

---

# AppGate 9.2.3

## RELEASE NOTES

### Changes in 9.2.3

#### Changes in server functionality

1. **The siteinfo script now reports hardware status .**
2. **ag\_webproxy truncated cookies with values containing '=' .**
3. **A Satellite problem was fixed .** Fixed problem with writing faulty/empty ip server addresses in the generated satellite configuration.
4. **IP tunneling now always block ICMP redirects .** This is a minor security improvement.
5. **ag\_sslc.cgi could dump core .** This could happen when a session was "half registered"
6. **Satellite problem fixed .** agsh: generated satellite configuration was bad if a DNS server was defined but there was no search base.
7. **The ag\_webproxy demon could dump core .** This could happen when transforming traffic to SSL (https).
8. **Restore of backups .** Made ag\_restore not choke on file names containing "
9. **SSL module fixed .** ag\_sslc/apache: fixed rewriting problems when SSL front-end was listening on != 443
10. **A double free problem in the SSL module was fixed. .**
11. **A problem with short read i the RDP proxy demon was fixed. .**
12. **A problem with the SSL module was fixed .** It will now set the client.iptunneling/firewall/identd/platform attributes
13. **A problem in the SSL module was fixed .** hostnames are no longer case sensitive.
14. **A problem with radius as account source was fixed .**
15. **A security issue in sshd was fixed .**
16. **Fixed a problem with very large roles .**

#### Changes in the AppGate console

1. **Fixed VLAN configuration .** It was not possible to configure VLAN on some platforms. This was partly a server and a console fix.

#### Changes in the AppGate client

1. **Fixed tab dance in client .**
2. **A problem causing slow debug output wss fixed .**
3. **Support PKCS11 library loading on Mac OS X (10.4 or later) .**
4. **Make sure to trim all property values (trailing spaces caused problems) .**

5. **A problem in the Client for Citrix and Terminal Servers wss fixed .** The agmud process not properly clean up when a client died.
6. **A problem when it could be impossible to select certificate method was fixed .**
7. **Linux xlock problem fixed .** linux xlock integration did not work if the server connection was lost and the user reconnected.
8. **A client debug problem was fixed .** Report correct port number when reporting that we could not open a local listener (and skip the 118n of the number)
9. **Local print function improvement. .** It is now possible to select multiple jobs to print in the client print tab.

## **Changes in 9.2.2**

### **Changes in server functionality**

1. **Security issue in SSL mode fixed.** This version includes a security fix for the SSL module. The problem was that the SSL proxy could mix sessions so one user could sometimes get access to the session of another user.
2. **Server could fail to enable auto start services.** This could happen if the user was using IP-tunneling and the DNS system was slow. The system could sometimes fail to enable auto-started services for users. Users could work around this by manually stopping and starting the service.
3. **Added ability to limit LDAP group searches.** The AppGate server used to download all the groups defined in an AD server. This would become impractical if the AD contained lots of groups. This version therefore adds the ability to amend these searches to download only a subset of all groups.
4. **Sending log events to syslog server could stop working.** A bug in the system caused it to stop sending log events to an external syslog server whenever the network configuration was changed.
5. **Missing attribute handling changed.** Previous versions would end the user session if the user selected a role which contained a component which referred to an attribute which was not set. This version changes the behavior to rather just disabling the service which contains this broken component.
6. **NTP server keys.** Configured NTP server keys were not passed on to the ntpdate command.
7. **SSL file upload problem fixed.** This version fixes an issue in the file access component when used in SSL mode. The problem was that any upload, trough SSL, of a small file which ended with a blank line failed.
8. **Fixed busy-loop in web proxy.** There was a bug in the web proxy which could cause it to go into a busy loop when talking to certain web applications using SSL.
9. **Made RDP proxy more tolerant.** This version of the AppGate RDP proxy is more tolerant against the strange packets which the Microsoft Remote Desktop Connection v2.1.0 (Mac client) would generate when connecting.
10. **Fixed problem with defunct processes.** There was a bug in the server code which could cause ag\_logd to leave defunct processes. This could happen if there was a local command used to process logs.

