GENESYS™

Framework Migration Guide

Overview

12/20/2025

Contents

Overview

This page provides compatibility information for upgrading Management Framework to 8.5 and 9.0. 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.

Framework Component Changes In Release 7.6 to 9.0

Component Name	Type of Change	Component Release or Date	Details
Configuration Database	New functionality	8.5.100.24	Support for the Red Hat

Maintenance Scripts			Enterprise Linux AP 8 and virtualization (KVM) in Red Hat 8 operating system.
		8.5.100.22	New version of locale to support a generic Linux OS type for creating Linux hosts.
		8.5.100.19	Support for the CentOS Linux 7 operating system.
		8.5.100.18	Additional scripts to convert a single-tenant Configuration Database to a multi-tenant Configuration Database.

Configuration Server / Configuration Server Proxy	New functionality	8.5.101.50	• Configuration Server supports:
			
			  • MSSQL Server 2019 database on Windows and Linux.
			
			  • Oracle 19c database with Oracle client 12.x and Oracle 19c RAC database.
			
			  • Red Hat Enterprise Linux AP 8 and virtualization (KVM) in Red Hat 8 operating system.
			
			• Master Configuration Server now supports optional restrictions on a number of linked items that can be added/removed from properties of configuration objects in a single request. This applies to changes in Agent Group, Place Group, Access Group, Place, DN Group, and Folder objects that have fields linking

			other objects there. • Configuration Server Proxy (CSProxy) now provides local redundancy against prolonged failure/ unavailability of the master Configuration Server. This allows you to start/restart local CSProxy using configuration database in read-only mode.
		8.5.101.42	• Configuration Server external authentication now uses OpenSSL version 1.0.2s for Windows and Linux operating systems, and OpenSSL version 1.0.2r for AIX and Solaris operating systems. • New configuration option to specify the segmentation limit for the statistics log file. • Configuration Server now allows you to restrict the number of configuration objects or shortcuts that can be deleted within a particular time period for a user account. • Configuration Server now prohibits users from disabling the default user.
		8.5.101.41	Configuration Server external authentication supports caching of the user credentials.

		8.5.101.38	New configuration options to enable the following features: • Selectively delay data reload performed by multiple Configuration Server proxies at a time. • Print statistics on Configuration Server operations to a separate log file on a periodic basis. • Select ports for connections based on the listening port ID and the HA Sync attribute.
		8.5.101.36	Support for the Microsoft Hyper-V Server 2019 virtualization platform.
		8.5.101.33	• Support for the Windows 2019 operating system. • Configuration Server now supports SQL Server Authentication to connect to an MS SQL Configuration Database using Data Source Name (DSN). • The switchover process of Configuration Server has been improved. Refer to the *Configuration Server Release Note* for more information.
		8.5.101.32	• New configuration option to specify that an account will remain locked out (after multiple failed connection

			attempts) until an administrator manually unlocks it.
			
			• Support for the following databases:
			
			   • Oracle 18c database with Oracle client 12.x.
			
			   • Oracle 18c RAC

		8.5.101.29	• Configuration Server external authentication now uses OpenSSL version 1.0.2q. • Support for a generic Linux OS type when defining the host objects.

		8.5.101.2	• Support for the following operating systems:
			
			   • Oracle Linux 7 with Unbreakable Enterprise Kernel (UEK) 4.x
			
			   • SUSE Linux Enterprise 12
			
			• Enhanced Keep-Alive feature support on connections between LDAP and Configuration Server.
			
			• New configurable option to detect hang-up during the data loading process between the Configuration Server HA pair.

		8.5.101.24	Extended retention policies for audit log records in the configuration database.

			External authentication module supports usage of the User Principal Name (UPN)-style usernames.
		8.5.101.22	Support of MS SQL 2016 (and later) Always On with MultiSubnet Listener for disaster recovery and business continuity scenarios involving the Configuration Database. Improved audit performance with larger databases, including a new filter to extract records from a large set of results.
		8.5.101.21	New configuration option to skip all or some validation of changes in the Annex of a configuration object.
		8.5.101.20	Support of optional transaction serialization in environments where customized applications are used to modify Genesys configuration data. New configuration option to specify a limit on the number of Configuration Server Proxies that can upload information from the master Configuration Server. Support for the following new DBMS vendor clients: • Microsoft SQL client software on Linux and Windows with support for MS SQL Server 2017 • Oracle 12.1 client software on Linux and Windows • PostgreSQL 10.1 client software on Linux and Windows
		8.5.101.18	Support for the CentOS Linux 7 operating system.

