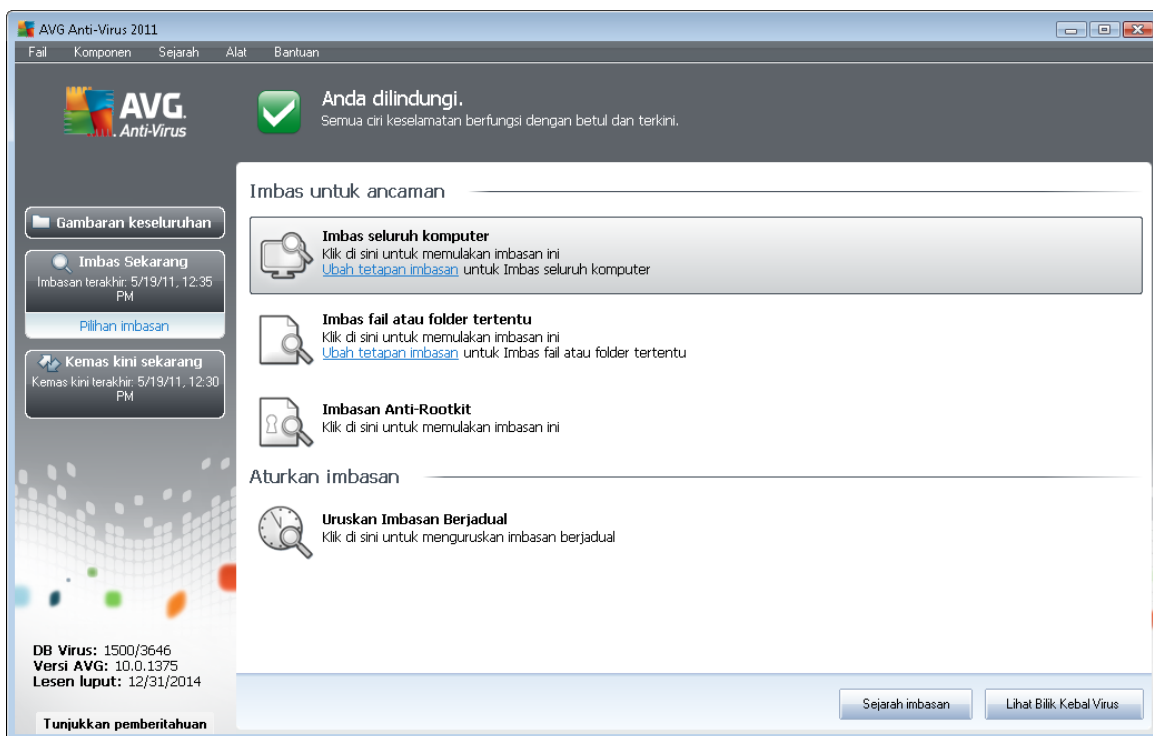
melayari Internet,

- [LinkScanner](#) untuk melindungi anda dari ancaman dalam talian lain yang disebut dalam bab ini.

10. Pengimbasan AVG

Pengimbasan adalah bahagian penting bagi kefungsiannya **AVG Anti-Virus 2011**. Anda boleh menjalankan ujian yang dalam permintaan atau [menjaduikannya untuk dijalankan secara berkala](#) pada masa yang sesuai.

10.1. Antara Muka Pengimbasan



Antara muka pengimbasan AVG boleh diakses melalui [pautan pantas](#) **opsyen Imbasan**. Klik pautan ini untuk beralih ke dialog **Imbas untuk ancaman**. Dalam dialog ini, anda akan menemui yang berikut:

- gambaran keseluruhan bagi [imbasan yang dipraktikkan](#) - tiga jenis pengimbasan yang ditentukan oleh vendor perisian sedia untuk digunakan dengan serta-merta mengikut permintaan atau jadual:
 - [Imbasan seluruh komputer](#)
 - [Imbas fail atau folder tertentu](#)
 - [Imbasan AntiRootkit](#)
- [imbas bahagian](#) yang dijadualkan - di mana anda boleh mentakrifkan ujian baru dan membuat jadual baru seperti yang diperlukan.

Butang kawalan



Butang kawalan tersedia dalam antara muka pengujian adalah yang berikut:

- **Sejarah imbasan** - memaparkan dialog [Gambaran keseluruhan keputusan imbasan](#) dengan sejarah keseluruhan imbasan
- **Lihat Bilik Kebal Virus** - membuka tettingkap baru dengan [Bilik Kebal Virus](#) - ruang di mana jangkitan yang dikesan dikuarantinkan

10.2. Imbasan Pratakrif

Salah satu ciri utama bagi **AVG Anti-Virus 2011** adalah pengimbasan dalam permintaan. Ujian dalam permintaan direka bentuk untuk mengimbas pelbagai bahagian komputer anda apabila kecurigaan bagi kemungkinan jangkitan virus berlaku. Walau bagaimanapun, ia amat disarankan untuk menjalankan ujian seperti itu secara tetap walaupun jika anda merasakan tiada virus yang boleh ditemui pada komputer anda.

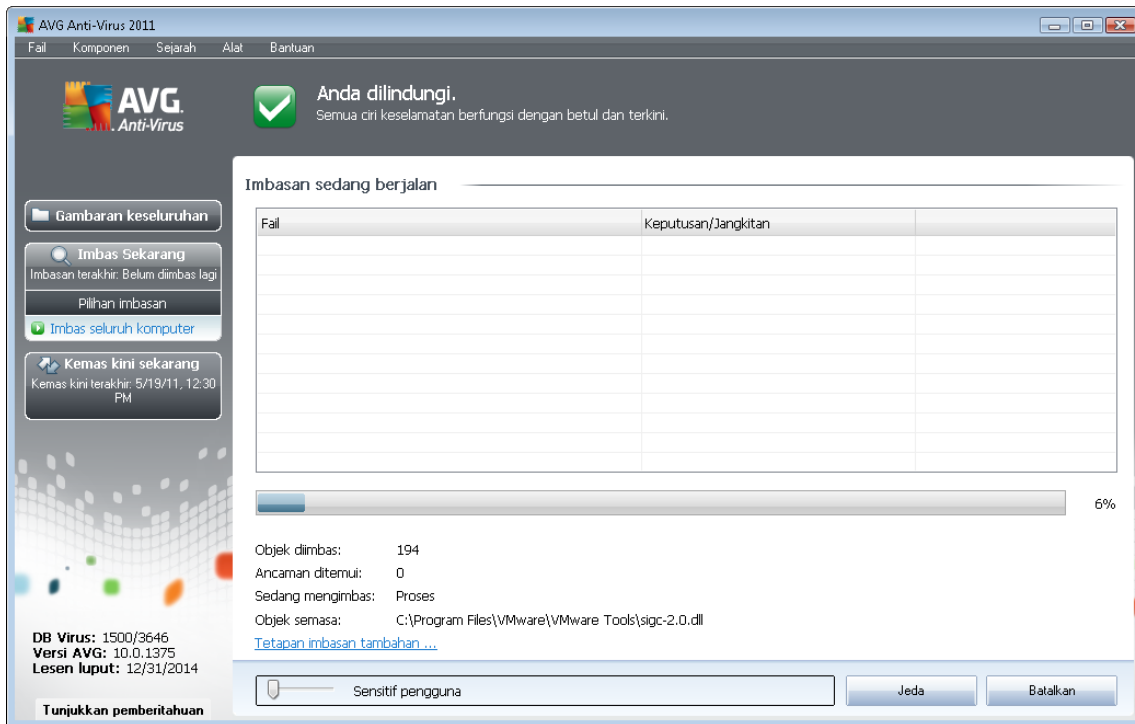
Dalam **AVG Anti-Virus 2011** anda akan menemui dua jenis pengimbasan yang dipratetapkan oleh vendor perisian:

10.2.1. Imbasan Seluruh Komputer

Imbasan Seluruh Komputer - mengimbas seluruh komputer anda untuk kemungkinan jangkitan dan/atau program berpotensi tidak dikehendaki. Ujian ini akan mengimbas semua pemacu keras komputer anda, akan mengesan dan memulihkan sebarang virus yang ditemui atau membuang jangkitan yang dikesan ke [Bilik Kebal Virus](#). Mengimbas seluruh komputer anda perlu dijadualkan pada stesen kerja sekurang-kurangnya sekali seminggu.

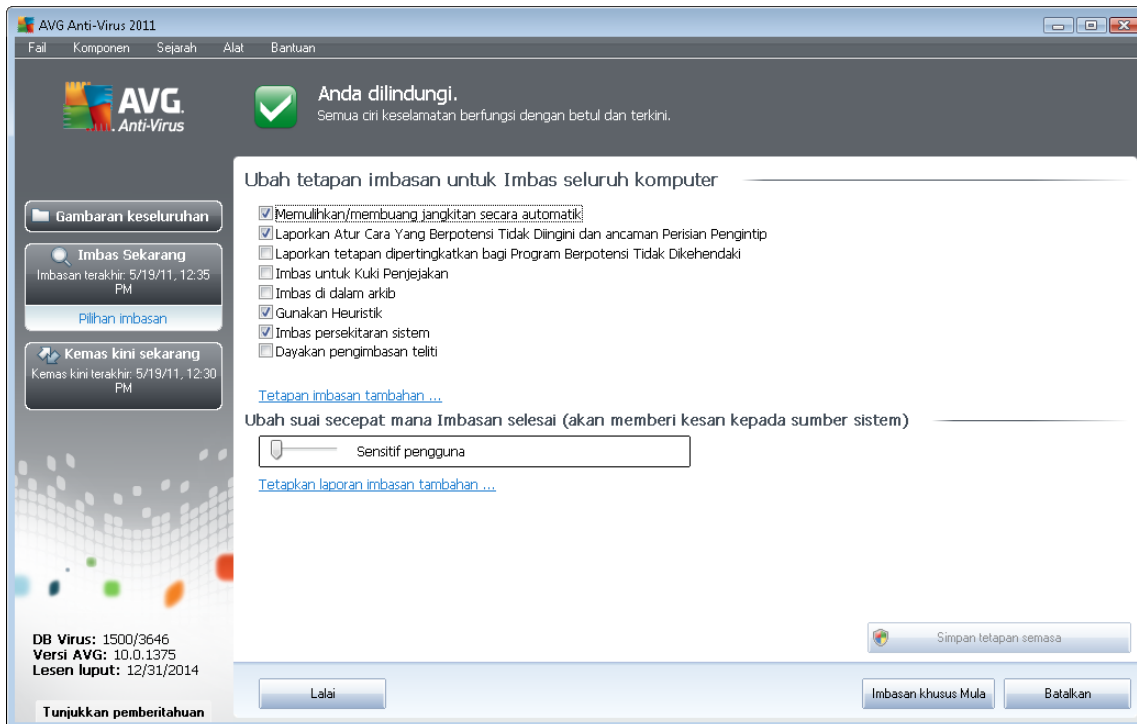
Lancarkan imbasan

Imbasan Seluruh Komputer boleh dilancarkan secara terus dari [antara muka imbasan](#) dengan mengklik pada ikon imbasan. Tiada tetapan khusus selanjutnya perlu dikonfigurasi untuk jenis imbasan ini, pengimbasan akan bermula dengan serta-merta dalam dialog **Imbasan sedang dijalankan** (*lihat gambar skrin*). Imbasan boleh diganggu sementara waktu (**Jeda**) atau dibatalkan (**Berhenti**) jika perlu.



Pengeditan konfigurasi imbasan

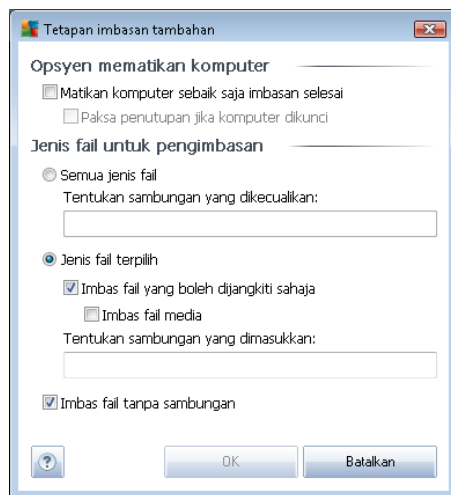
Anda mempunyai opsi untuk menyunting tetapan lalai dipraktifik untuk **Imbasan seluruh komputer**. Tekan pautan **Tukar tetapan imbasan** untuk pergi ke dialog **Tukar tetapan imbasan bagi Seluruh komputer** (boleh diakses dari [antara muka pengimbasan](#) melalui pautan **Tukar tetapan imbasan untuk Imbasan seluruh komputer**). **Adalah digalakkan untuk menyimpan tetapan lalai melainkan anda mempunyai alasan kukuh untuk menukarnya!**



- **Parameter imbasan** - dalam senarai parameter imbasan, anda boleh menghidupkan/mematikan parameter tertentu seperti yang diperlukan:
 - **Pulih/buang jangkitan secara automatik** (*dibuka secara lalai*) - jika virus dikenal pasti sewaktu imbasan, ia boleh dipulihkan secara automatik jika cara mengatasinya tersedia. Jika fail yang dijangkiti tidak boleh dipulihkan secara automatik, objek yang dijangkiti akan dialih ke [Bilik Kebal Virus](#).
 - **Laporkan Program Berpotensi Tidak Dikehendaki dan ancaman Perisian Pengintip** (*dibuka secara lalai*) - tandakan untuk mengaktifkan enjin [AntiPerisian Pengintip](#), dan imbas untuk perisian pengintip serta untuk virus. [Perisian pengintip mewakili kategori malware yang dipersoalkan, walaupun, ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat.](#) Kami mengesyorkan untuk mengekalkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.
 - **Laporkan set dipertingkatkan bagi Program Berpotensi Tidak Dikehendaki** (*ditutup secara lalai*) -tandakan untuk mengesan pakej yang diluaskan bagi [perisian pengintip](#): atur cara yang sangat ok dan tidak berbahaya apabila diperoleh dari pengilang secara terus, tetapi, boleh disalahgunakan untuk tujuan berniat jahat selepas itu. Ini adalah langkah tambahan yang meningkatkan keselamatan komputer anda dengan lebih lagi, walau bagaimanapun, ia boleh menyekat atur cara sah dan oleh itu, dimatikan secara lalai.
 - **Imbas untuk Kuki Penjejakan** (*ditutup secara lalai*)- parameter ini bagi komponen [AntiPerisian Pengintip](#) mentakrifkan bahawa kuki harus dikesan;kuki HTTP digunakan untuk mengesahkan, menjejaki dan mengekalkan maklumat khusus

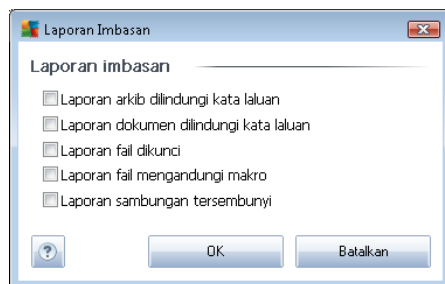
mengenai pengguna seperti keutamaan tapak atau kandungan kart beli-belah elektronik nya).

