

Release Notes

GVC

SonicWALL Global VPN Client 4.0.0

Contents

Pre-installation Recommendations
Platform Compatibility
New Features
Known Issues
Resolved Known Issues
Troubleshooting

Pre-installation Recommendations

SonicWALL strongly recommends you follow these steps before installing Global VPN Client (GVC) 4.0.0:

- **For Vista systems, it is required that you update device drivers for each Network Adapter card to the latest available versions. You can check the NIC vendor Web site for these updates.**
- **For systems with client based firewalls, verify that the firewall clients are Vista Compatible. Upgrade the firewall software to the latest version. Or, if you are not actively using the client, uninstall it prior to installing GVC.**
Note: Norton Internet Security can cause compatibility problems during installation. If it is not currently in use, it is recommended that you uninstall Norton before installing GVC.
- **GVC encounters run time conflicts when it co-exists with any 3rd party IPsec VPN clients. Uninstall all IPsec VPN clients prior to installing GVC.**
- **Fresh installs of the GVC 4.0.0 are recommended over upgrading from the beta release.**

Platform Compatibility

The SonicWALL Global VPN Client (GVC) 4.0.0 release supports the following platforms:

1. Network Security Appliance (NSA) E-Class series
2. TZ series
3. PRO series
4. TELE series
5. SOHO series
6. GX series

The SonicWALL GVC 4.0.0 release is compatible with the following firmware releases: 6.4.2.0, 6.5.0.4, 6.6.0.x, SonicOS 1.0.0.2, SonicOS Standard 2.0.0.2 (or higher), and SonicOS Enhanced 2.0.0.2 (or higher).

The SonicWALL GVC 4.0.0 release is compatible with the following operating systems: Windows 2000, Windows XP, and Windows Vista (32 bit).

Windows Vista (64 bit), Windows NT 4.0, Windows ME and Windows 98 are not supported.



Release Notes

New Features

The following new features are supported on the SonicWALL GVC 4.0.0 release:

- **Vista (32 bit) Compatibility:** GVC 4.0.0 is now fully compatible with the Windows Vista (32 bit) operating system. The following enhancements have been implemented:
 - o The virtual adapter now automatically matches its link speed to the link speed supported by the computer's Network Interface Card (NIC).
 - o The virtual adapter can be manually disabled when a GVC connection is not active or when the GVC application is not running. To disable the virtual adapter, go to **View > Options** and select the **Disconnect the virtual adapter when not in use** checkbox. This can be useful if the virtual adapter is causing networking problems when a GVC connection is not active.
- **Enhancements:**
 - o **Configuration File Backup:** GVC creates a backup configuration file which is an exact replica of the encrypted configuration file (*.rcf). The backup file is saved in the clear because it ONLY consists of basic connection information without user name, password, or PSK information. The backup file is saved in the same directory as the encrypted configuration file. If the encrypted configuration file cannot be decrypted then GVC will recover the connection information from the backup configuration file. Since PSK is not saved in the backup file, and the default provisioning key is not enabled on the firewall, the user will have to re-enter the PSK in order to complete IKE authentication. The backup file can also be used for distributing connection information to GVC users in an organization. In order to do this, copy the backup configuration file to the destination users directory.
 - o **GVC Report:** GVC report now shows the device driver version for each Network Adapter Card.
 - o **GVC Log:** The following new log messages have been added:
 - *"The downloaded policy configuration contains no destination networks"* (Error)
Indicates that the Group VPN Policy [zone] downloaded from the firewall to the Global VPN Client had no destination networks in it, because the SonicWALL administrator did not assign any VPN access network(s) to the user (and/or the user did not inherit any VPN access network(s) through the user group membership). When Global VPN Client logs this error, the connection status changes back to Disabled.
 - *"The ISAKMP float port (4500) is already in use. Port X will be used as the ISAKMP float source port"*
Indicates that a native IPsec client service is running in the OS, and GVC is not able to use the defined UDP port required when a NAT device is detected in the path to the peer.

