Global Information Assurance Certification Paper

Overview about how to protect your Enterprise against viruses with Symantec *AntiVirus Corporate Edition 8.0 in combination with the SAV Reporter*

written by Mike Leonardo
April 13, 2003

Abstract:

There are lots of discussions going on about how to protect your Enterprise against viruses and how to control all machines as much as possible, even when they are only partly or never connected (e.g. field representatives). The first thing I will explain is that it doesn't really matter what kind of software you use. If it is an Enterprise AntiVirus solution, it should cover most of the features mentioned on the following pages. Maybe you have to go for another sequence on realizing your plan. It is just a fact, that I know the Symantec product a little bit better than the rest. So this will be a description on how to use the latest Symantec AntiVirus solution to fulfil your company needs.
Of course you could spend ages on reading all the manuals and finally follow the steps written down in those papers to get something done. As already mentioned this document will guide you through this subject in about 15 to 20 pages and close to everything should be covered. In addition to the fact that the machines will be protected with the latest virus definitions at the moment the rollout of the software is done, you will learn more about methods to force the target systems to update frequently, which is a bit more tricky to realize on some systems. Last but not least, the document will inform you about the reporting options you have within the software and how an additional tool, the "SAV-Reporter", can monitor the AntiVirus business. This document is not designed for a certain size of company; it is nearly for all of the system administrators, who would like to make their life easier and not being afraid of any new virus attack that will be there in the future. You can implement protection without having all machines connected(unmanaged) and also with thousands of machines on separate networks. You will learn that there is a way to implement a "*Digital Immune System*" as well as there is an "Alert Management System(AMS)", which is very helpful. The way of getting the software onto a specific system can also be chosen, as well as the method of updating the virus scanner.
At the end of this document I will give you an impression of what kind of reports you can generate with the "*SAV Reporter*" and why it is better to use the "*SAV Reporter*" instead of using "only" the reporting functions of the Symantec System Center.

To answer an important question at the beginning: "Yes, the concepts described in the next pages will be for Windows platforms only. You can protect Novell Netware Servers and Macintosh machines as well, but I am sorry to tell you: There is no way of protecting a Unix or a Linux system with the Symantec AntiVirus Corporate Edition(SAV CE) 8.0. If you see it from another point of view: There are less risks of being infected with a virus on these operating systems, otherwise AntiVirus software companies would spend more time and money on developing virus protection solutions for such target systems.

For licensing and, as a result of this, also for the costs I can only say that for this specific product you will have to purchase one license per machine, where the software is loaded. It might be different on other products, but this is not an issue of this document. Here we are only talking about the technical facts.

Situation:

You are the system administrator of a network with Windows NT 4.0- and Windows 2000- servers and lots of desktop machines with a Windows operating system loaded are attached. The majority are Windows 2000 Professional and Windows NT4, a few Windows98 and Windows ME. There are some employees, who are working on Windows98 at their home offices. Their only way of communicating with the company is via email (Lotus Notes email clients). Your team is in charge of the support of **all** machines (In total round about 25 servers and an estimate of 500 workstations). *The email server itself is handled by another team, but you should co-ordinate your work with them, it is their job to look after the Virus protection of the mail server*.
The latest news about the damage viruses can do to enterprise networks made the corporate management have a look at this subject and in the near future they would like you to be able to monitor the network and implement an Enterprise AntiVirus solution, that is easy manageable from any location/machine on the network. They would also like to have reporting functionalities, so that even people with less IT-knowledge will understand what is going on. It is on you now to achieve the targets without additional budgets for manpower. Your team of administrators has to solve the issue without help or support from other parties.

How to start, what strategy should I go for?:

Here are some mandatory things you will have to find out and this is a list of what you have to consider:

1. *SERVER*
    a) How many servers are there to protect?
    b) What functions do these servers have(DB, Mail, PDC, BDC, Web,…)?
    c) Do you have special programs running on these servers?
    d) Do the servers fulfil the system-requirements for the AntiVirus Software?
    e) Do all server operating systems have to become a SAV CE Server or is it enough if the SAV CE client software will run.
    f) Would it make sense to load balance in a certain way, because of the functions the servers have?
    g) How are the servers connected to the Internet? Where is it necessary to have a direct connection to the Internet?
    h) Which server will be the Quarantine Server, which the Alert Management Server?

I won't open a discussion on if it is necessary to have those functions, because we are talking about a maximum protection with one AntiVirus enterprise solution. This is all part of it!

2. *WORKSTATIONS*

a) How many workstations are there to protect (connected or not connected to enterprise network)?
b) Where are these workstations (physical location)?
c) What kind of operating systems are loaded? Would it make sense to upgrade the operating system before loading the AntiVirus software to it?
d) Are applications loaded on the workstations you might have to pay attention to?
e) What is the network-speed between the machines on the corporate network (1GBit or modem)?
f) How to load the software to the clients (CD, through the network, Web,…)?
g) Which role will this machine play in the AntiVirus environment (SAV CE server or SAV CE client)?
h) What has to be loaded to the clients? Is really everything needed (documentation, Live Update,…)?

3. MAINTENANCE and REPORTING

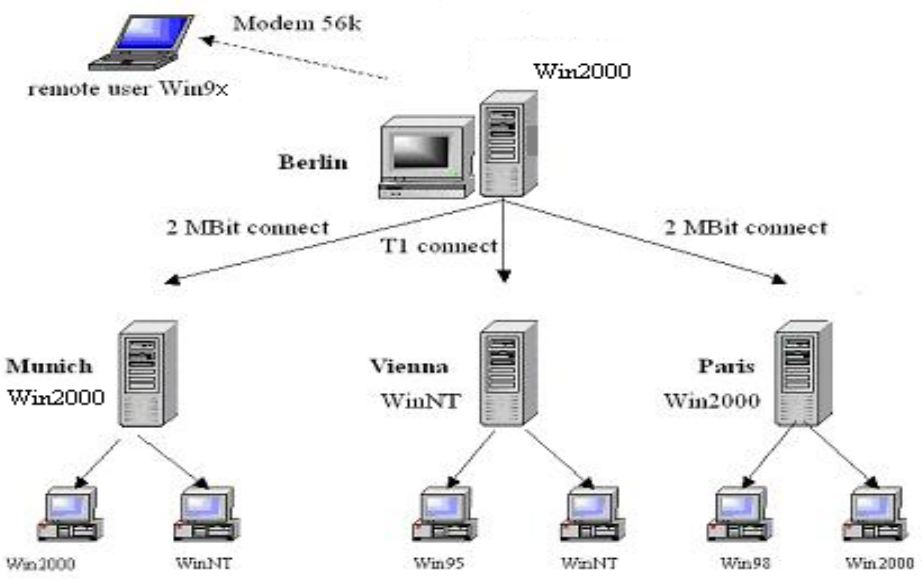
a) How much manpower is needed to handle the entire AntiVirus business?
b) How to implement upgrades and updates?
c) How much effort does it take to change configurations on clients/servers?
d) How can reports on the AntiVirus business be generated?