- **Imbas dalam arkib** (ditutup secara lalai - parameter ini menentukan bahawa imbasan harus memeriksa semua fail malahan yang disimpan dalam arkib, cth. ZIP, RAR, ...)
- **Gunakan Heuristik** (dibuka secara lalai) - analisis heuristik (perlagakan dinamik arahan objek yang diimbaskan dalam persekitaran komputer maya) akan menjadi salah satu kaedah yang digunakan untuk pengesanan virus sewaktu imbasan.
- **Imbas persekitaran sistem** (dibuka secara lalai) - imbasan juga akan memeriksa kawasan sistem komputer anda.
- **Dayakan pengimbasan teliti** (ditutup secara lalai) - dalam situasi khusus (mengesyaki komputer anda dijangkiti) anda boleh menandakan opsyen ini untuk mengaktifkan algoritma pengimbasan yang paling teliti yang akan turut mengimbas kawasan komputer anda yang sukar dijangkiti, sekadar untuk mendapatkan kepastian sepenuhnya. Namun ingat bahawa kaedah ini agak mengambil masa
- **Tetapan imbasan tambahan** - pautan membuka dialog **Tetapan imbasan tambahan** di mana anda boleh menentukan parameter berikut:



- **Opsyen mematikan komputer** - menentukan sama ada komputer patut dimatikan secara automatik sebaik saja proses pengimbasan selesai. Dengan mengesahkan opsyen ini (**Matikan komputer apabila imbasan selesai**), pengaktifan opsyen baru membenarkan komputer dimatikan walaupun jika ia sedang dikunci (**Paksa untuk dimatikan jika komputer dikunci**).
- **Tentukan jenis fail untuk pengimbasan** - seterusnya, anda harus menentukan sama ada anda hendak ia diimbaskan:
 - **Semua jenis fail** dengan kemungkinan bagi menentukan pengecualian daripada pengimbasan dengan memberikan senarai pemanjangan fail yang dipisahkan oleh koma yang tidak seharusnya diimbaskan;

- **Jenis fail yang dipilih** - anda boleh menentukan bahawa anda hendak mengimbas hanya fail yang berkemungkinan dijangkiti (*fail yang tidak boleh dijangkiti tidak akan diimbas, contohnya sesetengah fail teks biasa atau sesetengah fail bukan boleh laku*), termasuk fail media (*video, fail audio - jika anda membiarkan kotak in tidak ditandakan, ia akan mengurangkan lebih banyak masa kerana fail ini biasanya agak besar dan agak tidak berkemungkinan dijangkiti virus*). Sekali lagi, anda boleh menentukan sambungan fail mana yang sepatutnya sentiasa diimbas.
- Secara pilihan, anda boleh menentukan anda hendak **Mengimbas fail tanpa sambungan** - opsiyen ini dihidupkan secara lalai dan ia disyorkan untuk anda mengekalkannya melainkan anda mempunyai sebab sebenar untuk mengubahnya. Fail tanpa sambungan adalah lebih mencurigakan dan sepatutnya diimbas setiap masa.
- **Laraskan berapa cepat Imbasan selesai** - anda boleh menggunakan penggelongsor untuk menukar keutamaan proses pengimbasan. Secara lalai, nilai opsiyen ini ditetapkan kepada tahap *sensitif pengguna* bagi penggunaan sumber automatik. Secara alternatif, anda boleh menjalankan proses pengimbasan dengan lebih perlahan yang bermaksud muat sumber sistem akan diminimumkan (*berguna apabila anda perlu bekerja pada komputer tetapi anda tidak berapa kisah berapa lama imbasan berlaku*), atau lebih cepat dengan keperluan sumber sistem yang ditingkatkan (*cth. apabila komputer tidak digunakan sementara*).
- **Tetapkan laporan imbasan tambahan** - pautan membuka dialog **Imbas laporan** di mana anda boleh memilih jenis kemungkinan penemuan yang harus dilaporkan:



Amaran: Tetapan imbasan ini adalah sama dengan parameter bagi imbasan yang baru ditakrifkan - seperti yang diterangkan dalam bab [Pengimbasan AVG / Penjadualan imbasan / Cara untuk Mengimbas](#). Adakah anda akan memutuskan untuk mengubah konfigurasi lalai bagi **Imbas seluruh komputer** kemudian, anda boleh menyimpan tetapan baru anda sebagai konfigurasi lalai untuk digunakan untuk semua imbasan selanjutnya bagi seluruh komputer.

10.2.2. Imbas Fail atau Folder Tertentu

Imbas fail atau folder tertentu - mengimbas hanya kawasan komputer anda yang anda telah pilih untuk diimbas (*folder yang diimbas, cakera keras, cakera liut, CD, dll.*). Perkembangan imbasan jika pengesanan virus dan rawatannya adalah sama dengan imbas seluruh komputer: sebarang virus yang ditemui dipulihkan atau dibuang ke [Bilik Kebal Virus](#). Pengimbasan fail atau folder tertentu boleh digunakan untuk menyediakan ujian anda sendiri dan penjadualannya berdasarkan pada keperluan anda.

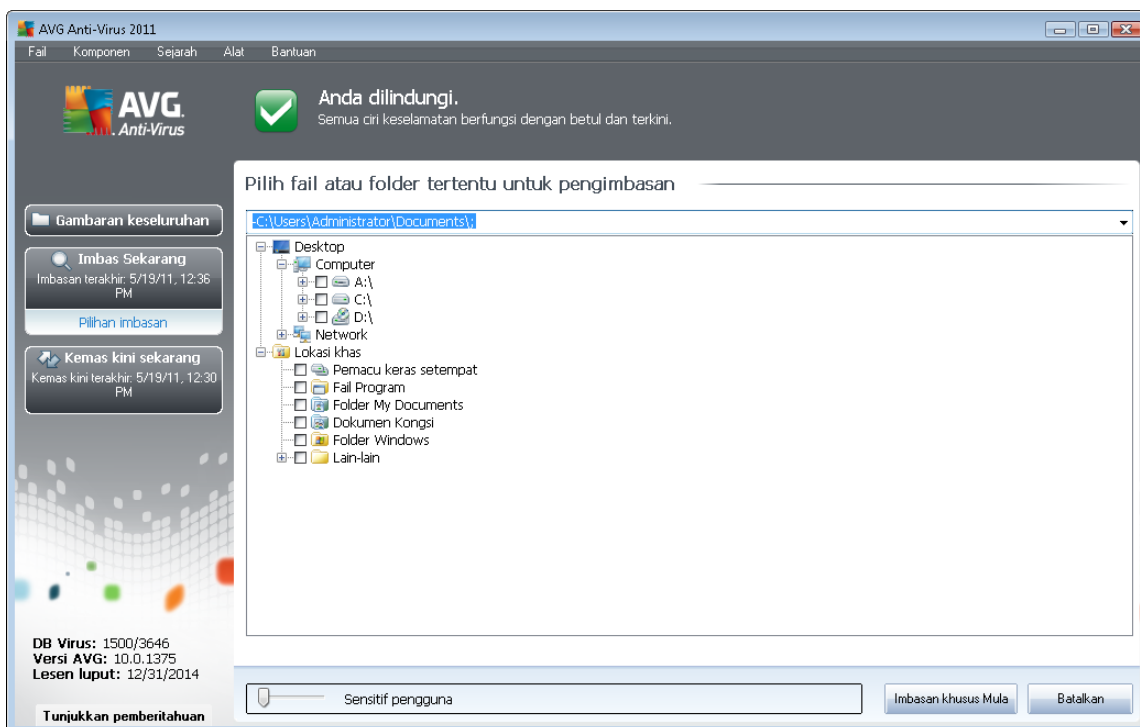


Lancarkan imbasan

Imbas fail atau folder tertentu boleh dilancarkan dari [pengimbasan antara muka](#) dengan mengklik pada ikon imbasan. Dialog baru yang dipanggil **Pilih fail atau folder untuk pengimbasan** terbuka. Dalam struktur pepohon komputer anda, pilih folder yang anda hendak imbas. Laluan kepada setiap folder yang dipilih akan dijana secara automatik dan muncul dalam kotak semakan di bahagian atas dialog ini.

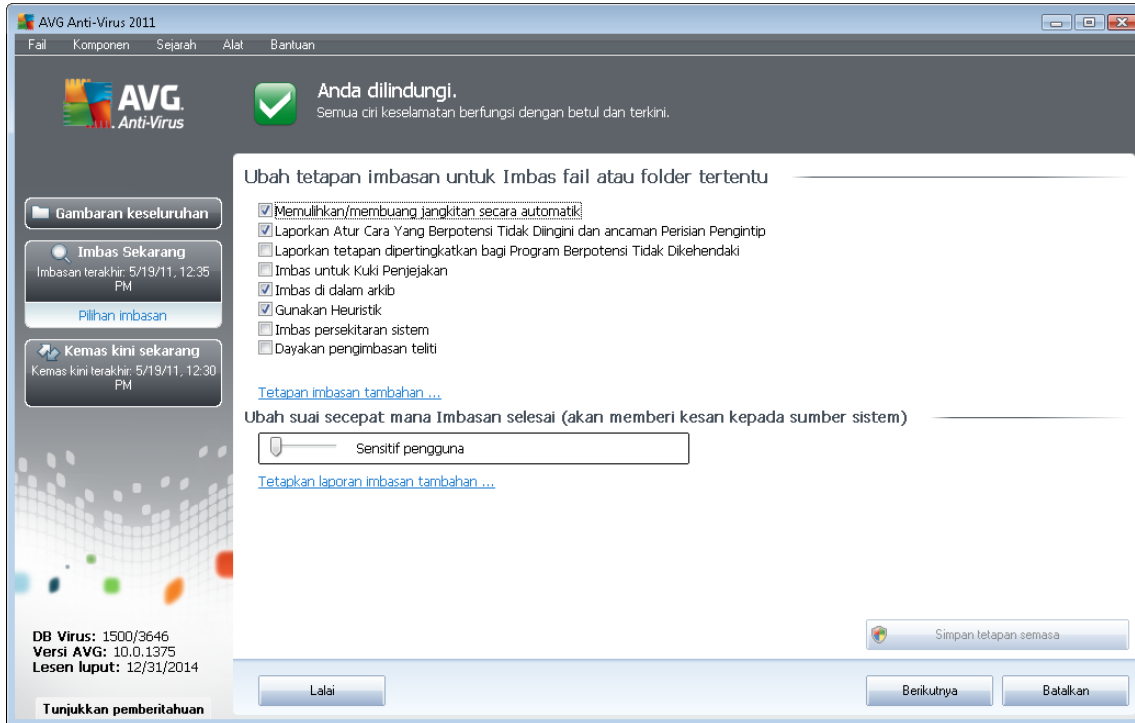
Terdapat juga kemungkinan mempunyai folder tertentu yang diimbas semasa semua subfoldernya tidak dimasukkan dalam imbasan ini, untuk melakukannya, tuliskan tanda tambah "+" di hadapan laluan yang dijana secara automatik (*lihat gambar skrin*). Untuk tidak memasukkan keseluruhan folder dari penggunaan imbasan, gunakan parameter parameter "!".

Akhir sekali, untuk melancarkan imbasan, tekan butang **Mulakan imbasan** ; proses pengimbasan itu sendiri adalah secara asasnya sama dengan [imbas Seluruh komputer](#).



Pengeditan konfigurasi imbasan

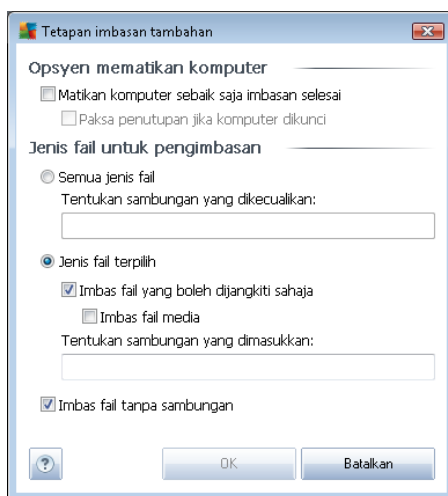
Anda mempunyai opsyen pengeditan bagi tetapan lalai yang dipratetapkan bagi **Imbasan fail atau folder tertentu**. Tekan pautan **Ubah tetapan imbasan** untuk pergi ke dialog **Ubah tetapan imbasan untuk Mengimbas fail atau folder tertentu** . **Adalah digalakkan untuk menyimpan tetapan lalai melainkan anda mempunyai alasan kukuh untuk menukarnya!**



- **Parameter imbasan** - dalam senarai parameter imbasan, anda boleh menghidupkan/mematikan parameter tertentu seperti yang diperlukan:
 - **Pulih/buang jangkitan secara automatik** (*dibuka secara lalai*) - jika virus dikenal pasti sewaktu imbasan, ia boleh dipulihkan secara automatik jika cara mengatasinya tersedia. Jika fail yang dijangkiti tidak boleh dipulihkan secara automatik, objek yang dijangkiti akan dialih ke [Bilik Kebal Virus](#).
 - **Laporkan Program Berpotensi Tidak Dikehendaki dan ancaman Perisian Pengintip** (*dibuka secara lalai*) - tandakan untuk mengaktifkan enjin [AntiPerisian Pengintip](#), dan imbas untuk perisian pengintip serta untuk virus. [Perisian pengintip mewakili kategori malware yang dipersoalkan, walaupun, ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat.](#) Kami mengesyorkan untuk mengekalkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.
 - **Laporkan set dipertingkatkan bagi Program Berpotensi Tidak Dikehendaki** (*ditutup secara lalai*) -tandakan untuk mengesan pakej yang diluaskan bagi [perisian pengintip](#): atur cara yang sangat ok dan tidak berbahaya apabila diperoleh dari pengilang secara terus, tetapi, boleh disalahgunakan untuk tujuan berniat jahat selepas itu. Ini adalah langkah tambahan yang meningkatkan keselamatan komputer anda dengan lebih lagi, walau bagaimanapun, ia boleh menyekat atur cara sah dan oleh itu, dimatikan secara lalai.
 - **Imbas untuk Kuki Penjejakan** (*ditutup secara lalai*) - parameter ini bagi komponen [AntiPerisian Pengintip](#) mentakrifkan bahawa kuki harus dikesan; *kuki HTTP digunakan untuk mengesahkan, menjejaki dan mengekalkan maklumat tertentu*

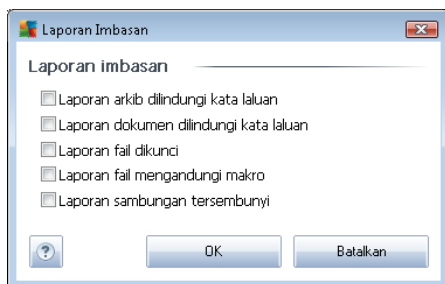
mengenai pengguna seperti keutamaan tapak atau kandungan kart beli-belah elektroniknya).

