NTS SECURITY

Enhancing your business

HƯỚNG DẪN SỬ DỤNG NHANH KSOS

Kaspersky Lab Việt Nam

Cập nhật tháng 7/2011

Mục lục

I. Cài đặt

1. Lưu ý trước khi cài đặt chương trình

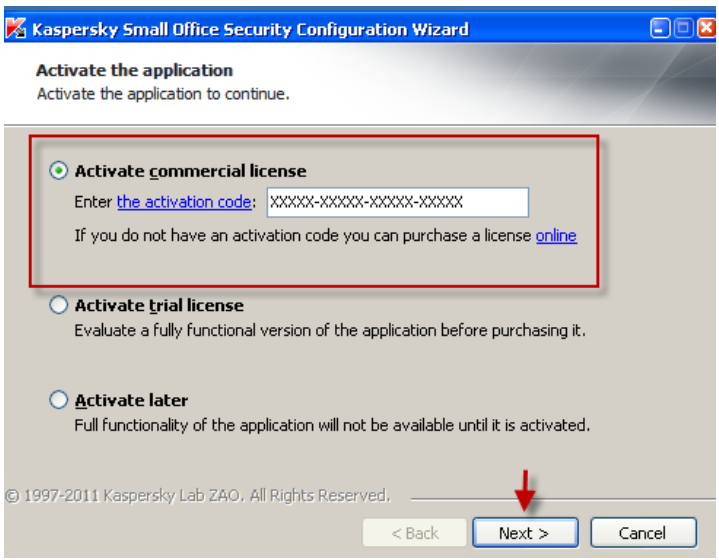
- Trước khi cài đặt, bạn phải remove sạch sẽ phần mềm antivirus của hãng khác
- Đảm bảo giờ hệ thống trùng khớp với hiện tại mới có thể kích hoạt được bản quyền
- Máy tính phải được kết nố Internet mới có thể kích hoạt được bản quyền
- Hệ điều hành hỗ trợ cài đặt:
  - Máy trạm: Windows 2000 Pro, Windows XP, Windows Vista, Windows 7 (bao gồm 64bit)
  - Máy chủ: Windows Server 2000, Windows Server 2003, Windows Server 2008 (bao gồm 64bit và R2)

2. Tiến hành cài đặt chương trình

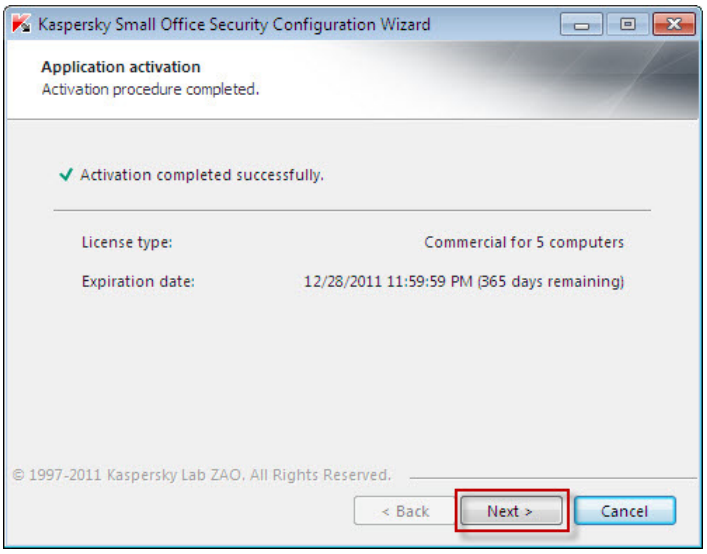
- Đến từng máy tính trong công ty, sử dụng source cài đặt được cung cấp trong CD để tiến hành cài đặt. Bạn cũng có thể tải source cài đặt tại: http://www.kaspersky.com/downloads_small_office_security

