Datalink Systems Inc
Wireless Data Solutions

DataGate Manual (6.9)

(Last updated: Thursday, 4 March 2021)

DataGate application window showing asset list and log output:

Asset ID	Description	Hardware Type	Last Report	Last Network	Group	Users
0.0.1	Florida Demo	MDT	Unknown	None	John's Towing	2
0.0.2	Test	Kenwood Radio	Unknown	Kenwood (search)	(Unassigned)	2
0.0.7	Mobius Test	iSeries/RMI	Unknown	Cellular [unknown]	(Unassigned)	2
1.0.0	Truck 100	PDT-100 (standalone)	Unknown	MSAT (123)	Tracking Com	2
255.255.200	Prototype	iSeries/RMI	2015/05/21 18:16:16	Radio (Local)	(Shared)	2

```
2016/02/16 16:10:11 <INFO> Cellular UDP B Port=9000
2016/02/16 16:10:11 <INFO> Cellular UDP C Port=1720
2016/02/16 16:10:11 <INFO> Cellular TCP A Port=3333
2016/02/16 16:10:11 <INFO> Cellular TCP B Port=3334
2016/02/16 16:10:11 <INFO> Ports opened. Waiting for data...
2016/02/16 16:10:12 <SMTP> Connecting to email server (secure.emailsrvr.com)
2016/02/16 16:10:15 <SMTP> Email sent OK to <tim@datalinksystemsinc.com>
```

Using data folder d:\datagate\data\

Contents

1.0 DataGate Overview

DataGate is the server application for the DataNet network. It acts as a gateway between mobile assets operating on various data networks and end-user clients, allowing these clients to access the assets through a central interface.

End-users can access the server directly through a web interface (WebGate), or via XML and web connections.

NOTE: DataGate requires a license key for activation. Please contact Datalink Systems for pricing and demonstration keys.

1.1 Versions

DataGate is provided as a single downloadable package, but the licensing process enables various features depending on the version purchased. Several license versions are currently available:

Standard: Entry-level DataGate with standard features.

DataGate-256: Adds AES encryption support. This allows certain devices to send data securely with up to 256-bit keys.

Enterprise: The Enterprise version adds asset email and SMS support. DataGate uses a built-in email server to act as a gateway between email clients and remote assets. It also includes an SMPP gateway interface, allowing SMS messages to be exchanged directly with phones and modems (requires an external SMPP server).

Plus: Advanced version includes Enterprise features, and adds enhanced radio network support (DMR, Hytera, P25, etc), power utility XML interface, Google reverse geocoding, and more.

Transit: Adds a public bus-tracking interface to provide live route information for transit operators.

1.2 Supported Devices

DataGate supports a wide range of asset tracking hardware, and is committed to adding new devices as required. The following list shows all devices currently supported:

- Airlink
- Antares Plus
- Arknav
- AXTracker
- Blackberry/Android (using Datalink apps)
- BlueTree
- Caitland PLD and RFU
- CalAmp
- Cerberus
- Ctek SkyRouter
- Cursor-on-Target
- Cypress Chameleon
- DataKnight D100

- Datalink MDT-214
- Datalink Mobius (Windows app)
- Datalink iSeries/RMI
- Datong
- DMR-200/SureLinx
- Enfora
- FT-2000
- Genx
- Globalsat
- Globalstar Smartone
- Globalstar SPOT and SPOTX
- GoTEK7
- GSatMicro
- Hytera Radios
- Icom Radios
- Iridium Extreme
- IsatData Pro
- IsatPhone Pro
- JRC with ITA
- Kenwood Radios (Fleetsync, NXDN, DMR, dPMR, Type-2 Trunking, P25)
- Lars Thrane
- LeoTrak
- Meitrack
- Mini-C
- Motorola Astro 25
- MSAT-G2
- MTData
- NAL Black Box
- NAL Shout
- Naviset
- NMEA (via UDP)
- PDT-100
- Piccolo (Wireless Links)
- Portman
- PotsDOCK
- PT2000
- Quake iQ
- Queclink GL200, GL300, GL500, GL520, GL530, GMT200, GT301, GV55, GV300, GV500, Prime
- Raveon Radios
- Relm Radios
- RIC-M
- SatMate i60
- SatMate i10
- Seagull
- Sectrack D+
- Sendum
- Sierra Wireless
- Sinocastel
- Skyhawk

- Skyhelp
- TAIP Generic Devices
- Tallysman Sprite
- Thrane Fleet Broadband
- Thuraya XT/SS
- TK-STAR
- Trax MT
- Trident Sensor
- Trident Tiger
- TT3000
- Ulbotech
- Veracity
- Vocalis GPS API
- GPS Watch
- Xact

2.0 Installation

2.1 System Requirements

- Microsoft Windows XP (SP3), Server 2003 (SP2) or later operating system
- Supports Windows 10 (32 and 64 bit) and Windows Server
- 1.4 GHz CPU or higher with 1 GB RAM or more
- 30 MB storage space for installation
- .NET Framework 4 Client Profile (web installer included in setup file, requires additional 600 MB storage space if the framework is not already installed)
- Additional storage space required for mapping programs and historical data
- Microsoft SQL Server 2008 or later. Express editions are supported, but these generally have a 10 GB database size limit, and can only use up to 1 GB of memory

2.2 Performance Notes

DataGate makes many small writes to the local file system. Performance may therefore be restricted if anti-virus software is monitoring these writes. It is recommended to exclude the datagate.exe process from such monitoring. If using a database server, similar exclusions may need to be made for database files.

2.3 Software Installation

DataGate is available as a setup executable from the Datalink website:

http://www.datalinksystemsinc.com/downloads.html

This installation must run under an Administrator account. Download and run the executable file to start the setup process. A User Account Control window may prompt you to allow the setup program to make changes to your computer. Select "Yes" to continue with the setup.

The DataGate installation wizard will then appear (see Figure 1) to guide you through the process.

Figure 1 – Installation program

During the installation, a search is made for any existing DataGate configuration file (datagate.ini). If a file is found, its location will be selected as the default storage location. You may modify this location, in which case you will be prompted to copy the existing configuration file to the new location. If not copied, the new installation of DataGate will use default settings.

If no existing installation is found, the default storage location is set to \DataGate on the system drive.

In a fresh installation, DataGate will create "data", "log", and "backup" folders inside the main storage folder. The location of these folders can be changed under DataGate options. See section 19.0 for details on the folders and files that are used by DataGate.

The final step of the wizard provides the following options:

- Run DataGate GUI – Start DataGate as a Windows application
- Start DataGate Service – Run DataGate as a Windows service
- Open DCOM Settings – Modify security permissions on the DataGate object
- Open Service Settings – Edit Windows service settings

You will need to run the DataGate GUI (graphical user interface) to set up licensing and initial settings.

See the following sections for more information on DCOM and service settings.

When the set-up program completes, there will be a shortcut to DataGate in the Windows Start menu under "Start/All Programs/DataNet" (assuming the default program group was selected during the set-up process), and also on the Desktop if selected. Select one of these shortcuts to start DataGate.

It is recommended that DataGate operators periodically check the Datalink downloads website for updated versions. Updates can be installed by installing the new version over the top of the current program. No data or history files will be overwritten when updating.

DataGate may be uninstalled using the Add/Remove Programs feature on the Windows Control Panel. Note that data and history files will not be erased during this process.

2.4 DataGate Windows User Account

It is recommended to run DataGate using an Administrator account. This reduces any issues with file access and/or database configuration. However, running under non-admin accounts is supported, as long as the user has the necessary access to DataGate data folders and the SQL database.

