

Kaspersky Administration Kit for Newbies

Copyright © 2006 ICE Systems, L.L.C. All rights reserved. 877-332-3250. www.useice.com

Introduction

The Kaspersky Administration Kit for Newbies is a document authored by the technical support team at ICE Systems, the largest re-sellers of Kaspersky Lab software solutions in North America. The scope of this document is limited to the installation and configuration of the Admin Kit using what we have determined to be the most ideal settings for the average business. This by no means covers all of the features and details of the Admin Kit. We strongly encourage you, (we'd force you if we could) to download all of the available product documentation that Kaspersky Labs has created and either read it prior to installation or at least browse through it so you have an idea what you can reference if additional help is needed. ICE Systems technical support is available for ICE Systems customers requiring assistance – but if the answer is in the doc...

What exactly is the KAV Admin Kit? The KAV Admin Kit is a centralized software management tool, which provides complete implementation and control of your enterprise anti-virus policy. In English, the KAV Admin Kit allows an individual (YOU) to install and control KAV software on all of the computers in your work environment. The KAV Admin Kit can manage KAV Business and Corporate Suite applications; these include KAV Workstation and KAV for File Servers, and most recently Kaspersky for Exchange. If you require AV protection for a Windows server you are required to install the Admin Kit as it acts as the native GUI for the KAV Server software.

Currently, the most recent version of the Admin Kit is 5.0.1149 – all screen shots and descriptions apply to this version.

Installation Requirements

Before you begin installing the KAV Admin Kit let's make sure your computer can handle it. The KAV Admin Kit will run on the following Windows operating systems:

- Windows 2000 SP 1, 2, 3, or 4
- Windows XP Pro SP 1 or 2
- Windows 2003 Server
- Windows NT4 SP 6.A

The hardware requirements are:

- Intel Pentium II processor, 400 Mhz or faster
- At least 64 MB free RAM
- 10 MB of free disk space

Copyright © 2006 ICE Systems, L.L.C. All rights reserved. 877-332-3250. www.ice-kav.com

Although it is not documented, the Admin Kit will also run on Windows 2000 Server, and will likely run on machines that do not have the 400 Mhz processor requirement. However, if you run into a serious problem with the Admin Kit and you are not running with a supported OS/hardware configuration you could be denied support until the requirements are met.

The above requirements are the MINIMUM requirements to install the KAV Admin Kit. If you have an assortment of Windows' versions in the group of computers in your work environment, choose the computer with the most recent version of Windows to install the KAV Admin Kit. If you have what it takes to install KAV, let's get going.

Installation

Before we begin the install process let's check to be sure we have the correct installation components downloaded. There are two installation components, one is required the other is optional in certain cases. The first component is KAV's version of the Microsoft Desktop Engine product, (MSDE). The MSDE component is required ONLY if you do not have a production copy of Microsoft SQL Server installed and running. A quick check of the C:\Program Files will tell you if you already have Microsoft SQL Server installed. If you DO have Microsoft SQL Server installed you can skip ahead to the section "Installing the Admin Kit". If you DO NOT have Microsoft SQL Server installed you need to install the KAV MSDE component. The MSDE installer program will be named something along the lines of msde2ksp3en.exe. DO NOT get slick and go out to the Microsoft download page and download the MSDE program from Microsoft. IT WILL NOT WORK with the KAV Admin Kit. You need the MSDE component delivered through Kaspersky Labs. The second installation component is the actual KAV Admin Kit installation program, usually named something intuitive like kasp5.0.1149_adminkiten.exe. If you are installing both components there is an installation order, MSDE first then the Admin Kit files second.

If you are installing the Admin Kit in order to administer computers running both KAV File Server and KAV Workstation, consider which computer will be easier to access and use for the KAV Admin Kit. If your Windows Server is in a closet and your computer will be using KAV Workstation, install the Admin Kit on your workstation.

Installing the MSDE Component

Here is the step-by-step guide to installing the MSDE component. It is strongly suggested that you follow these steps exactly. Deviating from these steps could cause you immense amounts of pain and suffering.

1. Double-click the msde2ksp3en.exe installer icon. The setup wizard will display a welcome message. Click 'Next' to continue.
2. Read the product license agreement. Click 'Yes' to continue.
3. Enter your name and your company name. Click 'Next' to continue.

4. The location where product files will reside is displayed. Click 'Next'.
5. SQL Server instance name, default is selected, click 'Next'.
6. Settings displayed. If they jibe with what you entered, click 'Next'.
7. Program files are installed. Progress window is displayed. If there are no errors you will see the final Wizard window indicating that the installation has completed successfully. You might also see a small popup informing you that the SQL Server is starting. The popup will disappear as soon as you hit 'Finish' in the final Wizard window.

The MSDE component just so you know, allows the KAV Admin Kit to create and use a database which we will soon see is named 'KAV', to store all of its important program information. When you eventually get to the point where you are creating groups and adding workstations to the groups, deploying software, and managing KAV program settings, all of these thingies are stored in the KAV database that the MSDE component facilitates. That was probably too much information. If it was, forget you ever read it. Let's get the rest of this product installed.

Installing the Admin Kit component

Okay, now all of the readers who already have Microsoft SQL Server installed and running can start paying attention again. We are now going to install the KAV Admin Kit program files. You will notice that some of the steps are marked "Domain Users Only". If you are not installing within a Windows Domain, but instead a Windows Workgroup certain Wizard screens will not be displayed.

1. Double click the installer icon (kasp5.0.1149_adminkiten.exe). The setup wizard will display a welcome message. Click 'Next'.
2. The next window displays the default location where the installation files will be extracted. This will not be the files' final resting place, just a temporary location. For now don't worry about it. Just take note of the folder and click 'Next'.
3. You will now see another progress bar tracking the extraction of the files to the C:\KAV folder. When finished another installer Wizard will begin.
4. The next installer Wizard opens and displays a welcome message. Click 'Next'.
5. The license agreement is displayed. Click 'Yes'.
6. Enter your customer and company info. Click 'Next'.
7. The destination location of the program files is displayed. Defaults are suggested. Click 'Next'.
8. The components of the Admin Kit are displayed with options on which to choose. In this case we want both components installed. Make sure both boxes are checked and click 'Next'.
9. Domain Users Only. The next window will ask you to choose a logon account for the Admin Server service. Choose the Domain User account. Click 'Next'.
10. Domain Users Only. Select a user account for the Admin Server service. Using the 'Browse' button select a user account that has administrator privileges on the domain, preferably the actual user "Administrator". DO NOT type in the user

