

---

# AppGate 8.2.3

## RELEASE NOTES

### Changes in 8.2.3

#### Client changes

1. **Share mounting fixed.** This version fixes a bug introduced in 8.2.2 which made share mounting fail if it was used together with either the IP-tunneling driver or the hostfile writer.
2. **Better Kerberos error logging.** Added more details to the Kerberos error messages. This makes it easier to debug Kerberos configuration problems.
3. **New attribute `ag_client_hosts`.** The client will now set an attribute named `ag_client_hosts` to `true` if it can update the hosts-file.

#### AppGate Console changes

1. **Stricter checks on share components.** The console will now also check that the name of a share component consists entirely of lowercase letters.
2. **Back button could have problems.** Pressing the back (and forward) button could sometimes lead to a seemingly random panel being shown.
3. **Console hang during update issue fixed.** There was a timing-dependent bug in the console which sometimes made it hang with a busy-cursor once the update had been uploaded to the server.
4. **Works better with the Nimbus Java Look & Feel.** Java 1.6.0\_10 and later contains a new Look & Feel mode named Nimbus. Nimbus makes things work a bit differently and this version adapts to that.

#### Server changes

1. **Auth method attribute changed for Kerberos.** The `ag_auth_method` attribute now gets the value `kerberos` for users using Kerberos to authenticate. Earlier versions did set it to `gss-api-with-mic`. Any systems using an access rule to check for Kerberos authentication must change this.
2. **Crypto method access rule behavior changed.** This version changes the way access rules match encryption algorithms. The new code only checks that the initial part of the actual algorithm name matches. For example `crypto{aes128}` now matches both `aes128-cbc` and `aes128-ctr`.
3. **Terminating a suspended session did not really kill it.** Terminating a suspended session removed it from the list of active sessions and made it impossible for the user to resume the session. But the session did still occupy a license and did so until it timed out. This has now been fixed so that the license is also returned when the session is killed.
4. **Better Kerberos error logging.** Added more details to the Kerberos error messages. This makes it easier to debug Kerberos configuration problems.
5. **Improved banned password logging.** Now explicitly logs that a password is banned when the user tries to log in with a banned password. Earlier versions logged an 'unknown error'.
6. **Fixed Java applets in IE7 through SSL proxy.** The cookies generated by the AppGate SSL module were previously marked for http only, which caused IE7 to not transfer these cookies to

any embedded java applets. This version removes this restriction so applets should again be able to make web requests through the SSL module.

7. **Fixed NTLM auth in SSL.** There were problems authenticating to sites protected by the AppGate SSL module when the sites were requesting NTLM authentication and the user used Internet Explorer. This has now been fixed.
8. **Web proxy more forgiving.** The web proxy now accepts requests which have blank lines preceding the actual request.
9. **Ag\_mgmtd could crash when creating a cluster.** There was a bug in ag\_mgmtd which could cause it to crash when creating a cluster.
10. **Fixed problem with empty appgate.conf.** There was a rare case where changing the network configuration in a cluster could lead to an empty appgate.conf file. This happened very seldom but was completely random.

## **Changes in 8.2.2**

### **Client changes**

1. **Client could fail under Java 1.6.0\_10 or later.** The client could encounter an error when running under Java 1.6.0\_10 or later. The symptoms was that the client did show an error dialog immediately when it had logged in and then died. This could happen if the access details tab was enabled. We have only seen this error on Vista.
2. **Applet failed under Java 1.6.0\_10 or later.** The applet would think it was a webstart client and therefore failed to download the configuration file.
3. **Encrypts proxy password.** The proxy password is now encrypted when stored in the client configuration file.
4. **Polish translation.** The AppGate client is now also available in Polish.
5. **NTLM proxy authentication could fail.** This happened when it required the MD4 digest calculation.
6. **Terminal server client could hang.** There was a potential deadlock problem in agmud which could make it hang. This would stop all user traffic from the terminal server it was installed on.
7. **Linux port mover could change permissions on /etc/hosts.** The Linux port mover could change the access permissions of /etc/hosts.
8. **Applet exception on slow clients.** The applet client could get a java exception if the window was too slow to appear on the screen.
9. **Wrong address written in lmhosts file.** The client could write the wrong local address in the hosts file when enabling an IP-access to port 139. The address written was 127.0.0.1 rather than the real address. The logic has also changed to do the same for port forwards to port 445.
10. **Trouble opening authenticated web pages in Java 1.6.0\_10 or later.** The client could fail to open webpages using NTLM authentication when using Java 1.6.0\_10 or later. The symptom was that the user got an extra authentication dialog first which they had to cancel before being able to continue.
11. **Switched to CTR-mode encryption.** There is a theoretical security issue in the aes-cbc encryption mode. An attacker has a very small ( $2^{(-14)}$ ) chance of decrypting 3-5 bytes of a connection. However this attack will destroy the connection and thus disconnects the user, even if it fails. But to be on the safe side we have switched to ctr-mode.

12. **Did not handle commas in client checks.** Commas in client check commands were not handled correctly.