If using Windows authentication to log in to a database, ensure the user account has the necessary permissions to access the database.
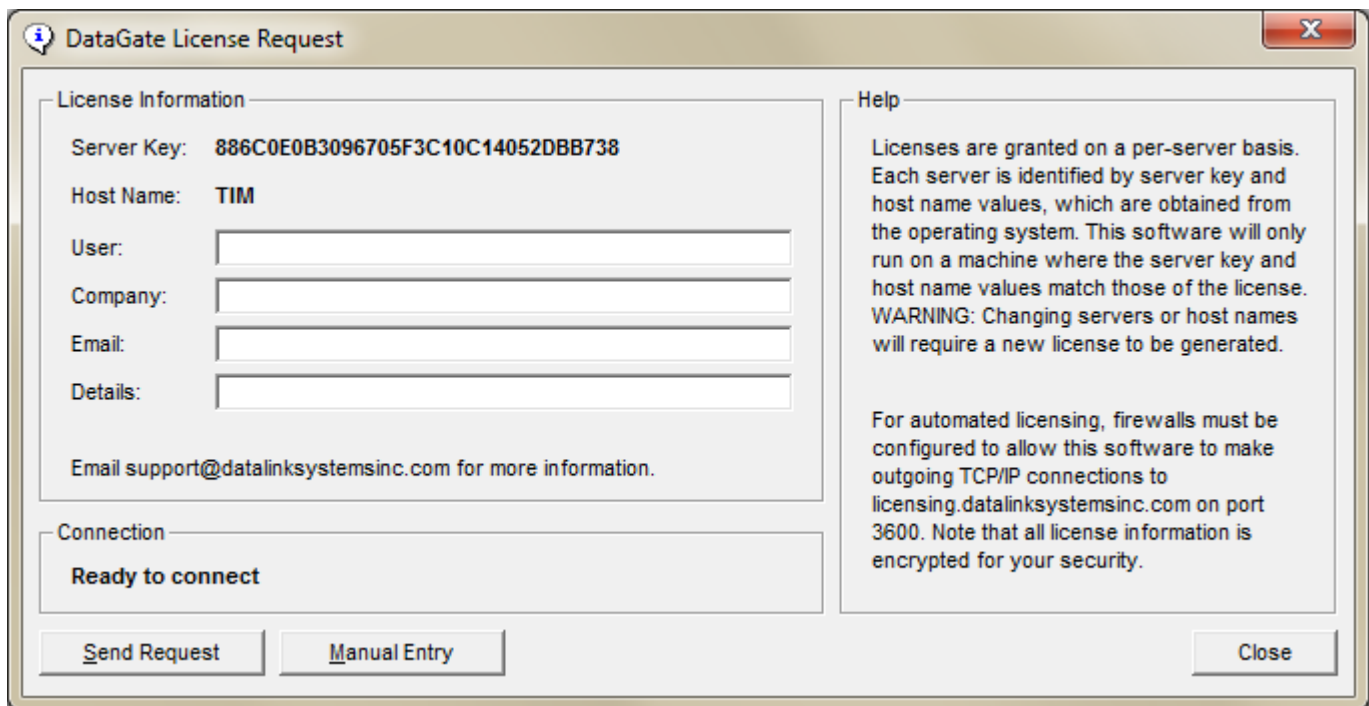
2.5 Loading DataGate GUI

The DataGate GUI can be opened through the Windows start menu shortcut under "DataNet". The GUI provides full access to all DataGate settings.

2.6 License Settings

When DataGate loads, it searches for a valid license key in the datagate.ini configuration file. If an invalid license is found, it will query the Datalink licensing server (licensing.datalinksystemsinc.com) to check for updates. If none is found, DataGate will either close (if running as a service), or prompt the user for information (see Figure 2).

When prompted, enter your user and company names, and include an email address where we can send you messages relating to the licensing process. The optional "Details" field can be used to indicate the reason for the license request. Note that licenses get assigned to a specific server, based on server information including the PC's host name. For this reason, it is important to perform the request from the machine where DataGate will be run.

Figure 2 – Initial settings

This information will be sent to the licensing server in order to obtain a license key. Press the "Send Request" button to transmit an encrypted copy of the license data to our server. The connection response is shown at the bottom of the window, including what steps to take to complete the process.

A validation email will be sent to the email address entered, requesting the user to follow an HTTP link to verify their email address. Once the address is validated, Datalink Systems will be in contact to discuss your requirements. Demonstration licenses are available for a full trial of the system.

Once a license has been created, use the "Send Request" button to pick it up from the server.

For systems that do not have access to the Internet, use the "Manual Entry" button to manually generate license requests and enter license keys.

See section 6.0 for more information about licensing.

2.7 Database Installation

DataGate requires a SQL database for storing information and historical data. We recommend using SQL Server or SQL Server Express (free).

The database can be installed on the same PC as DataGate, or on another server accessible via a network connection. The following section describes a typical SQL Server Express installation process.

2.7.1 SQL Server Installation

Use an existing SQL Server installation, or download the free SQL Server Express edition from Microsoft's website (version 2008 or later). Figure 3 shows the SQL Server 2017 installer.
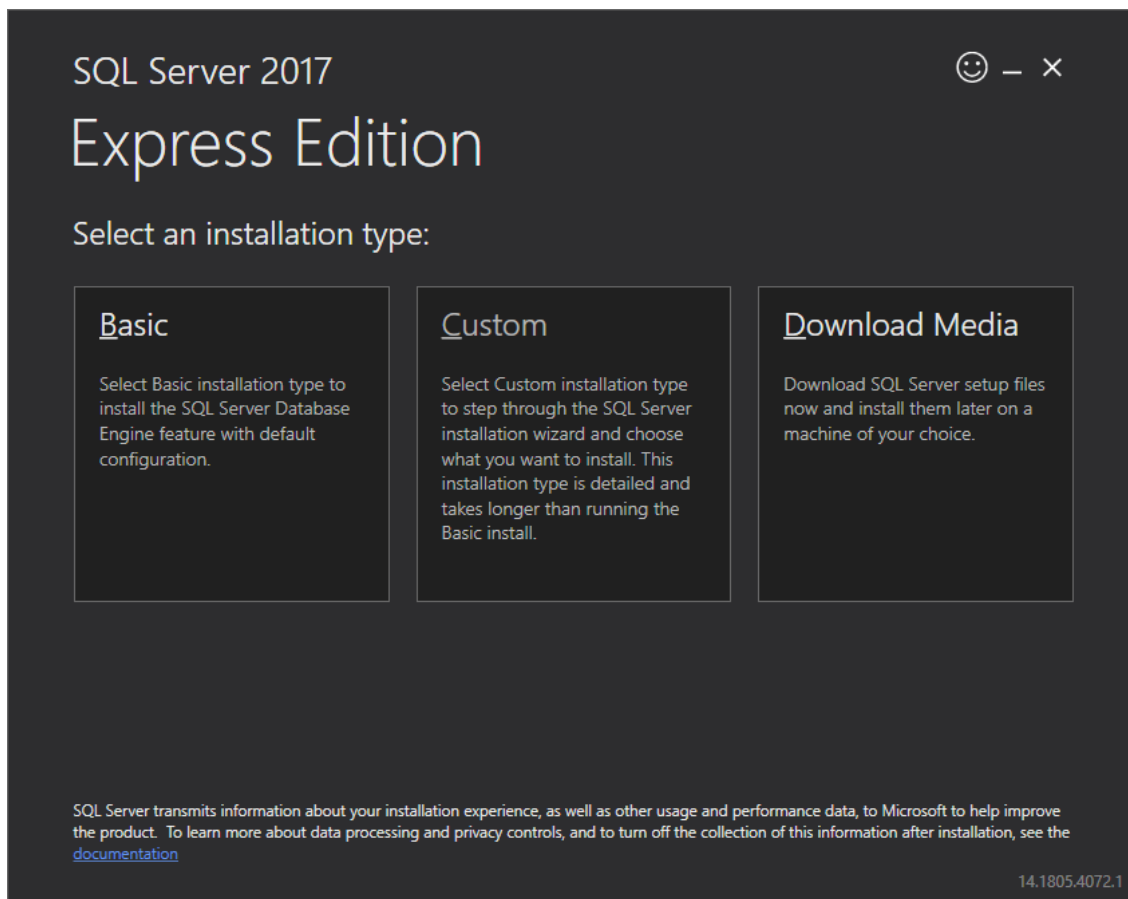
Figure 3 – SQL Server Download