- **Imbas dalam arkib** (*dibuka secara lalai*) - parameter ini menentukan bahawa imbasan harus memeriksa semua fail yang disimpan dalam arkib, cth. ZIP, RAR, ...
- **Gunakan Heuristik** (*ditutup secara lalai*) - analisis heuristik (*perlagakan dinamik arahan objek yang diimbas dalam persekitaran komputer maya*) akan menjadi salah satu kaedah yang digunakan untuk pengesanan virus sewaktu imbasan.
- **Imbas persekitaran sistem** (*ditutup secara lalai*) - imbasan juga akan memeriksa kawasan sistem komputer anda.
- **Dayakan pengimbasan teliti** (*ditutup secara lalai*) - dalam situasi khusus (*mengesyaki komputer anda dijangkiti*) anda boleh menandakan opsyen ini untuk mengaktifkan algoritma pengimbasan yang paling teliti yang akan turut mengimbas kawasan komputer anda yang sukar dijangkiti, sekadar untuk mendapatkan kepastian sepenuhnya. Namun ingat bahawa kaedah ini agak mengambil masa.
- **Tetapan imbasan tambahan** - pautan membuka dialog **Tetapan imbasan tambahan** di mana anda boleh menentukan parameter berikut:



- **Opsyen mematikan komputer** - menentukan sama ada komputer patut dimatikan secara automatik sebaik saja proses pengimbasan selesai. Dengan mengesahkan opsyen ini (**Matikan komputer apabila imbasan selesai**), pengaktifan opsyen baru membenarkan komputer dimatikan walaupun jika ia sedang dikunci (**Paksa untuk dimatikan jika komputer dikunci**).
- **Tentukan jenis fail untuk pengimbasan** - seterusnya, anda harus menentukan sama ada anda hendak ia diimbas:
 - **Semua jenis fail** dengan kemungkinan bagi pengecualian yang ditakrifkan daripada pengimbasan dengan memberikan senarai pemanjangan fail yang dipisahkan oleh koma yang tidak harus diimbas;

- **Jenis fail yang dipilih** - anda boleh menentukan bahawa anda hendak mengimbas hanya fail yang berkemungkinan dijangkiti (*fail yang tidak boleh dijangkiti tidak akan diimbas, contohnya sesetengah fail teks biasa atau sesetengah fail bukan boleh laku*), termasuk fail media (*video, fail audio - jika anda membiarkan kotak in tidak ditandakan, ia akan mengurangkan lebih banyak masa kerana fail ini biasanya agak besar dan agak tidak berkemungkinan dijangkiti virus*). Sekali lagi, anda boleh menentukan sambungan fail mana yang sepatutnya sentiasa diimbas.
- Secara pilihan, anda boleh menentukan anda hendak **Mengimbas fail tanpa sambungan** - opsyen ini dihidupkan secara lalai dan ia disyorkan untuk anda mengekalkannya melainkan anda mempunyai sebab sebenar untuk mengubahnya. Fail tanpa sambungan adalah lebih mencurigakan dan sepatutnya diimbas setiap masa.
- **Imbas keutamaan proses** - anda boleh menggunakan gelongsor untuk mengubah keutamaan proses imbasan. Secara lalai, nilai opsyen ini ditetapkan kepada tahap *sensitif pengguna* bagi penggunaan sumber automatik. Secara alternatif, anda boleh menjalankan proses pengimbasan dengan lebih perlahan yang bermaksud muat sumber sistem akan diminimumkan (*berguna apabila anda perlu bekerja pada komputer tetapi anda tidak berapa kisah berapa lama imbasan berlaku*), atau lebih cepat dengan keperluan sumber sistem yang ditingkatkan (*cth. apabila komputer tidak digunakan sementara*).
- **Tetapkan laporan imbasan tambahan** - pautan membuka dialog **Imbas Laporan** di mana anda boleh memilih apakah jenis kemungkinan penemuan yang harus dilaporkan:

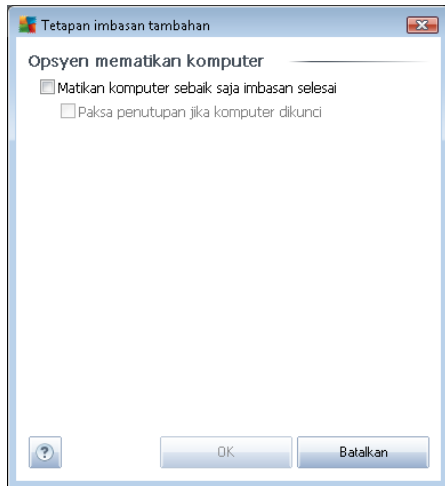


Amaran: Tetapan imbasan ini adalah sama dengan parameter bagi imbasan yang baru ditakrifkan - seperti yang diterangkan dalam bab [Pengimbasan AVG / Penjadualan imbasan / Cara untuk Mengimbas](#). Sekiranya anda hendak memutuskan untuk mengubah konfigurasi lalai bagi **Imbas fail atau folder tertentu** kemudian, anda boleh menyimpan tetapan baru anda sebagai konfigurasi lalai untuk digunakan untuk semua imbasan selanjutnya bagi fail atau folder tertentu. Serta, konfigurasi ini akan digunakan sebagai templat untuk semua imbasan yang baru dijadualkan ([semua imbasan yang dijadualkan adalah berdasarkan pada konfigurasi semasa Imbasan fail atau folder yang dipilih](#)).

10.2.3. Imbasan AntiRootkit

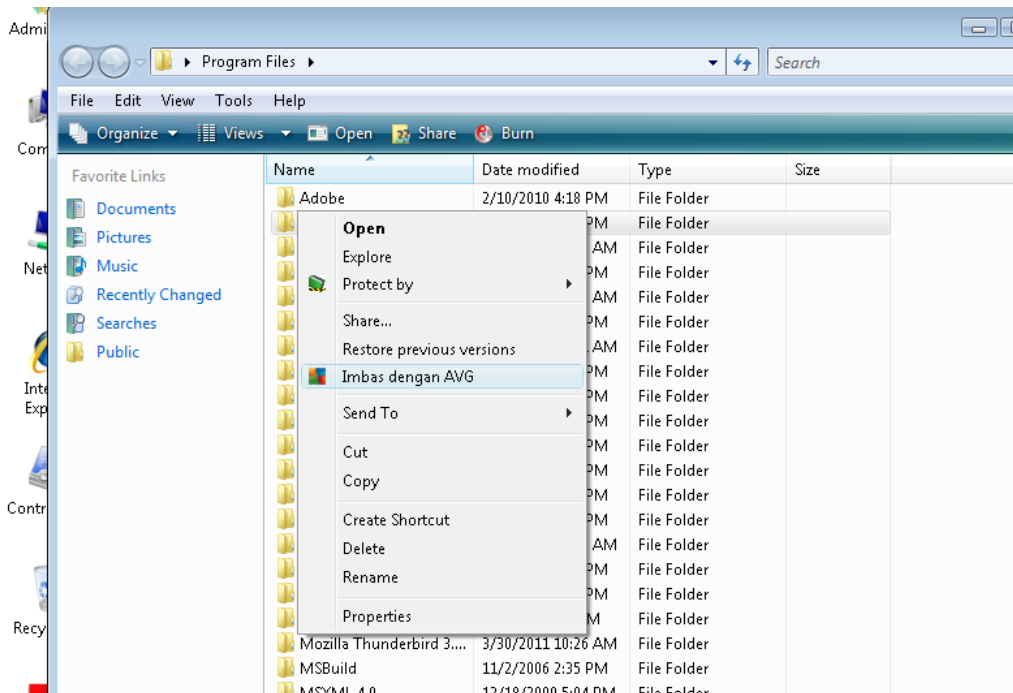
Imbasan AntiRootkit mencari komputer anda untuk kemungkinan rootkit (*atur cara dan teknologi yang boleh menutupi aktiviti malware dalam komputer anda*). Jika rootkit dikesan, ini tidak semestinya bermaksud komputer anda dijangkiti. Dalam sesetengah kes, pemacu atau bahagian tertentu aplikasi biasa mungkin telah mengesan rootkit dengan salah.

berkemungkinan **Paksa matikan jika komputer dikunci**):



10.3. Pengimbasan dalam Windows Explorer

Selain daripada imbasan dipratakrif yang dilancarkan untuk seluruh komputer atau kawasannya yang dipilih, **AVG Anti-Virus 2011** juga menawarkan pilihan bagi pengimbasan pantas bagi objek khusus secara terus dalam persekitaran Windows Explorer. Jika anda ingin membuka fail yang tidak diketahui dan anda tidak pasti mengenai kandungannya, anda mungkin mahu memeriksa dengan permintaan. Ikuti langkah-langkah ini:



- Dalam Windows Explorer, serlahkan fail (atau folder) yang anda hendak periksa



- Klik kanan tetikus anda pada objek untuk membuka menu konteks
- Pilih opsiyen **Imbas dengan AVG** supaya fail diimbis dengan AVG

10.4. Pengimbasan Garis Perintah

Dalam **AVG Anti-Virus 2011** terdapat pilihan bagi menjalankan imbasan daripada baris arahan. Anda boleh menggunakan opsiyen ini contohnya pada pelayan atau semasa membuat skrip kelompok untuk dilancarkan secara automatik selepas but komputer. Daripada baris arahan, anda boleh melancarkan pengimbasan dengan paling banyak parameter yang ditawarkan dalam antara muka pengguna grafik AVG.

Untuk melancarkan imbasan AVG daripada baris arahan, jalankan arahan berikut dalam folder di mana AVG dipasang.

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

Sintaks arahan

Sintaks arahan berikut:

- **avgscanx /parameter** ... cth. **avgscanx /comp** untuk pengimbasan seluruh komputer
- **avgscanx /parameter /parameter** .. dengan parameter berbilang, ini harus digariskan dalam barisan dan dipisahkan dengan ruang dan aksara garis condong
- jika parameter memerlukan nilai khusus untuk diberikan (cth. **/parameter** imbasan yang memerlukan maklumat mengenai apa kawasan apa yang dipilih pada komputer anda yang akan diimbis dan anda perlu memberikan laluan sebenar kepada bahagian yang dipilih), nilai dibahagikan melalui koma bertitik, contohnya: **avgscanx /scan=C:\;D:**

Parameter imbasan

Untuk memaparkan gambaran keseluruhan parameter sedia ada, taipkan arahan masing-masing bersama-sama parameter **/?** atau **/HELP** (cth. **avgscanx /?**). Satu-satunya parameter wajib adalah **/SCAN** untuk menentukan bahagian komputer yang harus diimbis. Untuk penerangan terperinci tentang opsiyen, lihat [gambaran keseluruhan parameter garis arahan](#).

Untuk menjalankan imbasan, tekan **Enter**. Semasa pengimbasan anda boleh menghentikan proses dengan **Ctrl+C** atau **Ctrl+Pause**.

Pengimbasan CMD dilancarkan dari antara muka grafik

Semasa anda menjalankan komputer anda dalam Windows Safe Mode, terdapat juga kemungkinan untuk melancarkan imbasan baris arahan daripada antara muka pengguna grafik. Imbasan itu sendiri



akan dilancarkan daripada baris arahan, dialog **Pengarang Baris Perintah** hanya membenarkan anda menentukan parameter pengimbasan paling banyak dalam antara muka grafik yang selesai.

Memandangkan dialog ini hanya boleh diakses dalam Windows Safe Mode, untuk penerangan terperinci bagi dialog ini, sila rujuk fail bantuan terbuka secara terus dari dialog.

10.4.1. Parameter Imbasan CMD

Sila cari senarai semua parameter yang tersedia berikut untuk pengimbasan baris arahan:

- **/SCAN** [Imbas fail atau folder tertentu](#) /SCAN=path;path (e.g. /SCAN=C:\;D:\)
- **/COMP** [Imbasan Seluruh Komputer](#)
- **/HEUR** Guna [analisis heuristik](#)
- **/EXCLUDE** Tidak termasuk laluan atau fail daripada imbasan
- **/@** Fail perintah /nama fail/
- **/EXT** Imbas sambungan ini/contohnya EXT=EXE,DLL/
- **/NOEXT** Jangan imbas sambungan ini /contohnya NOEXT=JPG/
- **/ARC** Imbas arkib
- **/CLEAN** Cuci secara automatik
- **/TRASH** Alihkan fail yang dijangkiti ke [Bilik Kebal Virus](#)
- **/QT** Ujian pantas
- **/MACROW** Laporkan makro
- **/PWDW** Laporkan fail yang dilindungi oleh kata laluan
- **/IGNLOCKED** Abaikan fail yang dikunci
- **/REPORT** Laporkan kepada fail /nama fail
- **/REPAPPEND** Lampirkan kepada fail laporan
- **/REPOK** Laporkan fail yang tidak dijangkiti sebagai OK
- **/NOBREAK** Jangan benarkan CTRL-BREAK dihenti paksa
- **/BOOT** Dayakan semakan MBR/BOOT
- **/PROC** Imbas proses aktif
- **/PUP** Laporkan "[Atur cara yang berkemungkinan tidak dikehendaki](#)"



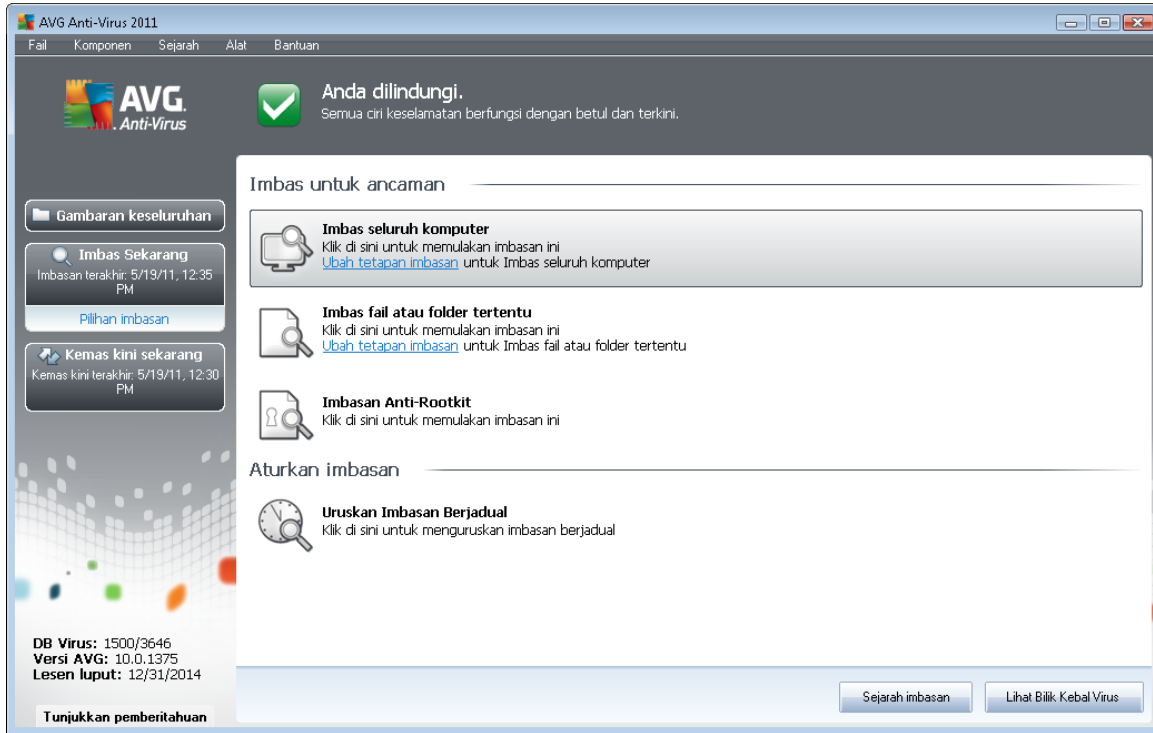
- **/REG** Imbas pendaftaran
- **/COO** Imbas kuki
- **/?** Memaparkan bantuan pada topik ini
- **/HELP** Paparkan bantuan pada topik ini
- **/PRIORITY** Tetapkan keutamaan imbasan /Rendah, Auto, Tinggi/ (lihat [Tetapan / Imbasan lanjutan](#))
- **/SHUTDOWN** Mematikan komputer apabila imbasan selesai
- **/FORCESHUTDOWN** Paksa komputer dimatikan apabila imbasan selesai
- **/ADS** Imbas Aliran Data Berganti-ganti (NTFS sahaja)
- **/ARCBOMBSW** Laporkan fail arkib yang dimampatkan semula