## Changes in the AppGate console

1. **Fixed bad behavior in remote log GUI.** The remote log configuration panel would not always save the external host name. The screen could also sometimes be completely blank.
2. **Exception when creating new direct access rule.** This version fixes a regression error in the AppGate console which made it impossible to create new direct access rules for satellites.
3. **Reachability checker and SMB.** The reachability checker in AppGate console did not properly understand the SMB server URI entered in file access components.
4. **Changed web access panel URL field.** The URL field has been split into multiple fields and radio-buttons. This should make it easier to see what the expected syntax is.

## Changes in the AppGate client

1. **Fixed bogus "This address is already in use" message.** This issue affected the IP-tunneling driver for windows. It would sometimes cause Windows to show a message saying something like "This address is already in use" when connecting. The message was harmless but should not appear any more.
2. **Applet would not work on non-Windows clients.** The applet version of the client would not start on MacOSX or Linux machines.
3. **Use correct role name in close dialog.** The client could present the wrong role name in the connection close confirmation dialog. This would happen if the connection used multiple combined roles. The client would present the first role name rather than the name "Combined".
4. **Fixed Linux multi user client on 64-bit systems.** The Linux multi-user client did not work on 64-bit systems.
5. **Web access to multiple servers.** Previous versions of the Linux client did not handle web access to more than one AppGate server at the same time.
6. **Can run in Java 1.4 again.** The previous version inadvertently used a couple of API calls not available in Java 1.4. This has now been fixed. But please note that Java 1.4 has been end-of-life'ed from Sun for quite some time now.
7. **Applet checks for supported browser/java combinations.** The AppGate applet will now check the browser and java combination and give an error message when bad combinations are found.
8. **Changed RDP settings.** This release changes the default RDP options passed to the Microsoft client. The changes is that compression is now enabled and the default bit depth is 24 (was 16). This resolves the problems some users have experienced where the connection stopped working when playing videos.

## Changes in 9.2.1

### Changes in satellite functionality

This release includes a satellite upgrade to version 1.3. Any connected satellites will automatically upgrade as soon as the AppGate server is upgraded.

1. **Satellites and load balanced clusters.** Satellites could have problems when connecting to load balanced clusters. The symptoms was that the satellite immediately disconnected.
2. **Keep invalid NAT mappings.** Do not remove NAT mappings from satellite if the satellite address pool is changed so the mappings are no longer valid. Instead the administrator may reassign the mappings or change the pool again.

3. **Show where satellite will connect to.** Show exactly which names/addresses and ports the satellite will connect to in the AppGate console. This should make it easier to spot configuration problems.
4. **Satellite routing issue.** Fixed satellite routing issue which could occur if the satellite pool was very small and the satellite used all available addresses.

### Changes in the AppGate console

1. **Fixed random crash at startup.** This version fixed a synchronization issue in the console which sometimes caused it to crash when connecting to a server.
2. **Allow host routes.** Version 9.2 of the console refused to add host routes. This is now fixed.
3. **"End time should always be now" button in log GUI did not work.** It was impossible to turn this function back on again if it had been disabled.