Select "Custom", and enter a download location to download and extract the required setup files. The SQL Server Installation Center should then step you through the setup process (Figure 4).
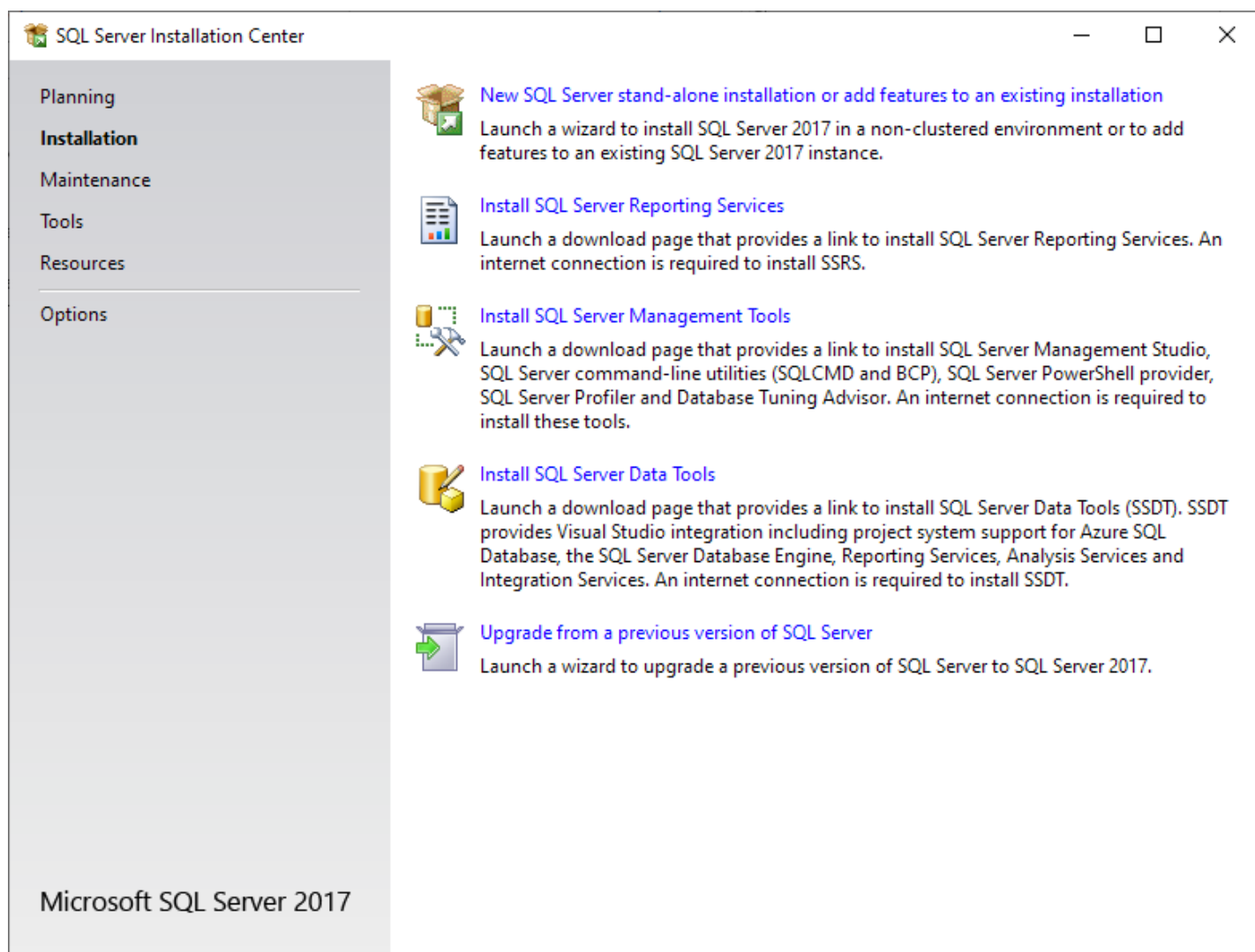
Figure 4 – SQL Server Installation Center

Select the "New SQL Server…" option to begin installation. The installer will begin by checking for required updates and potential problems. Update/fix as required, and agree to the license to continue.

At the Feature Selection step (Figure 5), ensure the "Database Engine Services" and "Client Tools Connectivity" features are selected. Other options may be added, but are not required by DatdGate.
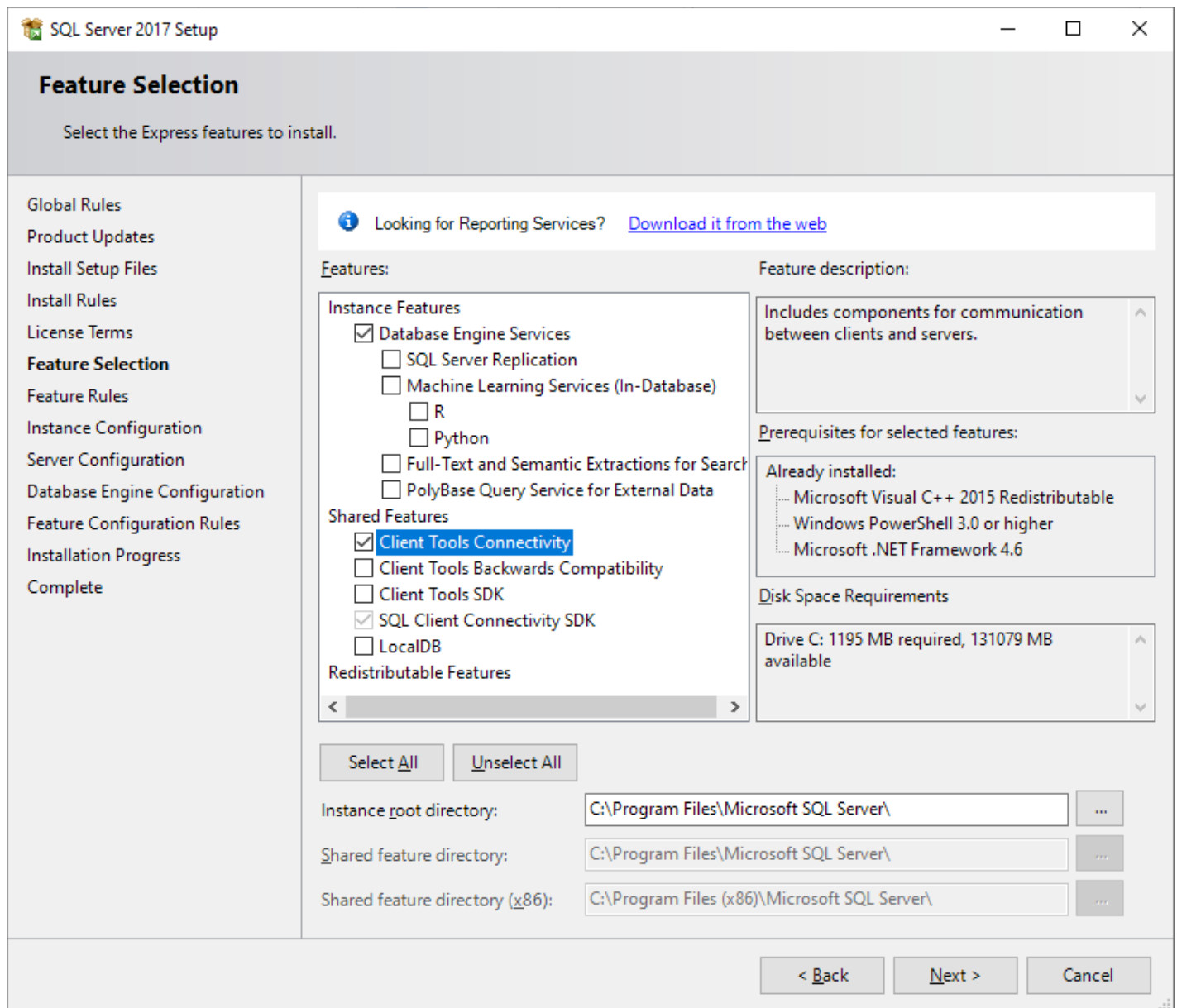
Figure 5 – SQL Server feature selection