Note: On WinXP/Win2K systems, GVC will disable the native IPsec client service on startup and claim the defined UDP source port for IKE protocol. On Vista systems, GVC must be started by selecting 'Run as administrator' in order to achieve the same function.
 - *"Required IKE ID type not found in certificate"*
Indicates that the expected IKE ID was not found in the selected certificate. GVC will prompt the user to select a new certificate.

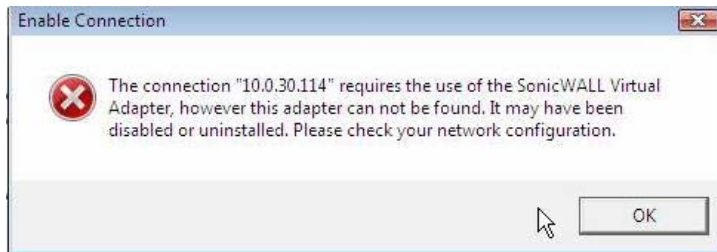


Release Notes

Known Issues

The following is a list of known issues in the SonicWALL GVC 4.0.0 release:

- **50330: Symptom:** Uninstalling GVC does not delete all the GVC components. **Condition:** Occurs when logged in as a power user but using administrator privileges to uninstall. **Work Around:** Login as administrator to uninstall GVC.
- **50323: Symptom:** Vista (32 bit) only: GVC connection is disabled and an error message is displayed when the system wakes up from sleep or hibernation mode. **Condition:** Occurs when the system goes to sleep or is put into Standby mode. **Work Around:** Disable the VPN connection before switching to sleep or hibernation mode. Alternatively, disable power saving features like sleep mode or hibernation while a VPN tunnel is open.



- **49452: Symptom:** GVC will not initiate IKE negotiations on Vista (32 bit) after the connection is enabled. **Condition:** Occurs when the higher three and half octets of the Virtual Adapter MAC address do not have the following format: 00-60-73-E. **Work Around:** If the Virtual Adapter MAC address is changed manually then it MUST be of the following format: 00-60-73-Ex-xx-xx. The upper three and half octets of the MAC address MUST be as shown in this definition. The only customizable digits are the ones shown as x.

Resolved Known Issues

The following is a list of issues resolved in the SonicWALL GVC 4.0.0 release:

- **53830: Symptom:** Windows Vista may crash when it goes to Hibernate/Sleep mode or when it wakes up from Hibernate/Sleep mode. **Condition:** Occurs if GVC is running while the computer is switched to Hibernate/Sleep.
- **53218: Symptom:** The GVC Virtual Adapter (VA) is always displayed in the system tray in a connecting state even when GVC is not in use. **Condition:** Occurs permanently once GVC has been installed, even when GVC is not in use.
- **52456: Symptom:** The GVC virtual adapter fails to renew its DHCP lease while running on Vista. **Condition:** Occurs when the virtual adapter tries to renew its DHCP lease from an appliance configured to use external DHCP servers.
- **52455: Symptom:** The connection status only displays "connecting" while going through the various steps of getting a DHCP lease. The connection status will continue to display "connecting" even if the process fails. **Condition:** Occurs when the Virtual Adapter failed to get a DHCP lease while the status being displayed was "connecting". A new state: 'Acquiring IP' was added to differentiate from the initial connection state.
- **51957: Symptom:** The Global VPN Client is vulnerable to attacks that abuse a format string vulnerability within the client. **Condition:** Occurs when an attacker convinces the user to import the attacker's maliciously crafted configuration file. The file exploits the client's vulnerability to execute arbitrary code in the context of the client itself.
- **51807: Symptom:** The Virtual Adapter's MAC address cannot be retained after a GVC uninstall. **Condition:** Occurs when the VA MAC address is configured manually prior to uninstallation. MAC address is lost even

Release Notes

if the “Retain MAC address” option is selected upon uninstalling.