### Changes in the AppGate client

1. **Bogus IP-tunneling error message.** The client would sometimes show an error message about not being able to remove IP tunneling routes when closing.
2. **Improved performance on Linux and Mac.** The interactive performance of both IP-tunneling and port forwards has been improved in the Linux and Mac clients.
3. **Fixed startup problem on MacOSX Snow Leopard.** This release includes a new Java stub which should work on the latest versions of MacOSX and Java.
4. **IP-tunneling installation on windows.** Changed the default installation to install 2 instances (so it can be used against two servers simultaneously). Also fixed a problem where an upgrade might fail silently.
5. **Unreadable error dialog fixed.** Error dialogs shown by the client could be unreadable if the screen was too small.
6. **Could not start web access services against two AppGate server simultaneously.** There was an addressing conflict in the AppGate client which prevented it from setting up web access services to more than one AppGate server at the same time.
7. **IP-tunneling to multiple servers on MacOSX.** It is now possible to use IP-tunneling to multiple AppGate servers at the same time also when using the MacOSX client.
8. **Better browser detection on Linux.** The client is now better at figuring out which web browser to start when running in a Linux environment.
9. **Port mover installation.** The port mover is a small helper which is needed on MacOSX and Linux. There were numerous problems with the installation and detection of this helper program. These have now been fixed.
10. **Local print crash on Linux.** The client could crash when performing local print on a Linux system.

### Changes in the AppGate server

1. **Latest model of Ax1 would not restart automatically after power loss.** This release fixes a problems where the Dell R210 (Ax1) server would not boot up again automatically after a power loss. This version also fixes a problem where the machine sometimes would refuse to recognize a locally connected USB keyboard.

2. **Using certificates as part of an authentication chain.** It was not possible to use certificate authentication in a chained authentication method. It is possible in this version, but the certificate method must be the first method.
3. **Ag\_stated could crash.** This release fixes two bugs in ag\_stated which could cause it to crash when performing certain attribute-related operations.
4. **FTP proxy did not log file sizes.** A limitation in the built in FTP proxy made it never log the sizes of any transferred files.
5. **Clean clientqueue periodically.** Older versions of the server would send emails every now and then, even if not configured. These would accumulate in a directory on the server and could eventually fill up the disk. This version will periodically clean up that directory to avoid this problem.

## **Changes in 9.2**

### **General changes**

1. **New AppGate Satellite support.** An AppGate Satellite is a small hardware box which can give an AppGate Server local presence on a remote network. The satellite is designed to automatically connect to the AppGate Server, through any firewall or NAT, and to be managed from the AppGate Server. The AppGate Satellite is also available as a virtual image for testing purposes.

With the AppGate Satellite it is possible to allow computers to talk to other computers, through the encrypted link between the AppGate Server and the satellites, without having to log on to the AppGate Server first. It is also possible to use the normal AppGate role mechanisms to control access.

More information about the Satellite can be found in the AppGate manual which is available from [www.appgate.com](http://www.appgate.com)

This satellite support replaces the earlier remote node feature.

2. **Attributes in database.** Most fields in the database now accept an attribute variable on the form `${src.value}`. The attributes are expanded when the user has selected a role. This replaces the old `%{foo.bar}` notation in client commands.

This makes the server even more flexible by now making it possible to customize the actual content of components for individual users.

This change also affects the syntax used by net groups from having been `$GROUPNAME` to `${net.GROUPNAME}`.

3. **Improved web agents.** It is now possible to pass the SSO password on to web agents. The web agent example has been rewritten and now shows how to automatically log on to a Citrix system.

Web agents is a way to achieve single sign on to web applications which do forms-based logins.

4. **Added web access filters for Sharepoint 2007/2010.** This version includes web access filters which are specially tailored to Sharepoint 2007 and 2010.
5. **Direct RDP access.** It is now possible to configure an RDP access component to bypass the RDP proxy in the AppGate Server. The AppGate can not help with SSO in this configuration.
6. **Changed factory default menu.** The factory default menu has undergone significant changes. The possible actions should now be more obvious and there is more feedback.

The factory default menu allows administrators to reset passwords and to reset the system back to the factory default state.

7. **Improved hardware monitoring.** The AppGate Server will now catch more hardware warnings/errors and put the server in a yellow state. This will serve to alert the administrator as soon as possible when any hardware component has failed or is about to fail.
8. **Automatic log file archiving.** Log files older than 180 days are now automatically archived. The archived logs are still present on the server but are not accessible through the AppGate Console. The archived logs can be reinstated manually if needed. How long to keep the log files can be configured in the new log settings configuration panel.  
  