The Instance Configuration step (Figure 6) allows you to assign a name to this installation. This is useful if you will be running more than one instance of SQL Server on the same machine. Selecting the Default Instance option means that this SQL Server can be accessed without a name.

This page also lists any existing SQL Server instances present on the server.

Figure 6 – SQL Server instance configuration

At the Server Configuration step (Figure 7), you will be prompted to enter account names and startup types for the SQL Server services. The default accounts provide full access to all local resources, so it may be desired to use a standard user account to reduce security risks. More information on these choices is available on the Microsoft website.

Figure 7 – SQL Server service accounts

Make sure the SQL Server Database Engine service is set to start automatically.

The SQL Server Browser service is not required, but it will make it easier to find this installation if browsing for the database from other machines.

Next is the Database Engine Configuration step (Figure 8). It is recommended to use Windows authentication mode, where a user is automatically authenticated using the currently logged on Windows user account.

However, mixed mode is required if you wish to run DataGate under a non-admin Windows user account. In this case, enter a password for the special system administrator (sa) account. DataGate can connect using the "sa" account, or a new user account can be added after installation.
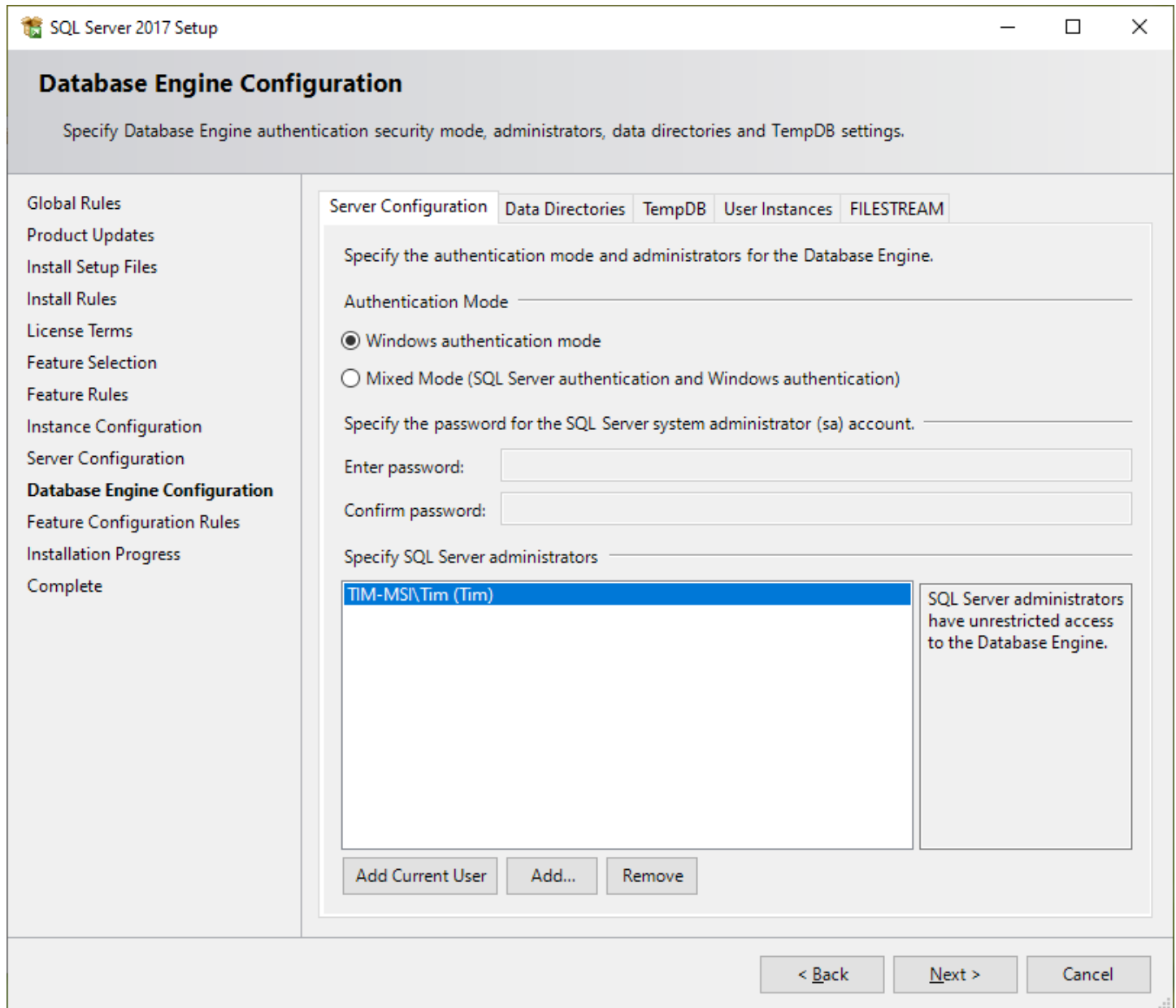
Figure 8 – SQL Server accounts

Specify one or more administrator accounts to allow these users to configure the database. It is recommended to use the current user.

This page also allows the selection of data directories if desired.

The next few steps will install the server software. After completion, it is highly recommended to install the SQL Server Management Studio (SSMS) to aid database configuration and maintenance. To do this, select "Install SQL Server Management Tools" from the SQL Server Installation Center. This should open a web page where SSMS can be downloaded. Figure 9 shows the install wizard.

RELEASE 18.2
Microsoft SQL Server Management Studio

Welcome. Click "Install" to begin.

Location:

C:\Program Files (x86)\Microsoft SQL Server Management Studio 18   Change

By clicking the "Install" button, I acknowledge that I accept the License Terms and Privacy Statement.

SQL Server Management Studio transmits information about your installation experience, as well as other usage and performance data, to Microsoft to help improve the product. To learn more about data processing and privacy controls, and to turn off the collection of this information after installation, see the documentation.