4. *EXPLAINATIONS and LINKS*

a) Abbreviations and shortcuts
b) Is there a way I can get support and if so, what do I have to do to get it?
c) Where do I find actual information about the product?

Imagine this (pic1) is how your network looks like. Of course there are more servers and lots of workstations connected to those in each location. The standard LAN speed is 100Mbit at each bigger location (Berlin, Munich, Vienna and Paris). You are at Berlin and each LAN has its own IT administrator. How the single domain is structured can be disregarded. On Windows NT and Windows 2000 based machines the domain administrators have local administrator privileges. The entire Internet traffic is going through a Gateway, which is loaded with a Virus Scanner for Http and Ftp (Companies that provide such Virus scanners are Symantec, Trend, Computer Associates,..)
Field representatives are only allowed to get onto the network via VPN (Virtual Private Network) connections and a few temporary contractors (in most cases students) mail from time to time some documents, which they have written or translated at their Windows 98 desktop machines at home.
Your task is to come up with a “AntiVirus-Software rollout-concept” for the corporate network. A plan on how you can track the software on the corporate network is required. It doesn’t matter if the machines are permanently connected or only a few minutes per day.

pic1



To start correctly of course you need to have the software. This is already the first point that you have to pay attention to. Your decision has been made for one product, you have already one version of the software. Make sure that this is also the latest build of this product. In most cases you'll find the information on the homepage of the vendor. E.g. for Symantec it is: http://service1.symantec.com/SUPPORT/ent-security.nsf/docid_p/2002091810595048.
Once you have ordered the latest build from support they should either send it to you via mail or give you an internet address where you can download it from.

Now that you have the "right" CD, you can **really start**. Install the Symantec AntiVirus solution to one dedicated server (e.g. Windows 2000 Advanced server). The exact hardware requirements are written down in the Installation Guide: ftp://ftp.symantec.com/public/english_us_canada/products/symantec_antivirus/symantec_antivirus_corp/8.0/manuals/savce80i.pdf , Chapter 4). The reason why you should choose a more or less powerful machine is that this will become our "primary server" or "master primary server". This is going to be one of the more important servers if not the **most important** server in our strategy. From now on we will go step by step through the installation:
Insert the CD and start the "setup.exe"(if it doesn't start automatically)→"Install Symantec AntiVirus"→"Deploy AntiVirus Server", select "install Symantec AntiVirus Server", select "I agree" and on the next screen you keep both options(Server program and Alert Management System (AMS²)) checked. In the left part of the next window you'll see the available computers. Choose the machine you would like to have the software installed to. On the right part of the window you can select an SAV CE-Server when you get to the installation of other SAV CE servers, but for the moment the right part of the window should be empty. Click the "Add"-button in the middle of the window. The machine from the left side pops up on the right side of the window as well. The program will show you where it is going to install the software to and finally it will ask you for a name of the Server Group. Choose a name which displays also describes the location of the machines that will be part of this group.

With the new version SAV CE 8.0 you **have to provide a password** for this specific Server Group.
Note: Choose a secure password, because everybody, who is able to open the SAVCE-Server console is also able to manipulate your AntiVirus policy.

A message will come up during the installation, telling you that the Anti Virus definitions are older 30 days. Of course you will change this fact as soon the software load is completed. A decision has to be made if the Symantec AntiVirus services should start *automatically* or *manually*. I suggest that you keep the default "*automatically*", because this will ensure that the scanner is started and running after any reboot. The only reason why you should have the Symantec AntiVirus-services put on "*manua*l" is that you come across with problems in connection with the SAVCE-scanner (e.g. an application interferes with the Virus scanner or the scanner is not able to scan certain files, because they are in use by a backup program). To track this you could stop the "realtime protection" and find out what's wrong. By starting each application in an certain order it is possible to realize the origin of the problem. The final step is to finish the installation after the progress bar is on 100% and the button "close" is available. The machine(server) will have to reboot and after the reboot your Windows 2000 server is protected.
Note: In general the AV Server doesn't have to be restarted, but because we have installed the "AMS-Server" as well, the machine needs a reboot. The first thing you should do is downloading the latest definitions from the Symantec Web-Site. The easiest method is via Live Update. The use of the Intelligent Updater is also possible. With this opportunity it is possible to implement the newest AntiVirus definitions without having your company connected to the Internet.
When all this is done you install the Symantec System Center Console(SSC). The console can be installed on any NT-based(Windows NT 4, Windows 2000 or Windows XP) machine. So it is possible to have several consoles installed for a various number of administrators (e.g.: each bigger location one console). Once the console with its plug-ins is installed you first have to declare your SAV CE Server to be a Primary Server. Without having done this you won't be able to configure anything. You can start now installing the Symantec AntiVirus Clients. The best way is to do this via the SSC, but there are several other ways to get the AV-software loaded onto corporate machines.
http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2002073014500548

- You can select the "NT Client Installation" from *tools* menu in the SSC. A window will come up and you have to choose a machine where you would like to have the SAV-Client installed to. The next step is to make decision for a Parent Server. When the installation is finished you will find the client under the server in the Symantec System Center Console.
- You can use the "NT Remote"-tool. It is on the SAV CE 8.0-CD in the following directory: \Rollout\NTClient\NTRemote.exe.
  Note: This tool is launched when you select the NT Client installation from the SSC.