			Support for the Oracle 12.2 DBMS client software on Linux and Windows.
		8.5.101.13	Support for the Microsoft Hyper-V Server 2016 virtualization platform.
		8.5.101.12	Support for the Windows 2016 operating system.
		8.5.101.11	Support for Oracle 12c Release 2 Multitenant Pluggable Database (PDB). Support for the Red Hat KVM (Kernel Virtualization Machine) virtualization platform.
DB Server	New functionality	8.5.100.06	Support for: • MSSQL Server 2019 database on Windows and Linux. • Oracle 19c database with Oracle client 12.x and Oracle 19c RAC database. • Red Hat Enterprise Linux AP 8 and virtualization (KVM) in Red Hat 8 operating system.
		8.5.100.02	New option to specify whether DB Server connects to the dbclient through the localhost or a network host.
		8.5.100.01	• Supports Linux 64-bit and Windows 64-bit operating systems only. Support is discontinued for AIX and Solaris operating systems.
DB Server 8.1.3	New functionality	8.1.302.09	• Support for the Windows 2019 operating system. • DB Server now

			supports SQL Server Authentication to connect to an MS SQL Configuration Database by using Data Source Name (DSN). • Support for the Microsoft Hyper-V Server 2019 virtualization platform.
		8.1.302.07	Support for the following databases: • Oracle 18c database with Oracle client 12.x • Oracle 18c RAC
		8.1.302.05	Support for the following operating systems: • Oracle Linux 7 with Unbreakable Enterprise Kernel (UEK) 4.x • SUSE Linux Enterprise 12
		8.1.302.02	Support of MS SQL 2016 (and later) Always On with MultiSubnet Listener for disaster recovery and business continuity scenarios involving the Configuration and Log databases.
		8.1.302.01	Support for the following new DBMS vendor client: • PostgreSQL 10.1 client software on Linux and Windows Support for MS SQL 2017 running on the Windows or Linux operating system

		8.1.302.00	Support for the following new DBMS vendor clients: • Microsoft SQL client software on Linux and Windows • Oracle 12.1 and 12.2 client software on Linux and Windows Support for MS SQL 2017 running on the Linux operating system
		8.1.301.18	Support for the CentOS Linux 7 operating system.
		8.1.301.16	Support for the Microsoft Hyper-V Server 2016 and the Red Hat KVM (Kernel Virtualization Machine) virtualization platforms. Support for Oracle 12c Release 2 Multitenant Pluggable Database (PDB). Support for the Windows 2016 operating system.
Local Control Agent	New functionality	8.5.100.36	Support for the Red Hat Enterprise Linux AP 8 and virtualization (KVM) in Red Hat 8 operating system.
		8.5.100.34	On Windows 64-bit operating systems, Local Control Agent now uses statically linked C runtime libraries.
		8.5.100.32 (Build 2)	• Support for the Windows 2019 operating system. • Support for the Microsoft Hyper-V Server 2019 virtualization platform.
		8.5.100.31	Support is discontinued for Genesys Deployment Agent (GDA).
		8.5.100.29	Support for the

			following operating systems: • Oracle Linux 7 with Unbreakable Enterprise Kernel (UEK) 4.x • SUSE Linux Enterprise 12
		8.5.100.25	New configuration option to specify time limit that LCA waits to receive response from an application for its mode change request before setting the application to Unknown. Support for debug configuration options specified in the LCA command line.
		8.5.100.23 (Build 2)	Support for the CentOS Linux 7 operating system.
8.5.100.22	Support for the Microsoft Hyper-V Server 2016 and the Red Hat KVM (Kernel Virtualization Machine) virtualization platforms. Support for the Windows 2016 operating system.		

Message Server	New functionality	8.5.100.30	• Support for:
			
			  • MSSQL Server 2019 database on Windows and Linux.
			
			  • Oracle 19c database with Oracle client 12.x and Oracle 19c RAC database.
			
			  • Red Hat Enterprise Linux AP 8 and virtualization (KVM) in Red Hat 8 operating system.