Install   Close

Figure 9 – SQL Server Management Studio installation

2.8 Database Creation

In the DataGate GUI, open the View/Options menu, and select the Storage tab.
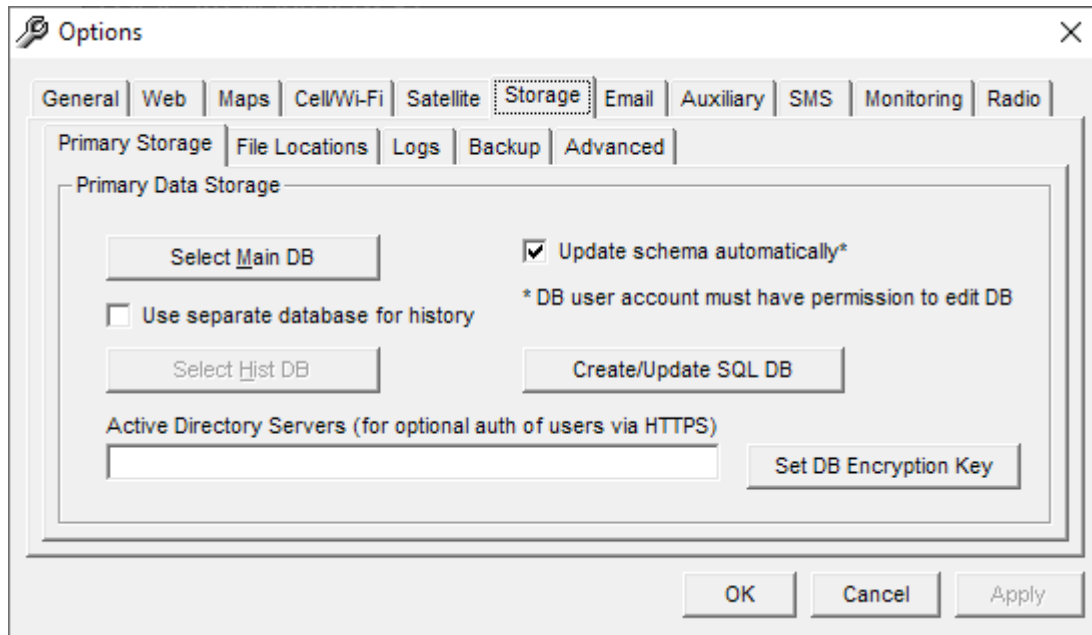
Figure 10 – Storage options

To create a new SQL database, click on "Create/Update SQL DB".
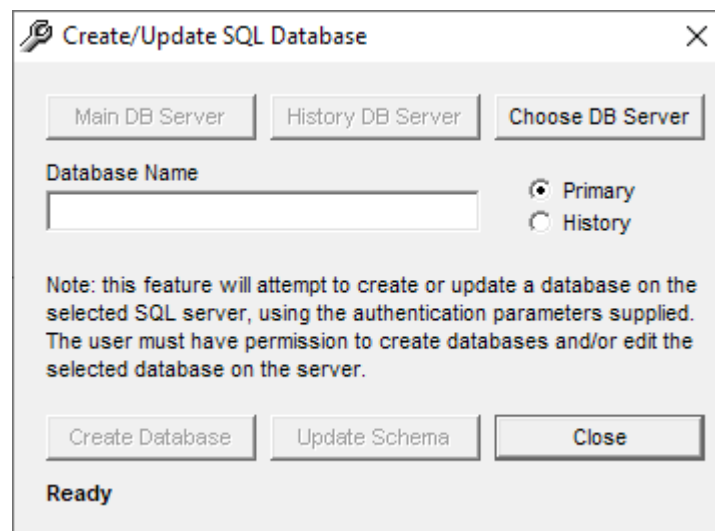
Figure 11 – Choose DB server

Click on "Choose DB Server" to open the Windows Data Link Properties window.
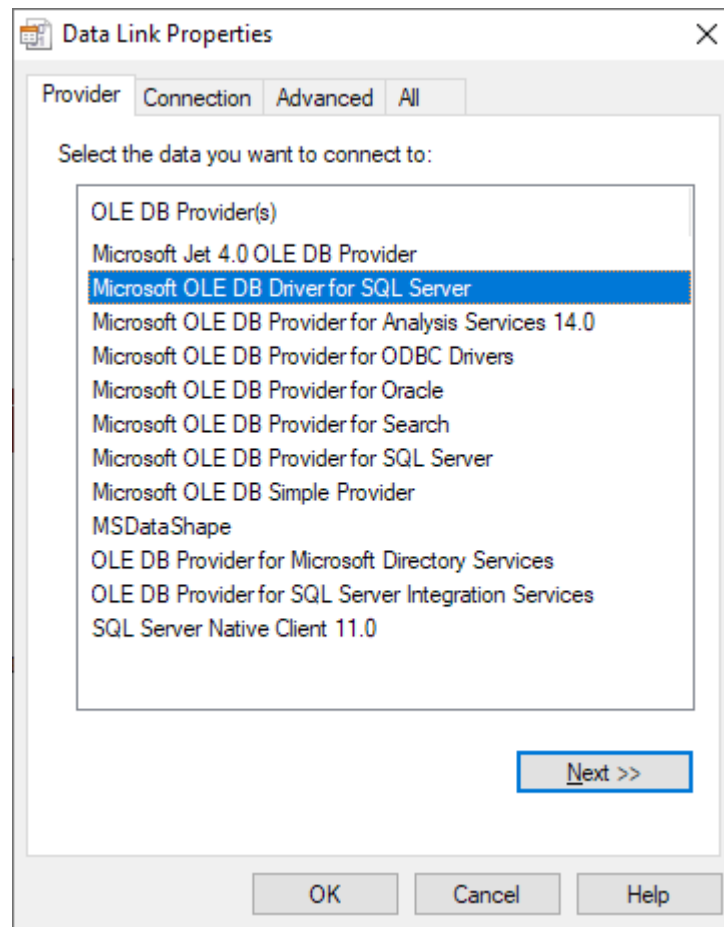
Figure 12 – Data Link Properties

On the Provider tab, select the Microsoft OLE DB Driver for SQL Server. Depending on your database version, you may need to use the SQL Server Native Client or Microsoft OLE DB Provider for SQL Server instead.
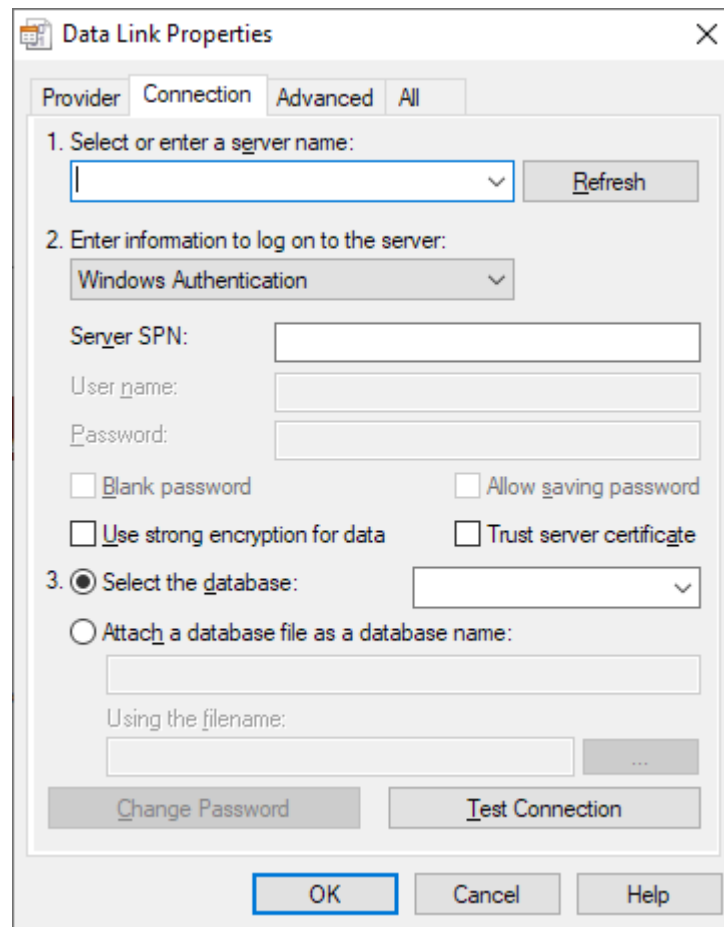
Figure 13 – Database connection

On the Connection tab, enter the database server name. Start with a single period to access the local machine, or enter a server name to access another machine. If SQL Server was installed as a named instance, follow the server name with a slash (\) and the instance name. For example, if an instance is named "DATAGATE" on the local machine, then the server name will be ".\DATAGATE".