- **51598: Symptom:** The GVC application freezes when coming out of standby if auto-reconnect is not enabled. **Condition:** Occurs when the computer returns from standby with active GVC connections.
- **50972: Symptom:** Error message “Failed to open IPsec driver”. **Condition:** Occurs when the IPsec driver failed to install during the GVC install on Vista even though no error was displayed during the installation.
- **50845: Symptom:** The Certificate Manager incorrectly shows the imported user certificate status as invalid. **Condition:** Occurs because the User Certificate validity check returns an error code. This can happen if the Basic Constraints were missing or incorrectly set.
- **50790: Symptom:** Vista only: The GVC connection disconnects after 5 minutes. **Condition:** Occurs when NAT ports are not open to allow DPD requests originating from the SonicWALL appliance.
- **49664: Symptom:** The GVC client does not use the route with the lowest metric when connecting to a peer. **Condition:** Occurs when there are multiple routes to a peer with different metrics.
- **49317: Symptom:** The GVC client cannot connect and displays the error message: “Failed to convert peer name X to an IP”. **Condition:** Occurs when the Fully Qualified Domain Name (FQDN) starts with a number.
- **49248: Symptom:** The Virtual Adapter fails to obtain a DHCP lease. **Condition:** Occurs when a second connection is attempted using DHCP after the previous connection failed due to an IKE Phase 1 error.
- **48833: Symptom:** IKE authentication using certificates fails. **Condition:** Occurs when multiple user certificates are imported using the Certificate Manager, and the actual user certificate is not the last one imported.
- **48832: Symptom:** When GVC is configured to use certificates for authentication, it instead prompts users to enter a pre-shared key. **Condition:** Occurs when a user attempts to login for a certificate-based authentication. If the user clicks **cancel** in the Certificate Selection window, a window prompts the user to enter a pre-shared key.
- **48612: Symptom:** GVC prompts users to uninstall GVC 3.x and reboot prior to installing GVC 4.x. **Condition:** Occurs on Vista only when upgrading from GVC 3.x to 4.x. The user can select InstallShield to automatically uninstall or the user can manually uninstall GVC.
- **48597: Symptom:** The Virtual Adapter fails to obtain a DHCP lease. **Condition:** Occurs after a failed connection attempt. This can occur when a connection is disrupted when the computer is put into Standby mode.
- **48550: Symptom:** Vista Only: IKE negotiation fails from behind certain NAT devices. **Condition:** Potentially occurs when GVC fails to use the defined IKE source ports, 500 and 4500 due to conflict with a native IPsec client. **Work Around:** Start GVC application as an administrator. GVC will then disable the native IKE service on Vista. It can then use the defined IKE source ports, 500 and 4500.
- **47986: Symptom:** Vista Only: GVC connecting with ‘tunnel all’ policy will not be able to route traffic to the Internet. **Condition:** The default route for VPN traffic has the same metric as the default route for the physical network card. **Work Around:** The problem existed in GVC beta version prior to 4.0.0.799. If you had this or earlier versions installed, you must do a clean install of GVC 4.0.0.810 to fix this problem.
- **45722: Symptom:** GVC connection properties are not saved when manually changed from default values. **Condition:** Occurs when any subsequent dialog box is cancelled after having configured connection properties, the properties are reset to default values voiding any changes made.
- **40255: Symptom:** RSA messages to the user are truncated. **Condition:** RADIUS responses that are longer than 2 lines are truncated by GVC, displaying the first two lines but not the rest of the message.
- **40254: Symptom:** GVC drops the connection with an error of "Bad user name or password". **Condition:** Occurs when trying to change or update a password to a 16 digit password. GVC is supposed to accept 4-16 digit passwords. It accepts 4 to 15 digits properly, but disconnects when receiving a 16 digit password. The password is accepted however and updated.