Having a lot of log files available for the console consumes a lot of memory on the server (for managing the indexes). This has proven to significantly affect performance on low end systems with limited amounts of memory.
9. **Masking LDAP/AD bind password.** This version will mask any LDAP/AD bind passwords stored in `appgate.conf`. Earlier versions stored these passwords in the clear.
10. **Enhanced `ag_stated_query`.** The `ag_stated_query` program has been enhanced and now accepts arguments `-a` to list states on all nodes in a cluster and `-n node-name` to list sessions on a specific cluster node.

## Changes in the AppGate Console

1. **New Notifications panel under Monitor and Status.** The new Notifications panel can be used to configure where and how alarms should be sent. On this panel it is possible to configure SMTP server to send reports via and which email addresses to send them to.  
  
This panel is also used to configure where SNMP traps should be sent.
2. **Configure logging via syslog in AppGate Console.** It is now possible to use the AppGate Console to configure external syslog servers to which copies of log events should be sent. This configuration is done in the new Logging panel under System Settings.
3. **New notes area.** There is a new notes area available in the top node of the AppGate Console tree. This area accepts any text and is meant for administrators. The notes are stored in a global file on the server so all administrators will see and edit the same text.
4. **Confirmation dialogs changed to have the safe choice as the default option.** Most confirmation dialogs in the console have been changed so that the default choice is the safe alternative. This alternative will usually abort the requested operation.
5. **Check reachability of servers.** The console will now test that the AppGate Server can establish a connection to servers entered into components. The test works so that the AppGate Server will try to establish a TCP connection to the server:port. The status of the test will be indicated by a small icon to the right of the server name field.  
  
The test happens in the background and the console will pop up a warning dialog when saving a service where the test has not been successful.
6. **Show traffic statistics for SSH sessions.** The console will now show how much data has been transferred in each active session. The values displayed include both how much data has been passed and how much was actually transferred over the wire as well as how much the data was compressed.
7. **Session information panel has been redesigned.** The Session Information panel, where detailed information about sessions can be seen, has been redesigned. The attributes are now presented in a sorted scrollable list. Also the values shown in this panel can now be copied into the clipboard.

8. **Tighter checks on network ranges.** This version of the AppGate Console will automatically check any network ranges entered (like 10.1.1.0/24) and show a warning if the address given is not the first address in the range. It will also offer to correct the first address if needed.
9. **Close connection to cluster when rebooting.** This version of the console will close the connection to the cluster immediately when the administrator has requested a reboot.  
  
Earlier versions would wait for the user to acknowledge that the reboot command had been issued before disconnecting. This could lead to the cluster losing the connection and showing error messages if the administrator did not acknowledge within a few seconds.
10. **Sort list of roles in drop down menu.** This version will sort the list of roles in the drop down menus used when configuring AD group to role mappings.
11. **Improved license dialog.** This version is more tolerant against newlines in the license key when extracting license from the clipboard.
12. **Slight changes to web access panel.** This version add a new check box to the web access component panel which should make it easier to understand when the start URL is used and when it is not.

## Changes in the AppGate Clients

1. **Multiple IP-tunneling connections.** The AppGate Client is now able to use IP-tunneling against more than one AppGate Server at a time. Previous versions were limited to one IP-tunneling session at a time.
2. **AppGate Client for multi user Linux system.** The multi user client for Linux works like the Citrix client. It allows multiple users to each run their own instance of the AppGate Client and a central daemon (ag\_mud) will serve to keep the different sessions apart.  
  
This makes it possible for multiple users to run AppGate Clients on the same Linux server at the same time without interfering with each other.
3. **Screen locker for Linux based terminals.** The AppGate Client can now interact with a special screen locker on Linux. This locker can lock the screen when the user has been idle for a while, and to unlock the screen the user must authenticate to the AppGate Server again.  
  
This functionality is intended for dumb Linux terminals where the user does not have a local account.
4. **Applet version of AppGate Client.** There is now an applet based version of the AppGate Client. The client launched is the same as when using Java Web Start but the mechanism through which it is started differs.  
  