10.5. Penjadualan Imbasan

Dengan **AVG Anti-Virus 2011** anda boleh menjalankan imbasan dengan permintaan (contohnya, apabila anda mengesyaki jangkitan telah dibawa ke komputer anda) atau berasaskan perancangan yang dijadualkan. Ia amat disyorkan untuk menjalankan imbasan berdasarkan jadual: dengan cara ini, anda boleh memastikan komputer anda dilindungi dari sebarang kemungkinan daripada dijangkiti dan anda tidak perlu risau jika dan di mana untuk dilancarkan

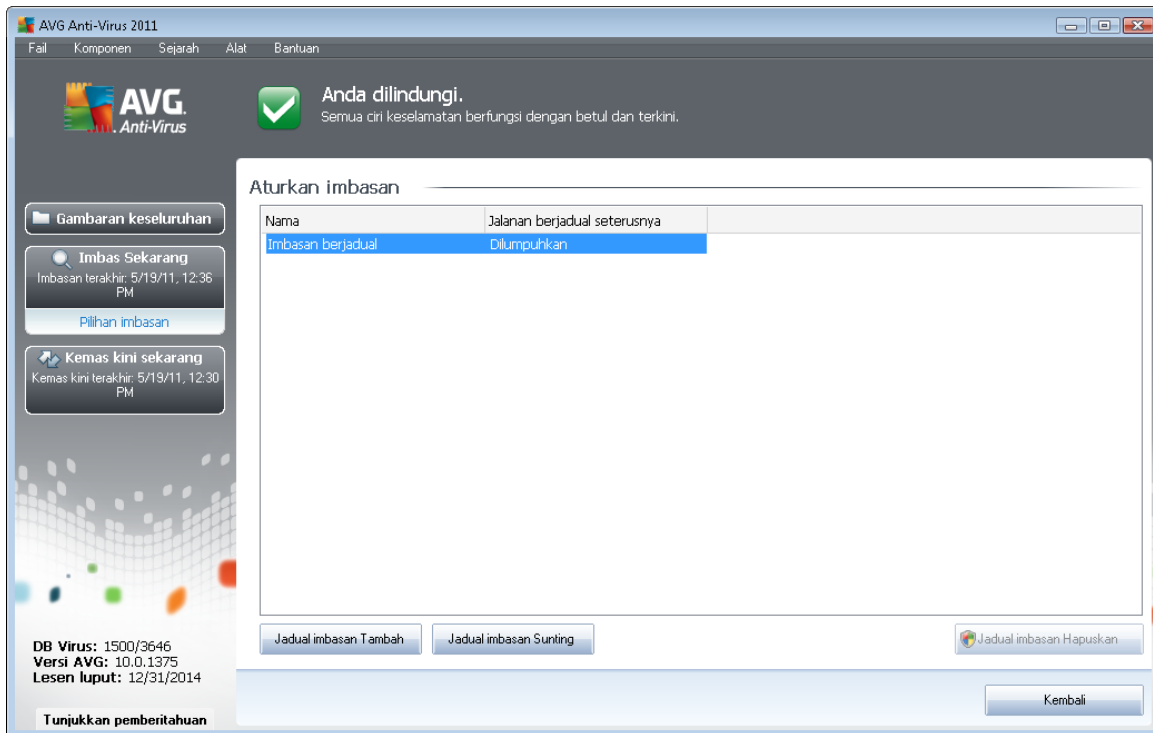
Anda harus melancarkan [imbasan Seluruh komputer](#) secara tetap, sekurang-kurangnya sekali seminggu. Walau bagaimanapun, jika boleh, lancarkan imbasan keseluruhan komputer anda setiap hari - seperti yang disediakan dalam konfigurasi lalai jadual imbasan. Jika komputer "sentiasa dihidupkan", kemudian, anda boleh menjadualkan imbasan di luar waktu bekerja. Jika komputer kadangkala dimatikan, kemudian, imbasan yang dijadualkan untuk berlaku [pada permulaan komputer semasa tugas telah terlepas](#).

Untuk membuat jadual imbasan baru, lihat [antara muka imbasan AVG](#) dan cari bahagian bawah yang dipanggil **Jadualkan imbasan**:



Jadualkan imbasan

Klik ikon grafik dalam bahagian **Jadualkan imbasan** untuk membuka dialog **Jadualkan imbasan** di mana anda menemui senarai semua imbasan yang sedang dijadualkan:

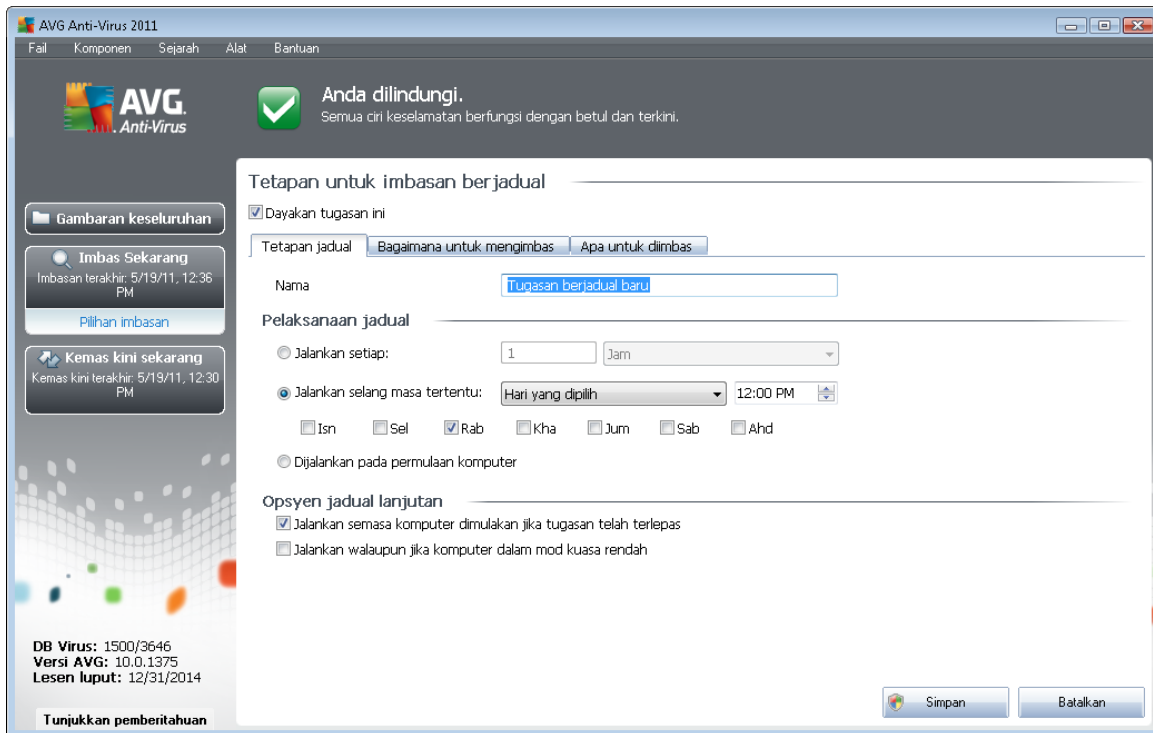


Anda boleh mengedit / menambah imbasan menggunakan butang kawalan berikut:

- **Tambah jadual imbasan** - butang tersebut membuka dialog **Tetapan untuk imbasan yang dijadualkan**, tab **Jadualkan tetapan**. Dalam dialog ini, anda boleh menentukan parameter bagi ujian yang baru ditakrifkan.
- **Edit jadual imbasan** - butang ini hanya boleh digunakan jika sebelum ini, anda telah memilih ujian sedia ada dari senarai ujian yang dijadualkan. Dalam keadaan tersebut, butang menjadi aktif dan anda boleh mengkliknya untuk beralih ke dialog **Tetapan untuk imbasan yang dijadualkan**, tab **Tetapan jadual**. Parameter bagi ujian yang dipilih telah ditentukan di sini dan boleh diedit.
- **Padam jadual imbasan** - butang ini juga aktif jika sebelum ini, anda telah memilih ujian sedia ada dari senarai ujian yang dijadualkan. Kemudian, ujian ini boleh dipadamkan dari senarai dengan menekan butang kawalan. Walau bagaimanapun, anda boleh membuang ujian anda sendiri; **Jadual imbasan seluruh komputer** yang dipraktikkan dalam tetapan lalai tidak boleh dipadam.
- **Kembali** - kembali ke [antara muka pengimbasan AVG](#)

10.5.1. Tetapan Jadual

Jika anda mahu menjadualkan ujian baru dan pelancaran tetapnya, masuk ke dialog **Tetapan untuk ujian yang dijadualkan** (klik butang **Tambah jadual imbasan** dalam dialog **Jadualkan imbasan**). Dialog ini dibahagikan ke dalam tiga tab: **Tetapan jadual** - lihat gambar di bawah (tab lalai yang anda akan diarahkan semula secara automatik ke), **Bagaimana untuk mengimbas** dan **Apa yang hendak diimbas**.



Pada tab **Jadualkan tetapan** anda boleh menanda/menyahtandakan dahulu item **Dayakan tugas ini** untuk menyahaktifkan ujian yang dijadualkan buat sementara dan menghidupkannya semua apabila perlu.

Seterusnya, berikan nama kepada imbasan yang anda akan buat dan jadualkan. Taipkan nama dalam medan teks dengan item **Nama**. Cuba gunakan nama yang ringkas, deskriptif dan sesuai untuk imbasan untuk membuatkan ia mudah untuk mengenal pasti imbasan dari yang lain.

Contoh: Ia tidak sesuai untuk memanggil imbasan dengan nama "Imbasan baru" atau "Imbasan saya" memandangkan nama ini tidak merujuk kepada apa yang sebenarnya imbasan periksa. Sebaliknya, contoh nama deskriptif adalah "Imbasan kawasan sistem" dll. Serta, tidak perlu untuk menentukan jika nama imbasan sama ada ia adalah imbasan seluruh komputer atau hanya imbasan fail atau folder yang dipilih - imbasan anda sendiri yang akan sentiasa menjadi versi khusus bagi imbasan bagi fail atau folder yang dipilih.

Di dalam dialog ini anda boleh menentukan lebih lanjut parameter imbasan yang berikut:

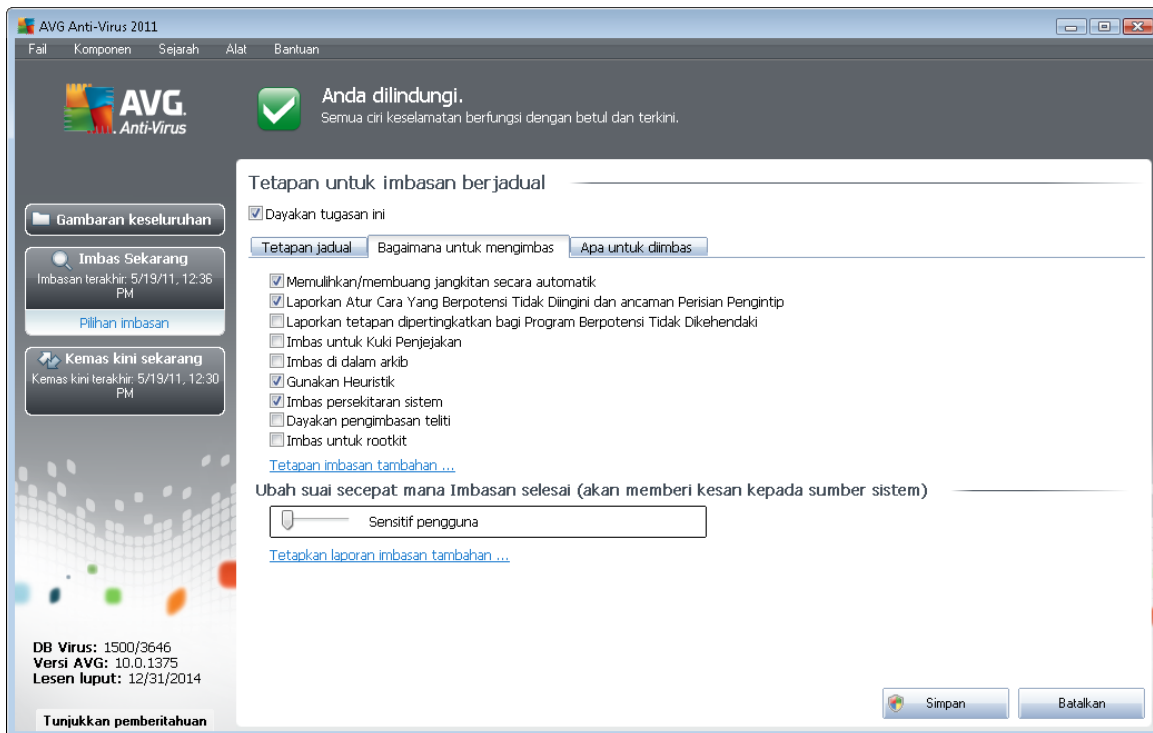
- **Jadualkan untuk dijalankan** - tentukan selang masa untuk pelancaran imbasan yang baru dijadualkan. Pemasaan boleh menjadi sama ada ditentukan oleh pelancaran imbasan berulang selepas satu tempoh masa tertentu (**Jalankan setiap ...**) atau dengan menentukan tarikh dan masa sebenar (**Jalankan dalam masa tertentu ...**), atau berkemungkinan dengan menentukan peristiwa yang pelancaran imbasan harus dikaitkan (**Tindakan berdasarkan pada permulaan komputer**).
- **Opsyen jadual lanjutan** - bahagian ini membenarkan anda menentukan di bawah syarat mana imbasan harus/tidak harus dilancarkan jika komputer berada dalam mod kuasa rendah atau dimatikan sepenuhnya.

Butang kawalan Tetap untuk dialog imbasan berjadual

Terdapat dua butang kawalan yang tersedia pada semua ketiga-tiga tab dialog **Tetapan untuk imbasan yang dijadualkan** (**Jadualkan tetapan**, [Cara untuk mengimbas](#) dan [Apa yang hendak diimbas](#)) dan ini mempunyai kefungsiian yang sama tidak kira pada tab mana yang anda sedang berada:

- **Simpan** - menyimpan semua perubahan yang anda telah lakukan pada tab ini atau pada sebarang tab lain bagi dialog ini dan beralih semula ke [dialog lalai antara muka pengimbasan AVG](#). Oleh itu jika anda ingin mengkonfigurasi parameter ujian pada semua tab, tekan butang untuk menyimpan ia hanya selepas anda telah menyatakan semua keperluan anda.
- **Batal** - membatalkan sebarang perubahan yang anda telah lakukan pada tab ini atau pada sebarang tab lain bagi dialog ini dan beralih semula ke [dialog lalai antara muka pengimbasan AVG](#).