Release Notes

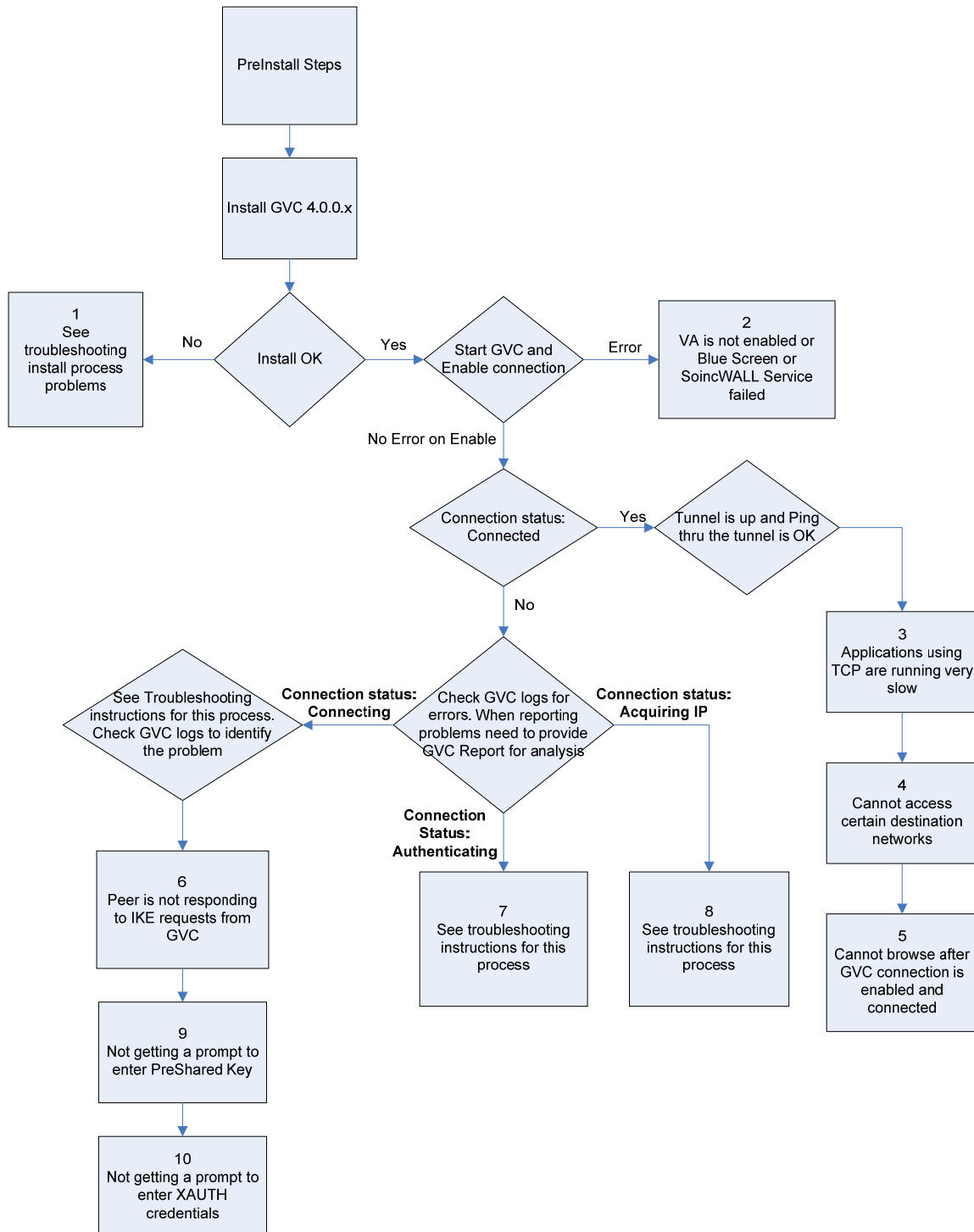
- **34309: Symptom:** GVC 3.x does not save peer gateway specific pre-shared keys when using redundant gateways in a connection. The user is forced to re-enter IKE PSK information every time. **Condition:** Occurs when using a DNS server that resolves peer gateway FQDN to multiple 'A' records (multiple IP addresses) as a form of load balancing. GVC does not save the peer gateway specific IKE PSK information.
- **33107: Symptom:** Logoff scripts fail if they try to run a command after the tunnel has been disabled. **Condition:** Occurs when a command is run after the VPN tunnel is closed.

