Framework Migration Guide

Management Framework 8.5.1

1/5/2022

Table of Contents

Management Framework Migration Guide

Use this guide to upgrade Management Framework and database schema to 8.5 and later, if required.

For information about migrating to releases earlier than 8.5, refer to the Genesys Migration Guide.

Overview

Compatibility

Feature Availability, by Component

Required Database Schema to Support Available Feature

Secure Protocols Compatibility

Upgrade Components

Interoperability

Local Control Agent

Management Layer Server Components

Configuration Server (and Roll Back)

Upgrade Component Definitions

Loading Latest Locale

Updating the Configuration Database Locale

Upgrade DB Schema

Updating the Configuration Database Schema

Upgrading the Centralized Log Database Schema

Convert Configuration Environments

Converting Single-language Environment to a Multi-language Environment

Converting Single-tenant Configuration

Localized Environments

Upgrading Localized Database

Updating Single-language Database With the Latest Language Definitions

Database to a Multi-tenant Database

Adding and Updating Languages in Multi-language Databases

Migrate to Net-SNMP

Adding Net-SNMP Functionality to a Configuration

Converting Genesys SNMP Master Agents to Net-SNMP Master Agents

Enable New Functionality

New and Changed Configuration Options by Release

Mandatory Changes in Configuration of Framework Components

Mandatory Changes in Secure Protocol Configuration

Configuration Conversion Wizard (CCW)

Installing CCW

Specifying the Database Connection

Using CCW to Migrate Your Configuration Database or Locale

Overview

This page provides compatibility information for upgrading Management Framework to 8.5. To help you decide if you need to upgrade at all, or just upgrade the locale or database schema, it also summarizes feature availability by component, and what database schema is required to support available features.

There are no special steps required. Management Framework software is generally backward-compatible and interoperable, with exceptions noted.

For information about migrating to releases earlier than 8.5, refer to the Genesys Migration Guide.

Management Framework Compatibility

Management Framework components have been designed to work in environments in which different versions are in use. All new versions are backward-compatible, and can be used side-by-side with prior versions of other components, unless noted otherwise. At the same time, components that are part of High-Availability deployments (such as primary-backup pairs of servers), must run the same version and must be upgraded at the same time. There are other exceptions, when certain components should run particular versions when working together; these are noted either in this section and/or in Release Notes.

The level of functionality that you get out of your Management Framework deployment also depends on the combination of the versions of components and database formats being deployed. While newer components can still interoperate with older versions of peer components and/or database schema, some features of the latest Management Framework release may not be available unless you have all related components running specified versions.

Feature Availability

This section describes the availability of Management Framework features and of the database schemas which are required to support them.

Availability of Management Framework Features by Framework Components

The following table indicates the availability of Management Framework features, based on the component in which they were introduced, since the earliest supported release.

[+] Show table

Framework Component Changes In Release 7.6 to 8.5

Component Name	Type of Change	Release	Details

All Framework components	New functionality	8.5	Support for the MS SQL Server 2016 DBMS. Support for the Red Hat Enterprise Linux AP 64-bit x86 7 operating system. If a natural, man-made, or unintended event occurs at the main site, forcing Configuration Server, Solution Control Server, and Message Server to fail, Genesys now recommends two architectures that can be used to maintain operations. Migration of Management Framework components is improved, enabling the upgrade to occur with minimal downtime and impact to the production environment. Instructions for migration to Management Framework 8.5 and later are also simplified, more straight-forward, and less release-specific.
Configuration Database Maintenance Scripts	New component	8.5	New scripts enable you to upgrade the locale and schema of your Configuration Database when needed. Additional tools are included in this component to help you maintain and analyse the performance and data integrity of the Configuration Database.
Configuration Database	New functionality	8.5	The password for the Configuration Database can now be encoded using an asymmetric encryption algorithm, with the encryption and decryption keys stored in external files.
	Changed functionality	8.5	Starting in release 8.5.1, you cannot deploy a new single-tenant Configuration Database. However, you can continue to use your existing database with Management Framework 8.5.1.
	New object types	8.5	Configuration Database can now store the

			following new Application types: • Genesys Knowledge Center CMS (190) • Genesys Knowledge Center Server (191) • License Reporting Manager • Reporting Cryptographic Server
Configuration Server / Configuration Server Proxy	New functionality	8.5	You can now set a timeout for a client to expect a TCP success or failure response from the server to which it is connecting. This timeout applies to the following connections: • Primary or backup Configuration Server Proxy connecting as a client to primary master Configuration Server • Backup master Configuration Server connecting as a client to primary master Configuration Server • Backup Configuration Server Proxy connecting as a client to primary Configuration Server Proxy Configuration Server now supports simplified deployment of Genesys Administrative Applications in environments that use single sign-on. You can now specify a default management port (TCP/IP port) on Configuration Server Proxy that management software uses to monitor and control the operation of the proxy server. This port, and the equivalent port on Configuration Server, open just after the servers are

			initialized. Configuration Server Proxy 8.5, in both primary and backup mode, can, during migration, start and operate against Configuration Server 8.1.3. Support for bootstrap logging (generating logs starting at the very beginning of startup until the main configuration is loaded from the Configuration Database) when starting Configuration Server/ Configuration Server Proxy from the command line. Starting with Configuration Server release 8.5.100.01, you can now migrate 8.1.3 Configuration Servers in an HA pair and using the 8.1.1 Configuration Database schema to an HA pair of 8.5.101 Configuration Servers without any loss of backup functionality. Configuration Server can now use Windows Authentication to access an MS SQL Configuration Database. Configuration Server now supports secure connections to the Message Server designated for the Centralized Log. Configuration Server now supports the following databases: • Microsoft SQL Server 2014 • IBM DB2 10.5 database Configuration Server now supports the VMware ESXi 6 virtualization environment. Configuration Server can now be configured to execute requests, submitted via an internal brief API, taking into account permissions of the parties involved. Separate ports that are restricted for use only by client User Interface type (UI) applications can be configured on Configuration Server and Configuration Server Proxy.

			Secure connections between Configuration Server and an Oracle, PostgreSQL, or Microsoft SQL database can be configured. Configuration Server now checks and confirms that the license file is valid before starting for the first time. Support for Genesys License Reporting Manager (LRM) 8.1. Language Pack support for localization of Configuration Layer. Refer to the "Translation Support" section of the Configuration Server 8.5.x Release Note for information about compatibility of these Language Packs. Configuration Server supports an extended audit trail of changes. A new utility outputs a report of all configuration changes in the Configuration Database, including previous values. New configuration options to handle the treatment of business attributes in the Environment tenant. Configuration Server can be configured to control the flow of responses to client requests, to reduce the risk of unexpected termination due to memory starvation. Clusters of Configuration Server Proxies can now support load balancing using the F5 load-balancer for agent-facing interfaces. For one of the ways in which this functionality can be implemented, refer to the "Load Balancing Using Clusters" section of the *Workspace Desktop Edition Deployment Guide*.
	Changed functionality	8.5	Single-tenant and multi-tenant Configuration Server IPs have been consolidated into one Configuration Server IP, which can be used for configuration environments with one or more tenants. Single-tenant Configuration Servers are still supported, but can no longer be deployed. DB Server is not required for access to the Configuration

			Database.
	Deleted functionality	8.5	Starting with Configuration Server 8.5.101.00, License Reporting Manager (LRM) is no longer integrated with Configuration Server.
Local Control Agent	Changed functionality	8.5	LCA now supports the VMware ESXi 6 virtualization environment. Genesys Deployment Agent is no longer installed automatically with Local Control Agent by default.
Message Server	New functionality	8.5	Support for bootstrap logging (generating logs starting at the very beginning of startup until the log configuration is loaded from the Configuration Database) when starting Message Server from the command line. Message Server can now use Windows Authentication to access an MS SQL Log Database, whether accessing the database directly or by using DB Server with DB Client 8.5.1 or higher. A new Message Server script, **drop_tables_<DBMS>.sql** drops existing tables and procedures, and must be run before the initialization script if you have to re-initialize an existing Log Database. Message Server now supports Microsoft SQL Server 2014. Secure connections between Message Server and Oracle, PostgreSQL, or Microsoft SQL databases can be configured. Hangup detection has been added to the database process thread used by Message Server.
	Changed functionality	8.5	The Log Database initialization scripts no longer drop existing tables and procedures. If you have to re-initialize an existing Log Database, run the **drop_tables_<DBMS>.sql** script before running the

			appropriate initialization script. DB Server is not required for access to the Log Database.
Solution Control Server	New functionality	8.5	Support for bootstrap logging (generating logs starting at the very beginning of startup until the log configuration is loaded from the Configuration Database) when starting Solution Control Server from the command line. SCS now supports secure connections to the Message Server designated for the Centralized Log. SCS now supports the VMware ESXi 6 virtualization environment. SCS now supports Net-SNMP, in addition to Genesys SNMP Master Agent, to provide SNMP functionality. The SCS IP now contains the Application template for a generic SNMP Master Agent, which can be configured to use Net-SNMP or the built-in SNMP functionality of Genesys SNMP Master Agent.
Security Pack on UNIX	New functionality	8.5	Security Pack now uses OpenSSL version 1.0.2j. Security Pack includes a new script **convert_priv_key.sh** that automatically converts private keys in security certificates to other formats. Security Pack sends out intermediate certificates with the endpoints certificate when certificate chains are involved. Genesys Security Pack on UNIX now uses OpenSSL instead of RSA to facilitate communication in the SSL/TLS protocol suite. Security Pack scripts have been changed to use SHA1 by default, with an option to use SHA256.
SNMP functionality	New functionality	8.5	Management Framework can now use a 3rd-party Net-SNMP Master Agent to

			communicate with SNMP-enabled network monitoring systems. New instances of Net-SNMP Master Agents can be deployed along with Genesys SNMP Master Agents. Existing Genesys SNMP Master Agent Application objects can also be migrated to Net-SNMP Master Agent Application objects, enabling the removal of any dependency on Genesys-provided SNMP Master Agents completely.
Logs and alarms	New functionality	8.5	Throttling can be applied to log outputs to prevent a log queue from growing to a size that could impact normal operation of an application. Some log events provide extended information, such as Application type.
External authentication	New functionality	8.5	You can now increase the robustness of the LDAP external authentication connection by enabling this Keep-Alive mechanism (where supported by the operating system). The maximum accepted Kerberos token size has been increased from 12 KB to 64 KB. You can now configure Configuration Server or Configuration Server Proxy to perform case-insensitive searches to identify Persons objects authorized by the Kerberos ticket. This feature is especially useful if you are using Microsoft Windows Active Directory as the Key Distribution Center. Support for Kerberos external authentication for user logins. Configuration Server can operate with Windows Active Directory and MIT key distribution centers to facilitate Single Sign-on for Genesys user interface applications.

			All users in a Tenant can be configured to use external authentication. All users in a Tenant can be configured to be authenticated internally. LDAP Server returns the DN (Distinguished Name) attribute for each entry it searches in LDAP. Configuration Server ignores any other attributes in the **ldap-url** option.
DB Server	New functionality	8.5	Selected applications can be now be configured to access MS SQL Server databases using Windows Authentication, if DB Server is using DB client 8.5.1 or higher. DB Server now supports the VMware ESXi 6 virtualization environment. DB Server 8.1.301 now supports IBM DB2 10.5 databases. DB Server 8.1.3 now supports Microsoft SQL Server 2014. The DB Server 8.1.3 IP now contains database client processes for use with Framework 8.5 databases. When installed (not by default), these new processes enable the configuration of secure connections between DB Server 8.1.3 and Oracle databases.
	Discontinued component	8.5	DB Server is not part of Management Framework 8.5. It is required only if using Configuration Conversion Wizard to convert a database to the current format.
Management Framework-related Wizards	Discontinued component	8.5	All Management Framework-related configuration and deployment wizards are no longer available with Management Framework, except Configuration Conversion Wizard.

All Framework components	New functionality	8.1	Genesys Framework now supports IPv6 on most connections. Genesys Framework now supports the FlexLM 11.9 license manager. TLS as implemented by Genesys is consistent with the Federal Information Processing Standards (FIPS). This applies to those components that support TLS. The minimum permissions required to set up and operate Management Framework are now documented.
Configuration Conversion Wizard	New functionality	8.1	You can use CCW to convert: • An existing Configuration Database from its current character encoding to a multi-language Configuration Database encoded using UTF-8 • A single-tenant Configuration Database to a multi-tenant Configuration Database
Configuration Database	New functionality	8.1	The Configuration Database can now store encrypted data using database encryption capabilities, but only if the Database Management System (DBMS) supports the encryption. (This refers to Transparent Data Encryption (TDE)). Migration is not required for Configuration Database 8.1.1; optional upgrade of locale information using CCW is all that is required. New multi-language environments are supported starting in release 8.1.2. Configuration Database and client databases must be configured appropriately when the database is first created.