10.5.2. Bagaimana untuk Mengimbas



Pada tab **Cara untuk mengimbas** anda akan menemui senarai parameter pengimbasan yang boleh dihidupkan/dimatikan secara pilihan. Secara lalai, kebanyakan parameter dibuka dan kefungsiannya akan dilaksanakan semasa pengimbasan. Melainkan anda mempunyai alasan yang sah untuk mengubah tetapan ini, kami menyarankan untuk mengekalkan konfigurasi dipraktakrif:

- **Pulih/buang jangkitan secara automatik (dibuka secara lalai)**: jika virus dikenal pasti sewaktu imbasan, ia boleh dipulihkan secara automatik jika rawatan tersedia. Jika fail yang

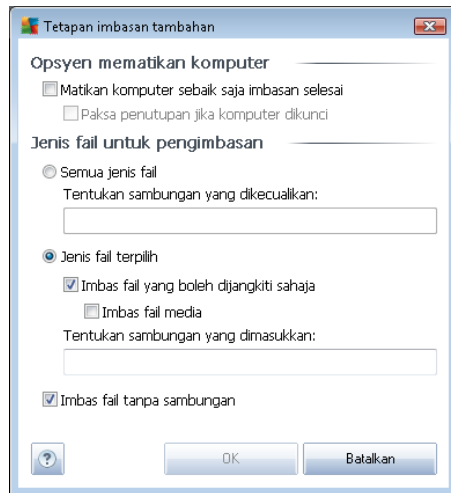


dijangkiti tidak boleh dipulihkan secara automatik atau jika anda memutuskan untuk mematikan pilihan ini, anda akan diberitahu mengenai pengesanan virus dan perlu memutuskan apa yang perlu dilakukan dengan jangkitan yang dikesan. Tindakan yang disarankan adalah untuk membuang fail yang dijangkiti ke [Bilik Kebal Virus](#).

- **Laporkan Atur Cara yang Berpotensi Tidak Diingini dan ancaman Perisian Pengintip (dibuka secara lalai):** tandakan untuk mengaktifkan enjin [AntiPerisian Pengintip](#), dan imbas untuk perisian pengintip serta virus. [Perisian pengintip mewakili kategori malware yang dipersoalkan, walaupun, ia biasanya mewakili risiko keselamatan, sesetengah atur cara ini boleh dipasang dengan niat.](#) Kami mengesyorkan untuk mengekalkan ciri ini diaktifkan kerana ia meningkatkan keselamatan komputer anda.
- **Laporkan set dipertingkatkan bagi Atur Cara yang Berpotensi Tidak Diingini (ditutup secara lalai):** tandakan untuk mengesan pakej yang diluaskan bagi [perisian pengintip](#): atur cara yang sangat ok dan tidak berbahaya apabila diperoleh daripada pengilang secara terus, tetapi, boleh disalahgunakan untuk tujuan berniat jahat selepas itu. Ini adalah langkah tambahan yang meningkatkan keselamatan komputer anda dengan lebih lagi, walau bagaimanapun, ia boleh menyekat atur cara sah dan oleh itu, dimatikan secara lalai.
- **Imbas untuk Kuki Penjejakan (ditutup secara lalai):** parameter ini bagi komponen [AntiPerisian Pengintip](#) mentakrifkan bahawa kuki harus dikesan sewaktu imbasan (*kuki HTTP digunakan untuk mengesahkan, menjejaki dan mengekalkan maklumat tertentu mengenai pengguna seperti keutamaan tapak atau kandungan kart beli-belah elektronik mereka*).
- **Imbas dalam arkib (ditutup secara lalai):** parameter ini mentakrifkan bahawa pengimbasan harus memeriksa semua fail walaupun jika ia dibungkus dalam sejenis arkib, cth. ZIP, RAR, ...
- **Gunakan Heuristik (dibuka secara lalai):** analisis heuristik (*perlagakan dinamik bagi arahan objek yang diimbas dalam persekitaran komputer maya*) akan menjadi salah satu kaedah yang digunakan untuk pengesanan virus sewaktu imbasan.
- **Imbas persekitaran sistem (dibuka secara lalai):** imbasan juga akan memeriksa kawasan sistem komputer anda.
- **Dayakan pengimbasan terperinci (ditutup secara lalai)** - dalam situasi tertentu (*mengesyaki komputer anda dijangkiti*) anda boleh menandakan opsiyen ini untuk mengaktifkan algoritma pengimbasan yang paling terperinci yang akan mengimbas kawasan komputer anda yang tidak pernah dijangkiti, sekadar untuk memastikan sepenuhnya. Jangan lupa bahawa kaedah ini agak mengambil masa.

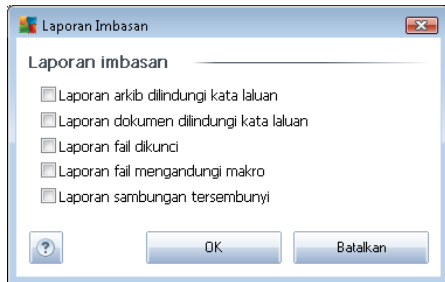
Kemudian, anda boleh mengubah konfigurasi imbasan seperti berikut:

- **Tetapan imbasan tambahan** - pautan membuka dialog **Tetapan imbasan tambahan** di mana anda boleh menentukan parameter berikut:



- **Opsyen mematikan komputer** - menentukan sama ada komputer patut dimatikan secara automatik sebaik saja proses pengimbasan selesai. Dengan mengesahkan opsyen ini (**Matikan komputer apabila imbasan selesai**), pengaktifan opsyen baru membenarkan komputer dimatikan walaupun jika ia sedang dikunci (**Paksa untuk dimatikan jika komputer dikunci**).
- **Tentukan jenis fail untuk pengimbasan** - seterusnya, anda harus menentukan sama ada anda hendak ia diimbas:
 - **Semua jenis fail** dengan kemungkinan bagi menentukan pengecualian daripada pengimbasan dengan memberikan senarai pemanjangan fail yang dipisahkan oleh koma yang tidak seharusnya diimbas;
 - **Jenis fail yang dipilih** - anda boleh menentukan bahawa anda hendak mengimbas hanya fail yang berkemungkinan dijangkiti (*fail yang tidak boleh dijangkiti tidak akan diimbas, contohnya sesetengah fail teks biasa atau sesetengah fail bukan boleh laku*), termasuk fail media (*video, fail audio - jika anda membiarkan kotak in tidak ditandakan, ia akan mengurangkan lebih banyak masa kerana fail ini biasanya agak besar dan agak tidak berkemungkinan dijangkiti virus*). Sekali lagi, anda boleh menentukan sambungan fail mana yang sepatutnya sentiasa diimbas.
 - Secara pilihan, anda boleh menentukan anda hendak **Mengimbas fail tanpa sambungan** - opsyen ini dihidupkan secara lalai dan ia disyorkan untuk anda mengekalkannya melainkan anda mempunyai sebab sebenar untuk mengubahnya. Fail tanpa sambungan adalah lebih mencurigakan dan sepatutnya diimbas setiap masa.
- **Laraskan berapa pantas Imbasan selesai** - anda boleh menggunakan penggelongsor untuk menukar prioriti proses imbasan. Secara lalai, nilai opsyen ini ditetapkan kepada tahap *sensitif pengguna* bagi penggunaan sumber automatik. Secara alternatif, anda boleh menjalankan proses pengimbasan dengan lebih perlahan yang bermaksud muat sumber sistem akan diminimumkan (*berguna apabila anda perlu bekerja pada komputer tetapi anda tidak berapa kisah berapa lama imbasan berlaku*), atau lebih cepat dengan keperluan sumber sistem yang ditingkatkan (*cth. apabila komputer tidak digunakan sementara*).

- **Tetapkan laporan imbasan tambahan** - pautan membuka dialog **Imbas laporan** di mana anda boleh memilih jenis kemungkinan penemuan yang harus dilaporkan:



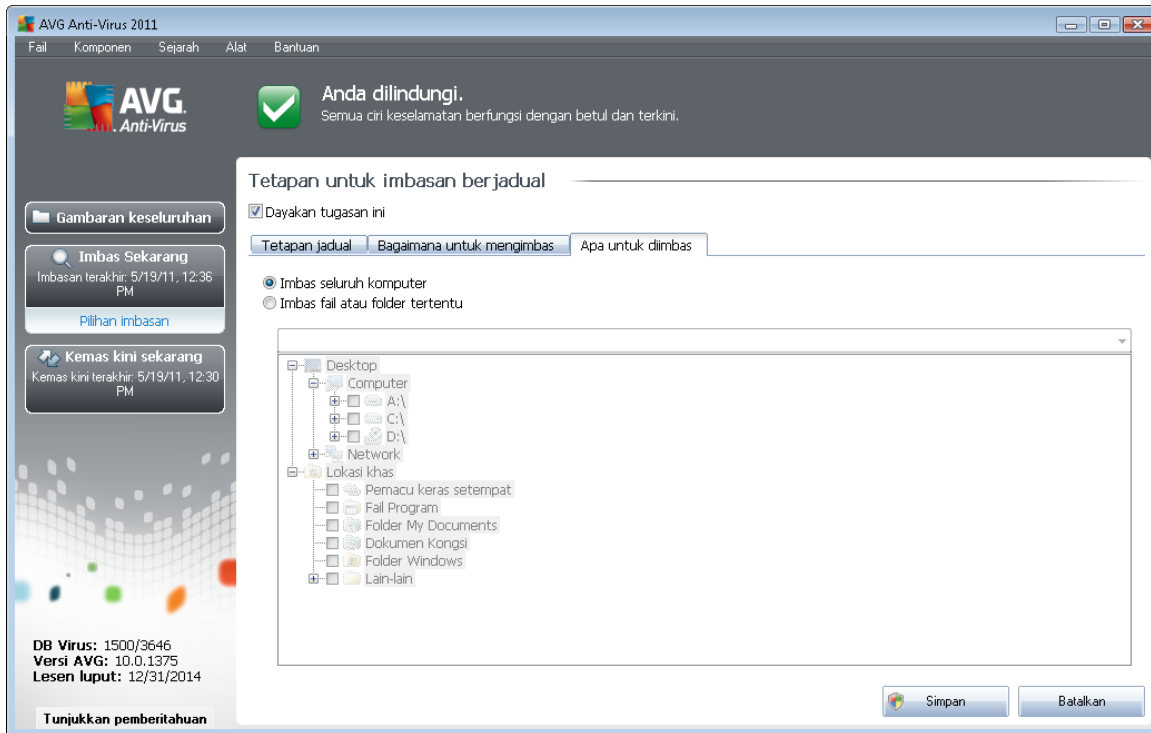
Nota: Secara lalai, konfigurasi pengimbasan disediakan untuk prestasi optimum. Melainkan, anda mempunyai alasan yang sah untuk mengubah tetapan pengimbasan, ia sangat disyorkan untuk kekal dengan konfigurasi yang dipraktakrif. Sebarang perubahan konfigurasi sepatutnya dilakukan oleh pengguna berpengalaman sahaja. Untuk opsyen pengimbasan selanjutnya, lihat dialog [tetapan Lanjutan](#) yang boleh diakses melalui item menu sistem **tetapan Fail / Lanjutan** .

Butang kawalan

Ini adalah dua butang kawalan yang tersedia pada semua ketiga-tiga tab bagi dialog **Tetapan untuk imbasan berjadual** ([Tetapan jadual](#), [Cara untuk mengimbas](#) dan [Apa yang hendak diimbas](#)) dan ini mempunyai kefungsiian yang sama tidak kira tab mana yang anda gunakan:

- **Simpan** - menyimpan semua perubahan yang anda telah lakukan pada tab ini atau pada sebarang tab lain bagi dialog ini dan beralih semula ke [dialog lalai antara muka pengimbasan AVG](#). Oleh itu jika anda ingin mengkonfigurasikan parameter ujian pada semua tab, tekan butang untuk menyimpan ia hanya selepas anda telah menyatakan semua keperluan anda.
- **Batalkan** - membatalkan sebarang perubahan yang anda telah lakukan pada tab ini atau pada sebarang tab lain bagi dialog ini dan beralih semula ke [dialog lalai antara muka pengimbasan AVG](#).

10.5.3. Apa untuk Diimbas



Pada tab ***Apa yang hendak diimbas*** anda boleh menentukan sama ada anda mahu menjadualkan [pengimbasan seluruh komputer](#) atau [pengimbasan fail atau folder tertentu](#).

Jika anda memilih pengimbasan bagi fail atau folder tertentu, di bahagian bawah dialog, struktur pepohon yang dipaparkan mengaktifkan dan anda boleh menentukan folder untuk diimbas (*perluaskan item dengan mengklik nod tambah sehingga anda menemui folder yang anda hendak imbas*). Anda boleh memilih berbilang folder dengan mengklik pada kotak berkaitan. Folder yang dipilih akan muncul dalam medan teks di bahagian atas dialog, dan menu jatuh bawah akan menyimpan sejarah imbasan terpilih anda untuk kegunaan nanti. Secara alternatif, anda boleh memasukkan laluan penuh ke folder yang diingini secara manual (*jika anda masukkan berbilang laluan, adalah perlu untuk memisahkannya dengan koma bertindih tanpa ruang tambahan*).

