

---

# AppGate 9.1.4

## RELEASE NOTES

### Changes in 9.1.4

1. **Various SSL issues fixed.** This version fixes a bug introduced in 9.1.3 which would make the SSL mode stop working on midnight. It also fixes bugs related to the incoming request redirection as well as some memory leaks.
2. **Improved logging.** This version adds a few new log events. The sshd will log why it suspends a session when the client does not respond to alive checks. Improved log message from ag\_userd when it fails to create an LDAP search expression due to missing user attributes. And added an explicit log message telling that a user did not have any roles available when trying to log in (this could be due to access rules etc).
3. **It is now possible to run a cluster in FIPS mode.** In earlier versions it was not possible to run a cluster when the system was configured for FIPS mode. The machines were simply unable to contact each other.
4. **IP-tunneling on Vista.** This version fixes a problem where routes for IP access components were removed when the machine resumed from a standby. This made IP-tunneling effectively stop working for the user. We have only seen this problem on Vista, but the problem could exist on other Windows versions as well.
5. **Added download timeouts to check.exe.** The check.exe included in this version will only try to download binaries for 5 seconds before giving up. This should fix any problems where sessions sometimes hang on login.
6. **Improved email client detection in agstart.exe.** Agstart.exe could fail to start the email client. And it would sometimes start the email client in compose new email mode. This version fixes these problems.
7. **Updated included java runtime to 1.6.0\_17.** The java runtime included with some clients has now been upgraded to version 1.6.0\_17.
8. **ag\_webproxy and RPC over http.** The built-in web proxy had problems coping with RPC over http.

### Changes in 9.1.3

1. **Single sign on password was not always captured.** This version fixes a bug which caused single sign on to not work. The problem was that the password was not always captured for users having access to multiple authentication methods.
2. **It was not possible to create a new web access component.** A last minute change in 9.1.2 turned out to have the unfortunate side-effect of making it impossible to create new or clone existing web access components.
3. **Fixed 'packet is too small' error in IP-tunneling.** There was a subtle bug in ag\_galed which sometimes caused it to sometimes falsely complain that a packet was too small. This led to dropped packets and could give really bad performance through IP-tunneling.
4. **Fixed problem where console could lose contact.** This version fixes a problem where the AppGate administration console could lose contact with the server while performing a backup or performing other data-heavy operations over slow network links.
5. **SSL access now enforces server names.** The SSL module requires that the host name the user uses to access the Appgate server is the same as the host name of the network interface the con-

nection is using. Strange problems will appear if these names do not match. This version includes code in the server which will redirect users to the correct name if they used the wrong name when accessing the system.

This feature can be used to make SSL work in a load balanced environment as well. In this case one can use a round-robin DNS name which steers the user to one of the AppGate nodes. That node will then see that the user did not use the correct host name for that node and redirect the user to the correct host name. The next user may be directed to another node by the round-robin DNS-name and will therefore be redirected to the host name of that node.

6. **SSL module warns if interface names are not fully qualified.** The SSL module will now show a warning if any enabled interface lacks a fully qualified domain name. A short name can be used under some special circumstances but is normally a confusing bug waiting to happen.

## **Changes in 9.1.2**

1. **SSL protocol vulnerability CVE-2009-3555 fixed.** This version works around a security vulnerability found in the SSL protocol. The vulnerability allows an attacker to inject data at the head of the data stream from the client. This only applies to the SSL-module of AppGate. The normal SSH-based AppGate clients are not affected.

The vulnerability is a design issue in the SSL protocol and involves session renegotiation. The only fix is to disable session renegotiation in the server. Due to the nature of the attack this can not be done in the SSL server. This means that SSL connections originating from the AppGate server (for example to the AD server) can not be protected by any AppGate fix. They must instead be protected by updating whichever server they are connecting to.

2. **IP-tunneling signing fixed.** There was a problem in the IP-tunneling signing in 9.1 which made Vista and Windows 7 not realize that the driver actually is signed. This has now been fixed.

## **Changes in 9.1.1**

1. **SSL mode check that user has access to the auth method.** There is a potential security issue that the SSL module does not check that the user really has permission to use the authentication method the user uses.

An user could for example authenticate using radius even though the user did not have access to radius according to the AppGate configuration. The user could do this if the AppGate server was configured to list radius as one of the authentication methods for SSL. The user still had to be able to complete the radius challenge in order to do this.

