Global Information Assurance Certification Paper

"Auditing Symantec AntiVirus Corporate Edition"

GSNA Certification Practical
Jonathan G. Lampe
Version 1.2 - December 11, 2001

GSNA Assignment 1 - Research in Audit, Measurement Practice and Control

Focus of Audit

- Symantec AntiVirus Corporate Edition ver 7.5-7.6
- "Central Management and Deployment"
- Includes: Core Anti-Virus Software (Administration Console, LiveUpdate, Server and Desktop), Evaluation of Server Recovery, Incident Response, Security of Software, Basic Quarantine Procedure
- Excludes: OS-Level Integrity of Symantec Servers and Desktops, Security vs. Scalability Concerns, "Email Gateway" Anti-Virus Protection, Firewall/Router/Network Configuration/Scalability

Current State of Practice

Symantec (aka "Norton") is one of several "big-name" vendors in the large-installation anti-virus market. Large installations require central management features to deploy and configure any number of desktop applications, and anti-virus applications are by no means an exception to this rule.

Symantec follows the increasingly common architecture of "console-server-client" to satisfy this requirement. A "console" is a management piece of software used to define how servers and clients interact and are configured and may be run from various administrators desktops. "Servers" are responsible for updating and controlling access to repositories of information (i.e., virus definitions) and "clients" actually perform the work. (Again, as is common in this model, a server acts as its own client so it can enjoy a superset of the features available to individual clients.) From an auditor's point of view it will be important to ensure controls are in place to allow administrative access only to specific people and/or workstations, that appropriate information is backed up on the servers, that clients are not allowed to ignore information from the server and/or adminstrators and that administrators are provided enough information to identify the weaknesses of their current deployment and find out what defensive actions the system has taken in response to specific perceived threats.

Symantec's core antivirus engine is quite mature as are the products of its major competitors. Like most mature antivirus products the fidelity of Symantec's antivirus detection system depends much less on a bug-free engine than the age of the signatures the engine has available to itself. Therefore in addition to effective settings an auditor should look at the way updates are collected from the antivirus vendor and disseminated to desktop clients.

To sum up, I believe a complete audit of Symantec's system (and similar distributed anti-virus systems) should consist of the following basic components arranged in the framework suggested below. In place of a "console" section I instead elected to use a "global" section to reflect options set across entire installations. Finally because virus protection is basically an automated incident response utility, I simply folded SANS six incident response steps into the client section below.

"Computer Security Incident Handling: Step-by-Step," SANS Institute Publications.
(http://www.sans.org/newlook/publications/incident_handling.htm)

Suggested Distributed Anti-Virus Auditing Framework

- Globals (TBA)
- Clients
  - Preparation - Are clients active and configured properly?
  - Identification - Do clients have latest signature files? Can they identify virus-like behavior?
  - Containment - Can clients keep viruses from spreading?
  - Eradication - Can clients eliminate viruses?
  - Recovery - Can clients notify administrators to restore damaged systems?
  - Follow-up - Is a log of client behavior available to adminstrators?
  - Unauthorized Use - How much control over settings are users allowed? Can virus protection be disabled?
- Servers
  - Recovery - Are servers properly backed up?
  - Fidelity - After clients pass off information to the server, how is it protected, authenticated and retained?
  - Unauthorized Use - Are servers protected from unauthorized configuration changes? Are servers protected against "read" actions against the configuration, viral signatures, console software downloads, etc.

To find the state of distributed anti-virus auditing I turned of course to the Internet.

I performed a number of searches on the Internet on November 23, 2001 through the Google search engine ("www.google.com"), SANS search ("www.sans.org") and Symantec ("www.symantec.com") In particular, I used the following words in various combinations: Symantec, Norton, Antivirus,

Audit, Auditing, Checklist, Procedure, Hints, Policy, Configuration, Enterprise Edition, Best Practices. All but a few of the pages found in response to these searches basically noted that antivirus software was a good thing, but generally avoided specifics of any kind.

From the few articles which did go into specifics it seems that although there are a variety of well-known effective practices, a collection of these practices has not been codified. (In particular, my most tantilizing find was a cached page with dead links to best practice policies regarding this antivirus product - further searches on Symantec's site and google failed to find the documents this page referenced.)

"Symantec Security Response: Best Practice Policies: Enterprise Security Manager: Norton AntiVirus CE 7.5 Server on Windows 2000 - ISO 17799," google.com cache. August 24, 2001.
(http://www.google.com/search?q=cache:y6GL0VBlH_o:www.symantec.com/avcenter/security/Content/best.practice.policies/esm/2001.08.10.html+symantec+antivirus+best+practices&hl=en)

The following article by Bob Green gives a personal face to the dilemma of no specific documentation.

"One of our systems had to be rebuilt, and when the anti-virus software was re-installed something went wrong. With no set procedure for installing the anti-virus software we are not exactly sure what went wrong. ...there was no written procedure to follow, no documentation, no verification and no auditing. We just don't know what happened."

Mr. Green goes on to state that he feels better now with "near real-time updates," centralized reporting and the ability to find workstations with outdated signature files.

Green, Bob. "I Thought We Had Virus Protection: The Mistakes that Made Us Vulnerable to the W32/SirCam@mm Virus," SANS Information Security Reading Room. August 16, 2001.
(http://www.sans.org/infosecFAQ/malicious/sircam.htm)

Another article aimed at Yale univerity students and faculty asks them to update signatures weekly. As someone who has been burned by viruses in an environment with a weekly policy and then again with a daily policy, I am inclined to lend more credidence to Mr. Green's suggestions, but as an auditor I must believe that fitness of "frequency of updates" must be installation-specific. (Faster, fresher updates are generally better.)

Yale University Information Technology Services. "Getting the most out of your Anti-Virus software," Yale University.
(http://www.yale.edu/its/security/new-index.html?http://www.yale.edu/its/security/antivirus.html)

Also designed with academic users in mind, the following article lends more credidence to the idea of a sliding score for updates, noting that off-campus (not connected to the network) users should get weekly updates while on-campus (connected to the network) users should get daily updates. (Another topic for another day: estimating exposure based on number of contacts, i.e. emails, received in a day vs. freshness of viral signatures.)

"Norton Antivirus (Corporate Edition) - An Overview, " Georgia State University Computing and Communications Services. October 4, 2001.
http://www.gsu.edu/~wwwccs/docs/norton/nav.htm

A fourth article about securing roaming devices snotes that "malware" (including viruses) is most threatening when users are allowed to disable virus protection. (This may seem like yet another obvious concept, but please remember we are still defining what collection of threats we are evaulating our selected controls against.)

McAleer, Sean P. "A Defense-in-Depth Approach for Securing Mobile Devices and Wireless LANs," SANS Information Security Reading Room. January 24, 2001.
(http://www.sans.org/infosecFAQ/wireless/defense.htm)

A fifth article repeats what we already know: fresh virus signatures are good and workstations with disabled protection are bad.

Mallion, Bob. "Enterprise-Wide Virus Protection (So You Think You're Protected from Malicious Code!)," SANS Information Security Reading Room. November 20, 2000.
(http://www.sans.org/infosecFAQ/email/protection.htm)

A sixth article notes that virus updates should be pushed to users.

Zocco, Paul A. "Ten Days to Network Security," SANS Information Security Reading Room. August 6, 2001.
(http://www.sans.org/infosecFAQ/securitybasics/10days.htm)

I was very excited to see an "Antivirus Checklist" pop up on Symantec's site, but was disappointed to see that it was for uninstalling email gateway protection on Microsoft Exchange - an application beyond the scope of this audit.

"How to uninstall Norton AntiVirus for Microsoft Exchange manually and verify rights in Microsoft Windows NT and Exchange," Symantec Knowledge Base. October 15, 2001.
(http://service2.symantec.com/SUPPORT/ent-security.nsf/361fc4a260e563b1882568180069e1c0/99f795937d5be9b788256a3400750926?OpenDocument)

A seventh article contains a nice installation guide (with screenshots) which again recommends a personal user check for new definitions once a week, but has little to say about central management.

"Norton AntiVirus Corporate Edition for Windows 95, 98, Me, NT and 2000 Installation and Configuration," University of Virginia Information Technology and Communication. June 22, 2001.
(http://www.itc.virginia.edu/desktop/docs/navdoc/)

Finally a number of text-only procedures from the University of Indiana describe server procedures but do not specifically state what good values are for various settings. (i.e. "Check the box next to Schedule for automatic updates, then choose how often you would like the server to download virus

definitions.") However nearby documents contain good information about preventing unauthorized access to servers.

"How do I set up Norton AntiVirus Enterprise Edition so that my departmental workstations can update virus definitions automatically?," Indiana University Knowledge Base. January 12, 2001.
(http://kb.indiana.edu/data/ajar.html)

"In Norton AntiVirus Enterprise Edition, how do I prevent unauthorized users from connecting to my Norton AntiVirus server?," Indiana University Knowledge Base. January 16, 2001.
(http://kb.indiana.edu/data/ajcv.html)

Areas in Need of Improvement

Based on the framework I described above and my research, I believe improvements can be made in almost every area.

Clients-Preparation and Clients-Identification are the two best-documented audit framework sections and I expect to use elements from several checklists already in use to compose this list.

Clients-Eradication and Clients-Containment will be "gimme" categories - without delving into the source code we pretty have to take the vendors word (and the successful experiences of millions of users) and assume the software contains and eradicates viruses as advertised.

Clients-Recovery and Clients-Followup will by nature require some subjective analysis not only of the software but the skill of the administrators. A tactful checklist will need to be devised here.

Clients-Unauthorized use again does not have checklists readily available, but testing for this use and devising a quantifiable checklist should be relatively easy.

Servers-Recovery can borrow from any number of backup checklists with attention paid to Symantec's quirks.

Servers-Fidelity will require some reseach in Symantec's manuals and other sources and there exists the possibility that there will be no "settings" to audit, simply a statement of Symantec's capabilites in this area.

Servers - Unauthorized Use has a few procedures available from which I can begin to create a checklist, but more work and testing will be required to make it a full checklist.

Objective Measures

Most of the measures required to set clients up and check if they are really active are completely objective with few if any mitigating factors to worry about. The contents of logs and recovery options are also objective items. Backup checks are objective items because it can be tested whether or not a system is being backed up properly through exacting tests. Finally, the protection of logs and settings can easily be determined and graded against a set scale.

To meet these objective requirements auditors will have to collect a variety of screenshots and conduct several tests. (Specifics will be covered in the Annotated Audit Checklist below.)

Subjective Measures

Even though it is a major component of the usefulness of a virus protection scheme, the "ideal" value to use between checks for new viral signatures will continue to be a subjective component of these audits. The usefulness of an engine's ability to detect virus-like behavior will also continue to be debated and its "ideal" setting will therefore also remain a subjective component. The ability of the software to not destroy key files and for staff to respond appropriately to anti-viral alerts is a third subjective component. Finally, the appropirate length of time virus logs and server backups should be retained continues to be debated; both of these items are subjective measurements.

To meet these subjective requirements auditors will need to interview network administrators. (Specifics will be covered in the Annotated Audit Checklist below.)

Annotated Audit Checklist

Conventions and Definitions

(From this point forward a great deal of specific information has been adapted from Symantec product manuals, specifically Norton AntiVirus Corporate Edition 7.5/7.6 Implementation Guide and Symantec System Center Version 4.6 Implementation Guide. Exceptions to this rule (i.e. information from Symantec's web site) as well as information from third-party sources will still be separately noted.)

A "Server Profile" is a collection of information about a specific computer such as IP address, NetBIOS name, etc. (A server profile contains the minimum amount of information required to uniquely identify a specific computer on the network.)

A Symantec "Primary Server" holds all configuration information about a single Server Group. A Primary Server is also very frequently a Parent Server.

A Symantec "Parent Server" is the server to which clients connect to retrieve virus definitions, configurations and software updates. Parent servers collect this information from Primary Servers. In most cases a Parent Server will be a Primary Server and visa-versa, but Symantec allows administrators to divide the functions across multiple servers. (It is quite likely this functionality was added provide finer control over the network traffic various updates generate. Microsoft has recently added similar functionality to its Active Directory products for similar reasons and Symantec itself spends several pages in its manuals discussing the network traffic ramifications of various architectures.)

A Symantec "Secondary Server" is a server ready to stand in for a Primary Server. (In many respects these servers behave much like the original Windows NT Backup servers did minus the automatic promotion and limitations on the number of backup servers.)

A Symantec "Master Primary Server" is a primary server which carries the additional responsibility of collecting new virus definitions and software updates from Symantec and making them available to other primary servers in an organization.

Preparing for the Audit

Before the audit the auditor should request the following materials from the network administrator staff:

- Complete list of authorized administrators and workstations from which console operations are allowed and/or at which console software is installed.
- Server group documentation detailing purpose of group, administrator(s) responsible for group and important servers (primary, secondary and parent) within each group.
- Approximate total number of clients protected and clients per server group.

Determining the Scope of the Audit

The auditor can use the materials requested and the answers to the following questions to determine the scope of the audit he or she must perform. (Ideally the answers to the following questions would be determined by direct observation.) The primary goal of this section is to estimate the number of unique server group and/or client configurations the auditor must examine. (i.e. 5 unique server groups + 3 unique clients = 8 unique configurations.) In addition, a small amount of additional work will be required to audit the "global" configuration of the System Hierachy and the Quarantine Server.

WARNING: If the organization notes that group-wide configurations are not used and no other controls exist to ensure client configurations conform to approved standards, the auditor may advise discontinuing the audit and implementing such controls immediately.

How are servers grouped?

Choices: (Use the following terms, use as many as appropriate.)

- Universe (Everyone belongs to a single group.)
- Organization (Each department gets its own group.)
- Geography (Each location gets its own group.)
- Security (Resources experiencing similar threats or with more sensitive information are grouped.)

(Objective Item - Should be documented with a diagram which indicates the primary and optional secondary/parent servers within each group as well as the administrator(s) responsible for the group.)

Are servers grouped in an appropriate way?

(Subjective Item - Analyst should interview network adminstrators and management to determine the answer after considering factors such as adminstrative workload, security and the organization's special needs.)

Are changes applied to server groups or individual clients?

Choices: (Select one of the following.)

- Groups
- Clients

(Subjective Item - Should be documented through observation.)

If changes are applied to individual clients, do additional controls exist to ensure changes conform to a set standard?

(Subjective Item - Should be documented through observation.)

Once an auditor has determined the scope of the audit (and/or an appropriate fee has been agreed upon) the real audit can begin. Using the worksheets below and their accompaning explanations, an auditor can determine how well a Symantec Antivirus installation is performing.

Master Worksheets

"Global" Checklist

Perform these items once for an **entire Symantec hierarchy**. (i.e. once per company.)

Time estimate: 4 hours

Item	Pass/Warning/Fail
Server-Groups Locked When Not In Use	
Server-Group Passwords are Strong and Unique	
Administrative Saved-Passwords/Consoles are Secure	
Administrators are Aware of Virus Attacks	
Administrators React Properly to Virus Attacks	
Quarantine is Enabled	
Quarantine-Symantec Communication is Secure	
Quarantine-Symantec Submissions are Depersonalized	
Quarantine-Symantec Contact is Provided	
Quarantine-Symantec Patches are Auto-Installed	

"Client" Checklist

Perform these items once for each **server group** and/or **individually configured machine**.

Time estimate: 3 hours *per server group or machine*

Item	Pass/Warning/Fail
Scheduled Scan is Active	
Scheduled Scan is Configured Properly	
Realtime Protection is Active	
Server Realtime Protection is Configured Properly	
Client Realtime Protection is Configured Properly	
Client "Administrator-Only" Options are Configured Properly	
Client "Login" Options are Configured Properly	
Clients are Obtaining Latest Signature Files	

"Server" Checklist

Perform these items once for each **server group**.

Time estimate: 1 hour *per server group*

Item	Pass/Warning/Fail
Server is Obtaining Latest Signature Files	
Server is Protected Against Unauthorized Configurations	
Server is Properly Backed Up	

"Global" Checklist

The following checklist examines a few important elements related to the "Symantec Hierarchy" (the framework under which all server groups lie in the Microsoft Management Console snap-in) and the "Central Quanantine" (the central server to which copies of viruses and potential viruses are saved and/or sent from to Symantec for further analysis).

Server Groups Locked When Not In Use

Individual server groups may be "locked" or "unlocked". Unlocked groups may be edited by anyone; they are not password-protected. Locked groups require an administrator type in a password before changes are allowed. Administrators are not often aware that unlocked groups do not become locked after a certain timeout period; administrators should explicitly lock server groups after making changes. (The "Lock all server groups when exiting console" is not generally a reliable way to lock groups.)

This category judges how careful administrators are with unlocked groups. (locked=, unlocked= )

Choices: (Select one of the following.)

- PASS - Only those groups currently being edited are unlocked.
- WARNING - Most groups are locked, but some administrators have forgotten to lock their server groups after making changes.
- FAIL - Most or all groups are unlocked.

(Objective Item - Should be documented through observation including a SCREEN SHOT of console when System Hierarchy is first expanded.)

(Back to Global Checklist)

Server Passwords are Strong and Unique

Unlocking a server group requires a password. Each server group SHOULD use its own password, but large organizations may find that a common password for several groups is a necessity for everyday operations. Also note Norton does not enforce ANY kind of password strength, so administrators need to make good password choices.

Auditors should test the passwords of each server group and make notes regarding the results, but should not make their own copies of the passwords.

Choices: (Select one of the following.)

- PASS - Each server group has a hard-to-guess unique password or some server groups share hard-to-guess unique passwords.
- WARNING - All server groups use the same hard-to-guess password.
- FAIL - Passwords are easy to guess. (i.e. Any server group password is "symantec" or "joe".)

(Objective item - Should be documented simply with a note about problem areas.)

(Back to Global Checklist)

Administrative Saved-Passwords/Consoles are Secure

Server group passwords are saved by the Symantec System Central to the registry using DES encryption. The risk is not so much that these passwords could be cracked (although DES is fairly weak these days) but that someone with access to the console would have immediate access to the virus configuration of the enterprise as easily as they could click the "Symantec System Center" from their Start menu.

Choices: (Select one of the following.)

- PASS - Administrative consoles are secure and/or server group passwords are not saved
- WARNING - Administrative consoles are in IT departmental area and server group passwords are saved locally.
- FAIL - Server group passwords are saved locally on consoles outside of IT.

(Objective Item - Should be documented through observation including attempts to "double-click open" server groups from selected consoles without being challenged for a password.)

(Back to Global Checklist)

Administrators are Aware of Virus Attacks

Although Norton contains many features which seem to make it a "fire-and-forget" product, administrators should still be aware of the virus threat level in their networks as part of their overall security awareness.

On the positive side, Norton features extensive logging capabilities and configurable alerts. On the negative side, Norton's alert filters make it hard for adminstrators to be notified about ONLY the things they care about. (i.e. Tell me when X people get the same virus within Y minutes. Tell me when a machine has gone X days without an update. Page me at home if a virus was detected but could not be deleted, quarantined or cleaned.)

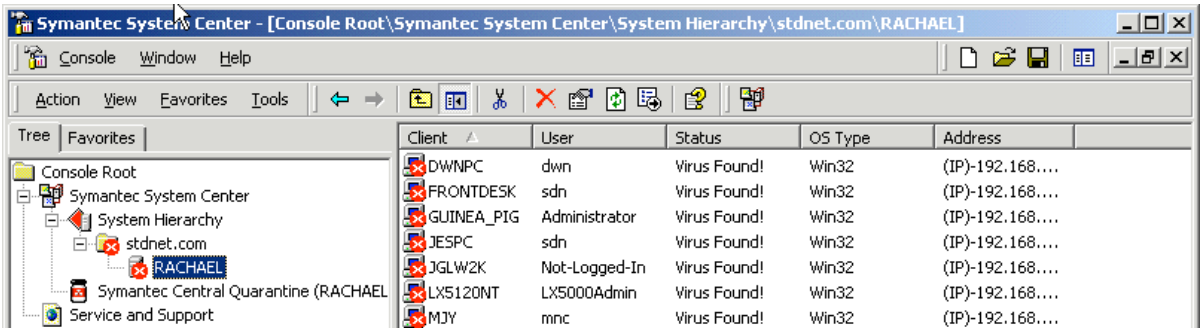
Many administrators will find the alerts to be too numerous to respond to and may be better off watching the console. (Norton begins to turn clients, servers, server groups and hierachies RED as viruses are detected.)