External Authentication	New functionality	8.1	LDAP external authentication can now be configured on Configuration Server Proxy so authentication requests will be performed directly without forwarding them to the master Configuration Server. Configuration Server Proxy now supports multiple LDAP servers.
	Changed functionality	8.1	Only users with External IDs will be considered for external authentication. You can now configure Configuration Server to use LDAP external authentication by setting configuration options, instead of modifying the Configuration Server configuration file and the **ldapclient.conf** file. You can now configure Configuration Server to use RADIUS external authentication by setting configuration options instead of modifying the Configuration Server configuration file.
Configuration Server / Configuration Server Proxy	New functionality	8.1	You can now configure Configuration Server to execute requests, submitted via an internal brief API, taking into account permissions of the parties involved. Configuration Server now supports heartbeat detection functionality used by Local Control Agent (LCA) to detect unresponsive Genesys applications. A system administrator, or a user with equivalent access rights and permissions, can configure: • Additional attributes for user passwords, such as case, punctuation, character type, expiration, and reuse. • A user to be required to change his or her password at first login (if forced

			password reset is supported by the user interface). • Whether an account can be locked out after a specified number of unsuccessful login attempts. • Whether an account can be considered to be expired after a specified time of inactivity. The hash algorithm for the secure storage of passwords has been updated. If you are using Configuration Server Proxies running previous versions, you must set up Configuration Server to use the older version of the password hash until you upgrade all Configuration Server Proxies. When a user is editing an object that is linked to other objects, only a user with access to one or more of those linked objects can change the link between their linkedobjects and the object being edited. When configuring two applications as an HA pair, both applications must be started from the same account. Configuration Server now supports LDAP full referrals returned by Microsoft Active Directory. New multi-language startup mode that enables storage of data in UTF-8 format in most fields. A change of Wrap-up Time made at the Agent Login level now also appears in the configuration of the Agent. High capacity connections for SIP Server are now available on Linux systems. Users can now configure a writable Configuration Server Proxy to allow its clients to add, delete, or modify

			configuration objects and their permissions. Configuration Server Proxy now supports heartbeat detection functionality used by Local Control Agent (LCA) to detect unresponsive Genesys applications. Configuration Server Proxy now supports Client-Side Port Definition on all its connections. Client connections are now restored automatically by the backup Configuration Server Proxy after a switchover of the proxy servers.
	Enhanced support for Outbound Contact Solution	8.1	When configuring a Campaign Group, users can now select Average Distribution Time or Maximum Gain as an optimization method. Target Value for Maximum Gain is a calculated value based on Established Gain and Abandoned Loss.
	Enhanced support for Routing Solution	8.1	Support of Oracle's large objects (LOB) data type for Routing Strategies, making storage of Routing Strategies more efficient. Support of UTF-8 encoding for Business Attribute objects.
Configuration Manager	New configuration object types	8.1	You can now configure the following new types of configuration objects in Configuration Manager: • Application types—Advisors Cisco Adapter, Advisors Genesys Adapter, Advisors Platform, Contact Center Advisor, Frontline Advisor, Business Rules Execution Server, Business Rules Application Server, CSTA Connector, Federation Server,

			Federation Stat Provider, Genesys Administrator Server, OT ICS OMP Infra, OT ICS Server, Social Messaging Server, UCM Connector, VP MRCP Proxy, VP Policy Server, Web Engagement Backend Server, Web Engagement Frontend Server, and Web RTC Gateway • Script types—Business Rules Data • Switch types—Aastra MX-ONE, Broadsoft BroadWorks
Local Control Agent (including Genesys Deployment Agent)	New functionality	8.1	Applications on a Host now connect to the LCA on that Host using a loopback interface. This enables the connection to remain stable regardless of the status of the Network Interface Card. Local Control Agent can now monitor the state of NTP services. New logs report when an NTP service ceases to be available and when it becomes available. In addition, users can now change the signature of an NTP service/daemon. Local Control Agent and Genesys Deployment Agent now support TLS, including enabling you to secure specified ports using the TLS Protocol.
Log Database	New functionality	8.1	The Log Database can now store encrypted data using transparent database encryption as described for specified databases.
Solution Control Server	New functionality	8.1	Solution Control Server now supports heartbeat detection functionality used by Local Control Agent (LCA) to detect

			unresponsive Genesys applications.
Solution Control Server utilities	New functionality	8.1	You can now install the Solution Control Server utilities without installing Solution Control Server. Previously, the utilities were only installed automatically with Solution Control Server. The **mlcmd.exe** utility now uses names or DBIDs, and requires that the user provide credentials sufficient to access Configuration Server information to use the utility. In addition, parameters have been added that: • clear all active alarms • report CPU usage for each thread of a given process of a given application • store the results in an XML file
Message Server	New functionality	8.1	Error messages for authentication errors no longer contain a hint or direct indication of the reason that authentication failed. Message Server now supports Client-Side Port Definition and TLS on all its connections, and enables you to secure specified ports using the TLS Protocol. If Message Server is unable to enter a log into the Log Database, a log event is generated, and can be used to trigger an alarm.
Logs and Alarms	New functionality	8.1	You can now enable and disable log filtering for individual applications. Alarm Detection and Alarm Condition scripts now use the name of the affected configuration object by default, instead of the database identifier (dbid). This ensures seamless XML import and export of Alarm Detection and Alarm Reaction script definitions.

			Host and Tenant attributes have been added to audit logs. New options enable sensitive data in logs to be marked for post-processing by the user, such as deletion, replacement, or hiding
Deployment Wizards	Removed functionality	8.1	You can no longer use Framework Deployment Wizards on the new versions of software introduced in release 8.1.
Configuration Database	Extended functionality	8.0	GVP objects are now stored in the Configuration Database. You can manage them using Genesys Administrator, or with Configuration Manager and Solution Control Interface.
DB Server	New functionality	8.0	DB Server can now detect database failures and try to reconnect. DB Server now supports the PostgreSQL Database Management System.
Configuration Server	Extended functionality	8.0	You can now configure hierarchical multi-tenant environments, where each Tenant is a parent Tenant, child Tenant, or both. Advanced Disconnect Detection Protocol (ADDP) is now supported between primary and backup Configuration Servers.
	New functionality	8.0	All Management Framework clients of Configuration Server now subscribe for only necessary notifications, improving system performance. You can now configure, at the Tenant level, a minimum length for all passwords used to gain access to applications within that Tenant. You can now configure a master Configuration Server

			running 8.x to ensure that Configuration Server Proxy running 7.6 or earlier reads configuration data correctly, even if using a different database schema. The History Log is now stored in the Configuration Database by all Configuration Servers (the HA pair), except Configuration Server Proxies.
Configuration Manager	New configuration objects and types	8.0	You can now configure the following new configuration objects in Configuration Manager: • Application types—Advisors, Capture Point, Customer View, ESS Extensible Services, iWD Manager, iWD Runtime Node, Interaction Workspace, Orchestration Server, Rules ESP Server, SMS Server • GVP Voice Platform Profiles • Script types—ESS Dial Plan, Interaction Workflow Trigger, Outbound Schedule • Switch types—Avaya TSAPI, Cisco UCCE, Huawei NGN You can now set the following new values for Business Attributes of type Media Type: • smssession • mms • mmssession
	New functionality	8.0	By selecting an object in a Search results list, you can now directly open the folder containing that object, or view its list of dependent objects. You can set Configuration Manager to Emergency Mode,

			which provides read-only access to all Users except members of the Super Administrators access group. The on-line Help file now includes keyboard shortcuts.
	Changed functionality	8.0	You can now enter up to 4 KB of text when defining flexible option values of configuration objects. Disabled users can no longer log in to any Genesys Application.
Local Control Agent	New functionality	8.0	The Genesys Deployment Agent is now deployed with LCA. The Genesys Deployment Agent works with Genesys Administrator to deploy Genesys Applications and Solutions on the Host. Local Control Agent can now detect unresponsive Genesys applications for which you can configure appropriate actions, including alarms if required.
Solution Control Server	New functionality	8.0	In a Distributed Solution Control environment, any Solution Control Server can detect the failure of a remote site controlled by another Solution Control Server. You can now use the **mlcmd.exe** command line utility to stop and start Applications and Solutions; to retrieve the status of Applications, Solutions, and Hosts; and to create and send a custom log message.
Solution Control Interface	New functionality	8.0	You can now shut down an Application gracefully, if the Application supports Graceful Stop. Likewise, you can shut down a Solution gracefully, if the Applications that make up the Solution support Graceful Stop. After a user logs in, the date and time when anyone last logged in using that account is displayed. Platform status is now color-coded, to provide a quick visual reference as to the

			state of the system. A user can now be granted read-only access to the alarm interface, allowing them to monitor system status, including alarms, but prohibiting them from clearing alarms. The on-line Help file now includes keyboard shortcuts.
	Enhanced functionality	8.0	If you upgrade the Log Database to 8.0 or later, SCI now displays log records in descending order of generation with no effect on performance for large log databases. This upgrade is optional.
Logs and Alarms	Changed functionality	8.0	You can now specify a greater number of files (segments) before logs expire.
Wizard Manager	New functionality	8.0	Now supports the user inactivity timeout feature introduced in 7.6.
Configuration Import Wizard	New functionality	8.0	You can now enter configuration changes data in an XML file, and then use the new **x2c.exe** command line utility to apply those changes to the configuration data.
External Authentication	New functionality	8.0	New log events allow users to better monitor the connection between Configuration Server and the RADIUS or LDAP external authentication server. When logging in, you will receive messages from the RADIUS and LDAP servers indicating the success or failure of your login. You can now configure Configuration Server to accept an empty password if the external authentication server allows it. You can now configure RADIUS external authentication on Configuration Server Proxy.

Management Framework Deployment Manager	Removed functionality	8.0	Replaced by the Deployment Wizard in Genesys Administrator.
Configuration Server	New functionality	7.6	You can now improve system performance for large History Log updates.
	Changed functionality	7.6	By default, new users are no longer added automatically to a user group. To enable new users created in 7.6 or later to be assigned automatically to pre-defined Access Groups, you must manually disable this feature.
Configuration Manager	New functionality	7.6	During installation, you can configure the circumstances under which a Security Banner, which you can also design, to appear at login. You can now configure a time period after which users who have been inactive during that time will be forced to log in again.
Solution Control Interface	New functionality	7.6	During installation, you can configure the circumstances under which a Security Banner, which you can also design, to appear at login. You can now configure a time period after which users who have been inactive during that time will be forced to log in again.
External Authentication	New functionality	7.6	You can now configure multiple LDAP external authentication servers.
Logs and Alarms	New functionality	7.6	You can now customize log events for an application by changing the log level of an event, or by disabling the event.

Required Database Formats for Available Features

Management Framework 8.5 and later generally allows you to use database formats of prior releases without updating those formats.

> **Important**
>
> Database formats 8.0 or earlier are not supported by the latest versions of Management Framework components. If you are running Configuration Server 8.0 or earlier, you must upgrade your database format when moving to 8.5 or later versions.

The following table summarizes key features and the level of Configuration Database required.

[+] Show Table

Management Framework 8.5 Features and Compatible Configuration Database Formats

Feature	Compatible Configuration Database Format	
	Release 8.1	Release 8.5
Logging enhancements: • Reliability Logging • Log Resilience	Yes	Yes
Database access without DB Server	Yes	Yes
Support for new DBMS: • Oracle 12c • Microsoft SQL 2012 • Microsoft SQL 2014	Yes [a]	Yes
Kerberos Single Sign-on for Genesys Workspace Desktop Edition	Yes	Yes
Language Packs support	No	Yes
History of Configuration Changes audit trail	No [b]	Yes
Disaster Recovery / Business Continuity architecture	Yes	Yes

a. Support for new Database Management Systems is not provided by CCW. However, the Database can be moved to a new platform using DBMS tools. Consult the DBMS vendor for details and instructions.

b. The audit trail exists in the release 8.1 configuration environment, and can be accessed using the Configuration Server utility. However, it does not contain some information, such as previous values for each change. You need the latest Configuration Database format for the full feature to work as documented.

Secure Protocols Compatibility

When secure connections (using Transport Layer Security–TLS) have been deployed between Genesys components, keep in mind that a newer version of a component might have stricter requirements and fail to establish a connection with an older component that uses a less secure version of TLS and/or does not provide the security parameters required by the newer component to operate.

Windows-based Components

For Windows-based Framework components, minimum supported TLS versions and parameters are defined by the Windows operating system. Check Microsoft documentation before deploying components on new or patched versions of the Microsoft Windows operating system.

Linux/UNIX-based components

For each upgraded Linux/UNIX-based Framework component that is using secure connections, you must also deploy Genesys Security Pack on UNIX. The version of the Security Pack must match that of the component. For example, if you are deploying Configuration Server 8.5, make sure you also deploy Security Pack 8.5, and make Shared Object modules of this Security Pack available for the Configuration Server process to load, such as setting the **LD_LIBRARY_PATH** environment variable when starting Configuration Server. You can have multiple versions of Security Pack SO modules installed in different folders on the same machine.

