Configuration Server

8.5.000.14

12/21/2025

8.5.000.14

Configuration Server 8.5.x Release Notes

Release Date	Release Type	Restrictions	AIX	Linux	Solaris	Windows
04/25/14	General		X	X	X	X

Contents

What's New

There are no restrictions for this release. This section describes new features that were introduced in this release of Configuration Server.

- DB Server is no longer required for access to the Configuration Database. Refer to the *Framework 8.5 Database Connectivity Reference Guide* for more information.
  If you are going to use the Configuration Conversion Wizard (CCW) to convert your database, you will need the DB Server for the conversion.
- If a natural, man-made, or unintended event occurs at the main site, forcing Configuration Server and other Management Framework components to fail, Genesys now recommends a multi-site deployment model to maintain operations.
- Migration of Configuration Server is improved, enabling the upgrade to occur with minimal downtime and impact to the production environment. Refer to the *Genesys Migration Guide* for more information.
- Configuration Server now supports a flow control mechanism, whereby you can specify the maximum size of memory used to store unsent notifications from Configuration Server or Configuration Server Proxy. When this amount of memory is used, the server stops processing the client requests until the amount of memory used by the unsent notifications drops below the configured threshold. Only then does the server start to process client requests again. Previously, the unsent notifications sometimes accumulated to the point where performance was negatively affected, or Configuration Server or Configuration Server Proxy terminated unexpectedly due to memory starvation.
- Configuration Server now requires a valid license before it will start for the first time with an 8.5 database that has been newly initialized or converted using CCW. Genesys License Reporting Manager (LRM) is also supported; it works with Configuration Server to ensure that each application has a valid license before it can be installed and started.
- Configuration Server now allows you to install language packs to enable support of a particular language in which messages are displayed.
- Configuration Server now allows users to change or remove predefined business attributes, such as Media Type. Options have been introduced to enable this, and to control how predefined business attributes are inherited when additional tenants are created.
- Configuration Server now supports an extended audit trail of all changes in the Configuration Database, including new and previous values. A new utility outputs a report of this information when necessary.
- Configuration Server now supports Kerberos for user logins. Configuration Server can operate with Windows Active Directory and MIT key distribution centers to facilitate Single Sign-on via Genesys UI applications that are Kerberos-enabled.
- All active sessions are immediately invalidated for a user who is disabled in, or removed from, the Configuration Database.
- Configuration Server now supports the following new types of application objects:
  - LRM Server

Helpful Links

Releases Info

- List of 8.5.x Releases
- 8.5.x Known Issues
- 8.5.x Product Alert

Product Documentation

Management Framework

Genesys Products

List of Release Notes

  - Recording Crypto Server
- Configuration Server supports new versions of Database Management Systems and a new virtualization platform. Refer to the *Genesys Supported Operating Environment Guide* for more information.
- Starting with this release, Configuration Server external authentication uses OpenSSL version 1.0.1g for secure connections to LDAP Servers.

Resolved Issues

This release contains the following resolved issues:

Configuration Server Proxy now handles expired passwords and their subsequent resets properly. Users are prompted to change their passwords, and after the change, are permitted to log in to other applications to which they have access. Subsequent logins are permitted using the new password. Previously, Configuration Server Proxy would notify users that their passwords had expired, let them change their password, and then log in, as is proper behavior. But after logging out, Configuration Server Proxy would notify them again the next time that they tried to log in. In addition, once logged in, they were unable to log in to other applications with their new passwords. (MFWK-15673)

Configuration Server now sends correct notifications of a password change by an agent that does not change the user's status as an agent. Previously, when an agent changed his or her password because the Reset Password flag had been set, Configuration Server sent incorrect notifications to its clients that the Person object was not an agent. (MFWK-15466)

When authentication fails, both the master Configuration Server and Configuration Server Proxy close the `tcp` connection, enabling new clients to connect to the master server. Previously, Configuration Server Proxy did not close its `tcp` connection, and after repeated authentication failures, the number of available `tcp` connections available for the process was exhausted, meaning that new clients could not connect. (MFWK-15316)