- Các bước cài đặt bạn chọn theo tùy chỉnh mặc định

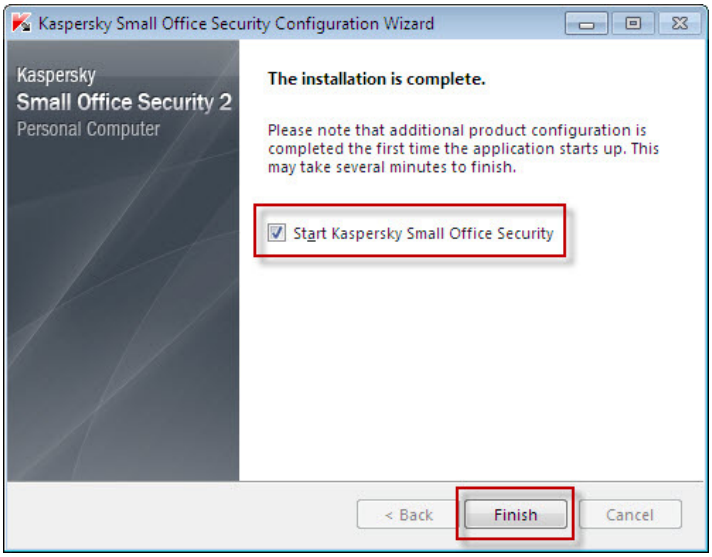
- Sau khi cài đặt thành công, bước kích hoạt bản quyền xuất hiện như hình dưới: bạn điền vào mã "Activation code" được ghi trên thẻ bản quyền (bao gồm 20 ký tự) sau đó chọn **Next**



Sau khi kích hoạt thành công, thông tin bản quyền sẽ xuất hiện. Bạn chọn **Next** để qua bước tiếp theo.

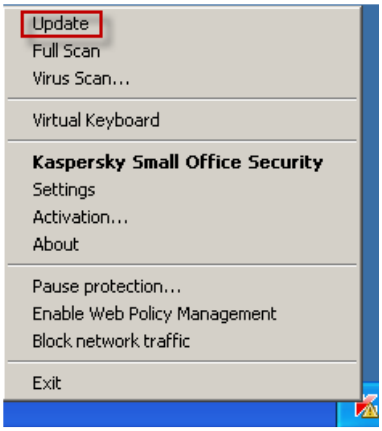


Quá trình cài đặt hoàn thành, chọn **Finish**

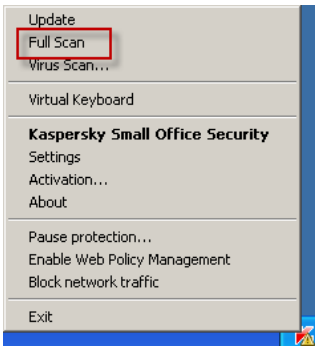


II. Các bước nên thực hiện sau khi chương trình được cài đặt thành công

- **Cập nhật cơ sở dữ liệu cho chương trình**: Click chuột phải vào biểu tượng chương trình Kaspersky ở góc phải cuối màn hình chọn **Update** (hình dưới). Lần đầu quá trình cập nhật tốn khoảng thời gian nhất định để hoàn thành (vì dung lượng gói cập nhất lớn). Những lần cập nhật sau này diễn ra rất nhanh chóng



- **Quét virus toàn bộ máy tính**: Sau khi cập nhật thành công, bạn nên tiến hành quét toàn bộ máy tính cho chương trình. Click chuột phải vào biểu tượng chương trình Kaspersky ở góc phải cuối màn hình chọn **Full Scan** (hình dưới). Mục đích của quá trình Full Scan là giúp Kaspersky loại bỏ tất cả các chương trình độc hại đang có trên máy tính (tính từ lúc cài Kaspersky về trước) và giúp Kaspersky ghi nhớ, đánh dấu các tập tin của máy tính, giúp chương trình hoạt động hiệu quả sau này.



III. Một số lưu ý để sử dụng tốt chương trình

Kaspersky bảo vệ máy tính trong thời gian thực.Tuy nhiên, trong quá trình sử dụng, bạn nên thực hiện những lưu ý sau để giúp chương trình hoạt động hiệu quả nhất:

- Đảm bảo chương trình được cập nhật (update) thườngxuyên: Nếu chương trình không được cập nhật thường xuyên, chương trình không có khả năng tiêu diệt các virus mới xuất hiện.

