Symantec Norton AntiVirus Configuration for the GCS-3000 Targeted Genotyping System – Technical Note

How to activate Norton AntiVirus 2005 on the GCOS Instrument Workstation and GTGS Workstations, and how to customize Norton AntiVirus on GCOS

Affymetrix bundles Symantec's Norton AntiVirus software with all GCOS Instrument Control and GTGS computers. The software is pre-installed, but is only activated by the system administrator if desired.

Norton AntiVirus provides comprehensive virus prevention, threat detection, and repair software for your computer. It automatically detects and repairs known viruses. It detects viruses and other potential risks in instant messenger attachments as well as in email messages, Internet downloads, and other files. Norton Antivirus can be configured to automatically update its virus definitions over the Internet, to be prepared for the latest threats. It includes expanded threat detection of both known and emerging threats, such as spyware and other files that could put your computer at risk. It also scans files inside of compressed files.

In the 2005 edition of Norton AntiVirus, Symantec introduced Internet Worm Protection. Internet Worm Protection default settings blocks communication between GeneChip® Operating Software (GCOS) and GeneChip® Targeted Genotyping Analysis Software (GTGS), which exist on different computers.

Section 1 describes how to activate Norton AntiVirus on all machines, and checks that it doesn't interfere with existing Microsoft Windows Firewall settings.

Section 2 describes how to open ports 135 and 1025 through 1035 on the GCOS Instrument Workstation within the Norton AntiVirus, so that GCOS can communicate with GTGS using DCOM.

Note: The only antivirus solution supported by Affymetrix is Norton Antivirus.

Note: It is necessary to have local administrative rights to make changes to the Norton AntiVirus settings.

Section 1: Norton AntiVirus 2005 Activation

NOTE: Do the following activation steps for the GTGS Pre-Amp and Post-Amp Lab Workstations, and the GCOS Instrument Control Workstation

- 1. Log in to Windows as **Administrator**. Unless your system administrator has changed it, the password will be blank.
- 2. Check existing Firewall settings
 - Navigate to Start Menu > Control Panel > [Security Center] > Windows Firewall (This control panel may not exist if the computer isn't using Windows XP Service Pack 2. If the Windows Firewall control panel doesn't exist, skip to step 3.
 - In the General tab record whether the firewall is ON or OFF.
- 3. If the following NAV window isn't already open, right-click on its icon in the Task Bar in the lower right corner of the screen.



- 4. Click **Next** to begin the configuration process.
- 5. Accept the license agreement and click Next.

1 Welcome	License Agreement	
2 Connect	SYMANTEC SOFTWARE LICENSE AGREEMENT	
3 Security	IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES (NYSWANTECA TO AUTULING TO LICENSE THE SOFTWARE TO YOU	
4 Thank You	AS THE INDIVIDUAL. THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE OTLIZING THE SOFTWARE (REFERENCED BELOW AS "YOO" OR 'YOUN') ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE ACREMENT. THIS IS A LEGAL AND ENFORCEMELE CONTIACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "ACCEPT" OR "YESP SUITON OR OTHERWISE	>
	C I accept the License Agreement C I do not accept the License Agreement	

6. Either register basic information now, or just click **Register Later**.

Welcome	Registration Privacy policy: www.symantec.com
Connect	Registration can help keep you informed about product upgrades and new information that is important to you or your business. Registration is optional
Security	Fill in the applicable fields below to register your software with Symantec.
Thank You	I would like to receive email from Symantec Email Address:
	It's OK to contact <u>me</u> by phone Phone number:
	Book Nort Boolean Joy

7. At the subscription expiration date window, click Next.

😣 Norton AntiVirus		×			
1 Welcome	Norton AntiVirus Sub	scription			
2 Connect	Symantec's antivirus experts continuously update Norton AntiVirus to protect your computer from the latest viruses and malicious code threats				
3 Security 4 Thank You	Those reproductive and the activity of the second s				
	Start Date: 11/29/2005	Expiration Date: 2/27/2006			
	Back	<u>N</u> ext			

8. At the Security window, click Next.

😣 Norton AntiVirus	
1 Welcome	Security
2 Connect	✓ Use my Norton Internet Worm Protection instead of Windows Firewall. (Recommended) Norton AntiVirus is protecting your computer from viruses, worms and other
3 Security	Internet threats. For optimal performance, turn off Windows Firewall.
4 Thank You	$\fbox{\ \underline{D}}$ on the normalized product $$. (Recommended)
	To minimize security exposure, use Norton products to manage their security status and alerts.
	<u>B</u> ack <u>N</u> ext

