CÔNG TY CỔ PHẦN DỊCH VỤ CÂY DÙ ĐỎ
Phòng G.3B, E.Town 1, 364 Cộng Hòa, P.13, Q.Tân Bình, HCM.
Tel: +(84-8) 3812 5678 I Fax: (84-8) 3812 5320

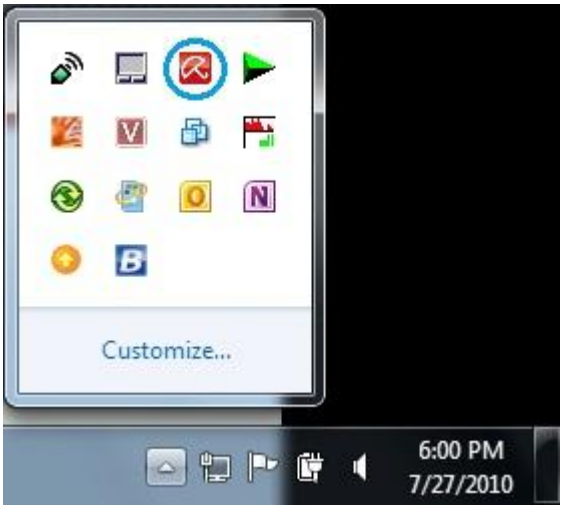
HƯỚNG DẪN SỬ DỤNG
PHẦN MỀM DIỆT VIRUS AVIRA

Mục lục

1. Mở chương trình

Để mở chương trình, thực hiện như sau

Kích đôi vào biểu tượng chương Avira AntiVir Premium

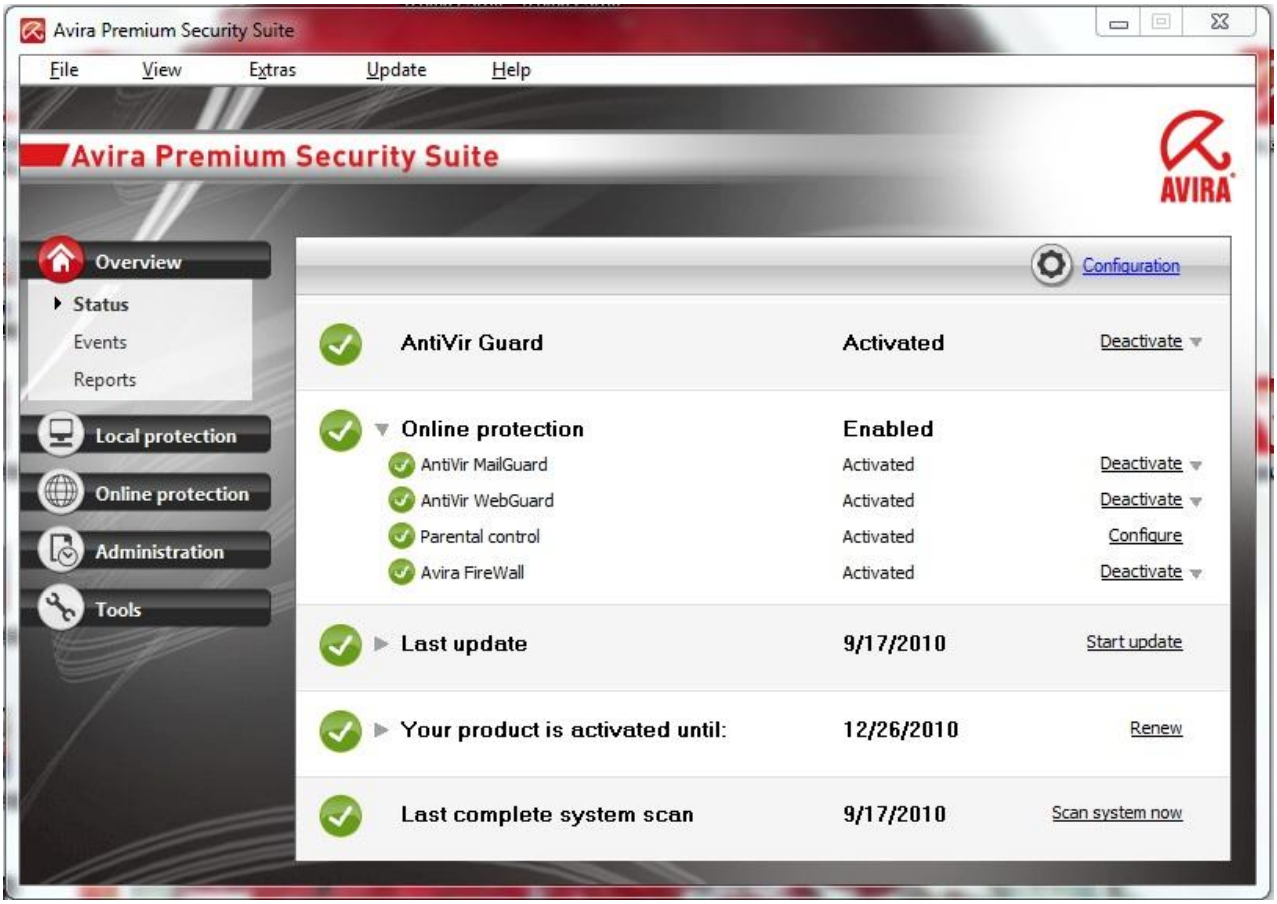


Chú ý:

- Bạn cũng có thể mở chương trình từ menu Windows Start , hoặc kích vào biểu tượng chương trình Avira AntiVir Control Center trên Desktop

2. Giao Diện Chính Của Chương Trình

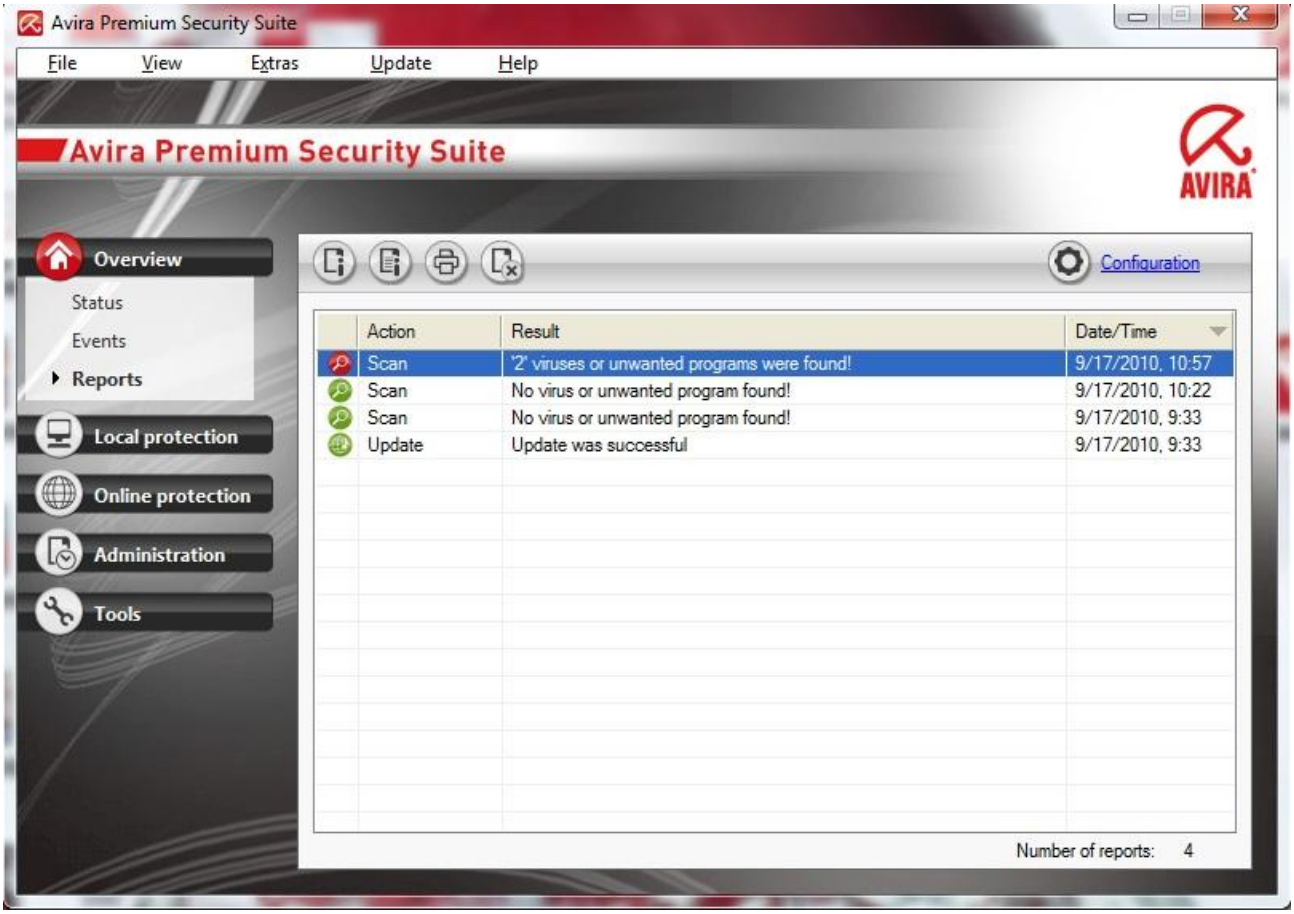
Khi bạn mở chương trình, màn hình giao diện chính của chương trình sẽ được mở ra. Tình trạng bảo vệ máy tính được hiển thị phía trên màn hình giao diện chính. Bạn có thể thấy được tình trạng bảo vệ của máy tính cũng như các thông số chung trên máy tính của bạn, thông tin license hết hạn. Bạn có thể thiết lập đặc tính bảo mật bằng cách click vào biểu tượng **Configuration**.



Click vào **Events** để xem thông tin đang chạy của chương trình:

Biểu tượng	Mô tả
	Xem thông tin chi tiết dòng được chọn.
	Xuất ra tập tin dòng được chọn.
	Xóa dòng được chọn.

Click vào **Report** để xem các báo cáo về lần quét virus, lần update gần nhất.

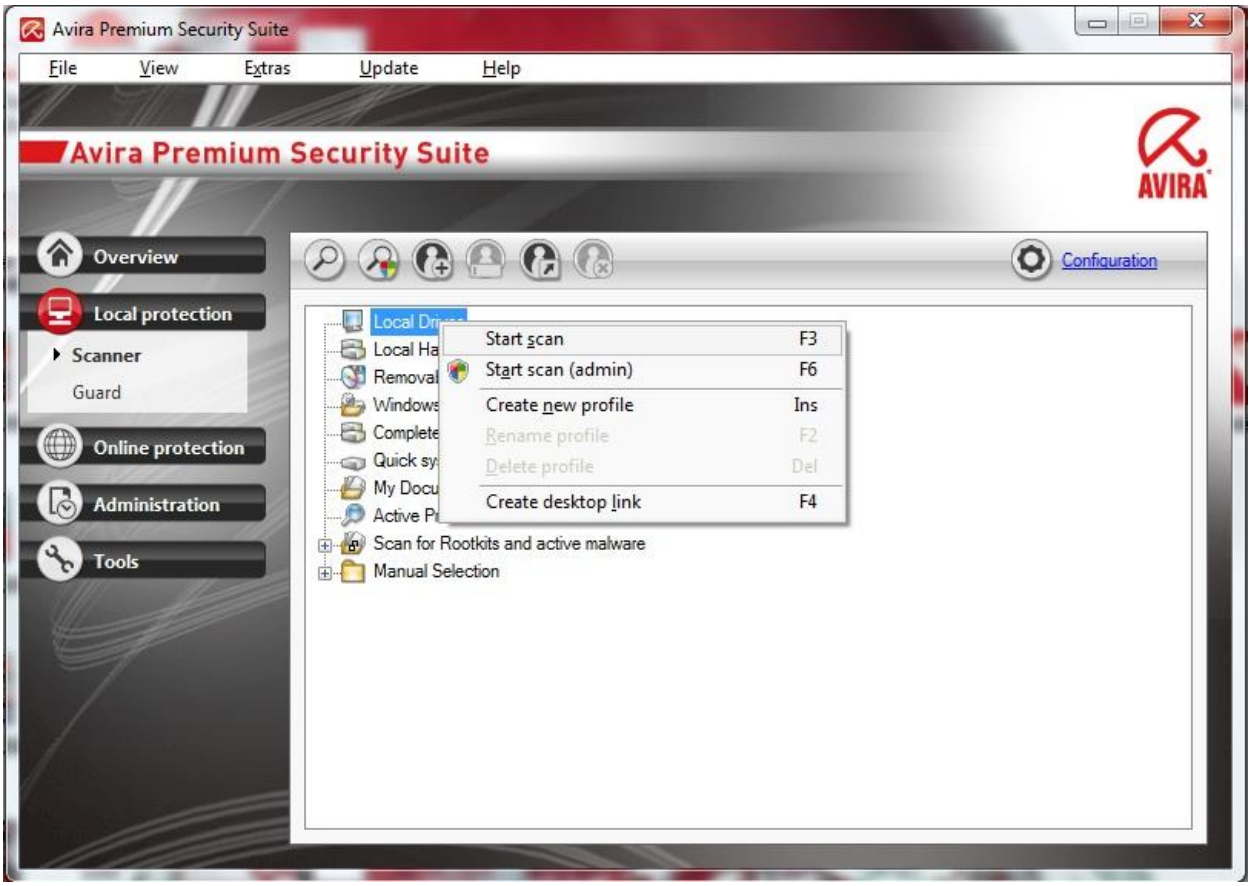


Biểu tượng	Mô tả
	Xem thông tin chi tiết dòng được chọn.
	Xem thông tin chi tiết dòng được chọn dưới dạng tập tin.
	In ra máy in thông tin dòng được chọn.
	Xóa dòng được chọn.

3. Quét Virus

Từ màn hình chính của phần mềm bạn chọn biểu tượng **Local protection** 

, sau đó click chuột vào menu **Scanner**



Bạn có thể chọn một mục bất kỳ và click chuột phải, chọn **Start scan** để thực hiện quét virus cho ổ đĩa hoặc thư mục được chọn.