2. **IP-tunneling problem fixed.** The `ag_arpd` daemon could crash if the server had a virtual interface which did not have an ether address. This would effectively make it impossible to use IP-tunneling. It only happened for certain types of interfaces (like `e1000g`).
3. **Web access component problems fixed.** This version fixes problems with web page rewriting, URL rewriting and cookie handling.
4. **Swivel Pinsafe authentication method support.** Added support for Pinsafe authentication. This is an authentication method which builds on challenge images and a pin-code.
5. **ag\_stated\_query can print data for one session.** `ag_stated_query` can now take a session id as argument and will then only show that session. Also fixed a bug which caused `ag_stated_query` to print the session id in network byte order.
6. **Support more than one interface per network.** It is now possible to connect more than one interface per host to one network. This makes it easy to make a system listen two two different IP-addresses on one network. It was possible to achieve the same effect earlier by defining multiple instances of the same network.

7. **Chained auth for LDAP fixed.** Version 9.1 required that LDAP users using a chained authentication method also had access to each of the included submethods separately.
8. **Wrong auth method was logged when using chained auth.** The server logged the user as having used one of the submethods when actually using a chained authentication method.
9. **IP\_tunneling driver now supports Mac OS X Snow Leopard.** Earlier versions of the IP-tunneling driver do not work on Mac OS X 10.6 (Snow Leopard).
10. **Fixed problems with UTF-8 characters in certificates.** There were problems using CA and user certificates which used UTF-8 characters.
11. **Do not filter out non us-ascii characters when printing logs.** Earlier versions would replace any non us-ascii character in the logs with a '#' when showing the logs with logcat or forwarding to an external syslog host. This version will not be that aggressive, instead it will only replace control characters.
12. **Fixed problem with pre-logging from client.** The server has a feature where it can accept log events from the mobile client before the user has logged in. A bug prevented this from working in 9.1.
13. **Fixed bug in ag\_distd.** There was a bug in ag\_distd which could cause it to crash if it failed to open a temporary file.
14. **Fixed configuration upgrade on restore.** A bug caused the server to not upgrade the configuration and database if a backup from 9.0 was restored.
15. **Fixed console communication error.** There was a concurrency problem in the console communication code. This could lead to the console receiving data out of order from the server and would result in various mysterious errors.
16. **AppGate console did not disconnect cleanly on reboot.** The AppGate console did not always disconnect immediately when the server was rebooting. This could cause the console to pop up various warnings about lost contact etc. The console could also hang if a reboot was cancelled.
17. **Fixed filter selection in web components.** It was not really possible to select a customer web filter for web access components.
18. **Update AD role mapping when role name is changed.** Earlier versions did not properly update the AD group membership to AppGate role mapping when the AppGate role changed name.
19. **Fixed account expiration setting.** Earlier versions had a bug which made it impossible to change the month in the account expiration date pop up on Linux. It was however still possible to enter the date manually.
20. **Paste license from clipboard is smarter.** It will now handle licenses where the key has been split into multiple lines.
21. **Fixed AppGate console table update bug.** A bug in the table updating code of AppGate console made newly added elements not show up until the item was saved. This could for example happen when attaching existing services to a role. This has now been fixed.
22. **Fixed some cases of unresponsive close button.** This version fixes some cases where the close button might be unresponsive.
23. **Fixed spaces in client commands on Windows.** Earlier versions had a problem which made it impossible to have a client command path with spaces in it on the windows platform. This version fixes that so spaces can now be used if the path or argument is enclosed by quotes.

## **New and changed features in 9.1**

1. **New chained authentication method.** It is now possible to create new chained authentication methods. A chained authentication method consists of two or more other authentication methods. The user must complete all the included authentication methods (and in the right order) to be logged in.

This can be used to combine for example Kerberos and Password or Radius and password authentication. The client login screen will adjust itself to the auth method and will ask for all needed data in the first dialog.

2. **Authentication prompts.** The labels of the various authentication data fields presented during login have been changed. The default label is now the name of the relevant authentication method.

For example, if the password authentication method is named "Password" then the label for the password field in the login window will be "Password". But if the method is renamed (in the AppGate console) to "Magic Cookie" then the label will also change to "Magic Cookie".

These labels can also be customized via the normal client settings mechanism.

3. **Radius.** This version adds the ability to use any password from a Radius exchange for further SSO. The administrator can define which answers the server should look for and use.

It is also now possible to customize the initial prompt for Radius authentication.

4. **Web proxy is more configurable.** The web proxy can now handle application-specific rewrite rules. The new system lets the administrator specify the application in the web access components. This solves the problem where different applications require different, conflicting, rewrites.

Note that any old filtering on URLs will not be converted to the new syntax. The administrator must reenter these URLs manually.

5. **Connect client and applet have been removed.** The AppGate connect client (which was a light-weight client) and applet have been removed. An applet version of the ordinary client will appear in the next version.

6. **SSL mode can autostart services.** The SSL module will now automatically open any web-pages in auto starting services when the user logs in.