When components are set to use different versions of Security Pack, review the Security Pack on UNIX Release Notes for details on recent changes that may affect compatibility.

Upgrading Components

This section defines the order of the steps necessary to upgrade software. You might also consider upgrading the database schema and/or reloading the locale, if necessary, as part of the software upgrade procedure. See the following sections for details of database-related activities.

> **Important**
> You do not have to update both the software and the database schema at the same time, unless you want particular new features to work with new software.

Interoperability

There are several items to consider regarding interoperability:

- When upgrading a configuration environment running in Distributed mode, first upgrade Configuration Server to the newer version, then upgrade all Configuration Server Proxies as soon as possible. Genesys does not support running different versions of Configuration Server components, except during the migration from one version to another. During this phase, different versions of Configuration Server can co-exist in the same environment to ensure minimal downtime; however, do not attempt to enable any new features until you remove older versions of Configuration Server from the environment.
- When upgrading Configuration Server in Disaster Recovery/Business Continuity mode, make sure you upgrade dormant copies of master Configuration Servers. If the Configuration Database was also upgraded, be sure to replicate the upgraded database before you start any of the dormant instances.
- License Reporting Manager (LRM) 8.5 is no longer integrated with Configuration Server. If you are upgrading from a configuration environment using LRM 8.5, you must uninstall it. Refer to the LRM Technical Advisory for more information.

Upgrading Local Control Agent

Use the following procedure to upgrade Local Control Agent (LCA).

[+] Show procedure

Prerequisites

- LCA is installed and running on a host.

- SCS is controlling this host, has been upgraded to the latest version, and is connected to LCA.
- There are no active alarms on the host or any ready to be installed.

Procedure

1. In the options of all Solution Control Servers that control the hosts in which the LCA upgrade is performed, set the value of the **disconnect-switchover-timeout** option in the **[general]** section to, for example, `600` (10 minutes).
2. Upgrade LCA on those hosts in the environment that are running either:
   - No Solution Control Servers, or
   - One Solution Control Server (SCS) that is not configured in an HA pair. In this case, ensure that you shut down this SCS before upgrading LCA. Note that you will have no Management Layer control of this environment until SCS is back on line.

   This step should be repeated one host at a time.

   > **Warning**
   > If the upgrade of every host takes any longer than the value set for the **disconnect-switchover-timeout** option, an incorrect switchover could occur.

3. Upgrade LCA on the host that runs the primary SCS, as follows:
   a. Shut down the primary SCS. Wait until the switchover is complete and the backup SCS is running in primary mode.
   b. Upgrade LCA on the host.
   c. Start the primary SCS. It should be running in backup mode.
4. Upgrade LCA on the host that runs the backup SCS in primary mode, as follows:
   a. Shut down the backup SCS running in primary mode. Wait until the switchover is complete and the primary SCS is running in primary mode.
   b. Upgrade LCA on the host.
   c. Start the backup SCS. It should be running in backup mode.
5. In the options of all Solution Control Servers in the environment, delete the **disconnect-switchover-timeout** option set in Step 1.

Limitations

There is no switchover of HA components on the host where LCA being upgraded if any of them or their peers fail, until one of the following occurs:

- A new LCA is installed and running, or
- The timeout defined by the **disconnect-switchover-timeout** option has elapsed.

Upgrading Management Layer Server Components

Important

- When upgrading a Management Layer server component, you must stop it using the Management Layer (using Genesys Administrator), to prevent it from being restarted during the upgrade process.
- Use the Management Layer to prevent them from being restarted during the upgrade process to start the components, except when a single Solution Control Server (SCS) (not part of an HA pair) is being upgraded. In this case, start SCS using the appropriate operating system commands on its host, and then confirm that Genesys Administrator can reconnect to this SCS.

Use the following procedure to upgrade Management Layer Server Components.

[+] Show procedure

For the SCS and Message Server components, the same sequence of steps applies.

Prerequisites

- All new Installation Packages (IPs) are delivered to the relevant hosts and are ready to be installed.

Procedure

1. Shut down the server to be upgraded. If the server is part of an HA pair, shut down the backup first.
2. Save the configuration options of the server shut down in Step 1 to provide a rollback path if the older version must be restored. Use Genesys Administrator to export options into the XML file and save the file.
3. Using Genesys Administrator, upload a new Application Template and metadata file into the configuration environment and associate the existing configuration object, originally associated with the shut-down server application, with the new Application Template. Select the option to add new options from the template.
4. Install the new version of the component, providing the same Application object name that was used by the server (updated in Step 3), using the same host where a previous backup has been installed. Follow deployment and configuration guidelines for the particular component.
5. (Message Server only) If the upgrade requires that the Log Database be updated, refer to the instructions in Updating the Centralized Log Database Schema.
6. Start the newly upgraded server component and, if a part of an HA pair, ensure it becomes backup for the currently running primary server.
7. (HA servers only) If the newly upgraded server component is part of an HA pair, shut down the current primary server (if it is still running). Ensure that the newly installed component becomes primary and begins serving clients. Follow the same steps to upgrade the other component of the HA pair.

Limitations

Availability of the component being upgraded might be limited during the downtime of backing up, installing, and starting the new version.

Upgrading Configuration Server

Warning

- Do not enable any new features of Configuration Server until you finish upgrading all Configuration Server Proxies to the version that supports the new features.
- Both Configuration Servers configured as an HA pair must be running the same version when migration is complete. If there are requirements for related components (such as DB Server), upgrade those components first.

Recommendation

Preserve the legacy Configuration Database for some period of time to ensure rollback is possible, if needed. Rollback can be carried out using the same sequence of steps if the legacy Configuration Server was 8.5; for older servers, it is required to shut down both currently running servers in the master Configuration Server pair before starting any previous version.

Limitations

- Client sessions are not preserved between older and newer versions of servers when upgrading the database. There might be other cases when session restoration will not work during upgrade – refer to the Release Notes of the particular version.
- During the upgrade procedure, the Configuration Server environment remains read-only and the master Configuration Server is not redundant until the new server is fully initialized.
- During upgrade, SCS might not be able to switch over applications as long as it is configured to accommodate the startup of new Configuration Servers, or it might not be able to control applications on the host of the newly installed Configuration Server if LCA was shut down using the previous steps.

Prerequisites

- All new Installation Packages have been delivered to the relevant hosts and are ready to be installed.
- The latest version of LCA is installed on the Configuration Server hosts.
- The latest version of SCS is deployed in the environment.

Upgrading a Standalone Configuration Server

Use the following procedure to upgrade a standalone Configuration Server.

[+] Show procedure

Procedure

1. Back up your Configuration Database.
2. Install (but do not start) a new Configuration Server instance by selecting **Configuration Server Master Backup** installation mode when installing from the Installation Package. Note the following:
   - When prompted to provide a name for the Application object, enter the same name as the Application object that is being upgraded, but select a new folder for your installation.
   - Confirm that, in the configuration file of the newly upgraded server, the section name corresponds to both:
     - The name of the Application object for which this instance has been

installed.

- The value of the **-s** option in the command line to start this instance.

3. If the database schema of the Configuration Database must be upgraded, refer to Migrate the Database for detailed instructions.
4. Using Genesys Administrator, shut down the instance you are replacing. This will cause some downtime for Configuration Server clients.
5. Back up the folder of the instance that was shut down in the previous step. Change the folder name to be version-specific and replace it with the content of the relevant folder prepared in Step 2.
6. Launch the new version of the Configuration Server instance from the replaced folder and wait for it to initialize. Make sure it completes initialization before continuing. At this stage, note the following:
   - The time when the server instance completes initialization will end the downtime window for Configuration Server clients.
   - If you are upgrading the database schema and a disaster recovery (DR) deployment is in place, set up replication from the migrated database to a remote DR site where the corresponding new database should be created. Follow the same guidelines as discussed in the *Framework Deployment Guide*.

Upgrading an HA Pair of Configuration Servers

If you want to upgrade to 8.5.101 an HA pair of Configuration Servers running version 8.1.3 against a Configuration Database with an 8.1.1 schema, you can upgrade the two servers without losing or interfering with any of the backup functionality. Use the following procedure:

[+] Show procedure

Upgrading HA Configuration Servers, Using Same Configuration Database Schema 8.1.1, from 8.1.3 to 8.5.101

1. Back up your Configuration Database.
2. First, upgrade the backup Configuration Server. Deploy (but do not start) a new backup 8.5.1 Configuration Server instance by selecting **Configuration Server Master Backup** installation mode when installing from the Installation Package. Note the following:
   - When prompted to provide a name for the Application object, enter the same name as the Application object that is being upgraded, but select a new folder for your installation.

- In the configuration file of the newly upgraded server, confirm that the section name corresponds to the name of the Application object for which this instance has been installed.

3. Stop the 8.1.3 backup instance using Genesys Administrator, then back up its folder. Change the folder name to be version-specific and replace it with the content of the relevant folder prepared in Step 2.
4. Launch the 8.5.101 Configuration Server instance from the replaced folder and wait for it to initialize. Standard-level log messages **21-25303** followed by **21-22172** should be generated, indicating that the 8.5.101 Configuration Server is running as backup to the 8.1.3 primary Configuration Server. If these log messages are not generated, you have to force the upgrade—use the other procedure for upgrading from 8.1 to 8.5.
5. After the new primary 8.5.101 Configuration Server has initialized, shut down the primary 8.1.3 Configuration Server. This forces the clients of the 8.1.3 server to try to connect to the primary 8.5.101 Configuration Server that will be brought into primary mode momentarily by Solution Control Server. Clients can restore their sessions.
6. After all clients are finished migrating to the primary 8.5.101 server instance (monitor this either by checking all client applications for successful reconnection messages or by the `total number of clients` message reported by both servers when the log level is set to debug), install an 8.5.101 version of of Configuration Server the on the host where the original 8.1.3 server from that pair was installed. Be sure to use the same Application name (use `confserv` if the remaining server is configured as primary).
7. Start the newly-installed 8.5.101 Configuration Server. Use the normal starting procedure; no special steps or options are required. The new Configuration Server recognizes that its HA peer (the primary 8.5.101 Configuration Server in upgrade mode) is already upgraded, and initializes as the backup server.
8. After the newly-installed 8.5.101 server has fully initialized as backup and generated log message **21-22172**, shut down the primary 8.5.101 backup Configuration Server that is in upgrade mode. SCS immediately promotes the backup 8.5.101 backup server to primary. Clients are able to restore their sessions normally, and they switch over to the new upgraded primary server.
9. Start the backup Configuration Server (formerly in upgrade mode), manually or using Genesys Administrator. The migration is complete. The only messages in the 8.5.101 log will be those relating to the migration.

If you just want to upgrade the HA pair to an 8.5 Configuration Server from an 8.1 version or an earlier 8.5 version, regardless of whether they are using the same Configuration Database schema, use the following procedure:

[+] Show procedure

Upgrading HA Configuration Servers

1. Back up your Configuration Database.
2. First, upgrade the backup Configuration Server Install (but do not start) a new backup Configuration Server instance by selecting **Configuration Server Master Backup** installation mode when installing from the Installation Package. Note the following:
   - When prompted to provide a name for the Application object, enter the same name as the Application object that is being upgraded, but select a new folder for your installation.
   - Confirm that, in the configuration file of the newly upgraded server, the section name corresponds to the name of the Application object for which this instance has been installed.
3. Use Genesys Administrator or any other suitable tool or utility to force the currently running Configuration Server into Read-Only mode. This prevents any changes being made to your configuration during the switchover.
4. If you have upgraded the database, make sure that the new instance of Configuration Server is configured to start against the new database.

> **Important**
>
> If you are upgrading the database schema and a disaster recovery (DR) deployment is in place, set up replication from the migrated database to a remote DR site where the corresponding new database should be created. Follow the same guidelines as discussed in the *Framework Deployment Guide*.

5. Stop the backup instance using Genesys Administrator, then back up its folder. Change the folder name to be version-specific and replace it with the content of the relevant folder prepared in Step 2.
6. Launch the new version of the Configuration Server instance from the replaced folder and wait for it to initialize. Monitor the new instance for any of the following Standard-level log messages:
   - The new Configuration Server should enter upgrade mode automatically when detecting another instance is not fully compatible. Log event **21-25301** is generated soon after the newly started Configuration Server is able to contact the current primary server in this case. If you don't see this message after log event **21-22911** but before event **21-22902**, and your primary Configuration server is older than 8.5, you must stop the new server and review Configuration Server Release Notes. You might need to force the new version into upgrade mode using the **upgrade-mode=1** option in the configuration file and/or in the command line.
   - There is no need for upgrade mode if you are replacing Configuration Servers that are fully compatible, and are running against the same Configuration Database. This is the case if you observe log event

21-22902, followed by log event **21-22172**, from the newly installed server. In this case, you can ignore the rest of the steps in this procedure, which describe only situations where have to proceed with having one Configuration Server in upgrade mode.