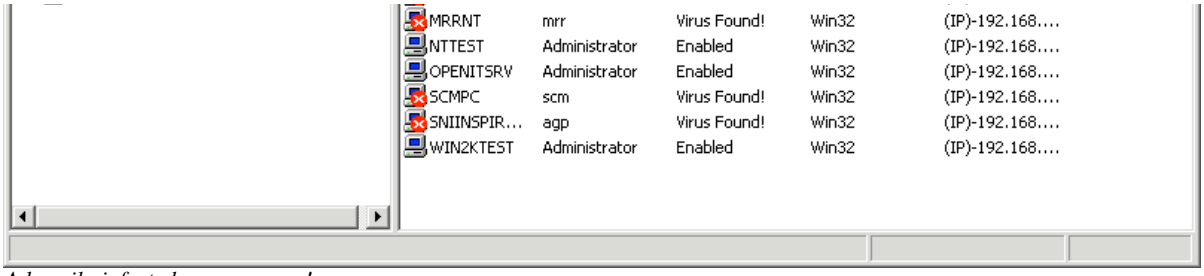
Regardless of the operational process however, administrators should be tuned into the health of the system and the best way to find out how well is to do some interviews. Questions similar to the following should help auditors get a feel for the adminstrators' familiarity with the environment.

- What are the top three viruses in your system right now?
- Which (server) group typically picks up the most viruses?
- What are the top three virus vectors into your system?

Another test would be to blanket a number of machines with EICAR test strings at some unannounced time and see if any administrators ask about it.

Finally, auditors should take time to walk up to the console at some unannounced time. A screen full of "infected" machines is probably a sign that administrators are not paying attention.





A heavily infected server group!

Choices: (Select one of the following.)

- PASS - Administrators seem to be paying attention and can confidently describe the viral health of their network.
- WARNING - Administrators seem to be paying attention most of the time and can describe the viral health of their network.
- FAIL - Administrators do not seem to be paying attention and/or cannot describe the viral health of their network..

(Subjective Item - Above all an auditor is asked to evaluate whether or not administrators are getting timely and useful information out of the system despite its limitations.)

(*Back to Global Checklist*)

Administrators React Properly to Virus Attacks

Despite Norton's ability to isolate, remove and fix files containing viruses, administrators still play a significant role in containing viruses, particularly if they appear to be progating throughout the network. This section involves more interviews and questions similar to the following questions may be useful.

- What do you do when you see that a client has been infected? (A good answer will involve checking that client's VIRUS HISTORY and determining whether or not Norton took care of the problem. If Norton did NOT take care of the problem the box should be isolated.)
- How do you tell if a virus is propogating through your network? (A good answer will include mention that the SAME VIRUS is detected on multiple boxes in a short period of time.)
- How do you prevent a virus from propogating through your network? (A good answer will involve checking Symantec's web site or a similar site to learn how the virus propogates and isolating known infected machines and perhaps key resources.)
- What kind of credentials do you use to sign onto the Quarantine system? (NT Domain credentials are used instead of "the usual" Symantec credentials.)
- Name three attributes retained in the Quarantine system besides the infected file itself. (Local machine name, operating system, contact infomation, etc.)
- What do you say to a user who just called to report a virus? (A good answer should involve identifying that user, that user's client and finding out whether or not the virus has been rendered harmless or not through the log facilities. In addition, the adminstrator may have specific advice for that user. i.e. No more ".exe" attachments!)

(Symantec offers a great training template regarding proper reaction to viruses in its Knowledge Base.)
"Example of an Emergency Containment Plan to respond to a virus infection," Symantec Knowledge Base. November 1, 2001.
(http://service4.symantec.com/SUPPORT/ent-security.nsf/552ba2f7636bedf088256818006f78bf/d4fe4fd2aa5d954c88256aab0064959f?OpenDocument&prev=http://search.symantec.com/custom/us/techsupp/enterprise/kb/query.html?*col=kb%20us*st=1*nh=10*pcode=*qp=url:/ent-security.nsf/552ba2f7636bedf088256818006f78bf,url:us-sarc,url:us-ts,url:us-lu,url:us-cs*qt=what%20needs%20to%20get%20backed%20up*miniver=nav-75-ce*sone=nav-75-ce_tasks.html*stg=*prod=Norton%20AntiVirus*ver=7.5%20Corporate%20Edition*base=http://www.symantec.com/techsupp/enterprise/products/nav/nav-75-ce/*next=&sone=nav-75-ce_tasks.html&stg=&prod=Norton%20AntiVirus&ver=7.5%20Corporate%20Edition&base=http://www.symantec.com/techsupp/enterprise/products/nav/nav-75-ce/&next=&src=ent&pcode=)

Choices: (Select one of the following.)

- PASS - Administrators have the knowledge and authority to isolate networks if necessary. Adminstrators are familiar with the Quarantine system. Administrators can tell infected boxes from uninfected boxes.
- WARNING - Administrators have the knowledge but may lack the authority to isolate networks if necessary. Adminstrators are familiar with the Quarantine system. Administrators can tell infected boxes from uninfected boxes.
- FAIL -Administrators lack the knowledge to appropriately isolate networks if necessary. Administrators are unfamiliar with the Quarantine system. Administrators cannot tell infected boxes from uninfected boxes.

(Subjective Item - Above all an auditor is asked to evaluate whether or not administrators respond appropriately to virus attacks given what they can find out about the situation through Norton's logs, displays and direct contact with end users.)

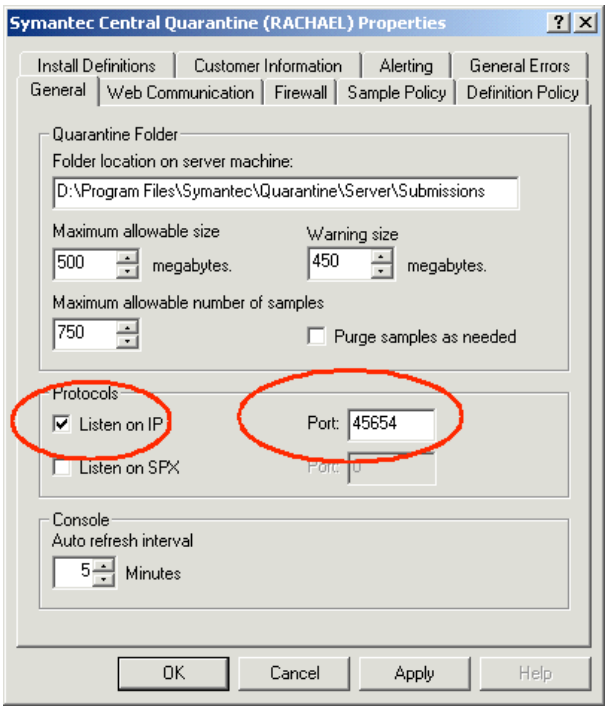
(*Back to Global Checklist*)

Note: Regarding Quarantine Configuration...

Symantec's Central Quarantine is a server in charge of collecting samples of the viruses discovered by various clients in one location. It also has the ability to automatically forward potential viruses found "in the wild" to Symantec and accept "beta" patches which may help defend the rest of the network against similar attacks by emerging threats.

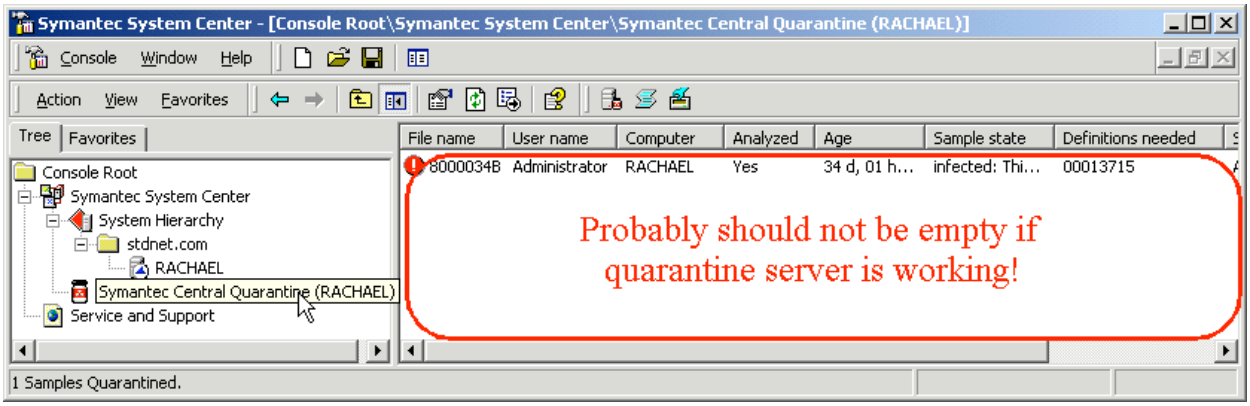
Quarantine is Enabled

The Quarantine server listens on an administrator-defined port. If no port has been defined, the Quarantine server cannot communicate with any clients.



(ConsoleRoot/SymantecSystemCenter/SymantecCentralQuarantine - Properties - TAB:General)

To confirm a working quarantine server, auditors can simply open the "Symantec Central quarantine" from the Symantec System Center. (Auditors will need a domain username and password to sign on.) After a few seconds the right panel should display a list of viruses quarantined. An empty list is generally a bad sign in all but the smallest organizations unless the organization has elected not to use the quarantine server at all.



Choices: (Select one of the following.)

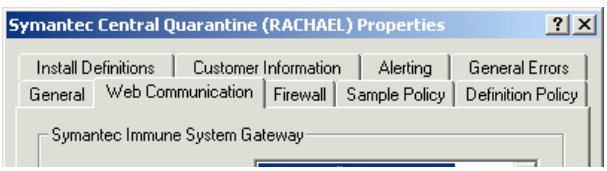
- PASS - Quarantine server is enabled on PROTOCOL PORT # and appears to be working.
- FAIL - Quarantine server is not enabled or is not listening on any port.

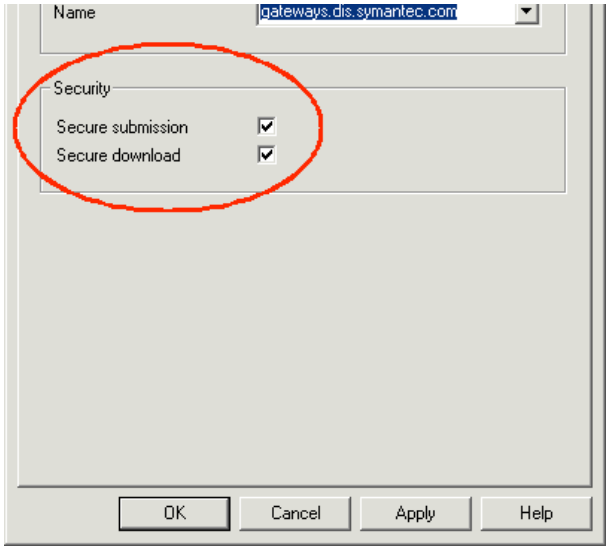
(Objective Item - Should be documented with a shot of configuration screen and a shot of the system console showing entries in the quarantine file.)

(Back to Global Checklist)

Quarantine-Symantec Communication is Secure

It may be a surprise to most adminstrators that Symantec offers enterprises the option of sending their data across the wire in the clear. (By default data is transmitted securely.)





(ConsoleRoot/SymantecSystemCenter/SymantecCentralQuarantine - Properties - TAB:WebCommunication)

Choices: (Select one of the following.)

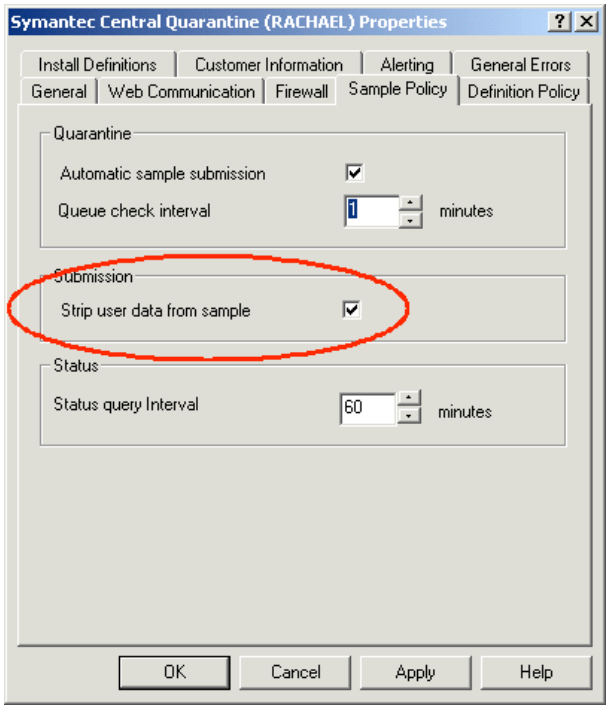
- PASS - Quarantine server uses secure submission and download options.
- FAIL - Quarantine server does NOT use BOTH secure submission and download options.

(Objective Item - Should be documented with a shot of this screen.)

(Back to Global Checklist)

Quarantine-Symantec Submissions are Depersonalized

Symantec offers a feature which attempts to strip potentially sensitive data out of virus samples before forwarding them. This option should be enabled. (By default data is NOT stripped.)



(ConsoleRoot/SymantecSystemCenter/SymantecCentralQuarantine - Properties - TAB:SamplePolicy)

Choices: (Select one of the following.)

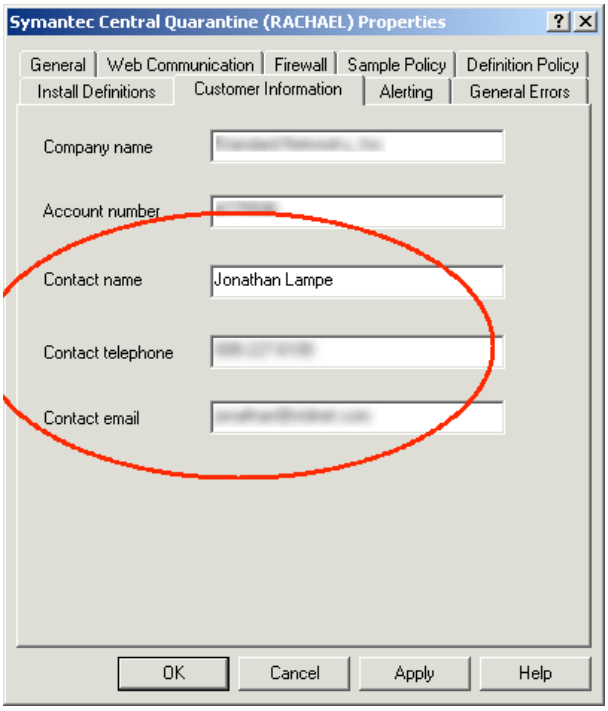
- PASS - "Strip user data from sample" is ENABLED.
- FAIL - "Strip user data from sample" is DISABLED.

(Objective Item - Should be documented with a shot of this screen.)

(Back to Global Checklist)

Quarantine-Symantec Contact is Provided

Symantec may need to contact administrators for additional information or to distribute a patch. The information Symantec will use to contact administrators is controlled on the Customer Information panel.



(ConsoleRoot/SymantecSystemCenter/SymantecCentralQuarantine - Properties - TAB:CustomerInformation)

Choices: (Select one of the following.)

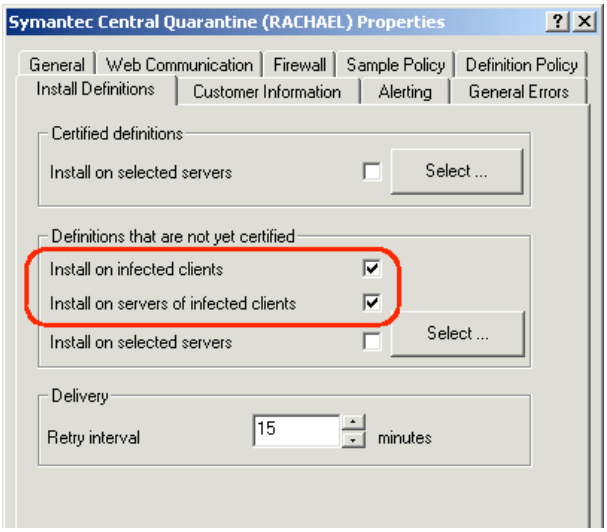
- PASS - Valid, specific information is provided. (i.e. person, IT Security department, IT department in a small organization)
- WARNING - Valid, general information is provided. (i.e. IT department in a large organization)
- FAIL - Bogus, no or overly general information is provided. (i.e. organizational switchboard, main number)

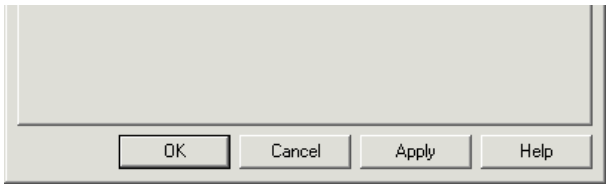
(Objective Item - Should be documented with a shot of this screen.)

(Back to Global Checklist)

Quarantine-Symantec Patches are Auto-Installed

Symantec may make test patches available to an organization and the Quarantine server has the ability to automatically apply these "uncertified definition" patches to the machines which registered a detect and to their parent servers. (Optionally, administrators may specify additional "high-value/vulnerability" servers on which to place these patches.) For Symantec to properly perform its job, the "infected clients" and "servers of infected clients" install options should be set.





(ConsoleRoot/SymantecSystemCenter/SymantecCentralQuarantine - Properties - TAB:Install Definitions)

Choices: (Select one of the following.)

- PASS - "infected clients" and "servers of infected clients" options are ENABLED
- WARNING - "infected clients" option is ENABLED
- FAIL - "infected clients" option is DISABLED

(Objective Item - Should be documented with a shot of this screen.)

(Back to Global Checklist)

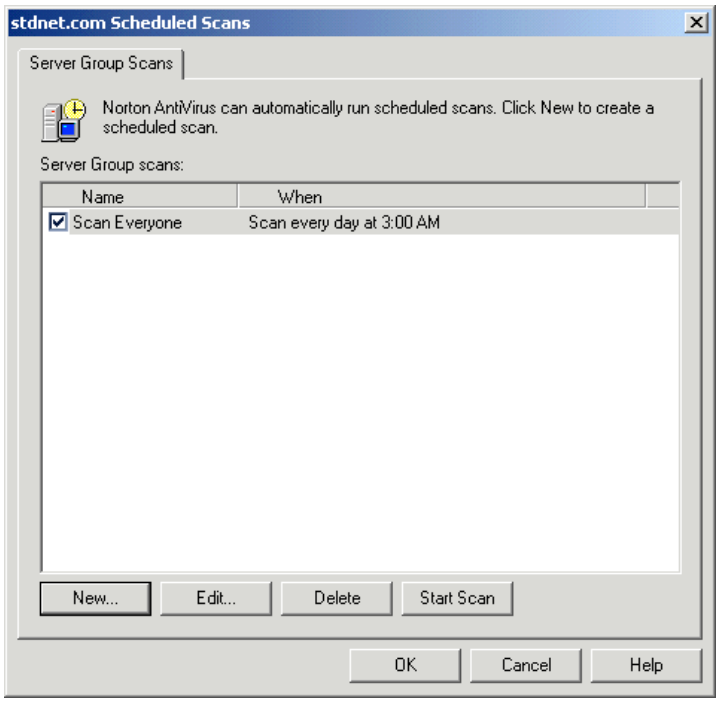
"Client" Checklist

The following checklist should be used against each unique server group and or individually configured machine.

Scheduled Scan is Active

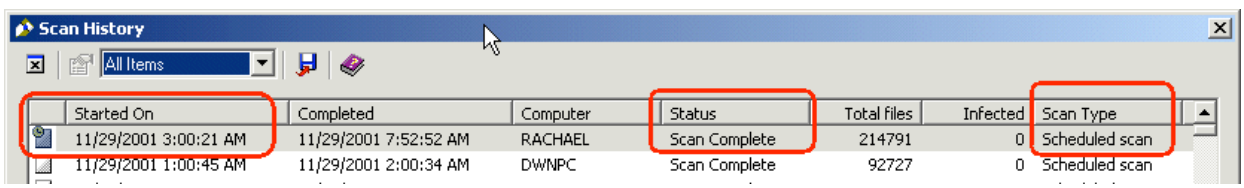
WEEKLY scheduled scans of the complete contents of hard drives are a good idea to find viruses "real time" checks have missed. Ideally these scans should be performed during "offhours" (non-business hours for most desktops and file servers) because these scans use up processing power and "churn" the hard drive while in action.