- Không tắt chương trình trong mọi thời điểm: Lúc bạn tắt chương trình Kaspersky, một số dòng virus có thể xâm nhập vào máy tính và vô hiệu hóa hoạt động của chương trình antivirus hoặc phá hoại dữ liệu dẫn đến việc không còn khả năng cứu chữa

- Định kỳ một khoảng thời gian (có thể 1 tháng) tiến hành quét toàn bộ máy tính một lần: Việc quét toàn bộ máy tính giúp gia tăng hiệu quả hoạt động của chương trình Kaspersky, giúp chương trình loại bỏ hoàn toàn tất cả tập tin và phần mềm độc hại, phát hiện lỗi hệ thống, lỗi chương trình, ghi nhớ tập tin,…

- Đặt password bảo vệ chương trình để không cho người khác can thiệp tùy chỉnh hoặc tắt chương trình đi. Nếu nhân viên công ty thường xuyên tắt chương trình Kaspersky đi, hoặc tiến hành các tùy chỉnh không đúng, làm chương trình hoạt động không đúng cách. Trường hợp này, sau khi tiến hành các tùy chỉnh theo ý của bạn, bạn nên tiến hành đặt password cho chương trình để nhân viên không thể tắt, chỉnh sửa cấu hình chương trình Kaspersky

IV. Một số tùy chỉnh thường sử dụng

1. Đặt mật khẩu cho chương trình

- Mục đích của việc đặt password là không cho người khác can thiệp, tùy chỉnh tính năng của chương trình, không cho tắt chương trình (sẽ có yêu cầu hỏi mật khẩu)

- Thực hiện: Vào giao diện chính của chương trình > chọn Settings > chọn thẻ Password > chọn Enable Password Protection > bạn điền password vào > chọn thêm Application Settings Configuration (để khi thay đổi cấu hình sẽ cần mật khẩu)

2. Tùy chỉnh update theo ý bạn

- Mặc định, chương trình Kaspersky cứ 2h sẽ kết nối đến máy chủ của hãng Kaspersky để cập nhật cơ sỡ dữ liệu antivirus. Bạn có thể tạo ra một lịch update theo ý bạn. Vd: tạo lịch update là 8h Kaspersky sẽ cập nhật 1 lần hoặc sẽ cập nhật vào lúc 12h 15PM hàng ngày, hoặc,…

- Thực hiện: Vào giao diện chính của chương trình > chọn Settings > chọn thẻ Update > chọn Setting > tại thẻ Run mode > bạn cấu hình chính sách cập nhật theo ý bạn

3. Quản lý các tập tin bị Kaspersky xử lý

- Mặc định, khi Kaspersky xử lý (xóa, cách ly) bất cứ một tập tin nào, chương trình đều lưu lại tập tin đó tại phần Detected của Kaspersky. Bạn có thể vào đây để xem, phục hồi tập tin (nếu nó rất quan trọng), xóa luôn, gửi mẫu,..Thực hiện: mở giao diện chính của chương trình > chọn Quarantine > tại đây sẽ hiện tất cả các tập tin đã bị Kaspersky xử lý và bạn có thể tiến hành thực hiện các hành động cần thiết

4. Add tin tưởng chương trình

- Vd: Kaspersky nhận dạng lầm một chương trình nội bộ của công ty bạn là virus, và không cho chương trình này hoạt động. Tuy nhiên, bạn chắc rằng chương trình này không hề nguy hiểm và bạn rất cần để mở chương trình này gấp. Trước tiên, bạn đưa chương trình này vào vùng tin tưởng của Kaspersky để cho chương trình tạm thời hoạt động. Sau đó, bạn có thể gửi mẫu chương trình đến virus@kaspersky.vn để Kaspersky Lab phân tích chương trình xem có chứa mã độc hại không, nếu không có, trong lần update tiếp theo Kaspersky sẽ không nhận dạng chương trình chứa mã độc nữa.