Release Notes

Troubleshooting

The following is the troubleshooting procedure for the SonicWALL GVC 4.0.0 release:

Trouble Shooting Process for GVC:



Release Notes

Note: If you need to debug run time problems after a successful GVC install, refer to the GVC logs to detect the error condition(s). Some problems may also require information from the firewall logs. Reporting GVC run time problems to technical support requires that you submit GVC and/or Firewall logs for analysis.

Troubleshooting

Detailed troubleshooting processes are explained for the following issues:

- Debug Install Issue
- Post-Install Errors
- TCP Applications on Vista are Slow
- Cannot Access Certain Destination Network
- Cannot Browse the Internet After GVC Connection is Enabled and Connected
- Peer is not Responding to ISAKMP Requests from GVC; Check GVC Logs to Verify
- Stuck on Authenticating When GVC Connection is Enabled
- Failed to Obtain DHCP Lease for the Virtual Adapter
- Not Getting a Prompt to Enter a PreShared Key (PSK)
- Not Getting a Prompt to Enter XAUTH Credentials

Process 1: Debug Install Issue

Note: If GVC was an upgrade install then first uninstall GVC, reboot your computer and then run setup again. If you encounter an error follow the troubleshooting instructions.

A) Blue Screen during Install Process:

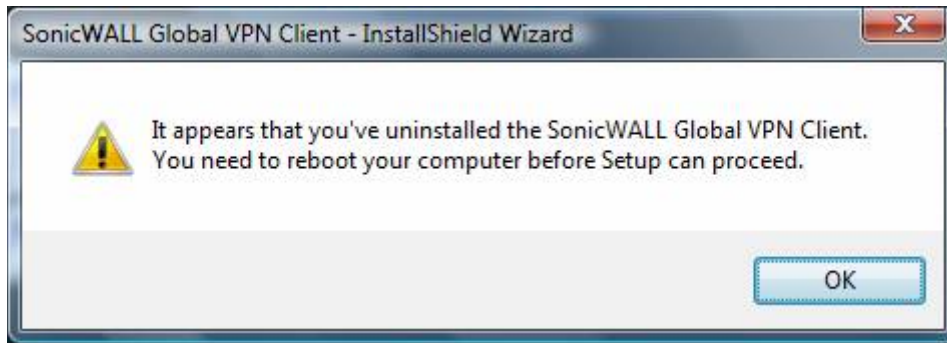
After the upgrade to GVC 4.0.0.x if you get a blue screen, provide the following file
%SystemRoot%\Minidump.dmp (%SystemRoot% is usually C:\Windows) to Tech support in order to troubleshoot further.

For someone who can reproduce the BSOD, choosing 'Kernel memory dump' could be of even more help as it should have more information. To get detailed memory dump need to set the following;

Start->Computer, right click on 'Computer' and select 'Properties'. Choose 'Advanced system settings' and then choose 'Settings' under 'Startup and Recovery'. The settings are under the 'System failure' section. The dump file will by default be written to the %SystemRoot%\MEMORY.DMP file.

Release Notes

B) GVC install fails due to the following error:



This error could happen in the following cases;

- a) Installing GVC without a reboot after GVC uninstall.
- b) Hard reset during the install operation.
- c) GVC install is an upgrade from an earlier GVC Beta version.

Reboot your computer and then run setup again. If it still results in the same error then do the following.

- 1) Right click on the Command Prompt icon and select 'Run as administrator'
- 2) Change directory **%SystemRoot%\system32\drivers** (%SystemRoot% is C:\Windows)
- 3) Type net stop rcfox (You may see either return success or failure)
- 4) Then rename rcfox.sys to rcfox.sys.bak (If rcfox.sys exists in this directory)

Now run setup again and install GVC.

C) GVC Install is stuck while installing the SonicWALL Virtual Adapter:

You may have to do a hard reset if the installation is stuck during the install of the Virtual Adapter. After power up, uninstall GVC and reboot your computer. Now verify that SonicWALL Virtual Adapter does not exist. Go to Start->Control Panel->Network and Internet->Network and Sharing Center->Manage network connections page. If it still exists after GVC uninstall it is most likely due to registry corruption during the hard reset.