The following dialog box shows a properly scheduled scan. This dialog is available by selecting a server group (or individual machine, if you are auditing a specific configuration), right-clicking and selecting "AllTasks>NortonAntiVirus>ScheduledScans..."



Auditors should confirm that scheduled scans are actually being conducted by looking for matching entries in the Scan History log. (The Scan History log is available by selecting a server group, right clicking and selecting "AllTasks>Logs>ScanHistory")

Specifically, auditors should make sure scans took place at the proper time, completed without errors and were initiated by a "Scheduled Scan" (as opposed to a "Manual Scan").



Choices: (Select one of the following.)

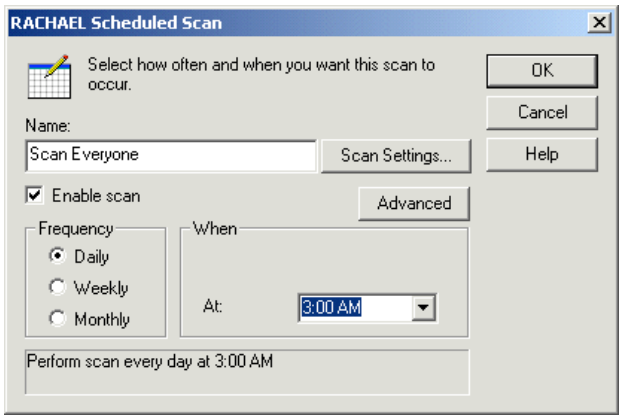
- PASS - Scan is run against all clients at least once a week.
- WARNING - Scan is run against all clients periodically or does not run against all clients.
- FAIL - Periodic scans are not run, infrequently run, or only run on a handful of machines.

(Objective Item - Should be documented with screenshots.)

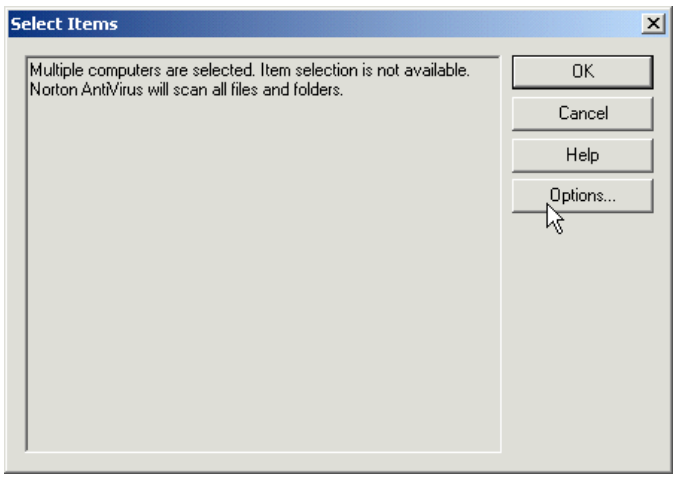
(*Back to Client Checklist*)

Scheduled Scan is Configured Properly

Auditors should click up (or "Edit...") scheduled entries and check their settings. The following dialog displays an entry being edited.



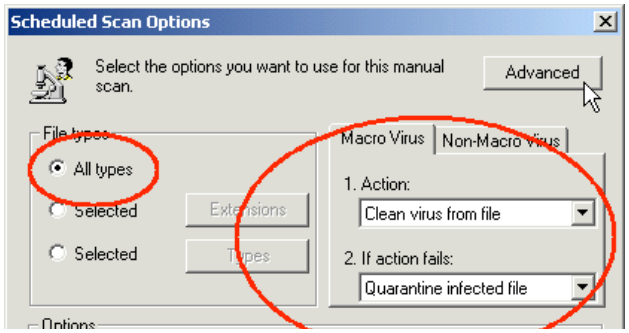
From this dialog, auditors should click the "Options..." button...

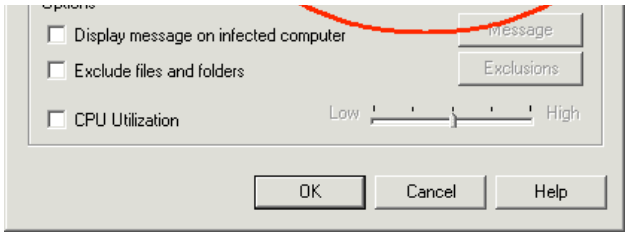


...and note the settings on the Scheduled Scan Options box. One entry to check here is found in the "File Types" box - make sure the "All Types" option is checked.

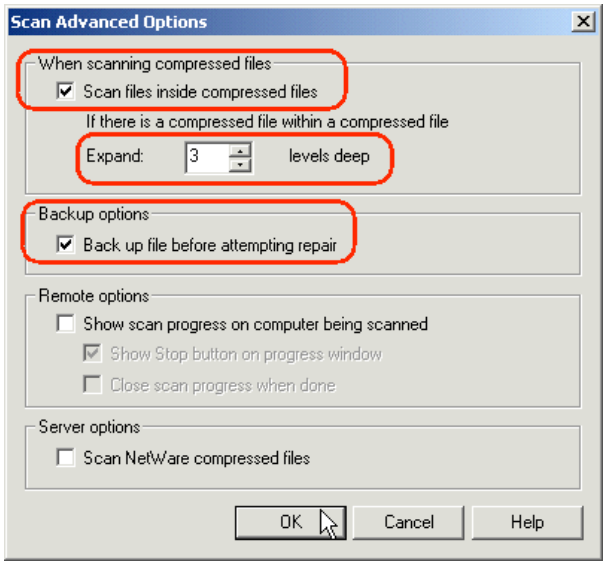
Also check the "Action" and "If Action Fails" option for BOTH Macro Viruses and Non-Macro Viruses. The "Action" should be EITHER "Clean virus from file" OR "Delete file". The "If Action Fails" should be EITHER "Quarantine infected file" OR "Delete file."

Finally, press the "Advanced" button for one more dialog.





In the "Scan Advanced Options" dialog, make sure compressed files ARE being scanned and that the scanner is looking at least 3 levels down into each compressed file for "hidden" viruses. For safety auditors should also check to see that "backup file before attempting repair" is checked.



Choices: (Select one of the following.)

- PASS - All options have been set correctly.
- WARNING - One or two options have been set incorrectly.
- FAIL - Three or more options have been set incorrectly.

(Objective Item - Should be documented with screenshots.)

(*Back to Client Checklist*)

Realtime Protection is Active

Modern virus protection depends on active clients deployed throughout an organization. Auditors may use the following procedure to spot-check clients throughout an organization. (At least two different clients and the primary server should probably be tested within any server group.)

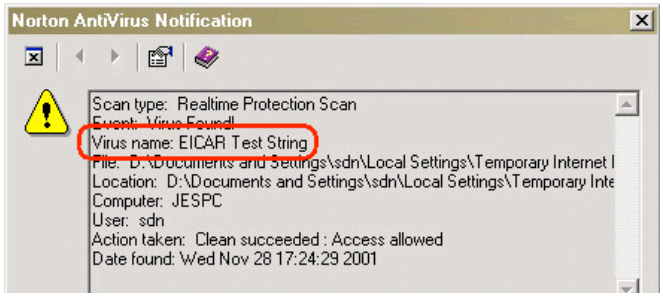
The following string is known as the EICAR test string. It will trip most virus signature engines but the string itself is harmless.

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

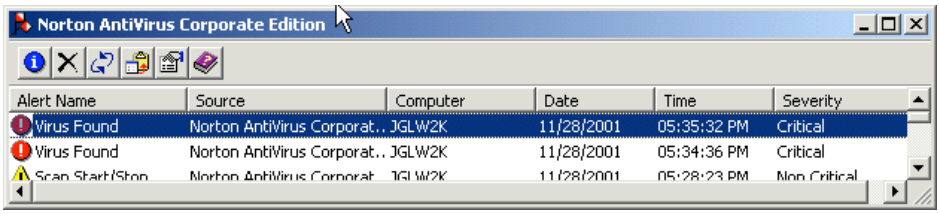
To test clients, auditors should perform one or both of the following tests:

- Save this string by itself in a text file named "eicar.com" to a client's hard drive.
- If an organizations' email clients integrate well with Norton and no email gateway is in place, an auditor may send this string as both the SUBJECT and BODY of a regular email to people working on machines which should have active clients. (The auditor may have to use a non-integrated email client like Eudora or even telnet over port 25 to send the string.)

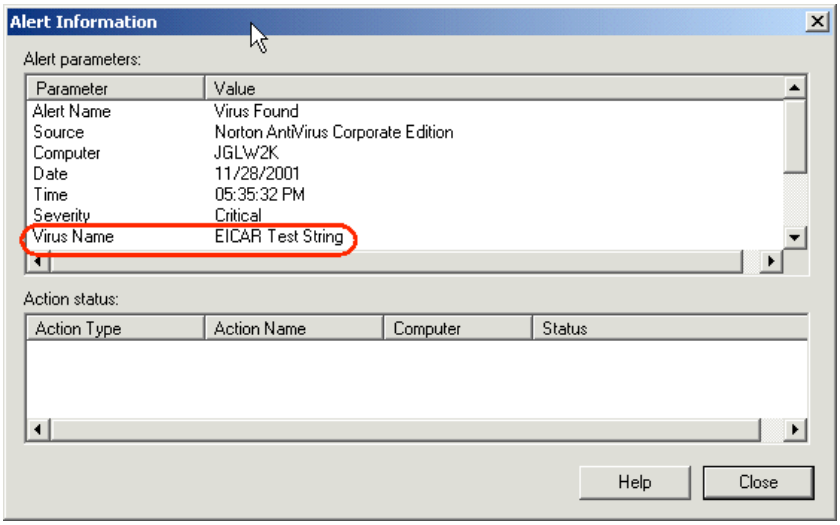
If the client detects a virus, the user will most likely see the following message box pop up on his or her screen. (Note the use of "Virus name: EICAR Test String" indicates this is a harmless "virus"!)



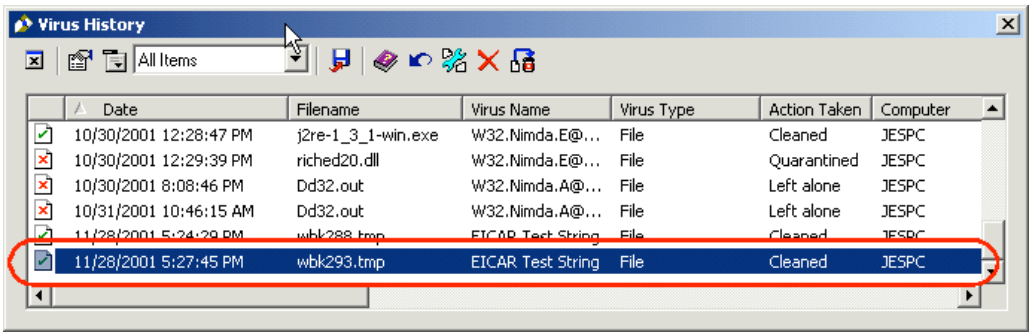
Auditors will want to confirm the detection in their logs. (Remember, logs are stored for each server group!) The following log view is (normally) available from the AMS Log within any selected server group.



Entries can be "clicked up"; clicking up the first entry shows that it is indeed a successful detect of the harmless EICAR string.



(Another way to verify detects: right-click the "infected" machine and select "AllTasks>Logs>VirusHistory..." The following dialog will show a list of viruses found.)



Choices: (Select one of the following.)

- PASS - All clients tested detected and logged test strings.
- WARNING - Almost all clients (i.e. 95%) detected and logged test strings.
- FAIL - Several clients missed test strings or failed to log them.

(Objective Item - Should be documented with a worksheet listing each client tested (by server group) and whether or not it picked up the test signatures.)

(Back to Client Checklist)

Server Realtime Protection is Configured Properly

Realtime Protection provides the first line of defense against viruses in most organizations by flagging and disabling known viruses. Norton allows different settings for servers and clients within the same server group; this section covers the servers.

The Realtime Protection configuration dialog may be accessed by right-clicking a server group and selecting "AllTasks>NortonAntivirus>ServerRealtimeProtectionOptions".

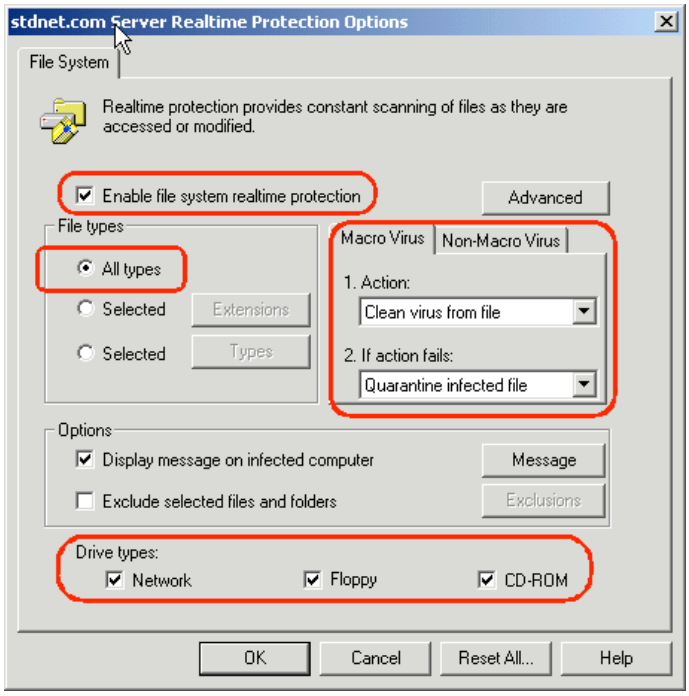
The most important option which should be checked is "Enable file system realtime protection."

All file types should be included in the scan unless there is a COMPELLING reason not to scan certain files. (For example, ".xyz" files may encrypted using AES - the scanner can do nothing against them and may actually yield false-positives against the random strings in the encrypted file. Alternatively, ".xyz" files may be your private stash of test viruses if you are an security company - you already know they are viral and do not want the scanner to wax them.)

Also check the "Action" and "If Action Fails" option for BOTH Macro Viruses and Non-Macro Viruses. The "Action" should be EITHER "Clean virus from file" OR "Delete file". The "If Action Fails" should be EITHER "Quarantine infected file" OR "Delete file."

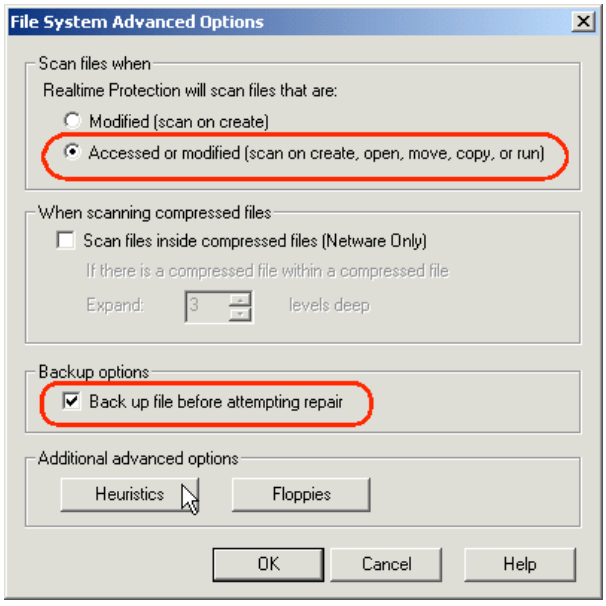
Finally, check that ALL THREE drive types are checked. (Checking network drives is a good second line of defense against viruses on what should be already protected servers. Checking CD-ROMs is becoming increasingly more important as CDRs continue to grow in popularity.)

Press the "Advanced" button for more options.

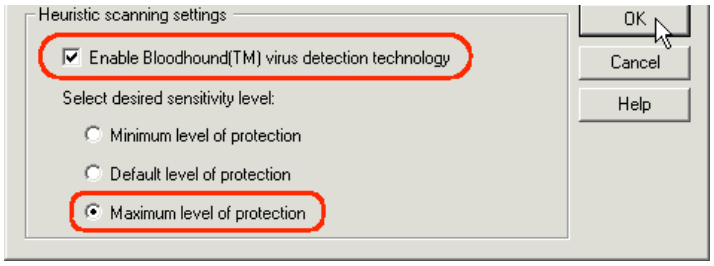


On the "File System Advanced Options" dialog, make sure files are scanned when "Accessed or modified" and that the client will "Back up file before attempting repair."

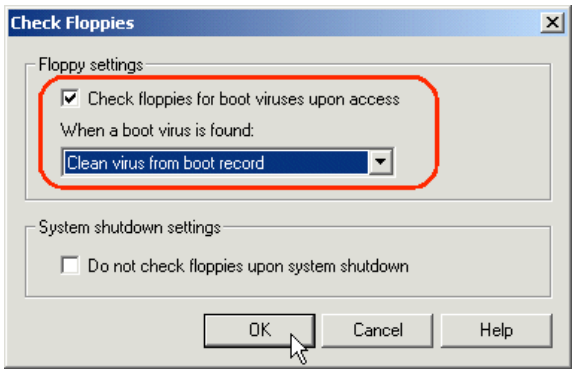
Check the "Heuristics" and "Floppies" buttons for even more options.



On the "Heuristic Scanning Options" dialog, make sure "Bloodhound" is enabled and set to the "Maximum level". (NOTE - Bloodhound uses an engine which attempts to detect "virus-like" behavor rather than the usual virus signatures. Some sites may find this engine imcompatible with existing applications and may have a compelling reason to disable this feature or set its "protection level" to a lower value.)



On the "Check Floppies" dialog, make sure floppies are checked "upon access" and that boot viruses are cleaned.



Choices: (Select one of the following.)

- PASS - All options have been set correctly.
- WARNING - One or two options have been set incorrectly.
- FAIL - Three or more options have been set incorrectly.

(Objective Item - Should be documented with screenshots.)

(*Back to Client Checklist*)

Client Realtime Protection is Configured Properly

Realtime Protection provides the first line of defense against viruses in most organizations by flagging and disabling known viruses. Norton allows different settings for servers and clients within the same server group; this section covers the clients.

The Realtime Protection configuration dialog may be accessed by right-clicking a server group and selecting "AllTasks>NortonAntivirus>ClientRealtimeProtectionOptions".

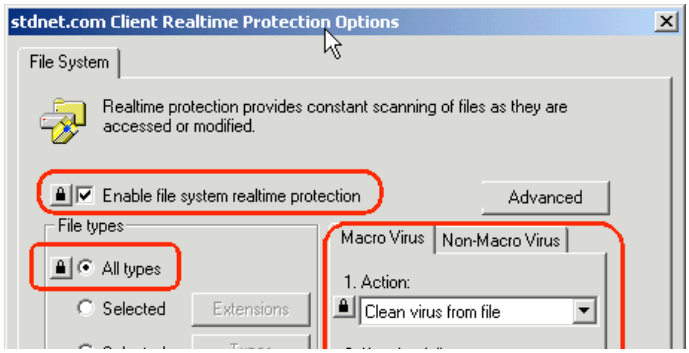
The most important option which should be checked is "Enable file system realtime protection." All important options should also be LOCKED so end users cannot change settings which would decrease the effectiveness of the virus protection. (locked=🔒, unlocked=🔓)

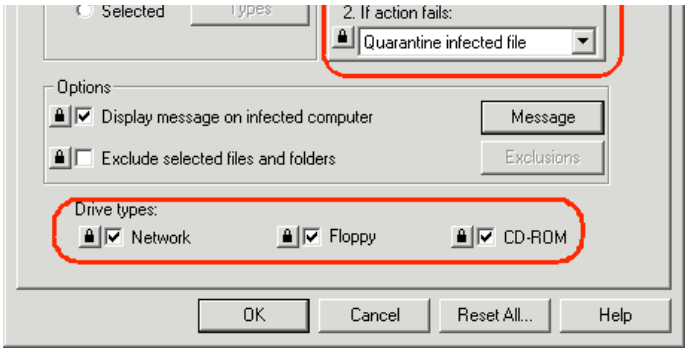
All file types should be included in the scan unless there is a COMPELLING reason not to scan certain files. (For example, ".xyz" files may encrypted using AES - the scanner can do nothing against them and may actually yield false-positives against the random strings in the encrypted file. Alternatively, ".xyz" files may be your private stash of test viruses if you are an security company - you already know they are viral and do not want the scanner to wax them.)