Dalam struktur pepohon, anda juga boleh melihat dahan yang dipanggil **Lokasi khas**. Berikut, cari senarai lokasi yang akan diimbas sebaik sahaja kotak semakan masing-masing ditanda:

- **Pemacu keras tempatan** - semua pemacu keras bagi komputer anda
- **Fail Atur cara**
 - C:\Program Files\
 - dalam versi 64-bit C:\Program Files (x86)
- **Folder My Documents**



- o untuk Win XP: C:\Documents and Settings\Default User\My Documents\
- o untuk Windows Vista/7: C:\Users\user\Documents\

- **Dokumen Kongsi**

- o untuk Win XP: C:\Documents and Settings\All Users\Documents\
- o untuk Windows Vista/7: C:\Users\Public\Documents\

- **Folder Windows** - C:\Windows\

- **Lain-lain**

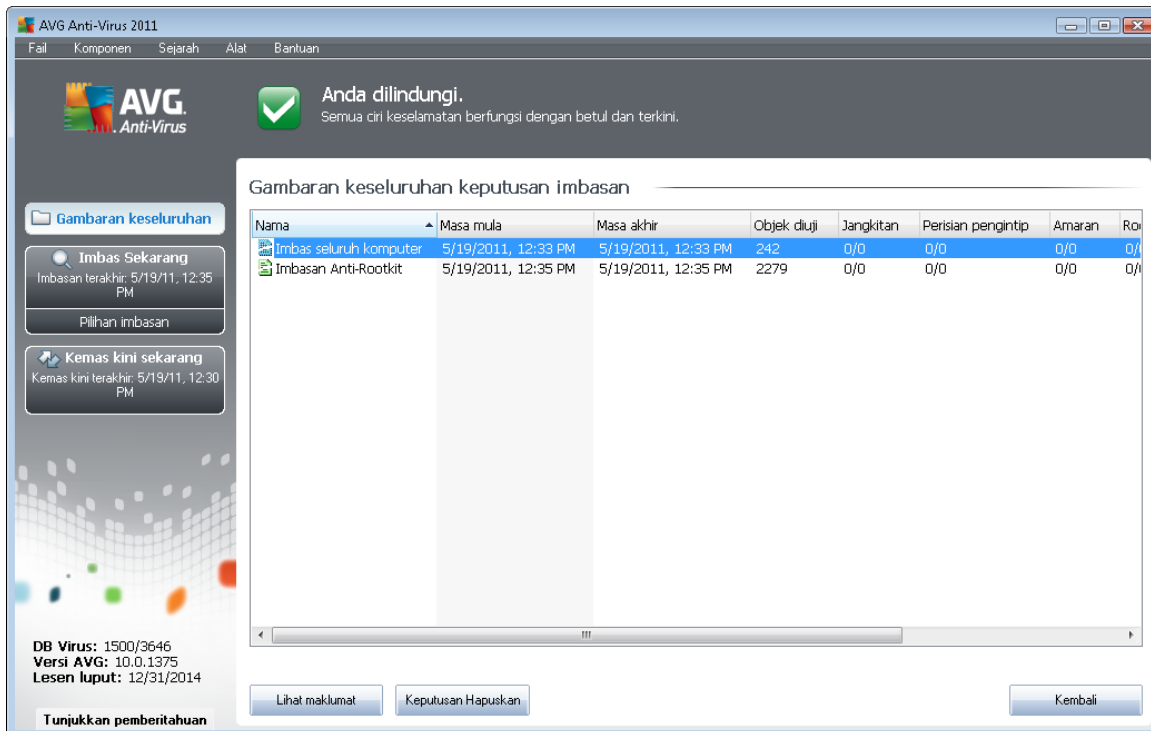
- o *Pemacu sistem* - pemacu keras di mana sistem pengendalian dipasang (biasanya C:)
- o *Folder sistem* - C:\Windows\System32\
- o *Folder Fail Sementara* - C:\Documents and Settings\User\Local\ (Windows XP); atau C:\Users\user\AppData\Local\Temp\ (Windows Vista/7)
- o *Fail Internet Sementara* - C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (Windows XP); atau C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (Windows Vista/7)

Butang kawalan Tetap untuk dialog imbasan berjadual

Terdapat dua butang kawalan yang tersedia pada semua ketiga-tiga tab dialog **Tetapan untuk imbasan yang dijadualkan** ([Jadualkan tetapan](#), [Cara untuk mengimbasi](#) dan [Apa yang hendak diimbasi](#)) dan ini mempunyai kefungsiannya yang sama tidak kira pada tab mana yang anda sedang berada:

- **Simpan** - menyimpan semua perubahan yang anda telah lakukan pada tab ini atau pada sebarang tab lain bagi dialog ini dan beralih semula ke [dialog lalai antara muka pengimbasan AVG](#). Oleh itu jika anda ingin mengkonfigurasi parameter ujian pada semua tab, tekan butang untuk menyimpan ia hanya selepas anda telah menyatakan semua keperluan anda.
- **Batalkan** - membatalkan sebarang perubahan yang anda telah lakukan pada tab ini atau pada sebarang tab lain bagi dialog ini dan beralih semula ke [dialog lalai antara muka pengimbasan AVG](#).


10.6. Gambaran Keseluruhan Keputusan Imbasan




Dialog **Imbas gambaran keseluruhan keputusan** boleh diakses dari [antara muka pengimbasan AVG](#) melalui butang **Imbas sejarah**. Dialog memberikan senarai semua imbasan yang dilancarkan sebelum ini dan maklumat keputusannya:

- **Nama** - imbas pelantikan; ia boleh jadi sama ada nama salah satu [imbasan yang dipratetap](#) atau nama yang anda telah berikan kepada [imbasan anda yang dijadualkan sendiri](#). Setiap nama termasuk ikon yang menunjukkan keputusan imbasan:

 - ikon hijau memberitahu tiada jangkitan yang dikesan sewaktu imbasan

 - ikon biru mengumumkan terdapat jangkitan dikesan sewaktu imbasan tetapi objek yang dikesan dibuang secara automatik

 - ikon merah memberi amaran terdapat jangkitan dikesan sewaktu imbasan dan ia tidak boleh dibuang!

Setiap ikon boleh menjadi sama ada tegar atau dipotong separuh - ikon tegar adalah untuk imbasan yang telah selesai dan yang diselesaikan dengan betul; ikon yang dipotong separuh bermaksud imbasan telah dibatalkan atau diganggu.

Nota: Untuk maklumat terperinci mengenai setiap imbasan, sila lihat dialog [Keputusan Imbasan](#) yang boleh diakses melalui butang **Lihat butiran** (di bahagian bawah dialog ini).

- **Masa mula** - tarikh dan masa semasa imbasan dilancarkan



- **Masa tamat** - tarikh dan masa imbasan ditamatkan
- **Objek yang diuji** - bilangan objek yang diperiksa sewaktu imbasan
- **Jangkitan** - bilangan [jangkitan virus](#) yang dikesan / dibuang
- **Perisian pengintip** - bilangan [perisian pengintip](#) yang dikesan / dibuang
- **Amaran** - bilangan [objek mencurigakan](#)
- **Rootkit** - bilangan [rootkit](#)
- **Imbas maklumat log** - maklumat berkaitan dengan tempoh imbasan dan keputusan (biasanya pada penyelesaian atau gangguan)

Butang kawalan

Butang kawalan untuk dialog **Imbas gambaran keseluruhan hasil** adalah:

- **Lihat butiran** - tekannya untuk beralih ke dialog [Imbas keputusan](#) untuk melihat data terperinci bagi imbasan yang dipilih
- **Padam keputusan** - tekannya untuk membuang item yang dipilih daripada gambaran keseluruhan keputusan imbasan
- **Kembali** - mengalihkan semula ke dialog lalai bagi [antara muka imbasan AVG](#)

10.7. Butiran Keputusan Imbasan

Jika dalam dialog [Imbas Gambaran Keseluruhan Keputusan](#) imbasan tertentu dipilih, kemudian, anda boleh mengklik butang **Lihat butiran** untuk beralih ke dialog **Imbas Keputusan** yang memberikan data terperinci mengenai tempoh dan keputusan imbasan yang dipilih.

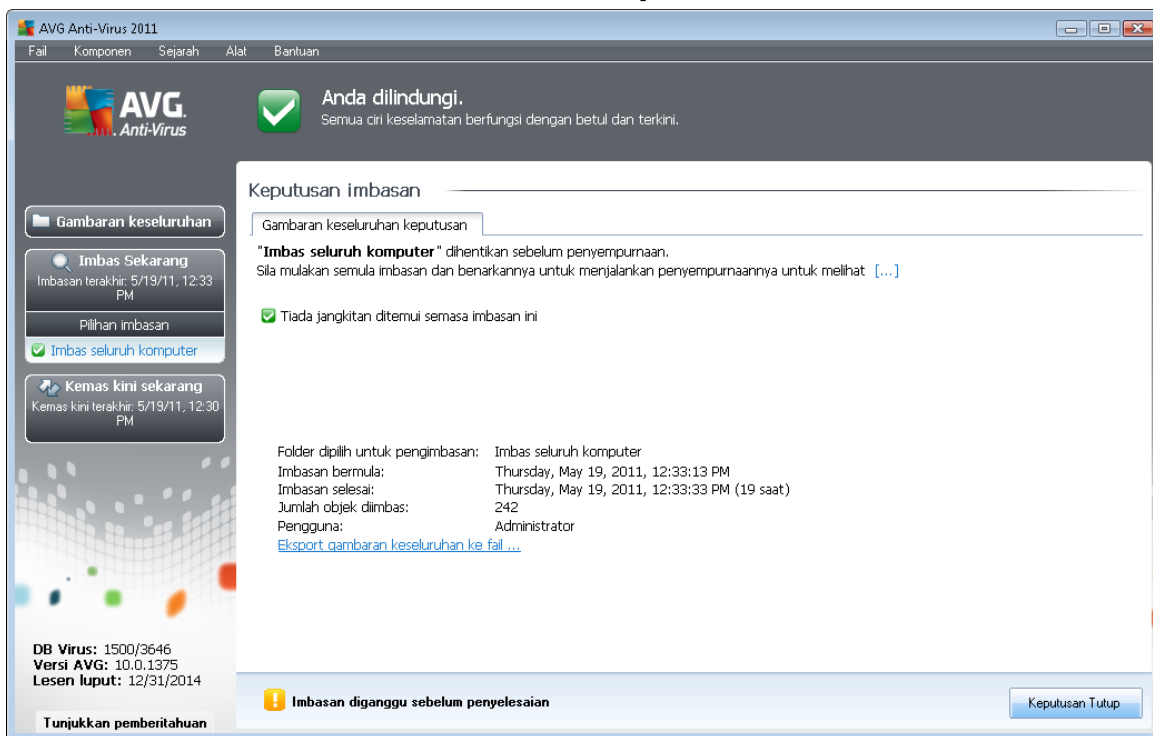
Dialog tersebut seterusnya dibahagikan ke dalam beberapa tab:

- [Gambaran Keseluruhan Keputusan](#) - tab ini dipaparkan pada setiap masa dan memberikan data statistik yang menerangkan perkembangan imbasan
- [Jangkitan](#) - tab ini dipaparkan hanya jika [jangkitan virus](#) dikesan sewaktu pengimbasan
- [Perisian pengintip](#) - tab ini dipaparkan hanya jika [perisian pengintip](#) dikesan sewaktu pengimbasan
- [Amaran](#) - tab ini dipaparkan sebagai contoh jika kuki dikesan sewaktu pengimbasan
- [Rootkit](#) - tab ini dipaparkan hanya jika [rootkit](#) dikesan sewaktu pengimbasan
- [Maklumat](#) - tab ini dipaparkan hanya jika beberapa kemungkinan ancaman dikesan tetapi ini tidak boleh diklasifikasikan sebagai mana-mana kategori di atas; kemudian, tab tersebut memberikan mesej amaran mengenai penemuan. Serta, anda akan menemui di sini



maklumat mengenai objek yang tidak boleh diimbas (cth. arkib yang dilindungi kata laluan).

10.7.1. Tab Gambaran Keseluruhan Keputusan



Pada tab **Imbas keputusan** anda boleh mendapatkan statistik terperinci dengan maklumat pada:

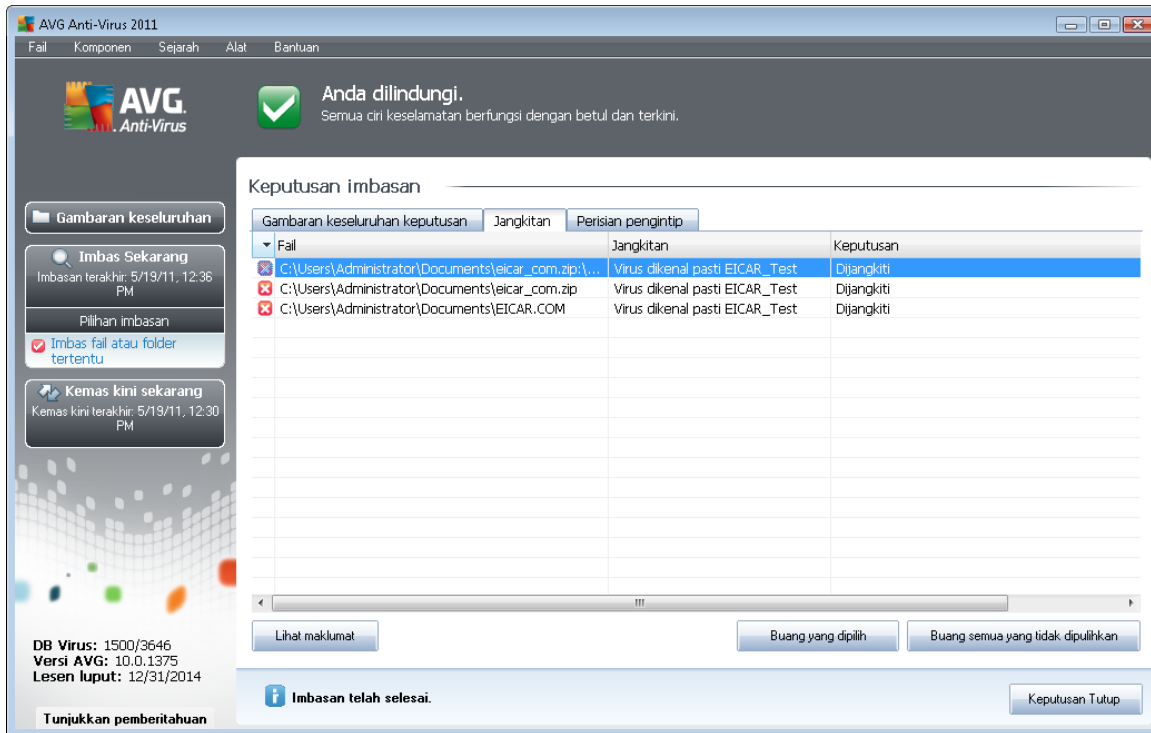
- [jangkitan virus](#) / [perisian pengintip yang dikesan](#)
- [jangkitan virus](#) / [perisian pengintip yang dibuang](#)
- bilangan [jangkitan virus](#) / [perisian pengintip](#) yang tidak boleh dibuang atau dipulihkan

Selain daripada itu, anda akan mendapat maklumat mengenai tarikh dan masa sebenar pelancaran imbasan, dengan jumlah bilangan objek yang diimbas, pada tempoh pengimbasan dan bilangan ralat yang berlaku sewaktu pengimbasan

Butang kawalan

Terdapat hanya satu butang kawalan yang tersedia dalam dialog ini. Butang **Tutup keputusan** kembali ke dialog [Imbas gambaran keseluruhan](#).