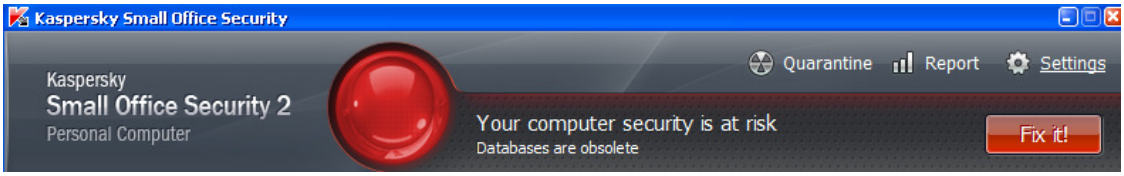
- Thực hiện đưa chương trình vào vùng tin tưởng: Mở giao diện chính của chương trình > Chọn Settings > chọn Protection > chọn Threat and Exclusion > chọn Setting tại phần Exclusion

    - Tại tab Trusted application: bạn có thể tiến hành add tin tưởng chương trình dựa trên tập tin thực thi chính của chương trình (tập tin thực thi chính của chương trình là “exe”)
    - Tại tab Exclusion rules: bạn có thể add tin tưởng một folder (có thể là folder chứa dữ liệu hoặc folder chứa file chương trình) vào vùng tin tưởng của Kaspersky.

5. Xem trạng thái bảo vệ máy tính

- Mở giao diện chính của chương trình. Dòng thông báo như hình bên dưới sẽ cho bạn thấy được trạng thái hoạt động của chương trình Kaspersky là đang an toàn hay gặp nguy hiểm

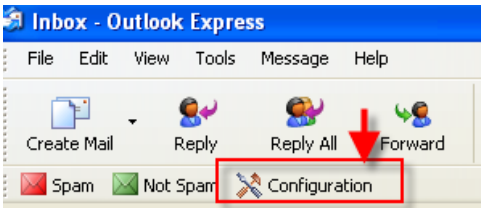
- Nếu thông báo là “Your computer security is at risk”> máy tính của bạn có khả năng gặp nguy hiểm. Bạn bấm vào dòng thông báo, lúc này chương trình sẽ hiển thị các lý do tại sao gặp nguy hiểm (lâu ngày không cập nhật, một vài tính năng quan trọng bị tắt đi,…) và đề xuất bạn cách xử lý các lỗi này.
- Trong trường hợp bạn tắt một vài tính năng mà bạn thấy là không cần thiết của Kaspersky (vd: tắt Anti-Spam) > lúc này chương trình báo là máy tính có khả năng gặp nguy hiểm > bạn không cần quan tâm đến vấn đền này vì bạn biết rõ nguyên nhân dẫn đến thông báo này và nó không ảnh hưởng đến khả năng bảo mật của máy tính



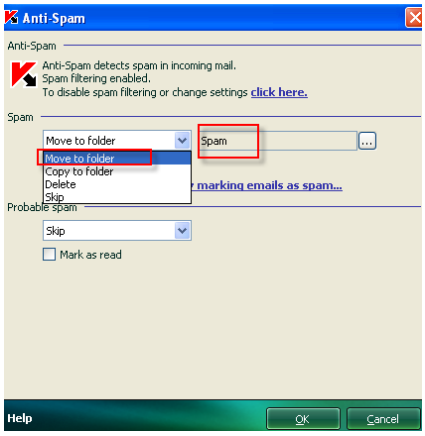
6. Cấu hình tính năng Anti-Spam

Tính năng Anti Spam của Kaspersky tích hợp với các chương trình email: Outlook Express, Microsoft Outlook, Windows Mail,…cung cấp khả năng xử lý thư rác. Khi đã nhận dạng được một email là thư rác, mặc định chương trình sẽ bỏ qua thư rác này (không xóa thư mà chỉ thêm chữ Spam vào tựa đề email). Nếu bạn muốn thay đổi tùy chỉnh hành động của Kaspersky đối với thư rác bạn làm như sau:

- Nếu đang dùng Microsoft Outlook, bạn mở chương trình Microsoft Outlook > Vào Tools > Option > Anti-Spam. Nếu dùng Outlook Express bạn chọn vào Configuration (như hình dưới)



- Cửa sổ cấu hình hành động xuất hiện, bạn có thể đưa ra hướng xử lý khi một thư rác được phát hiện. Chúng tôi khuyến khích bạn đưa ra hướng xử lý là Move to folder để bạn dễ quản lý thư rác đồng thời không sợ bị mất email (hình dưới)



7. Phục hồi cấu hình về mặc định

- Bạn tiến hành nhiều tùy chỉnh của chương trình và làm cho chương trình hoạt động không hiệu quả và không đúng cách. Tuy nhiên, bạn quên không biết làm sao để phục hồi lại các tùy chỉnh của mình về mặc định
- Bạn có thể tiến hành khôi phục lại tùy chỉnh mặc định của chương trình Kaspersky bằng cách: Mở giao diện chính của chương trình > chọn Settings > tại thẻ General > chọn Restore > các bước tiếp theo bạn giữ mặc định và chọn Next để hoàn thành