The main differences between this new applet and the applet client from earlier versions are:
  - a. The client launched is the normal AppGate Client. The earlier applet launched the AppGate Connect client which used a different and more spartan GUI.
  - b. The applet is no longer tied to the browser. With the new applet it is just a loader which works as an applet. The loader downloads the files needed and then launches the AppGate Client as a local application. A consequence of this is that the client will no longer be killed when the browser leaves the applet loading window.
5. **Check.exe can check status in Windows Security Center.** The check.exe binary included in the version is able to check the status of Anti Virus, Firewall etc in the Windows Security Center.

Note that this check.exe has been available for download from [www.appgate.com](http://www.appgate.com) for a while.

6. **Various improvements to the login dialog.** The login dialog of the AppGate Client has undergone a number of changes.
  - The list of previous servers is now sorted after login time (last used server is first) and the list is limited to 23 entries.
  - It will now show the port number used if this is not 22. This behavior can be disabled by setting the `gui_hideport` client property to `true`.
  - Previous versions would reset all fields in the dialog when a previously unknown server name was entered. This version will instead keep the settings already made. This is very useful if the server name has been misspelled because the fields will keep their values when the server name is corrected.
  - New guru mode which makes the client always show the server field, even if the server configuration tells it to hide it. Guru mode is enabled by creating a file named `guru_mode` in the directory which holds the `hostkeys` directory.
7. **Support 64-bit Java on Windows and Linux.** This version adds support for 64-bit Java on Windows and Linux. Earlier versions would refuse to load the native libraries when using a 64-bit Java.
8. **IP Tunneling now supported on Linux 64-bit.** This version adds support for IP Tunneling on 64-bit Linux.
9. **Slightly faster login.** A change to the internal protocols made in this version has decreased the number of round trip packets which needs to be sent during the login process.
10. **Crypto algorithm selection removed from client.** It is no longer possible to select which encryption algorithm to use in the client GUI. Instead the client will use the first strong one which the server offers.
11. **Changed the way double clicking on a file works in the File Access Module.** Previous versions would create a temporary local copy of the file and upload it whenever it was changed. The new code will instead create a temporary directory and then upload every file which appears in this directory. This should eliminate any nasty surprises from programs saving the file under another name.
12. **Added missing local print features.** Added missing local print features which allows administrators to set description son printers and a timeout.
13. **agstart has a new "netuse" directive.** It is now possible to issue a client command like:  

```
agstart netuse z: server share
```

to make it easier to map shares when using IP tunneling.

## Removed features

1. **Support for Windows versions earlier than XP SP3.** The clients included in this version may not work on versions of Windows older than Windows XP SP3. It is however still possible to use the older clients on old systems and connect to this new system with them.
2. **Entrust authentication.** The native Entrust authentication has been removed since the needed Entrust libraries are not available for the x86 platform. It is however still possible to use normal certificates issued by an Entrust CA for authentication.
3. **Manual suspend/resume in AppGate Console.** It is not longer possible to manually do a suspend and resume of the network connection in the AppGate Console.
4. **Sync4j configuration panel.** The Sync4j addition for synchronizing calendar information on certain phone models is obsolete and the configuration panel has therefore been removed.

5. **'Cut' menu entry in file access.** The 'Cut' menu entry did not really work, and it is not possible to get it to work either. So it has been removed.