Select Windows Authentication to use the currently logged in Windows user account to log on to the server. When using this option, DataGate must always be run under a user account that has access to the database.

If you enabled mixed mode authentication when installing SQL Server, you can also select the SQL Server Authentication option. In this case, enter the desired SQL username and password.

Leave the database name blank, and click on "Test Connection" to check that the link is OK. Click on OK to continue.
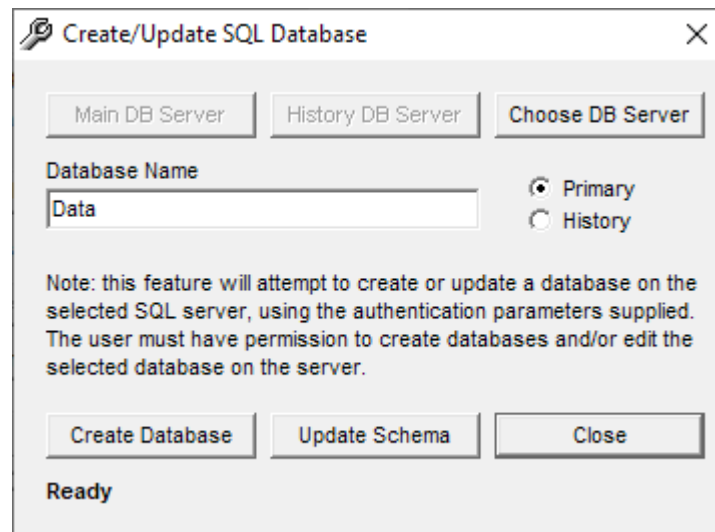
Figure 14 – Create SQL database

Enter the desired database name, and select Primary to set up the main DataGate database. Click "Create Database" to begin the creation process.
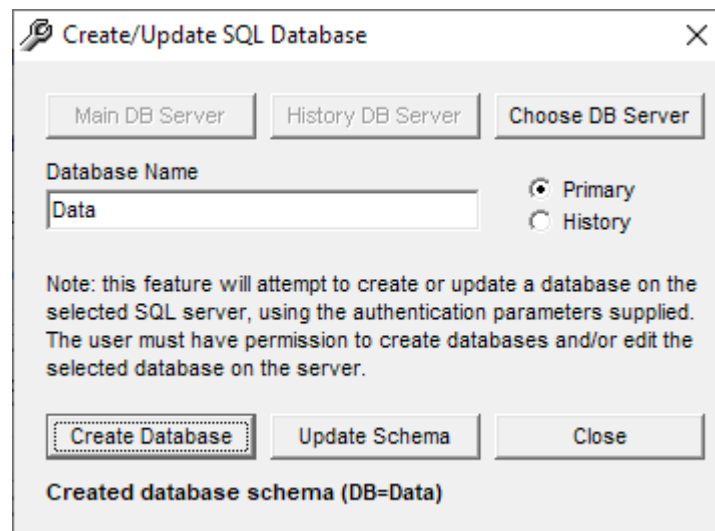
Figure 15 – Created SQL database

The status will be shown at the bottom of the window. Once the database has been created, click on Close to return to the DataGate settings screen.

When prompted, select Yes to update the DataGate database server and name to match the database just created.
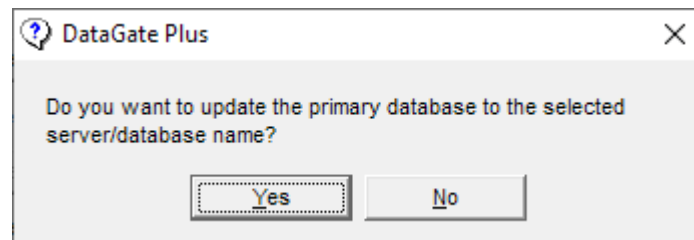
Figure 16 – Update database server settings

DataGate supports using a separate database for storing historical data. The main reason for using a separate database is to reduce backup times, as DataGate does not back up the history database when running its automatic backups. If you want to keep history backup up, then it is not advised to use a separate database.

If you do wish to use a separate database, then repeat the above process, but change the database name and select the History button.
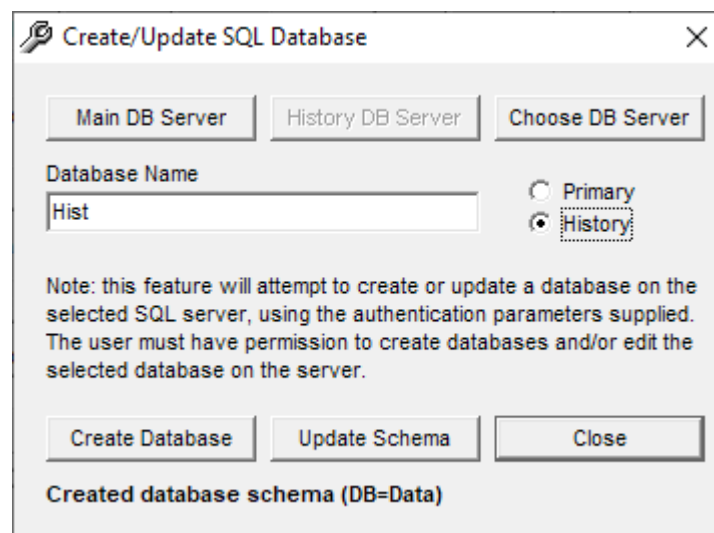
Figure 17 – Create History database

When prompted, select Yes to update the DataGate history database server and name to match the database just created.
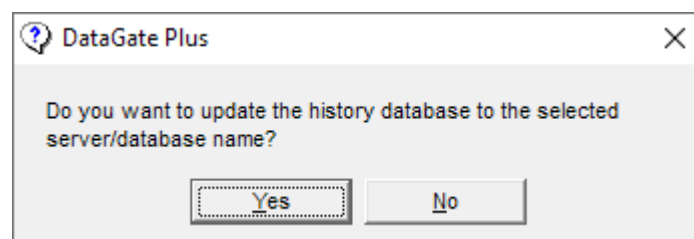
Figure 18 – Update history database server settings

Finally, click OK on the settings screen to save the settings and connect to the database(s).

2.9 Service Settings

During the set-up process, a Windows service named "DataGate Service" is installed. This service is used to start DataGate as a background process, allowing it to run before a user logs in.