- This new instance will initialize as the primary Configuration Server in upgrade mode (that is, it detected upgrade mode automatically and generates log event **21-25301**, or it was started with the command-line parameter **-upgrade-mode1** or configuration option **upgrade-mode=1** and generates log event **21-25300**). It might compete with the original primary server for database access, if you are starting it against the same database (that is, you are not upgrading the database upgrade at the same time). Both servers will automatically enter Read Only mode during upgrade, when they share the same database.
- Solution Control Server detects the presence of two primary Configuration Servers and tries to force the new server (in upgrade mode) into backup mode, but the new instance refuses these requests and continues to initialize. This is normal situation during upgrade. You might observe log event **21-25302** reported several times by Configuration Server in upgrade mode; this is not considered an error in this situation.
- You must see that log event **21-22170** or **21-22171** has been generated by the new instance of Configuration Server before you can continue with the next steps.**21-22170** is generated when Configuration Server upgrade steps are performed in an environment with the same Configuration Database. **21-22171** will be generated if you are upgrading the database at the same time.

7. After the new primary Configuration Server, still in upgrade mode, has initialized, shut down the original primary Configuration Server. This forces the clients of the original server to try to connect to the new primary Configuration Server (the one in upgrade mode). The clients of the original Configuration see this as a temporary disconnection, and try to connect to the backup server (which is currently running as the new primary server, in upgrade mode). However, a backup server in upgrade mode does not support session restoration, so clients must re-read the configuration to ensure they get the data in the appropriate schema.
8. After all clients are finished migrating to the new server instance (monitor this either by checking all client applications for successful reconnection messages or by the `total number of clients` message reported by both servers when the log level is set to debug), install the new version of the remaining server in the HA pair on the host where the original server from that pair was installed. Ensure that the same Application name has been used (use `confserv` if the remaining server is configured as primary). If database upgrade was part of this migration, also provide the new server with the reference to the upgraded database.
9. Start the new Configuration Server. Use the normal starting procedure; no special steps or options are required. The new Configuration Server recognizes that its HA peer (the new primary Configuration Server in upgrade mode) is already upgraded, and initializes as the backup server.

10. After the new backup server has reported log event **21-22172** after becoming fully initialized , shut down the primary Configuration Server that is in upgrade mode. SCS immediately promotes the new backup server to primary. Clients are able to restore their sessions normally, and they switch over to the new upgraded primary server.
11. Start the backup Configuration Server (formerly in upgrade mode), manually or using Genesys Administrator, to ensure uninterrupted operations in the future.

Upgrading a Configuration Server Proxy

To upgrade Configuration Server Proxies, if any, use the previous procedures, depending on how they are configured—as standalone Configuration Server Proxies or in HA pairs. In either case, note the following exceptions to the referenced procedures:

- If the master Configuration Server 8.1.3 is using the Configuration Database in single-language mode, both primary and backup instances of Configuration Server Proxy 8.5 can, during migration, start and operate against Configuration Server 8.1.3. In all other cases, you must upgrade the master Configuration Server before any of its associated Configuration Server Proxies.
- You do not need to put the configuration environment into read-only mode, but Genesys strongly recommends that you ensure no updates are pending and/or scheduled.
- You do not need to copy any ***.conf** files from one folder to another when preparing new instances.
- You might want to back up configuration options of individual Configuration Server objects using Genesys Administrator, by selecting the Application object's options and exporting them into XML.
- When installing the new Configuration Server Proxy instance for upgrade purposes, you must specify the same Application object name as that of the instance being replaced, and perform all configuration (using the master Configuration Server) using the options of that Application object.

Rolling Back Configuration Server

If you need to return to a previously stable version of Configuration Server, an installed but inactive old instance should be used to boot up the stable version. If rollback of both the master and Configuration Server Proxy are required, the rollback order depends on the operational state of the master, as follows:

- If the master is fully operational, roll back the Configuration Server Proxy instances first. **[+] Show procedure**

  1. Using Genesys Administrator, shut down the currently running backup instance. This begins your rollback window. If there is no HA pair, shut down the currently running instance; this starts a downtime window.
  2. Log into the configuration environment and manually reset the startup

parameters of the stopped instance to point to a location of the original target installation folder for this instance before the upgrade.

3. Start the corresponding old instance of Configuration Server and wait for it to initialize. If you are not using an HA pair, this will end the downtime\ rollback window. You do not need to continue with the rest of the steps.
4. Using Genesys Administrator, shut down the remaining instance you want to roll back. This causes a temporary loss of connectivity for Configuration Server clients. The second (already downgraded) instance is brought into primary mode momentarily and clients can reconnect. Confirm that this second instance successfully entered primary mode before continuing.
5. In the configuration environment, manually reset startup parameters of the stopped instance to point to the location of the original installation before the upgrade.
6. Launch the second old instance and wait until it is initialized and enters backup mode.
7. Verify that you have correctly specified locations (installation folders) of old instances in the configuration database (in respective Application objects) as well as in any external scripts and/or Windows service definitions that you may have set up previously. Back up and disable any external scripts and/or Windows service instances that are being used to deal with recently instances that were rolled back. This ends your rollback window.

- If the master is not operational, roll back the master instance first. **[+] Show procedure**

1. If you determine that immediate rollback is needed after unsuccessful execution of the upgrade procedure, follow these steps:
   a. Shut down the newly installed second instance that is having problems (if it is still running) and restart the first (old) instance that was shut down at first when you started the upgrade. There will be intermittent downtime until the old instance is fully initialized.
   b. When the old instance takes over as primary, log into the configuration environment and manually reset the startup parameters of the second instance (that was replaced by the new installation of the upgrade procedure) to point to a location of the original target installation folder for that instance before the upgrade.
   c. Restart the second instance.

   This completes the immediate rollback procedure. You do not need to continue with other steps.
2. If you performed the database upgrade, the old database is still available. Follow the same procedure as described in Step 1, but launch the old instance against the old database. You do not need to continue with future steps.

3. If the database rollback is needed to restore the normal operation and you have a database backup, do the following:
   a. Shut down any DB Server instances that are being used by master Configuration Servers. This will initiate a rollback window.
   b. Take DBMS offline and restore DBMS to the previous state.
   c. Proceed to Step 6 of the rollback procedure.
4. If the database rollback is not performed, log into the configuration environment and manually reset startup parameters of all to point to the location of the original target installation folder for each instance before the upgrade.
5. If the database rollback is not performed, force the currently running master Configuration Server into read-only mode, or ensure there are no pending changes to the configuration. This will initiate a rollback window.
6. Using Genesys Administrator, shut down the currently running backup instance and replace the folder with the backup copy from the previous version.
7. If the database rollback is performed, make sure the DBMS is online and start any DB Servers that are being used by the master Configuration Servers.
8. Start the corresponding old instance of Configuration Server from the restored folder and wait for it to initialize as backup. If you are not using an HA pair, this will end the downtime\rollback window. You do not need to continue with the rest of the steps.
9. Using Genesys Administrator, shut down the remaining instance you want to roll back. This will cause a temporary loss of connectivity for Configuration Server clients. The second (already downgraded) instance will be brought into primary mode momentarily and clients should be able to reconnect. Confirm that this second instance successfully entered primary mode before you continue.
10. Replace the folder with the backup copy from the previous version for the instance that is currently down, and launch the second old instance. Wait until it is initialized and enters backup mode.
11. Verify that you have correctly specified locations (installation folders) of old instances in the Configuration Database (in respective Application objects) as well as in any external scripts and/or Windows service definitions that you may have set up previously. Back up and disable any external scripts and/or Windows service instances that are being used to deal with recently instances that were rolled back. This will end your rollback window.

Updating Configuration Definitions

The Genesys Configuration database includes a set of predefined data items that enumerate available products and their capabilities. This information is located in separate database initialization scripts **CfgLocale_xxx.sql** (where xxx is the abbreviation for the particular DBMS being used), and match database schema initialization scripts. Locale data identifies what is being translated to national languages. In a localized environment, default local content has been extended (in a multi-language database) or replaced (in a single language database) with translated locale. Translated locales are available as parts of localization packs (for 8.5 and later), discussed below.

Locale data changes more frequently than the database schema itself, and you might find the need to load updated locale from time to time to enable new products in your existing environment. The procedure of updating locale discussed below.

Locale files are tied to a particular Configuration Database schema version (not the Configuration Server version). If an update of the locale is necessary, pick up the latest available locale that match your target schema version. For example, if you are running database schema 8.1, you must obtain the latest locale available for Configuration Server 8.1. Likewise, if you are using database schema 8.5, you must select the latest locale available for 8.5.

Updates of the locale independent of the database schema is supported starting from release 8.1.1. For releases prior to 8.1.1, you must update the entire schema to get new application types and other definitions.

Loading and Uploading Latest Locale Definitions

In release 8.5.1 and above, locale scripts are located in the **locale** folder of the Database Maintenance Scripts IP. In releases prior to 8.5.1, they are located in the **scripts** folder of the Configuration Server IP.

If you are looking for particular definitions to be added to your existing database, please review the Release Notes for Configuration Server and/or Configuration Database Maintenance Scripts, and Release Notes of particular Genesys products to determine what definitions you want to use, to determine the earliest version from which version of Configuration Server and/or Configuration Maintenance Scripts contain the locale with these definitions.

If you cannot see a definition available in any versions of Configuration Server or Maintenance Scripts packages suitable for your database schema, the definition is not compatible or is not yet available. Consider upgrading the database schema to the latest version where these definitions are present.

After you have determined which IP contains the locale you want to use, download and install it to obtain the locale scripts. For Release 8.5.1 and above, install the latest Configuration Database Maintenance Scripts package and get the locale script from the **locale** subfolder in the IP. For previous releases, install the latest Configuration Server package, select the **Standalone Database Initialization Scripts** option during installation, and get the locale files from the **scripts** subfolder in the IP.

Updating the Configuration Database Locale

Install the Upgrade Scripts package on the host where DBMS client software is installed and can access the target Configuration Database. You can upgrade the locale using the database upgrade scripts directly, or by using the Configuration Conversion Wizard (CCW).

Using the Upgrade Scripts directly

Use the following procedure to upgrade the locale. **[+] Show procedure**

1. Downtime is necessary when upgrading the locale. If Configuration Server is configured in HA mode, refer to Minimize Downtime while the primary Configuration Server and its backup are stopped for the upgrade. Otherwise, be prepared to stop and start the lone Configuration Server, using any hints from Minimize Downtime to minimize the downtime.
2. Use the command line (see the table below) and/or the vendor-provided User Interface to connect to the Configuration Database and execute the SQL scripts.

DBMS	Command Lines

DB2	Create a Windows bat file **update_CFG.bat**:
	`db2 connect to %DBID% USER %USER% USING %PASSWORD%`
	`db2 –vf CfgLocale_db2.sql`
	`exit`
	Run the command line:
	`db2cmd update_CFG.bat`

MSSQL	`sqlcmd -S %HOST%\%PORT% -U %USER% -P %PASSWORD% -d %DBID% -i CfgLocale_mssql.sql`

Oracle	Connect to Oracle :
	`sqlplus`
	`connect %USER%/%PASSWORD%@%SID% as default`
	`sqlplus> @CfgLocale_ora.sql`

Postgre	`set PGPASSWORD=%PASSWORD%` `psql -h %HOST% -d %DBID% -U %USER% -p %PORT% -a -w -f CfgLocale_postgre.sql`
Where:	

DBMS	Command Lines
%HOST% is the database server host %PORT% is the database server port %USER% is the database user name %PASSWORD% is the database user password %DBID% is the database name	

3. Use the script file in the ConfigDBMScrpt IP **locale** folder that matches the DBMS type.
4. Restart Configuration Server (and its backup, if in HA mode).

Minimize Downtime

You can minimize downtime when upgrading your locale by either using a backup Configuration Server, or by ensuring that the single instance of Configuration Server is running but is not connected to the Configuration Database while you are upgrading the locale.

If you have a backup Configuration Server, use the following procedure. If you have only a single Configuration Server, follow steps in the procedure for a primary server. Downtime might be longer in this case, because the single server will have to be restarted and become fully operational before any client can connect.

[+] Show steps

1. Stop the backup Configuration Server.
2. Modify the configuration file of the backup Configuration Server to include the **upgrade-mode=**1 option to enable side-by-side startup without contacting the configured peer server.
3. In Solution Control Server (SCS), set **disable-switchover=**`true` in the **[general]** section so that SCS will not automatically perform the switchover.
4. Disconnect the primary Configuration Server from the database (set **force-offline=**`true` in the Configuration Database section), or shut down all DB Servers that the primary server is configured to use.
5. Apply the upgrade locale script to the database.
6. Start the backup server and let it initialize in primary mode.
7. Stop the original primary server that is running in read-only mode. Clients will fail over to the backup server currently running in primary mode.
8. When the upgrade locale script is applied, reverse the previous steps, as follows:

a. In SCS, set **disable-switchover=**`false`, or remove it altogether, to restore automatic switchovers.

b. In the configuration file of both Configuration Servers, remove the **upgrade-mode=**1 option to re-establish communication between the two servers at startup.

c. Restart the backup server normally.