Also check the "Action" and "If Action Fails" option for BOTH Macro Viruses and Non-Macro Viruses. The "Action" should be EITHER "Clean virus from file" OR "Delete file". The "If Action Fails" should be EITHER "Quarantine infected file" OR "Delete file."

Finally, check that ALL THREE drive types are checked. (Checking network drives is a good second line of defense against viruses on what should be already protected servers. Checking CD-ROMs is becoming increasingly more important as CDRs continue to grow in popularity.)

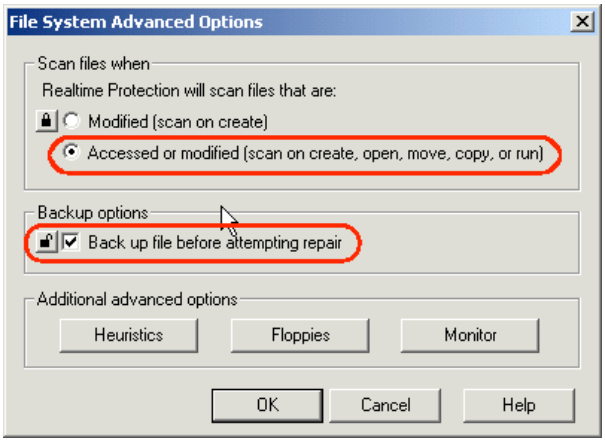
Press the "Advanced" button for more options.



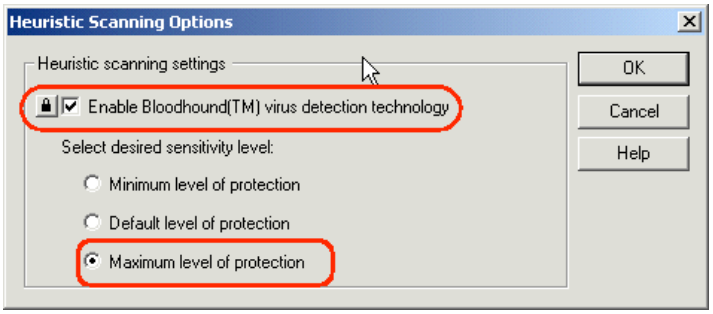


On the "File System Advanced Options" dialog, make sure files are scanned when "Accessed or modified" and that the client will "Back up file before attempting repair."

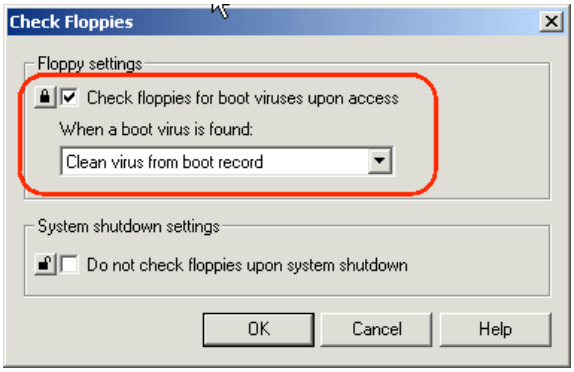
Check the "Heuristics," "Floppies" and "Monitor" buttons for even more options.



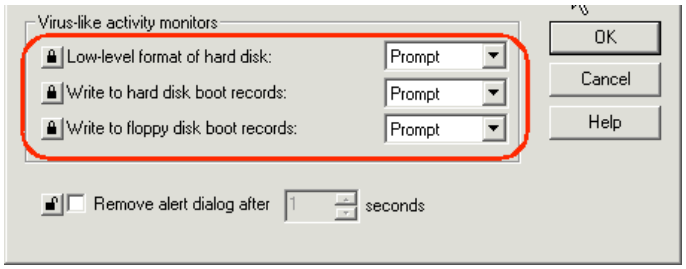
On the "Heuristic Scanning Options" dialog, make sure "Bloodhound" is enabled and set to the "Maximum level". (NOTE - Bloodhound uses an engine which attempts to detect "virus-like" behavor rather than the usual virus signatures. Some sites may find this engine imcompatible with existing applications and may have a compelling reason to disable this feature or set its "protection level" to a lower value.)



On the "Check Floppies" dialog, make sure floppies are checked "upon access" and that boot viruses are cleaned.



On the "Virus-like Activity Option" (pops up when the "Monitor" button is presses) make sure the user is prompted to confirm all three kinds of dangerous behavior. Alternatively, values of "Don't Allow" for both "Low-level format of hard disk" and "Write to hard disk boot records" are legal. (Setting a value of "Don't Allow" to the "Write to floppy disk boot records" is likely to interfere with floppy disk formats.)



Choices: (Select one of the following.)

- PASS - All options have been set correctly.
- WARNING - One or two options have been set incorrectly.
- FAIL - Three or more options have been set incorrectly.

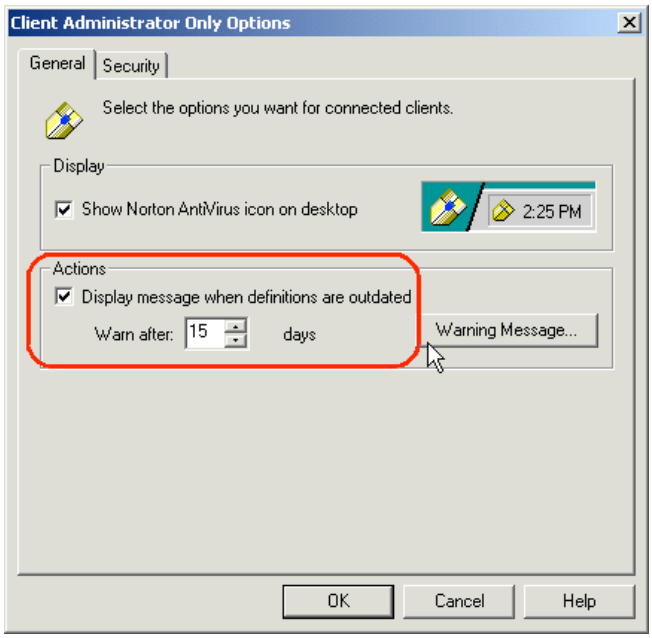
(Objective Item - Should be documented with screenshots.)

(Back to Client Checklist)

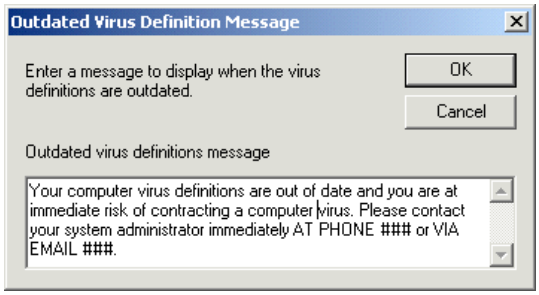
Client "Administrator-Only" Options are Configured Properly

Symantec's "Administrator-Only" options provide a catch-all space for a variety of miscellaneous security options. The following dialog may be accessed by right-clicking any server group and selecting "AllTasks>NortonAntivirus>ClientAdminstratorOnlyOptions..."

A warning message should be displayed to end users when definitions are out of date. The default time is probably too long (90 days?) but a time of 1 or 2 days is too short. A compromise value is one in the range of 7-21 days (1-3 weeks). Also click up the "Warning Message"...



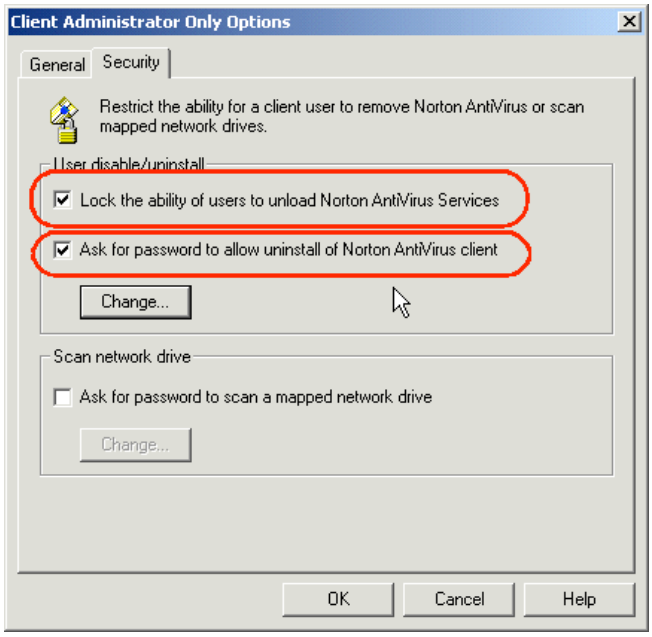
...and make sure end users are provided with the contact information of someone who can address their problem.



On the "Security" tab there are two related options which should be checked. The first prevents end users from shutting down virus protection. The second prevents them from uninstalling virus protection.

One hole which exists here however: end users MAY uninstall virus protection if they can guess a single password. (By default, this password is "symantec" - this fact is documented in the help file!) To confirm that use of the default password is not negating uninstall protection, auditors should attempt the following procedure from a client machine within each server group.

1. From the client PC, try to uninstall virus protection
2. If the auditor is not challenged, FAIL this section
3. If the auditor is challenged but is allowed to uninstall after typing "symantec", also FAIL this section



Choices: (Select one of the following.)

- PASS - All options have been set correctly and outdated definition message provides contact information.
- WARNING - All options have been set correctly but outdated definition message does not provide contact information.
- FAIL - One or more options have been set incorrectly.

(Objective Item - Should be documented with screenshots and results of uninstall test.)

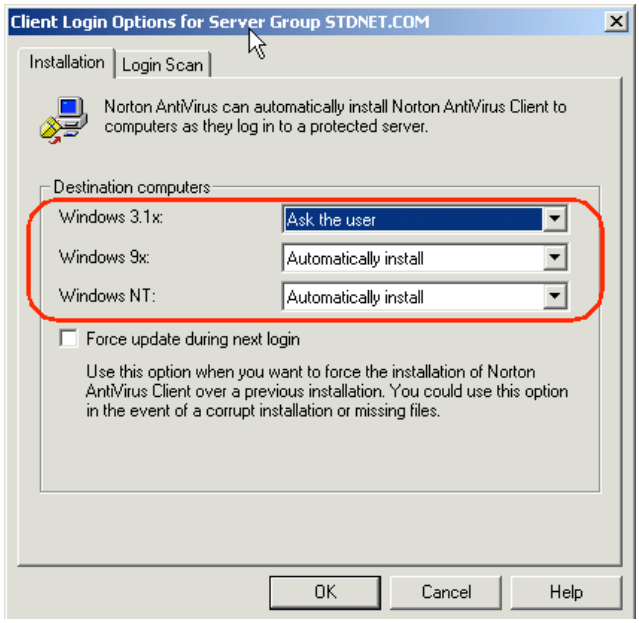
(*Back to Client Checklist*)

Client "Login" Options are Configured Properly

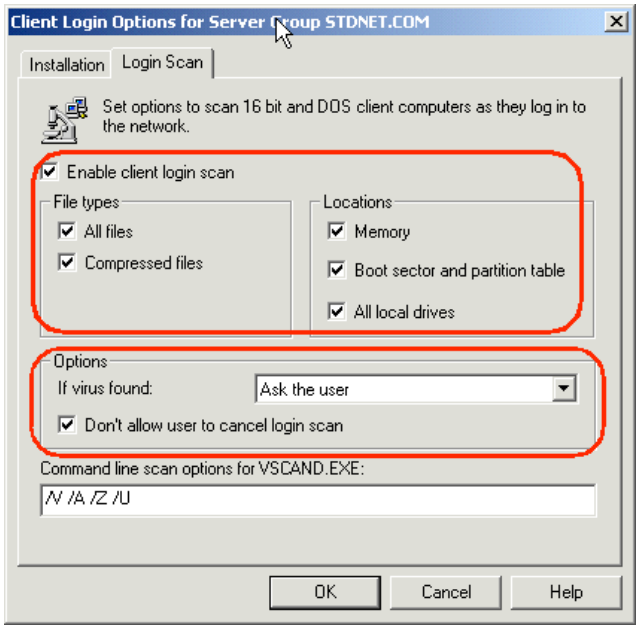
Login Options provide a second level of protection against machines which threaten a group of computers because those machines have no virus protection. Unfortunately the automatic installation of virus protection software may not be possible in environments which are very sensitive to client installs (i.e. shops which mostly live off of "ghosted" images) or network traffic spikes during certain times of the day.

The following dialog may be accessed by right-clicking any server group and selecting "AllTasks>NortonAntivirus>ClientLoginScanAndInstallation"

Automatic installs on Windows 9x and NT (etc.) are very useful. Automatic installs on Windows 3.1x should probably be prompted because there is a good chance any remaining Windows 3.1x platforms still use Windows 3.1x because their key applications are too sensitive to be run on anything newer and an automatic push COULD break something vital on these machines.



The "Login Scan" tab has a variety of options for 16-bit and DOS clients. Some enabled combination of MOST of these elements should probably be implemented, but certain elements may not be appropriate for all environments.



Choices: (Select one of the following.)

- PASS - All options have been set well for this environment.
- WARNING - Almost all options have been set well for this environment.
- FAIL - No enough options have been set well for this environment.

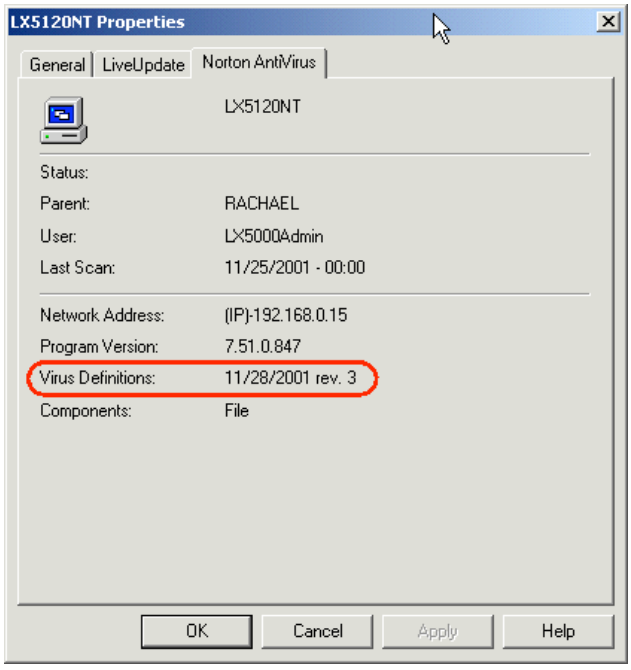
(Subjective Item - This section has many "depends on your installation" qualifications and cannot be completed without at least a brief interview with local system administrators. - Should be documented with screenshots and results of uninstall test.)

(Back to Client Checklist)

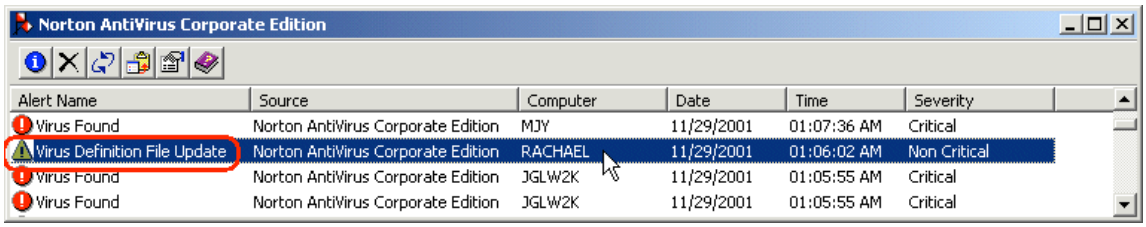
Clients are Obtaining Latest Signature Files

If the server has been correctly configured, clients should faithfully download new signatures from the central server. There are no further configuration options to consider, but auditors should check the logs of various clients to verify that they are in fact receiving the proper updates.

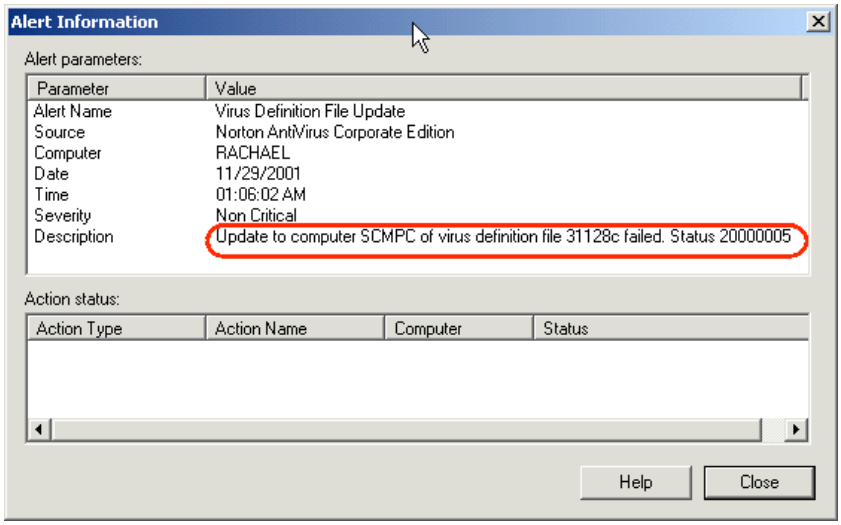
One fast way to check individual clients is to right-click a CLIENT and select "Properties". Then select the "Norton AntiVirus" tab and make sure the "Virus Definitions:" date and version number match those of the server's definitions.



Finally, auditors should pull up the virus definition update "exception log" available through the "AMS Log" facility. This log is accessible by right-clicking the SERVER GROUP and selecting "AllTasks>ViewAMSLog". Auditors should look for "Virus Definition File Update" entries white note FAILED updates. Healthy systems will have few if any of these entries; unhealthy systems will have many of these entries.



Note that a single failed entry will list the name of the computer which failed to get its signatures in the DESCRIPTION field, not the computer field!



Choices: (Select one of the following.)

- PASS - All clients are regularly getting the latest signature files.
- WARNING - Most clients are regularly getting the latest signature files.
- FAIL - Several clients are not regularly getting the latest signature files.

(Objective Item - Should be documented with screenshots. However, an argument for subjectivity could be made with regards to the "few or many" analysis of the log files.)

(Back to Client Checklist)

"Server" Checklist

The following checklist should be used against each server group.

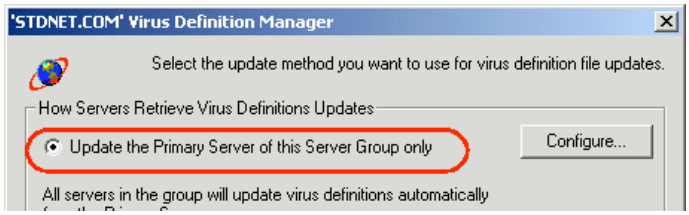
Server is Obtaining Latest Signature Files

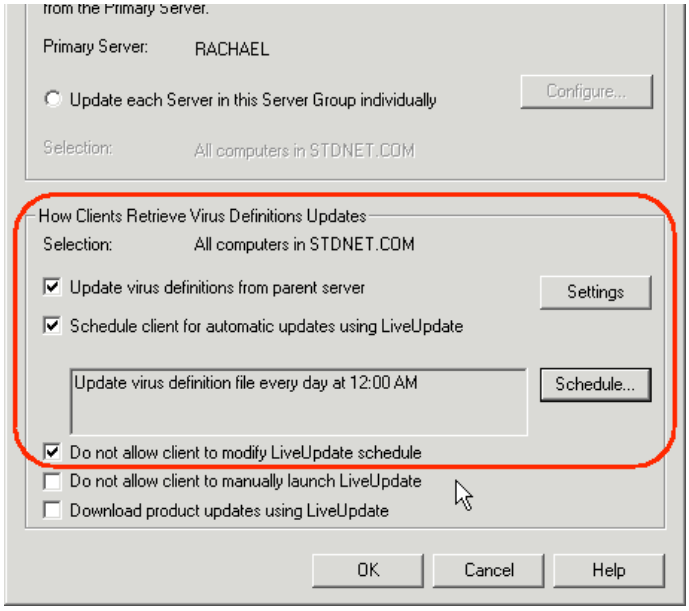
Servers should be obtaining virus definitions from Symantec or some master primary server which itself obtains virus definitions from Symantec. The following information assumes servers are obtaining signatures from Symantec.

