
AppGate Client for S60 3rd Edition, version 1.4.0

RELEASE NOTES

1. New and changed features since version 1.3.0

1. **Experimental support for local customization of client dialogues .** Via a configuration file it is possible to customize a small subset of the client dialogue strings. The keywords are prefixed *ag_msg_* and will use built-in default strings if left empty. Only those strings indicated by the configuration file are customizable, currently that is mainly strings used for certificate management.
2. **New configuration options .** *ag_ask_username* when set, the user will always be asked for a username during password authentication. *ag_numerical_passwords* when set, passwords and certificate passphrases will be entered in numerical mode. Both default to false.
3. **Improved support for centrally managed configuration .** Via a configuration file it is possible to manage the settings and to lock selected settings from being changed by the user via the GUI.
4. **Protection of certificate and private key .** The client now uses the available OS mechanisms to protect the user's certificate or private key file. On Symbian the client uses the data caging mechanism and moves the certificate to the AppGate client's own private directory which can not be accessed by other applications. On Windows Mobile the file is marked as hidden. A new client check has been created, which tells how the certificate or private key is protected.
5. **The certificate can be removed after too many failed attempts to unlock it .** A new configuration option makes it possible to limit the number of attempts to unlock the certificate. If the user enters the wrong passphrase too many times the certificate is deleted from the device.
6. **The client sends a log message to the server when the user fails to unlock the certificate .** When the user enters the wrong passphrase for the certificate the client will send a log message to the server. For the server to accept this it needs to be running at least version 8.2.2 and the sshd configuration parameter *LogMsgLen* must be set.
7. **New settings screen .** The menu-based settings interface has been replaced by a screen which contains both login settings and advanced settings. The aim is to have a look and feel which is more similar to the built-in settings dialogs on the device.
8. **Support for launching MIDlets .** The client now supports launching installed Java MIDlets through a special client command.
9. **Integration with third-party PKI management .** Two new client commands 'installcert' and 'requestnewcert' makes it possible to distribute and manage certificates with minimal hassle. This requires a configured third-party PKI server. Both commands take the URL of the server as argument.
10. **Hiding of menu and settings entries depending on authentication method .** The menu entry 'Change password' is hidden when using certificate-based or public key-based authentication. The settings entry 'Login name' is hidden and cleared when using certificate-based authentication.
11. **Client suggests connection at startup .** The startup wizard has been replaced by a dialog which asks the user whether the settings screen should be opened, assuming that the required settings are not locked for user modification. If there are enough settings to make a connection, the dialog will instead ask the user whether a connection should be made.
12. **Improved error messages .** When the server name could not be resolved the error message is now "Host not found" instead of a generic error message.

2. Fixed bugs since version 1.3.0

1. **Client could crash when given wrong certificate passphrase .** The client could crash or report an "Out of memory" error while deciphering the user's certificate, if the provided passphrase was wrong. This had the additional consequence that wrong-passphrase-counter events were lost.
2. **A bug caused poor performance in large transfers .** A bug in the client limited the throughput in large data transfers. This affected the Windows Mobile client more than the Symbian based clients.

3. New and changed features since version 1.2.3

1. **Login time and bytes transferred in GUI .** The client now displays the login time and the amount of data transferred in the session. This information is helpful when traffic fees are an issue.
2. **Support for certificate and public key authentication .** The client now supports certificate authentication using a PKCS #12 soft certificate, and public key authentication using a PuTTY private key file.
3. **Choose access point by name .** When using automatic access point selection on S60 devices, the client will now give GPRS/3G access points with "Internet" or "GPRS" in their names a slight advantage over other GPRS/3G access points. This helps in situations where the OS lists, for instance, an MMS access point as a GPRS access point.

4. Fixed bugs since version 1.2.3

1. **Configuration SMS was deleted even if configuration download failed .** If a configuration SMS is flagged for deletion, it will not be deleted before the configuration download has succeeded. This was only partially fixed in version 1.2.3.

5. New and changed features since version 1.2.2

6. Fixed bugs since version 1.2.2

1. **Configuration SMS was deleted even if configuration download failed .** If a configuration SMS is flagged for deletion, it will not be deleted before the configuration download has succeeded.

7. New and changed features since version 1.2.1

1. **AppGate password can be used with mail servers .** When automatically defining a mail account on the device, the password used for logging into the AppGate server can be used in the account. This is driven by a client command option.
2. **Better tolerance for network problems when roaming not available .** The client has improved tolerance for situations where the server is temporarily unavailable, when the roaming functionality is not available. Previous versions were more prone to display an error message and disconnect.
3. **Roaming mode Automatic renamed to On demand .** The roaming mode "Automatic", which corresponds to a combination of auto-suspend and auto-resume in the non-mobile AppGate Client, has been renamed to "On demand", which we think more accurately describes its function.
4. **Ability to upload log messages .** It is now possible to send a number of recent log messages to the server by choosing "Upload log" under "Advanced" in the menu. This functionality is useful for diagnosing problems together with an administrator.
5. **Support for browser bookmarks in pre-FP1 devices .** The client can now create browser bookmarks in the "Web" browser on devices prior to S60 3rd Edition Feature Pack 1.