Using CCW

If you want to use the new types and enumerators, you can use CCW to update only the localization information stored in the database. Otherwise, you do not need to do anything - the new version of Configuration Server 8.5 will run against your current Configuration Database. Future versions of Configuration Server will include extensions to the list of application types you can utilize without migrating your system.

Warning

- Carefully select the location of the localization scripts that you are loading using CCW. Selecting the incorrect localization script can damage the database.
- Genesys strongly recommends that you make a backup of your current database using DBMS tools before you start the update.

Use the following procedure to update the locale of your Configuration Database without affecting the data.

[+] Show procedure

Prerequisites

- Your Configuration Database must be in release 8.1.1 or later schema.
- You must be using the version of CCW that matches the version of the database being updated.

Procedure

1.

Determine the version of Configuration Server that contains the required definitions. Use documentation provided with new products that require the new types and enumerators.

2. Launch Configuration Conversion Wizard (CCW). Make sure that you are using the latest available version of CCW to ensure that you can update the locale without being required to make a copy of your database.
3. From the list of possible procedures that CCW displays, select **Upgrade Configuration Database**.
4. When CCW prompts you to re-load the localization script, select **Yes**.
5. When CCW prompts you for which localization script to execute, do one of the following:
   - To load the English localization data from the Wizard's internal source, select **Default localization data (from internal source)**.
   - To load localization data from an external source, select **Load specific localization script**.
6. Select the CfgLocale script in the installation package for the Configuration Server version identified in Step 1, or in the **sql_scripts** folder within the directory if that (or later) version of Configuration Server is installed.
   The following table provides a list of database types and their corresponding localization script names for an enterprise or multi-tenant environment.

Database Type	Script Name
DB2	`CfgLocale_db2.sql`
MS SQL	`CfgLocale_mssql.sql`
Oracle	`CfgLocale_ora.sql`
PostgreSQL	`CfgLocale_postgre.sql`

> **Important**
>
> Updating the locale of an Informix or Sybase database is not supported in release 8.5 or later.

   CCW loads the new locale into the database.
7. When a message appears indicating that the database upgrade is complete:
   a. Click **Statistics** to review a report on how many objects in each database table have been added or modified.
   b. Click **Finish** to exit CCW.
8. Restart Configuration Server and its backup, if configured.

Updating the Database Schema

Management Framework Configuration Server can operate with database versions from 8.1.1 and up without the need for migration. If you are using an older version of Configuration Server, or if you want to take advantage of the latest features that require the latest database schema, you must upgrade the database schema. If you already have a compatible database schema version, you can convert to a newer version either when upgrading Configuration Server or at any time later.

If you only need to pick up the latest definitions (such as new application types, media type definitions, and so on) and you are already using Configuration Service 8.1.1 or later, you do not need to update the database schema. You only have to update the database locale to get the required definitions. See Upgrading Configuration Definitions for detailed instructions.

When upgrading the database schema, you stay with the same type of database (single-tenant or multi-tenant) and the same deployment mode (single-language or multi-language) as the original database that is being updated. Configuration Database, version 8.0 or later, can be upgraded to the latest available schema of a single-language database.

Management Framework Message Server can operate with a Centralized Log Database version 7.6 and up without needing to be migrated. Optionally, you can upgrade to the latest available version of the Centralized Log Database to increase efficiency and/or use new features.

This Migration Guide assumes that you have deployed separate databases for each product, and that you have not altered the database schema for those databases. In addition, note the following:

- Database conversion requires additional time, compares to upgrading the software, so plan accordingly.
- Genesys strongly suggests that you make a backup copy of any database being migrated, to enable you to rollback changes quickly in case any errors occur during or after the migration.

> **Warning**
>
> If you have changed the original database schema structure, or you use the same database to keep multiple schemas for other products, you are responsible for handling any data entered into the modified structure. Upgrade scripts may not work properly in this case. If you encounter any issues while migrating databases for which the schema was altered, or if the database is shared with other products, you might want to involve Genesys Professional Services to investigate the impact before moving forward.

Updating the Configuration Database Schema

Install the Upgrade Scripts package on the host where DBMS client software is installed and can access the target Configuration Database. You can upgrade the database schema using the database upgrade scripts directly, or, in some cases, by using the Configuration Conversion Wizard (CCW).

Using the Upgrade Scripts directly

Use the following procedure to upgrade the locale. **[+] Show procedure**

1. Downtime is necessary when applying the upgrade scripts. If Configuration Server is configured in HA mode, refer to Minimize Downtime while the primary Configuration Server and its backup are stopped for the upgrade. Otherwise, be prepared to stop and start the lone Configuration Server, using any hints from Minimize Downtime to minimize the downtime.
2. Use the command line (see the table below) and/or the vendor-provided User Interface to connect to the Configuration Database and execute the SQL scripts.

DBMS	Command Lines

DB2	Create a Windows bat file **update_CFG.bat**:
	`db2 connect to %DBID% USER %USER% USING %PASSWORD%`
	`db2 –vf upg_cfg_%VER%_db2.sql`
	`exit`
	Run the command line:
	`db2cmd update_CFG.bat`

MSSQL	`sqlcmd -S %HOST%\%PORT% -U %USER% -P %PASSWORD% -d %DBID% -i upg_cfg_%VER%_mssql.sql`

Oracle	Connect to Oracle :
	`sqlplus`
	`connect %USER%/%PASSWORD%@%SID% as default`
	`sqlplus>@upg_cfg_%VER%_ora.sql`

Postgre	`set PGPASSWORD=%PASSWORD%` `psql -h %HOST% -d %DBID% -U %USER% -p %PORT% -a -w -f upg_cfg_%VER%_postgre.sql`
Where: %HOST% is the database server host %PORT% is the database server port %USER% is the database user name %PASSWORD% is the database user password %DBID% is the database name %VER% is the upgrade version VVV_to_TTT	

3. Use the script file in the ConfigDBMScrpt IP **upgrade** folder that matches the DBMS type. It is a single- or multi-language file (depending on the Configuration Server option **multi-languages**), and matches the current

and target Configuration Database version.

4. Apply the upgrade script to upgrade the Configuration Database from version VVV to a next version TTT. If the current and target versions are separated by one or more intermediate versions, you must upgrade the database across those intermediate versions to get to the required target version. Apply the appropriate upgrade scripts to apply sequentially.
5. Restart Configuration Server (and its backup, if in HA mode).

Minimize Downtime

You can minimize downtime when upgrading your database by either using a backup Configuration Server, or by ensuring that the single instance of Configuration Server is running but is not connected to the Configuration Database while you are running the upgrade scripts.

If you have a backup Configuration Server, use the following procedure. If you have only a single Configuration Server, follow steps in the procedure for a primary server. Downtime might be longer in this case, because the single server will have to be restarted and become fully operational before any client can connect.

[+] Show steps

1. Stop the backup Configuration Server.
2. Modify the configuration file of the backup Configuration Server to include the **upgrade-mode=**1 option to enable side-by-side startup without contacting the configured peer server.
3. In Solution Control Server (SCS), set **disable-switchover=**`true` in the **[general]** section so that SCS will not automatically perform the switchover.
4. Disconnect the primary Configuration Server from the database (set **force-offline=**`true` in the Configuration Database section), or shut down all DB Servers that the primary server is configured to use.
5. Apply the upgrade script to the database.
6. Start the backup server and let it initialize in primary mode.
7. Stop the original primary server that is running in read-only mode. Clients will fail over to the backup server currently running in primary mode.
8. When the upgrade script is applied, reverse the previous steps, as follows:
   a. In SCS, set **disable-switchover=**`false`, or remove it altogether, to restore automatic switchovers.
   b. In the configuration file of both Configuration Servers, remove the **upgrade-mode=**1 option to re-establish communication between the

two servers at startup.

c. Restart the backup server normally.

Using CCW

If your current Configuration Database is using the 8.1.1, or later schema, you do not have to migrate your database to get new data types and enumerators. The new version of Configuration Server 8.5 will run against your current Configuration Database. Future versions of Configuration Server will include extensions to the list of application types you can utilize without migrating your system. However, if you want to update the database schema, you can use CCW. Refer to Configuration Conversion Wizard (CCW) for detailed information.

> **Tip**
> After upgrading the database schema to 8.5 (single language mode) and before the first start of Configuration Server, make sure that the Configuration Server configuration file contains the configuration option **langid** set to 1033 (or another appropriate value if you are applying Language Packs).

Updating the Centralized Log Database Schema

If you have upgraded your Message Servers to 8.1 or later, you might also want to update the schema of your Log Databases, as follows:

[+] Show procedure

> **Warning**
> Updating a large Log Database with a large number of records can take a significantly long time.

1. For each Message Server configured on the Log Database to be updated, set

the configuration option **db_storage** to `false`.

2. Execute the script **upgrade_7Xto80_<DBMS type>.sql** for the type of DBMS that you are using.
3. After the upgrade script has completed running, set the configuration option **db_storage** to `true` for those Message Servers configured on the updated database, as necessary.

Converting Configuration Environments

This section contains information to help you convert the following:

- Single-language to a multi-language deployment
- Single-tenant database to a multi-tenant database format
- Cross-DBMS conversion (one DBMS to another DBMS)

Single-language to a Multi-language Deployment

You can perform this conversion at any time, although Genesys recommends that you do so when you are migrating to a new release or locale of the Configuration Database. Use the following procedure:

[+] Show procedure

> **Warning**
>
> - Perform this procedure on an exact copy of the original Configuration Database. If unforeseen problems occur, you can then go back to the original database without any loss of data.
> - The production Configuration Database must be in Read-Only mode until the conversion is completed.

Prerequisites

- The original database must be in the current schema.
- Permissions to the Environment tenant have been changed to allow full access for Administrators.
- A new blank database in which the encoded data will be stored has been created and initialized with a multi-language locale. Refer to the *Framework Deployment Guide* for instructions about creating and initializing a multi-language database.
- Migration is supported by CCW 8.1.3 or later. Your database schema must

match CCW (8.1 or 8.5) to proceed. If your schema and CCW do not match, upgrade your schema and/or obtain the correct version of CCW.

Procedure

1. Launch Configuration Conversion Wizard (CCW).
2. From the list of possible procedures that CCW displays, select **Maintenance**. If the **Maintenance** option is disabled, the database is not in the current schema. See Updating the Database Schema to update the schema of your database, then retry this procedure.
3. From the list of maintenance activities, select **Migrate database to UTF-8 mode**.
4. When prompted, select the character encoding used by the original database, and enter the parameters of the new database (and the DB Server, if used) as requested.
   After performing some checks, CCW will start the migration. This might take a while, depending on the size of your Configuration Database.
5. When the migration is completed, do one of the following:
   - Press **Next** to view migration statistics, a list of tables that are in the database, and the number of rows in each that were migrated.
   - Press **Back** to return to the list of maintenance activities.

Single-tenant Configuration Database to Multi-tenant Configuration Database Format

You can use CCW to convert your single-tenant Configuration Server to a multi-tenant Configuration Server. In effect, your enterprise (single-tenant) environment becomes a multi-tenant environment, with only one tenant—yours—as the root (or Environment) tenant. This provides you with the flexibility to perhaps expand or better organize your operations.

This procedure only converts the Configuration Database model inside Configuration Server itself. Other Genesys applications might have to be reconfigured or reinstalled, as required by their usage guidelines, to operate in a multi-tenant environment.

Important

- Starting in release 8.5.1, you cannot deploy a new single-tenant database. However, you can continue to use your existing database with Management Framework 8.5.1, and

then use the procedure in this section at any time.

- If you are using CCW with a database that is in UTF-8 format already and with which Configuration Server is currently running, you must set the **allow-mixed-encoding** option to `true` in Configuration Server. This ensures that CCW can connect to Configuration Server.

You can perform this conversion at any time, although Genesys recommends that you do so when you are migrating to a new release or locale of the Configuration Database. Use the following procedure.

[+] Show procedure

Warning

- You must perform this procedure on an exact copy of the single-tenant Configuration Database. CCW compares the copy to the original database, and will not perform the conversion if they are not identical.
- The production Configuration Database must be in Read-Only mode until the conversion is completed.

Prerequisites

- The single-tenant database must be in the current schema.
- Permissions to the Environment tenant allow full access for Administrators.
- An exact copy of the single-tenant database exists. It is this copy that will be converted to the multi-tenant structure. CCW does the conversion only if the two databases are identical.
- If the single-tenant database is already migrated to UTF-8 format, and is running with Configuration Server, the **allow-mixed-encoding** option is set to `true` in Configuration Server.
- Migration is supported by CCW 8.1.3 or later. Your database schema must match CCW (8.1 or 8.5) to proceed. If your schema and CCW do not match, upgrade your schema and/or obtain the correct version of CCW.

