



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

# Workforce Management Administrator's Guide

MS SQL Database Replication

12/18/2025

---

## Contents

- 1 MS SQL Database Replication
  - 1.1 System Requirements
  - 1.2 Setting Up the Database Replication
  - 1.3 Maintaining Database Replication
  - 1.4 Application-Level Access Limitations

# MS SQL Database Replication

This topic contains information that will help you to replicate and maintain your MS SQL database for your Workforce Management deployment, based on the assumption that there is an existing single database instance.

Before you begin replicating the database, ensure that the existing instance is updated to the latest version. For new WFM installations, create a database as described in [Create Your WFM Database](#).

## System Requirements

The replication solution requires MS SQL Server 2008 R2 Enterprise Edition server.

## Setting Up the Database Replication

There are two ways to set up the replication: copying during replication and copying before replication.

### Copying Data During Replication

**Purpose:** To create a copy of the WFM database during replication.

**Prerequisite:** Your original WFM database has been updated to the latest WFM Database version (if it is not a new installation of WFM).

#### Start of Procedure

1. Use the WFM Backup-Restore Utility (BRU) to backup the original database.
2. Create new database instances in all locations; On each instance, run the BRU to create the WFM table structure. (In this case, the original WFM database is not used.)
3. Set up replication:
  - a. Enable distribution on all servers manually, or by using a script named `1 Before Replication. Enable Distribution - run on all servers.sql`, that is provided by the BRU in the installation directory `\scripts\`.
  - b. Create a Publication on one Database Server manually, or by using the script named `2 Before Replication. Create Publication - run on one server only.sql`, that is provided by the BRU in the installation directory `\scripts\`.
  - c. Make the Publication *peer-to-peer* manually, or by using the script named `3 Before Replication. Enable Peer-To-Peer Replication - run on one server only.sql`, that is provided by the BRU in the installation directory `\scripts\`.

### Important

For the scripts listed in steps 3a, 3b, and 3c, specific Database Server names—and in some cases, other information, such as database name, files location, publication name, user login, and password—must be entered into the script before running it.

- d. Configure the ranges for the primary key values. Identity value ranges must be assigned for replicated tables which use auto-incremented identify fields. WFM Backup-Restore Utility provides a script named 4 Reseed. Change Identify Field Ranges - run on all servers.sql, that you can find in the installation directory \scripts\.

### Important

The identity ranges on each database instance must be unique and values in the script must be modified manually, based on the number of database instances used.

5. Use the Backup-Restore Utility to restore the WFM database backup (from Step 1 above) to any single database instance.

Restored data is synchronized across all locations by MSSQL Server replication.

### End of Procedure

## Copying Data Before Replication

**Purpose:** To create a copy of the WFM database before replication.

**Prerequisite:** Your original WFM database has been updated to the latest WFM Database version (if it is not a new installation of WFM).

### Start of Procedure

1. Back up your WFM database, using BRU backup or MSSQL backup tools.
2. Create new additional database instances, if needed. (In this case, the original WFM database is not used.)
3. Create and restore the database on each new instance using WFM Backup-Restore Utility or restore the MSSQL backup from Step 1.
4. Set up replication:
  - a. Enable distribution on all servers manually, or by using a script named 1 Before Replication. Enable Distribution - run on all servers.sql, that is provided by the BRU in the installation directory \scripts\.
  - b. Create a Publication on one Database Server manually, or by using the script named 2 Before Replication. Create Publication - run on one server only.sql, that is provided by the BRU in the installation directory \scripts\.
  - c. Make the Publication *peer-to-peer* manually, or by using the script named 3 Before Replication. Enable Peer-To-Peer Replication - run on one server only.sql, that is provided by the

BRU in the installation directory \scripts\.

### Important

For the scripts listed in steps 4a, 4b, and 4c, specific Database Server names—and in some cases, other information, such as database name, files location, publication name, user login, and password—must be entered into the script before running it.

- d. Configure the ranges for the primary key values. Identity value ranges must be assigned for replicated tables which use auto-incremented identity fields. WFM Backup-Restore Utility provides a script named 4 Reseed. Change Identify Field Ranges - run on all servers.sql, that you can find in the installation directory \scripts\.

### Important

The identity ranges on each database instance must be unique and values in the script must be modified manually, based on the number of database instances used.

## End of Procedure

## Maintaining Database Replication

After you have backed up your database, you can use the procedure and other information in this section to restore it.

### Restoring Replicated Databases from Backup

**Purpose:** To restore a back up of the replicated database.

#### Start of Procedure

1. Verify that none of the database instances are in use.
2. For MSSQL backups, use Microsoft tools and documentation to restore the backup of the replicated database.
3. For WFM Backup-Restore Utility backups, use the Database Restore functionality on a single instance of the database.

**All data will be replicated and synchronized across the instances.**

#### End of Procedure

## Replication Issues

Due to unforeseen usage scenarios or operational mistakes in access rights configuration, there

---

might be occasional data collisions caused by replication. Solve these collisions on a case-by-case basis, using MSSQL conflict resolution tools.

## Application-Level Access Limitations

Genesys recommends that you deploy the WFM application so that all actively running WFM Server and WFM Data Aggregator components access the same database instance. (*Actively running* means that these components are updating the database.) You could set up WFM Server instances to access and write to different instances of database; If you do, Genesys recommends certain applications and user restrictions (see [Site Access Rights](#) and [Module Access Rights](#)).

Using certain deployment and access limitations ensures that multiple database instances are not modifying the same data at the same time. The MSSQL database replication does not resolve data collisions caused by complex simultaneous modifications of the same data records on different database instances. To prevent collisions on the application level, assign access rights and restrict certain functionality so that it is performed only on the *main* database instance.

### Site Access Rights

When you are configuring the system you must decide which site will be configured by using WFM Web, and on which database instance.

For users who connect to that instance and want to change the data by using WFM Web, you must limit access to only those sites that are to be modified in that particular database instance.

### Module Access Rights

WFM Web contains functionality that involves the modification of data for multiple sites, or data that is not related to a site object and therefore, cannot be protected by site access rights. There are also subsystems which provide access to data that is also modified by WFM Server through the WFM Web interface. Accessibility to this functionality must be limited only to users who are connecting to the main database by using WFM Server.

The following list of subsystems, menu items, or functions must be restricted in local database instances, and be available only to users who are connecting to the main database server:

- User Security—Security option Configuration > Users and Configuration > Roles
- Skills—Security option Configuration > Organization > Skills
- Time Zones—Security option Configuration > Organization > Time Zones
- Organization/BU, Sites—Enable only the security option Configuration > Organization > Add/Edit/Delete
- Organization Teams—These can be accessible on remote sites, but only in read only mode. Enable only the security option Configuration > Organization > Read
- Schedule State Groups—Enable only the security option Configuration > Schedule State Groups

### Important

On the Master database, users must enable both options: Modules > Configuration > Organization > Read and Modules > Configuration > Organization > Add/Edit/Delete. This setting enables users to perform any action on BUs, Sites and Teams.

In Remote locations, users must enable only Modules > Configuration > Organization > Read. This setting enables users to move agents between teams, but they cannot delete or create a BU, site or team.

Disable the Modules > Configuration > Organization > Add/Edit/Delete option for users who connect to and work on remote locations or databases.