- name. When you select it from the list of displayed user names you will notice that the domain name is pre-pended to the user name. Enter the password for the selected user. Click 'Next'.
11. The next window will show you the name of the default SQL server and the database name that will be created. If you installed the MSDE component earlier you should click 'Next' here after looking at the settings. You do not need to change the server name "(local)". Leave it alone. If you have MS SQL Server installed, this is the window where you can choose which instance/server to create the KAV database.
 12. The next window asks you to choose the Authentication Mode for the SQL Server instance. We suggest using Microsoft Windows Authentication Mode, there are no passwords to remember. Click 'Next'.
 13. This window shows you where the shared folder will be created that the Admin Kit requires. The shared folder is used to deploy software to clients as well as to facilitate remote av database definition updates. We will talk more about this later. For now let the KAV Admin Kit create the shared folder where it wants. Click 'Next'.
 14. The TCP/IP ports that the KAV Admin Kit uses to communicate with client computers are displayed. The default settings are ports 13000 (SSL) and 14000, (non SSL). Other programs rarely use these ports but if you are running Windows XP service pack 2, you might want to check and make sure the integrated firewall is not blocking these ports. If you don't understand what I mean by ports, TCP/IP and SSL, just click 'Next'.
 15. The next window displays options for the authentication certificate that the Admin Kit uses to authenticate connections to the Admin Server. If this is a fresh install of the Admin Kit accept the default settings. The next window will ask you to choose a folder where the certificate is backed up.
 16. Your choices are displayed for you to review. If you were a good installer you selected all program defaults and everything will be fine. Click 'Next'.
 17. The program files are installed, the progress bar is displayed. Once you get to the Finish window the product is installed.

Starting the Admin Kit

Open the Admin Kit by clicking your Windows 'Start' button and selecting the Admin Kit from the 'All Programs' menu. When the Admin Kit opens you will see a window displayed that looks like this:

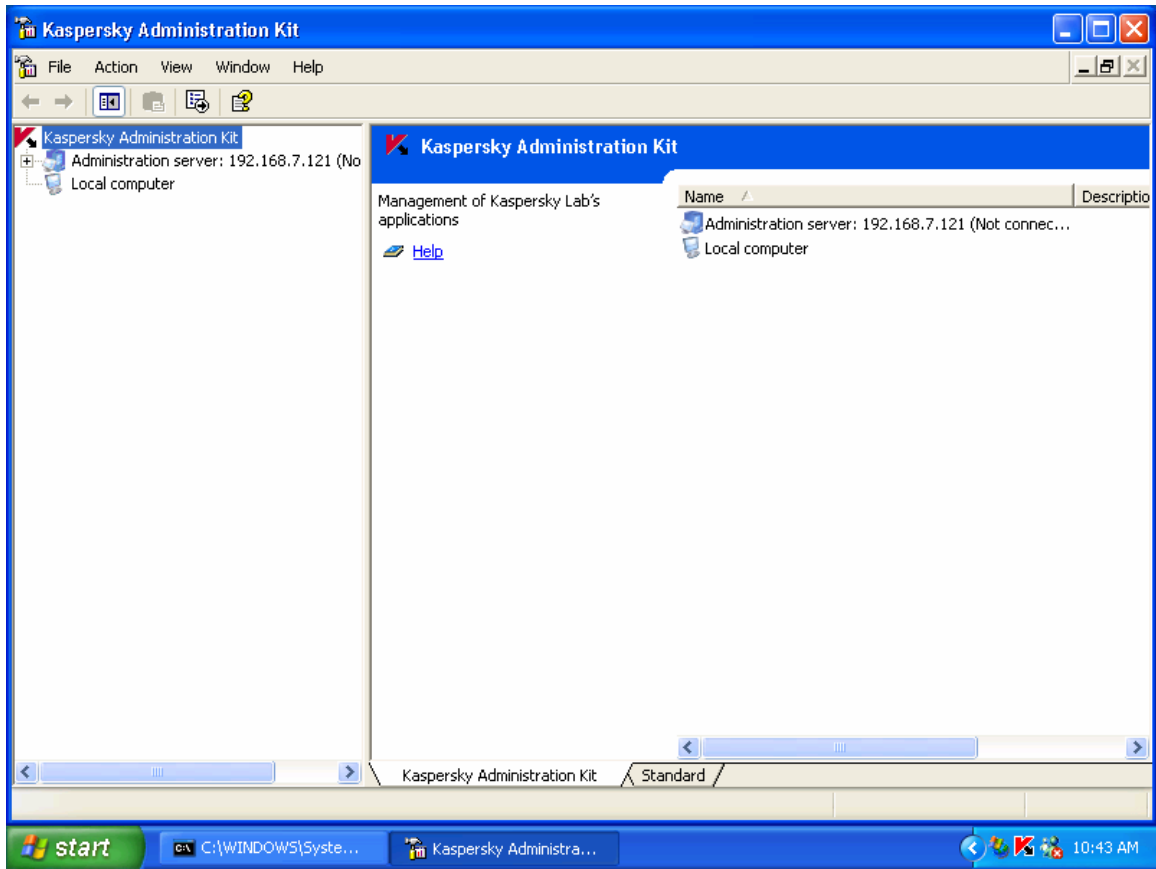


Figure 1 The Kaspersky Administration Kit (Admin Console).

Figure 1 shows us what the Admin Console looks like. Remember when we were installing the Admin Kit, in Step 8 we chose what components of the Kit we wanted to install. We chose both the Admin Console and the Admin Server. Before we go any further let's clarify the difference between these two components and get an idea of what they both do.

Admin Console – The Admin Console is the main program interface for the Admin Kit. The Admin Console will be used to create, configure and manage your group of computers that run KAV software.

Admin Server – The Admin Server is the “back end” or brains of the Admin Kit. When we add computers, configure their settings, and manage their activity the information regarding these tasks or actions are stored in the Admin Server. Actually this information is stored in a database that was created by the MSDE component that we installed first, or for users with MS SQL Server, in a database they chose. The Admin Server runs as a restartable service.

In Figure 1 above, we see an ip address listed that represents the host running the Admin Server and we see it is not connected. You might also see, instead of the ip address,

'localhost' listed to represent the machine running the Admin Server. The 'Not connected' message you will see means that the Admin Console has not yet connected to the Admin Server. In order for the Admin Console to do its thing it first needs to connect to the Admin Server, even though both the Admin Console and Admin Server are on the same computer in this exercise. If you double click the ip address or 'localhost' icon, or right click it and choose 'Logon Server', a connection to the Admin Server will be initiated and you will see:

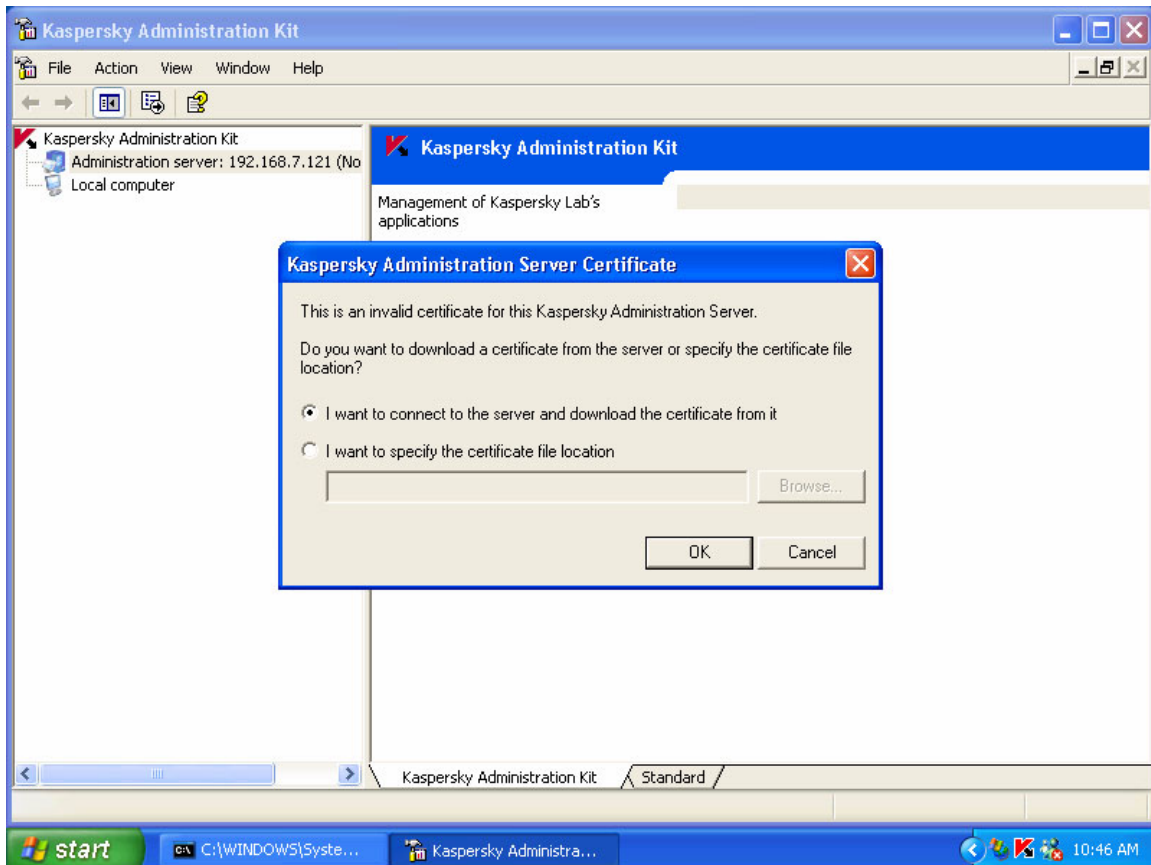


Figure 2 Server Certificate popup displayed upon first connection between Admin Console and Admin Server.

The message displayed in the popup is a bit misleading. Without going into too much detail here, the Admin Server and Admin Console are authenticating their connection. A certificate that the Admin Server holds is used to facilitate this authentication. Since we have both the Admin Server and Admin Console installed on the same machine we can chose the first option, which is already selected for us, and download the certificate. This process happens “behind the scenes” and requires no action on your part other than clicking the ‘Ok’ button. The only time that you will see the certificate popup window is during the first connection between the Admin Console and Admin Server.

After you have clicked ‘Ok’ and the certificate popup window goes away another popup window will appear, this one asking you if you want to run the Quick Start Wizard. Don’t

run this, we want to learn the Admin Kit by doing the actual tasks that the Wizard does for us. Click the 'Close' button.

Once the Quick Start Wizard popup closes you should see this displayed in the Admin Console:

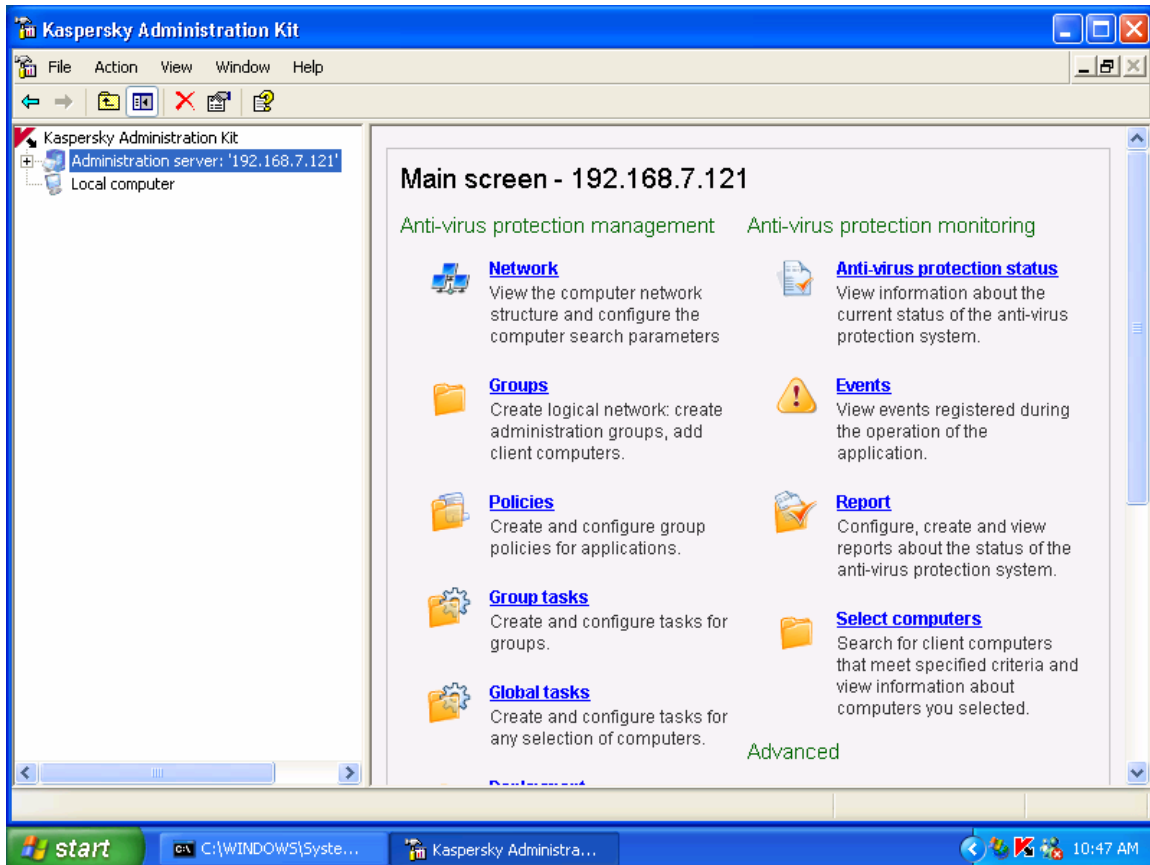


Figure 3 The Admin Console view after connecting to the Admin Server.

Configuring the Admin Kit

Creating the Logical Network

Now that we have the Admin Kit installed and open we are ready to begin the configuration process. The first thing we need to do is create a logical network that will contain all of the computers we need to manage. The logical network will consist of a group or groups that you create and the computers that you add to it/them. Before creating our group we need to find all the computers available in our network. The Admin Kit uses basic Windows networking to locate available hosts within your local network as well as any hosts on sub-networks that route traffic to the network supporting the host running the Admin Kit. Kaspersky software is not required on the hosts in order for the Admin Kit to detect them – again it uses Windows networking to locate machines.