## **Bugs fixed since 9.1.6**

1. **Ag\_userd could fail to pick up changes.** The ag\_userd could fail to pick up changes in AD group to role mappings if it had problems talking to the AD server, even if the problem is temporary.
2. **SSL mode would display 'Login failed' when waiting for OTP.** The SSL login page would have the title 'Login failed' while waiting for the user to enter their OTP password. This has now been fixed.
3. **Fixed ag\_galed 'Packet too small' error.** The IP-tunneling daemon ag\_galed code could sometimes say that a packet was too small even though it was not.
4. **Made radius code more tolerant.** The radius daemon is now more tolerant towards unrecognized attributes in packets from the Radius server.
5. **Fixed proposed gateway for new routes.** The console will now do a better job at guessing the gateway to use for new routes.
6. **Stability issues.** A couple of bugs which could affect stability of various server daemons have been fixed.
7. **It was not possible to create CPU monitoring conditions.** A bug in the AppGate Console, which has now been fixed, made it impossible to create CPU monitoring conditions.
8. **Web fixes for iPhone and Android.** A number of fixes have been done to the SSL module and the built in web pages to make them render better on mobile devices like the iPhone and Android.
9. **Fixed anti-spoofing rules.** The AppGate Server could use too restrictive IP-filter rules when different interfaces contained overlapping routes.
10. **Made client more robust when port-forwards fail.** This version fixes a bug which could cause the client to throw an exception if a port-forward failed on the server. This could happen if the remote server was not responding.
11. **IP-tunneling allows some ICMP packets.** This version of IP-tunneling will let through certain ICMP packets (i.e. fragmentation needed) which are associated with an active TCP/UDP state.
12. **SSL mode could use the wrong single sign on password.** A bug in ag\_ssld could cause it to store the wrong SSO password from the login process. This could happen when using radius auth as part of a chained authentication method.
13. **Upgrade process could fail to report progress of other cluster nodes.** A bug in ag\_mgmtd could hide any progress messages from other nodes than the master node when upgrading.
14. **SSL-mode fixes.** This version fixes a number of issues with web page and URI rewriting in the SSL module. The SSL login page should also render better on iPhone and Android devices.
15. **Client connection properties dialog fixes.** The connection properties dialog in the client would not always show the correct auth method details. There was also a potential client crashing bug in the authentication method code.
16. **User already logged in problem fixed.** The user already logged in warning only worked for users with an unix account. This has now been fixed.

17. **Fixed IP-filter health check.** The IP-filter health check script would not sound the alarm even if IP-filter was turned off. Also added a new option to `ag_watchd inhibit_ipf_test` which disabled the `IP_filter` test.
18. **Changed default SecurID second prompt.** When selecting SecurID authentication the client would default to show one entry dialog (for pin and code). But if the number was out of sync then the server would generate a new query but this time with two fields, one for pin and one for code. This version changes the default behavior of the server to only have one field (for pin and code) in the query.

## **Upgrading to 9.2.3 from earlier versions**

Only servers running version 9.0 or later can be upgraded to 9.2.3. Machines running earlier versions must first be upgraded to 9.0 or later.

The upgrade can be applied without disturbing users who are using the system. But the system must be rebooted in order to activate the upgrade.

### **Upgrading a cluster running 9.1 to 9.1.6**

There is a bug in the AppGate Console version 9.1 (up to and including 9.1.6) which sometimes makes the console only show upgrade progress data from one node in the cluster.

The work around is relatively simple. Before upgrading log on to any node in the cluster and run:

```
secmsg_query | grep ag_mgmd
```

The look for the line which shows where `ag_mgmd` is registered (not the standby lines). This line should also show which node in the cluster the daemon is registered on. Make sure the console is logged in to this node of the cluster before applying the upgrade.

### **Upgrading a cluster running 9.0 or 9.0.1**

There is a bug in the AppGate Console for 9.0 and 9.0.1 which must be taken into account when upgrading a cluster. The upgrade will apply without problem, but the reboot button in the upgrade status window will only reboot one of the systems. The workaround is simple:

1. Do not use the reboot button on the upgrade status screen. Instead just close it once the upgrade is complete.
2. Go to the file system manager panel. There should be a new clone where the upgrade has been applied. Press the button in the boot column to make this clone the next booted clone. Do not press the reboot now button in the dialog which pops up (this is also broken).
3. Go to the top node in the admin tree where there is a shutdown button. Use this to reboot the entire cluster.