Manually uninstall SonicWALL Virtual Adapter as follows; Go to Start->Computer, and right click on 'Computer' to select 'Properties'. Choose 'Device Manager' and then choose 'Network adapters' to select 'SonicWALL VPN Adapter', right click and Uninstall this adapter. Also check 'Delete the driver software for this device'. Then go to %SYSTEMROOT%\System32\Drivers directory and delete RCVPN.SYS. Reboot your machine. After power up install GVC again.

D) GVC Install fails due to following error:

"RampartSVC Module has Stopped Working"

This error indicates that the installer failed to install SonicWALL services. Run GVC installer for the second time.

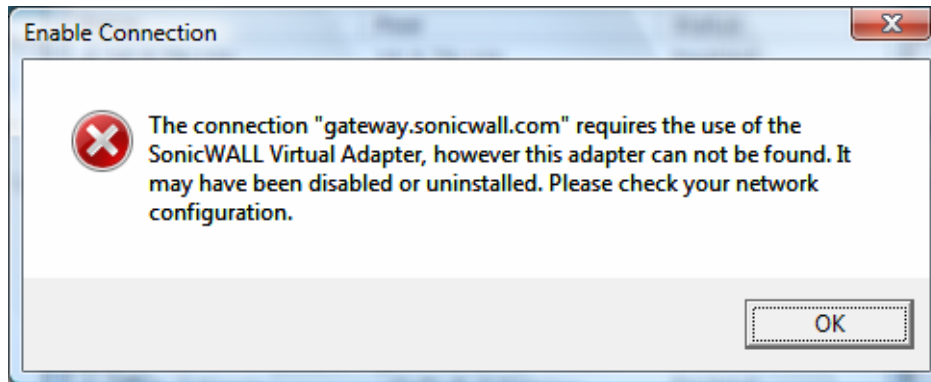
Release Notes

Process 2: Post-Install Errors

These problems are seen after the successful install.

- 1) Virtual Adapter (VA) is not enabled.
- 2) Blue Screen
- 3) Failed to run SonicWALL service.

VA is not enabled:



- A) GVC has a new checkbox option, "Disconnect the virtual adapter when not in use". This checkbox is located on View->Options->General tab. ONLY if it is checked, uncheck it, exit and restart GVC and enable the connection again. If VA is still disabled, then go to step B.
- B) On Vista go to Start->Control Panel->Network and Internet->View network status and tasks->Manage network connections.

Then right click on SonicWALL Virtual Adapter->Properties->Configure button. If the VA is disabled then you need to enable it here.

Now start GVC application and enable the connection again.

Blue Screen:

Network Adapter Card drivers: Check if you are using the latest driver for each Network Adapter card installed on your computer. If it is not, then you have to first upgrade to this latest version of the driver and then run GVC again.

Trend Micro firewall: If you have installed this client based firewall, then check to make sure it is the latest version from the Vendor Website. If it is and you are still getting Blue screen, then disable the Trend Micro Common firewall driver binding from the properties of the Virtual adapter. On Vista, go to Start->Control Panel->Network and Internet->View network status and tasks->Manage network connections. Select SonicWALL Virtual adapter and right click to select properties and then disable Trend Micro Common firewall driver binding.

If the blue screen still persists then you need to provide the following to tech support for further investigation.

After the upgrade to GVC 4.0.0.x if you get a blue screen, provide the following file
%SystemRoot%\Minidump (%SystemRoot% is usually C:\Windows) to Tech support in order to troubleshoot further.



Release Notes

For someone who can reproduce the BSOD, choosing 'Kernel memory dump' could be of even more help as it should have more information. To get detailed memory dump need to set the following;

Start->Computer, right click on 'Computer' and select 'Properties'. Choose 'Advanced system settings' and then choose 'Settings' under 'Startup and Recovery'. The settings are under the 'System failure' section. The dump file will by default be written to the %SystemRoot%\MEMORY.DMP file.