		8.5.100.25	• Support for the Windows 2019 operating system. • Message Server now supports SQL Server Authentication to connect to an MS SQL Configuration Database by using Data Source Name (DSN). • Support for the Microsoft Hyper-V Server 2019 virtualization platform.
		8.5.100.23	Support for the following operating systems: • Oracle Linux 7 with Unbreakable Enterprise Kernel (UEK) 4.x • SUSE Linux Enterprise 12 Support for the following databases: • Oracle 18c database with Oracle client 12.x • Oracle 18c RAC
		8.5.100.19	Support of MS SQL 2016 (and later) Always On with MultiSubnet Listener for disaster recovery and business continuity scenarios involving the Log Database.
		8.5.100.16	Support for the following new DBMS vendor clients: • Microsoft SQL client software on Linux and Windows with support for MS SQL

			Server 2017 • Oracle 12.1 and 12.2 client software on Linux and Windows • PostgreSQL 10.1 client software on Linux and Windows
		8.5.100.14 (Build 2)	Support for the CentOS Linux 7 operating system.
		8.5.100.14	Support for the Microsoft Hyper-V Server 2016 and the Red Hat KVM (Kernel Virtualization Machine) virtualization platforms. Support for Oracle 12c Release 2 Multitenant Pluggable Database (PDB). Support for the Windows 2016 operating system.
Solution Control Server	New functionality	8.5.100.46	Support for the Red Hat Enterprise Linux AP 8 and virtualization (KVM) in Red Hat 8 operating system.

		8.5.100.42	• The following utilities are no longer installed by default with Solution Control Server:
			
			  • logmsg
			  • mlcmd
			  • gstuckcalls
			  • Scripts for gstuckcalls
			  • SNMP utilities and scripts
			
			• New configuration option to specify whether SCS connects to the Genesys SNMP Master Agent through the localhost or a

			network host.
		8.5.100.41	Support for the Microsoft Hyper-V Server 2019 virtualization platform.
		8.5.100.40	Support for the Windows 2019 operating system.
		8.5.100.36	Support for the following operating systems: • Oracle Linux 7 with Unbreakable Enterprise Kernel (UEK) 4.x • SUSE Linux Enterprise 12
		8.5.100.31	Support for debug configuration options specified in the SCS command line. Support for new log statements to create alarms to detect "split brain" or "no brain" state of applications.
		8.5.100.26	New timeout in which Solution Control Server can expect a TCP success or failure response from Configuration Server to which it is connecting. Support for the CentOS Linux 7 operating system.
		8.5.100.25	Support for the Microsoft Hyper-V Server 2016 and the Red Hat KVM (Kernel Virtualization Machine) virtualization platforms. Support for the Windows 2016 operating system.
Security Pack on UNIX	New functionality	8.5.100.23	• Support for the Red Hat Enterprise Linux AP 8 and virtualization (KVM) in Red Hat 8 operating system.

			• Supports Server Name Indication (SNI) extension in TLS handshake.
		8.5.100.21	Security Pack now uses 1.0.2s for Windows and Linux operating systems, and OpenSSL version 1.0.2r for AIX and Solaris operating systems.
		8.5.100.19	Security Pack now uses OpenSSL version 1.0.2q.
		8.5.100.18	• Support for the following operating systems: • Oracle Linux 7 with Unbreakable Enterprise Kernel (UEK) 4.x • SUSE Linux Enterprise 12 • Security Pack now includes FIPS 140-2 encryption compliance on Linux only.
		8.5.100.14	Support for the CentOS Linux 7 operating system.
		8.5.100.13	Support for the Microsoft Hyper-V Server 2016 and the Red Hat KVM (Kernel Virtualization Machine) virtualization platforms. You can now set alternative IP addresses when running create_cert.sh.
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 scripts are included in this component toh elp you maintain and analyse the performance and data integrity of the 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.
Configuration Database	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 SCS 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 functionality	8.1.101.04	Support Windows 10, version 1809 and Windows Server 2016 operating systems.
	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.
Solution Control Interface	New functionality	8.0.301.05	Support for Windows 10, and Windows Server 2012 and 2016 operating systems.
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.\n\nDB 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.\n\nAdvanced 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.\n\nYou can now configure, at the Tenant level, a minimum length for all passwords used to gain access to applications within that Tenant.\n\nYou 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.

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.