Administrator Tools

This panel contains a collection of tools to assist your GMS 7 administrator. The **Administrator tools** panel contains the following tools:

Attachments analyzer

This tool is helpful in database clean-up by finding attachments not attached to records. Selecting this tool from the **Administrator tools** panel generates an Excel document which details all of the attachments in your database, their sizes and to which record they are attached. Those records listed as **orphaned** are stored in the database, but are not currently associated with a records.

Back up your data

GMS Administrators are responsible for ensuring the system database is intact regardless of what situation arises. Backups can be run while other using are in GMS and you can run this function at any time during the day.

Best Practices: We recommend that you make a backup of everything daily. Backups can be run from the command line, which allows you to run backups using Windows scheduling tools.

To complete a backup of GMS 7, select **Back up your data** from the **Administrator tools** panel. Set your options in the **Data backup** screen. Enter the name of your backup file in the **Backup file to create** field. To begin the backup process, select **Run**. When complete, a message will be displayed showing that the backup was successful along with the name and size of your backup file.

Census exporter

This tool allows you to create standardized census export files for SOI. Select the **Census exporter** tool from the **Administrator Tools** panel. When fields are completed, select **Run**. The **.zip** file is saved to the fold you chose and ready to be sent to SOI.

Check for duplicate IDs

Within GMS, all internal ID codes should be unique. However, occasionally, more than one record will contain the ID code. The **Check for duplicate IDs** tool validates tables and checks for records that may have the same internal ID codes and corrects them so no two IDs are alike.

Best Practices: We recommend that you run this check on a regular basis, when an error report indicates a potential duplicate ID, or when importing a large amount of data from another GMS database.

To run a **Check for duplicate IDs**, be sure all users have exited GMS. GMS will check all entry and certification tables, unless you de-select those checkboxes. Select **Run** to initial the check. When complete, GMS will display an on-screen report of the number and types of records that were updated. When **Run in read-only mode** is checked, GMS will look for possible issues, but will not repair them. This is useful as a diagnostic tool.

Check for zip/postal code IDs

GMS can use US and Canadian zip/postal codes to determine its city, state/province, county and country, as well as gauge how far it is from other zip/postal codes. To initiate an installation, from the **Zip/postal code update** tool, select the desired update and then select **Install**. GMS will download the complete update, then apply it to your “sips” table.

Note: The Canadian postal codes database is huge – almost 200MB – therefore non-Canadian user may want to refrain from downloading and installing this file. The United States file is substantially smaller, so Canadian organizations with cross-border traffic and mailings may benefit from having both tables installed.

Concurrent users monitor/who’s logged in

GMS provides a dynamic listing of the people currently using the program. Normally this tool is used to track how many licenses are in use for organizations which have purchased concurrent user licenses, but it’s also helpful for finding out who’s in GMS when maintenance of updates need to be performed. To view who is currently logged in, simple select the **Concurrent users monitor/who’s logged in** tool in the **Administrator tools** panel. Select the **Refresh** link to update the list.

Database connections

This tool allows you to setup new database connections to GMS. Select **Create new** to selected either SQL Server or NexusDB. Complete the Connection name, Server address and Database as appropriate and select **Save** to store the connection. Multiple database connections may be stored in GMS 7.

Edit DQ codes

This tool allows you to maintain DQ codes in GMS 7. Select **Add new DQ code** to make additions to this table.

Encryption key manager

Encryption is a way to encode sensitive data so that only authorized users have access to that information. Encryption keys are used to protect and restrict designated data from unauthorized access. Using encryption keys, you can secure data, even from people who work directly with the data and have access to the database. Data that is encrypted can only be retrieved using the appropriate **decryptions keys**. GMS 7 uses a form of encryption called **public key encryption**. It allows data to be entered and secured without the user being able to read that data later. The **encryption key** is available to all users, but only those with a **decryption key** can read the data. The **decryption key** is stored on a USB flash drive, not the in the database itself. **Decryption keys** can be created and used by specific individuals, such as administrators, to read the secured data. These keys are protected by the use of a passphrase, and that passphrase can be revoked at any time, even without access to the physical key. So, in the event the key is missing (lost or stolen), the data remains protected. There are two types of keys:

Master encryption keys do not have associated passphrases and cannot be revoked.