Procedure

1. Launch (CCW).
2. From the list of possible procedures that CCW displays, select **Maintenance**, and click **Next**.
   If the **Maintenance** option is disabled, the database is not in the current schema. See Updating the Database Schema to update the schema of your database, then retry this procedure.
3. From the list of maintenance activities, select **Migrate database to multitenant mode**, and click **Next**.
4. If you have not yet created an exact copy of the database to be converted, do so now.
5. Enter the name of the copy of the database to be converted, and click **Next**.
   CCW will connect to that database, and compare it to the original. If they are identical, CCW will perform the conversion, ending with a final notification that the migration is complete.
   If they are not identical, CCW will not perform the conversion, and display a warning. The two databases must be identical before CCW will proceed with the conversion.

After the conversion, you might notice a few changes to your database, such as:

- All folders previously located in the Resources Tenant are now in the Environment Tenant.
- There is no longer a Tenant called Resources; it has been removed.

Cross-DBMS conversion (one DBMS to another DBMS)

Genesys does not provide a tool for migration of a Configuration Database in one DBMS to another DBMS. As a general workaround to perform the cross-DBMS migration, do the following:

1. Upgrade the original (earlier) Configuration Database to the latest format in the same DBMS.
2. Use CCW to export the upgraded Configuration Database. The output SQL statements will be written in the syntax of the source DBMS.
3. If the SQL syntax of the source DBMS is different from that of the target DBMS, manually convert the exported SQL statements into the syntax necessary for the new DBMS.
4. Initialize the newly created Configuration Database in the target DBMS by running only the initialization script. For example, if the target DBMS is Oracle and the database is for a single-tenant configuration, use the file **init_single_ora.sql**. Do not run the file **CfgLocale_ora.sql**.

Important

There will be some duplicate statements in the initialization file, at least for `default` and `confserv` applications, for some ACEs, and for MAXDBID. These duplicate statements should be removed from the database after initialization by running a delete script using SQL syntax of the target DBMS, such as the following: **[+] Show sample script**

```
delete from cfg_ace
/
delete from cfg_alarm_condtn
/
delete from cfg_app_prototype
/
delete from cfg_application
/
delete from cfg_enum_value
/
delete from cfg_enumerator
/
delete from cfg_field
/
delete from cfg_folder
/
delete from cfg_format
/
delete from cfg_format_field
/
delete from cfg_group
/
delete from cfg_hdb_last_login
/
delete from cfg_log_event
/
delete from cfg_max_dbid
/
delete from cfg_parameters
/
delete from cfg_person
/
delete from cfg_port_info
/
delete from cfg_refresh
/
delete from cfg_server
/
delete from cfg_tenant
/
delete from cfg_time_zone
/
delete from cfg_max_dbid
/
delete from cfg_locale
/
delete from cfg_app_option
/
```

Execute the transformed export file using the target DBMS. Do not use CCW for this purpose.

Localized Environments

The Genesys Configuration Server executable is language independent. You can always use the latest available (for your release) version of Configuration Server to upgrade your environment, no matter the language of your database is.

In release 8.1 and earlier, Genesys provided separate localized Installation Packages (IP) of of the Configuration Server component for each language. Every package included both the Configuration Server executable and locale-dependent database initialization scripts. Once you created the database of selected language, you could use any future version of Configuration Server (regardless of the IP language) that support this version of database schema.

Starting from release 8.5, the Configuration Server IP is available only in a neutral language (English/US). Additional Language Pack IPs are available to switch/extend the database to support additional languages. Language Pack IPs are released independently from Configuration Server to provide the opportunity to update configuration definitions in each language separately from delivering fixes to the Configuration Server executable itself. The process is similar to the update of locale described earlier. Language Packs provide a way to periodically update the locale of localized environments in the same way as the Configuration Database Maintenance Scripts IP allows you to update the locale of the default (English/US) deployment.

In contrast, multi-language environments are not tied to a particular language and can accept additional Language Packs at any time. Upgrade of a multi-language database schema follows the same procedure for a general database upgrade procedure, as described earlier. When you have completed the database upgrade, you can add additional languages, available for your target release, as outlined in this topic.

Upgrade of Localized Database

> **Important**
>
> - You cannot change the language of single-language database once it is created.
> - These steps apply to 8.5 and newer database schemas that support Language Packs.

Genesys supports localization of Configuration Server by updating the content of the Configuration Database to have definitions in the selected languages. The 8.5 process is different than in previous releases, so Genesys recommends that you migrate to database schema 8.5, and use Configuration Server 8.5.x (or newer) to ensure smooth operation and seamless future updates of localized definitions when new application types are introduced.

If you are using a localized version of Configuration Server 8.1 or earlier, you must use the relevant upgrade scripts to upgrade the database into the 8.5 single–language format, before you can add the latest languages using language packs.

To upgrade a localized Configuration Database schema to the latest version, follow the instructions in Upgrading Database Schema. After you have completed those steps, including loading the default locale, use one of the instructions in the next sections, as appropriate.

Updating a Single-language Database With the Latest Language Definitions

1. Obtain the latest Language Pack for your release, for the same language that was used during the initial database creation. You can later apply a Language Pack with the English/US locale to the database if you have initially created this database to handle national characters, as per DBMS vendor instructions, and you have never entered any data in a language other than English/US and/or the selected national language.
2. Follow instructions from the *Framework Deployment Guide*, in the section *Single-Language Configuration Database*, to apply the Language Pack for a single-language database.

> **Important**
>
> Do not apply a new locale from the Configuration Server Maintenance Scripts IPs to the database where Language Packs are deployed in case you need new definitions to appear in this database. Instead, use locale files from the latest versions of Language Pack IPs.

Adding and Updating Languages in Multi-language Databases

If you create the Configuration Database in multi-language mode, you can add additional languages when you need them. You might also want to update language definitions for all active languages periodically, when new versions of Language Packs for your release become available.

Follow instructions in the *Framework Deployment Guide*, in the section *Multi-Language Configuration Database*, to apply Language Packs to a multi-language database.

Migrating to Net-SNMP

Starting in release 8.5.1, you can use Net-SNMP, instead of the Genesys SNMP Master Agent component, to implement SNMP functionality. Net-SNMP and Genesys SNMP Master Agent can run in parallel on the same system, if the following conditions are met:

- Only one connection to an SNMP Master Agent can be configured on each Solution Control Server (SCS).
- The ports used by the SNMP Master Agents must be unique, and not used by any other application.

Solution Control Server and Local Control Agent support both implementations.

To migrate to Net-SNMP from Genesys SNMP Master Agent, you must:

1. Install Net-SNMP on each host machine on which you will be using Net-SNMP Master Agent, using the instructions in the "Installing Net-SNMP" section of the *Framework Deployment Guide*.
2. Convert each Genesys SNMP Master Agent to a Net-SNMP Master Agent, using the following steps: **[+] Show steps**
   a. Locate the Genesys SNMP Master Agent Application objects that you want to replace.
   b. Stop and uninstall the Genesys SNMP Master Agent applications. There is no data loss but, during this time, the NMS cannot query SNMP information from those components configured to report their status through the Genesys SNMP Master Agents being replaced.
   c. In the **Server Info** section of the **Configuration** tab of the Application objects, make the following changes (if the field is not already set to the appropriate value):
      - Set **Host** to the Host object on which this Net-SNMP Master Agent will be running.
      - Update **Listening Ports** as necessary.
      - Set **Working Directory** to the Net-SNMP installation folder.
      - Set **Command Line** to the name of the Net-SNMP executable.
      - Set **Command Line Argument** to the same command-line argument used to start the service or process. This information is used by LCA to identify that Net-SNMP is started and running a third-party application.
   d. In the **Options** tab, make the following changes:
      i. Create the section **[snmp]** if it does not already exist.
      ii. In the **[snmp]** section, set the **netsnmp-enable** option to `true`. This enables Net-SNMP in the SNMP Master Agent Application object. If this option is not set, or set to `false` (the default), SCS and LCA treats the object as a Genesys SNMP Master Agent.
   e. In the **Annex** tab, make the following changes:
      i. Create the section **[start_stop]** if it does not already exist.
      ii. In the **[start_stop]** section, set the **start_command** and **stop_command** options to the path and filename of the batch or shell scripts to start and stop (respectively) the Net-SNMP application.
   f. Save your changes.

Important

SCS reads the configuration settings of the SNMP Master Agent Application object and uses the option values to connect to Net-SNMP. Therefore, you must ensure that the option values configured for the SNMP Master Agent Application object in the Configuration Database match the actual configuration settings in your SNMP Master Agent.

Enabling New Functionality

As a rule, newer versions of Framework components by default behave in the same way and rely on the same configuration as prior versions they are replacing. This allows you to use components as drop-in replacements and continue using the software in the same way that you are used to. In some cases, when you want to activate a particular new feature or behavior, you must add or change configuration options after you have installed a new release. A list of changes in configuration options is provided in New and Changed Configuration Options by Release.

Some versions may introduce changes that require you to take action before you can launch the new component after upgrading it in the existing environment. A list of mandatory configuration changes that has to be made when upgrading certain component is provided in Mandatory Changes in Configuration of Framework Components.

New and Changed Configuration Options by Release

The tables in this section document all configuration option changes in specific Framework server components from release 7.6 through 8.5, with the most recent changes listed first. The changes are listed by component.

Refer to the *Framework Configuration Options Reference Manual* for detailed descriptions of all of the Framework configuration options, with the following exceptions:

- Configuration options for the Configuration Conversion Wizard are described in detail in CCW Configuration Options.
- Configuration options related to external authentication are described in detail in the *Framework External Authentication Reference Manual*.

General Configuration Option Changes

The following table lists all changes in common configuration options (that is, those that are supported by all Genesys server applications), from release 7.6 through 8.5, with the most recent changes listed first.

All Genesys server applications support the unified set of log options (called common log options) in addition to application-specific log options. The common log options are configured for each application in the following sections: **log**, **log-extended**, **log-filter**, and **log-filter-data**.

All Genesys Server applications also support a set of common options for operations that are not related to logs.

[+] Show table

Changes in Common Options

Option	Configuration Section	Type of Change	Changed in Release	Additional Information
compatible-output-priority	log	Removed	8.5	
enable-thread	log	New	8.5	
expire	log	Modified	8.5	
message-format	log	Renamed	8.5	Formerly named message_format
no-memory-mapping	log	New	8.5	
segment	log	Modified	8.5	
snapshot	log	New	8.5	
throttle-period	log	New	8.5	
throttle-threshold	log	New	8.5	
hide-tlib-sensitive-data	log-filter	New	8.5	
sec-protocol	security	New	8.5	
tls-mutual	security	New	8.5	
autostart	sml	New	8.5	
n/a	dbserver	Removed	8.5	Section removed
dml_retry	dbserver	Moved	8.5	Moved to Configuration Server
sec-protocol	Transport Parameters	New	8.5	
enable-async-dns	common	Modified	8.1	
cipher-list	security	New	8.1	
tls-crl	security	New	8.1	
tls-target-name-check	security	New	8.1	
n/a	security-authentication-rules	New	8.1	New section
account-override-lockout	security-authentication-rules	New	8.1	
last-expired-at	security-authentication-rules	New	8.1	Read-only
last-locked-at	security-authentication-rules	New	8.1	Read-only
no-change-	security-	New	8.1	

password-at-first-login	authentication-rules			
override-account-expiration	security-authentication-rules	New	8.1	
heartbeat-period	sml	Modified	8.1	
default-filter-type	log-filter	Modified	8.1	
filtering	log-filter	New	8.1	
<key-name>	log-filter-data	Modified	8.1	
dml-retry	dbserver	New	8.1	
enable-ipv6	common	New	8.1	
cipher-list	Transport Parameters	New	8.1	
ip-version	Transport Parameters	New	8.1	
expire	log	Modified	8.0	
default-filter-type	log-filter	Modified	8.0	
<key-name>	log-filter-data	Modified	8.0	
n/a	security	New	8.0	New section
disable-rbac	security	New	8.0	
heartbeat-period	sml	New	8.0	
heartbeat-period-threadclass-<n>	sml	New	8.0	
hangup-restart	sml	New	8.0	
suspending-wait-timeout	sml	New	8.0	
alarm	log	Moved	7.6	Moved from Solution Control Server.
x-conn-debug-open	log	New	7.6	Use only when requested by Genesys Customer Care.
x-conn-debug-select	log	New	7.6	
x-conn-debug-timers	log	New	7.6	
x-conn-debug-write	log	New	7.6	
x-conn-debug-security	log	New	7.6	
x-conn-debug-api	log	New	7.6	
x-conn-debug-dns	log	New	7.6	
x-conn-debug-all	log	New	7.6	
n/a	common	New	7.6	New section

rebind-delay	common	New	7.6	Use only when requested by Genesys Customer Care.
enable-async-dns	common	New	7.6	Use only when requested by Genesys Customer Care. Use only with T-Servers.
n/a	extended-log	New	7.6	New section
level-reassign-<eventID>	extended-log	New	7.6	
level-reassign-disable	extended-log	New	7.6	
address	Transport Parameters	New	7.6	
backup-port	Transport Parameters	New	7.6	
port	Transport Parameters	New	7.6	

DB Server

The following table lists all configuration option changes in DB Server from release 7.6 through 8.1, with the most recent changes listed first.