10.7.2. Tab Jangkitan



Tab **Jangkitan** hanya dipaparkan dalam dialog **Imbas keputusan** jika [jangkitan virus](#) dikesan sewaktu pengimbasan. Tab ini dibahagikan kepada tiga bahagian menyediakan maklumat berikut:

- **Fail** - laluan penuh ke lokasi asal bagi objek yang dijangkiti
- **Jangkitan** - nama bagi [virus](#) yang dikesan (*untuk butiran mengenai virus khusus, sila rujuk kepada [Ensiklopedia Virus](#) dalam talian*)
- **Keputusan** - mentakrifkan status terkini bagi objek yang dijangkiti yang dikesan sewaktu imbasan:
 - yang dijangkiti- objek yang dijangkiti dikesan dan ditinggalkan dalam lokasi asalnya (*contohnya, jika anda telah [mematikan opsyen pemulihan automatik](#) dalam tetapan imbasan khusus*)
 - yang dipulihkan- objek yang dikesan dipulihkan secara automatik dan ditinggalkan dalam lokasi asalnya
 - **Dialih ke Bilik Kebal Virus** - objek yang dijangkiti dialihkan ke kuarantin [Bilik Kebal Virus](#)
 - yang dipadamkan- objek yang dijangkiti dipadamkan
 - **Ditambah ke pengecualian PUP** - penemuan dinilai sebagai pengecualian dan ditambah kepada senarai pengecualian PUP (*dikonfigurasi dalam dialog*

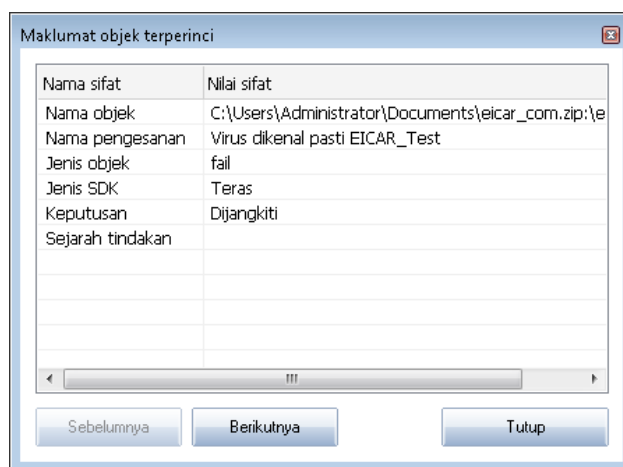
[Pengecualian PUP](#) bagi tetapan lanjutan)

- **Fail dikunci - tidak diuji** - objek tersebut dikunci dan oleh itu, AVG tidak dapat mengimbasnya
- **Berkemungkinan, objek berbahaya** - objek dikesan sebagai berkemungkinan berbahaya tetapi tidak dijangkiti (*sebagai contoh, ia boleh mengandungi*); maklumat harus diambil sebagai amaran sahaja
- **But semula diperlukan untuk menyelesaikan tindakan** - objek yang dijangkiti tidak boleh dibuang, untuk membuang sepenuhnya, anda perlu memulakan semula komputer anda

Butang kawalan

Terdapat tiga butang kawalan yang anda dalam dialog ini:

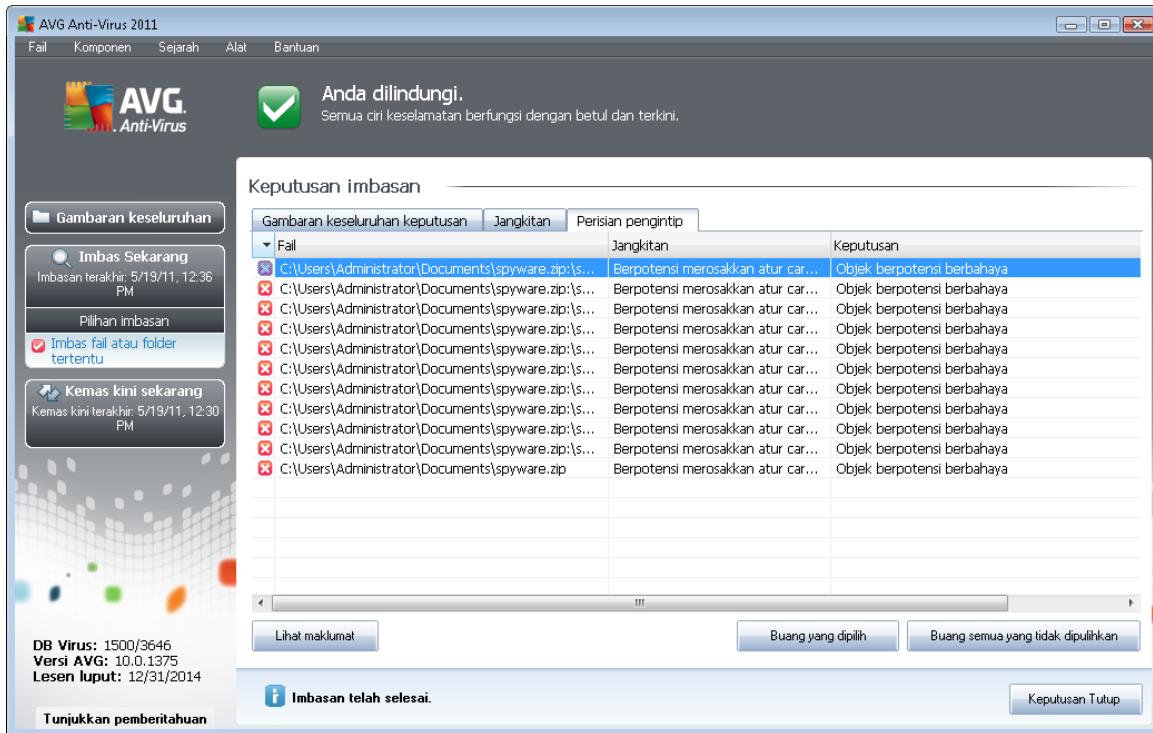
- **Lihat butiran**- butang ini membuka tettingkap dialog baru yang dinamakan **Maklumat objek terperinci**:



Dalam dialog ini anda boleh menemui maklumat terperinci mengenai objek boleh berjangkit yang dikesan (*cth. nama dan lokasi objek yang dijangkiti, jenis objek, jenis SDK, hasil pengesanan dan sejarah tindakan yang berkaitan dengan objek yang dikesan*). Menggunakan butang **Sebelumnya** / **Seterusnya** anda boleh melihat maklumat pada penemuan tertentu. Gunakan butang **Tutup** untuk menutup dialog ini.

- **Buang yang dipilih** - gunakan butang ini untuk mengalih penemuan yang dipilih ke [Bilik Kebal Virus](#)
- **Buang semua yang tidak dapat dipulihkan** - butang ini memadam semua penemuan yang tidak dapat dipulihkan atau dialihkan ke [Bilik Kebal Virus](#)
- **Tutup keputusan** - tamatkan gambaran keseluruhan maklumat terperinci dan kembali ke dialog [Imbas gambaran keseluruhan keputusan](#)

10.7.3. Tab Perisian Pengintip



Tab **Perisian Pengintip** hanya dipaparkan dalam dialog **Imbas keputusan** dalam [perisian pengintip](#) **jika** dikesan sewaktu imbasan. Tab ini dibahagikan kepada tiga bahagian menyediakan maklumat berikut:

- **Fail** - laluan penuh ke lokasi asal bagi objek yang dijangkiti
- **Jangkitan** - nama [perisian pengintip](#) (yang dikesan (*untuk butiran mengenai virus tertentu, sila rujuk [Ensiklopedia Virus](#)*) dalam talian
- **Keputusan** - mentakrif status objek semasa yang dikesan sewaktu imbasan:
 - dijangkiti - objek yang dijangkiti dikesan dan dibiarkan dalam lokasi asalnya (contohnya, jika anda telah [mematikan opsyen pemulihan automatik](#) dalam tetapan imbasan khusus)
 - yang dipulihkan- objek yang dikesan dipulihkan secara automatik dan ditinggalkan dalam lokasi asalnya
 - **Dialih ke Bilik Kebal Virus** - objek yang dijangkiti dialihkan ke kuarantin [Bilik Kebal Virus](#)
 - yang dipadamkan- objek yang dijangkiti dipadamkan
 - **Ditambah pada pengecualian PUP** - penemuan dinilai sebagai pengecualian dan ditambah pada senarai pengecualian PUP (*dikonfigurasi dalam dialog [Pengecualian](#)*)

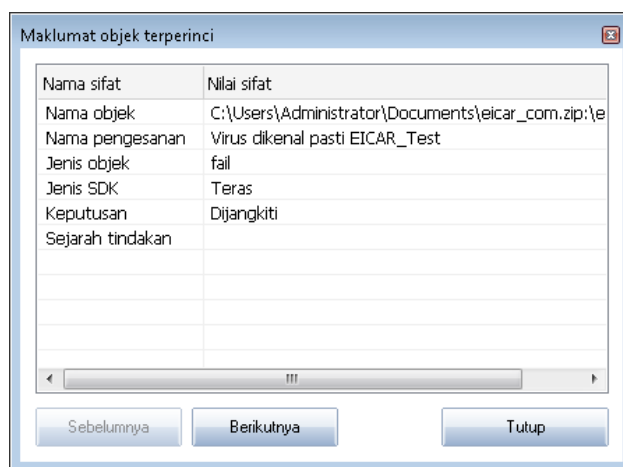
[PUP](#) bagi tetapan lanjutan)

- **Fail yang dikunci - tidak diuji** - objek masing-masing dikunci dan oleh sebab itu, AVG tidak dapat mengimbasnya
- **Objek berpotensi berbahaya** - objek dikesan sebagai berpotensi berbahaya tetapi tidak dijangkiti (sebagai contoh, ia boleh mengandungi makro); maklumat adalah hanya amaran
- **But semula diperlukan untuk menyelesaikan tindakan** - objek yang dijangkiti tidak boleh dibuang, untuk membuang sepenuhnya, anda perlu memulakan semula komputer anda

Butang kawalan

Terdapat tiga butang kawalan yang anda dalam dialog ini:

- **Lihat butiran**- butang ini membuka tettingkap dialog baru yang dinamakan **Maklumat objek terperinci**:



Dalam dialog ini anda boleh menemui maklumat terperinci mengenai objek boleh berjangkit yang dikesan (*cth. nama dan lokasi objek yang dijangkiti, jenis objek, jenis SDK, hasil pengesanan dan sejarah tindakan yang berkaitan dengan objek yang dikesan*). Menggunakan butang **Sebelumnya** / **Seterusnya** anda boleh melihat maklumat pada penemuan tertentu. Gunakan butang **Tutup** untuk meninggalkan dialog ini.

- **Buang yang dipilih** - gunakan butang ini untuk mengalih penemuan yang dipilih ke [Bilik Kebal Virus](#)
- **Buang semua jangkitan yang tidak dapat dipulihkan** - butang ini memadam semua penemuan yang tidak dapat dipulihkan atau dialihkan ke [Bilik Kebal Virus](#)
- **Tutup keputusan** - tamatkan gambaran keseluruhan maklumat terperinci dan kembali ke



dialog [Imbas gambaran keseluruhan keputusan](#)

10.7.4. Tab Amaran

Tab **Amaran** memaparkan maklumat pada objek yang "disyaki" (*biasanya fail*) yang dikesan sewaktu pengimbasan. Apabila dikesan oleh [Perisai Residen](#), fail ini disekat daripada diakses. Contoh biasa bagi jenis penemuan ini adalah: fail tersembunyi, kuki, kekunci pendaftaran yang disyaki, dokumen atau arkib yang dilindungi kata laluan, dll. Fail seperti itu tidak membawa sebarang ancaman terus kepada komputer atau keselamatan anda. Maklumat mengenai fail ini biasanya berguna jika terdapat adware atau perisian pengintip yang dikesan pada komputer anda. Jika hanya terdapat Amaran yang dikesan oleh ujian AVG, tiada tindakan yang diperlukan.

Ini adalah penerangan ringkas bagi contoh yang paling biasa bagi objek seperti itu:

- **Fail tersembunyi** - Fail tersembunyi adalah secara lalai tidak boleh dilihat dalam Windows, dan sesetengah virus atau ancaman lain mungkin cuba mengelakkan pengesanan dengan menyimpan failnya dengan atribut ini. Jika AVG anda melaporkan fail tersembunyi yang anda mengesyaki berniat jahat, anda boleh mengalihkannya ke [Bilik Kebal Virus](#) anda.
- **Kuki** - Kuki adalah fail teks biasa yang digunakan oleh tapak web untuk menyimpan maklumat khusus pengguna yang kemudiannya digunakan untuk memuat reka letak tapak web, prapengisian nama pengguna, dll.
- **Kekunci pendaftaran yang disyaki** - Sesetengah malware menyimpan maklumatnya ke dalam pendaftar Windows, untuk memastikan ia dimuat pada permulaan atau untuk meluaskan kesannya pada sistem pengendalian.

10.7.5. Tab Rootkit

Tab **Rootkit** memaparkan maklumat mengenai rootkit yang dikesan semasa pengimbasan jika anda melancarkan [imbasan AntiRootkit](#).

[Rootkit](#) adalah atur cara yang direka bentuk untuk melakukan kawalan asas sistem komputer tanpa kebenaran daripada pemilik sistem dan pengurus yang sah. Akses kepada perkakasan jarang diperlukan kerana rootkit bertujuan untuk menyita kawalan sistem pengendalian yang sedang dijalankan pada perkakasan. Biasanya, rootkit bertindak untuk mengaburi kehadirannya pada sistem melalui subversi atau pengelakan daripada mekanisme keselamatan sistem pengendalian. Biasanya, ia juga adalah Trojan, dengan itu, menipu pengguna dengan mempercayai bahawa ia selamat untuk dijalankan pada sistemnya. Teknik yang digunakan untuk melaksanakan ini termasuk menyembunyikan proses yang sedang dijalankan daripada menyelia atur cara atau menyembunyikan fail atau data sistem daripada sistem pengendalian.

Secara asasnya, struktur tab ini adalah sama seperti [tab Jangkitan](#) atau [tab Perisian Pengintip](#).

10.7.6. Tab Maklumat

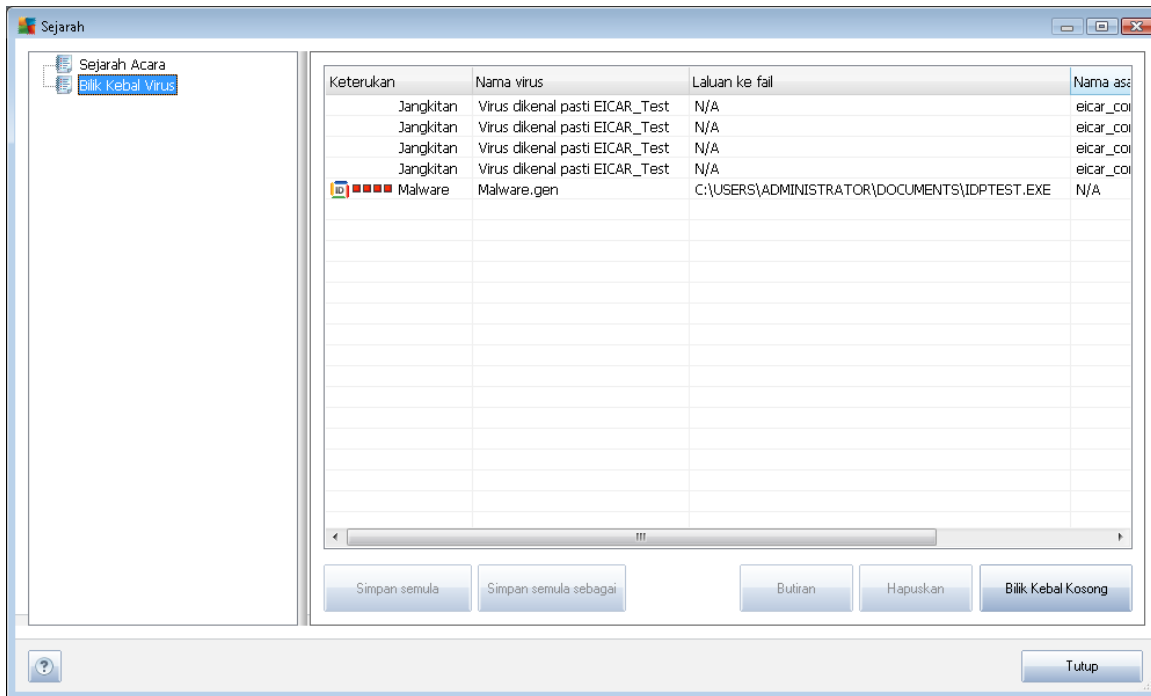
Tab **Maklumat** yang mengandungi data mengenai "penemuan" seperti itu yang tidak boleh dikategorikan sebagai jangkitan, perisian pengintip, dll. Ia boleh sama ada dilabel secara positif sebagai berbahaya tetapi ia masih berbaloi untuk perhatian anda. Imbasan AVG boleh mengesan fail yang mungkin tidak dijangkiti tetapi disyaki. Fail ini dilaporkan sama ada sebagai [Amaran](#) atau sebagai **Maklumat**.