Biểu tượng	Mô tả
	Khi bạn chọn một mục bất kỳ, và click biểu tượng này, chương trình sẽ thực hiện quét virus trên mục bạn đã chọn. Hoặc bạn có thể click chuột phải vào một mục bất kỳ và chọn **Start scan** để thực hiện chức năng này.
	Chức năng này để tạo ra một profile mới với các thư mục hoặc ổ đĩa bạn muốn quét sẽ được lưu vào đây. Giúp bạn dễ dàng hơn trong những lần quét về sau. Hoặc bạn có thể click chuột phải vào một mục bất kỳ và chọn **Create new profile** để thực hiện chức năng này.

	Tạo một biểu tượng quét vào mục bạn đã chọn ra ngoài Desktop. Việc này giúp cho việc quét virus sau này vào thư mục bạn chon một cách nhanh chóng chỉ với 1 cú click chuột vào biểu tượng Desktop mà chương trình đã tạo, sẽ tự động quét mà không cần thao tác mở chương trình lên. Hoặc bạn có thể click chuột phải vào mục bất kỳ và chọn **Create desktop link**
	Xóa dòng được chọn.

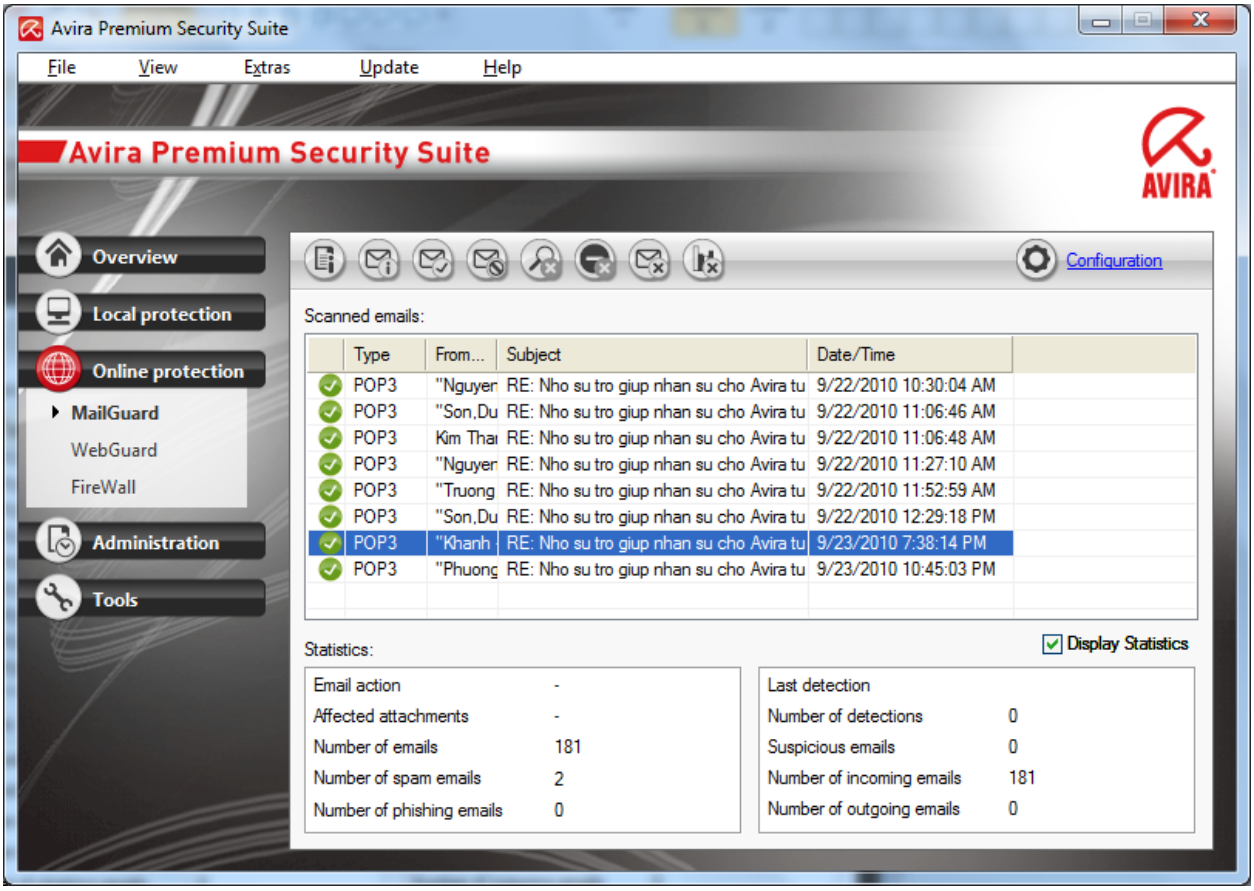
4. Theo dõi bảo mật cho kết nối mạng

Chương trình sẽ giám sát và lọc lưu lượng kết nối mạng giữa máy tính của bạn và Internet. Chương trình cũng sẽ ẩn máy tính của bạn đối với mạng Internet, và ghi log tất cả các nổ lực tấn công đến máy tính của bạn. Chương trình được cập nhật tự động, đảm bảo máy tính của bạn được bảo vệ trước các nguy cơ từ Internet.

Từ màn hình chính của phần mềm bạn chọn biểu tượng **Online protection** 

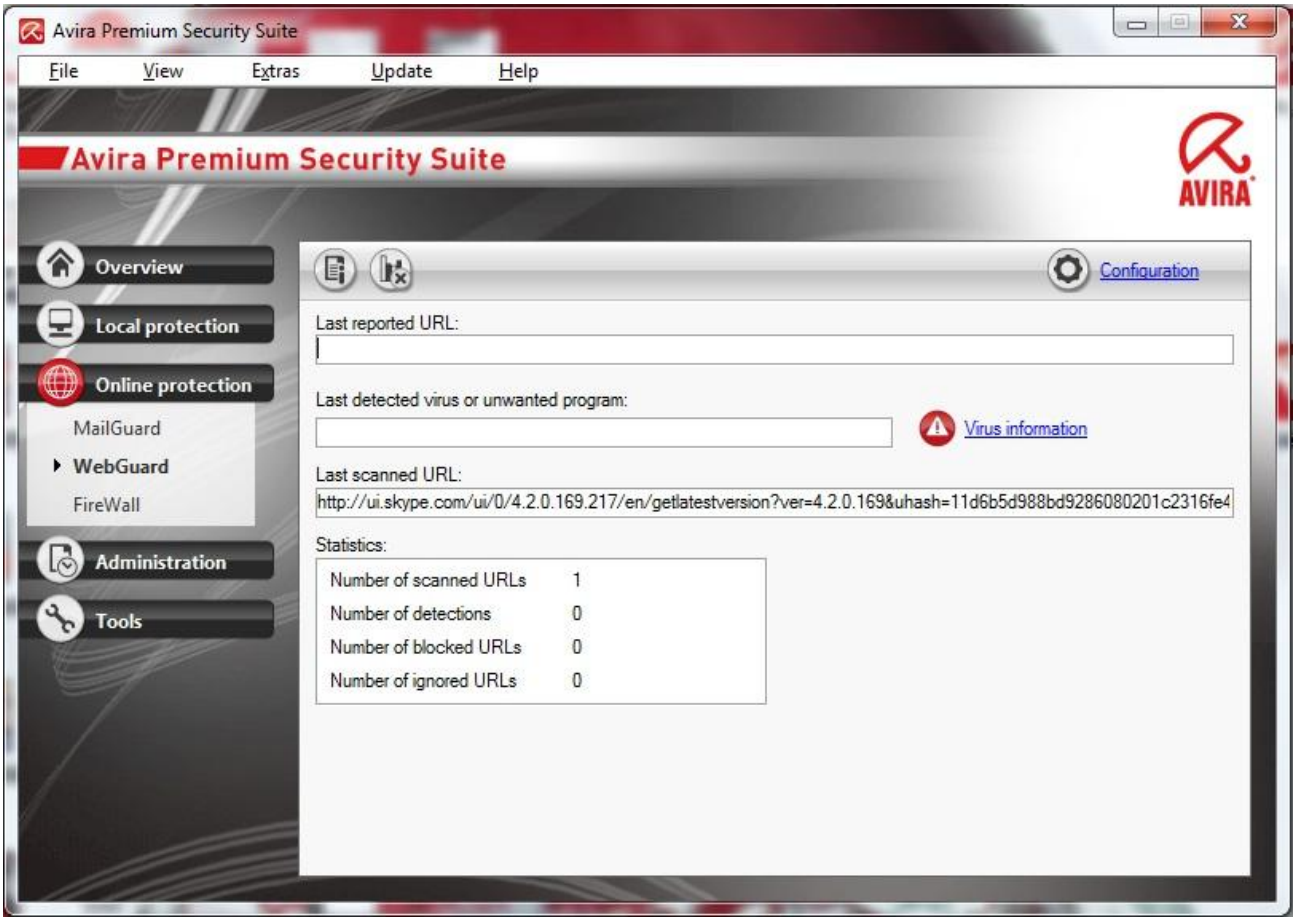
, sau đó click chuột vào menu **MailGuard**

Chương trình sẽ hiển thị các email đã đến và đi trong máy tính của bạn thông qua các phương thức nào, và email đó an toàn hoặc là có nhiễm virus hay không.

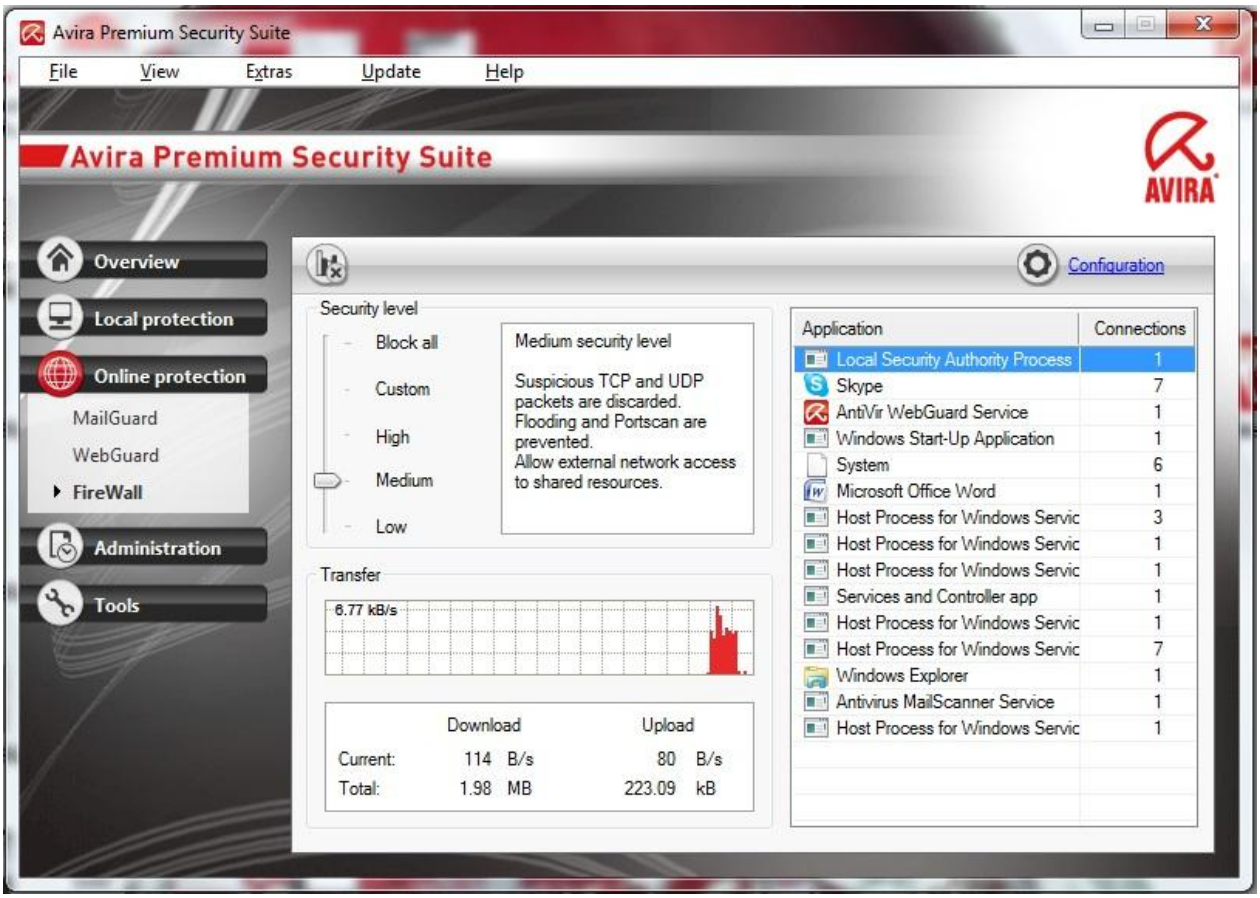


Biểu tượng	Mô tả
	Các email an toàn.
	Các email có khả năng gây nguy hại.

Click vào **WebGuard** để theo dõi các website mà bạn đã truy cập vào có nguy cơ nhiễm virus. Màn hình sẽ hiển thị link website cuối cùng bạn đã truy cập và bị cảnh báo có nguy cơ virus, spyware, madware cao.



Click vào **Firewall** để theo dõi các băng thông truy xuất mạng (số lượng download cũng như upload) và theo dõi các chương trình đang chạy và có mở kết nối internet.