By default, the DataGate service will run under the local system account, and start automatically when Windows loads. These properties can be edited through the Services console (shown in Figure 19) available under Administrative Tools in Windows.
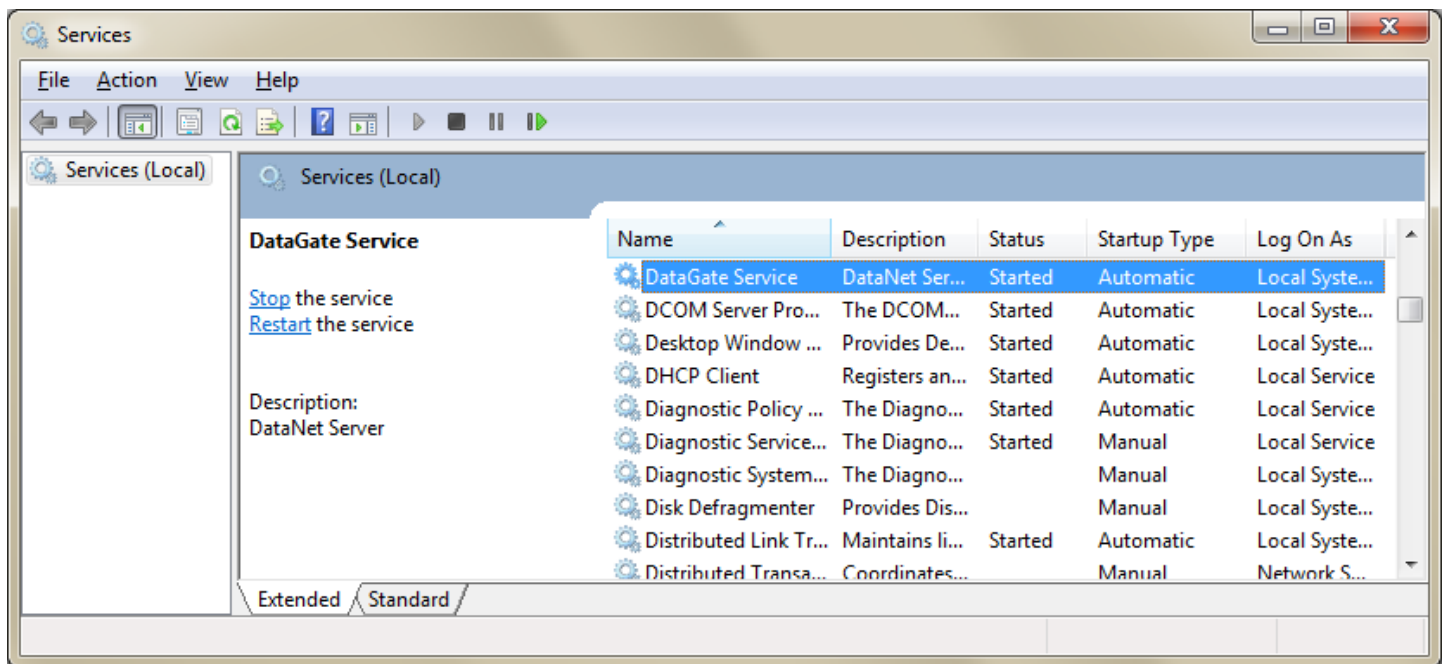
Figure 19 – Windows services

Double-click on the DataGate Service entry to access its properties. The properties page provides settings to control startup type (automatic or manual), manual controls for starting and stopping the service, and log on settings.

Each service is assigned a user account to run under. By default, DataGate uses the local system account, which provides full access to the server. It may be desirable to change this account to a local administrator account. Ensure this user has the necessary permissions to access DataGate data folders. To change the account, simply enter the username and password under the Log On tab on the service properties screen (see Figure 20).
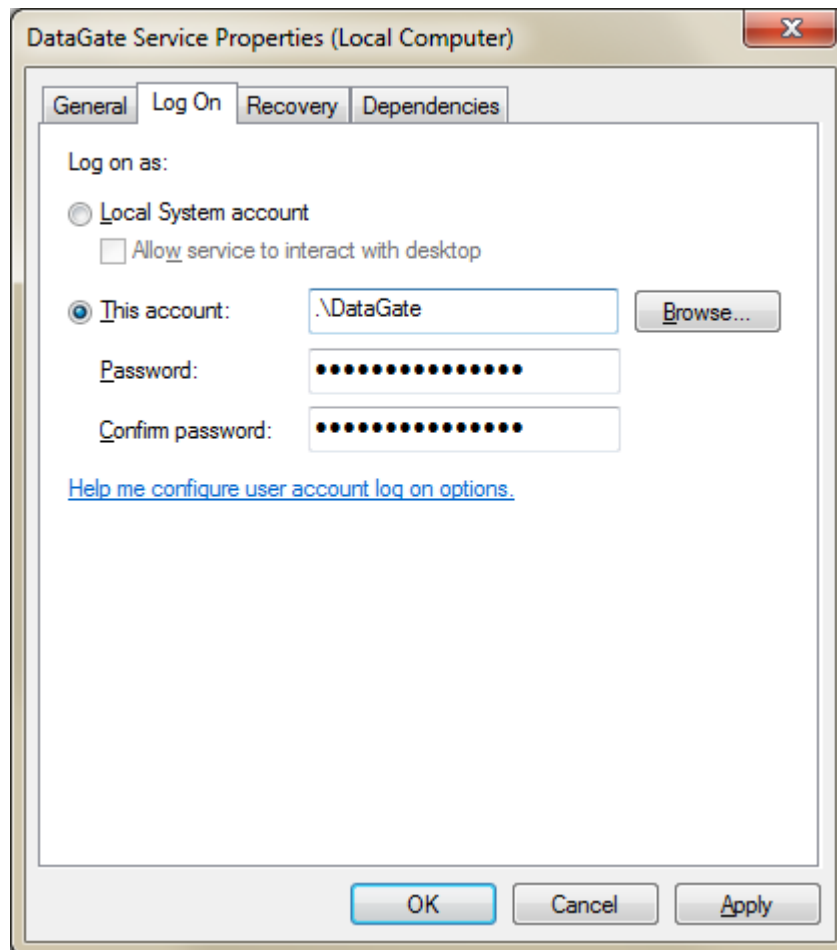
Figure 20 – Service Log On settings

2.9.1 Running under a non-admin account

The DataGate service can be set to run under a standard (non-administrator) user account, but it will not be allowed access to the DataGate COM component by default. To enable access, you will need to edit the server permissions using the Windows Component Services utility. Run "MMC COMEXP.MSC /32" to open the utility, select Component Services/Computers/My Computer/DCOM Config, then right-click on DataGate.Server and select properties. Under Security, select "Customize" for the Launch and Activation Permissions, then "Edit" to open the permissions window. Add the user account you wish to give access to DataGate, and then make sure it has Local Launch and Local Activation permissions.

This account will also need the necessary file and network permissions required by DataGate.

If using Windows authentication to log in to a database, ensure the service's user account has the necessary access to the database.

2.10 Wireless Networks

Most wireless data networks can be accessed over the Internet. DataGate will normally require a public static IP address to allow mobile assets to access it. A dynamic DNS record can be used, but is not recommended for production systems due to switching delays.

Certain networks may require an intermediate utility (called Source Program) to allow DataGate to connect. Currently the following networks are supported (with the required source programs shown):

Cellular:	Internet.
Globalstar:	Internet.
ICOM:	ICOM IDAS base radios can connect via IP using a serial to Ethernet converter, or directly to a local COM port.
IsatM2M:	Internet.
IsatData Pro:	Internet.
Inmarsat (other):	Uses Simplex email address.
Iridium:	Uses either an external email address, or a direct IP connection (Internet).
Kenwood:	Fleetsync/NXDN base radios can connect via a remote PC running the Kenwood Source program, via IP using a serial to Ethernet converter, or directly to a local COM port. Direct IP console connections (from DataGate to radio repeaters/gateways) are also supported.
Local Radio:	Base radios connect via a remote PC running the Radio Source program, via IP using a serial to Ethernet converter, or directly to a local COM port.
Motorola MUPS:	Requires IP connection to a MUPS server.
MSAT-1:	MSAT Source connects to ground station over Internet. Optional MET Source connects to a base satellite transceiver to communicate over satellite (allows secure comms without Internet).
MSV-G2:	Internet. DataGate runs a web service to accept connections from the G2 gateway.
Raveon:	Raveon Source connects to Raveon base radio.
Simplex:	Uses either a web service to accept connections from the Globalstar gateway (Internet), or an external email address.
SMS:	SMS messages can be received via an external SMPP gateway (Internet). Messages can be sent through the same SMPP gateway, or via an external email address. DataGate supports SMS messages from Thuraya and Inmarsat handsets, as well as Queclink, GPS Watch, Globalsat, Caitland and Smartphone devices.
Spot:	Internet. DataGate uses a web service to accept connections from the Spot gateway.
Thrane FleetBB:	Internet.
Trax:	Trax Source connects to Trax base radio.