Keseriusan **Maklumat** boleh dilaporkan untuk salah satu sebab berikut:

- **Masa jalan dipek** - Fail dipek dengan salah satu pembungkus masa jalan yang kurang biasa, yang mungkin menunjukkan cubaan untuk mengelakkan pengimbasan fail seperti itu. Walau bagaimanapun, bukan setiap laporan bagi fail seperti itu menunjukkan virus.
- **Rekursif jalan masa yang dipek** - Sama dengan yang di atas, walau bagaimanapun, kurang kerap di kalangan perisian biasa. Fail seperti itu adalah mencurigakan dan pembuangannya atau penghantarannya untuk analisis harus dipertimbangkan.
- **Arkib atau dokumen yang dilindungi kata laluan** - Fail yang dilindungi kata laluan tidak boleh diimbas oleh AVG (*atau biasanya sebarang atur cara antimalware lain*).
- **Dokumen dengan makro** - Dokumen yang dilaporkan mengandungi makro yang mungkin berniat jahat.
- **Sambungan tersembunyi** - Fail dengan sambungan tersembunyi mungkin muncul menjadi *cth.* gambar, tetapi sebenarnya, ia adalah fail boleh laku (*cth. picture.jpg.exe*). Sambungan kedua tidak boleh dilihat dalam Windows secara lalai dan AVG melaporkan fail seperti itu untuk mengelakkan pembukaannya secara tidak sengaja.
- **Laluan fail tidak betul** - Jika beberapa fail sistem penting dijalankan daripada selain laluan lalai (*cth. winlogon.exe yang dijalankan dari selain daripada folder Windows*), AVG melaporkan percanggahan ini. Dalam sesetengah kes, virus menggunakan nama bagi proses standard untuk membuatnya kurang ketara dalam sistem.
- **Fail dikunci** - Fail yang dilaporkan dikunci, seterusnya, tidak boleh diimbas oleh AVG. Ini biasanya bermaksud bahawa sesetengah fail digunakan oleh sistem secara berterusan (*cth. fail pertukaran*).

10.8. Bilik Kebal Virus



Bilik Kebal Virus adalah persekitaran selamat untuk pengurusan objek disyaki/dijangkiti yang dikesan sewaktu ujian AVG. Apabila objek yang dijangkiti dikesan sewaktu imbasan dan AVG tidak boleh memulihkannya secara automatik, anda diminta untuk memutuskan apa yang perlu dilakukan dengan objek yang disyaki. Penyelesaian yang disyorkan adalah untuk mengalihkan objek ke **Bilik Kebal Virus** untuk rawatan selanjutnya. Tujuan utama bagi **Bilik Kebal Virus** adalah untuk menyimpan sebarang fail yang dipadamkan untuk tempoh masa tertentu supaya anda boleh memastikan anda tidak memerlukan fail lagi dalam lokasi asalnya. Jika anda mendapati ketiadaan fail menyebabkan masalah, anda boleh menghantarkan fail yang dipersoalkan untuk analisis, atau menyimpannya semula ke lokasi asal.

Antara muka **Bilik kebal virus** terbuka dalam tettingkap berasingan dan menawarkan gambaran keseluruhan maklumat mengenai objek dijangkiti yang dikuarantin:

- **Keterangan** - jika anda memutuskan untuk memasang komponen [Perlindungan Identiti](#) dalam **AVG Anti-Virus 2011**, pengenalan grafik bagi keterangan penemuan masing-masing pada skala empat tahap daripada yang tidak boleh dibantah (■□□□) sehingga kepada sangat berbahaya (■□■□) akan diberikan dalam bahagian ini; dan maklumat mengenai jenis jangkitan (*berdasarkan pada tahap jangkitannya - semua objek yang disenaraikan boleh menjadi secara positif atau berkemungkinan dijangkiti*)
- **Nama Virus** - menentukan nama jangkitan yang dikesan menurut [Ensiklopedia virus](#) (dalam talian)
- **Laluan ke fail** - laluan penuh ke lokasi asal bagi fail yang boleh dijangkiti dikesan
- **Nama objek asal** - semua objek yang dikesan yang disenaraikan dalam carta telah dilabel



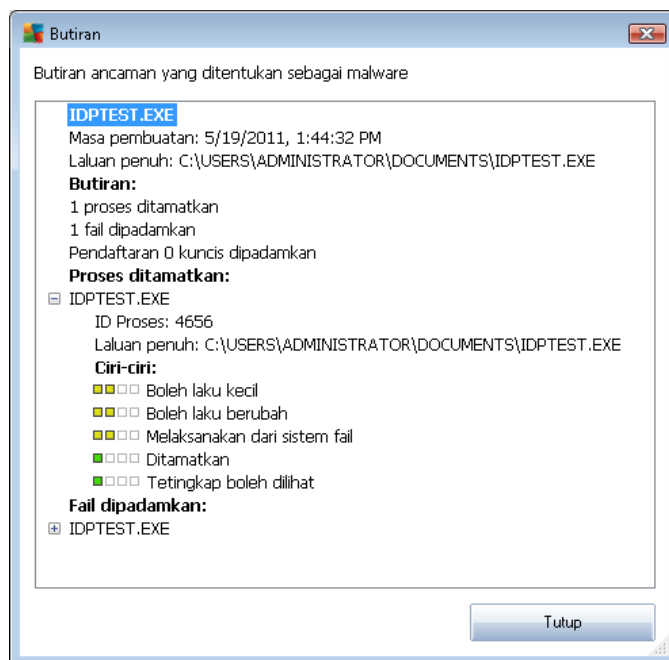
dengan nama standard yang diberikan oleh AVG sewaktu proses imbasan. Jika objek mempunyai nama asal khusus yang diketahui (*cth. nama lampiran e-mel yang tidak memberi respons kepada kandungan sebenar lampiran*), ia akan diberikan dalam kolom ini.

- **Tarikh simpanan** - tarikh dan masa fail yang dijangkiti dikesan dan dibuang ke **Bilik Kebal Virus**

Butang kawalan

Butang berikut boleh diakses dari antara muka **Bilik Kebal Virus**.

- **Simpan semula** - membuang fail yang dijangkiti kembali ke lokasi asalnya pada cakera anda
- **Simpan Semula Sebagai** - mengalih fail yang dijangkiti ke folder yang dipilih
- **Butiran** - butang ini hanya digunakan pada ancaman yang dikesan oleh **Perlindungan Identiti**. Dengan mengklik, ia memaparkan gambaran keseluruhan sinopsis gambaran keseluruhan bagi butiran ancaman (*apakah fail/proses yang telah dijangkiti, ciri-ciri proses dll.*). Sila maklum bahawa untuk semua item lain selain yang dikesan oleh IDP, butang ini berwarna kelabu dan tidak aktif!



- **Padam** - membuang fail yang dijangkiti daripada **Bilik Kebal Virus** sepenuhnya dan tidak boleh diundur
- **Kosongkan Bilik Kebal** - membuang semua **kandungan** Bilik Kebal Virus sepenuhnya. Dengan membuang fail dari **Bilik Kebal Virus**, fail ini dibuang tanpa boleh didapatkan kembali dari cakera (bukan dialihkan ke tong kitar semula).



11. Kemas kini AVG

Memastikan AVG anda terkini adalah penting untuk memastikan semua virus yang baru ditemui akan dikesan secepat mungkin.

Memandangkan kemas kini AVG tidak dikeluarkan mengikut sebarang jadual tetap tetapi sebaliknya sebagai reaksi kepada jumlah dan keseriusan ancaman baru, adalah disyorkan untuk menyemak kemas kini baru sekurang-kurangnya sekali sehari atau lebih kerap. Hanya dengan cara ini anda boleh memastikan **AVG Anti-Virus 2011** sentiasa terkini sepanjang hari.

11.1. Tahap Kemas kini

AVG menawarkan dua tahap kemas kini untuk dipilih dari:

- **Kemas kini definisi** mengandungi perubahan yang diperlukan untuk perlindungan antivirus yang boleh dipercayai. Biasanya, ia tidak termasuk sebarang perubahan kepada kod dan mengemas kini hanya pangkalan data definisi. Kemas kini ini harus digunakan sebaik sahaja ia tersedia.
- **Kemas kini atur cara** mengandungi pelbagai perubahan atur cara, pembaikan dan peningkatan.

Apabila [menjadualkan kemas kini](#), anda boleh memilih tahap keutamaan mana yang patut dimuat turun dan digunakan.

Perhatian: Jika persamaan masa bagi kemas kini atur cara yang dijadualkan dan imbasan yang dijadualkan berlaku, proses kemas kini adalah lebih utama dan imbasan akan diganggu.

11.2. Jenis Kemas Kini

Anda boleh membezakan antara dua jenis kemas kini:

- **Kemas kini dalam permintaan** adalah kemas kini AVG segera yang boleh dilakukan pada bila-bila masa jika perlu.
- **Kemas kini yang dijadualkan** - dalam AVG, anda boleh [mempratetapkan rancangan kemas kini](#). Kemudian, kemas kini yang dirancang dilakukan secara berkala mengikut konfigurasi persediaan. Apabila fail kemas kini baru terdapat pada lokasi tertentu, ia dimuat turun sama ada secara terus dari Internet atau dari direktori rangkaian. Apabila tiada kemas kini lebih baru yang tersedia, tiada apa yang berlaku.

11.3. Kemas Kini Proses

Proses kemas kini boleh dilancarkan dengan serta-merta apabila perlu menggunakan [pautan pantas Kemas kini sekarang](#). Pautan ini tersedia pada setiap masa dari sebarang dialog [antara muka pengguna AVG](#). Walau bagaimanapun, adalah masih amat disyorkan untuk melakukan kemas kini secara tetap seperti yang dinyatakan dalam jadual kemas kini boleh diedit dalam komponen [Pengurus kemas kini](#).

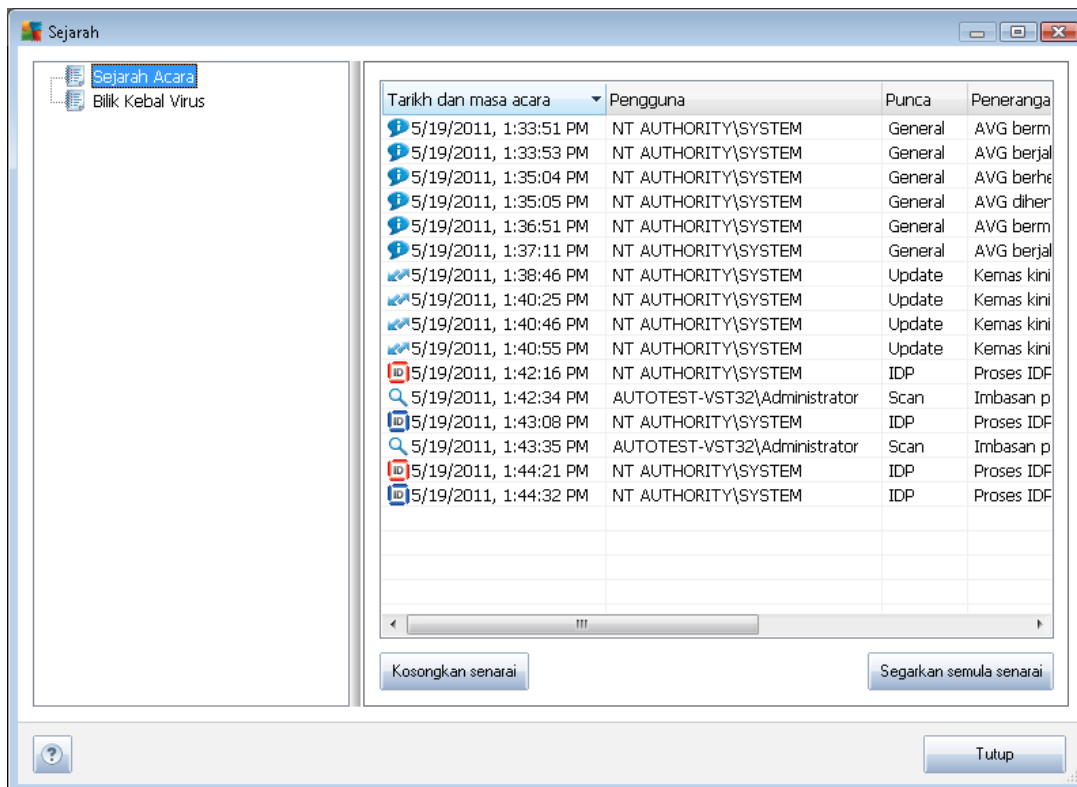
Apabila anda memulakan kemas kini, pertama sekali, AVG akan mengenal pasti sama ada terdapat fail kemas kini baru yang tersedia. Jika ada, AVG memulakan muat turun dan melancarkan proses



kemas kini dengan sendiri. Sewaktu proses kemas kini, anda akan diarahkan semula ke antara muka **Kemas kini** di mana anda boleh melihat perkembangan proses dalam persembahan grafiknya serta seperti dalam gambaran keseluruhan parameter statistik yang relevan (*kemas kini saiz fail, data yang diterima, kelajuan muat turun, masa berlalu, ...*).

Nota: Sebelum kemas kini atur cara AVG melancarkan titik pemulihan sistem dibuat. Jika proses kemas kini gagal dan sistem pengendalian anda hancur, anda sentiasa boleh memulihkan OS anda dalam konfigurasi asal dari titik ini. Pilihan boleh diakses melalui Start / All Programs / Accessories / System tools / System Restore. Disyorkan kepada pengguna berpengalaman sahaja!

12. Sejarah Acara



Dialog **Sejarah** boleh diakses dari [menu sistem](#) melalui item **Sejarah/Log Sejarah Acara**. Dalam dialog ini, anda boleh menemui ringkasan peristiwa penting yang berlaku sewaktu operasi **AVG Anti-Virus 2011**. **Sejarah** merekodkan jenis acara berikut:

- Maklumat mengenai kemas kini aplikasi AVG
- Imbasan, bermula, tamat atau berhenti (*termasuk ujian yang dilakukan secara automatik*)
- Acara yang bersambung dengan pengesanan virus (oleh [Perisai Residen](#) atau [imbasan](#)) termasuk lokasi tempat berlaku
- Acara penting lain

Bagi setiap acara, maklumat berikut disenaraikan:

- **Tarikh dan masa acara** memberikan masa dan tarikh tepat acara berlaku.
- **Pengguna** menyatakan siapa yang memulakan acara
- **Sumber** memberikan komponen sumber atau bahagian lain sistem AVG yang mencetuskan acara



- ***Penerangan acara*** memberikan maklumat ringkas apa sebenarnya berlaku

Butang kawalan

- ***Kosongkan senarai*** - memadam semua entri dalam senarai acara
- ***Muat semula senarai*** - memadam semua entri dalam senarai acara



13. Soalan Lazim dan Sokongan Teknikal

Jika anda mempunyai sebarang masalah dengan AVG anda, sama ada perniagaan atau teknikal, sila rujuk kepada bahagian [Soalan Lazim](#) bagi tapak web AVG (<http://www.avg.com/>).

Jika anda tidak berjaya dengan mendapatkan bantuan begini, hubungi jabatan sokongan teknikal melalui e-mel. Sila gunakan borang hubungan yang boleh diakses daripada menu sistem melalui ***Bantuan / Dapatkan bantuan dalam talian***.