The following dialog may be accessed by right-clicking any server group and selecting "AllTasks>NortonAntivirus>VirusDefinitionManager..."

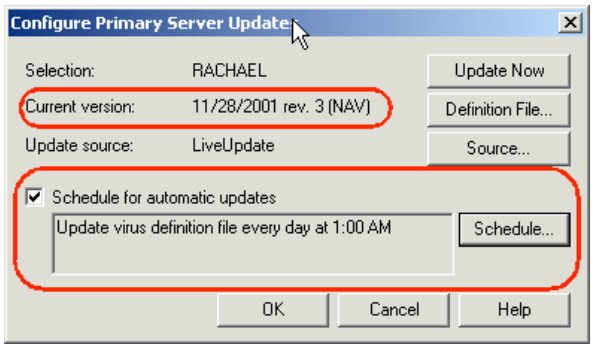
Updates should be pulled to the Primary Server in the server group unless there is a compelling reason to do otherwise. (i.e. large, distributed network where remote servers enjoy better connectivity to the Internet than to the "home office")

Clients should retrieve virus definitions from their parent servers. All clients should check at least once a day; the time between checks is configurable as network conditions warrant. Clients should use LiveUpdate and should not be allowed to modify the schedule. (However clients may be allowed to launch LiveUpdate to initiate immediate transfer of signatures.)



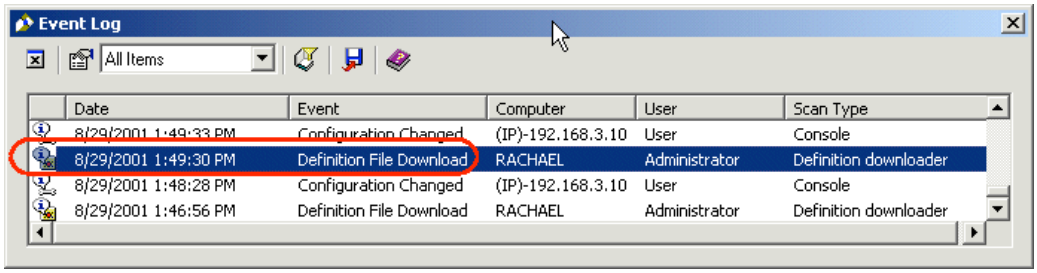


Press the "Configure" button to see more settings. Make sure the "Current Version" is a recent version (generally it is less than a week old) and that DAILY checks for fresh updates are scheduled.



To make sure server virus definition updates are actually occuring, auditors should check the server group event log. This log is available by right-clicking any server group and selecting "AllTasks>Logs>EventLogs..."

Server definition file updates will appear as "Definition File Download" entries in the log.



Choices: (Select one of the following.)

- PASS - All options have been set correctly, server has very recent version of virus definitions and regularly obtains new versions without problems.
- WARNING - All options have been set correctly, but server does not have very recent version of virus definitions (older than a week, less than a month) and/or regularly fails to obtain new versions.
- FAIL - One or more options have been set incorrectly or server has older version of virus definitions (more than a month).

(Objective Item - Should be documented with screenshots.)

(Back to Server Checklist)

Server is Protected Against Unauthorized Configurations

Norton installs a rather large security hole with its latest versions. According to a recent report posted on SecurityTracker.com, the all-important GRC.DAT server-group configuration file is left on an unprotected share ("Everyone:Full Control") which anyone in the domain can access. Smart users could very easily disable or make changes to an organzation's virus protection settings by changing the contents of GRC.DAT.

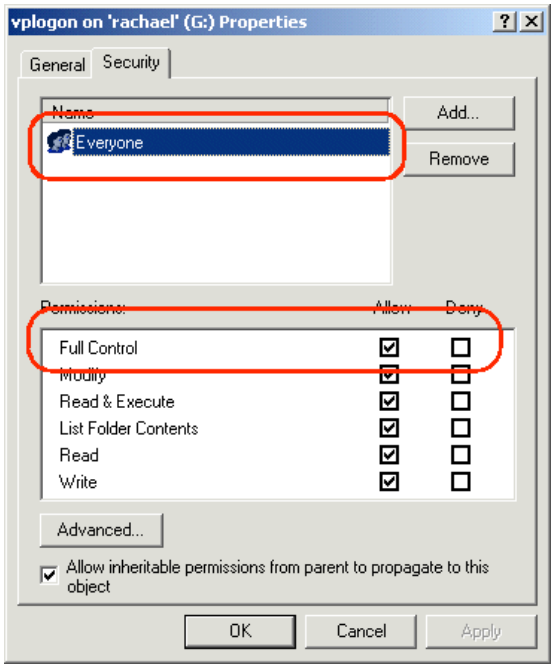
"Norton AntiVirus Corporate Edition Lets Local and Remote Users Change Anti-Virus Configuration," SecurityTracker.com. November 23, 2001. (http://www.securitytracker.com/alerts/2001/Nov/1002814.html)

Auditors can use a short procedure to test for this vulnerability. Go to a client PC (one where the user is not signed on as an administrator!), open a command window and type the following commands, substituting the name of a primary server for "rachael" where appropriate.

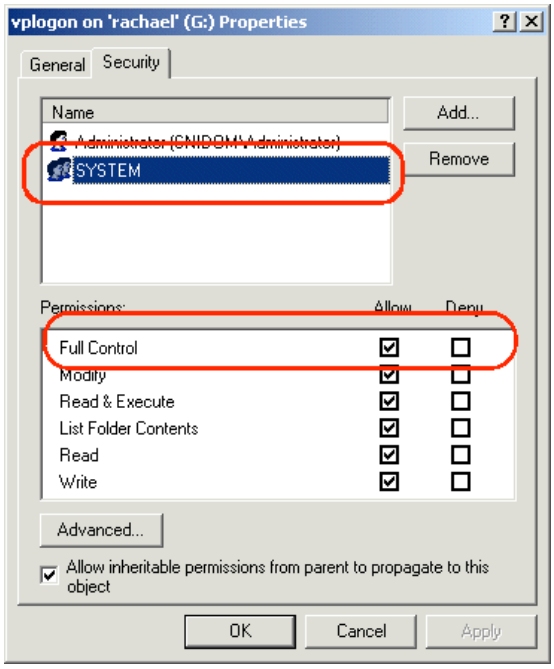
```
C:\>net use g: \\rachael\vplogon
The command completed successfully.

C:\>echo helloworld > g:\frog.txt

C:\>type g:\frog.txt
helloworld
```

The first command connects a drive letter to the exposed share. The second attempts to write a file to it as proof of WRITE privileges. The third attempts to read the brand new file back as proof of READ privileges.

With a mapped drive attached to the share, an auditor can pop up that drive's properties and examine the "Security" tab. Notice the "Everyone" group enjoys FULL CONTROL.



To address this problem it is advised administrators allow only the built-in SYSTEM account and *maybe* an administrative account/group FULL CONTROL on this folder. (The Everyone group should be removed!) When secured properly, not only will the second and third test commands fail from a test PC, but the folder security properties will appear quite different as well.



Choices: (Select one of the following.)

- PASS - Servers has protected share.
- FAIL - Server has unprotected share.

(Objective item - Should be documented with output from DOS commands above.)

(Back to Server Checklist)

Server is Properly Backed Up

Other than the issue regarding the unprotected share, this section is the only section which deals with something normally left to operating system audits. Are the servers being properly backed up? (Note: Backup software should also back up registry.)

Choices: (Select one of the following.)

- PASS - Server is backed up daily. Backup process and media have been tested (partial write back to disk).
- WARNING - Server is backed up weekly. Backup process and media have not been tested.
- FAIL - Server is not backed up regularly.

(Objective item - Should be documented with backup logs.)

(Back to Server Checklist)

(End of Checklists - End of Assignment 1)

GSNA Assignment 2 - Application of Audit Techniques to a Real World System

Identify the Item to Be Audited

I am auditing the Norton Antivirus Enterprise Edition 7.5 system at a small credit union. This system provides virus protection to desktops and file servers throughout the organization. This system has no additional antivirus "gateway" for email or other specialized vectors.

(As part of identifying the "item" to be audited, this step is an appropriate time to conduct the "before the audit" portion described in Assignment 1.)

Complete List of Authorized Administrators and Workstations from which Console Operations are Allowed

- Administrators: Sally, Larry
- Workstations: Sally's Desktop, Larry's Desktop, Primary Server ("NORTON")

Server Group Documentation Detailing Purpose of Group, Adminstrator(s) Responsible for Group and Important Servers (primary, secondary and parent) within the Group

- Internal Group: All Machines in Internal Network.. Admins: Sally, Larry. Key Servers: NORTON (Primary)
- Internet Group: All Machines in "DMZ". Admins: Sally, Larry. Key Servers: MAILMAN (Primary)

Approximate Total Number of Clients Protected and Clients per Server Group

- Internal Group: 33 Clients
- Internet Group: 2 Clients
- Total Clients: 35 Clients

How are servers grouped?

- Resources have been placed in security groups; resources accessible from the Internet all share a single configuration and resources on in the internal segments all share a single configuration.

Are servers grouped in an appropriate way?

- Internal group may benefit from the designation of a secondary server or two.
- Internet group has a primary server on the DMZ segment itself. Credit union should be aware of tradeoffs of this server's position, but otherwise this configuration is also fine. (i.e. Primary server stands a higher chance of being hacked, but no "holes" in the firewall are required to support this configuration other than support for a connection to Symantec for virus updates/quarantine communication and a connection from the inside to manage the server.)

Are changes applied to server groups or individual clients?

- Changes are applied to groups only.

If changes are applied to individual clients, do additional controls exist to ensure changes conform to a set standard?

- Changes are not applied to individual clients.

Based on this "before the audit" information, we can determine the following checklist work will need to be performed to evaluate this system:

- 1 Global Checklist
- 2 Client Checklists (1 for Internal, 1 for Internet)
- 2 Server Checklists (1 for Internal, 1 for Internet)

Evaluate the Risk to the System

This system is probably less at risk to internal mischief than larger shops. (Fewer non-security IT personell may mean less chance of people disabling virus protection "to speed [an application] up".) However the installation of Norton in this particular site is a relatively recent event and the two people in the IT shop may either be inexperienced with Norton and/or watching a central anti-virus server rather than waiting to hear from irate users.

The Internet server group is an unusual group. If the Credit Union's firewall is configured properly there is a limited set of vectors through which viruses may infect the protected devices (mainly through the "approved" protocols of HTTP and SMTP) and a limited number of ways they may pass viruses onto other machines. (Outbound connections to random IP addesses are not permitted.) However Symantec may require more ports to be open between these boxes and internal machines than we would normally feel comfortable with for management purposes. A few settings may have to be loosened up on the firewall or the Symantec system itself to make this arrangement work.

Probably the greatest procedural risk to the system in this environment is the possible lack of change control in a two-person IT shop. I will try to pay special attention to client configurations to make sure one sysadmin or the other is not making client changes instead of server group changes.

Conduct the Audit

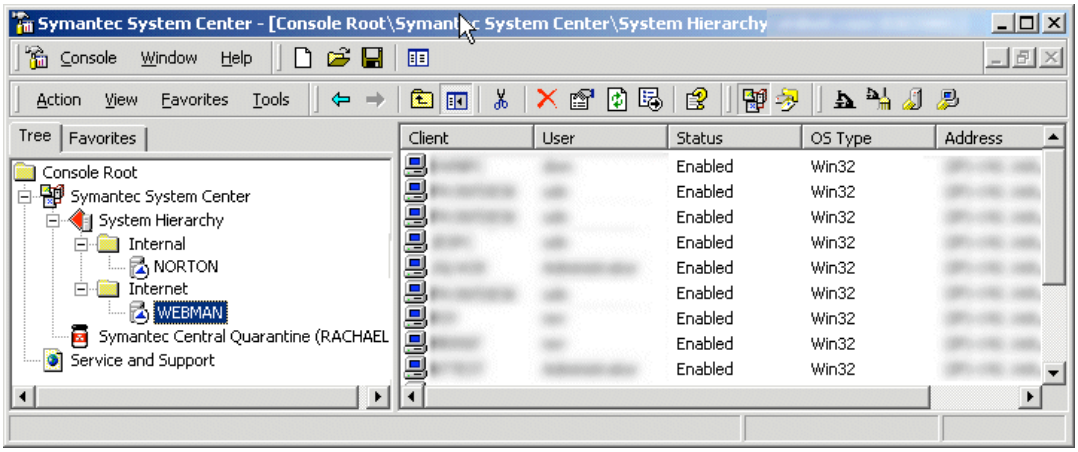
An audit using THREE of the FIVE checklists described above follows. (I omitted both "Internet" checklists for the sake of brevity in this report. A complete "real-world" audit would of course need to include these.)

Global Checklist

Item	Pass/Warning/Fail
Server-Groups Locked When Not In Use	**FAIL**
Server-Group Passwords are Strong and Unique	**PASS**
Administrative Saved-Passwords/Consoles are Secure	**PASS**
Administrators are Aware of Virus Attacks	**PASS**
Administrators React Properly to Virus Attacks	**WARNING**
Quarantine is Enabled	**PASS**
Quarantine-Symantec Communication is Secure	**PASS**
Quarantine-Symantec Submissions are Depersonalized	**PASS**
Quarantine-Symantec Contact is Provided	**PASS**
Quarantine-Symantec Patches are Auto-Installed	**FAIL**

Server-Groups Locked When Not In Use - FAIL

Both groups were left unlocked. The following screenshot taken when the console was first open shows both groups open and available when the System Hierachy is first expanded.



Server-Group Passwords are Strong and Unique - PASS

Sally provided me with passwords to both groups. Both were fairly strong (8 and 9 characters, a mix of letters and numbers, no dictionary words, names, etc.). I locked both groups and opened them again with the passwords Sally provided me to verify that those passwords were in fact the real administrative passwords.

Administrative Saved-Passwords/Consoles are Secure - PASS

Sally noted that administrators do not save their passwords on their console machines. Because there were only three console machines to choose from (Sally's desktop, Larry's desktop and NORTON) I was quickly able to verify this statement; I was challenged for a password for both server groups from all three locations.

Administrators are Aware of Virus Attacks - PASS

I conducted short interviews with both administrators to gauge their familiarity with the Norton system.

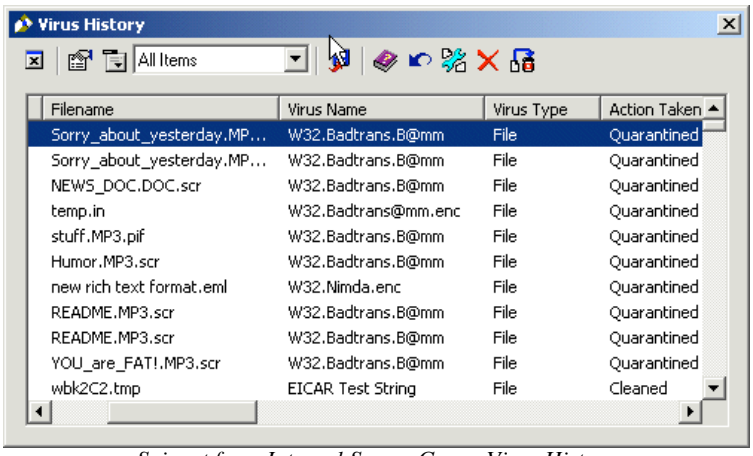
Sally provided the following answers to the following questions.

- *What are the top three viruses in your system right now?* BadTrans, Nimda, Stages
- *What (server) group typically picks up the most viruses?* Internal
- *What are the top three virus vectors into you system?* Email, Shareware, Floppies?

Larry provided the following answers to the following questions.

- *What are the top three viruses in your system right now?* BadTrans, Nimda?
- *What (server) group typically picks up the most viruses?* Internal
- *What are the top three virus vectors into you system?* Email, Shareware, Floppies?

I pulled up the Virus Histories for both the Internal and Internet server groups and noted that "BadTrans" was indeed the number one virus in the system and that "Nimda" was a distant second. (A few "Stages" hits were also found earlier in the logs.) In addition, the bulk of all hits came from the Internal server group.



Snippet from Internal Server Group Virus History

A random drop of EICAR strings via floppy disk to various teller machines was also noticed by Sally "upstairs"

Finally, at no time did I ever see more than four "infected" machines on the console - another good sign that the administrators were paying attention.

All of this information seemed to support the idea that administrators were actively watching their network, although Sally may be the stronger administrator.

Administrators React Properly to Virus Attacks - WARNING

The WARNING given in this section mostly had to do with the administrators' unfamiliarity with the the quarantine system. (Both administrators provided good answers to test questions and had the authority to isolate machines and or networks.)

Sally provided the following answers to the following questions:

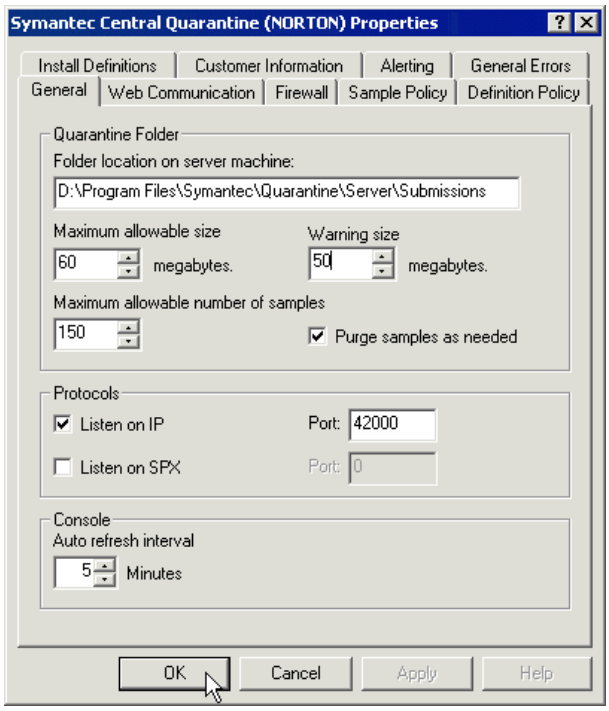
- *What do you do when you see that a box is infected?* "I pull up the (client) virus history and see what they got...if the virus is still there I call the user and tell them to power down the machine until I arrive (to unplug and clean it)."
- *How do you tell if a virus is propogating through your network?* "If I see a number of machines light up (turn red) and when I check the logs I see the same virus has hit most of them."
- *What kind of credentials do you use to sign onto the Quarantine system?* "NT username/password"
- *Name three attributes retained in the Quarantine system besides the infected file itself.* (Didn't know)
- *What do you say to a user who just called to report a virus?* "I ask them what they were doing when they got the message, such as opening an email, what program they ran. Then I ask them to read me the message on their screen or check the logs to see if they are okay or not ...if they opened an attachment or did something I don't want them to do I generally give them a lecture".

Larry provided the following answers to the following questions:

- *What do you do when you see that a box is infected?* "I check the logs (virus history) and see if (Norton) got it or not. If it didn't I contact the user and have them turn off their machine until I get there."
- *How do you tell if a virus is propogating through your network?* "If the same virus hits different machines. ...checking the logs on various 'red' machines."
- *What kind of credentials do you use to sign onto the Quarantine system?* (Didn't know)
- *Name three attributes retained in the Quarantine system besides the infected file itself.* (Didn't know)
- *What do you say to a user who just called to report a virus?* "I have them tell me what the message says and what they were doing when it popped up. Since they often call after they close the message, I often have to go to the logs... If they are okay I generally don't pursue it much further except to point out that they shouldn't be opening attachments or doing joke lists if it's obvious".

Quarantine is Enabled - Pass

The Central Quarantine server was enabled and listening. I noticed that it was listening on (TCP) port 42000 on NORTON by clicking up the Central Quarantine server properties.