Failed to run SonicWALL Service:

Open a DOS command prompt window by right clicking on the icon and select 'Run as administrator'. Change directory to GVC install directory, (Usually \Program Files\SonicWALL\SonicWALL Global VPN Client) and type the following commands.

```
Net stop Rampartsvc  
Net start Rampartsvc
```

Process 3: TCP Applications on Vista are Slow

The issue is caused by Windows Scaling being handled incorrectly by the firewall device. To manually disable windows scaling, run the following command from the command prompt:
"netsh interface tcp set global autotuning=disabled"

Refer to the following URL for more information on this problem:

<http://support.microsoft.com/kb/934430>

Process 4: Cannot Access Certain Destination Networks

- A) From GVC menu select, File->Properties->Status tab. In the connection section, select Details button. Verify the destination network you are trying to reach, exists in the Destination Proxy IDs list. The information is user specific and can be controlled in the Group VPN Policy on the firewall. This verification can also be done from a GVC report and can be found under the following heading;

- i. Destination Networks
- ii. -----
- iii. 192.168.0.0/255.255.255.0/BOOTPS: Phase 2 Complete
- iv. 192.168.0.0/255.255.255.0/Any: Idle

This destination proxy ID list is generated on a per user basis so it is possible the user access list is missing the required destination networks.

- B) If Step 1 is verified and it still fails, then verify the route to and from the destination network is correct on the firewall side. This may require a packet capture either on the SonicWALL appliance or an external packet capture on the host you are trying to reach.



Release Notes

Process 5: Cannot Browse the Internet after GVC Connection is Enabled and Connected

Generate GVC report (Help->Generate Report menu) and verify if the policy is a tunnel all policy. Check that the default route points to the correct interface. If the policy is tunnel all, then a packet capture on the SonicWALL appliance should provide information if the packet is dropped at the firewall due to an incorrectly configured or unavailable rule to route the internet packets. In order to help trace this, start a continuous ping from GVC client to 4.2.2.2 and use the packet capture utility on the firewall to trace the packet destination.

Process 6: Peer is not Responding to ISAKMP Requests from GVC; Check GVC Logs to Verify

- A) Verify host running GVC application has internet connectivity and can browse the internet. If not then fix this problem and then go to Step B.
- B) Verify the Peer gateway is running and the <zone> Group VPN policy is enabled. If you have other GVC clients connecting to the same firewall on the same interface of the firewall then this is not a problem. Go to Step C.
- C) GVC works from certain locations and this error message only shows up when you are behind certain NAT device. There are two possible scenarios.
NAT device is blocking IKE traffic from GVC (Vista OS) since it is not using defined UDP source port (500) for IKE. This is currently only a problem with GVC running on Vista. In order for GVC to use the defined IKE source port, start GVC by right clicking on the icon and then select 'Run as administrator'. If GVC still cannot connect then go to Step D
- D) It is possible that this NAT device is blocking IKE traffic hence requires a rule (policy) to allow IKE packets from GVC.

To verify if the IKE traffic from GVC is reaching the Peer gateway, use the event logs (Network Debug Category enabled) or packet capture on the SonicWALL appliance. If the Peer gateway does not get the IKE packets then it is the NAT device in the middle or ISP that is dropping the IKE packets. Consult the NAT device manual or ISP to troubleshoot this problem.

Process 7: Stuck on Authenticating when GVC Connection is Enabled

Important: Check GVC logs to get the state of the connection progress. Most likely causes:

- A) Group VPN Configuration error on the Firewall. Check if the user has VPN access list assigned. (With or Without XAUTH this is required)
- B) GVC logs show Phase 2 error. This should never happen with GVC. Delete the connection and create a new one and then try to connect again. The user has to enter the preshared key if the firewall GroupVPN setting "Use Default Key for Simple Client Provisioning" is not enabled. They will also enter their XAUTH credentials as they normally do on new connections, if the firewall XAUTH checkbox is on for GroupVPN
- C) GVC logs shows Phase 2 error. This should never happen with GVC. Delete the connection and create a new one and then try to connect again. The user has to enter their XAUTH credentials and the preshared key if default provisioning key is not enabled.
- D) Check if the firewall has license for GVC connection. If it has then check if the number of concurrent GVC connections does not exceed the licensed number.