8. Cấu hình chương trình tự động xử lý trong quá trình scan bằng tay

- Khi bạn tiến hành ra lệnh bằng tay để Kaspersky thực hiện Full Scan (quét toàn bộ máy tính), hoặc Quick Scan (quét nhanh hệ thống). Nếu phát hiện một tập tin độc hại, chương trình sẽ yêu cầu bạn đưa ra hướng xử lý (xóa, bỏ qua, cách ly,…)

- Bạn có thể cấu hình cho chương trình tự động xử lý luôn (tẩy xóa mà không hỏi người dùng) bằng cách: vào giao diện chính của chương trình > chọn Settings > chọn thẻ Scan > đánh dấu vào ô “Select action” trong phần Full Scan và Quick Scan

9. Chạy an toàn

- Tính năng chạy an toàn giúp bạn chạy một chương trình hay truy cập Internet trong một môi trường ảo hoàn toàn, virus không thể nào lợi dụng chương trình đang chạy hay qua các trang web mà bạn truy cập để lây nhiễm vào máy tính. Tính năng này rất phù hợp trong trường hợp bạn cần test phần mềm lạ hay truy cập các trang web không tin tưởng

- Cách sử dụng: khi muốn chạy an toàn, bạn click chuột phải vào biểu tượng trình duyệt Internet hoặc biểu tượng của ứng dụng chọn “Safe Run”

10. Quản lý truy cập Internet và sử dụng máy tính

Bạn có thể cấu hình ngăn truy cập đến một số trang web chỉ định cũng như có thể giới hạn thời gian truy cập Internet của nhân viên

Mở giao diện chính của chương trình > chọn Web Policy Management > chọn Enable Web Policy Management > chọn account đăng nhập máy tính (account của nhân viên đang sử dụng) mà bạn cần áp đặc policy

- Nếu bạn muốn giới hạn thời gian truy cập Internet > trong phần Internet > chọn Usage > chọn Enable control > chọn Limit usage on the selected days > bạn sử dụng chuột để đánh dấu khoảng thời gian bị khóa truy cập web. Ngoài ra, bạn cũng có thể đánh dấu chọn Limit daily usage time nếu muốn áp đặt chính sách là trong một ngày được phép truy cập Internet bao nhiêu giờ
- Nếu bạn muốn ngăn truy cập một số địa chỉ web > trong phần Internet > bạn chọn Access to Websites > chọn Enable control > chọn Blocked URLs > điền vào địa chỉ web cần ngăn (vd: kaspersky.vn)
- Bạn cũng có thể ngăn tải về nhạc, video, chương trình bằng cách cấu hình tại downloading file

Ngoài ra, bạn cũng có thể cấu hình thời gian được phép sử dụng máy tính bằng cách cấu hình tại phần Computer > chọn usage > chọn Enable control > chọn Limit usage on the selected days > bạn sử dụng chuột để đánh dấu khoảng thời gian bị khóa sử dụng máy tính. Bạn cũng có thể đánh dấu chọn Limit daily usage time nếu muốn trong một ngày được phép sử dụng máy tính bao nhiêu giờ (quá thời gian cho phép máy tính sẽ bị khóa không cho sử dụng)

Bạn cũng có thể cấu hình khoảng thời gian cho phép sử dụng một ứng dụng nào đó bằng cách: tại phần Computer > chọn Running applications > chọn Enable control > chọn Allowed > chọn add > tại đây bạn sẽ lựa chọn file chạy của chương trình cũng như cấu hình khoảng thời gian nào ứng dụng đó không được phép sử dụng

Bạn cũng có thể cấu hình cấm sử dụng luôn một ứng dụng nào đó bằng cách chọn thẻ Blocked > chọn Add > đi đến đường dẫn file chạy của ứng dụng mà bạn cần cấm sử dụng!