In the event that you are not using Windows networking, for example you are a Novell user, the Admin Kit can accommodate you. The 'View IP subnets' options under the Network option in the Admin Kit provides Novell users with the ability to add computers by ip subnet range instead of by Domain or Workgroup. Refer to your product documentation for more details.

To access the list of computers that the Admin Kit/Windows can see, click on the 'Network' icon on the right hand side of the Admin Console's main screen. Here is what you'll see:

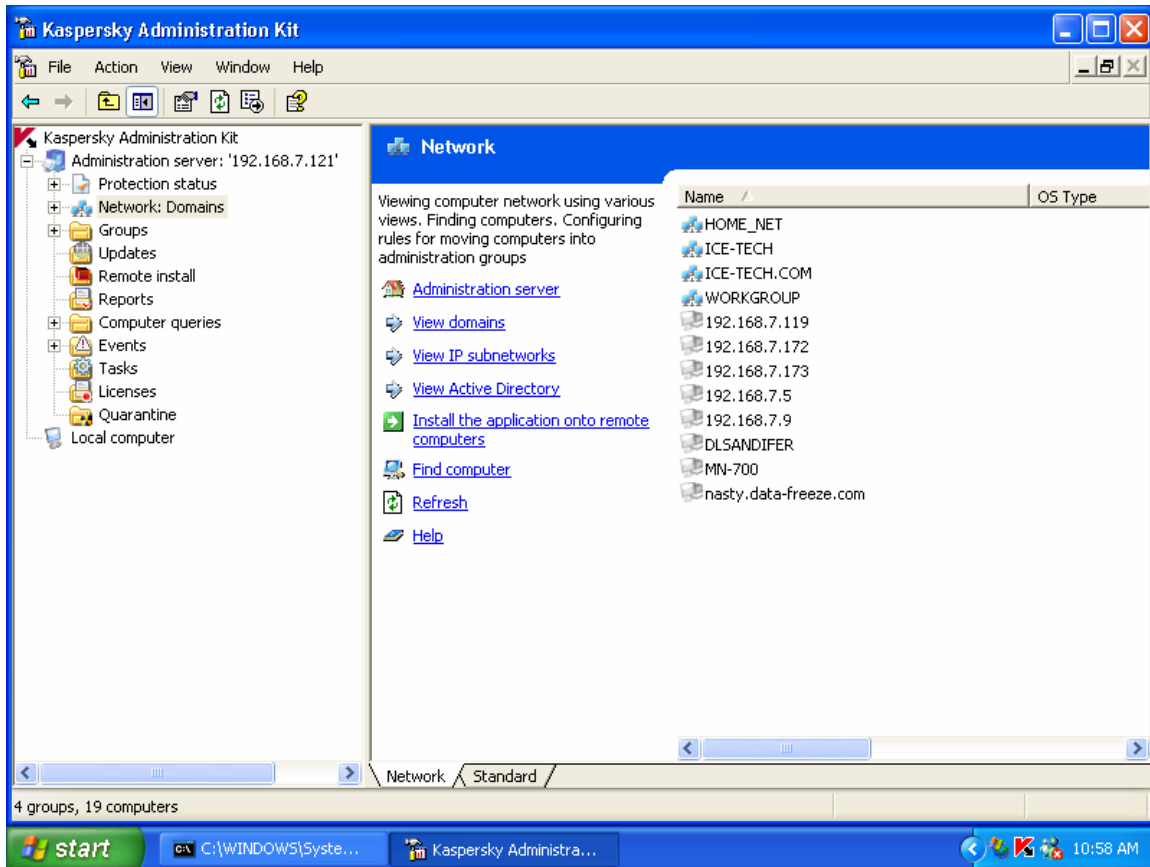


Figure 4 The visible network is displayed. The trio of monitors represents domains or Workgroups; individual computers are displayed by name if possible or ip address.

Our complete network is displayed in Figure 4 above. Again, for more details on the various other options you see reference your product doc. In this exercise we only need to identify the domain or workgroup that contains the workstations or servers we need to add to our logical network. In this exercise these computers will reside in the 'WORKGROUP' and 'ICE-TECH' domains.

The first thing we need to do is open the WORKGROUP domain icon and locate all of the workstations we will add to our group. After opening the WORKGROUP icon I see this:

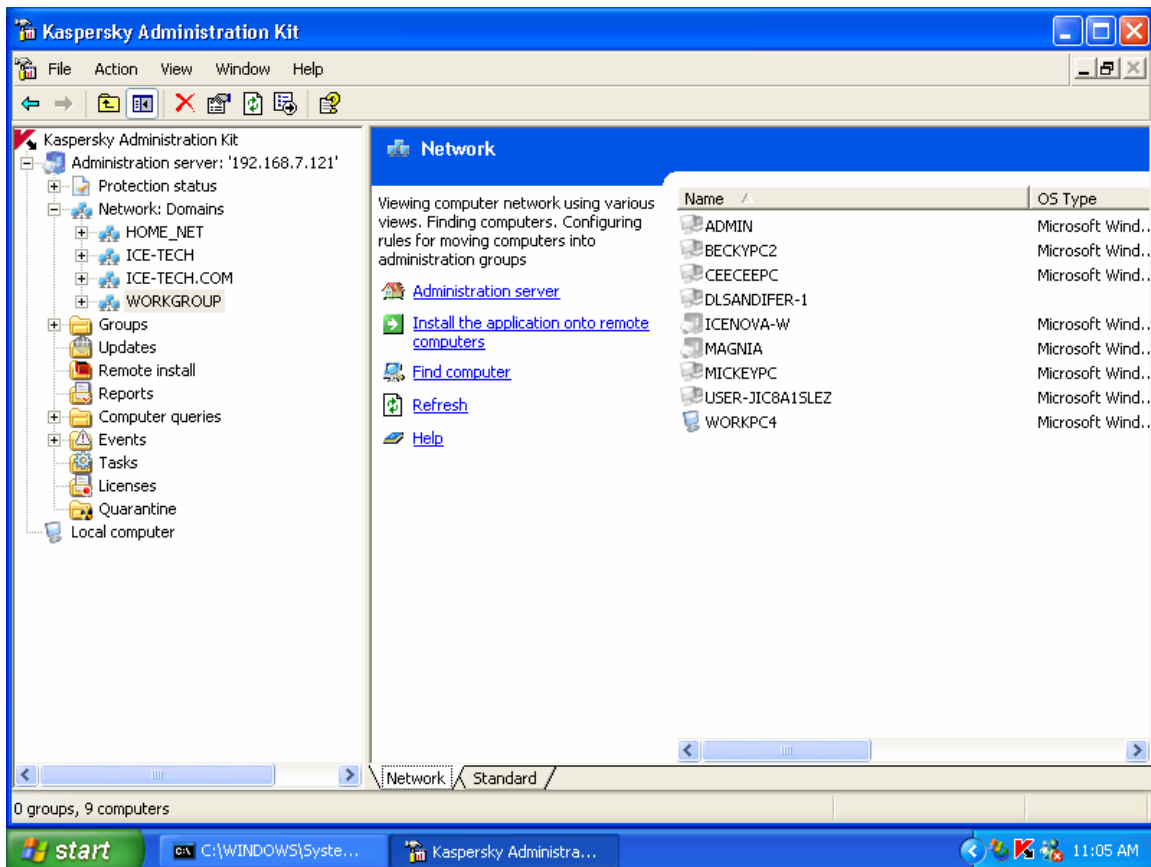


Figure 5 Shows the contents of the WORKGROUP domain.