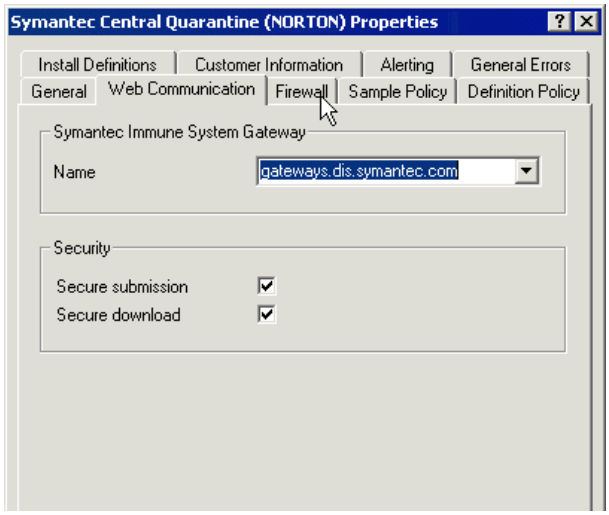


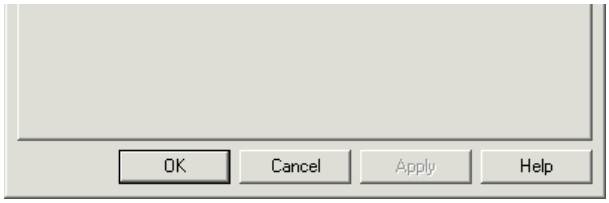
I also saw several recent entries in the quarantine file list from various machines in the network indicating the server really was listening and receiving virus submissions.

- Listen on IP: CHECKED
- Port: 42000

Quarantine-Symantec Communication is Secure - Pass

Communications between the Quarantine server and Symantec were configured to be secure. If I had serious doubts about the veracity of this claim I probably could have applied a sniffer and waited for a new virus to come along, but otherwise this is a very hard item to test.

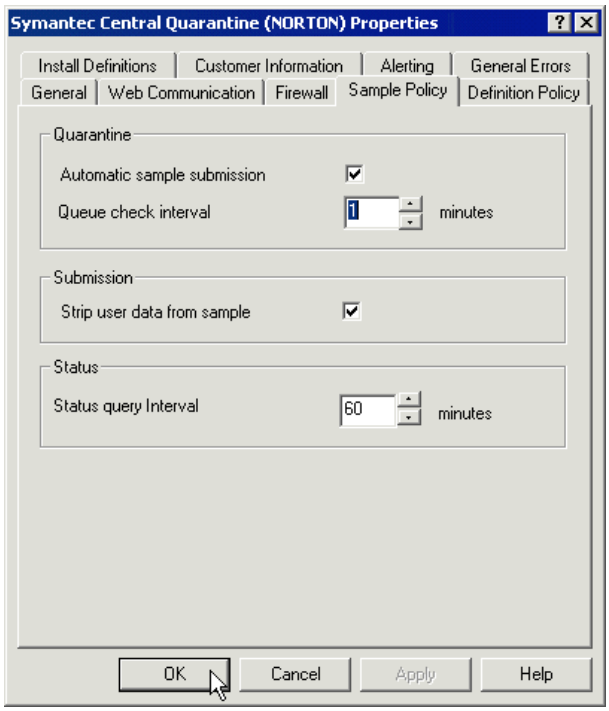




- Secure submission: CHECKED
- Secure download: CHECKED

Quarantine-Symantec Submissions are Depersonalized - Pass

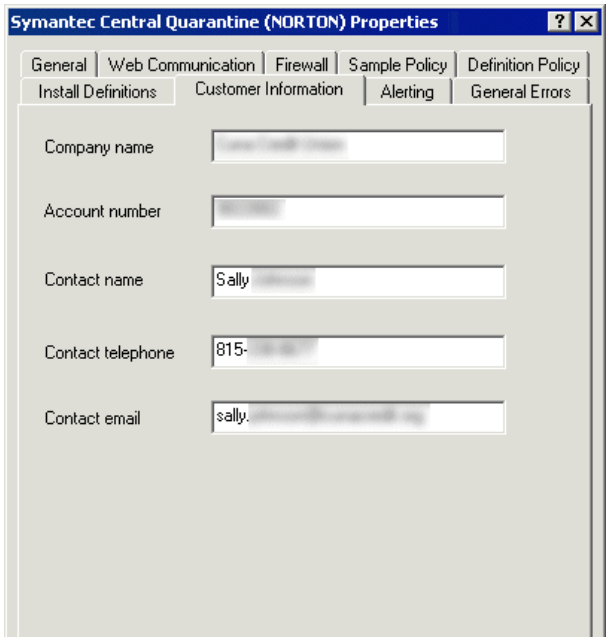
User data should be stripped from submissions to Symantec. Testing this one would be even more difficult than testing secure communications; you would need to invent a new virus, get it to infect a file with known customer information and see if that information was stripped out before it was sent to Symantec.

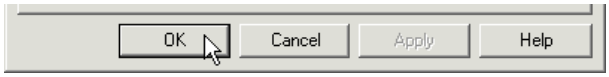


- Strip User Data from Sample: CHECKED

Quarantine-Symantec Contact is Provided - Pass

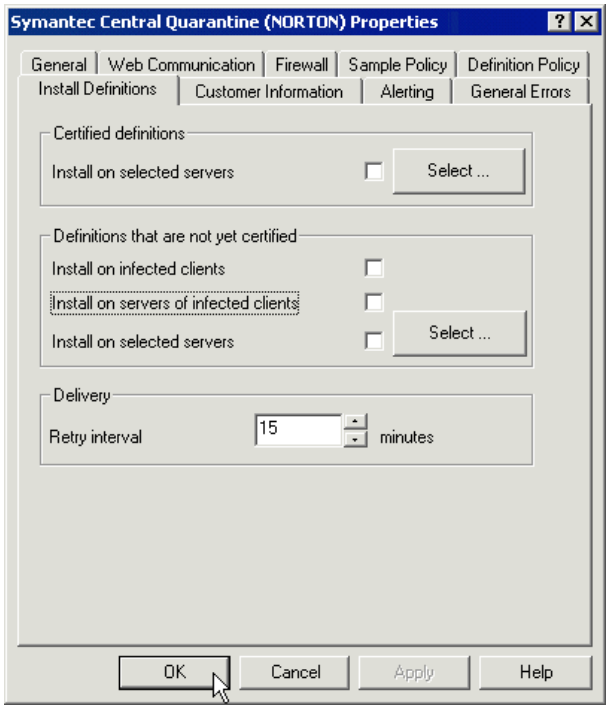
Specific information to contact Sally has been provided.





Quarantine-Symantec Patches are Auto-Installed - Fail

Sally and Larry did not know what the "Install Definitions" settings were for so they disabled everything they could find. Disabling these settings obviously meant that their organization would not enjoy any projection from interim patches Symantec may devise to disable new viruses discovered in their system.



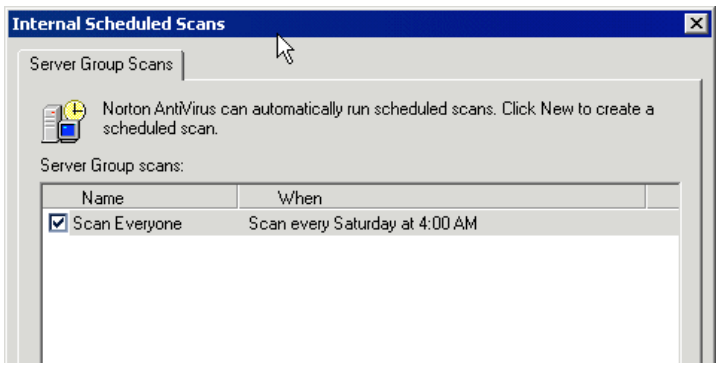
- Definitions that are not yet certified:
  Install on infected clients: UNCHECKED
  Install on servers of infected clients: UNCHECKED

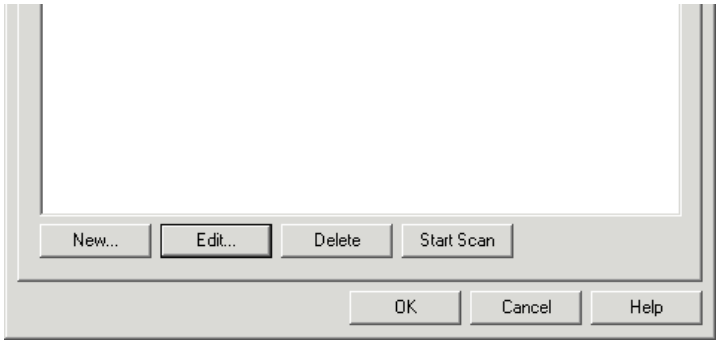
Client Checklist - Internal Server Group

Item	Pass/Warning/Fail
Scheduled Scan is Active	PASS
Scheduled Scan is Configured Properly	PASS
Realtime Protection is Active	PASS
Server Realtime Protection is Configured Properly	WARNING
Client Realtime Protection is Configured Properly	FAIL
Client "Administrator-Only" Options are Configured Properly	FAIL
Client "Login" Options are Configured Properly	PASS
Clients are Obtaining Latest Signature Files	WARNING

Scheduled Scan is Active - PASS

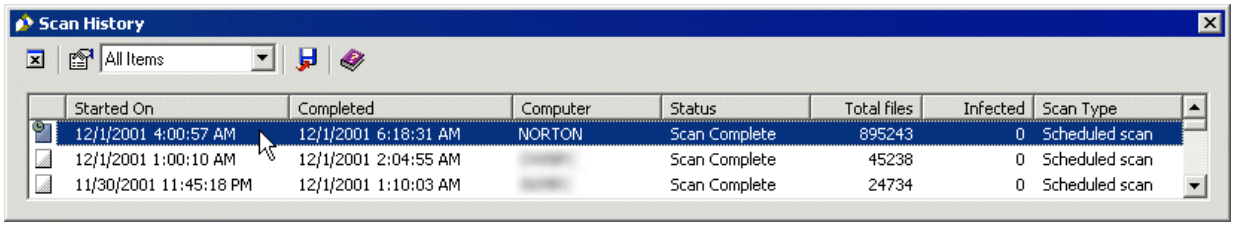
A complete scan is run against this server group every Saturday morning at 4:00am.





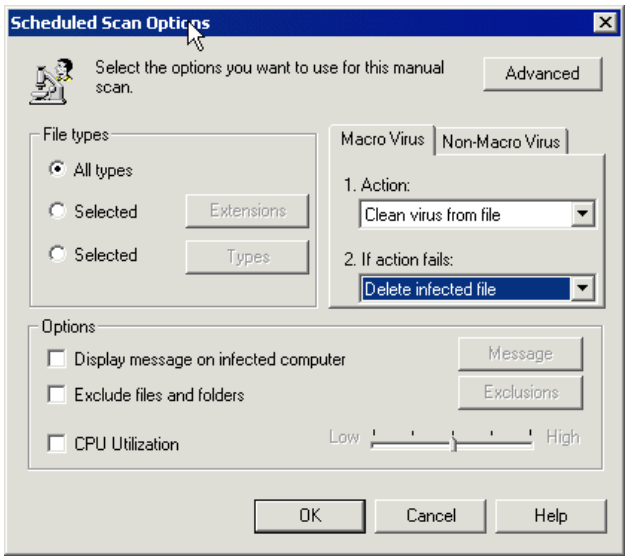
- Scan is configured to run during off-hours at least once a week

By checking the server group scan history we can also confirm the scan really runs and that it is really initiated by the scheduler, rather than "by hand."

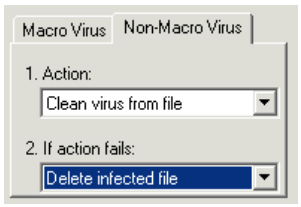


Scheduled Scan is Configured Properly - PASS

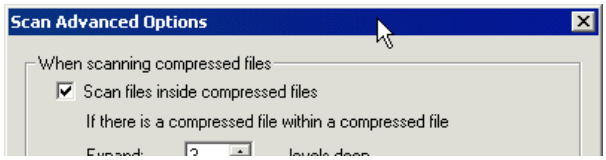
We already saw that scans were configured to run at an appropriate time. (4:00am on Saturdays.) We now need to make sure the appropriate actions are being taken in response to virus attacks.

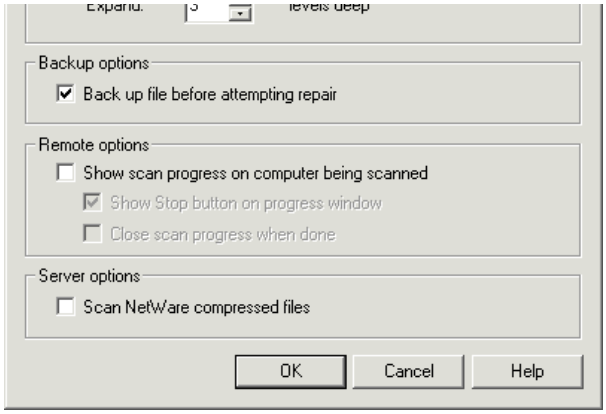


- File types: All types
- MacroVirus Action: Clean Virus from file
- MacroVirus If action fails: Delete infected file



- Non-MacroVirus Action: Clean Virus from file
- Non-MacroVirus If action fails: Delete infected file





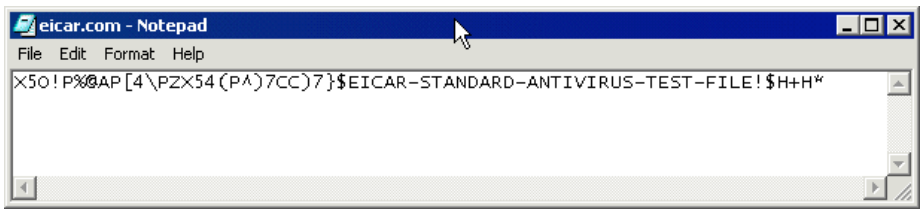
- When scanning compressed files: Scan files inside compressed files
- Expand: 3 levels deep
- Back up file before attempting repair: CHECKED

All important options have been set well so this category passes.

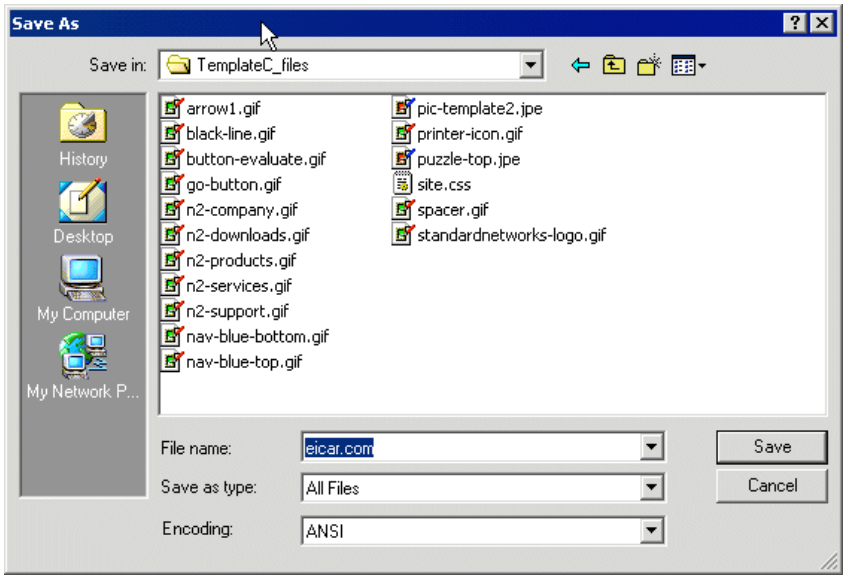
Realtime Protection is Active - PASS

To test realtime protection I popped open Notepad on a server machine with write permissions to several client desktops and copied the EICAR test string into Notepad. I then saved this file as "eicar.com" on several desktop machines. All machines tested detected the string correctly.

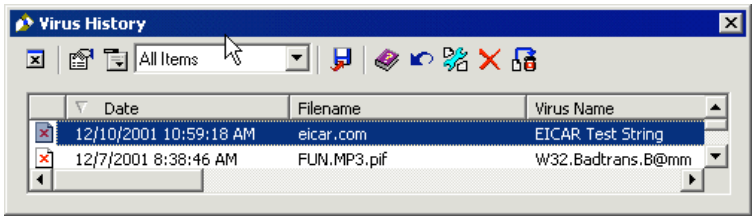
Here is a screenshot of the EICAR string in Notepad. (No "real time" detects will occur until this file is saved.)



Here is a screenshot of the file being saved to a remote machine (via its shared folders).

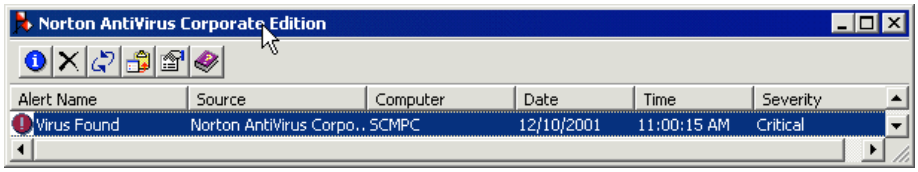


Here is the log entry we see when we click up the virus history (log) for each machine we "infected."

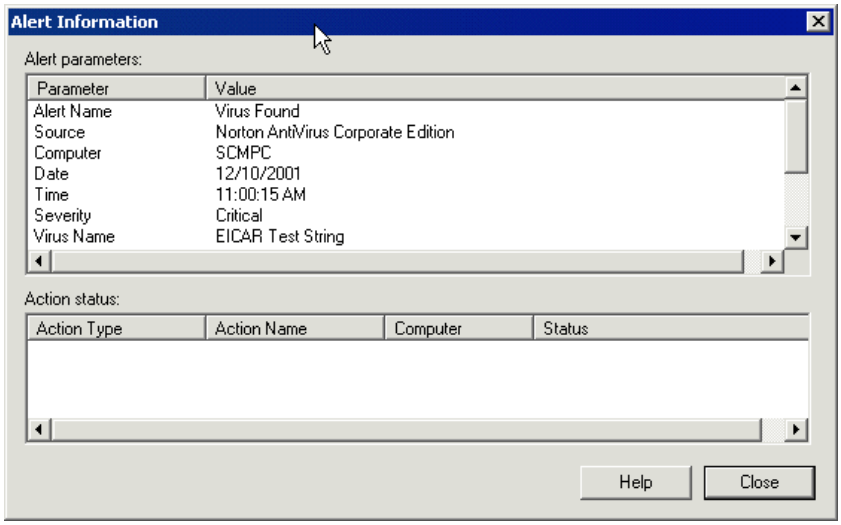


(Of the 33 clients, 15 were tested in this manner by hand. All found the test string.)

Alternatively, I could have checked the AMS log for the same entry. Here is what the same Eicar detect entry looks like in the AMS log:

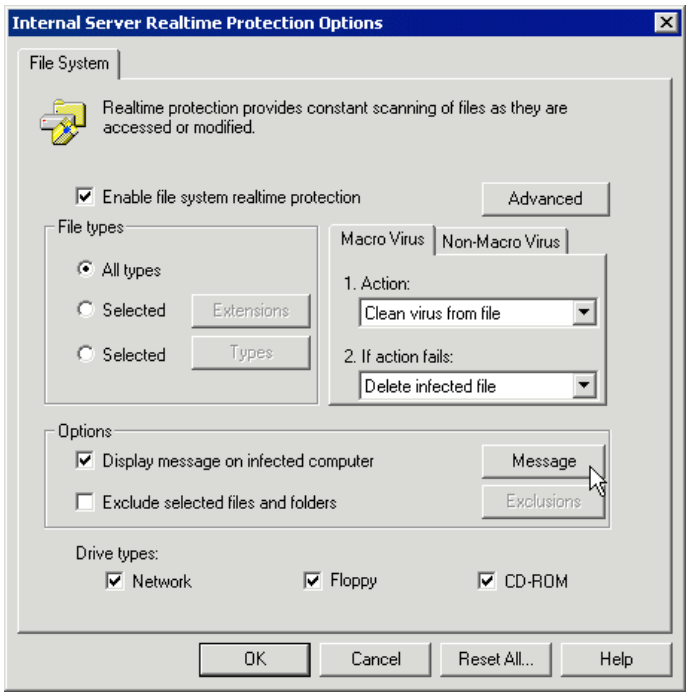


...and "clicked-up"...