- You can start the SAV CE Client installation from the CD. Start the "setup.exe" on the root of the CD, choose "Install Symantec AntiVirus" and then "Install AntiVirus Client". Compared to the first two installations you will be asked for what kind of AntiVirus-client you would like to install, an "*unmanaged*" or a "*managed*" one with the name of its Parent Server.
  Note: You won't be able to see any "unmanaged clients" in the console.
- The Symantec Packager is a new feature added to the AV-software bundle. This tool allows you to manipulate the software package you would like to install on a client or a server.
- Installation via Logon Scripts. You can edit your existing Logon-scripts with the necessary entries for the Logon-script based installation of a Symantec AntiVirus Client. In most cases this method is used for Windows 3x or 9x machines, because these machines cannot be installed via the NT Remote tool.
- You can do a Web install. If you have a Web Server in your Company, where you can put the SAV CE-client software, you make the software accessible for the company's employees and send them the URL(Uniform Resource Locator) from where they can download the software. This method is used for networks with Windows 9x workstations without having Logon Scripts (see further information on ftp://ftp.symantec.com/public/english_us_canada/products/symantec_antivirus/symantec_antivirus_corp/8.0/manuals/savce80i.pdf , page 120).

In addition to the product integrated methods you can distribute the SAV CE-software via any software distribution tool. Because you are able to create *MSI packages* or self-executables with the Symantec Packager it is also possible to implement these packages into a *Windows 2000 Active Directory Group Policy* (*http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolicyintro.asp*), so that a machine gets loaded with the AV client as soon as it goes online.

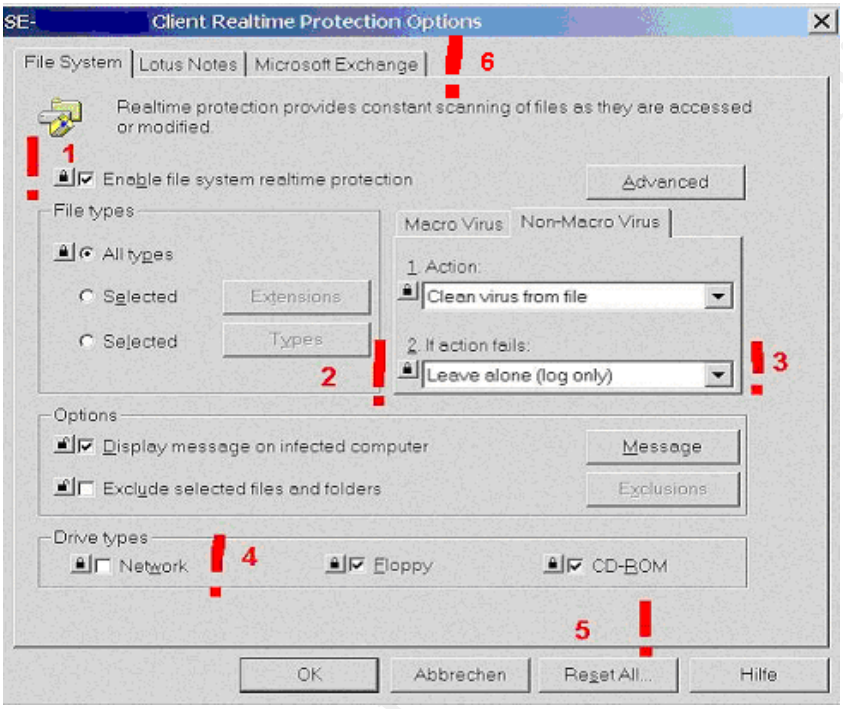
Note: For any installation on an NT based operating system it is mandatory to have local administrative privileges!

Now that the software is installed we get to point where we have to decide which Symantec AntiVirus-settings the machines should have and which strategy we go for. There are several facts that will influence the decision. E.g.: the type of email client installed is as well important as the applications running on the machines.
I will provide to you some standard rules for planning and configuring:

1. Computers with databases installed should be tested with the Virus scanner installed. If the database is too big, exclude the database from realtime protection.
2. **Network scans** should always be disabled, because machines on the network should have their own AntiVirus realtime protection installed.
3. If there isn't any **Microsoft Exchange**- or **Lotus Notes Email-client** installed, the "plug-in" does not need to be installed.

4. If you install the software to a **mail server**, make sure to exclude the mail-database file from realtime protection.
5. If possible try to allocate at least one dedicated machine only for the Primary Server function. It wouldn't make sense to load the Symantec AntiVirus Server software to a **Domain-Controller** or a **Database-, Mail- or Web- server** if these servers have to provide functions to hundreds or thousands of users. The Symantec AntiVirus Cient Software can be installed instead.
Note: In smaller network environments the Symantec AntiVirus Server software can also be installed to servers with other functions.

Pic4



1. Realtime Protection should always be turned on and only a small number of employees should have the right to turn it off(e.g. developers)
2. Make sure that all changes you've done are confirmed by closing the padlock in front of the section before you click "*OK*". Otherwise the changes will only take effect on new client-installations.
3. The 2nd option for "*Non Macro Virus*" should be set to "*Leave alone, log only*". Yes, it looks strange, but imagine what would happen, if such a file is a mandatory part of an operating system (e.g.: *.dll, *.sys,…). In the worst case it won't be able to restart! For an important system like an internal Database or Web Server, on which the majority of the employees work, this would be fatal for your company.

   Note: With a good alerting system implemented you have time to react and to make decisions on how to continue. A controlled shutdown of an important system is possible and sometimes much better than any disaster recovery as a result of missing files.

4. In general every machine on your network should be protected with a local installed AV-scanner, so the option "*Network*" under the section "*drive types*" should be turned off. If it is turned on, it is possible that this leads to performance problems. (e.g.: several users scanning the same drive)
5. If you are not sure that the changes will become effective on the target-systems, you can push the "*Reset All*"-button. This will have as a result, that all selected clients will receive the entire configuration update, regardless of what part of configuration already exists.
6. The second and the third tab give you the ability to set up realtime-protection options for the email scanner installed. "Only" Microsoft Exchange and Lotus Notes based email clients can be protected. The "plug ins" will grab into the mail files and detect any Virus, as soon the mail is downloaded from a mail server. Even if the email client is not installed, the "plug in" can be installed with the Symantec AntiVirus Client Software. *Note:* If a Microsoft Exchange mail client will be loaded after SAV CE-Software the Symantec AntiVirus Software with its "plug in" has to be reinstalled.