Notice in the above screen shot that a solid blue monitor represents the WORKPC4 computer whereas the others are transparent. In this exercise WORKPC4 is the host running the Admin Kit – it is already visible via the Kaspersky Admin Kit’s communication module (more on this soon) so it shows up with the different shaded icon. The other hosts are visible via Windows Networking but do not have any Kaspersky software installed yet.

After locating the computers we want in the group we can now create the group. Right click on the ‘Groups’ folder located on the left side of the Admin Console, and choose ‘New-Group’, as shown in Figure 6 below:

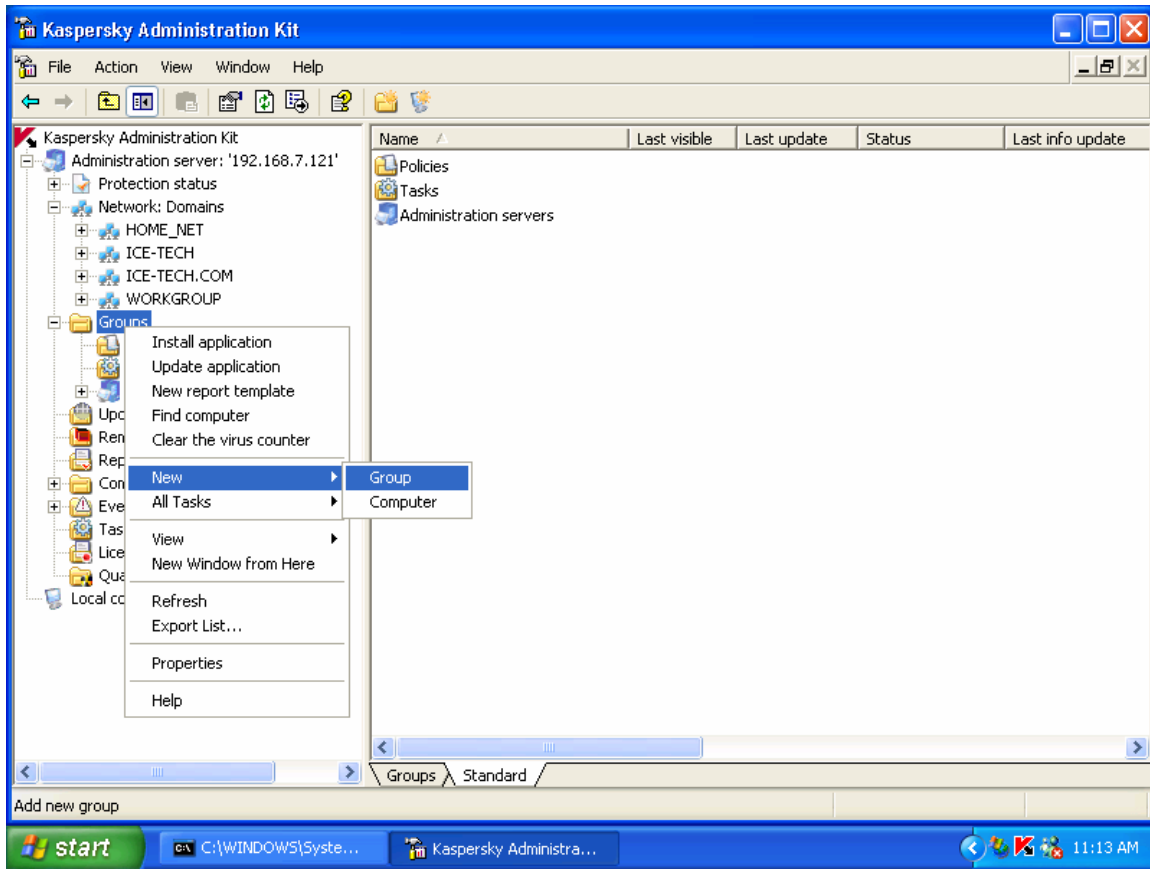


Figure 6

After clicking ‘New-Group’ you will be asked to name the group, choose an intuitive name. In this exercise we will name the group ‘TESTING’. After naming the new group your group will appear below the ‘Groups’ folder, it will be highlighted, and the contents of the group will be displayed on the right side of the screen. The contents of the newly created group will be a Policies folder, a Tasks folder, and an Administration Server icon. We will not detail these at this time but will cover the first two later. The Administration Server icon is used for hierarchical deployment of multiple Admin Kits and is beyond the scope of this article.

We have our group created, now let’s add our computers to the new group. Here are the steps to add the computers you will be managing to your new group.

1. Right click on the Group icon that you just created. Select ‘New’ -> ‘Computer’.
2. The familiar Wizard will open again, this time it will be an ‘Add Workstation Wizard’. Don’t be confused if you are adding servers to your group. The ‘Add Workstations’ wizard applied to servers as well. Click ‘Next’.
3. The next screen in the Wizard will give you the option to choose how to add the workstations to the group. The first option, “I want to add computers to a group using Windows networking” is THE best option. It will be selected by default. Click ‘Next’.

4. You will now see the 'Network' folder with a '+' mark next to it. Click the '+' mark, opening the folder. As I mentioned earlier, you will now see the list of Windows domains or workgroups that the Admin Kit can recognize. If you open the workgroup or domain icon the list of computers that you can add to your group are displayed. If all of the computers you need to manage are all in the same group under the 'Network' folder, simply click the box next to the workgroup or domain name and all of the computers will be added to the group you created. After selecting which computers to add, click 'Next' followed by 'Finish'.

If at a later date more computers need to be added to your group you can simply repeat the above steps and add any new computer as it appears in the 'Network' folder.

Now you have created a logical network; you created a group and added all of the computers you need to manage to your group. You should now see all of the computers that you added to the group displayed on the right hand side of the Admin Console. You will notice they are all a light shade of pink, depending on the resolution of your monitor, except for the computer with the Admin Kit installed. The dark red icon that represents the host running the Admin Kit indicates that we can connect to this host via Kaspersky's communication module (covered soon) but there are issues with the host – namely the fact that no AV software is installed. The light pink icons representing the other hosts we added to the group have no AV software installed nor do they have a Kaspersky communication module installed. This will soon change...