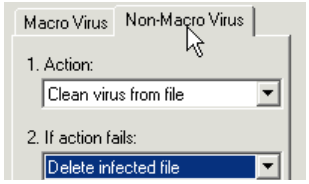


Server Realtime Protection is Configured Properly - WARNING

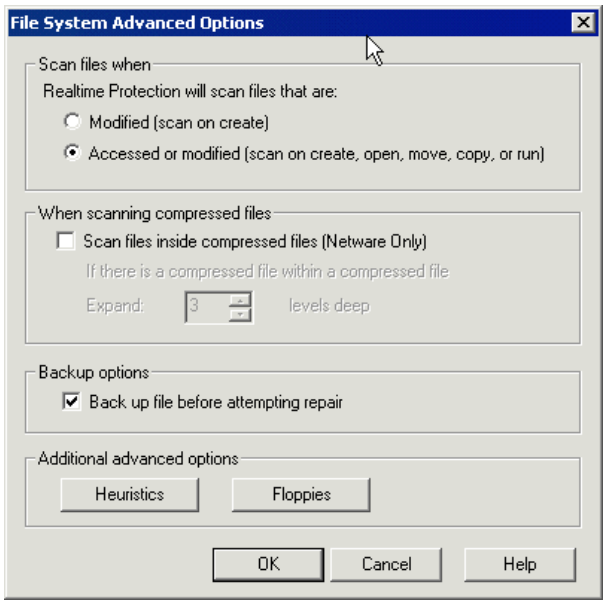
The main screen of server realtime properties looks perfect.



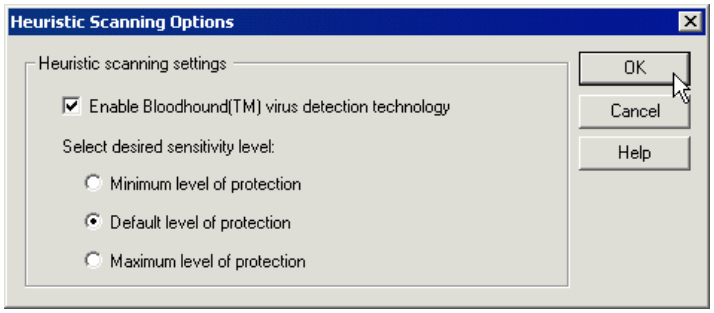
- File types: All types
- MacroVirus Action: Clean virus from file
- MacroVirus If action fails: Delete infected file
- Drive types: Network, Floppy, CD-ROM



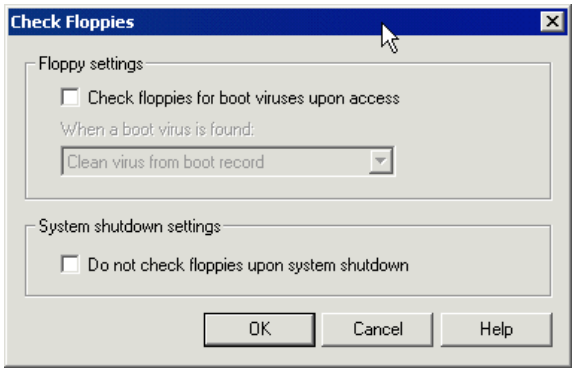
- Non-MacroVirus Action: Clean virus from file
- Non-MacroVirus If action fails: Delete infected file



- Scan files when: Accessed or modified
- Backup options: Back up file before attempting repair



- Enable Bloodhound: CHECKED
- Sensitivity level: Default *(should be Maximum)*

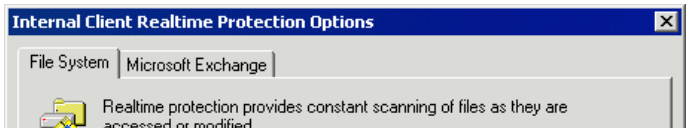


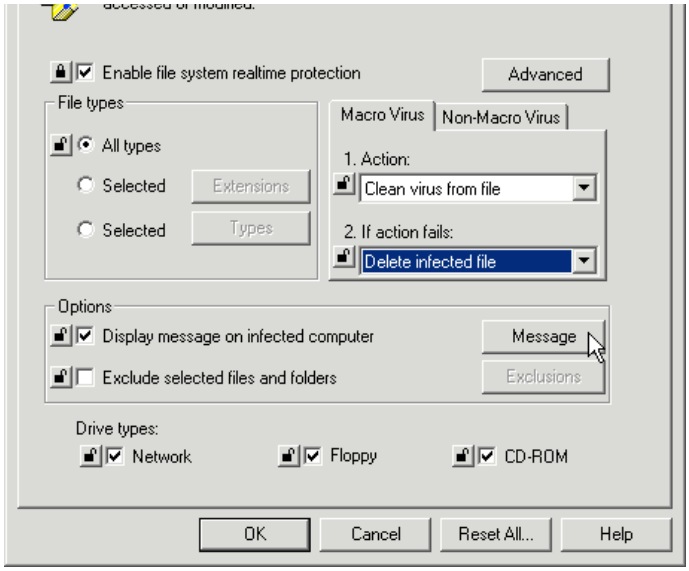
- Check floppies for boot viruses upon access: UNCHECKED *(should be CHECKED)*

Two options have been set poorly so this category scores a "WARNING".

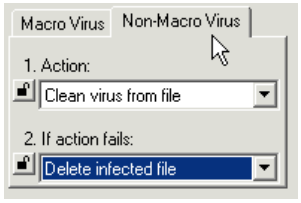
Client Realtime Protection is Configured Properly - FAIL

We immediately notice that most keys options are "unlocked", meaning clients can change them at will. This alone may be enough to "fail" this category, but we will still look at the other options configured.

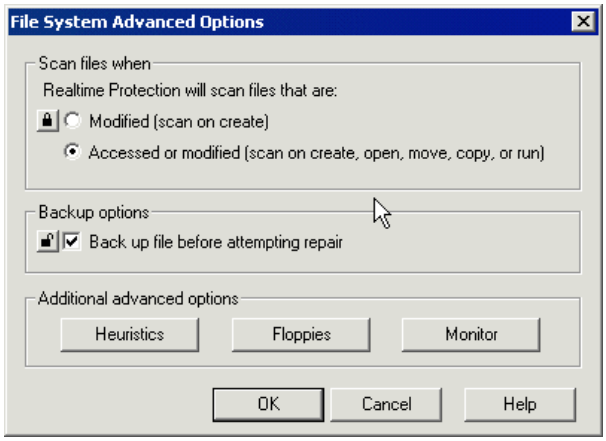




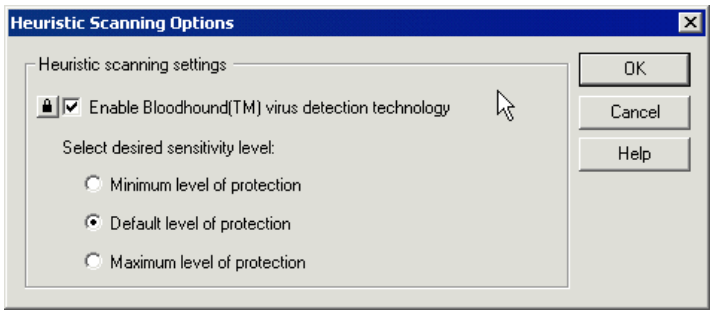
- File types: All types
- MacroVirus Action: Clean virus from file
- MacroVirus If action fails: Delete infected file
- Drive types: Network, Floppy, CD-ROM



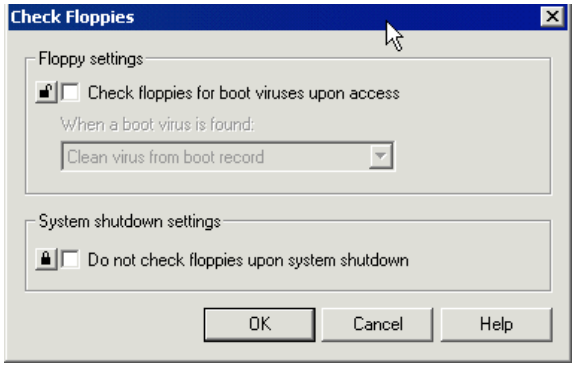
- Non-MacroVirus Action: Clean virus from file
- Non-MacroVirus If action fails: Delete infected file



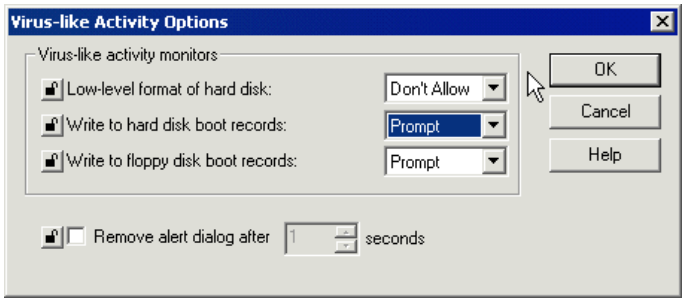
- Scan files when: Accessed or modified
- Backup options: Back up file before attempting repair



- Enable Bloodhound: CHECKED
- Sensitivity level: Default *(should be Maximum)*



- Check floppies for boot viruses upon access: UNCHECKED *(should be CHECKED)*

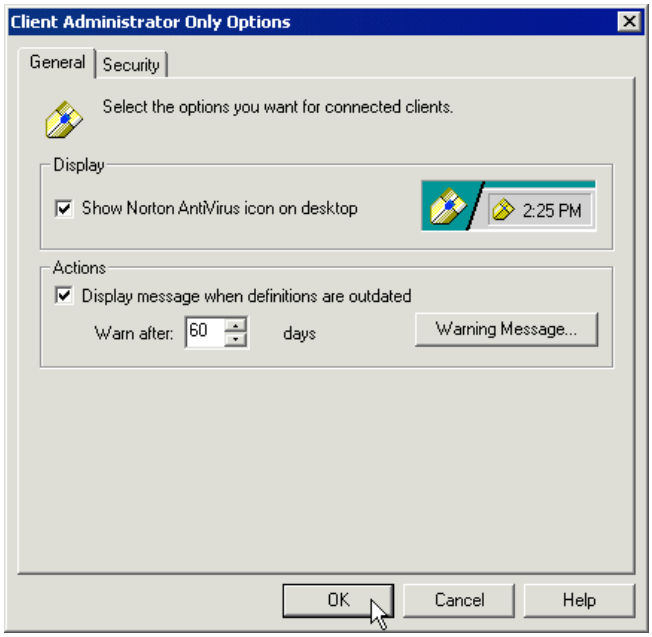


- Low-level format of hard disk: Don't Allow *(Prompt or stronger is okay.)*
- Write to hard disk boot records: Prompt
- Write to floppy disk boot records: Prompt

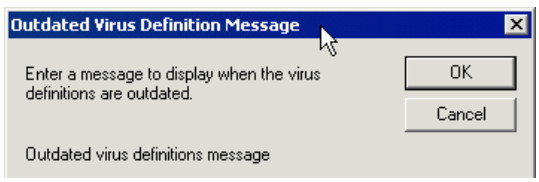
Only two options were incorrectly configured before considering the unlocked properties. That would have yielded a "WARNING" in this category; instead we grade a "FAIL."

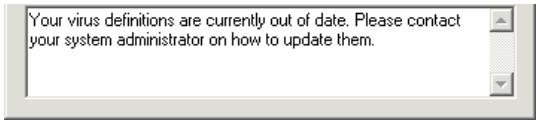
Client "Administrator-Only" Options are Configured Properly - FAIL

This category earned a true "FAIL". Outdated definition alert messages were being displayed after too much delay and failed to tell the end user what to do about them. Possibly worst of all, testing found the default uninstall password was still "symantec."

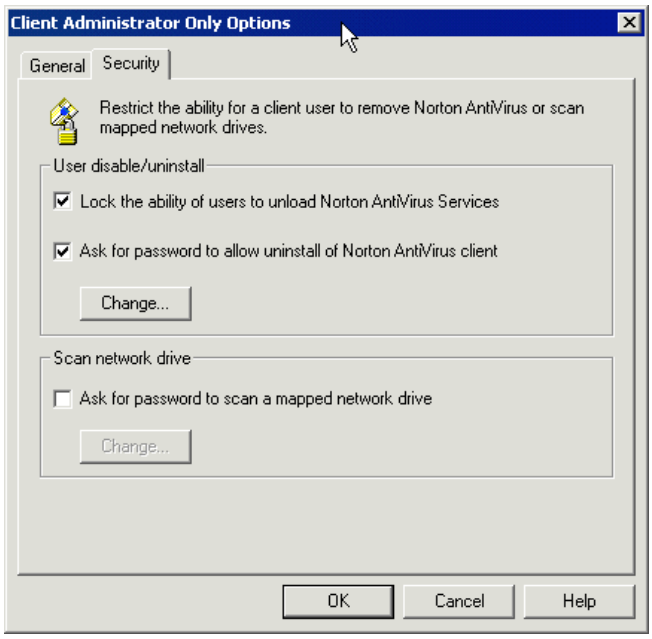


- Display message when definitions are outdated: CHECKED
- Warn after: 60 days *(Should be 15 or less)*





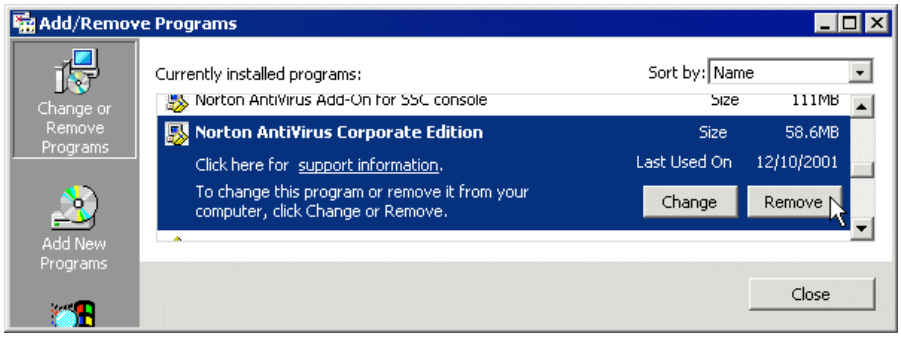
- Outdated virus definitions message: Your virus definitions are currently out of date. Please contact your system administrator on how to update them. *(Should tell end user how to contact someone who can fix the problem.)*



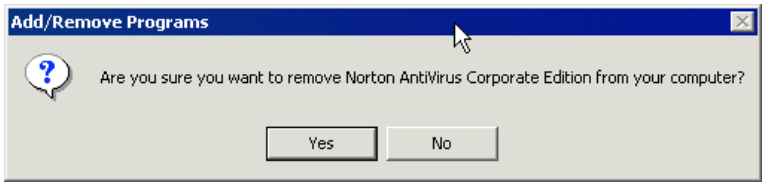
- Lock the ability of users to unload Norton AntiVirus Services: CHECKED
- Ask for a password to allow uninstall of Norton AntiVirus client: CHECKED

The following test was performed from 3 of the 33 clients with identical results. All confirmed that the default uninstall password of "symantec" was still in use.

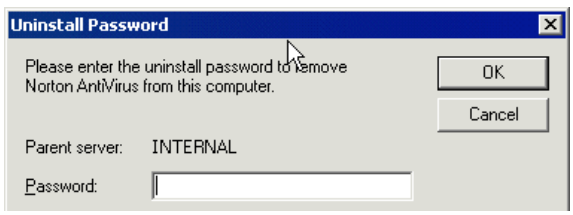
We opened the "uninstall programs" control panel on each machine. (These screenshots were taken from a Windows 2000 Professional desktop.)



We then selected "Norton AntiVirus Corporate Edition" and pressed the "Remove" button.



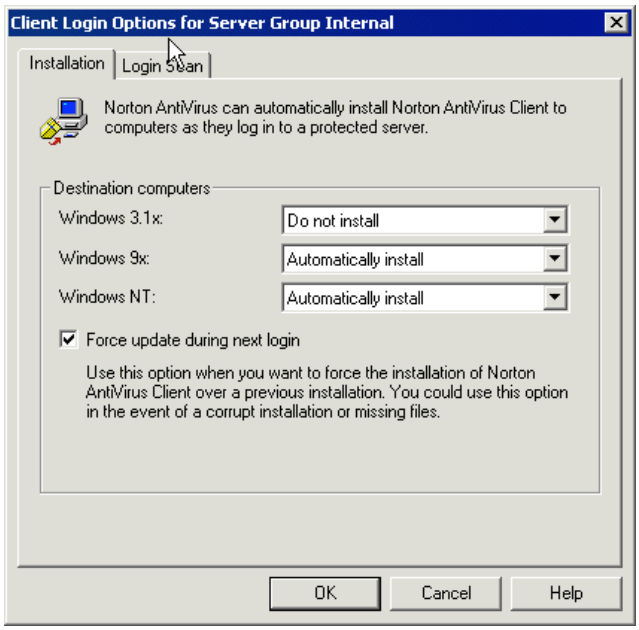
We answered "Yes" to the remove confirmation. At this point an "Uninstall Password" dialog appeared and challenged us for a password. In each instance we entered a password of "symantec" and were allowed to uninstall our virus protection package.



Client "Login" Options are Configured Properly - PASS

To properly grade this subjective item we first had to find out a little more about the environment Symantec's software was operating in. The credit union operates a single branch so network traffic is probably not going to be much of an issue. (They do not have any remote locations served by slow-speed lines.) All of their client machines are Windows 98, Windows NT or Windows 2000; all DOS and Windows 3.1 machines have been retired.

Based on this information, we can now consider the "login" settings in the proper context.

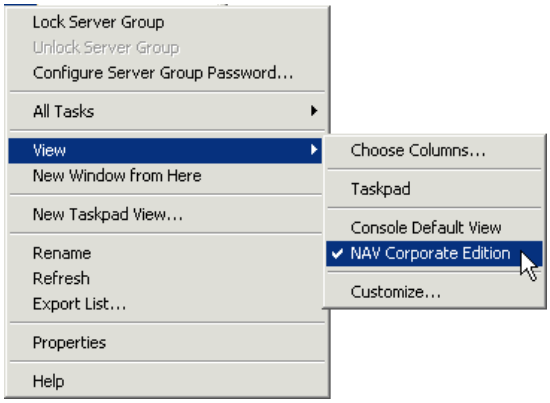


- *Windows 3.1x: Do not install (We can IGNORE this setting in this environment.)*
- Windows 9x: Automatically install
- Windows NT: Automatically install
- Force update during next login: CHECKED

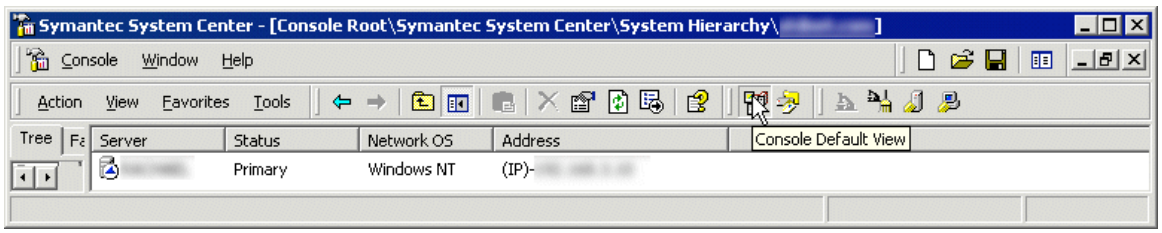
We can see that installations are automatically forced on all of this server groups clients and that updates are also forced. This appears to be an appropriate and sound implementation of these features at this installation, so we "PASS" this category. (We can safely ignore all options on the "Login Scan" panel because they only apply to 16-bit operating systems.)