Master Configuration Server no longer sends incorrect notifications on password reset if a folder containing Person objects is disabled and later enabled. Previously in this scenario, the master Configuration Server sent incorrect notifications about a password reset for the objects contained in the folder, which prevented users from logging in to Configuration Server Proxy until it was restarted. (MFWK-14980 [MFWK-15175])

Configuration Server properly does not propagate new permissions to the child objects contained in a folder when permissions are changed on that folder such that the new permissions coincide with the permissions on its parent object. Previously, newly applied permissions were propagated in the database, but not in the in-memory image of the child objects. The resulting discrepancy between the in-memory permissions and the permissions stored in the database caused database-level errors upon subsequent attempts to change permissions on the contained objects. (MFWK-14962)

Configuration Server now accepts the login of a username containing a \5c byte (backslash character) in a multi-byte character. Previously, a multi-byte username containing this character was not a valid username. (MFWK-14869)

Users in a new Tenant object can be authenticated externally while existing users are authenticated internally by not specifying the **password-min-length** option for the new users. This option is not to be used with external authentication, and the documentation has been updated to reflect that. (MFWK-14816)

The History Logs for Configuration Server and Configuration Server Proxy no longer get out of synchronization in the following scenario:

1. The master server is processing a very large number of configuration updates.
2. The proxy server loses its connection with the master server and reconnects, but cannot restore the session because its History Log has expired.
3. The proxy server disconnects all of its clients to force them to reload data, and starts to reload data from the master server. But while it is reloading data, it is receiving a very large number of configuration update notifications.

Previously in this scenario, Configuration Server Proxy may have lost some notifications for events which occurred while it was reloading data. When the clients reconnected, they received obsolete data.

(MFWK-14542)

TLS connections to a Genesys server running Windows no longer fail if the security certificate is generated using a tool other than Windows certificate services and then manually imported into Windows. Previously, if you used something other than Windows certificate services and manually generated the certificate, the `CERT_TRUST_REVOCATION_STATUS_UNKNOWN` validation error was generated, and the TLS connection to the Genesys server failed. (MFWK-14166/ER# 324547671)

Configuration Server now correctly stores privileges in the Role objects after they were removed then reassigned back to the role. Previously, modified privileges were lost when Configuration Server restarted. (MFWK-14156 [MFWK-15158])

When enabled for multi-language support, Configuration Server now supports strings and section/option names greater than 256 bytes in length if the environment variables are set correctly. Refer to the *Framework 8.5 Database Connectivity Guide* for detailed information about the required environment settings. Previously, strings and names longer than 256 bytes were not stored. (MFWK-14141/ER# 324029037, MFWK-14140/ER# 324029035)

Configuration Server no longer drops responses to external authentication requests that come from the same client within a very short time span. Previously, Configuration Server dropped the response to an authentication request if the next request from the same client arrived before the external authentication server had responded to the previous request. (MFWK-14099 [MFWK-14853])

The default user can now use the GVP Deployment Wizard on a newly initialized database to move Application objects to the Applications folder. Previously, the objects were not moved and the following error was generated:

```
Insufficient permissions to perform this operation
```

(MFWK-14081)

Configuration Server now responds promptly to Advanced Disconnect Detection Protocol (ADDP) when it performs a lengthy atomic operation (such as removing an object with many subordinate objects or serving a large portion of the history log to a client). Previously in this scenario, Configuration Server sometimes did not respond promptly to ADDP, so clients with ADDP timeouts set to smaller values sometimes experienced a disconnection. (MFWK-13830/ER# 315580751)

The backup Configuration Server and Configuration Server Proxy no longer incorrectly process notifications about changes to permissions and accounts. These notifications were lost, and ultimately resulted in the server having incorrect or outdated permission and account data. (MFWK-12759)

Users can now enter up to 255 characters of address data for a Person object. Previously, only a maximum of 64 characters could be entered. (MFWK-10587)

Upgrade Notes

No special procedure is required to upgrade to release 8.5.000.14.