The SAV CE strategy also includes the plan which workstations and servers will have the same configuration-set and which machines should be treated different or maybe separately. You can create Client groups and generate configuration sets for those. Open the System Center Console and right click the "*groups*" section inside the Server Group you would like to create a Client Group→Select "*New Group*" and type in a name. This name should stay for a part of your organisation or machines which will have the same configuration. This helps to organize your Symantec AntiVirus enterprise network. Privileges are one argument for implementing groups as well as the connection speed could be a good reason for having a specific group. E.g.: The Remote users on their Windows 98 machines(pic1). Since these machines will not be frequently connected, they should have the right to start Live Update instead of receiving their updates via VDTM. To combine both update methods, you can use the "*Continuous Live Update*". Even the computer that is not very often connected to the corporate network, the client will still be managed. The advantage of this strategy would be, that you still have some kind of control on such workstations, while you would never get any feedback from an "*unmanaged client*".
Note: Since the release Symantec AntiVirus Corporate Edition 8.0, I don't see any reason anymore for having unmanaged clients inside a corporate network.

With the Symantec System Center you have certain amount of reporting and alerting, but there are disadvantages, which make the administration of your Symantec AntiVirus network more difficult the more machines you have on your network. Some things have to be considered when we talk about the Symantec Console:

- There is no structured information with Alert Management System-Mails
- You have only one view for filters in Symantec System Center
- No possibility for a quick overview in Symantec Console in big network-environments with many computers
- Alert Management System-Log-view has no filters or other sort orders

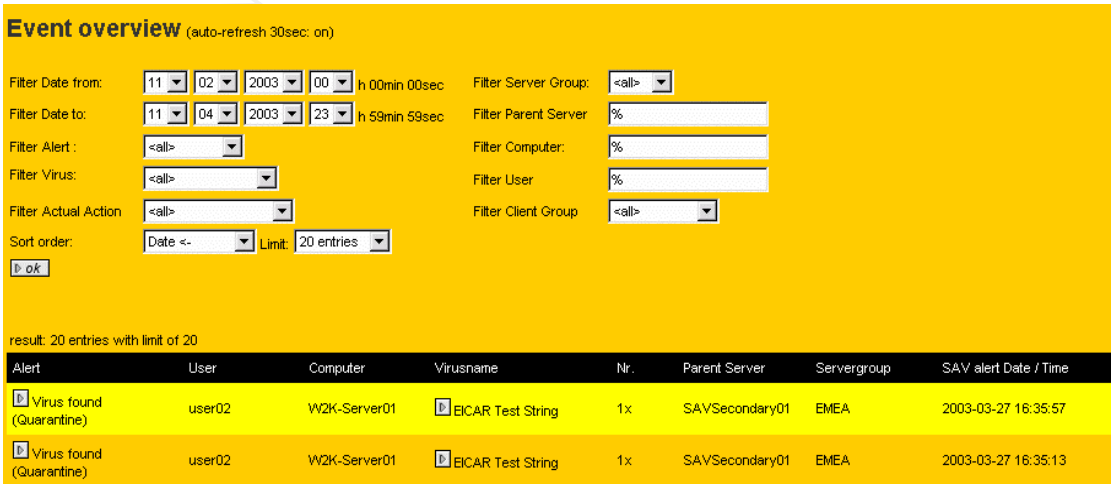
- If you have configured the Alert Management System for alerting with emails you will have your mailbox filled up with a huge amount of AMS-emails.
- There is no way of realizing a tendency of virus appearance
- Only a maximum number of 5000 AMS-events can be stored
- It is not possible to get an event-report for single computers history
- With the AMS-log there is no “sort functionality” included
- The Symantec AntiVirus product can “only” handle the Symantec AntiVirus Corporate Edition Software
- Even different Symantec AntiVirus scanner, e.g.: Symantec AntiVirus for SMTP Gateways or for Symantec AntiVirus for Exchange cannot be monitored.

One solution is to go for the **SAV Reporter**, because this tool can solve all of these problems and it is easy manageable. This tool provides:

- A quick overview even without SSC from anywhere, because it is manageable via a Web interface
- Multiple data filter, e.g.: by user or a role based model, are possible
- There is only one notification agent
- Building statistics and importing them immediately into charts, and it is easy to develop new statistics or reports (e.g. who has had the most viruses)
- No more mails from SAV-Alerter in your mailbox
- Tracking back on historical data, because everything is saved in an database
- Monitoring many Symantec AntiVirus-tools in one console
- Easy to develop modules for other tools than Symantec AntiVirus
- A worldwide overview without a strong network-connection. While the Symantec System Center – Symantec Anti Virus-communication requires a good network-connection, the SAV-Reporter is able to collect email-alerts from everywhere.