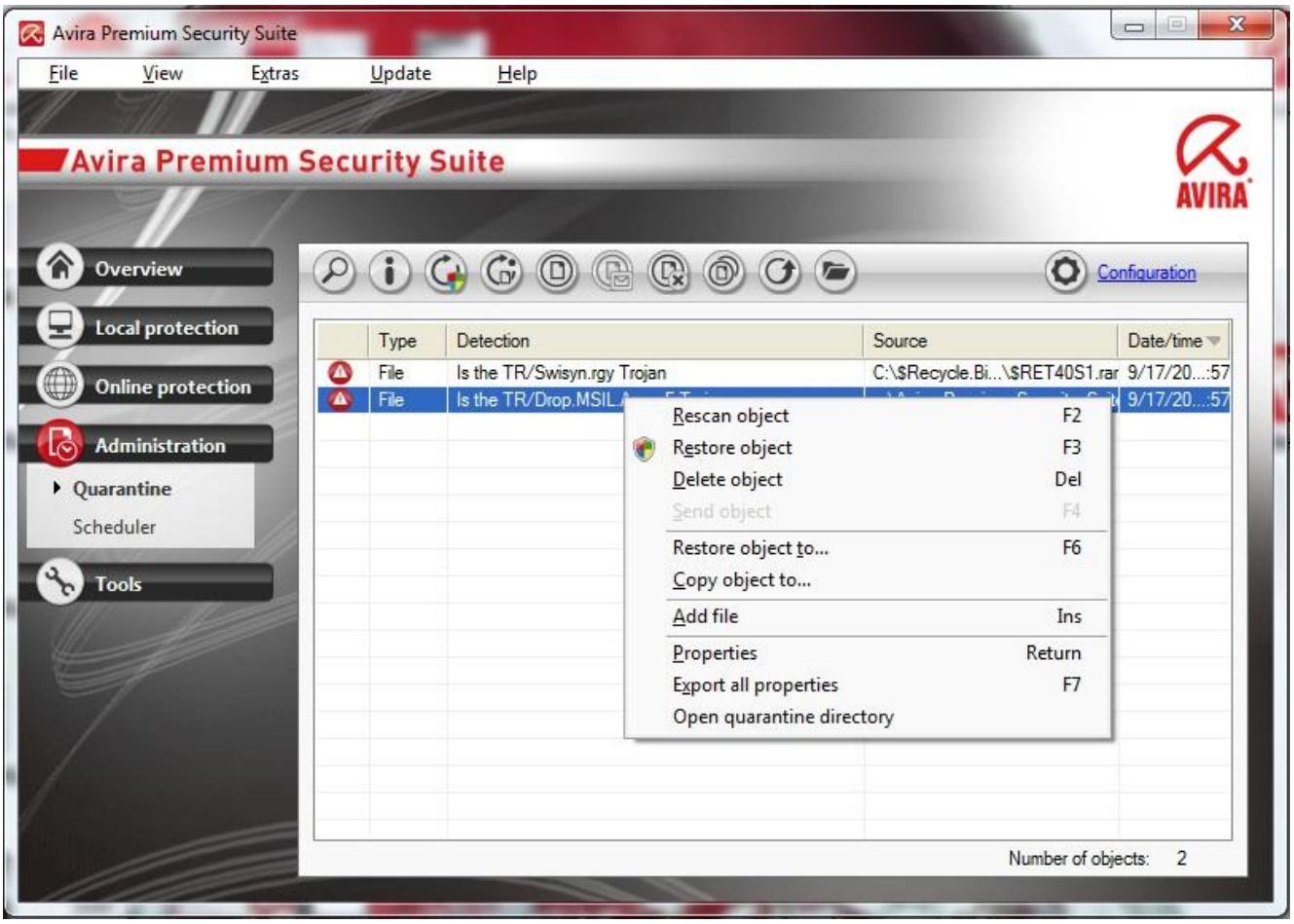


5. Xem báo cáo, theo dõi lại các tập tin virus

Chương trình sẽ ghi lại lịch sử các lần quét và các tập tin đã nhiễm virus và chương trình đã đưa vào các thư mục cách ly của chương trình. Bạn hoàn toàn có thể vào để xem lại các tập tin đã được cách ly này và có thể phục hồi lại chúng nếu cần thiết.

Từ màn hình chính của phần mềm bạn chọn biểu tượng **Administration** 

, sau đó click chuột vào menu **Quarantine**



Biểu tượng	Mô tả
	Khi bạn chọn một dòng bất kỳ và click vào biểu tượng này, chương trình sẽ quét lại tập tin này. Hoặc bạn có thể chọn một dòng bất kỳ và click chuột phải, sau đó chọn chức năng **Rescan object** để thực hiện quét lại tập tin này.
	Hiển thị thông tin chi tiết về tập tin đã bị nhiễm virus mà bạn chọn.

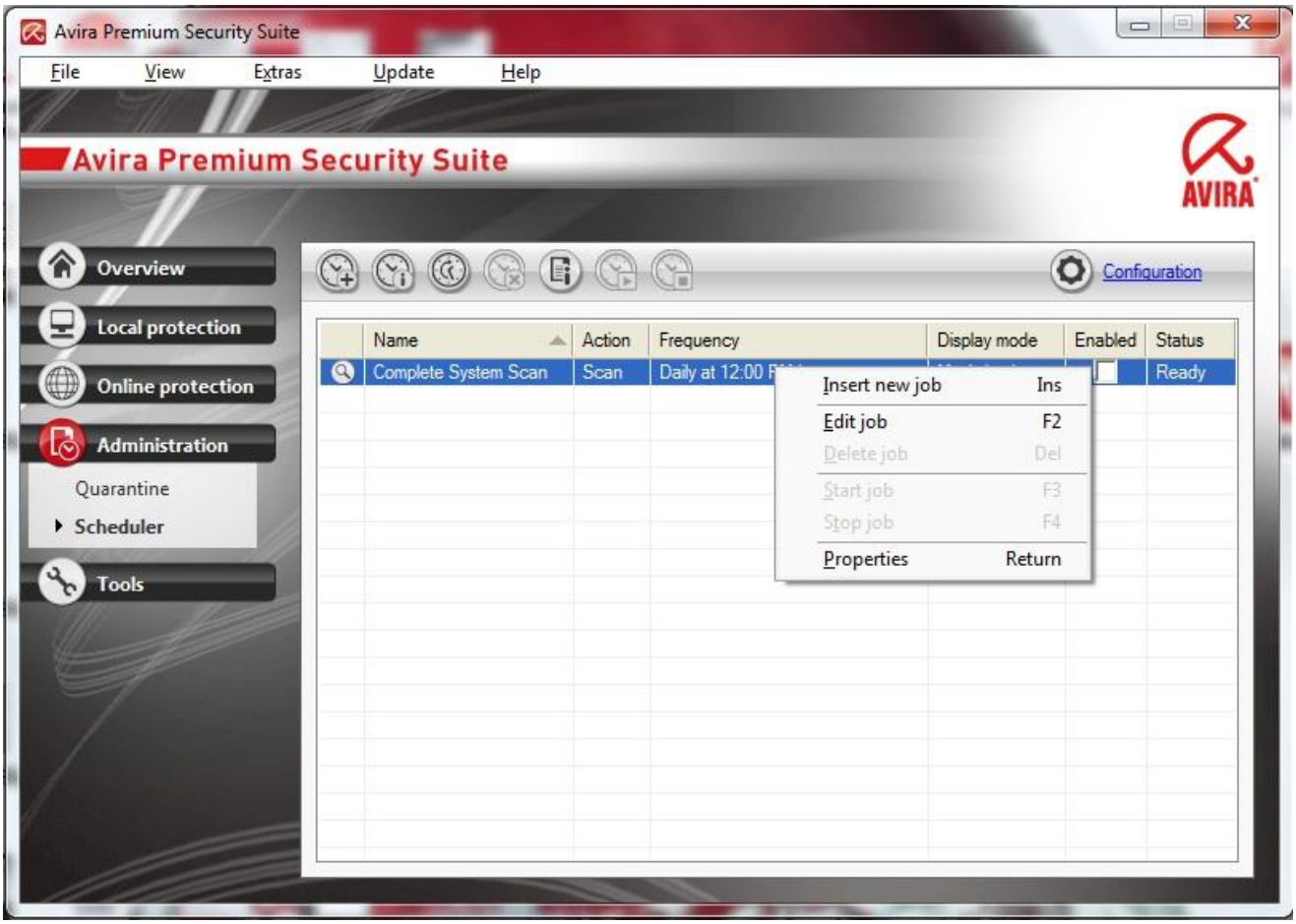
	Hoặc bạn có thể click chuột phải và chọn chức năng **Properties.**
	Dùng để phục hồi lại tập tin mà bạn đã chọn. chức năng này sẽ phục hồi lại tập tin vào đúng thư mục ban đầu. Hoặc bạn có thể click chuột phải vào tập tin muốn phục hồi và chọn **Restore object.**
	Tương tự như chức năng Restore object ở phía trên và để phục hồi lại tập tin đã bị nhiễm virus và cho phép bạn phục hồi tập tin đó tới thư mục được chỉ định. Hoặc bạn có thể click chuột phải vào tập tin muốn phục hồi và chọn **Restore object to…**
	Chức năng này cho phép bạn thêm vào tập tin chưa bị nhiễm virus nhưng bạn cảm thấy nghi ngờ về tập tin này, bạn có thể đưa vào để chương trình cách ly.
	Nếu bạn muốn tìm hiểu về tập tin mà bạn cảm thấy nghi ngờ hoặc tìm hiểu về tập tin virus đã bị cách ly này. Bạn có thể dùng chức năng này để gửi email đến cho bộ phận phát triển của Avira. Hoặc bạn có thể dùng chức năng này bằng cách thực hiện click chuột phải vào tập tin muốn gửi cho Avira và chọn **Send object.**
	Xóa tập tin nhiễm virus khỏi thư mục cách ly của chương trình. Hoặc bạn có thể dùng chức năng này bằng cách click chuột phải vào tập tin và chọn **Delete object.**
	Xuất thông tin chi tiết về tập tin được chọn ra tập tin văn bản. Hoặc bạn có thể dùng chức năng này bằng cách click chuột phải vào tập tin và chọn **Export all properties.**

6. Lập lịch quét virus

Bạn có thể dùng **Sheduler** để quét virus toàn bộ máy tính hoặc update virus tại thời điểm lựa chọn thích hợp, ví dụ hằng ngày, hằng tuần hoặc hằng tháng.

Để sử dụng chức năng **Scheduler** bạn chọn biểu tượng **Administration** 

, sau đó click chuột vào menu **Scheduler**.



Bạn có thể tạo ra nhiều lịch trình làm việc khác nhau, và kích hoạt vào lịch trình nào mà bạn muốn hoạt động bằng cách chọn (đánh dấu √) vào cột **Enabled**.

Biểu tượng	Mô tả
	Tạo một lịch trình mới cho chương trình. Hoặc bạn có thể chọn một dòng bất kỳ và click chuột phải, sau đó chọn chức năng **Insert new job** để thực hiện quét lại tập tin này.
	Hiển thị thông tin chi tiết của lịch trình mà bạn chọn. Hoặc bạn có thể click chuột phải vào lịch trình cần xem và click chuột phải,

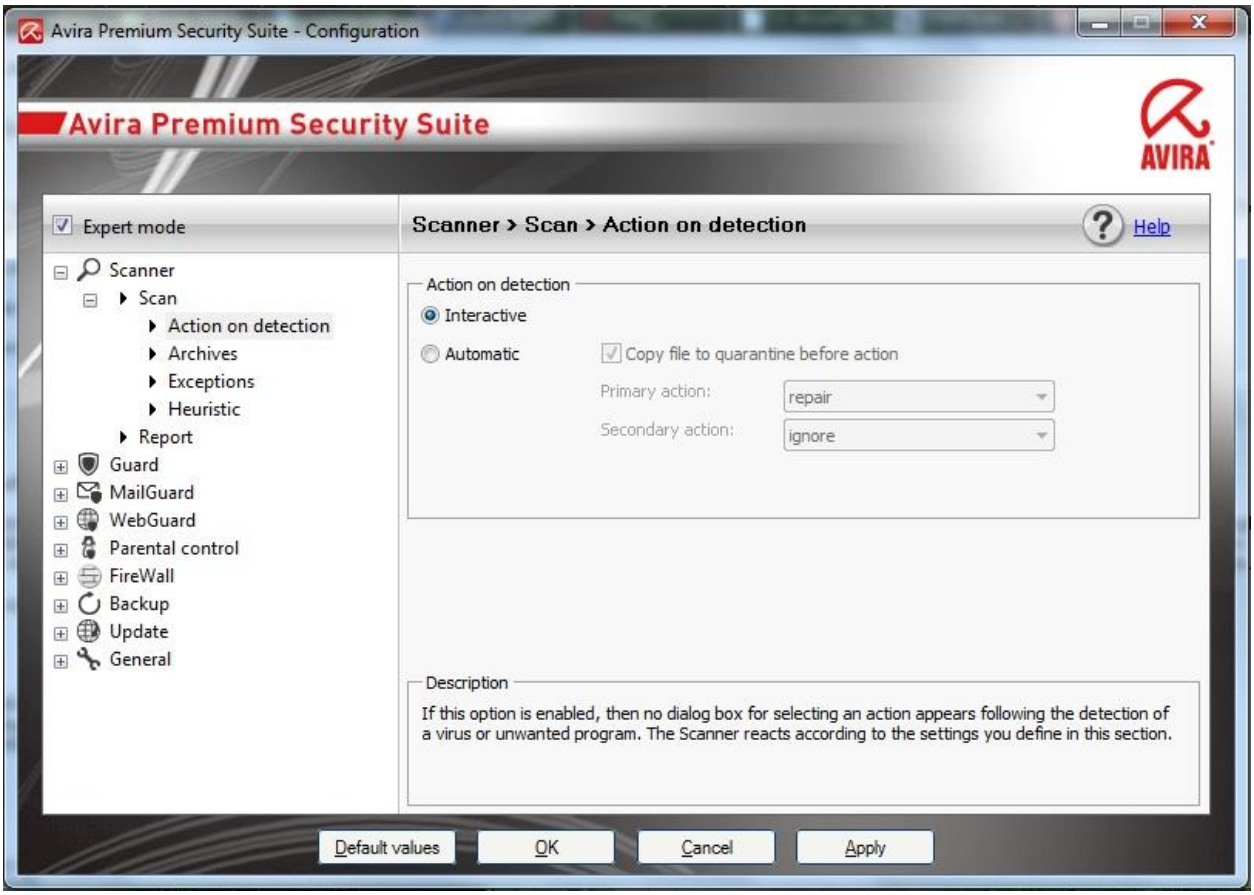
	sau đó chọn chức năng **Properties**.
	Dùng để thay đổi lại thông tin của lịch trình. Hoặc bạn có thể click chuột phải vào lịch trình cần thay đổi và chọn chức năng **Edit job**.
	Xóa lịch trình đang chọn. Hoặc bạn có thể click chuột phải vào lịch trình cần xóa và chọn chức năng **Delete job.**
	Chức năng này cho phép bạn thực thi lịch trình bạn chọn mà không cần đợi tới thời điểm đã thiết lập. Hoặc bạn có thể chọn lịch trình muốn thực thi và click chuột phải, sau đó chọn chức năng **Start job**.