9. In the Thank You window, click Finish.

😣 Norton AntiVirus	X
1 Welcome	Thank You
2 Connect	These tasks launch immediately after you click 'Finish'.
3 Security	Kun LiveUpdate Uses your Internet connection to download the latest virus protection and program updates.
4 Thank You	Scan for Viruses Performs a full system scan on your computer.
	Back Einish

10. In the LiveUpdate window, click **Next**.



11. After LiveUpdate completes, click **OK** when informed to re-run LiveUpdate.



- 12. Click Finish.
- 13. You will be asked to restart the computer. Click OK.



14. After the computer restarts, log in as Administrator.

15. Wait for Norton AntiVirus to automatically start up and start scanning all files for possible problems. When it has completed, click **Finish**. The window will close.

8	Norton AntiVirus			
1	Scan Progress	Scan Pro	gress: Scan for Threats	
2	Repair Wizard Fix	Scanning for t	hreats:	
	Quarantine	Current Item C:\Documents	and Settings\abupp\Application	
3	Delete Manual Removal	1993962763-7 bc86-9b568d5	25345543-23412\77182eb6-5e70-45e5- 323bc	-
4	Summary	Action	Files	
		Scanned	506	
		Detected	0	
		Fixed	0	
		Deleted	0	
			Pause Stop Scan	

16. Norton AntiVirus will display the System Status. Click **Turn On** to turn on Automatic LiveUpdate.



17. Close the Norton AntiVirus window.

NOTE: Norton AntiVirus may have changed the Windows Firewall settings. The following steps will undo this change.

- 18. Navigate to Start Menu > Control Panel > [Security Center] > Windows Firewall (This control panel may not exist if the computer isn't using Windows XP Service Pack 2. If the Windows Firewall control panel doesn't exist, you're done with Norton activation for this computer.
- 19. If Windows Firewall does exist, open it.
 - In the General tab record whether the firewall is ON or OFF.
 - If the Windows Firewall is in a different state (ON or OFF) than it was before, change it back to the way it was before Norton was activated.

Section 2: Configure Norton Antivirus on the GCOS Instrument Workstation to allow GCOS to communicate with GTGS

NOTE: Do the following steps **ONLY** for the GCOS Instrument Control Workstation.

1. From the GCOS Instrument Workstation, navigate to the Start menu, and select "Programs" > "Norton AntiVirus" > "Norton AntiVirus 2005".

😵 Norton AntiVirus			
LiveUpdate 🗹 Options			② <u>H</u> elp & Support ▼
Norton AntiVirus	System Statu <mark>s: OK</mark> 📀		
Stat <u>u</u> s	Security Scanning Features		
Scan for Viruses	Auto-Protect	On	Auto-Protect
Reports	Internet Worm Protection	On	Provides continuous protection from viruses
	Email Scanning	On	threats.
	Eull System Scan	9/23/2005	More Info
	Subscription Service		
	Virus Definitions	10/26/2005	
	🔗 <u>Renewal Date</u>	9/24/2006	
	Automatic LiveUpdate	On	
Symantec.	N	orton Anti	Virus ²⁰⁰⁵

- 2. If "Internet Worm Protection" is "On", click **Options** at top of window. If it is "Off", then stop now, because no more configuration is needed.
- 3. Select Internet Worm Protection on the left half of the Options screen, and then click General Rules.

System	Internet Worm Protection	ore Info
Auto-Protect Script Blocking Manual Scan	How to stay protected from certain Internet Worm attacks Enable Internet Worm Protection (recommended)	
nternet	Configure Exclusions	
Email		
Internet Worm Protection	How to customize your settings	
Instant Messenger	Program Control	
LiveUpdate		
Other	General Rules	
Threat Categories	Irojan Rules	
Miscellaneous	AutoDirect Dates	
	Autobiock Rules	
Default All	OK Cancel Pare Defaulto	