Release Notes

Process 8: Failed to Obtain DHCP Lease for the Virtual Adapter

Note: Try a reboot first. If that does not help follow these steps:

- A) Verify that no 3rd party IPsec VPN clients are installed on your computer. Uninstall any existing IPsec VPN clients (including GVC), reboot, and then install GVC again.
- B) Dell Wireless WLAN 4.10+ wireless network driver includes VLAN Priority Support which conflicts with getting a DHCP lease for the SonicWALL Virtual Adapter. Check if VLAN Priority Support is enabled. If it is, disable it by performing the following steps:
 - 1. Right-click **My Computer** on the desktop and click **Properties**.
NOTE: If there is no **My Computer** icon on the desktop, click **Start** and right-click **My Computer** on the right column of the **Start** menu.
 - 2. When the **System Properties** window appears, click the **Hardware** tab and click **Device Manager**.
 - 3. When the **Device Manager** window appears, click the <+> next to **Network Adapters** and double-click **Dell Wireless WLAN Adapter**.
 - 4. When the **Dell Wireless WLAN Adapter Properties** window appears, click the **Advanced** tab.
 - 5. Scroll down to **VLAN Priority Support** and click to highlight.
 - 6. Select **Disable** from the drop-down menu under the **Value:** field.
 - 7. Click **OK** to close the **Dell Wireless WLAN Adapter Properties** window.
 - 8. Click the **X** button in the upper right-hand corner of the **Device Manager** window to close it.
- C) Verify DNE binding is enabled for the SonicWALL Virtual Adapter. Go to Start->Control Panel->Network and Internet->Network and Sharing Center->Manage network connections page. Select SonicWALL Virtual Adapter and right click on properties. On the properties page verify Deterministic Network Enhancer binding is enabled.
- D) If this is a new setup, verify configuration on the firewall. Enable Network Debug category logs to show the DHCP transaction messages. Based on the logs you can determine if the DHCP request is received from the client and if the DHCP server responded to this request. If it is an already working setup, and only GVC on Vista is having this problem then go to step B.
- E) If you are running a client-based software firewall on the Vista machine, check if the version is Vista compatible. If it is not, then upgrade to the latest version. If it does not work after the upgrade then add a rule to allow TCP/UDP port 67/68. If this does not fix the problem then go to step C. **(Note: There were numerous problems reported with Norton Internet Security Suite. If you have this software installed then the final try is to uninstall Norton and reboot your computer and then try again)**
- F) Disable the software firewall completely and then try again. If this does not work then go to Step E.
- G) If the above steps fail then here is work around.
 - 1. Run VPN client and enable a connection and it should get stuck at Acquiring IP. (or Connecting if GVC version prior to 4.0.0.830)
 - 2. Disable the VPN connection
 - 3. Go to Start->Control Panel->Network and Internet->View network status and tasks->Manage network connections. Disable SonicWALL Virtual adapter.
 - 4. Now enable SonicWALL virtual adapter.
 - 5. Then enable the connection again.
- H) Change the default setting for this connection for NAT Traversal from Automatic to Disabled. To select the connection, go to File->properties->Peer->Edit tab to change this setting.



Release Notes

Process 9: Not Getting a Prompt to Enter a PreShared Key (PSK)

This could happen due to process 6 error condition above. If that is not the case, then PSK prompt is only available if the Simple provisioning key is not enabled on the <zone> Group VPN Policy. After the PSK is entered for the first time, it is saved in the encrypted configuration file. Unless the PSK in Group VPN policy is changed the PSK is never prompted again.

Process 10: Not Getting a Prompt to Enter XAUTH Credentials

This could happen due to process 6 error condition above. If that is not the case, then XAUTH prompt is only available if it is enabled on the <zone> GroupVPN Policy. XAUTH credentials are allowed to be cached in the encrypted configuration file only it is allowed on the <zone> Group VPN policy.