Pic 6

Results of predefined filter



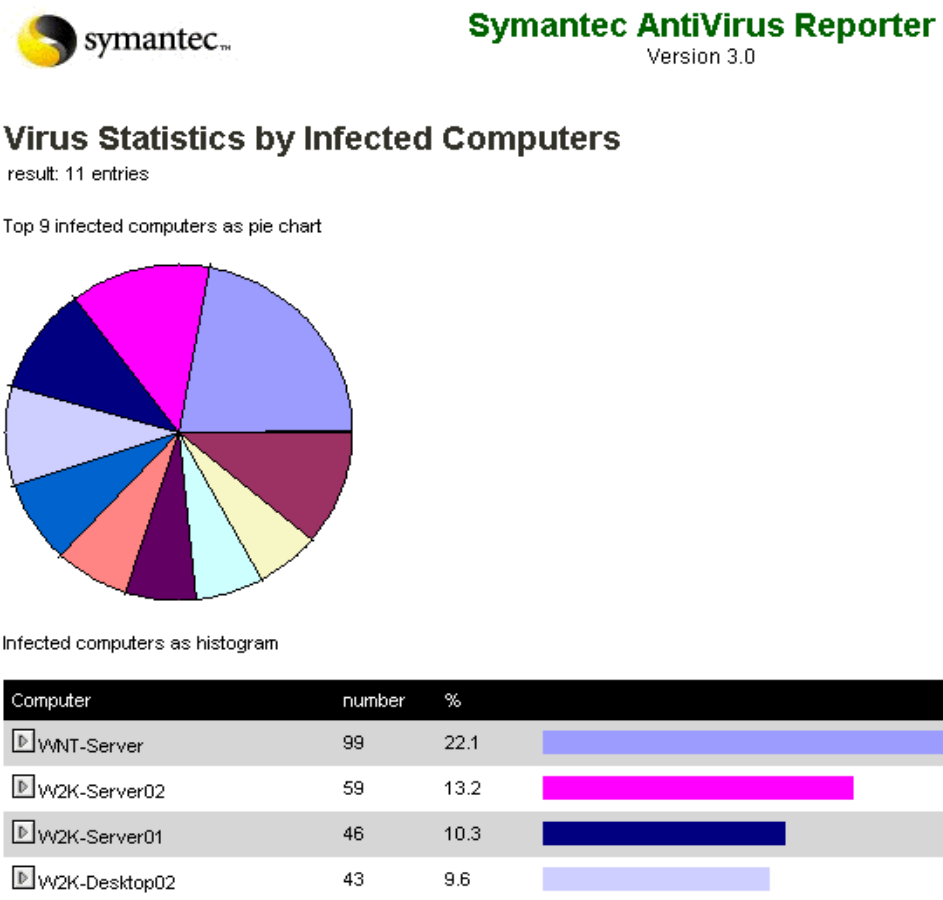
Alert Message from the SAV Reporter

symantec™ Detail Alert Information

Customer's Logo

Alert No	464
Server-/Clientgroup	EMEA /W2K Server
Parentserver	SAVSecondary01
Alert:	Virus found
Alert DB Insert Date:	2003-03-27 16:43:02
Alert SAV Server Date:	2003-03-27 16:35:57
Severty	
Source	
Logger	6619237
Virus Name	EICAR Test String (1x)
File/Path:	C:Documents and Settings avqaLocal SettingsTemporary Internet FilesContent.IE5W83RU0ICeicar.com[1].txt
Actual Action	Quarantine
Requested Action	Clean
Description	

Reports and charts



symantec™

Symantec AntiVirus Reporter

Version 3.0

Virus Statistics by Infected Computers

result: 11 entries

Top 9 infected computers as pie chart

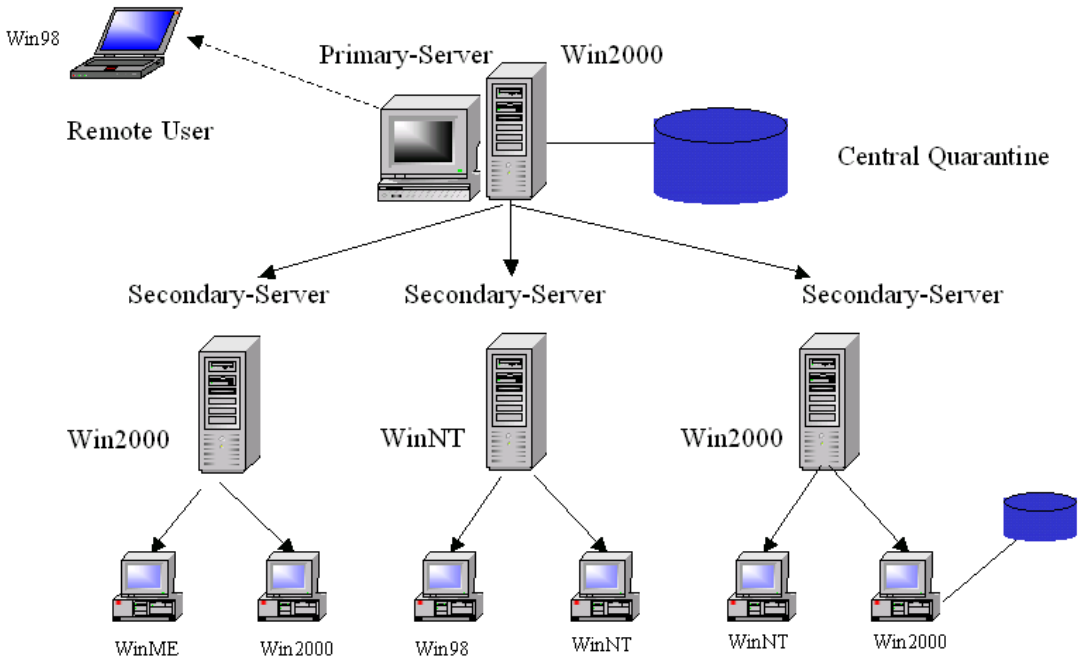
Infected computers as histogram

Computer	number	%
WNT-Server	99	22.1
W2K-Server02	59	13.2
W2K-Server01	46	10.3
W2K-Desktop02	43	9.6

An Online-Demo exists, where you can have a look at the SAV-Reporter and if you would like to have additional information mail to: Volker Rath, Sr. Security Consultant Symantec Security Services, the developer of the SAV-Reporter.
His goal is it to improve this tool wherever it is possible and therefore he appreciates any comments or suggestions for improvements.

Summary:

This is how it could look when you are finished with the implementation of Symantec AntiVirus Corporate Edition 8.0. Any Windows NT based machine could have the Symantec System Center Console loaded. The SAV Reporter could be attached to any Apache Web Server or Microsoft Internet Information Server.



You have read about how to protect your network against viruses and what you have to consider. But all of this is useless if you don't get your employees working with you. You have to make all employees aware of the importance of the AntiVirus business. You can set up the best configurations for the machines on your network if e.g.: developers abuse the privilege "turn off realtime protection" to keep the AntiVirus scanner turned off the entire day. It doesn't really matter which AntiVirus product you choose, but one important thing you have to keep in mind: What type of support will I have with the AntiVirus product. The Symantec AntiVirus Corporate Edition has four basic types of support, but this is very often an issue of having the budget for additional support. Only with an Internet- connection to the Symantec Web-Site, you can already handle the majority of support cases. If there is **one** dedicated system administrator, who looks after the AntiVirus business in each bigger location, it should be enough. Since the basic strategy is developed by your entire team, every system administrator, responsible for Symantec AntiVirus, is able to work as a backup for another colleague, who is temporary not available.
After a certain amount of time you might find out, that some parts of the Symantec AntiVirus protection strategy have to be reconsidered(e.g.: SAV CE Clients have to get different parent servers) and afterwards re-arranged. By transferring the GRC.dat

to the machines which have to be reconfigured, the change of a whole strategy will be done.
If you have made your decision to go for Symantec AntiVirus Corporate Edition 8.0, than integrate the SAV Reporter as well. It might be a little bit more work at the beginning, but once it is implemented correctly, you will get the maximum AntiVirus protection for File-servers and Desktop-machines.