### AppGate Console changes

1. **Table sorting fixed.** A bug in 8.2.1 disabled the sorting of most tables in the console. This release fixes that bug and also adds sorting to more tables in the network configuration area.
2. **Web access panel checks host name.** The web access component will warn if the destination host name is not a fully qualified name (when transforming to https).
3. **Errors when editing a network interface.** There could be error messages when editing a network interface which had just been created.
4. **Got locking error when creating key pair for user.** It was not possible to create a key pair for a user who had just been created.
5. **Horizontal divider could shrink tree portion.** Sometimes when showing the access rules panel the horizontal divider could move spontaneously to the left.
6. **Certificate CRL type problems.** Changing the CRL type of a certificate could reset all the fields for that certificate.
7. **Null pointer exception when adding cluster node.** The console could throw a null pointer exception when connecting to new cluster members.
8. **Fixes for backslash handling.** Ending the description of a component with a backslash could make the database corrupt. Also editing a component with a backslash in the description would double the number of backslashes.
9. **Focus problem in table editing.** It was sometimes impossible to edit data in a table even though it should be possible. This could happen if the previous selected object was in the same column of the table.

### Server changes

1. **Could not find matching session log message removed.** The IP-tunneling module often logged that it could not find a matching session for a packet. This was logged as a suspect event but is actually quite normal since servers often try to send packets even after the client is gone. The severity level of this message has been changed to debug.
2. **SSL-module disable TRACE/TRACK.** The TRACE and TRACK methods have now been disabled in the SSL module since these may be abused for cross-site scripting.
3. **SSL-module allow pass through NTLM auth.** Previous versions of the SSL module did not allow pass through NTLM authentication.
4. **Restore fixed.** A small bug made it impossible to restore backups from the console. Also the AppGate version of the files on a backup must now match the version of the server they are being restored on exactly.
5. **Entrust authentication speedup.** Some unneeded but heavy checks performed during Entrust authentication have been removed.
6. **Webpages could be truncated.** Webpages downloaded through the AppGate could be truncated under some circumstances.
7. **LDAP plugin may think all passwords are expired.** A compiler bug could cause the ldap plugin think that all user passwords had expired. This only happened on sparc-based systems (i.e. not any of the Ax-machines).

8. **Watch daemon could crash.** An error in ag\_watchd could make it crash when the configuration was changed.
9. **Could not allow extra FTP commands.** The ftp proxy refused to run when extra commands had been enabled (like SITE).
10. **Web proxy failed to handle 100/101 status codes.** This happened after the user had been authenticated.
11. **Non us-ascii characters in LDAP/AD passwords.** This version properly supports non us-ascii characters in LDAP/AD passwords.
12. **IP-tunneling pools on virtual interfaces.** The AppGate server failed to handle arp requests on virtual interfaces.
13. **SSL module could show unavailable roles.** The SSL module could show unavailable roles on the logins screen. It was not possible for the user to select any roles they did not have access to.
14. **Check MAC address on boot.** A hardware bug in some interfaces can cause the MAC address to change to a factory default when rebooting. This version checks for that and changes the address to the real value if needed.
15. **IP-tunneling fixes.** Too many users could cause ag\_galed to crash. There was also an error where ag\_galed could erroneously close the connection to the tunneling device thereby stopping all IP-tunneling traffic.
16. **Roaming sessions could time out too early.** There was a bug which could cause roaming sessions to timeout before they should do so.

## **Changes in 8.2.1**

1. **Compression problems fixed.** An appliance which had been upgraded to 8.2 would not support compression when talking to the AppGate clients. Older versions of the AppGate client would refuse to connect if compression had been enabled. This version fixes this issue and re-enables compression.
2. **Ag\_userd could lose temporary accounts.** A locking problem in ag\_userd could cause it to lose all the temporary accounts. These accounts are used for users who do not have permanent accounts. The symptoms of this was that users suddenly could not log on.
3. **Ag\_webproxy could lose part of webpages.** Downloaded webpages could be truncated under some, rare, circumstances.

## **New and changed features in 8.2**

1. **The ability to assign fixed IP-tunneling addresses for users.** This new feature allows the administrator to assign fixed IP-tunneling addresses to users. That is one user will always get the same address. This feature is supported for local users and users fetched from LDAP/AD.
2. **Read-only admin access.** It is now possible to give users read-only admin access. Users with this level of access can see the service database (roles, folders, services components, local users etc) but not change anything. These users can also browse the logs.
3. **IP-tunneling driver signed for Vista.** The IP-tunneling driver included in this release has been signed for Windows Vista (32 and 64-bits). The driver should work with any AppGate client version 7.1.2 or later.
4. **Appgate server may be more tolerant against TCP packets in IP-tunneling.** We have observed one instance where clients (Leonovo T60/T61) running Windows XP SP2 send illegal

TCP packets (with data outside the TCP window). Normally this seems to work just fine but the AppGate IP-tunneling code has strict checks and eventually killed these sessions. The end result was that users failed to transfer large chunks of data through IP-tunneling.

