
AppGate Client for Windows Mobile, 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 **New settings screen .** The menu-based settings interface has been replaced by a screen which contains both login settings and advanced settings.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. **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.
9. **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.

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. **Manual network selection on Windows Mobile .** It is now possible to manually select the desired network on Windows Mobile. This has to be done only once, and acts as a work-around for devices that are configured to use a WAP proxy even if a direct connection is possible. The network choice Manual has been renamed to None. The new choice is named User selected.
4. **Smarter installation on Windows Mobile .** The installation package will now reboot the device, which the user had to do manually before. It will also keep the old settings when upgrading.
5. **ActiveSync account setup disables PC e-mail synchronization .** The client command syncaccount could fail on some Windows Mobile devices, where e-mail synchronization with a PC was enabled. It is a requirement from Microsoft that e-mail can only be synchronized with a PC or an Exchange server, not both. Therefore, the client will now disable synchronization with the PC before enabling synchronization with the Exchange server. This had to be done manually by the user.

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.
2. **ActiveSync account setup did not support odd characters in passwords .** The client command syncaccount did not succeed when the password contained characters such as <, > and &.
3. **Provisioning did not work on some Windows Mobile devices .** On some Windows Mobile devices the client failed to download the settings. This is now fixed by starting the internet connection first.

5. New and changed features since version 1.2.2

1. **Support for registry client checks .** The client supports the client checks -regexists and -regprint, which work the same way as in check.exe.
2. **Support for AppGate Filter in client checks .** The client supports the client check -filterversion, which returns the version of the installed AppGate Filter, if any.

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.
2. **ActiveSync account setup was broken .** The client command syncaccount always resulted in a crash.

7. New and changed features since version 1.2.1

1. **AppGate password can be used with mail and ActiveSync servers .** When automatically defining a mail or ActiveSync 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.

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.
3. **Settings were not deleted on uninstall .** On Windows Mobile, the settings were not deleted when uninstalling the client. This made it difficult to provision new settings.

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.
2. **Support for idle mode .** The client can now detect when the phone comes back from idle mode, and will try to resume if the connection was broken and manual roaming is used.

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 1.0

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 and Exchange synchronization 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 new roaming protocol .** Support for the more reliable roaming protocol, which was introduced in version 8.0 of the AppGate server.
11. **Terminal Services Client can be launched automatically. .** On the AppGate server, a client command can be set, which launches the built-in Terminal Services Client on Pocket PC devices and fills in the server address.
12. **No need to verify the server's host key fingerprint .** The default behaviour of the client is to accept the server's host key at the first connection. Advanced users can turn off this feature before connecting for the first time.
13. **Support for hostname-to-network mapping .** The client now supports the hostname-to-network mapping feature in Windows Mobile, which means that custom network definitions and exceptions are supported.
14. **Client check functionality is built into the client .** No binary file needs to be installed on the server, or downloaded from the server onto the device. This saves time for both administrators and users.
15. **New set of client check commands .** In an effort to standardize the set of client check commands on all mobile platforms, some Windows Mobile-specific checks were removed, such as *-regrprint* and *-downloadto*. At the same time, some client checks targeted at mobile platforms were added, such as *-imei* and *-imsi*. Of the remaining check commands, several have been renamed.
16. **Standardized look and feel on all mobile platforms .** The user interface on Windows Mobile has been changed in order to standardize look and feel on all mobile platforms. The views Log and Advanced have been removed. The views Tunnels and Web sites have been replaced with message boxes.
17. **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.
18. **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.
19. **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.
20. **Faster to start and shut down .** The client has been optimized internally so that it is faster to start and shut down.
21. **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.
22. **Faster login procedure .** The time between authentication and role selection is shorter due to optimizations.
23. **A copy of the previous log file is saved .** If the client would terminate due to some error without the user taking notice, the next activation of the client will start the client anew. In previous

versions, this caused the (valuable) log file to be overwritten. From now on, a backup of the previous log file is saved.

24. **Log file wraps at 1 MB .** The log file will no longer grow to a size of several megabytes. When the size reaches one megabyte, the file is overwritten from the start, so that new messages gradually overwrite older messages.
25. **Client explains why resume fails .** The client can fail to resume for several reasons; the server might be down or the user's session could have timed out. Now the client informs the user about the (probable) reason.

12. Fixed bugs since version 1.0

1. **Some tunnels were not opened .** In the previous version, IPv6 tunnels would often not be opened, depending on the order of components in the server's configuration, and this would cause problems with Internet Explorer and ActiveSync.
2. **Backspace key on Windows Mobile 5 Smartphone did not work .** Under Windows Mobile 5 Smartphone, the Back key is commonly used as backspace in input dialogs, but this requires special support from the application. The client now supports this feature.
3. **Some one-time password SMS messages were not recognized .** The client required a very strict formatting of one-time password messages; no text was allowed after the password. This has been fixed.
4. **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.
5. **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.
6. **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.
7. **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.
8. **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.

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. **One-time password SMS messages are not caught .** Due to a limitation in the operating system, "flash" SMS messages can not be caught. The authentication server must be configured to send ordinary SMS messages. This symptom may also arise if the device is not powered down and back on after the installation of the AppGate client.
4. **A duplicate mail account is created .** Due to a limitation in the operating system, the client can not detect mail accounts created by the user, and therefore it may create an identical mail account. The recommended solution is to delete the user-defined account from the device.