Glossary:

Manuals for the *Symantec AntiVirus Corporate Edition 8.0* are located in the folder "*docs*" on the CD or on the Symantec Web-Site:
ftp://ftp.symantec.com/public/english_us_canada/products/symantec_antivirus/symantec_antivirus_corp/8.0/manuals/
Symantec AntiVirus definitions are placed under:
ftp://ftp.symantec.com/public/english_us_canada/antivirus_definitions/norton_antivirus/

Index:

Symantec AntiVirus Corporate Edition Server(SAV CE Server):
A SAV CE Server is able to distribute Virus Definitions and configuration sets to other machines. Such a server can have four roles: It could be a Master Primary Server, a Primary Server, a Secondary Server or a Standalone Server.

Primary Server:
The server in a Server Group that loads down the virus definitions from another location (from the Symantec Web-Site or from a Master Primary Server) and pushes them to the secondary severs.

Master Primary Server:
If you have several Server Groups with Primary Servers included, but you would like to centralize the virus definitions update process than you can go for this opportunity. Other Primary Servers will download their definitions from this server and will not go to the Symantec Web Site directly.

Server Group:
Every Symantec AntiVirus Server has to be in an AntiVirus server group. Such a group can only contain one Primary Server. The number of Secondary Servers can be variable as well as the number of Symantec AntiVirus Clients.

Secondary Server:
A machine loaded with the AntiVirus Server component. In addition to that it receives its updates from a Primary Server. Usually the AV-Server has AV-Clients attached.

Standalone Server:
A Symantec AntiVirus Server without other Symantec AntiVirus Servers or Symantec AntiVirus Clients attached to it.

Note: One reason to have such a server is for example the integration in an operating system migration process to have a temporary Symantec AntiVirus Server, so that the clients have a complete protection.

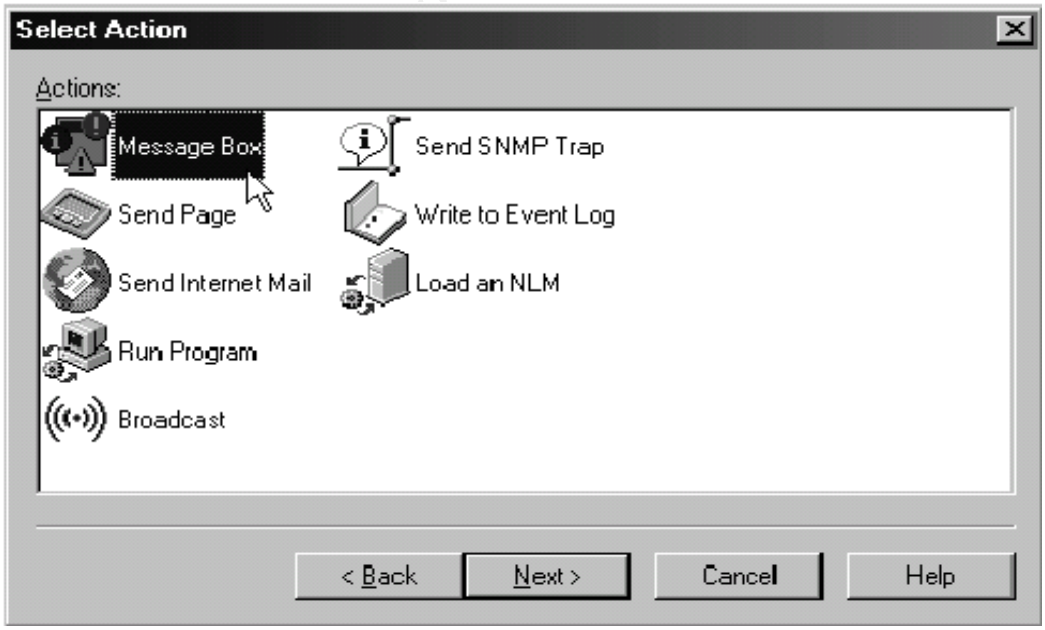
Symantec AntiVirus Client(SAV Clients):
A machine on which the SAV CE client is loaded. It can even be "*managed*" or "*unmanaged*". A "*managed*" AV client has an entry for its Parent Server. An unmanaged client hasn't got any Parent Server information and will never be seen from the Symantec System Center Console.

Symantec System Center Console:
If the console is loaded, you can manage your Symantec AntiVirus environment easily. You can distribute the SAV CE Software as well as changing configurations on AntiVirus -servers and -clients.

Parent Server:
Any Symantec AnrtiVirus Server that has SAV CE Clients attached. It can be a MasterPrimary-, Primary- or Secondary-Server.

Alert Management System (AMS²):
An additional function is coming with the product. You can setup an alerting system, which makes life easier to react in cases of a virus infection. Several actions can be set up through the Alert Management System. These options can also be combined, e.g.: An entry to the event log will be created in addition to that an Internet Mail is going to be sent to the administrators.
Note: AMS is helpful for the SAV Reporter, because this tool will read the information provided by the Alert Management System.

Pic5



Live Update (LU):
A *Pull-mechanism* that allows you to download the latest Virus Definitions from any location(In most cases the Symantec Web-Site) via http-, ftp- or LAN- connection. It needs to be configured either from the console, or through the Live Update Administration Utility, or manually at the machine itself.

Virus Definition Transport Method (VDTM):
One of the big advantages using SAV CE is this update method. Once you have told an AntiVirus-machine, what its parent will be, the update of the definitions will run automatically, without any action to be done at the "Secondary-Server" or "AntiVirus-client" itself. This mechanism which is integrated in the program can be seen as an opposite of the "*Pull-mechanism"* of the Live Update. The VDTM-method is a "*Push-mechanism"*.

Live Update Administration Utility:
A tool that helps you setting up a Live Update configuration for single clients. A "host-file" generated with this tool has to be copied to the SAV machine's Live Update directory (\\documents and settings\AllUsers\application data\symantec\liveupdate).
Note: Be careful, from this moment on the client is managed again and you change settings in the SSC, you will change also the Live Update settings.