Uploading and Deploying Software

Now that we have the Admin Kit installed and created a logical network we can begin creating tasks to install KAV software on all of the computers. Before we begin we need to be sure that we have proper relationships established between the computer running the Admin Kit and all of the computers in the logical network. When you run tasks to install software on all of the computers in the logical network you will be doing it as a user who installed the Admin Kit. Can that user logon to all of the computers in the logical network using the same username and password? If you installed the Admin Kit within a Windows Domain as the domain admin you do not need to worry. If you are installing within a Windows Workgroup however this might be a concern. You can test this out by clicking on the Windows 'Start' button, choosing 'Run' and typing '\\computername'. Windows Workgroup users need to have trusted relationships established between the Admin Kit machine and all of the clients in order to mass-deploy the AV software, otherwise each machine will need to be deployed one at a time, with the user name and password of that machine's admin account included in the task setup details, (more on this later – just understand that if you are not running within a Windows Domain it is strongly encouraged that you have an account created on all workstations with a common password for an admin account).

If your Admin Kit is installed on a computer running Windows XP Pro (you should not install the Admin Kit on XP Home, nor have computers in your logical network running

XP Home) you should disable 'Simple File Sharing'. This suggestion is not mentioned in the official Admin Kit doc, but to avoid possible problems it is suggested. To do this right click on ANY folder and choose 'Explore'. After the Explorer window opens, from the main menu choose 'Tool' – 'Folder Options'. A 'Folders Options' popup will appear. Click the 'View' tab, scroll all the way down the list of items, and UNCHECK the box marked 'Use simple file sharing'. See figure 5 below:

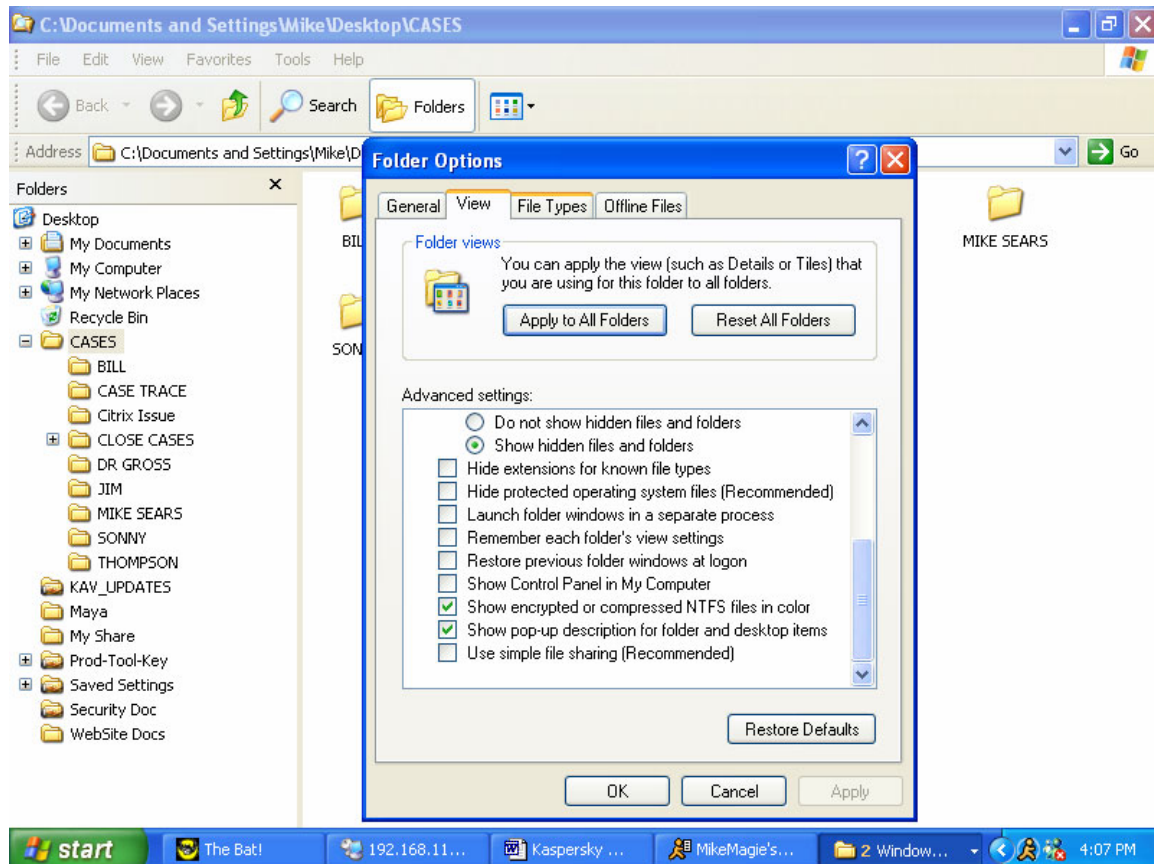


Figure 5 Simple file sharing must be disabled in order to deploy software packages when the Admin Kit is installed on Windows XP Pro.

The host running the Admin Kit requires anti-virus protection so we will locally install the appropriate software here first, without using the Admin Kit. We do this for one main reason; when the software is installed it creates subfolders under C:\KAV, one of which will contain a file named 'workstation.kpd' or 'fileserver.kpd' depending on the software being installed. The .kpd file is the deployment file that the Admin Kit uses to upload and deploy the software to the other clients in your logical network. If the Admin Kit is installed on a Windows Server that will be protected by KAV for File Server and you also have computers that need to run KAV Workstation software do not fret, we can get the requisite .kpd file for the workstations by doing a partial install of KAV Workstation on the File Server. We will cover this in a minute. Also, if the Admin Kit is installed on a Windows Workstation but you also have a Windows File Server that requires av

protection via KAV for File Server we can do a partial install of the File Server software on the workstation to get the needed .kpd file as well.

Let's assume for simplicity that your KAV Admin Kit is installed on a Windows Workstation and you have 5 other workstations and 3 File Servers that need KAV software. You should first install the KAV Workstation software locally, i.e. on the computer where the KAV Admin Kit is installed. During the local installation if you are prompted to overwrite files that already exist choose 'Yes to All', doing this will insure that the latest copies of all required files are in place. After you have locally installed the KAV Workstation software you can upload the installation files to the Admin Kit, create a task to deploy it to our other workstations, and then run the task to install the software.

To upload the KAV Workstation deployment file to the Admin Kit:

1. Right click on the 'Remote Install icon' on the left hand side of the Admin Console and choose 'New' – 'Installation package'. The 'New Package Wizard' will appear. Click 'Next'.
2. Provide an intuitive name for the new task, i.e. "Deploy KAV Workstation". Click 'Next'.
3. The next window allows you to browse for the .kpd file mentioned earlier. The default selection 'Make Kaspersky Labs application package' is appropriate. Click the 'Browse' button and navigate to C:\kav\winworkstation\english\. Double click on the winworkstation.kpd file. You will see the version details of the package you selected displayed.
4. The license key window will now appear. Using the 'Browse' button navigate to the location of your KAV Workstation license key. When found, double click the key file. Notice the license key details are displayed. Make sure this is the correct key.
5. You will be notified that you are about to add a new package, click 'Next'. The KAV Workstation package will now be uploaded to the Admin Kit.