TÙY CHỈNH NÂNG CAO CÁC TÍNH NĂNG PHẦN MỀM DIỆT VIRUS AVIRA

7. Cấu hình chương trình tự động xử lý khi phát hiện virus

Mở giao diện của **Avira** > Click vào **Configuration** ở góc trên bên phải > Tick chọn **Expert mode** ở góc trên bên trái > Nhìn vào cột bên trái > Click vào đầu ô **Scanner** để mở cây thư mục > Mở cây thư mục **Scan** > Click chọn **Action on Detection** > Nhìn vào ô bên trái của phần **Action on Detection** có 2 mục **Interactive và Automatic**.

- Chọn **Interactive:** khi bạn muốn chương trình phát hiện virus và hiện lên các quyết định cho bạn chọn để xử lý virus này:
  - ✓ **Delete** – bạn có sẽ xóa tập tin bị nhiễm virus
  - ✓ **Quarantine** (Cách ly): đưa tập tin bị nhiễm virus vào khu vực cách ly
  - ✓ **Ignore** (Bỏ qua): khi bạn chắc rằng tập tin là an toàn không bị nhiễm virus thì bạn hãy chọn phương án này, vì nó sẽ bỏ qua tập tin này.



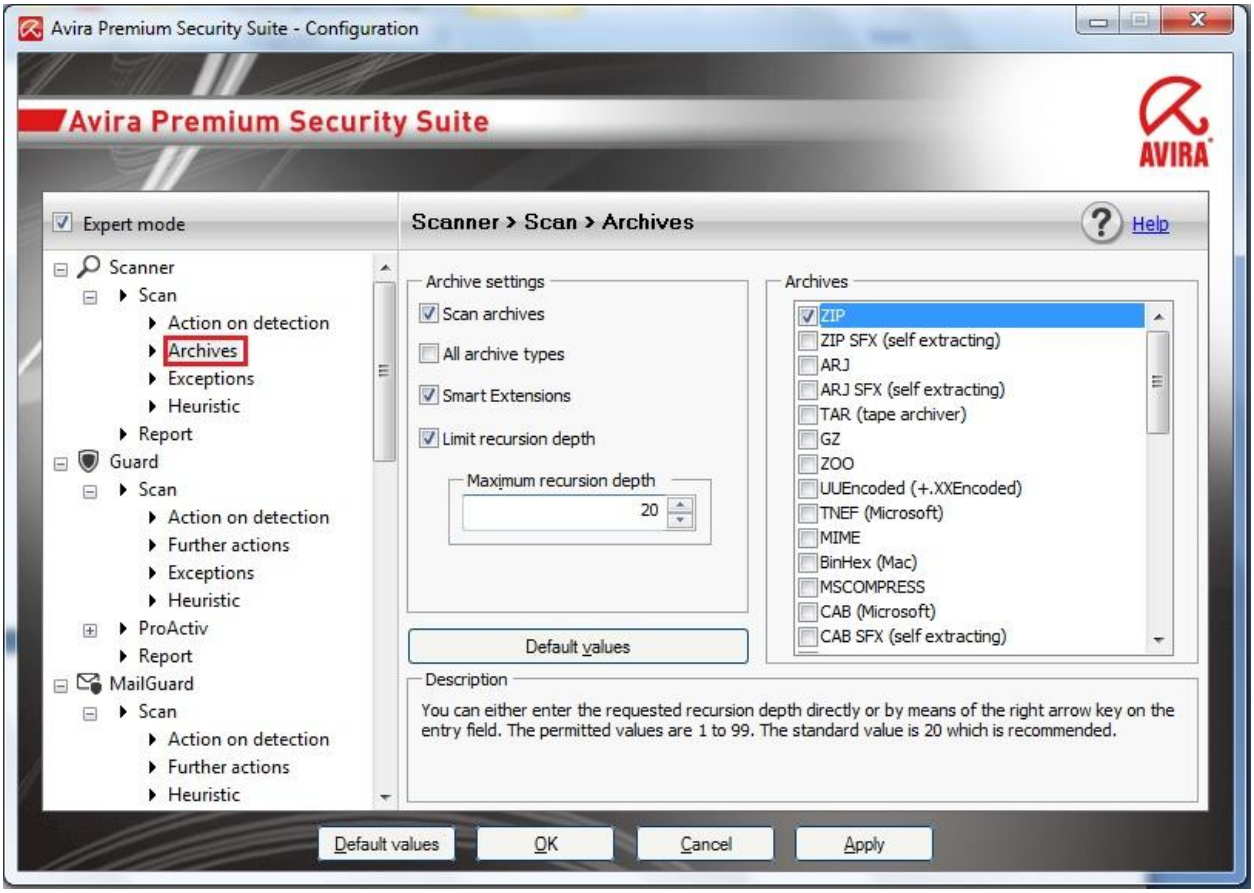
- Chọn **Automatic:** khi bạn quyết định cho chương trình tự động diệt và đưa vào vùng cách ly.
  - ✓ Check chọn vào ô **Copy file to quarantine before action**
  - ✓ **Primary Action** có 5 option, bạn nên chọn **Repair**
    - **Repair** (Sửa chữa)
    - **Rename** (Đổi tên)

- **Delete** (Xóa)
- **Ignore** (Bỏ qua)
- **Overwrite** and **Delete** (Chép đè lên và xóa)

Lưu ý: Đối với các chức năng **Guard, MailGuard, WebGuard** bạn cũng thực hiện tương tự các bước như để cấu hình cho chương trình khi phát hiện virus sẽ xử lý theo cách cài đặt của bạn.

8. Tùy chỉnh việc quét các file nén

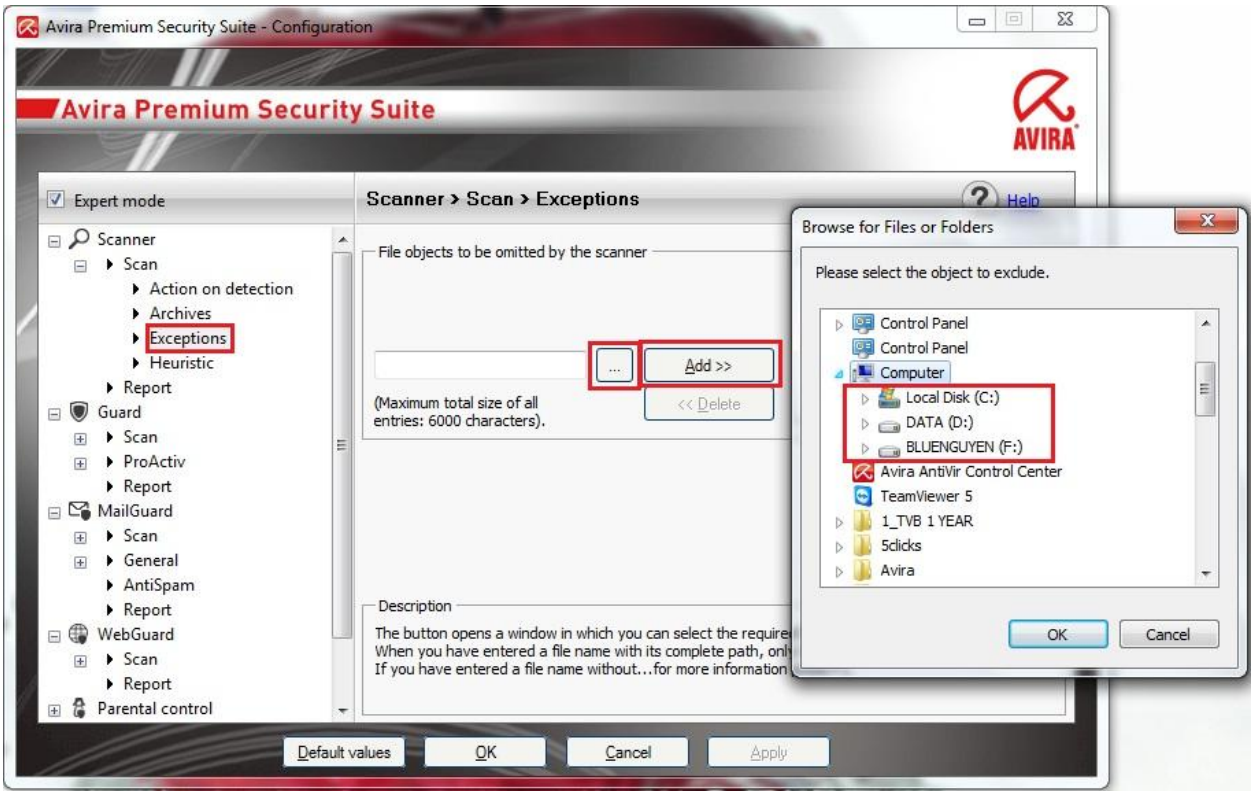
Bạn có thể tùy chọn các dạng file nén cũng như cấp độ các file nén mà Avira sẽ quét bằng cách thực hiện như sau:



- Scan **archives:** Khi được kích hoạt thì các dạng file nén bạn chọn trong list sẽ được quét.
- All **archive types:** Khi được kích hoạt thì tất cả các dạng file nén trong list sẽ được chọn và quét.
- Smart **Extensions:** Khi được kích hoạt thì Avira AntiVir Premium sẽ tự động chọn các dạng file để quét. Chức năng này sẽ quét chậm hơn nhưng sẽ bảo mật hơn khi bạn chọn dạng file để quét trong list.
- **Limit recursion depth:** Giải nén và quét đệ qui các file nén rất tốn thời gian và tài nguyên máy. Nếu chức năng này được kích hoạt,bạn có thể giới hạn được số cấp các file nén để quét.

9. Đưa file chương trình hoặc thư mục vào vùng tin tưởng

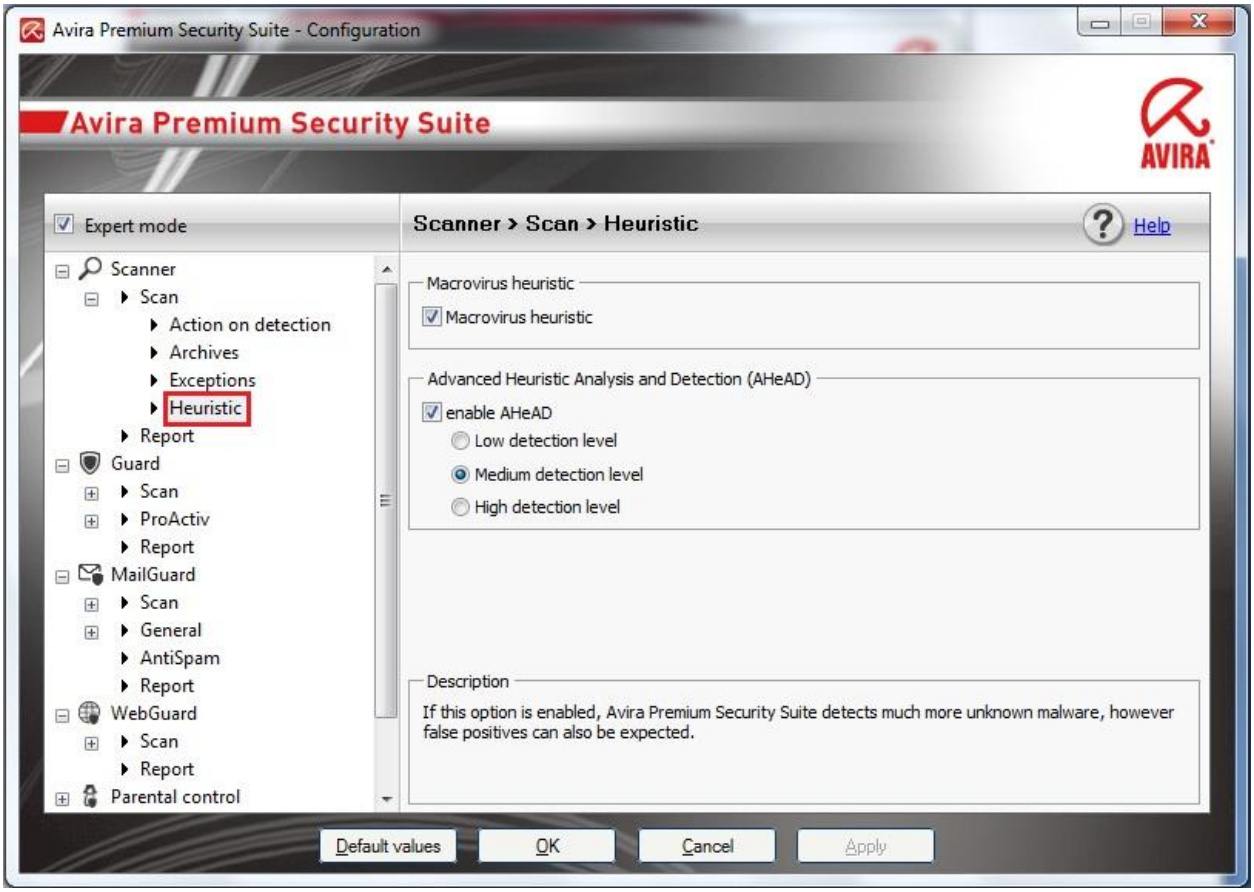
Exceptions > click vào [...] trước "Add" để tìm đến các file không muốn Avira quét khi thực hiện quá trình Scan hệ thống > **chọn file > OK > Add > Apply > OK.**



Lưu ý: Bạn có thể thiết lập cho mục **Guard** tương tự với các bước trên.