Intelligent Updater:
The third way of updating Virus Definitions, which is also supported by Symantec. You can download the definitions manually by going to the Symantec Site and download the newest virus definition-file.
http://securityresponse.symantec.com/avcenter/download/pages/US-SAVCE.html
When having the file on your local system it needs to be executed. The definitions will extract themselves to the dedicated installation directory and the new definitions will then be implemented into the software.
Note: If your company network is not connected to the Internet, this is a method to keep your AntiVirus definitions up to date.

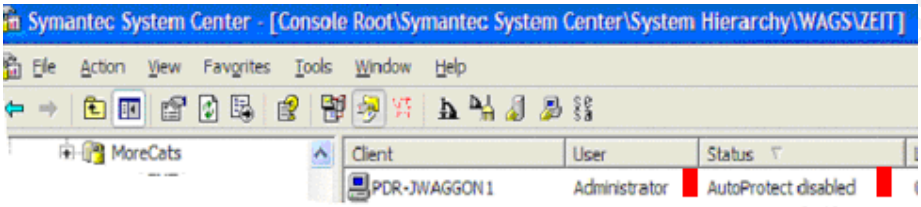
Continuous Live Update:
The continuous Live Update allows you to manage virus definitions file updates for Symantec AntiVirus Corporate Edition clients with an Internet connection, but infrequent or no connection to a parent server. You can specify a maximum number of days after which definitions are out-of-date. When definitions exceed this date, Symantec AntiVirus Corporate Edition automatically initiates a silent Live Update when it detects an available Internet connection.

Managed clients:
A managed SAV CE Client is a client, that has an entry for a Parent Server, so that it will be seen and managed by the console

Unmanaged clients:
Unmanaged SAV CE Clients don't have an entry for a Parent Server. Because of this you won't be able to see those clients in the Symantec System Center Console.
Note: With the GRC.dat it is possible to change the settings of client. By copying the GRC.dat onto the SAV CE Client , the machine will immediately be managed again.

Realtime protection:
A virus protection that is always online and that scans any change of files on local drives. Although this feature should be turned on at any time, in some cases it might be necessary to stop this service for a time period. Even if you've given the right to a single user or to a group of users to turn of the realtime protection, from the version 8.0 on you will see this in the Symantec System Center(pic2) and you are able to set an "auto re-enable"-option, which turns on the scanner after a predefined time period automatically.

Pic2



Symantec System Center Console(SSC):
The administrative tool to organize and configure your AntiVirus business. Installations, configuration changes, quarantine- and AMS- settings can be set up and report functions are also included. In every bigger location(in our example these are: Berlin, Munich, Vienna and Paris, pic1)
Note: If you start a Symantec AntiVirus Client installation from the console, the client will be installed from **this** console and not from the Server you've decided to be the Parent Server.

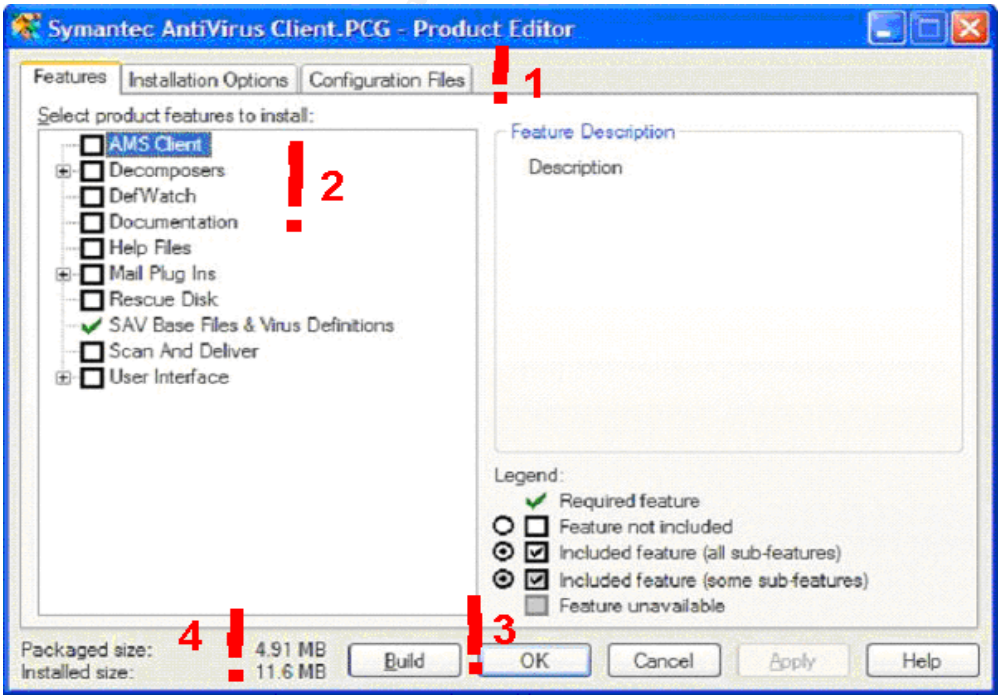
Digital Immune System:
The Digital Immune System is a fully automated, closed-loop antivirus system that manages the entire antivirus process, including virus discovery, virus analysis, and deployment of a repair to the affected computers. In addition, the Digital Immune System eliminates many of the manual tasks that are involved in the submission, analysis, and distribution processes. Automation dramatically reduces the time between when a virus is found and when a repair is deployed, which decreases the severity of many virus threats.

Quarantine Server:
The Server collects data from the corporate Symantec AntiVirus Clients' quarantine and **sends only the malicious code** to the Symantec Gateways. These Symantec Gateways check if there are already the right Virus Definitions exist. If not, the Symantec Gateways sent the possible infected data to the Symantec AntiVirus Research Center, where, in cases of true infections, new AntiVirus definitions will be generated and sent back to the dedicated customers. The other reaction is that the received data-string would be declared as "uninfected" and the information will be sent back to the customers Quarantine Server, so that finally the original file will be released from the machines local quarantine.