Clients are Obtaining Latest Signature Files - WARNING

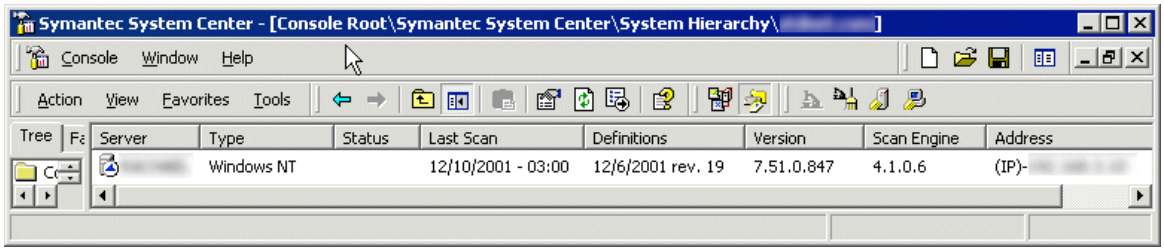
To speed this check up a bit I used a feature which should be available to most Norton Antivirus Administrators. Start by right-clicking a server group and selecting "View | NAV Corporate Edition,"



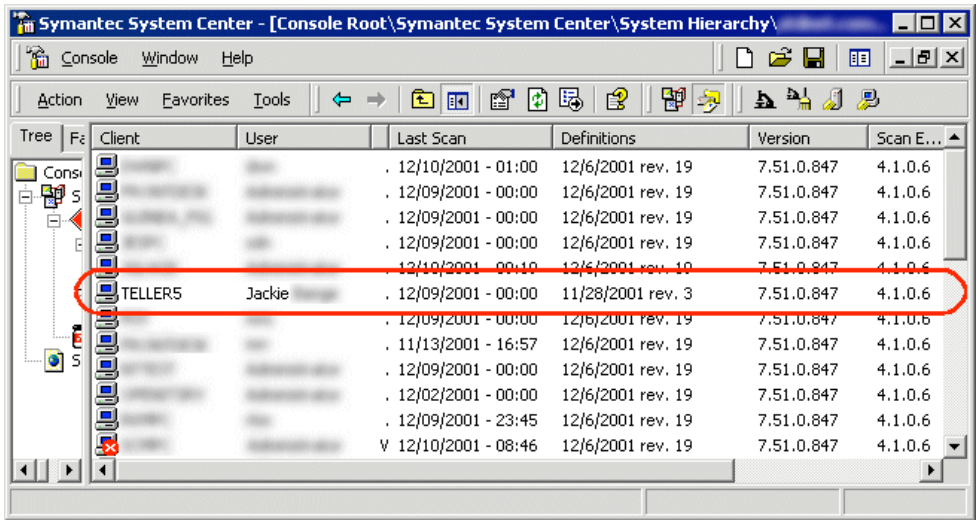
This option will switch the view from this...



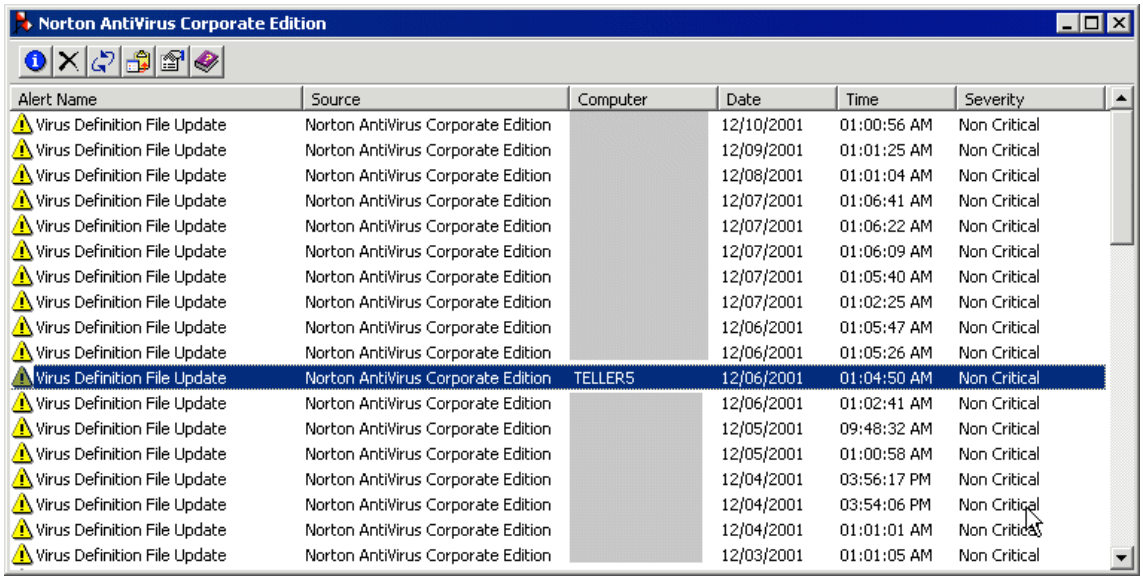
...to this.



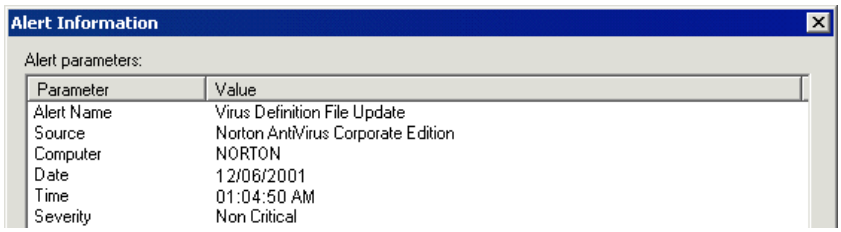
Note that definition dates and versions of updates are now visible from the central console. This makes it very easy to find any machines which are NOT getting updates. (Remember that in this view it is required to click on a SERVER within a SERVER GROUP to view the list of clients.) In the Internal Server Group we find a single machine which is not receiving updates.

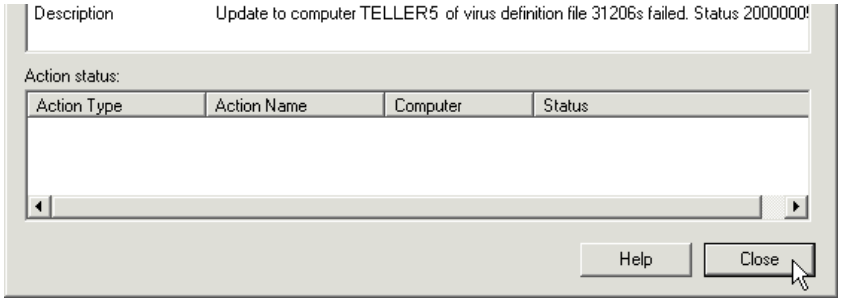


We spot-check a few clients from the client console as well as "TELLER5" to make sure this display is accurate, then cross-reference the failed updates against a filtered central ABS log. (Unfortunately Symantec logs both successful and unsuccessful attempts to update signatures as "non-critical" events, but selections by computer are possible.)



We can find several recent instances in which "TELLER5" was not updated. Other instances of clients not being updated are scattered throughout the file, but failed TELLER5 entries are found quite often.





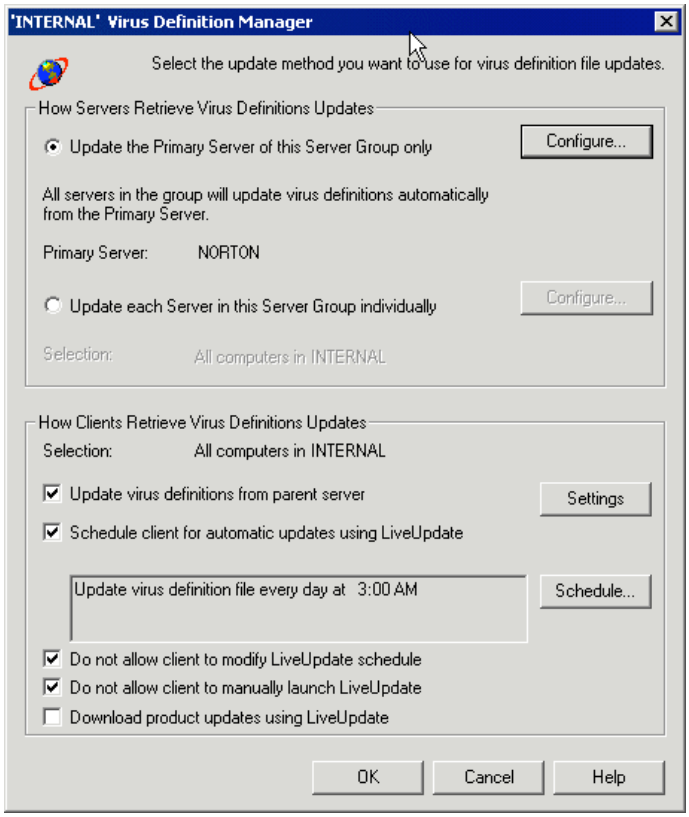
After this study of the logs, we still have only one machine to which updates are not being posted, so we award this category a "WARNING" score.

Server Checklist - Internal Server Group

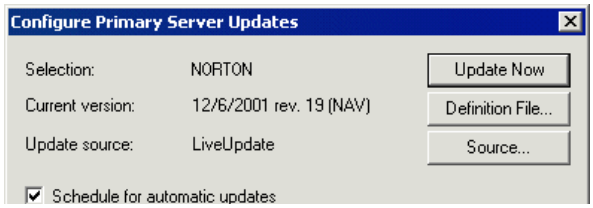
Item	Pass/Warning/Fail
Server is Obtaining Latest Signature Files	**PASS**
Server is Protected Against Unauthorized Configurations	**FAIL**
Server is Properly Backed Up	**PASS**

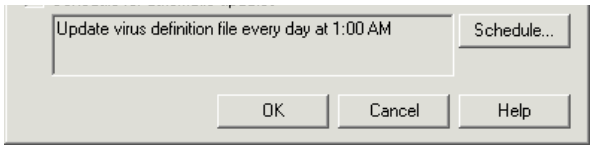
Server is Obtaining Latest Signature Files - PASS

The primary server ("NORTON") in this server group appears to be doing a good job retrieving new signature files in a timely manner. The group also appears to be configured to ensure clients receive their updates too.



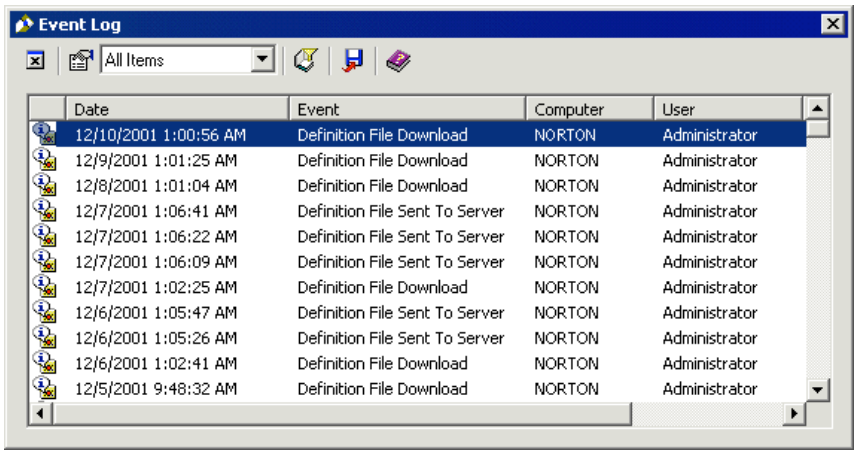
- How servers receive virus definition updates: Update the Primary Server of this Server Group only
- Update virus definitions from parent server: CHECKED
- Schedule client for automatic updates using LiveUpdate: CHECKED
- Scheduled update: "every day at 3:00 AM"
- Do not allow client to modify LiveUpdate schedule: CHECKED





- Version is current: YES
- Schedule for automatic update: CHECKED
- Scheduled update: "every day at 1:00 AM"

We should have checked for successful *client* updates in the *client* checklist; now we will check for successful server updates in the server group's event logs. (Filter for "Virus Definition File")



It appears the updates occur as regular as clockwork. This category earns a "PASS" score.

Server is Protected Against Unauthorized Configurations - FAIL

To test for the GRC.DAT security hole, we went to a client machine called "TELLER5", opened a DOS window and typed the test commands. We were allowed to perform the test without problems. This meant that any knowledgable user could make changes to the server group configuration.

Server is Properly Backed Up - PASS

NORTON is part of a large backup set which covers several key servers at the credit union. A full backup of the system (including the registry) is performed every evening. Although the backup media for the NORTON server itself is not a separate tape, elements of the backup set are regularly tested with partial reloads, so I believe the tapes really do contain the contents of the NORTON server.

(Normally a screenshot or two of backup logs would go here, but I could not pry those items out of the credit union for this assignment.)

Evaluate the System

From the Globals section we learned that the administrators of this system need to become more familiar with the Quarantine system and need to be more careful about locking their configurations after making changes.

From the Client - Internal section we learned that floppies were not being scanned for boot viruses and that the Bloodhound hueristics were not being allowed to run at their full potential. We also learned that end users have too much freedom to override antivirus settings or even uninstall the software

from their desktops. In addition, we learned that end users may recieve warnings about outdated signatures long after they should have and may not know what to do when they see one of these infrequent warnings.

From the Server - Internal section we noticed that the primary server is vulnerable to the widely found but seldom patched server-group configuration file vulnerability.

Other than these items we found the system to be in fairly good shape. Updates were being retrieved regularly from Symantec and most clients were faithfully receiving them. Administrators may not have configured the system to its full potential, but they are staying on top of the environment and clearly could master the remaining few essentials.

Specifically, the following configuration changes are recommended:

- In the **Quarantine configuration**, CHECK the following, currently unchecked items:
  Install on infected clients
  Install on servers of infected clients
- In **both the SERVER and CLIENT RealTime configurations**, make the following changes:
  Set Heuristic (Bloodhound) Sensitivity level to MAXIMUM
  CHECK the "Check floppies for boot viruses upon access" item
- In just the **CLIENT RealTime configuration**, make the following change:
  "LOCK" all key client options (all options noted in this audit)
- In the "**Administrator-Only" Client Options**, make the following changes:
  Set "Warn after" to 15 days
  Change the virus definitions message to something similar to:
  "Your computer virus definitions are out of date and you are at immediate risk of contracting a computer virus. Please contact Sally XXX or Larry XXX immediately at 555-5555 to correct this problem."
  Set the "uninstall password" to a strong password known only to administrators.
- To prevent unauthorized access to the GRC.DAT file, perform the following task on the **folder NORTON shares as "VPLOGON"**
  Add "Full Control" XXX to the SYSTEM group (and maybe the "Administrators" group or its equivilant)
  Remove "Everyone" from the list of groups with privileges to this folder

To make the configuration changes necessary to "fix" the system, less than an hour of time would be required. To learn about the quarantine system administrators should probably set aside two hours each. No additional software or hardware will be needed to carry out these tasks.

Evaluate the Audit

The Symantec administrative interface is so flexible that the phrase "there is more than one way do it" begins to apply to the various log views and entity lists. During the audit I used several shortcuts to view key information (such as virus definition versions) in managable groups. It may be a good idea to either rely on these shortcuts exclusively (if the shortcuts can be shown to enjoy high fidelity) or specify exactly how to test the fidelity of a particular server-group's information (if the shortcuts do not enjoy high fidelity.)

A "sub-checklist" of items on each dialog box may have helped in the raw checklist itself; I found myself building something similar under each dialog box screenshot as the audit progressed.

One other item at which I would have liked to look is the order of definition updates and daily scans. Ideally, the order would go something like this: 1) download from Symantec, 2) push to clients, 3) initiate client scan. Unfortunately there are only so many "off-hours" in a day and if the daily download from Symantec is scheduled too early, the possibility that the daily download from Symantec will miss the newest signature increases.

Validating and verifying many of the settings in this system is also difficult. For example, it would be difficult to test the quarantine process from start to finish (from detect, to the system, to Symantec, operating with an interim patch, etc.) It is also hard to test the Bloodhound heuristics; there is no known "Eicar-like" trigger to use against this system.

Other than these items I found the audit offered a good way to evaulate what may otherwise be a fairly complicated system and distill it into a concise overview of problem areas and suggestions. (Notice the overview in the "Evaluate the System" section above is much shorter and easier to read than the audit.)

In the area of future improvment, it would probably be easy to write a few scripts to test remote clients with Eicar strings automatically or compare a central configuration file against a list of known, good values.

Within the audit itself I may want to consolidate the four quarantine configuration options into a single "Quarantine is configured properly" item; doing so would allow the quarentine section to mirror the configuration sections of active clients.

Sources

(The following sources are listed alphabetically. All have been cited previously in assignment text.)

"Computer Security Incident Handling: Step-by-Step," SANS Institute Publications. (http://www.sans.org/newlook/publications/incident_handling.htm)

"Example of an Emergency Containment Plan to respond to a virus infection," Symantec Knowledge Base. November 1, 2001. (http://service4.symantec.com/SUPPORT/ent-security.nsf/552ba2f7636bedf088256818006f78bf/d4fe4fd2aa5d954c88256aab0064959f?OpenDocument&prev=http://search.symantec.com/custom/us/techsupp/enterprise/kb/query.html?*col=kb%20us*st=1*nh=10*pcode=*qp=url:/ent-security.nsf/552ba2f7636bedf088256818006f78bf,url:us-sarc,url:us-ts,url:us-lu,url:us-cs*qt=what%20needs%20to%20get%20backed%20up*miniver=nav-

75-ce*sone=nav-75-ce_tasks.html*stg=*prod=Norton%20AntiVirus*ver=7.5%20Corporate%20Edition*base=http://www.symantec.com/techsupp/enterprise/products/nav/nav-75-ce/*next=&sone=nav-75-ce_tasks.html&stg=&prod=Norton%20AntiVirus&ver=7.5%20Corporate%20Edition&base=http://www.symantec.com/techsupp/enterprise/products/nav/nav-75-ce/&next=&src=ent&pcode=)

Green, Bob. "I Thought We Had Virus Protection: The Mistakes that Made Us Vulnerable to the W32/SirCam@mm Virus," SANS Information Security Reading Room. August 16, 2001.
(http://www.sans.org/infosecFAQ/malicious/sircam.htm)

"How do I set up Norton AntiVirus Enterprise Edition so that my departmental workstations can update virus definitions automatically?," Indiana University Knowledge Base. January 12, 2001.
(http://kb.indiana.edu/data/ajar.html)

"How to uninstall Norton AntiVirus for Microsoft Exchange manually and verify rights in Microsoft Windows NT and Exchange," Symantec Knowledge Base. October 15, 2001.
(http://service2.symantec.com/SUPPORT/ent-security.nsf/361fc4a260e563b1882568180069e1c0/99f795937d5be9b788256a3400750926?OpenDocument)

"In Norton AntiVirus Enterprise Edition, how do I prevent unauthorized users from connecting to my Norton AntiVirus server?," Indiana University Knowledge Base. January 16, 2001.
(http://kb.indiana.edu/data/ajcv.html)

Mallion, Bob. "Enterprise-Wide Virus Protection (So You Think You're Protected from Malicious Code!)," SANS Information Security Reading Room. November 20, 2000.
(http://www.sans.org/infosecFAQ/email/protection.htm)

McAleer, Sean P. "A Defense-in-Depth Approach for Securing Mobile Devices and Wireless LANs," SANS Information Security Reading Room. January 24, 2001.
(http://www.sans.org/infosecFAQ/wireless/defense.htm)

"Norton Antivirus (Corporate Edition) - An Overview, " Georgia State University Computing and Communications Services. October 4, 2001.
http://www.gsu.edu/~wwwccs/docs/norton/nav.htm

Norton AntiVirus Corporate Edition 7.5/7.6 Implementation Guide

"Norton AntiVirus Corporate Edition for Windows 95, 98, Me, NT and 2000 Installation and Configuration," University of Virginia Information Technology and Communication. June 22, 2001.
(http://www.itc.virginia.edu/desktop/docs/navdoc/)

"Norton AntiVirus Corporate Edition Lets Local and Remote Users Change Anti-Virus Configuration," SecurityTracker.com. November 23, 2001.
(http://www.securitytracker.com/alerts/2001/Nov/1002814.html)

"Symantec Security Response: Best Practice Policies: Enterprise Security Manager: Norton AntiVirus CE 7.5 Server on Windows 2000 - ISO 17799," google.com cache. August 24, 2001."Symantec Security Response: Best Practice Policies: Enterprise Security Manager: Norton AntiVirus CE 7.5 Server on Windows 2000 - ISO 17799," google.com cache. August 24, 2001.
(http://www.google.com/search?q=cache:y6GL0VBlH_o:www.symantec.com/avcenter/security/Content/best.practice.policies/esm/2001.08.10.html+symantec+antivirus+best+practices&hl=en)

Symantec System Center Version 4.6 Implementation Guide

Yale University Information Technology Services. "Getting the most out of your Anti-Virus software," Yale University.
(http://www.yale.edu/its/security/new-index.html?http://www.yale.edu/its/security/antivirus.html)

Zocco, Paul A. "Ten Days to Network Security," SANS Information Security Reading Room. August 6, 2001.
(http://www.sans.org/infosecFAQ/securitybasics/10days.htm)