10. Kích hoạt tính năng phát hiện các virus tìm ẩn

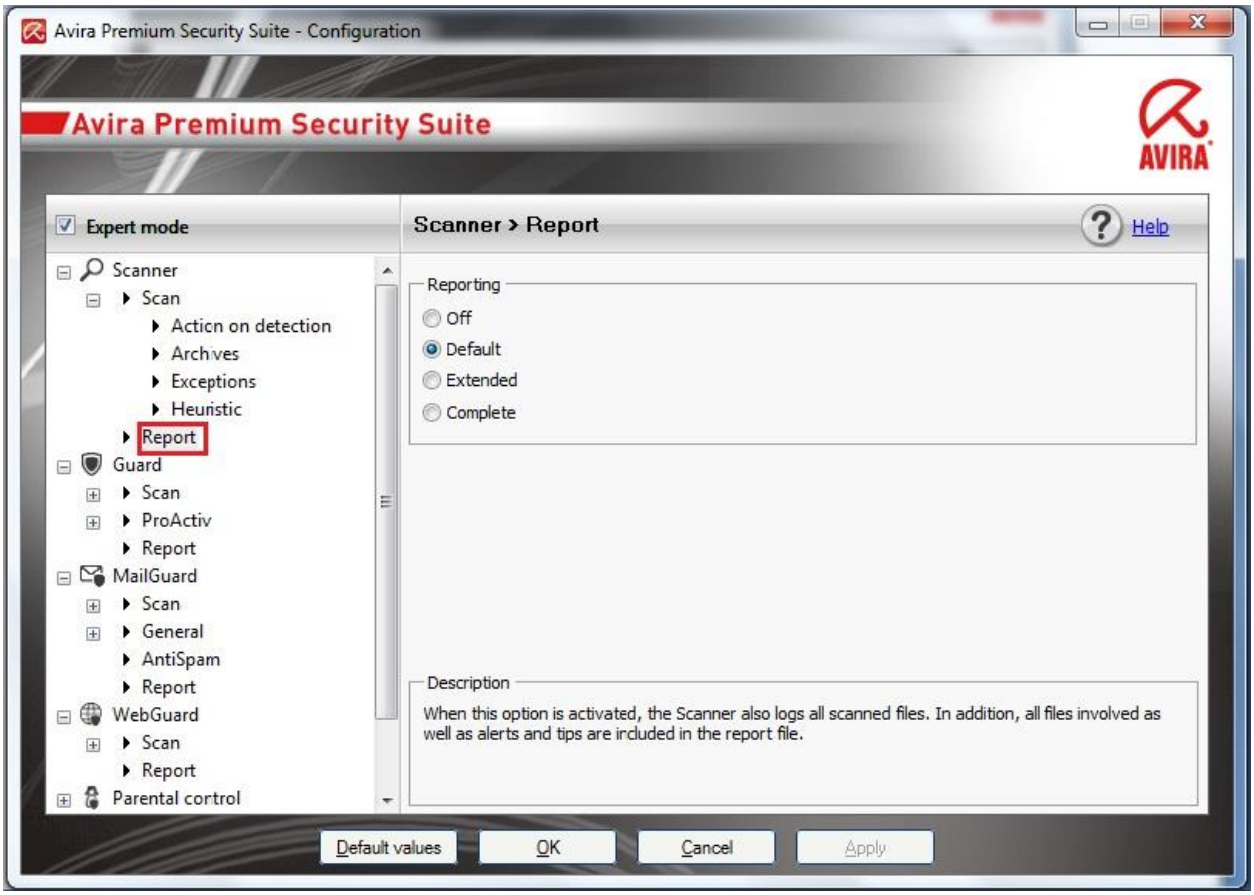
Click vào đầu ô **Scanner** để mở cây thư mục > Mở cây thư mục **Scan** > **Heuristic**



- **Macrovirus heuristic**: Khi được kích hoạt, Avira sẽ giúp bạn phát hiện được nhiều Macrovirus trong các tài liệu và sẽ hiển thị cảnh báo cho bạn biết.
- **AHeAD:** Phân tích virus mới dựa vào hành vi hoạt động của chúng. Khi kích hoạt bằng cách click chọn **Enable** bạn có thể chọn cấp độ:
  - ✓ Low detection level
  - ✓ Medium detection level
  - ✓ High detection level

11. Tinh chỉnh báo cáo

Click vào đầu ô **Scanner** để mở cây thư mục > **Report**



- **Off:** Khi chọn chức năng này thì Scanner sẽ không hiển thị các report về các kết quả khi bạn quét virus trên máy.
- **Default:** Khi chọn chức năng này các thông tin về quá trình scan máy sẽ được hiển thị đầy đủ trong file report.
- **Extended:** When this option is activated, the Scanner logs alerts and tips in addition to the default information. Khi chức năng này kích hoạt thì các cảnh báo và tips sẽ được thêm vào ngoài các thông tin mặc định
- **Complete:** Ngoài việc ghi logs các file đã quét, thì tất cả các file được Avira cảnh báo và Tips cũng sẽ được thêm vào report.

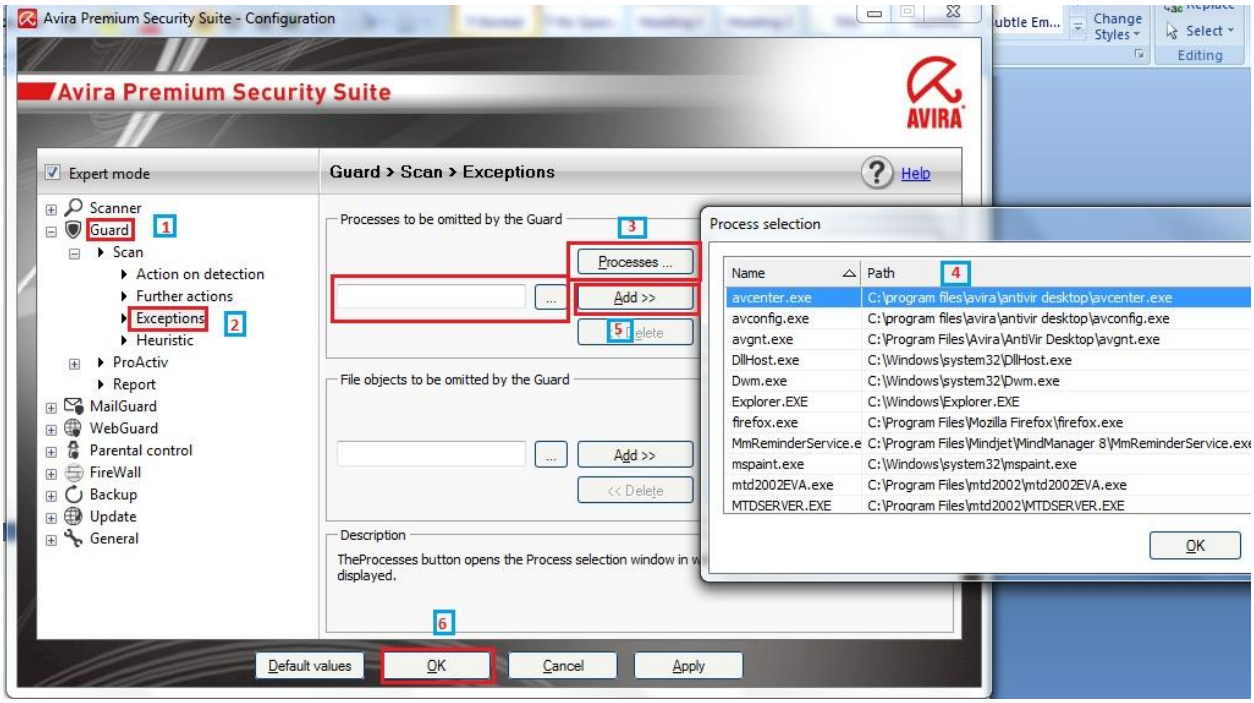
12. Đưa một chương trình, thư mục vào vùng tin tưởng

Trong trường hợp **Avira** nhận dạng lầm một ứng dụng chứa mã độc và xóa file chạy của chương trình hoặc ngăn một số hoạt động của chương trình làm chương trình hoạt động không đúng cách.

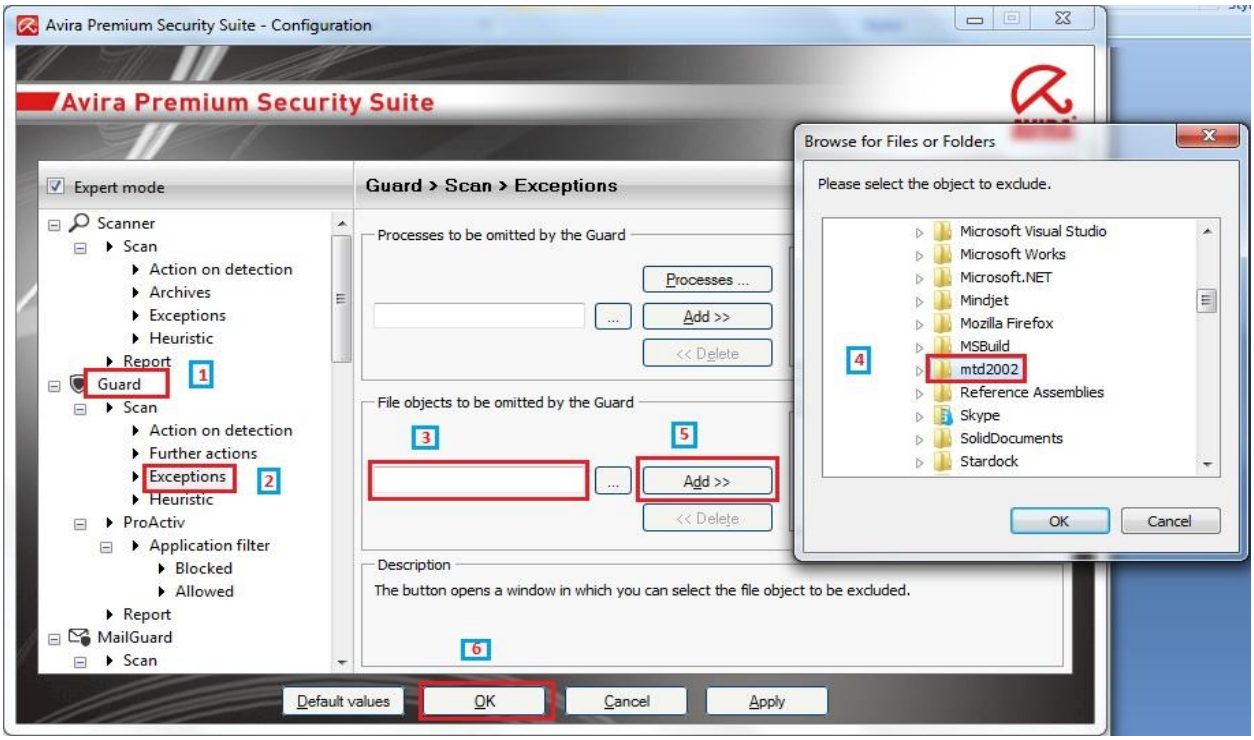
Ví dụ: Bạn có một thư mục **ABC**, một số file lưu trữ trong thư mục này bị **Avira** nhận dạng có chứa mã độc, tuy nhiên những file này rất quan trọng với bạn và bạn không muốn chúng bị **Avira** xóa đi

Để giải quyết trường hợp này, bạn có thể đưa chương trình đó vào vùng tin tưởng của **Avira**. Bạn thực hiện như sau:

- Mở giao diện của **Avira** > Click vào **Configuration** ở góc trên bên phải > Tick chọn **Expert** mode ở góc trên bên trái > Nhìn vào cột bên trái > Click vào đầu ô **Guard** để mở cây thư mục > Mở cây thư mục **Scan** > Click chọn **Exceptions** > Nhìn vào ô bên trái của phần **Exceptions** có 2 mục **Processes to be omitted by the Guard** và **File objects to be omitted by the Guard**
- **Process to be omitted by the Guard:** Chọn các chương trình không cần Avira quét.
- Chọn đường dẫn đến các process hoặc click vào **Process** để chọn bỏ qua không cần quét> **Add**> **OK**



- **File objects to be omitted by the Guard:** Chọn cách file hoặc thư mục không cần quét
- Chọn đường dẫn đến các File hoặc Folder > **Add**> **OK**

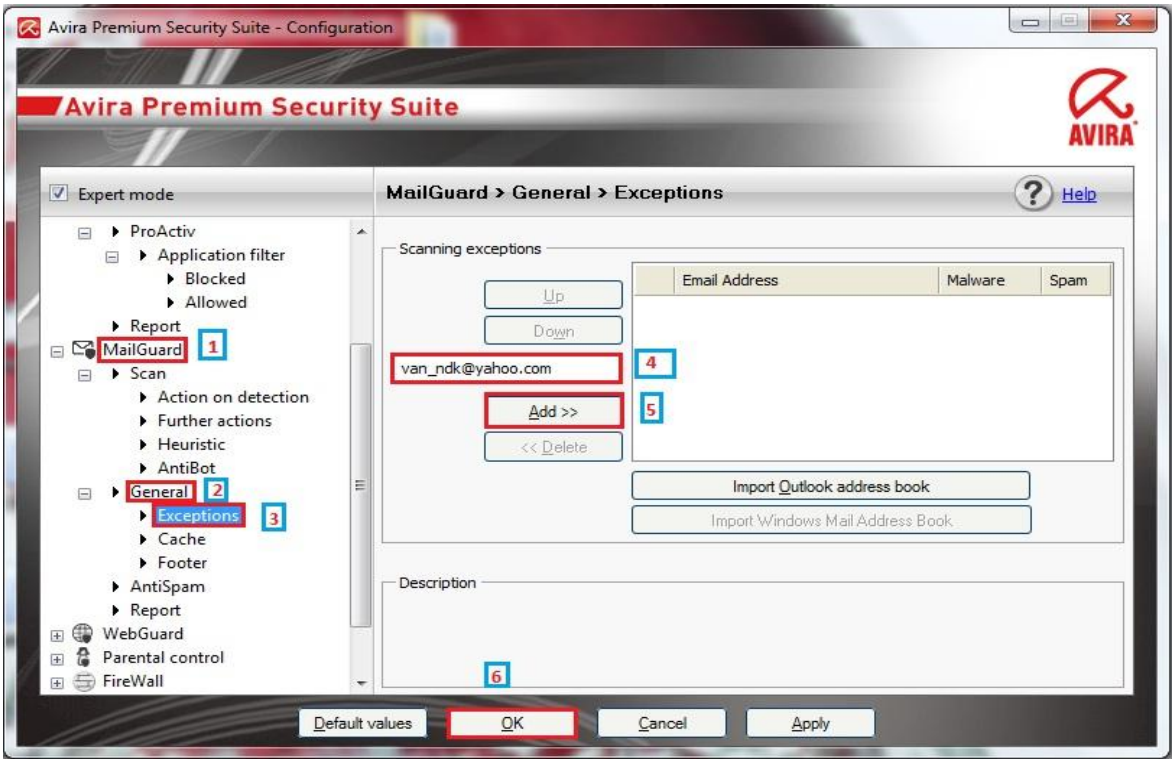


13. Cấu hình chống thư rác

Tính năng chống thư rác tích hợp với các chương trình gửi nhận mail phổ biến sau: **Microsoft Outlook, Outlook Express,** giúp phát hiện và xử lý thư rác tại ngay máy tính người dùng