Groups(Client Groups):
In SAV CE 8.0 it is possible to create certain Client Groups for "*managed*" machines, in which only client computers participate. In comparison to the previous version of Symantec Norton AntiVirus, there hasn't got to be a SAV CE Server included anymore, which makes life easier. The Parent Server can vary between the clients

GRC.dat:
The overall configuration file. If you have problems with your SSC or the communication between the server and the client fails for any reason, you can edit the GRC.dat and copy it to: (\\documents and settings\AllUsers\application data\symantec\norton antivirus corporate edition\7.5\) and in an interval of 3 minutes the file will be imported and the configuration change will be done.
Note: This is also the only way of changing the client from "*managed*" to "*unmanaged*", except for a complete new installation.

Symantec Packager:
An additional tool that give you ability to create Symantec AntiVirus software packages. Information about this very powerful utility will be found under:
ftp://ftp.symantec.com/public/english_us_canada/products/symantec_antivirus/symantec_antivirus_corp/8.0/manuals/sympckgr.pdf
A big advantage of this tool is that you can also change configurations on the target machines. If you have older versions of NAV CE installed it is also possible to create a removal package. Each developed package can be coupled with existing packages to create one overall package, to avoid distributing several packages instead of one.
Note: Only Symantec software products are supported by Symantec, but it works with other applications as well.
This is an example of how the packager looks like:
Pic3



1 The *Features* tab will show what physically will be installed on the target machine.
The *Installation Options* will give you the opportunity to add files and commands, like newer virus definitions.
Configuration Files are for example a new GRC.dat

2. You select or de-select what parts will be included in this installation package and if you highlight an option, a small description of the feature will show up.

3. The button "**Build**" is very important, because at the end of each configuration setup you have to push this button. You can change whatever you want; as long the button is not pushed the new package won't be created.

4. This part of the window is also important, because the Packaged size is different from the Installed size.
Note: For the installation you need to calculate with the sum of both sizes. The Package will exist on the target machine, as long the installation is running. Once the complete software is installed, the origin package will be removed.

The different types of support for Symantec AntiVirus products are:

1) Online Support via the Web Site: http://www.symantec.com/techsupp/enterprise/
Advantages: - no additional costs, up to date, search functions, product release information, immediate access, 24 hours – 7 days a week.
Disadvantages: Internet access needed, some times not detailed enough, no dedicated point of contact, the majority of the documentations are "only" in English, documents might have links to several other documents, which can lead into confusions and longer search intervals. Not all information is accessible like in the Platinum Support.
2) Call by call Support: For each country or region a telephone number exists, that can be called for one single incident. One price for the duration of the entire call.
Advantages: Direct contact person at Symantec, who is able to guide you through the information you are looking for, long search intervals will be avoided.
Disadvantages: "Only" during working hours from 09:00 AM until 6:00 PM. Much higher price for one call. Each telephone call you might get a different person to talk to, so you will have to explain your all facts each new call. In cases of new Virus alerts, it takes longer to get a free line. This is a matter of fact, because there is only a dedicated number of support people working in this team. Not all information is accessible like in the Platinum Support.

3) *Gold Support:* Also one phone number for each country/region
Advantages: 24 hours, 7 days a week, a direct contact person at Symantec, the information you would like to have saved by Symantec will be saved together with your customer ID, so you have to explain your company facts only once during the first call. This saves time and you can start immediately with the actual problem you have. Product updates are automatically sent to you, because the Gold Support contains an **upgrade insurance**.
Disadvantages: You don't have one single trusted person at Symantec, because it could be any member of the Symantec team, who you have to deal with and you still pay local phone calls. (For the US this is OK, but for Europe this means, that you have to pay per certain time interval. Not all information is accessible like in the Platinum Support.
4) *Platinum Support*: The phone calls are for free. The maximum support you can get from Symantec.
Advantages: Two named technicians are at Symantec, who know exactly how your environment looks like. They will support 24 hours, 7 days a week, and will visit your company frequently to build a good relationship. When problems exist, that you aren't able to fix, they will support you at your location. They keep you up to date with new product releases. All information is accessible via the Web. Beta-products will also be made accessible, so that you can participate in testing future product releases, where you can bring in your company needs and suggestions.
Disadvantages: It costs a lot of money and as long as there are no major incidents, you have to justify the money in front of the management.

Disadvantage for all types of support: The SAV Reporter is not supported by the Symantec. You can get support for this product from Volker Rath's team, but of course this is coupled with consulting business.

References for this document:

Books:

- **Configuring Symantec AntiVirus Enterprise Edition**
written by Robert Shimonski, ISBN: 1931836817
- **Symantec AntiVirus Corporate Edition 8.0 installation Handbook**, is delivered in written format with the product and on the CD in the directory: . \docs. In addition to this you find the installation handbook on the Symantec Web Site:
ftp://ftp.symantec.com/public/english_us_canada/products/symantec_antivirus/symantec_antivirus_corp/8.0/manuals/savce80i.pdf
- **Symantec AntiVirus advance student guide**, provided to you when you attend the "Configuring and troubleshooting Symantec AntiVirus" course

Links:

- **Symantec AntiVirus Corporate Edition 8.0 installation walk-through for Administrators.**
http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2002073014500548
For installation of the Symantec AntiVirus Corporate Edition it is a very helpful link.

- **Top requested installation and configuration articles for Symantec AntiVirus Corporate Edition 8.0**

http://service1.symantec.com/SUPPORT/ent-security.nsf/docid_p/2002112108541748?OpenDocument&src=plat_hot

You will find very helpful hints for configuring several options in the product.

- **In Norton/Symantec AntiVirus Corporate Edition, how do I go from an unmanaged to a managed installation in order to enable Automated Virus Definitions?**

http://kb.indiana.edu/data/akfs.html

This document includes web-links to information about uninstalling the product as well as some other facts.

- Because of the big amount of customers, who are using the product you find also news-groups or discussion-groups on the Internet with a lot of information on Symantec AntiVirus. This is an example:

http://www.experts-exchange.com/Security/Q_20540788.html

A few links to Web-Sites of companies which provide AntiVirus Software:

Symantec:	http://www.symantec.com
F-Secure:	http://www.f-secure.com/
Trend Micro:	http://antivirus.com
McAfee:	http://www.mcafee.com
Panda:	http://www.pandasoftware.com/
Sophos:	http://www.sophos.com/
Computer Associates:	http://www3.ca.com/virus/

Last Updated: September 25th, 2017

Upcoming Training

Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event