> **Important**
> DB Server is not a part of Management Framework 8.5.

[+] Show table

Option Changes in DB Server

Option	Configuration Section	Type of Change	Changed in Release	Additional Information
db-request-timeout	dbserver	New	8.0	
dbprocess_name	dbserver	Modified	8.0	
db2_name	dbserver	Modified	8.0	
informix_name	dbserver	Modified	8.0	
msql_name	dbserver	Modified	8.0	
oracle_name	dbserver	Modified	8.0	
postgre_name	dbserver	New	8.0	

sybase_name	dbserver	Modified	8.0	

Database Access Point

The following table lists all configuration option changes in Database Access Point from release 7.6 through 8.5, with the most recent changes listed first.

[+] Show table

Option Changes in Database Access Point

Option	Configuration Section	Type of Change	Changed in Release	Additional Information
utf8-ucs2	dbclient	New	8.1	
db-request-timeout	dbserver	New	8.0	

Configuration Server

The following table documents all configuration option changes in Configuration Server from release 7.6 through 8.5, with the most recent changes listed first. These options apply to Configuration Server operating in Master mode. Refer to Configuration Server Proxy for configuration option changes in Configuration Server 8.5 running in Proxy mode (also referred to as Configuration Server Proxy).

> **Important**
>
> In the following table, the Configuration Server section is referred to as *confserv* for changes in earlier releases.

[+] Show table

Option Changes in Configuration Server

Option	Configuration Section	Type of Change	Changed in Release	Additional Information
enforce-internal-auth	authentication	New	8.5	
allow-empty-password	Configuration Server	Modified	8.5	Corrected when Changes Take Effect
allow-external-empty-password	Configuration Server	Modified	8.5	Corrected when Changes Take Effect
cfglib-conn-async-tmout	Configuration Server	New	8.5	
client-connect-	Configuration	New	8.5	

timeout	Server			
client-response-timeout	Configuration Server	Modified	8.5	
dbthread	Configuration Server	New	8.5	
decryption-key	Configuration Server	New	8.5	
encryption	Configuration Server	Modified	8.5	
force-offline	Configuration Server	New	8.5	
force-connect-reload	Configuration Server	Moved	8.5	Moved to system section
langid	Configuration Server	New	8.5	
license	Configuration Server	Removed	8.5	
max-client-output-queue-size	Configuration Server	New	8.5	
max-output-queue-size	Configuration Server	New	8.5	
packet-size	Configuration Server	New	8.5	
primary-startup-tmout	Configuration Server	New	8.5	
upgrade-mode	Configuration Server	New	8.5	
addp	Configuration Database	Removed	8.5	
addp-timeout	Configuration Database	Removed	8.5	
addp-trace	Configuration Database	Removed	8.5	
dbengine	Configuration Database	Modified	8.5	
dbname	Configuration Database	Added new Valid Value	8.5	
dbserver	Configuration Database	Added new Valid Value	8.5	
dml-retry	Configuration Database	Moved	8.5	Moved from Common Configuration Options
history-log-guid	Configuration Database	Removed	8.5	
history-log-version	Configuration	Removed	8.5	

	Database			
host	Configuration Database	Removed	8.5	Used only if dbthread=false and with DB Server 8.1; refer to Framework 8.1 documentation.
port	Configuration Database	Removed	8.5	
reconnect-timeout	Configuration Database	Removed	8.5	
server	Configuration Database	Removed	8.5	
ignore-case-username	gauth-kerberos	New	8.5	
n/a	hca	Removed	8.5	Section removed
schema	hca	Removed	8.5	
x-dblib-debug	log	New	8.5	Use only when requested by Genesys Customer Care.
x-dblib-sql	log	New	8.5	
objbrief-api-permission-check	security	New	8.5	
n/a	soap	Removed	8.5	Section removed
client-lifespan	soap	Removed	8.5	
debug	soap	Removed	8.5	
port	soap	Removed	8.5	Used only if dbthread=false and with DB Server 8.1; refer to Framework 8.1 documentation.
n/a	system	New	8.5	New section
force-connect-reload	system	Moved	8.5	Moved from Configuration Server section.
postgre-standard-conforming-strings	system	Removed	8.5	
prevent-mediatype-attr-removal	system	New	8.5	
token-authentication-mode	system	New	8.5	
token-preambula	system	New	}8.5	
token-uuid	system	New	8.5	
skip-environment-enum-transfer	system	New	8.5	
write-former-value	history-log	New	8.5	

user	Application Parameters	New	8.5	
reconnect-timeout	Configuration Database	Modified	8.1	
allow-mixed-encoding	confserv	New	8.1	
enable-pre-812-security	confserv	New	8.1	
force-md5	confserv	New	8.1	
multi-languages	confserv	New	8.1	
password-change	confserv	New	8.1	
packet-size	confserv	New	8.1	
peer-switchover-tmout	confserv	New	8.1	
chase-referrals	gauth_ldap[_n]	New	8.1	
objbrief-api-permission-check	security	New	8.1	Added to version 8.1.300.27
port	soap	Modified	8.1	
all	history-log-section	Modified	8.0	Does not apply to master Configuration Server. Not documented in previous versions of this document.
failsafe-store-processing	history-log-section	Modified	8.0	
protocol	confserv/<application>	New	8.0	
addp-timeout	confserv/<application>	New	8.0	Same name as existing options, but placed in different configuration section.
addp-remote-timeout	confserv/<application>	New	8.0	
addp-trace	confserv/<application>	New	8.0	
fix_cs_version_7x	confserv	New	8.0	
allow-external-empty-password	confserv	New	8.0	
last-login	confserv	New	8.0	
last-login-synchronize	confserv	New	8.0	
objects-cache	confserv	New	8.0	
disable-vag-calculation	<application>	New	7.6	
all	history-log	Modified	7.6	
history-log-file-name c	confserv	Obsolete	7.6	Replaced by options in history-log section.
history-log-	confserv	Obsolete	7.6	

expiration				
history-log-client-expiration	confserv	Obsolete	7.6	
history-log-max-records	confserv	Obsolete	7.6	
history-log-active	confserv	Obsolete	7.6	
no-default-access	security	New	7.6	
all	history-log	New	7.6	
expiration	history-log	New	7.6	
client-expiration	history-log	New	7.6	
max-records	history-log	New	7.6	
active	history-log	New	7.6	
failsafe-store-processing	history-log	New	7.6	
backlog	Application Parameter	New	7.6	Use only when requested by Genesys Customer Care.

Configuration Server Proxy

The following table documents all configuration option changes in Configuration Server running in Proxy mode (also referred to as Configuration Server Proxy) mode from release 7.6 through 8.5, with the most recent changes listed first.

[+] Show table

Option Changes in Configuration Server Proxy

Option	Configuration Section	Type of Change	Changed in Release	Additional Information
enforce-internal-auth	authentication	New	8.5	
allow-empty-password	csproxy	New	8.5	
allow-external-empty-password	csproxy	New	8.5	
management-port	csproxy	New	8.5	
proxy-cluster-name	csproxy	New	8.5	
client-response-timeout	csproxy	Modified	8.5	
max-client-output-queue-size	csproxy	New	8.5	
max-output-queue-size	csproxy	New	8.5	
packet-size	csproxy	New	8.5	

proxy-cluster-name	csproxy	New	8.5	
ignore-case-username	gauth-kerberos	New	8.5	
active	history-log	Removed	8.5	
all	history-log	Removed	8.5	
expiration	history-log	Removed	8.5	
failsafe-store-processing	history-log	Removed	8.5	
max-records	history-log	Removed	8.5	
n/a	soap	Removed	8.5	Section removed
client-lifespan	soap	Removed	8.5	
debug	soap	Removed	8.5	
max-records	soap	Removed	8.5	
user	Application Parameters	New	8.5	
n/a	authentication	New	8.1	New section
library	authentication	New	8.1	
enforce-external-auth	authentication	New	8.1	
allow-mixed-encoding	csproxy	New	8.1	
client-response-timeout	csproxy	New	8.1	
packet-size	csproxy	New	8.1	
n/a	gauth_ldap	New	8.1	New section
ldap_url	gauth_ldap	New	8.1	
verbose	gauth_ldap	New	8.1	
retry_attempts	gauth_ldap	New	8.1	
retry_interval	gauth_ldap	New	8.1	
proxy-writable	csproxy	Modified	8.0	
last-login	csproxy	New	8.0	
last-login-synchronize	csproxy	New	8.0	
objects-cache	csproxy	New	8.0	
proxy-writable	csproxy	New	7.6	
expiration	history-log	Modified	7.6	
client-expiration	history-log	Modified	7.6	
max-records	history-log	Modified	7.6	
failsafe-store-processing	history-log	New	7.6	
all	history-log	Modified	7.6	

backlog	Application Parameter	New	7.6	Use only when requested by Genesys Customer Care.

Configuration Manager

The following table documents all configuration option changes in Configuration Manager from release 7.6 through 8.1, with the most recent changes listed first.

This table does not include configuration options for Genesys Administrator, which might have been set in the Configuration Manager Application object with which Genesys Administrator is bound, or associated, during its deployment.

> **Important**
> Configuration Manager was not updated in release 8.5.

[+] Show table

Option Changes in Configuration Manager

Option	Configuration Section	Type of Change	Changed in Release	Additional Information
inactivity-timeout	security	New	7.6	

Local Control Agent

Local Control Agents supports common log options which allows you to precisely configure log output for LCA. Because you do not configure an Application object for LCA, if you need to change the default log option settings, modify the configuration file called **lca.cfg** and specify new values for appropriate options. The file must be located in the same directory as the Local Control Agent executable file.

The following table documents all other configuration option changes in Local Control Agent from release 7.6 through 8.5, with the most recent changes listed first. For more information about the LCA configuration file and for related instructions, see the *Framework Deployment Guide*.

[+] Show table

Option Changes in Local Control Agent

Option	Configuration Section	Type of Change	Changed in Release	Additional Information
wmiquery-timeout	general	New	8.5	
lookup_clienthost	general	New	8.1	
upgrade	security	Correction	8.1	Originally documented as Host option

Genesys Deployment Agent

> **Important**
>
> Support is discontinued for Genesys Deployment Agent (GDA) in LCA release 8.5.100.31 and later.

Starting in release 8.0, the Genesys Deployment Agent is deployed with LCA. The Genesys Deployment Agent is used by of Genesys Administrator Extension to deploy Genesys Applications and Solutions on a Host. To enable this functionality, you must identify what port on the Host that the Genesys Deployment Agent will use to communicate with Genesys Administrator Extension. You provide this information in the Host's Annex, in the new section **rdm**, specifying the port number with the configuration option port.

Genesys Deployment Agent supports common log options which allows you to precisely configure log output for Genesys Deployment Agent. Because you do not configure an Application object for Genesys Deployment Agent, if you need to change the default log option settings, create a configuration file called **gda.cfg** (or rename and modify the **gda.cfg.sample** file that is located in the installation folder) and specify new values for appropriate options. The file must be located in the same directory as the Genesys Deployment Agent executable file (**gda.exe**).

> **Important**
>
> In release 8.5.1, Genesys Deployment Agent is not installed with Local Control Agent by default.

The following table lists all other configuration option changes in Genesys Deployment Agent from release 8.0 through 8.5, with the most recent changes listed first. For more information about the Genesys Deployment Agent, refer to the *Framework Deployment Guide*.

[+] Show table

Option Changes in Genesys Deployment Agent

Option	Configuration Section	Type of Change	Changed in Release	Additional Information
n/a	security	New	8.1	New section
transport	security	New	8.1	
n/a	web	New	8.0	New section
rootdir	web	New	8.0	

Message Server

The following table lists configuration option changes in Message Server from release 7.6 through 8.5, with the most recent changes listed first.

[+] Show table

Option Changes in Message Server

Option	Configuration Section	Type of Change	Changed in Release	Additional Information
dbthread	messages	New	8.5	
x-dblib-debug	log	New	8.5	
signature	MessageServer	New	8.0	
request-queue-size	messages	Removed	8.0	

Solution Control Server

The following table lists configuration option changes in Solution Control Server from release 7.6 through 8.5, with the most recent changes listed first.