Chọn **MailGuard**> click vào **General** > chọn **Exceptions** > Chọn các email không cần quét > Nhập địa chỉ email > **Add**> **OK**

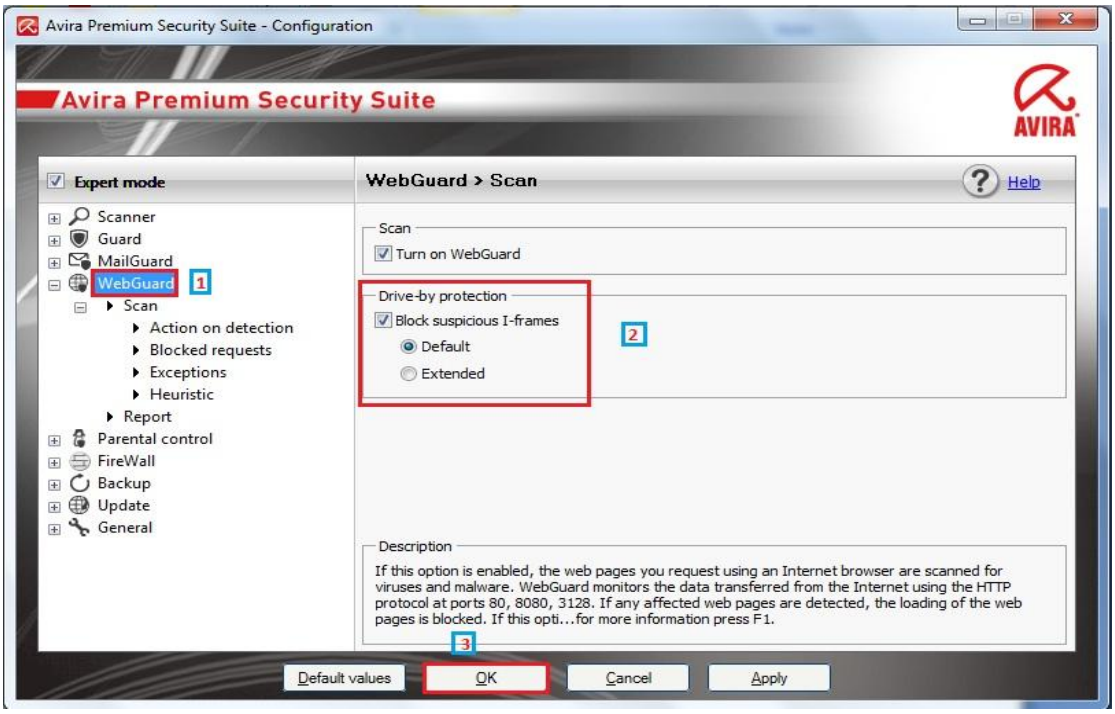
Bạn cũng có thể chọn list địa chỉ email từ **Outlook Adress Book**, click vào "**Import Outlook address book**"



14. Tính năng ngăn chặn quảng cáo

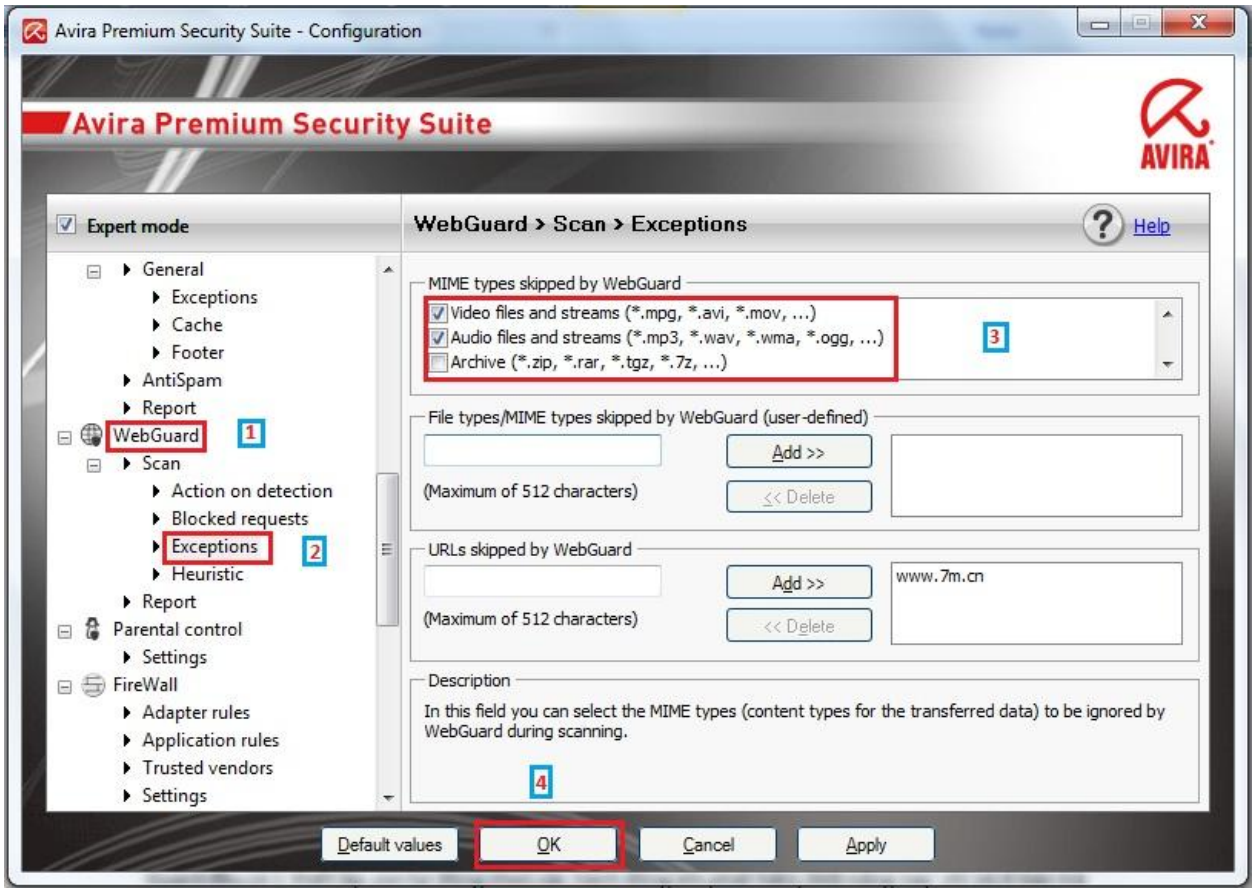
Click chọn **WebGuard** > Khung bên phải "**Drive-by protection**" rồi đánh dấu chọn vào **Block suspicious I-frames**

- **Default:** Các quảng cáo được xem là nguy hại sẽ được thay thế bằng logo của **APSS** kèm thông báo lỗi.
- **Extended :** Có tác dụng khóa banner ở cấp độ cao hơn, tuy nhiên trong một số trường hợp sẽ phá vỡ bố cục gốc của trang Web. Chọn xong, bạn bấm **OK** để cập nhật thay đổi.



15. Tùy chọn các chức năng bỏ quét các dạng file

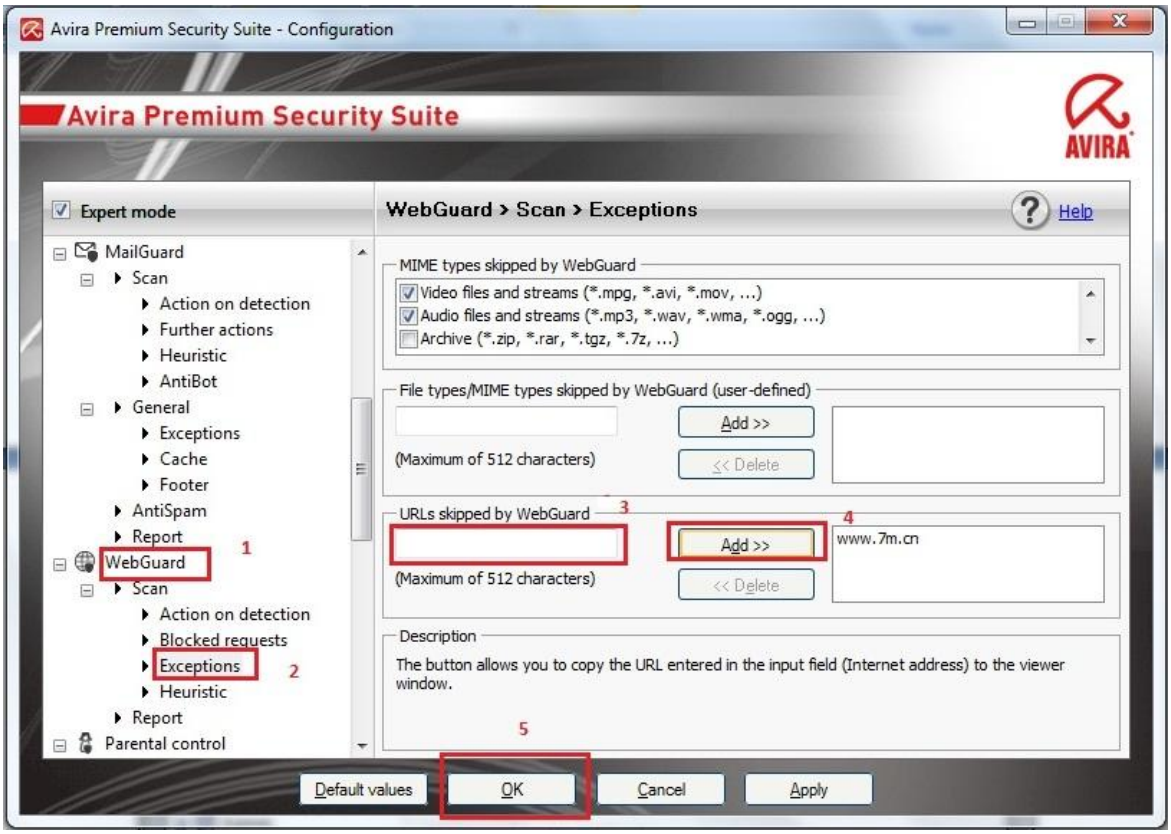
Click **WebGuard**> **Scan**> **Exceptions**> Khung bên phải phần "**MINE types Skipped by WebGuard**", chek chọn các dạng file bạn không muốn **Avira** quét > **OK**.



Bạn cũng có thể định dạng file mà bạn không muốn **Avira** quét bằng cách nhập vào ô textbox của phần "**File types/MIME types skipped by WebGuard**" > **Add** và click **OK**

16. Tùy chọn chức năng bỏ quét các website

Click **WebGuard**> **Scan**> **Exceptions**> Khung bên phải phần "**URL Skipped by WebGuard**", thêm địa chỉ web bạn muốn Avira không quét vào rồi **Add > OK**.



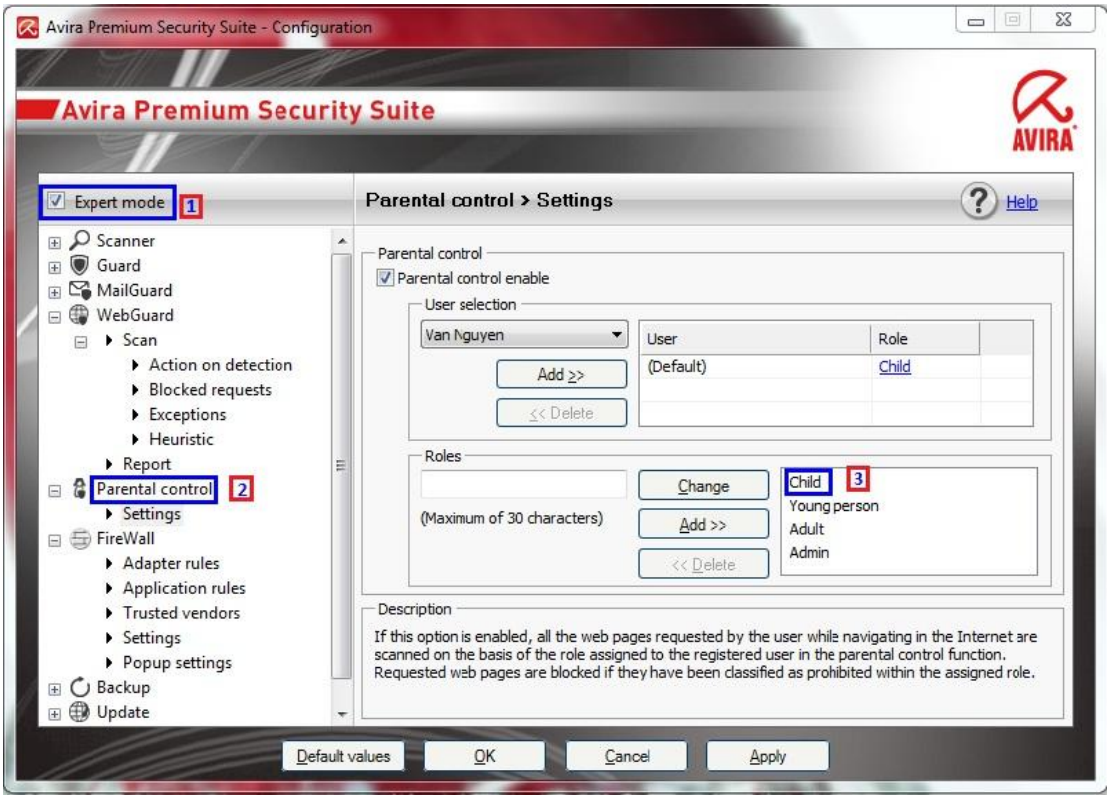
17. Tùy chỉnh tính năng kiểm soát người dùng (Parental Control)