8. Fixed bugs since version 1.2.1

1. **Mail client kept popping up .** On some phones, the mail client kept popping up every 60 seconds interrupting whatever the using was doing, when the "Keep mail alive" option was enabled and a mail account was defined using the option "-launch".
2. **Provisioning text messages were lost .** The format of the configuration text message has been changed. The previous format contained non-standard characters and this resulted in some messages being lost on the way.

9. New and changed features since version 1.2.0

1. **Support for browser bookmarks .** The client can create browser bookmarks. This is driven by client commands.

10. Fixed bugs since version 1.2.0

1. **Crash on role selection fixed .** The previous version could crash on role selection when only one role was available.

11. New and changed features since version 1.1

1. **Support for provisioning of settings .** The client can download the user's personal login settings the first time it is launched, if a settings SMS has been sent to the device.
2. **Support for provisioning of mail accounts .** The client can set up accounts for mail on the device. This is driven by client commands.
3. **Support for clustering .** The client now supports load balancing and failover within a cluster.
4. **Support for single sign on .** The client now supports the server feature "single sign on", which means that the built-in web proxy authenticates the user to web sites and web proxies.
5. **Support for changing password .** The client now supports the ability to change one's own login password while connected.
6. **Support for multiple Radius servers .** The client now supports multiple Radius servers.
7. **Support for named authentication methods .** The client now supports custom names which the administrator can assign to various authentication methods. For instance, one Radius method might be called "Nordic Edge". As a result of this, the method "Radius + SMS" has been removed and the ability to catch password SMS:es is enabled for all Radius methods.
8. **Support for combinable roles .** The client now supports the ability to choose all available combinable roles together.
9. **Support for user message component .** The client now supports the "User message" component.
10. **Support for web access components .** It is now possible to use web access components. However, this requires that the browser is configured to use the AppGate web proxy, and naturally the browser will not work unless connected to the AppGate server.
11. **Support for keeping mail client alive .** The Symbian operating system may shut down the mail client without notice when running low on memory. The AppGate client can now relaunch the mail client whenever it gets shut down.

12. **One-time password SMS messages are caught even if delayed .** The client will now wait indefinitely for a one-time password SMS message, while giving the user the option to fill in the password manually, or give up waiting.
13. **Time to suspend automatically is raised to three minutes .** When using Automatic roaming, the client will now wait three minutes instead of one minute before suspending due to inactivity.
14. **Resume is retried every two minutes .** When using Manual roaming, the client will now wait two minutes instead of five minutes before retrying a failed automatic resume.
15. **Faster to start and shut down .** The client has been optimized internally so that it is faster to start and shut down.
16. **Failure messages are sent to server .** When client commands and client check commands fail to execute on the device, error messages are sent to the server through attributes.
17. **Client detects loss of network coverage faster .** When the device loses network coverage, the client will respond within seconds. The previous version could need minutes to respond to the situation, or not respond at all.

12. Fixed bugs since version 1.1

1. **Some one-time password Radius prompts were not recognized .** The client required a very strict formatting of the Radius prompt asking for a one-time password sent over SMS. Now the client is more flexible, but still requires a keyword such as "one-time" to be present.
2. **Message Of The Day was displayed at every login .** The client now remembers the last Message Of The Day that was displayed, and will not display it more than once.
3. **Network connection was not refreshed when resuming .** The client will now release the network connection when suspending, and open a new when resuming. This increases reliability, as network connections, on some devices, may stop working properly until renewed.
4. **The client could freeze while trying to connect .** In some situations, the client could freeze for a long time while trying to connect or resume, even if it eventually would succeed. This process is now done in the background and can be canceled.
5. **The client would display roles that were not available .** The client would display roles that the user was a member of, but which were not available at the moment. This has been fixed.
6. **It was not possible to enter empty text .** It was not possible to hit "OK" when an input dialog was empty. This was temporarily fixed with a question when pressing "Cancel", but has now been fixed properly.

13. Known issues

1. **Client fails to resume .** The client may fail to resume a connection if large amounts of data are waiting to be transferred.
2. **Log messages are not sent during remote certificate renewal .** During remote certificate renewal, passphrase errors for the old certificate are not logged.
3. **Incompatibility warning on S60 5th Edition phones .** During installation on a S60 5th Edition phone an incompatibility warning will pop up. S60e5 is not 100% backwards compatible with S60e3. They differ at a handful of API calls, none of which are used in the AppGate mobile client.
4. **Window handling glitch after power save .** When a dialogue is left open until the screen goes blank from the power saving function, the dialogue will be hidden due to an incomplete rewrite of the screen.