[+] Show table

Option Changes in Solution Control Server

Option	Configuration Section	Type of Change	Changed in Release	Additional Information
default-audit-username	general	New	8.5	
disable-switchover	general	New	8.5	
distributed_sync_timeout	general	New	8.5	
hostinfo-load-timeout	general	New	8.5	
max_switchover_time	general	Removed	8.5	
ha_service_unavail_primary	general	New	8.1	
lookup_clienthost	general	New	8.1	
max-req-per-loop	general	New	8.1	
alarms-port	Transport Parameter	New	8.1	
backup-alarms-port	Transport Parameter	New	8.1	
alarm	log	Moved	7.6	Moved to common configuration options.

Solution Control Interface

The following table lists configuration option changes in Solution Control Interface from release 7.6 through 8.0, with the most recent changes listed first.

> **Important**
> Solution Control Interface was not updated after release 8.0.

[+] Show table

Option Changes in Solution Control Interface

Option	Configuration Section	Type of Change	Changed in Release	Additional Information
n/a	host-status-display	New	8.0	New section
critical-color	host-status-display	New	8.0	
major-color	host-status-display	New	8.0	
other-color	host-status-display	New	8.0	
inactivity-timeout	security	New	7.6	

SNMP Master Agent

The following table lists configuration option changes in Genesys SNMP Master Agent from release 7.6 through 8.1, and in SNMP Master Agent in 8.5, with the most recent changes listed first.

Note: Starting in release 8.5, you can use a 3rd-party Net-SNMP Master Agent instead of Genesys SNMP Master Agent, re-using the same configuration object. Refer to the *Framework Deployment Guide* for more information about Net-SNMP and Genesys SNMP Master Agent. See the instructions in Migrating to Net-SNMP to convert a Genesys SNMP Master Agent Application object to use with Net-SNMP.

[+] Show table

Option Changes in SNMP Master Agent

Option	Configuration Section	Type of Change	Changed in Release	Additional Information
netsnmp-enable	snmp	New	8.5	
n/a	snmp-v3-auth	New	8.1	New section
password	snmp-v3-auth	New	8.1	
n/a	snmp-v3-priv	New	8.1	New section
password	snmp-v3-priv	New	8.1	
v3priv_protocol	snmp	Modified	8.0	

Tenant

The following table lists Tenant- and User-level configuration option changes from release 7.6 through 8.5, with the most recent changes listed first.

[+] Show table

Tenant and User Option Changes

Option	Configuration Section	Type of Change	Changed in Release	Additional Information
account-override-lockout	security-authentication-rules	Modified	8.5	User-level option Corrected description of when set to `false`
force-password-reset	security-authentication-rules	New	8.1	
max-account-sessions	security-authentication-rules	New	8.1	
password-expiration	security-authentication-rules	New	8.1	
password-expiration-notify	security-authentication-rules	New	8.1	
password-no-repeats	security-authentication-rules	New	8.1	
password-req-punctuation	security-authentication-rules	New	8.1	
tenant-override-section	security-authentication-rules	New	8.1	
password-req-number	security-authentication-rules	New	8.0	Not documented in previous releases of this document.
password-req-mixed-case	security-authentication-rules	New	8.0	
password-req-alpha	security-authentication-rules	New	8.0	
account-lockout-threshold	security-authentication-rules	New	8.0	
account-lockout-duration	security-authentication-rules	New	8.0	
account-lockout-attempts-period	security-authentication-rules	New	8.0	
password-min-length	security-authentication-rules	New	8.0	

Host

The following table lists Host-level configuration option changes from release 7.6 through 8.5, with the most recent changes listed first.

[+] Show table

Host-Level Option Changes

Option	Configuration Section	Type of Change	Changed in Release	Additional Information
sec-protocol	security	New	8.5	
n/a	ntp-service-control	New	8.1	New section
signature	ntp-service-control	New	8.1	
cipher-list	security	New	8.1	
lca-upgrade	security	New	8.1	
n/a	transport	New	8.1	New section
ip-version	transport	New	8.1	
n/a	rdm	New	8.0	New section
port	rdm	New	8.0	Not documented in previous releases of this document.
n/a	security	New	8.0	New section
gda-tls	security	New	8.0	Not documented in previous releases of this document.
n/a	addp	New	7.6	New section
addp-remote-timeout	addp	New	7.6	Not documented in previous releases of this document.
addp-timeout	addp	New	7.6	

Mandatory Changes in Configuration of Framework Components

When upgrading Configuration Server to release 8.5, you must modify the existing configuration file to include the **[<name of conf server app>]dbthread**=`false` option to continue using your existing DB Server. Alternatively, consider installing and configuring DBMS client software on the same host where the Configuration Server instance resides (to make it available to Configuration Server) and set connection parameters in the configuration file to access the DBMS from that host (see the *Framework Deployment Guide* for details). In this case, you no longer need a separate DB Server for Configuration Server to access the database.

When updating the Configuration Database schema version to 8.5, and newer, in an environment where Configuration Server 8.5 is already being used (against a database schema of a prior version), you have to specify the **[<name of config server app>]langid** option. Set this option to `1033` when upgrading an English environment. See Localized Environments for details on how to set the option for other languages.

When upgrading Configuration Server from release 8.0 or older in environment where Configuration Server Proxies are being deployed, make sure you set the **force-md5** option to `true` on the master Configuration Server until you have completed upgrading all Configuration Server Proxies in your environment to the latest version.

Mandatory Changes in Secure Protocol Configuration

When you upgrade your Genesys applications that are configured to communicate securely using Genesys Security Pack on UNIX (or Linux), versions 8.5.1 or later, or you upgrade your Windows operating system to the latest version or Service pack, make sure you are using certificates that are signed using SHA1 or higher across all server applications with which new or updated components have to communicate. If you have previously generated MD5 signed certificates using tools provided with Genesys Security Pack, re-issue them as soon as possible using Security Pack 8.5.1 or later. MD5 certificates are no longer accepted by the latest secure protocol implemenations.

Configuration Conversion Wizard (CCW)

This section provides information about how to install and configure CCW, and how to use it to migrate your Configuration Database schema or locale.

Installing Configuration Conversion Wizard

Install Configuration Conversion Wizard only if you want or need to upgrade the Configuration Database (see the table here to help you decide). Use the following procedure:

[+] Show procedure

Prerequisite

- DB Server is installed and connected to the existing Configuration Database.
- No previous version of CCW is installed on this machine; if so, uninstall it before beginning this procedure.

Procedure

1. Locate the installation package on the Management Framework product DVD in the **configuration_layer/convers_wizard/window** directory.
2. Locate and double-click `Setup.exe` to start installation.
3. Specify the program folder to which you want to add CCW. By default, it is added to the **Genesys Solutions/Framework** folder.
4. When the CCW icons appear, click **Finish** to complete the installation.

When the setup program is finished, CCW is ready to start; however, to operate, it requires that you specify connection parameters, as specified in the following section, Specifying the Database Connection.

Specifying the Database Connection

To connect to your existing Configuration Database, CCW requires information about that database and the DB Server through which the database is to be accessed. You provide this information in one of two ways:

- As configuration option values within the database connection configuration file named **convers.cfg**. Use the instructions in Configuring the Local Configuration File.
- As values entered interactively, during startup. Use the instructions in Entering Connection Parameters Dynamically.

Configuring the Local Configuration File

To create a file listing database connection parameters, do the following:

1. Open the local configuration file (**convers.cfg**) in the directory where CCW is installed.
2. Within this file, specify the values for the configuration options described in this section. For configuration option values, use information about DB Server, the existing Configuration Database, and the DBMS user account through which the database is currently accessed. See “Sample Configuration File” for an example of a database connection configuration file.

> **Warning**
> Do not use the **Tab** key for entries in the configuration file.

3. Save the configuration file.

Entering Connection Parameters Dynamically

If you do not configure a configuration file with the connection parameters, CCW prompts you to enter the parameters during startup.

To provide CCW with information about the Configuration Database and about the DB Server through which CCW must access this database, the following parameters are required:

1. The host name of the computer running DB Server that provides access to the Configuration Database.
2. The TCP/IP port that clients should use to connect to the DB Server through which the Configuration Database is to be accessed.
3. The type of DBMS (engine) that handles the Configuration Database.
4. The name or alias identifying the DBMS that handles the Configuration Database.
5. The name of the Configuration Database to be accessed as specified in the DBMS that handles this database.
6. The user name established in the DBMS to access the Configuration Database.
7. The password established in the DBMS to access the Configuration Database.

CCW Configuration Options

Specify values for the following options to provide CCW with information about the Configuration

Database, and about the DB Server through which CCW must access this database.

> **Important**
>
> If you are changing the connection parameters after initial installation, you must save the configuration file and re-specify it in the **Connection to the Configuration Layer Database** screen of CCW.

host
Default Value: No default value
Valid Value: Any valid host name
Changes Take Effect: After configuration file is specified in CCW

Specifies the host name of the computer running DB Server through which the Configuration Database is to be accessed.

port
Default Value: No default value
Valid Value: Any valid TCP/IP port
Changes Take Effect: After configuration file is specified in CCW

Specifies the TCP/IP port that clients should use to connect to the DB Server through which the Configuration Database is to be accessed.

dbengine
Default Value: No default value
Valid Values: `oracle`, `mssql`, `db2`, `postgresql`
Changes Take Effect: After configuration file is specified in CCW

Specifies the type of DBMS that handles the Configuration Database.

dbname
Default Value: No default value
Valid Value: Any database name
Changes Take Effect: After configuration file is specified in CCW

Specifies the name of the Configuration Database to be accessed as specified in the DBMS that handles this database. A value for this option must be specified unless **dbengine=oracle**.

dbserver
Default Value: No default value
Valid Value: Any valid entry name
Changes Take Effect: After configuration file is specified in CCW

Specifies the name or alias identifying the DBMS that handles the Configuration Database.

dbtimeout
Default Value: No default value
Valid Value: Any positive integer
Changes Take Effect: After configuration file is specified in CCW

Specifies the maximum time, in seconds, before which CCW should cease attempting to make its

initial connection to DB Server.

dbrequest-timeout
Default Value: 30
Valid Value: 1 – 3000
Changes Take Effect: After configuration file is specified in CCW

Specifies the maximum time, in seconds, in which the database request should be completed. If the request does not complete in this time, the request is cancelled, the import procedure is aborted, and a corresponding message is displayed to the user.

username
Default Value: No default value
Valid Value: Any character string
Changes Take Effect: After configuration file is specified in CCW

Specifies the user name established in the DBMS to access the Configuration Database.

password
Default Value: No default value
Valid Value: Any character string
Changes Take Effect: After configuration file is specified in CCW

Specifies the password established in the DBMS to access the Configuration Database.

If required, you can encrypt this password in the database, so it does not appear in plain text in logs or other reports. For more information, refer to the *Genesys Security Deployment Guide*.

delete-in-size
Default Value: 200
Valid Value: 1 – 32767
Changes Take Effect: After configuration file is specified in CCW

Specified only when migrating from release 6.5; specifies the number of fields in an SQL query that uses the IN statement, such as:
`DELETE... FROM ... WHERE ... IN (X1, ..., An)` where n = value of **delete-in-size**.

Use this option to limit the length of SQL queries that use the IN statement.

Sample Configuration File

```
host = db-host
port = 4040
dbengine = mssql
dbserver = server_name
dbname = config
username = DBMS_user
password = DBMS_user_password
```

Using CCW to Migrate Your Configuration Database or Locale

You do not always have to migrate your Configuration Database to the current format—see the table here to determine if you need to upgrade to the 8.5 format, or just upgrade the locale. But if you do

need or want to upgrade, use CCW.

Migrate the Database

Use the Genesys Configuration Conversion Wizard (CCW) to convert existing data structures to the current format. CCW performs automatic migration from any release to the current release of Management Framework. When migrating the Configuration Database, CCW uses a copy of the original database, and migrates that copy. This enables you to keep the original Configuration Database and Configuration Server in service while you are performing the migration.

CCW only converts the database structures originally created with the Genesys initialization scripts. CCW does not convert any custom tables or columns that you might have added to the Configuration Database.

After the conversion, CCW generates a detailed report of conversion statistics, including database changes, for your review. The same information is stored in a log file that CCW creates for each working session.

Upgrade the Locale

If your current Configuration Database is using the 8.1.1 or later schema, you do not have to migrate your database to get new data types and enumerators that have been added in the new Configuration Database schema. If you want to use the new types and enumerators, you can use CCW to update only the localization information stored in the database. Otherwise, you do not need to do anything - the new version of Configuration Server 8.5 will run against your current Configuration Database. Future versions of Configuration Server will include extensions to the list of application types you can utilize without migrating your system.

To upgrade your locale, use the instructions in the **Using CCW** tab in Upgrading Configuration Definitions.

> ### Important
> To update the locale, you must use the version of CCW that is the same as your current database. For example, you must use CCW 8.1 for 8.1 databases, and CCW 8.5 for 8.5 databases. You can only upgrade your locale if the database has already been migrated. That is, CCW will not offer the option to upgrade the locale if the database is older than CCW itself.