Bạn muốn bảo vệ con em mình một cách an toàn khi chúng dạo chơi trên Internet vì bạn lo lắng rằng hiện nay có rất nhiều website không lành mạnh có tính chất bạo lực, người lớn,phân biệt chủng tộc,…Rất đơn giản, với chức năng ParentalControl bạn dễ dàng khóa các địa chỉ website trên với giao diện thân thiện, dễ sử dụng, thiết lập các điều kiện sàng lọc có sẵn hoặc các thông số dựa trên yêu cầu của bạn.
Một số cách thiết lập cơ bản nhưng hiệu quả như sau:

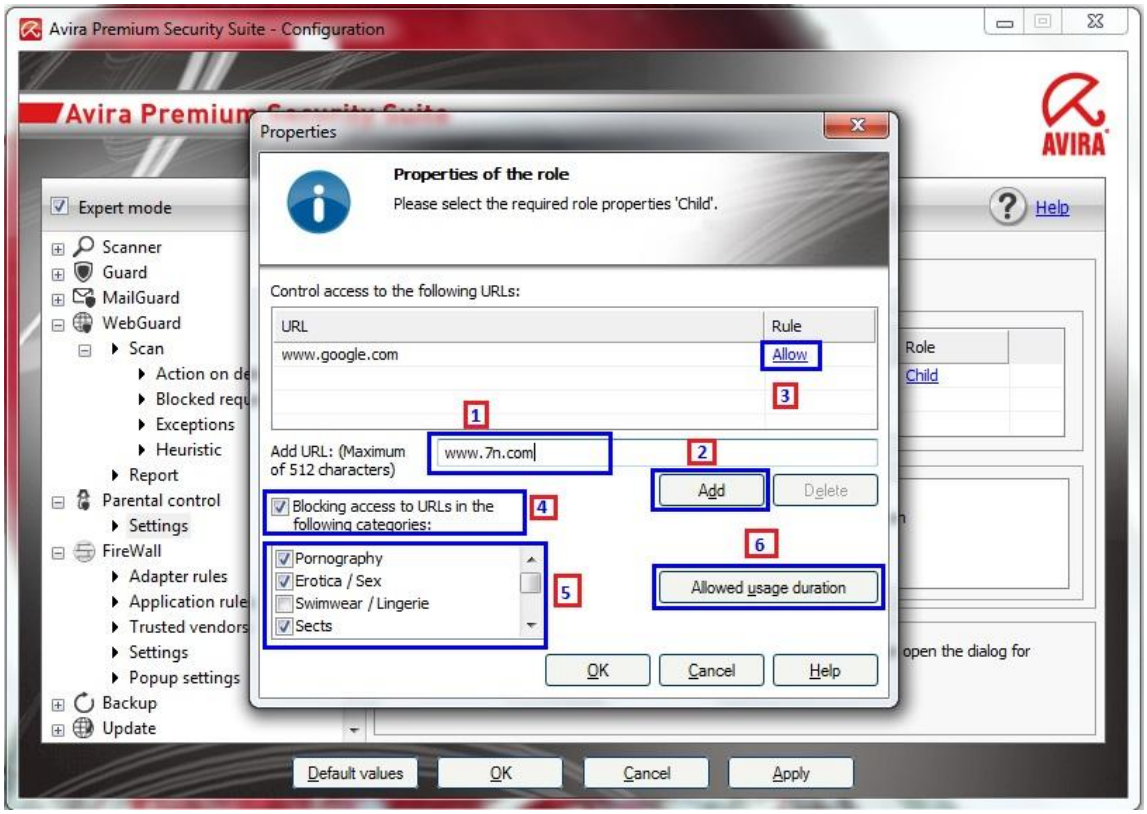
- **Cài đặt quyền truy cập cho các user sử dụng trong cùng 1 máy:**

Nhấn đúp chuột vào biểu tượng của APSS để mở **Avira** > Sau đó bạn nhấn **F8** > Đánh dấu chọn vào **Expert mode** và vào mục **Parental Control** > Khung bên phải của **Parental Control**

- ✓ **User selection:** Cài đặt quyền cho từng user bằng cách chọn User và nhấn vào Add. Bạn có thể thay đổi vai trò của từng User bằng cách nhấn đúp chuột vào từng Role.
- ✓ **Role:** Tạo các Role

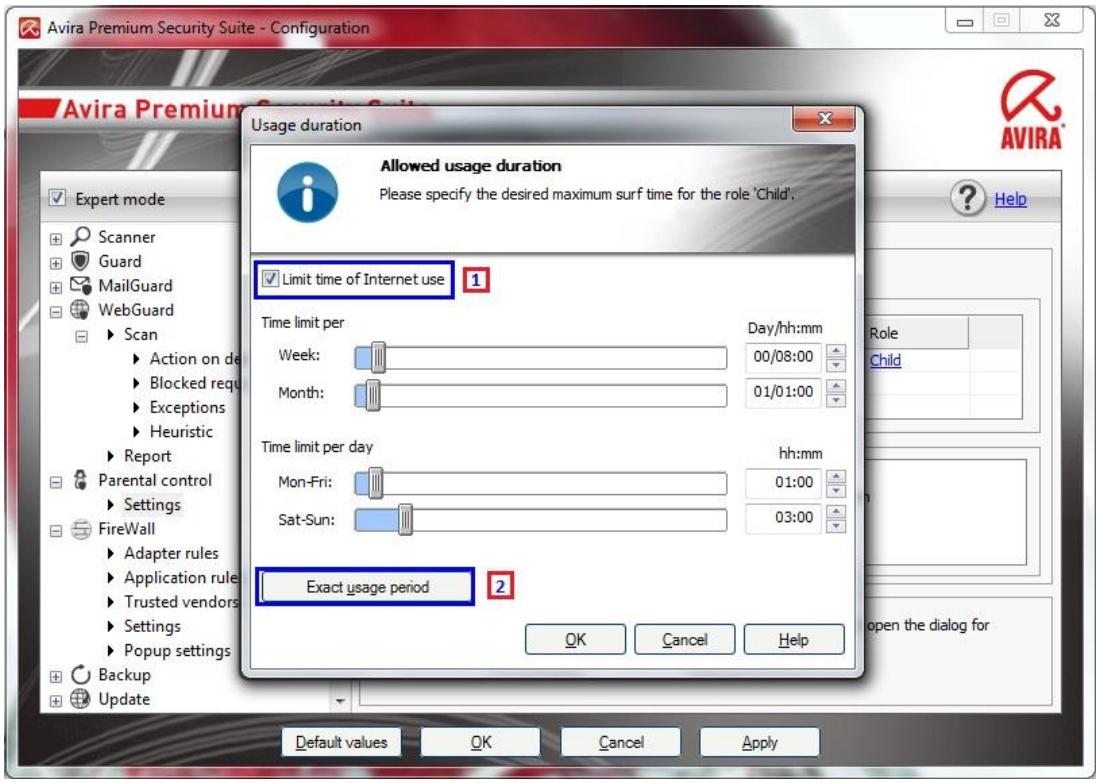


- **Cài đặt quyền cho từng Role:**
  Nhận đúp chuột vào từng Role **Child, Young person, Adult, Admin** để cài đặt
  - ✓ **Quyền truy cập website:**
    - Nhập đường link website vào Textbox **Add**
    - **URL** > Nhấn vào **Add** để thêm vào list> Nhấn vào **Role [3]** Cài đặt quyền **Allow** hoặc **Block**
  - ✓ Cấu hình các trang web được phép truy cập cũng như block các website nằm trong danh mục không phù hợp, lành mạnh: Đánh dấu chọn vào **Blocking access to URLs in the following categories[4]** > Đánh dấu chọn các thể loại website bạn muốn khóa **[5]**



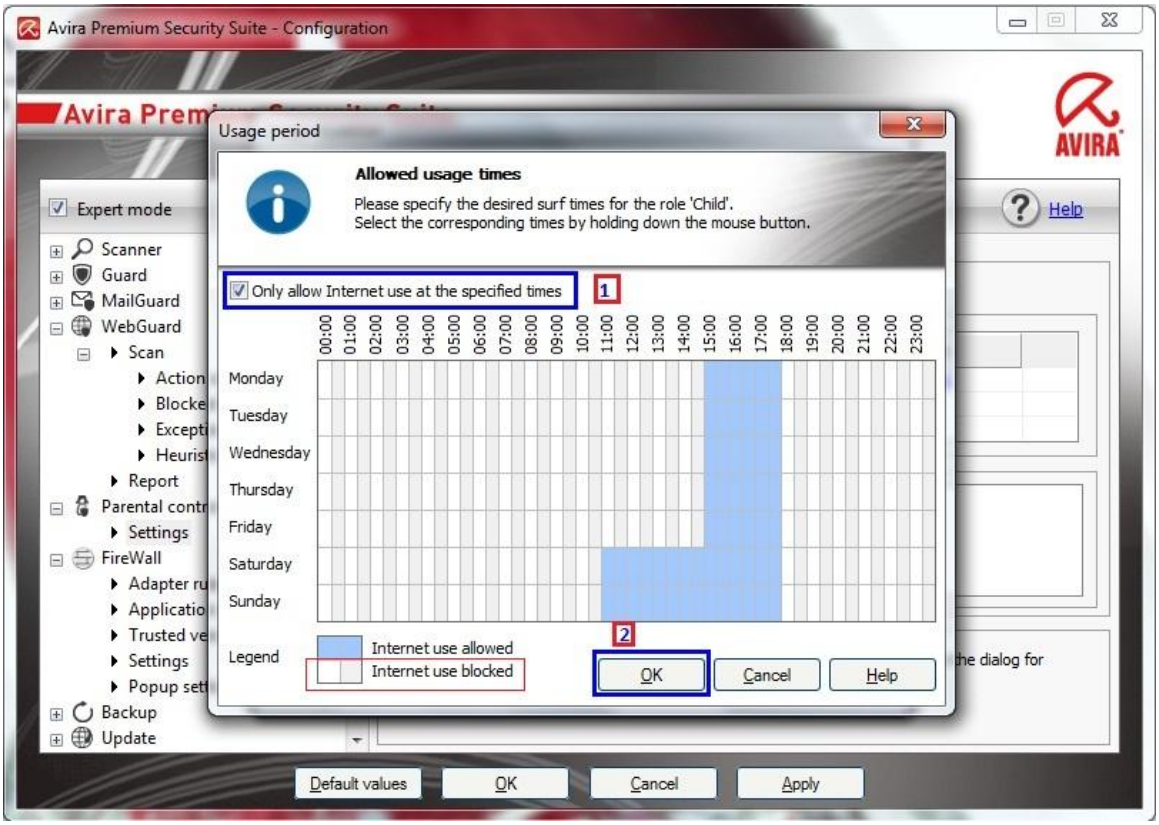
➢ **Cấu hình thời gian được phép truy cập:**

✓ Thiết lập thời gian sử dụng Internet bằng cách nhấn vào **Allowed usage duration[6]:** Đánh dấu chọn vào **Limit time of Internet use** > Cài đặt thời gian theo theo Tháng, Tuần, Ngày



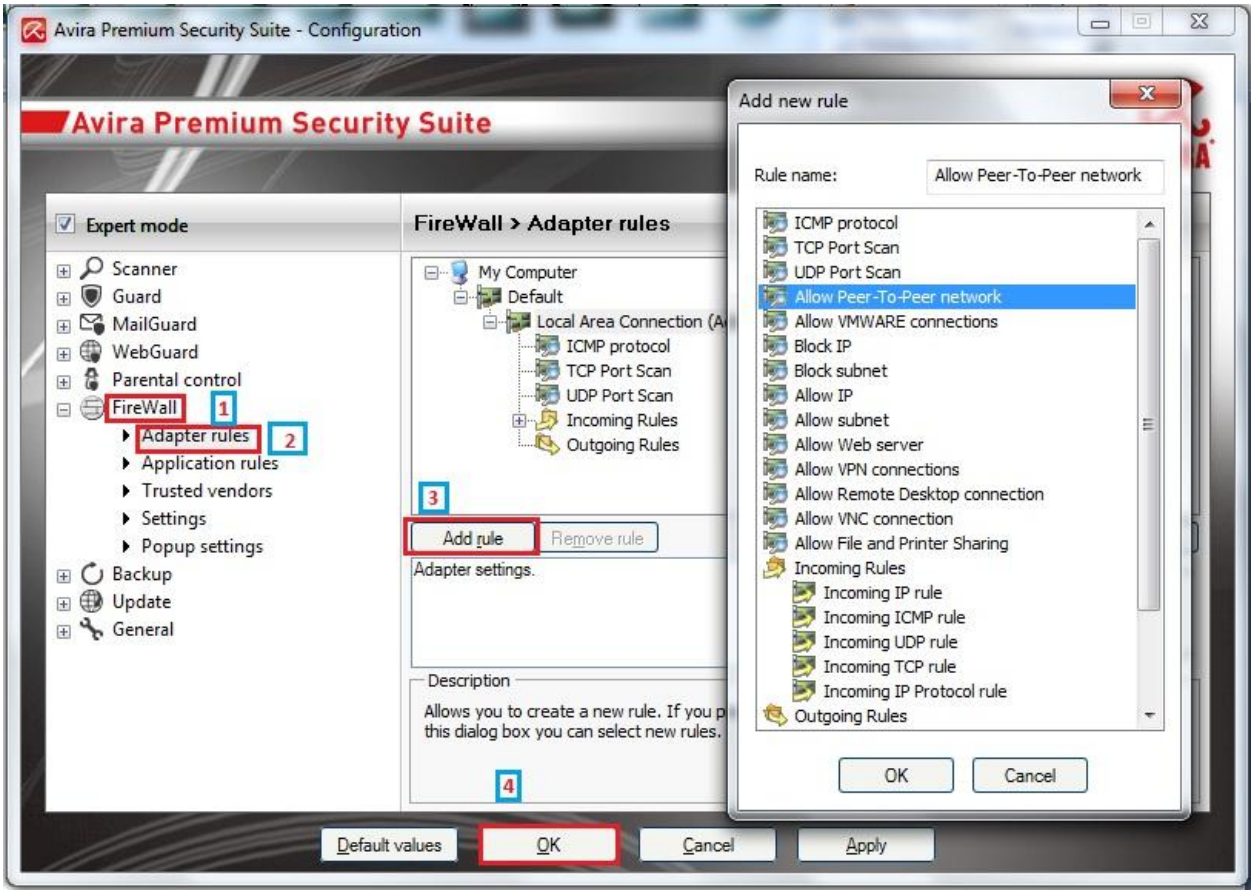
➢ **Nếu bạn muốn thiết lập chính xác thời gian theo từng ngày:**

✓ Nhấn đúp vào **Exact usage period** > Đánh dấu chọn vào **Only allow Internet use at the specified times** > Chọn thời truy cập hoặc khóa truy cập bằng cách nhấp đúp vào các hình chữ nhật theo ngày, giờ> Xong nhấn **OK** để kết thúc.