In AppGate 8.2 we added a flag `ag_galed.stricttcpwin` which can be set to zero to relax the TCP window checks. Setting this to zero allows these broken clients to continue to be able to send data. The default value is 1 which means that the current behavior is kept.

5. **Always enable compression.** Compression was disabled on some AppGate servers.
6. **Wrong SSO password could be cached.** The wrong password could be cached and used for SSO when the LDAP password was changed via the client.
7. **Rdesktop failed to mount home directory.** Rdesktop failed to map the home directory via the RDP access component. This applied to those running the rdesktop client on Linux or MacOSX. The local home directory could not be made available on the server.
8. **LDAP searches had trouble with certificates.** There were some problems with LDAP searches in conjunction with certificates. Missing attributes (for example when logging in with an authentication method other than certificate) caused the search to fail and there were a number of case-related problems with attribute names.
9. **Applet crashed with no combinable roles.** The AppGate applet and connect clients crashed if the user did not have any combinable roles available on login.
10. **Console GUI glitches fixed.** A couple of small GUI glitches have been fixed in the AppGate console
11. **Check for multiple default routes.** It was possible to configure a system with multiple default routes. A system with multiple default routes could alternate between them when sending traffic and this could lead to unexpected results. This version will check for this condition and give an error message when encountered.
12. **Upgrading could disable Radius.** Upgrading from a version prior to 8.1 could disable radius authentication for LDAP users. That is users defined in the LDAP database would not get access to Radius authentication.
13. **Userd could be slow to use new configuration.** A bug in `ag_userd` made it still use the old configuration for a while after the configuration had been changed. This could be very confusing when adding or removing account sources.
14. **Improved support for OWA.** This version contains a number of fixes for problems which could appear when running https on the inside against Outlook Web Access.
15. **Totals line in log graphs could be wrong.** Earlier versions could miscalculate the values shown in the totals graph lines on the log panel.
16. **Vista machine could report firewall rules changed on resume from hibernation.** A timing issue could cause a Vista machine to report that the firewall ruleset had unexpectedly changed when the machine woke up from hibernation.
17. **IP-tunneling driver version number upgrade.** The IP-tunneling driver version number was not updated when the code was changed. This had the side effect of making Vista not upgrade the actual driver when installing a new version of IP-tunneling. So Vista users who had the problem where IP-tunneling caused a system crash would continue to have the problem even after an upgrade while users installing it afresh would not experience the issue.
18. **Fixed crash bug in ag\_webproxy.** `Ag_webproxy` could crash if the user session disappeared while a request was being handled. There is no way this could be used to elevate privileges.

## **Connect client and applet will be discontinued**

The AppGate connect client and applet will be discontinued in a future version of AppGate. There will be an Applet version of the regular AppGate client introduced instead of the current Connect based applet.

## **Known issues**

1. **Upgrade fails with "Failed to verify integrity".** See the second paragraph under "Upgrading from earlier version" below.
2. **Passwords with non us-ascii characters may stop working.** Earlier versions (before 8.0) of AppGate used the client's local encoding when sending passwords to the server. This has some serious drawbacks, for example that LDAPv3 expects the password to be encoded in UTF-8. It would also break if the user moved between machines with different encodings.

To solve this, AppGate 8.0 and later recode the passwords to UTF-8 when sending them from the client to the AppGate server. The drawback is that this will make all old passwords which contains non us-ascii characters stop working (since they look differently on the server).

To mitigate this problem, AppGate has a backwards compatibility option where an upgraded system will recode the passwords back to iso-8859-1 (aka Latin1) before checking them or forwarding them to a Radius server. The actual character set used here can be changed. New installations will default to use UTF8.

We highly recommend making sure that the administration password only contains us-ascii characters before upgrading from a version prior to 8.0.

## **Upgrading to 8.2.3 from earlier versions**

AppGate servers running any non-CC version from 6.0 up to 8.2.3 can be upgraded. If a server is running an earlier version, please upgrade to a supported version before upgrading to AppGate 8.2.3.

AppGate versions below 8.0.1 must be manually patched before they can be upgraded. This is because the upgrade certificate these versions require has expired. The patch procedure is documented and the needed binaries are available in known issue #31 on the AppGate support pages ([http://www.appgate.com/support\\_area/known\\_issues/display.php?id=ID-031](http://www.appgate.com/support_area/known_issues/display.php?id=ID-031)).

If a cluster has been manually configured to use load balancing and NAT, then it should be verified that the settings are correct after the upgrade. The upgrade procedure tries to bring over the old settings, but depending on the exact details it may not always be successful. To verify the settings, go to System Settings -> Network/Cluster Management -> Load balancing. If the load balancing settings are incorrect when users connect it may be necessary to manually remove the `agclient.properties` file on the client computer before they can reconnect.

Upgrading an appliance or a cluster of appliances is done via the "Software update" function in the AppGate Console.

When upgrading a software installation cluster where the "Software update" function is not available in the AppGate Console, please contact [support@appgate.com](mailto:support@appgate.com) for advice on how to upgrade.

Note: It is important that date and time is synchronized on all servers in a cluster before any of the servers are upgraded.