If you now double click the 'Remote Install' icon on the left side of the Admin Console you will see the new deployment package we just created, "Deploy KAV Workstation", or whatever you named it, displayed on the right hand side of the Admin Console under the Network Agent package. We can now create a task to deploy the Workstation package. To do this:

1. Right click on the "Deploy KAV Workstation" entry and choose 'Install'.
2. The "Remote Installation Wizard" will appear. Click 'Next'.
3. The name of the task will appear; it will be the same name that you provided when you created the deployment package above, in Step 2.
4. Select the install method. We always like the 'push' method.
5. The next window displays download settings that the task will use. We want all of these defaults. If any of the machines being deployed to already have an older version of Kaspersky 5.0 installed you can uncheck the first box "Do not install on hosts which the product is already installed" – this way the older version will

- be overwritten by the newer one. If no Kaspersky AV is installed leave the options here alone.
6. Select the Network Agent package to include with this deployment. Make sure that the version of the Network Agent is the same as the Admin Kit's version. The Network Agent is the communication module that allows a client workstation to communicate with the Admin Kit. The Network Agent communicates with the server via UDP port 15000 – this port needs to be allowed access if the client is running Windows XP SP2 and the integrated Windows firewall is enabled.
 7. Select the computers to run the task on – using Windows Networking.
 8. Select the computers by opening the folder for your group and clicking the box next to each computer that needs the software. Exclude the local computer if you already installed the KAV Workstation software as instructed earlier.
 9. Specify the account name under which to run the task. If a Domain install, the default account is fine. If a Windows Workgroup install choose the username/password that has Admin rights on all computers that the task will run on.
 10. Schedule the task for 'Manually'; we want to run it as soon as it is created.
 11. Click 'Next' and 'Finish' to wrap it up.

You will now see the newly created task show up under the global task folder which sits in the main list of Admin Kit icons on the left, between Events and Licenses. Open this Tasks folder and double click on the newly created task. When the popup appears, click the 'Start' button. You can monitor the progress of the task via the 'History' button. Remember to click 'Refresh' if you want to see a running description of the task's progress.

Updating, Policies, and Tuning

The Updater is the KAV process that downloads anti-virus definitions from Kaspersky download servers and applies these definitions to the computers in your logical network. There are a few options for how you can configure these updates. We will cover the method preferred by ICE Systems and the great majority of our customer.

After the deployment of the workstation or file server software to the clients in the logical network the newly protected computers will individually receive updates automatically from the Kaspersky Lab servers via the Internet every 3 hours. We want to configure the Admin Kit to download these updates and let the computers in your logical network retrieve them from the Admin Kit. We also want to implement some general performance tuning settings and tighten up the general administration of our workstations and servers.

In order to facilitate this we need to create a policy. A KAV Admin Kit policy consists of a set of rules that apply to all of the groups or computers in the logical network. If you have two groups for example, one named 'File Servers' and the other 'Workstations', you would create a policy under each of these groups that applied only to the computers in the respective group. You could also create a global group policy that would apply to both the 'File Servers' and 'Workstations' groups. The policy settings are applied from the

BOTTOM up, meaning if we create a policy in our 'Workstations' group to get updates from the Admin Server for example, but a global group policy states that the updates are handled by the computers individually, the local group policy would take precedence and the updates would be obtained from the Admin Server. You will notice that under the folder named Groups there are two icons, tasks and policies. You will also notice that these two icons exist inside the group you created. Get it?

I suggest creating individual group policies if you have more than one group to avoid confusion and frustration. That said, let's create a policy for our group of workstations that will allow the computers in that group to get their database updates from the Admin Server among other things. We will tackle the updates first. Before we create the policy we need to first create a task for the Admin Kit to download the av updates from the Kaspersky Lab servers on the Internet.

1. Create a global task to download the updates to the Admin Server. To do this right click on the global 'Tasks' icon and select 'New'- 'Task'. This 'Task' icon is displayed on the left side of the Admin Console. It appears between the 'Licenses' and the 'Events' icons. You cannot create the task to download updates to the Admin Server from the 'Tasks' icon under the 'Groups' icon or under the icon for your 'Workstations' group.
2. The new task Wizard will appear. Click 'Next'.
3. Name your task 'Download Updates' or something else intuitive.
4. You will be given a choice as to which application the task applies and which task you want to create. Choose 'Kaspersky Administration Kit' and 'Download updates task'. Click 'Next'.
5. Choose the update's source. Select 'Kaspersky Update Service'.
6. Choose the account to run the task. Same as before; if you are running within a Windows domain, Default is fine. If you are not domain controlled, enter the account and password that has access to all of the computers in your logical network.
7. Schedule the task to run every 3 hours. This is the suggested setting straight from Kaspersky. Click 'Next', then 'Next' again to finish.

Okay now we have the task created that will allow the Admin Server to download the database updates our computers in our logical network will need to stay protected. Where do these updates get saved? If you guessed in the shared folder that was created when the Admin Kit was installed (named Share), you are correct. Now that we have the Download Updates task created and scheduled let's create the policy that tells all of the computers in our 'Workstations' group to get their updates from the Admin Server's shared folder as well as our performance tuning settings. Here are the steps:

1. Double click your group's group icon/folder. You should see all of the computers in the group displayed nicely on the right side of the Admin Console. Above the first computer listed you will also see a 'Tasks' and a 'Policies' icon. Right click on the 'Policies' icon and choose 'New' - 'Policy'.
2. The new policy Wizard will appear. Click 'Next'.

3. Name your policy.
4. Choose the application that the policy applies to; in this case it is 'Kaspersky Anti-Virus 5 for Windows Workstations'.
5. Click 'Next' when prompted, "You are about to add a new policy".
6. You will be asked to define the default protection level for all computers in the 'Workstations' group. We suggest setting this to 'High Speed'. Notice the small lock icon. Closing this will prevent your end users from modifying the settings you make relative to each Policy setting. It is up to you whether or not to lock your policy settings but we recommend it.
7. The next window allows you to configure the On-Demand scan task that runs by default every Friday evening at 8:00 pm. Again we suggest 'High Speed' for the protection level. In the main window here you can also configure how you want the scan to behave if infections are detected. By clicking the 'Advanced' tab you can exclude files from the scan if necessary or modify further the scan settings. We suggest simply changing the protection level setting to High Speed.
8. The next window will let you determine the Updater settings. The default is what we want, 'Kaspersky Administration Server'. The second update source (Kaspersky Lab servers) is listed as a backup in the event that the Admin Server were down. You can optionally remove this, though it is not suggested. Click 'Next'.
9. More Updater settings. The defaults are pretty good. I would suggest only one change. Change the setting 'Urgent updates' to 'All available updates'. Click 'Next'. Click 'Finish' and you have your policy created.