4. Click Add.

Internet Worm Protection		
General Rules		
		More Inf
hese rules determine how the Internet Worm Protec onnections. Rules that appear earlier in the list over	tion handles incol ride later rules.	ning and outgoing
✓ Description		
Default Non-Routable IPs Permit, Direction: Inbound, Computer: Spec Any, Protocol: TCP and UDP	ific, Adapter: Specific	, Communications:
Default Inbound ICMP Permit, Direction: Inbound, Computer: Any, Protocol: ICMP	Adapter: Any, Commu	inications: Any,
Befault Inbound DNS Permit, Direction: Inbound, Computer: Any, Protocol: UDP	Adapter: Any, Commu	inications: Specific,
🚐 📧 Default Inhound NetBIOS		~
Add Modify Remove	Move Up	Move Down
]	

5. Make sure "Permit" is selected, and then click **Next**.

Add Rule	
	More Info
Do you want to block or permit a new connection?	
Permit: Allow connections that match this rule.	
C Block: Do not allow connections that match this rule.	

6. Make sure "Any Computer" is selected, and then click **Next**.

🌡 Add Rule	×
Add Rule	
	More Info
What computers or sites do you want to permit?	
Any computer	
C Only the computers and sites listed below	
	~

7. Make sure that the permitted protocols are TCP and UDP.

😵 Add Rule	
Add Rule	
	More Info
What protocols do you want to permit?	
CITCP	
C UDP	
TCP and UDP	
CICMP	
What types of communication, or ports, do you want to permit?	
C All types of communication (all ports, local and remote)	
• Only the types of communication or ports listed below	
3	
Add Remove	
< <u>B</u> ack <u>N</u> ext > <u>C</u> an	cel

- 8. Change the permitted communication ports to **Only the types of communication or ports listed below**. Then click **Add**.
- 9. Change the "Filter by" to Individually specified ports.

😣 Specify Ports	
Specify Ports	
	More Info
Filter by:	Locality:
C Known ports from list	Cocal
Individually specified ports ○ Port range	C Remote
Enter port number or numbers. To e space between each entry. 135	nter multiple port numbers, use a
OK	Cancel

- For the port, enter **135**.
- Click **OK** to close window.

10. Back in the "Add Rule" window, click Add.

😣 Add Rule	×
Add Rule	
	More Info
What protocols do you want to permit?	
C TCP	
C UDP	
TCP and UDP	
CICMP	
What types of communication, or ports, do you want to permit?	
C All types of communication (all ports, local and remote)	
Only the types of communication or ports listed below	
local epmap (port 135)	
N N	
Add Remove	
< Back Next >	Cancel

11. Change the "Filter by" to Port range.

😣 Specify Ports		×
Specify Ports		
		More Info
Filter by:	Locality:	
C Known ports from list	Cocal	
C Individually specified ports	C Remote	
Port range		
Enter the starting port 1025		
Enter the ending port		
1035		
ОК	Cancel	

- For the starting port, enter **1025**.
- For the ending port, enter **1035**.
- Click **OK** to close window.
- 12. Click **Next** in the Add Rule window.
- 13. Check the Create an event log entry option.

🕹 Add Rule	×
Add Rule	
	More Info
You can choose to be notified when a connection matches this rule.	
When a connection matches a rule:	
Only Log event after it occurs 1 times	
Create an event log entry	

Note: Events are viewable by returning to the first Norton window, and navigating to "Reports" > "View Activity Log" > "Norton Internet Worm Protection" > "Activities".

- 14. Click Next.
- 15. Name this rule as **DCOM**.

Add Rule	Þ
dd Rule	
	More Info
What do you want to call this rule?	
This description appears in the Rule Summary list to help you identify this rule	
рсом т	

- 16. Click **Next**, then **Finish**.
- 17. Select the DCOM rule, and click **Move Up** until it is at the top of the list, so that it will be the first rule applied.

😣 Internet Worm Protection	×
General Rules	
Mo	re Info
These rules determine how the Internet Worm Protection handles incoming and outgoin connections. Rules that appear earlier in the list override later rules.	ıg
✓ Description	
Berlin, Direction: Inbound, Computer: Any, Adapter: Any, Communications: Specific, Protocol TCP and UDP, Tracking: Create a log entry	
Befault Non-Routable IPs Default Non-Routable IPs Arg. Protocot TCP and UDP Arg. Protocot TCP and UDP	
Default Inbound ICMP Permit, Direction: Inbound, Computer: Any, Adapter: Any, Communications: Any, Protocol: ICMP	
💷 Default Inhound DNS	~
Add Modify Remove Move Up Move Down	
ŌK	

18. Click **OK** to dismiss, then click **OK** again, and then close all Norton AntiVirus windows.