eServices Administrator's Guide

UCS Administration

4/30/2025

Contents

- 1 UCS Administration
  - 1.1 Access to Configuration Server
  - 1.2 Client Connection Timeout
  - 1.3 Contact Identification and Creation
  - 1.4 Character Sets
  - 1.5 TLS and IPv6
  - 1.6 Database Performance

UCS Administration

This section provides information for administrators regarding Universal Contact Server (UCS). In addition to the topics on this page, there is also the following:

- Special instructions on enabling a user who is not the schema owner to run UCS with an Oracle database
- Queries that users of the UCS database must have permission to run
- Updating interaction data in a routing strategy
- Limitations to observe in operating UCS
- Enabling full text searching of the UCS database
- Masking sensitive data, such as credit card numbers, phone numbers, and Social Security numbers, in UCS logs.

Access to Configuration Server

Be sure to run UCS with a user that has write access to the Configuration Server database for all the tenants associated with this UCS (that is, the user specified on the `Security` tab of the UCS Application object).

This means that UCS does not support Configuration Server Proxy version 8.0.2 and earlier, which has only read access to the Configuration Server database. UCS does support Configuration Server Proxy version 8.0.3 and later.

Client Connection Timeout

To avoid inconsistency, every client of UCS should have the timeout of its connection to UCS set to a higher value than the timeout of UCS's connection to its Database Access Point (DAP).

This allows UCS to consistently either perform long queries or abort them, in accord with the clients' requirements.

Contact Identification and Creation

When a new interaction enters the system, UCS performs the following tasks:

1. Contact identification—UCS checks whether this interaction is coming from a known contact: more precisely, whether the contact data included in the new interaction matches an existing contact in the

UCS database. UCS does this in response to a request from a media server, the `Identify Contact` Routing strategy object, or the Agent Interaction SDK `CreateInteraction` method.

2. Contact creation—If the contact does not exist in the database, UCS creates a new record to represent it.

Character Sets

Oracle

The character set `WE8ISO8859P1` does not have any representation of characters in the range 128–159. Because of this, with an Oracle database, attempting to save characters in this range in a column of type `NCHAR` or `NVARCHAR` results in corrupted data. Genesys recommends that for non-Unicode deployment you set the Oracle `NLS_CHARACTERSET` parameter to `WE8MSWIN1252` instead of `WE8ISO8859P1`. `WE8MSWIN1252` is a superset of `WE8ISO8859P1`, so there will be no data loss for most European languages (but data in non-Latin writing systems will still be corrupted).

For support of non-Latin charsets, use the following parameter settings in Oracle:

```
NLS_CHARACTERSET AL32UTF8

NLS_NCHAR_CHARACTERSET AL16UTF16
```

DB2 and PostgreSQL

DB2 and PostgreSQL must use the UTF-8 codeset for the UCS database.

Important

UCS support of PostgreSQL is limited and does not support the following:

- Multiple-site deployment
- Multi-tenant deplyoment
- Clusters
- High availability
- Load balancing

TLS and IPv6

The following two items also apply to E-mail Server.

TLS Connection as Windows Service

When UCS has Transport Layer Security (TLS) configured, either as a server on its ESP port, or as a client in its connection to Message Server, there are two ways to enable it as a Windows Service:

Log on As a Local Host User

1. Select the Windows service related to UCS.
2. Select the `Log On` tab. The default setting is `Log on as local system account.`
3. Select `Log on as this account` and provide the login/password of a local host user.

Import a Certificate to the Local System Account

Do one of the following:

- Run `psexec.exe -i -s mmc.exe`, then import a certificate for a user that is the local system account.
- Run `psexec.exe -i -s certutil -f -user -p [password] -importpfx [path to the certificate]`

Notes on `psexec.exe`:

- With the flag `-s`, `psexec.exe` executes the specified program under the system account.
- psexec is part of PSTools, which can be downloaded from http://technet.microsoft.com/en-US/sysinternals

Mixing IPv6 and IPv4

UCS and E-mail Server do not support the command-line option `transport-ip-version`. If either of these is connected to Configuration Server using IPv6 but connected to other components using IPv4, you must add the following argument to `(ContactServerDriver|JavaEmailServerDriver).ini`:

```
-Djava.net.preferIPv6Addresses=true
```

Database Performance

OLTP

For best performance, Genesys strongly recommends that you set up the UCS database as OLTP (online transaction processing).

Tuning for Attachments

UCS uses the `Content` field of the `Document` table to store attachments; also, the `Content` field of the `ixnContent` table stores raw e-mails, including attachment data. If you plan to store large attachments (bigger than 5 MB), you should tune the database according to the recommendations of

your database vendor.

For example, increasing the block size of database files for these fields can greatly enhance performance in access and storing of large attachments, at the cost of a slight loss of performance with smaller ones. Also, some databases offer the ability to partition data according to specified criteria. Both tables have a `theSize` column that you can use to do such partitioning. This could enable you to store small attachments in a specific file and large ones in another, for example.

Refer to the tuning guides of your database vendor for more information.