7. **Client configuration save location changed.** The AppGate client will now save hostkeys and configuration files under the APPDATA directory when running under Windows XP and Vista. The client will still read configuration from the previous location but new files are saved at the new location.

8. **Client can close when RDP session is closed.** The existing auto-close feature has been enhanced so that it can also react on RDP sessions. This means that it is possible to configure the client to automatically exit when the last RDP session is closed.

9. **Kerberos auth is more tolerant.** The client now also accepts a short name of the server when using Kerberos authentication. Previous versions required either a fully qualified name or an IP-address.

10. **Siteinfo can upload files to appgate.com.** The siteinfo command has been enhanced can now automatically upload the report to appgate.com if the administrator so chooses.

11. **Warn about clock differences.** The AppGate console will now warn if the clock on the client machine and the AppGate server differs too much (more than 24h).

12. **AppGate Free Edition ovf image added.** The AppGate free edition is now also available as an ovf (Open Virtualization Format) image. This can, for example, be used with newer versions of some vmware products.
13. **AppGate clients tested on Windows 7.** The AppGate clients and IP-tunneling driver have now been tested on Windows 7
14. **New attribute login.cert\_expires\_days.** There is a new attribute login.cert\_expires\_days which is set when the user uses a certificate to authenticate. This attribute contains the number of days until the certificate expires.
15. **Configure faculty on syslog events.** It is now possible to configure the faculty used when exporting log events to a separate server.
16. **List of banned passwords updated.** The list of banned passwords has been updated. These are passwords frequently seen in brute-force attacks. It is by default not possible to log in if the user password can be found in this list (this can be changed in the password panel). The default list includes the following passwords (where %u is the user name): "%u", "%u123", "123456", "password", "%u1", "%u12", "test", "passwd", "123", "test123", "1234", "12345", "%u%u", "%u1234", "changeme", "qwerty", "root", "abc123", "1q2w3e", "scricideea", "admin", "111111", "12345678"
17. **Create private keys without password.** It is now possible to create key pairs (for public key authentication) without a password. These keys are very useful for unattended logins.
18. **Changed client behavior on empty passwords.** Previous versions of the client would pop up a password dialog if the user left a password field blank in the login dialog. This version will instead send that empty password to the server directly.

## **Bugs fixed since 9.0.1**

1. **Avoid duplicate log id.** There could be log id collisions when switching between different clones.
2. **Console listed wrong ports for Ax4.** The console did not show the correct port labels for the new Ax4-machines (based on Sun X4140)
3. **Use local characters as auth method name.** It was not possible to use non us-ascii characters in an authentication method name.
4. **Web access hostname comparison was case sensitive.** The web proxy required that the server name exactly matched the case of what was written in the component.
5. **Log id was not included in all syslog events.** The log id of the session was not included in all events sent to a remote syslog server.
6. **Backup problems.** The backup could fail if a file name contained a non us-ascii character, and ag\_mgmt could therefore crash.
7. **NTLM proxy auth could fail.** The client could fail to authenticate against an NTLM proxy due to a missing MD4 digest class file.
8. **Web proxy could mix data from requests.** There was an instance where the web proxy could prepend data from a previous request to a request.
9. **Problems when listing many active sessions.** A number of different problems could assert themselves when listing the active sessions if there were a lot of sessions.
10. **Console could fail to connect.** The AppGate console could fail to connect to the server and wrongly complain that the user does not have access to the administrative service.

11. **Not all cluster members were rebooted.** The console only rebooted one cluster node after an upgrade or when changing the active partition.
12. **Terminal window could freeze.** The terminal window could freeze if it was resized at the same time as new data was being printed.
13. **Radius daemon would send double messages to server.** The radius daemon could send double radius auth requests to the radius server if the user entered the wrong data.
14. **IP-tunneling errors.** The management daemon could crash if there were too many IP-tunneling pools. It was also possible to get crashes when the pool was all used up. Finally a newly added pool could disappear in the console before it was committed.
15. **AppGate clients did not detect Windows 7/2008(R2).** The AppGate clients did not correctly identify Windows 7 and 2008(R2).
16. **RDP proxy could fail with Windows 2008 SP2 servers.** There were problems with the licensing which were fixed by handling all license requests in the proxy.
17. **File access GUI could hang.** This happened when renaming a newly created directory while in the details view.
18. **Client service icons were not updated in tree mode.** The client service icons were not updated immediately when a service was started while in tree mode.
19. **Problems with attribute setting script.** There were problems with the attribute setting script which was not always used, and some environment variables were inaccessible.
20. **Ssl daemon could crash.** The ssl daemon could crash if the user had an empty folder.

## **Upgrading to 9.1.4 from earlier versions**

Only servers running version 9.0 or later can be upgraded to 9.1.4. 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 from 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.