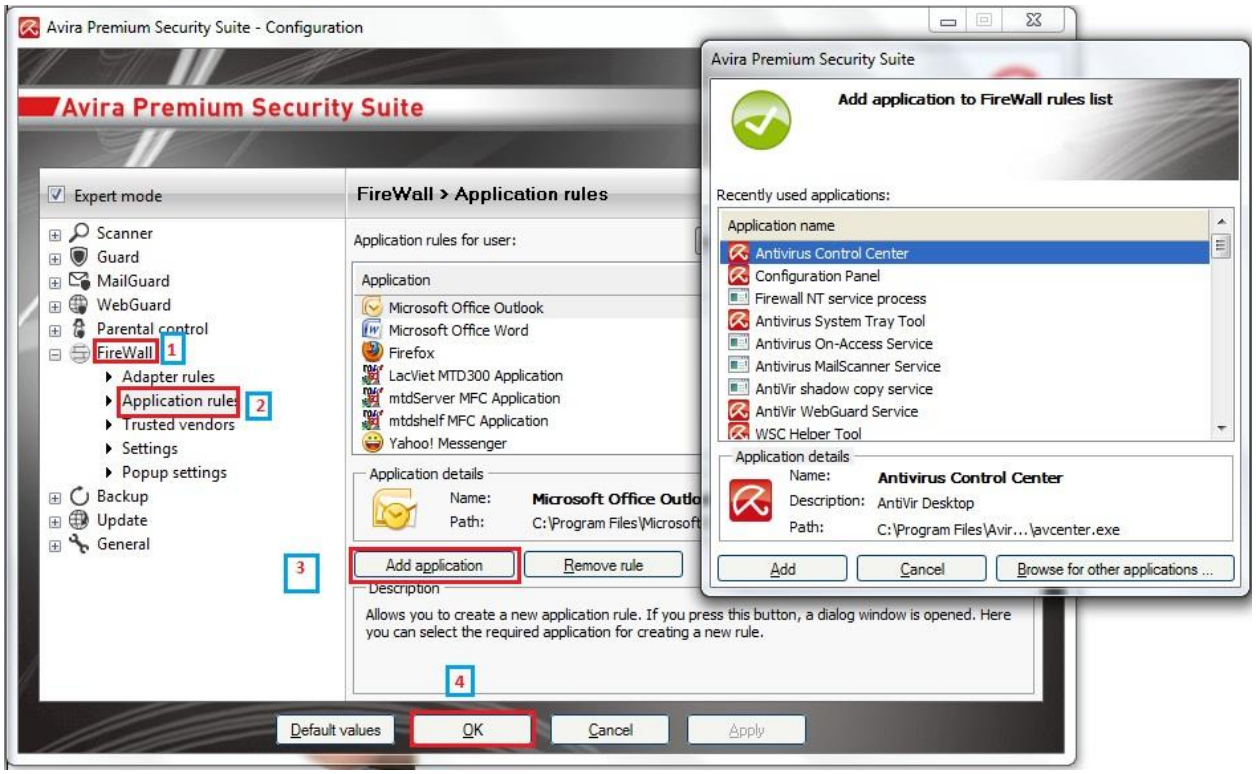
18. Khắc phục sự cố không kết nối được mạng nội bộ

Để khắc phục lỗi này, bạn vào **Firewall** > **Adapter rules** và bấm nút **Add rule**. Sau đó, trong danh sách liệt kê, bạn bấm **Allow Peer-To-Peer network** rồi bấm **OK**. Tiếp theo, bạn bấm **Add rule** lần nữa rồi chọn **Allow File and Printer Sharing** > **OK**.



19. Cấu hình các chương trình được sử dụng cho từng user

Bạn muốn thiết lập các chương trình được phép sử dụng cho từng user, bạn thực hiện như sau: Click vào **Firewall** > Click **Application Rule** > Khung bên phải "**Application**"> **Allow**> Bạn chọn **Allow** (Cho phép) hoặc **Deny**(Từ chối)



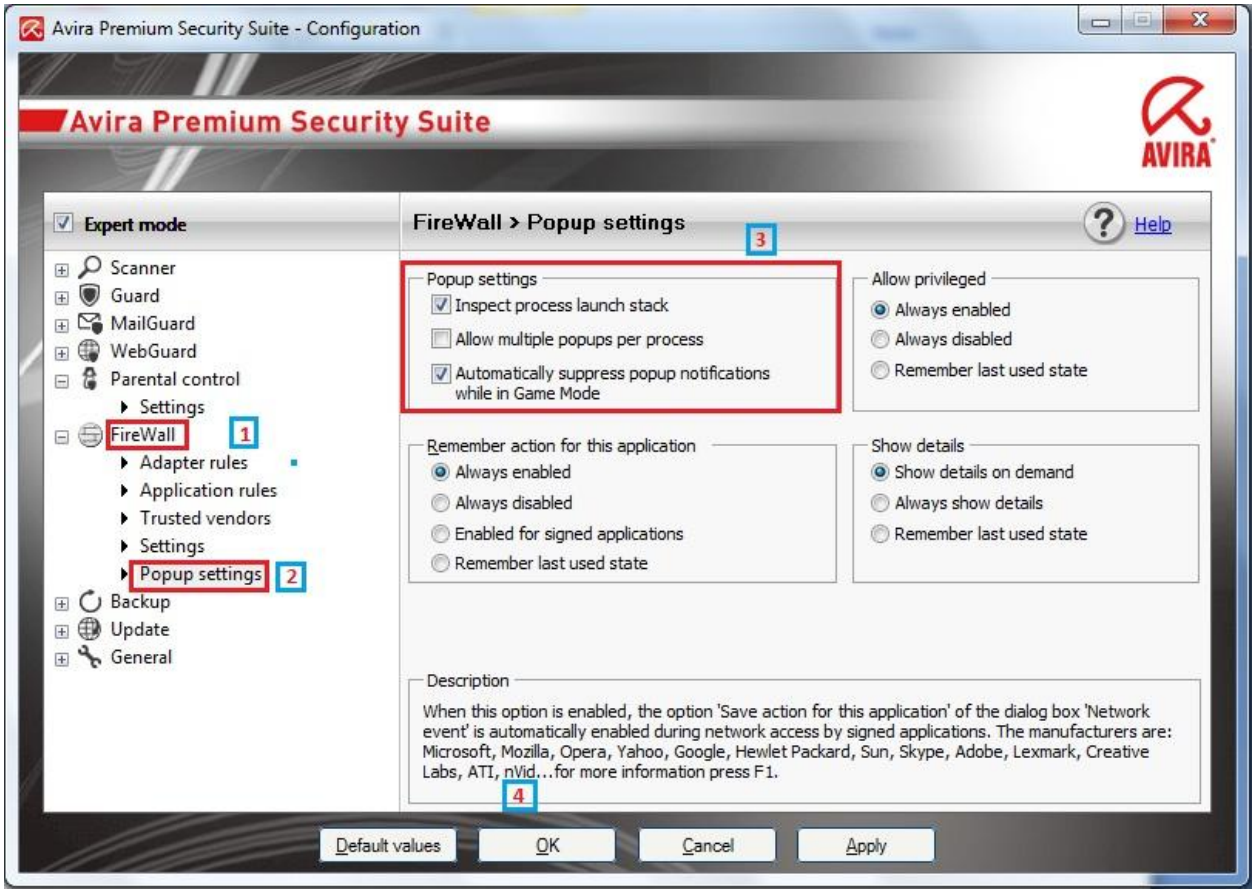
Để add thêm 1 chương trình mới :

- **Firewall > Application rules** > **Add application >** Chọn chương trình cho phép user đó sử dụng> **Add > OK**

20. Ngăn chặn pop-up

Firewall > **Popup settings :** Đánh dấu chọn vào **Inspect process launch stack**.

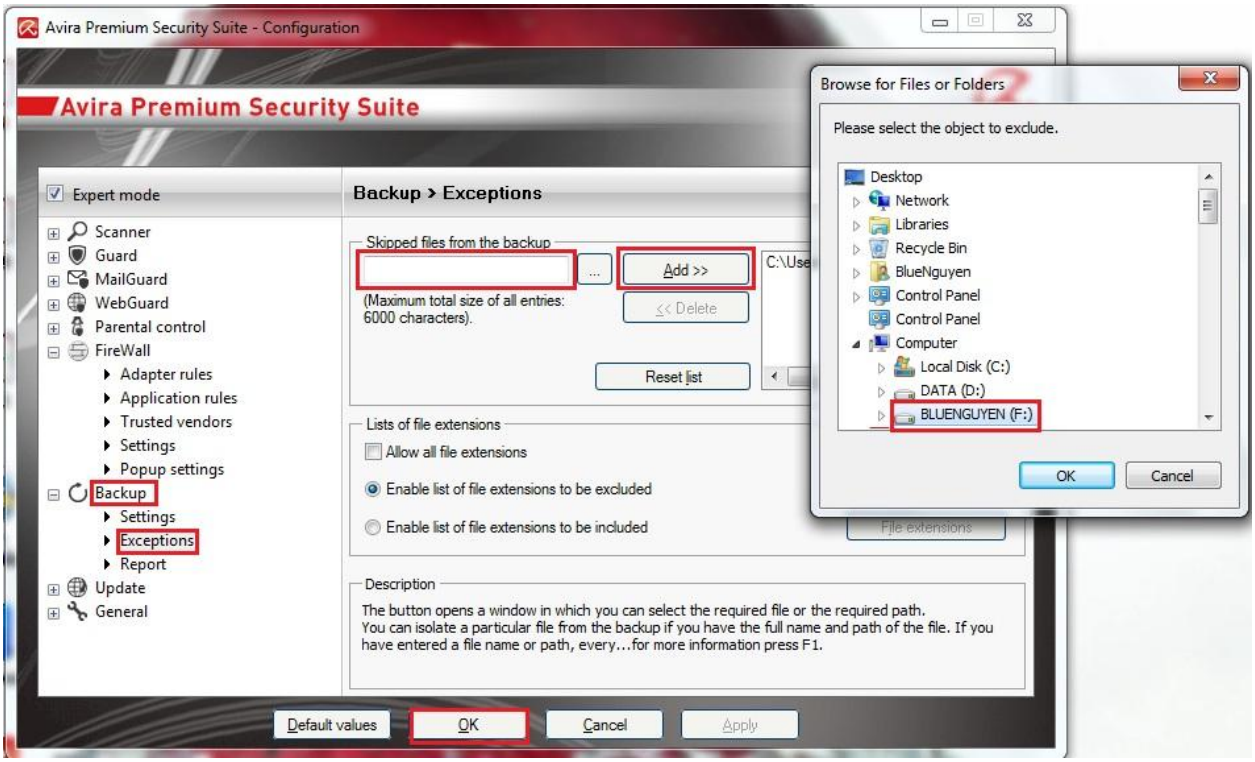
Khi chơi game thì APSS sẽ làm việc ở chế độ Game Mode, để chương trình ngăn chặn những pop-up xuất hiện ở khoảng thời gian này, bạn đánh dấu vào **Automatically suppress popup notifications while in Game Mode**. Chọn xong, bạn bấm **OK** để lưu lại.



21. Bỏ chọn các tập tin, thư mục không back-up

Firewall > **Popup settings:** Đánh dấu chọn vào **Inspect process launch stack**. Khi chơi game thì APSS sẽ làm việc ở chế độ Game Mode, để chương trình ngăn chặn những pop-up xuất hiện ở khoảng thời gian này, bạn đánh dấu vào **Automatically suppress popup notifications while in Game Mode**. Chọn xong, bạn bấm **OK** để lưu lại.

- **Backup** > **Exceptions:** Bỏ chọn các file không backup
- Khung bên phải "**Skipped files from the backup**" , bạn chọn file hoặc thư mục không **backup** > Click **Add > OK**



22. Thông tin hỗ trợ kỹ thuật

Công ty Cây Dù Đỏ sẽ hỗ trợ kỹ thuật về Avira từ **8h đến 22h** đêm hàng ngày (kể cả ngày thứ 7). Khi gặp bất cứ sự cố nào trong lúc sử dụng phần mềm, vui lòng liên hệ với chúng tôi theo các thông tin sau:

- Hỗ trợ qua điện thoại: **08. 3812 5678 – 0916. 06 2224 – 0907. 07 2224**
- Hỗ trợ qua Email: support@caydudo.com
- Hỗ trợ chat trực tuyến: vui lòng truy cập vào website www.caydudo.com để chat với các nick hỗ trợ kỹ thuật. Hoặc truy cập vào đường link sau: http://www.caydudo.com/ho-tro-khach-hang.aspx để nhập trực tiếp vấn đề bạn gặp phải và gửi về cho chúng tôi.
- Nếu bạn có vốn Anh Văn tốt có thể liên hệ trực tiếp với Avira quốc tế theo email sau: support.my@avira.com