11. Mã hóa dữ liệu

Tính năng mã hóa dữ liệu giúp bạn tạo một thư mục mã hóa để chứa các dữ liệu quan trọng trên máy tính của bạn. Khi một người nào đó muốn truy cập dữ liệu trong thư mục này, yêu cầu điền vào mật khẩu sẽ xuất hiện

Cấu hình: Mở giao diện chính của chương trình > chọn Tools > chọn Data Encryption > chọn Create container > điền tên thư mục cần tạo, dung lượng thư mục, mật khẩu của thư mục sau đó chọn Next > bước theo bạn chọn ổ đĩa nơi sẽ chứa thư mục > bước cuối cùng bạn chọn Create desktop shortcut và chọn Finish để hoàn thành quá trình

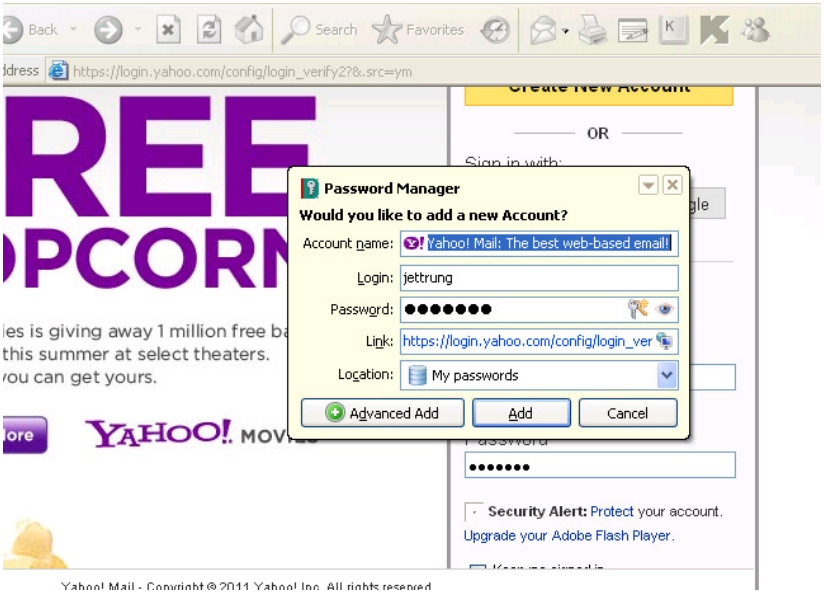
Lúc này trên màn hình desktop của bạn xuất hiện một ổ đĩa ảo mới được bảo mật bằng mật khẩu!

Khi muốn bảo mật thư mục > bạn click chuột phải vào ổ đĩa chọn Disconnect container > sau đó thử truy cập lại vào ổ đĩa ảo này > một mật khẩu sẽ yêu cầu bạn điền vào.

12. Quản lý password

Tính năng quản lý password mặc định không được bật, tính năng này cho phép bạn quản lý tất cả các mật khẩu của tất cả các trang web mà bạn truy cập. Để bật tính năng này bạn mở giao diện chính của chương trình chọn Tools > chọn Password Manager > chọn Start Password Manager > điền vào mật khẩu > chọn dòng I have read….sau đó chọn Next > bước tiếp theo bạn chọn Next

Khi bạn truy cập một trang web mà có yêu cầu điền mật khẩu: giao diện như hình bên dưới xuất hiện và bạn chọn Add để chương trình Kaspersky quản lý mật khẩu này! Sau này. khi bạn truy cập lại vào trang web này, bạn không cần điền vào mật khẩu lại, Kaspersky sẽ tự động đăng nhập giúp bạn, việc lưu mật khẩu hoàn toàn bảo mật và an toàn



13. Backup Restore data

Bạn có thể sử dụng tính năng backup and restore để backup dữ liệu quan trọng trên máy tính của nhân viên

Các sử dụng: Mở giao diện chính của chương trình > chọn Tools > chọn Backup and Restore > chọn Create > chọn các thư mục trên máy tính cần backup sau đó chọn Next > bước tiếp theo bạn chọn nơi chứa file backup, đặt password file backup cũng như số lượng file backup sẽ được lưu > bước tiếp theo bạn tạo lịch backup theo ý bạn > và hoàn thành thao tác

Khi bạn muốn Restore: bạn vào Tools > chọn Backup and Restore > chọn Restore > click chuột phải vào file backup cần phục hồi và chọn Restore để phục hồi dữ liệu đến thời điểm đó

V. Quản lý từ xa chương trình Kaspersky

KSOS cho phép người quản lý quản trị từ xa chương trình Kaspersky được cài đặt tại các máy tính của nhân viên.