Best Practices: At least one copy of the master key should be put in a safe or safe deposit box, off site. The data encrypted with the master key cannot be retrieved without at least one copy of this key or a user key derived from it. Encryption keys must never be stored on your computer's hard drive or on your network.

User decryption keys are passphrase protected and can be revoked, even without access to the physical key.

To create a **Master encryption key**, from the **Encryption key manager** tool, select **Create a new master key** link from the left-hand tools panel. The **New Master Key Encryption Wizard** will launch; select **Next** to view the **Key properties**. Select the desired **Encryption group** and **Next** to continue to the **Save keys** screen. Enter the file names of two places – USB flash drive or other removable media – to store the master decryption key and select **Next** to reach the **Finished!** screen. Select **Finish** to complete the creation of the **Master encryption key**.

To create a **User decryption key**, from the **Encryption key manager** tool, select **Create a new user key** link from the left-hand tools panel. The **New User Decryption Key Wizard** will launch. This is similar to the encryption key wizard, but instead creates a **user decryption key** and requires that a master key has already been created. Select **Next** to view the **Key properties** screen. Complete the **Key properties** fields and select **Next**. The **Save keys** screen will open: enter the file names of one or two places – USB flash drive or other removable media – the save the user's decryption key. Select **Next** to reach the **Finished!** Screen: select **Finish** to complete the creation of the **User decryption key**.

To revoke a user’s decryption key from the **Encryption key manager** screen, right-click on the key from the list and select **Revoke**. A **Confirm** window will be displayed alerting you to the fact that decryption key cannot be re-enabled and the user will not be able to access any encryption data unless a new key is generated.

To change a user’ decryption key passphrase requires both the physical data file and the user’s current passphrase. Right-click on a user decryption key and select **Change passphrase**. Enter the new passphrase twice and select **OK**. Choose the file in which to save the modified key.

Note: if a user’s key or passphrase has been compromised, do not just change the user’s passphrase. The passphrase is only associated with the copy of the key, therefore if a key has been copied, it could still be used with the old passphrase the access data. Instead, revoke the user’s key and create a new one, making the old key and all its copies useless.

Enter GMS 7 registration codes

Organizations using GMS 7 are given an organization-specific serial number, which is paired with their organization name. GMS won’t state without that company name/serial number combination. Enter a code by selecting the **Enter GMS 7 registration codes** link from the Administrator tools panel. The Organization name must match the one indicated in your contract for the serial numbers. As appropriate, user the **(add)** link to enter additional registration codes to enable add-on products.

Make a working backup of GMS 7 in another folder

This tool backs up your current data to a folder that you designate, copies GMS 7 and its configuration file into that folder, and places a shortcut on your desktop so that you can work with a copy of your main database in safe place.

You may wish to use this tool for training purposes, when evaluating a new version of GMS 7 without affecting your production database, and when testing a potentially dangerous process without endangering your data.

Select **Make a working backup of GMS 7 in another folder** from the **Administrator tools** panel. On the **Local Backup Tool** screen select a folder to use for this purpose. Select **Create backup**. When complete, a copy of **GMS.exe** will be present in whichever folder you chose. To run, you can double-click on the GMS icon on your desktop. When done testing or evaluating, you can simply delete the entire folder.

Note: You may choose to omit the “**trace**” and/or “**zips**” table as these can be large and not helpful for testing and training.

Photo resize tool

This tool is used to reduce the size of high resolution photos to prevent a slowdown of GMS. Select the **Photo resize tool** from the **Administrator tools** panel. Configure a maximum image size and any larger images will be reduced to this size. The default value is 600 x 800, which is our recommendation. The Groups and People types fields allow you to check and fix images for in these categories. Select **Run**. When complete, GMS displays a report of the names of people whose images were updated.