Now that we have the policy created let's open it up and take a look at it. It should be displayed on the right side of the Admin Console. If it is not, double click your group icon, and then double click the 'Policies' icon under the group. Here is what you should see:

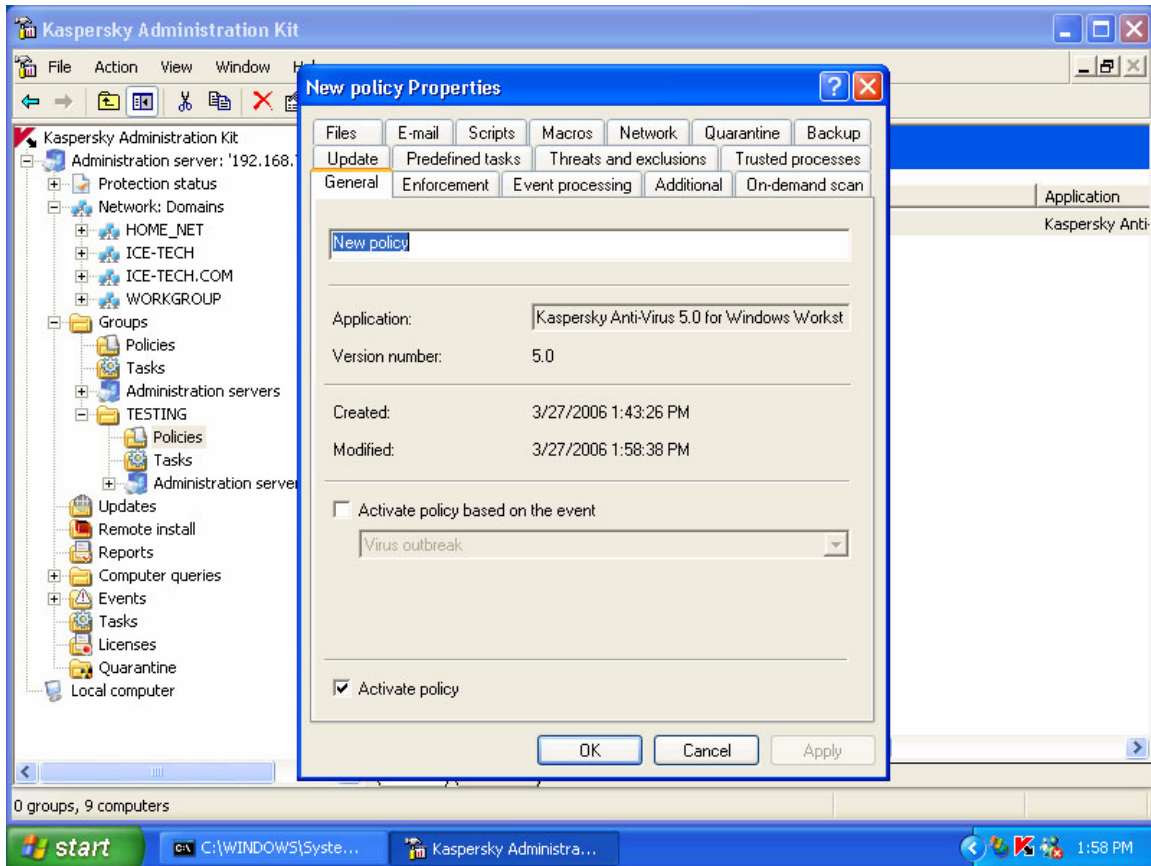


Figure 7 Shows the policy options.

Any computer that is already a member of the group for which the policy is defined will inherit the policy settings immediately if possible or as soon as any pre-existing running task completes. You can also force the settings to be applied by clicking the 'Enforcement' tab seen above, then the Modify Now button that is available under the 'Enforcement' tab. Any newly added computer will inherit the policy settings upon the first network refresh (these occur every 15 minutes) unless the policy is forcibly applied as just described via the Enforcement tab.

If you want modify the schedule of the update task (not the global task that downloads updates from the Internet to the Admin Server, but the local workstations update task) you will need to create a new update task and then disable the predefined update task. This also applies to a need to change the default on-demand scan schedule (every Friday at 8:00 pm). To disable these predefined tasks access the 'Predefined Tasks' tab inside your policy properties and uncheck the Update and On-demand scan tasks. Now the workstations will not get updates every 3 hours from Admin Server and the full scan scheduled for Friday night at 8:00 pm will not run. You will now need to create individual tasks to perform these operations. Use the same steps we used in this article to create these tasks. Remember, the location of the task will determine which machines it effects. A task created in a subgroup to scan computers at 6:00 a.m. Tuesday will not affect computers in a separate group.

More on the Network Agent

As mentioned earlier the Network Agent is the module that facilitates client-server communication between the Admin Server and the Windows clients. Every machine except the local host running the Admin Kit requires this component. In earlier versions of the Admin Kit the Network Agent was deployed as a separate package from the AV software but with the newer versions came the ability to include the Network Agent package with the AV software package. The Network Agent can still be deployed by itself; its installation package already exists inside the 'Remote Install' folder in your Admin Kit. Anytime the Admin Kit is reinstalled the Network Agent included with the new installation MUST be redeployed to all clients regardless of whether the Network Agent package had been previously installed.

For clients running Windows 98 or Windows ME, as well as those clients with Microsoft File and Print Sharing services disabled (such as Novell users) the Network Agent package will need to be installed either locally or via a login script. You are pretty much in your own when it comes to these configurations, but we can offer some help.

First off, you can do a simple single computer installation of the Network Agent on a local client fairly easily. The first thing you need to do is get all of the files from the (default location) C:\Program Files\Kaspersky Lab\Kaspersky Admin Kit\Share\Packages\Network Agent 1.0 folder. Move all of these files to the pc where the local install is required, double-click on setup.exe and away you go. Using this method to install will require intervention by the installee. There is only one parameter that needs to be modified during the local installation and that is Server setting in the main install screen. Make sure this is changed to the IP ADDRESS of the host where the Admin Kit is installed – by default it will be set to the name of the local host where we are installing the Network Agent. This is the ONLY change required during a verbose install of the Agent.

If you can run the setup.exe with the /s (silent install option) then the settings for the Network Agent will be detected, the correct host setting will be applied and the agent will install in silent mode with no user intervention. Again, the configuration of how the setup.exe /s gets exec'd is up to you but the process is fairly simple to understand.

Final Notes

I encourage you to examine the various options the Admin Kit offers. Click icons, right click, left click, and double click. Find out everything you can. Be a pioneer and explore the product your self. Just don't break anything ;-). Before you call us or email us with your Admin Kit question or problem check our FAQ to see if the question has already been answered. Our FAQ is located at:

<http://www.ice-kav.com/faqs.php>

Check www.ice-kav.com/applications.php regularly for product update information. The password is 'myaccess'. For more questions or if you encounter a problem, call our support line at 1-877-332-3250, select option 3. This support line is intended for ICE Systems customers only.