Việc quản trị từ xa sẽ giúp bạn: cập nhật tập trung cơ sỡ dữ liệu virus, ra lệnh quét virus từ xa, backup dữ liệu từ xa, đặt chính sách truy cập web, sử dụng máy tính từ xa, mã hóa dữ liệu từ xa,..

Với doanh nghiệp nhỏ có thể bạn không có nhu cầu quản lý từ xa, nhưng đôi khi việc quản lý từ xa sẽ giúp bạn tránh một số vấn đề, nó sẽ trở nên tế nhị hơn thay vì bạn đến trực tiếp máy tính của nhân viên để cấu hình. Vd: khi bạn muốn backup dữ liệu trên máy tính nhân viên, muốn đặt policy truy cập các trang web được phép cho nhân viên,…

Bạn có thể tải tài liệu riêng hướng dẫn cấu hình quản lý từ xa chương trình Kaspersky tại địa chỉ: http://download.nts.vn/support/Tai_lieu_su_dung_Kaspersky/KSOS/

VI. KSOS cho doanh nghiệp một tháng triển khai bản quyền là như thế nào?

KSOS cho bạn thời gian một tháng để triển khai hết tất cả các máy tính trong công ty. Ví dụ bên dưới cho bạn thấy được thời gian một tháng để triển khai là như thế nào?

Bạn mua bản quyền gói KSOS 10 PC+1 File Server vào ngày 22/7/2011.

- Ngày 22/7/2011 bạn cài cho 7PC+1 File Server > các máy này hết hạn vào 22/7/2012 (đủ 12 tháng sử dụng).
- Ngày 22/8/2011 (sau đúng 1tháng kể từ ngày mua bản quyền) bạn cài tiếp cho 2PC > 2 máy này hết hạn vào 22/8/2012 (đủ 12 tháng sử dụng).
- Ngày 22/9/2011 (sau 2 tháng kể từ khi mua bản quyền) bạn cài tiếp cho 1 máy tính còn lại > thời gian hết hạn của máy này là 22/8/2012 (chỉ còn 11 tháng sử dụng).

⇒ Khách hàng phải triển khai KSOS trong vòng một tháng kể từ lần kích hoạt bản quyền đầu tiên để tất cả các máy đều đủ 12 tháng sử dụng.

VII. Các câu hỏi thường gặp

1. Sau này nếu có phiên bản mới thì tôi có thể nâng cấp lên miễn phí hay không?

Nếu có phiên bản mới, trong thời gian bản quyền còn hạn sử dụng, khách hàng được phép nâng cấp lên phiên bản mới. Bạn có thể kiểm tra thường xuyên xem có phiên bản mới không tại website: http://www.kaspersky.com/downloads_small_office_security

2. Có thể kích hoạt bản quyền được nhiều lần không? Khi nào mã bản quyền bị khóa?

Vd: Máy tính A bị lỗi hệ điều hành, bạn có thể cài đặt lại hệ điều hành và kích hoạt lại bản quyền cho máy tính A (thời gian sử dụng là thời gian còn lại của bản quyền). Miễn sao cùng một thời gian, số lượng máy tính sử dụng bản quyền không được vượt quá số lượng cho phép. Kaspersky không chịu trách nhiệm bảo hành nếu mã bản quyền bị khóa do sử dụng vượt quá số lượng máy tính cho phép.

3. Sau này công ty tôi trang bị thêm vài máy tính thì vấn đề mở rộng sẽ như thế nào?

Khi công ty mở rộng số lượng máy tính, bạn chọn mua tiếp sản phẩm KSOS phù hợp để cài đặt bảo vệ các máy tính mới.

VIII. Liên hệ hỗ trợ kỹ thuật

Kaspersky Lab hỗ trợ kỹ thuật từ 8h sáng đến 22h đêm hàng ngày (kể cả thứ 7 và chủ nhật).Thông tin liên hệ hỗ trợ kỹ thuật:

- Tel: 19001787
- Email:support@kaspersky.vn
- Chát với các nick hỗ trợ kỹ thuật tại website www.kaspersky.vn