Certain networks will allow VPN connections over the Internet if security is a concern. VPNs are also recommended for cellular networks, where modems can be assigned private addresses, allowing mobile-terminated data (commands can be sent to the modems at any time).

2.11 Initial Configuration

It is recommended to add at least one Sys Admin account (see section 10.0 for user configuration). This user is able to log in through the web interface to add and edit assets, users, and groups. The DataGate can then be run as a service, with infrequent need to access its user interface.

2.12 Firewall Settings

DataGate receives and transmits data on several IP ports. Most of these ports are configurable under the DataGate options, and can be enabled or disabled as required. The following list shows all commonly used ports, and default values:

Description	Direction	Protocol	Port	Notes
License Requests	Outgoing	TCP	3600	To: licensing.datalinksystemsinc.com
Data Sources	Incoming	TCP	3607	Remote data sources
DNS Requests	Outgoing	UDP	53	Looking up email server addresses
Email SMTP	In/Out	TCP	25	Sending and receiving email
User HTTP	Incoming	TCP	80	Web interface
Device HTTP	Outgoing	TCP	80	Outgoing Globalstar SMS data
"	"	"	7777	Outgoing MSV G2 data
User HTTPS	Incoming	TCP	443	Secure web access
Cellular	Incoming	UDP	1720	Enfora, Portman, etc.
"	"	"	4004	iSeries, MDT, etc.
"	"	"	9000	PinPoint, Chameleon, etc.
"	"	TCP	3333	Sendum, Smartphones, etc.
"	"	"	3334	Naviset
"	"	"	3335	Cursor-on-Target
Email POP	Outgoing	TCP	110	Checking satellite email inboxes
Iridium	In/Out	TCP	10800	Direct IP data
IsatM2M	Outgoing	TCP	5102	Connection to Inmarsat gateway
Globalstar	Incoming	UDP	3615	Incoming Globalstar data
MUPS	Outgoing	TCP	5000	Motorola MUPS radio data
Kenwood IP	In/Out	UDP	50600	Kenwood IP console connections

Other ports will be required for some DataGate features, such as auxiliary feeds, SMPP, and terminal clients.

2.13 Updating DataGate

DataGate is updated regularly to correct bugs and add new features. Please visit our downloads page (https://www.datalinksystemsinc.com/resources/) to check for new versions. This page includes a DataGate Change Log file, which lists all the changes made for each new version.

To update DataGate, simply download the latest setup file and execute it on the server. Note that you will have to close any open DataGate GUI applications and stop the DataGate service for the setup to

complete. The setup process will update components as required, while keeping all settings and data intact.

Note: when DataGate is updated, it may add support for new tables or columns in the SQL database. If the "Update schema automatically" setting is enabled (see section 7.7.1), DataGate will attempt to update the schema when it starts up. This process can take several minutes if there have been changes made to large tables. It is therefore recommended to schedule updates for periods of low activity.

2.14 Migrating to a New Server

This applies if you are currently running a DataGate and wish to move it to a new server while retaining existing settings and/or historical records.

1) On the new server, download and install the latest DataGate package from our downloads page (https://www.datalinksystemsinc.com/resources/).
2) Copy DataGate settings from the old server to the new one by moving the "datagate.ini" file. You may want to edit the ini file to set data folder locations if they will be different on the new server. See section 19.0 for ini and data file locations.
3) Ensure the new server has the same host name as the old one. If the server name is changing, a new license will have to be granted. Contact support@datalinksystemsinc.com for assistance.
4) Make a note of the data and log folders used by the old DataGate. These are listed on the View/Options/Data Storage menu (or in the ini file).
5) The following steps are time-critical if you want to minimize down time.
6) If you want to ensure all data is transferred to the new server, you must stop the old DataGate at this point. This prevents the old data files and/or logs being updated after copying.
7) Copy all files from the data folder on the old server to the data folder on the new server. Optionally, copy the files from the log and backup folders, although these are not required for ongoing operation. See section 19.0 for details on DataGate data and log files. The file locations on the new server should match the settings in the new ini file.
8) If you are using an external database server you may choose to keep using this from the new machine, or move it to a new one. If you need to move it, or the database is running on the old machine, make a backup of the old database (using the database management program, such as SQL Server Management Studio), and then import this backup into the new machine. If using an external server, ensure the new server has access to this machine.
9) The old server can now be closed. If you are replacing it with another machine on the same network, you might want to change its IP address, and then assign the old IP address to the new server. This will ensure data is routed to the new machine.
10) Run the new DataGate. Check that it loads files and database OK. You may want to go through the View/Options menu and confirm all settings are correct. In particular, you may need to edit the database location if it is different from that used on the old server.
11) If the new server has been configured with a different IP address, redirect incoming asset data to the new machine. If you are keeping the same public IP address, then this should only involve making changes at your local router. If the public IP address has changed, this will require changes to be made at all assets to point to the new address.
12) Remember to move any required VPN connections too. Disconnect the VPN connections on the old server, and then set them up and connect them on the new server.

2.15 Automatic VPN Connections

It may be necessary for DataGate to connect to private networks to access device information. This is commonly required when connecting to a private radio network, where the radio repeaters or gateways are on a private network separate from DataGate. A VPN is also popular with some cellular providers, where the cell modems are only accessible via a VPN connection.

Once a VPN connection has been configured in Windows, it is recommended to add a scheduled task to ensure this connection stays open.

1) Open the Windows Task Scheduler (Control Panel -> System and Security -> Administrative Tools -> Schedule Tasks).
2) Add a new task (Action -> Create Task).
3) Assign an appropriate name.
4) Under "When running the task, use the following user account", make sure the selected account has access to the VPN.
5) Select "Run whether user is logged in or not".
6) Under triggers, add a new trigger with "Begin the task" set to "At startup". Set the task to repeat every 5 minutes for an indefinite duration.
7) Under actions, select "Start a program". Enter "c:\windows\system32\rasdial.exe" under the program/script setting. Under arguments, enter the VPN name in quotes, followed by the user name and password. For example: "Radio VPN" johnsmith pa$$word.
8) Under conditions, uncheck any limitations.
9) Under settings, check "Allow task to be run on demand", "Run task as soon as possible...", and "If the task is already running" set to "Stop the existing instance".
10) When saving the task, you may need to enter the password for the user account you have selected to run the task.
11) The VPN will automatically start the next time Windows is restarted, and will automatically reconnect in less than 5 minutes if the link drops.

To monitor the VPN connection, you can enter the address of a machine on the VPN network under the DataGate monitoring tab (see section 7.11). DataGate will then warn you if the VPN connection goes down for more than a defined period.

3.0 Starting and Stopping DataGate

3.1 Starting DataGate

The DataGate server is a Windows COM object, which can be run as a standard Windows application with a graphical user interface (GUI) or as a hidden process controlled by the DataGate Windows service.

Note that only one instance of DataGate can be run on a particular machine. If DataGate has been started by the service, the service will need to be stopped before running the GUI application.

When run as a Windows application, DataGate provides a GUI to access all configuration settings as shown in section 3.3.

If DataGate is already running (either as a service, or GUI), then a simpler screen will appear, as shown in Figure 21.
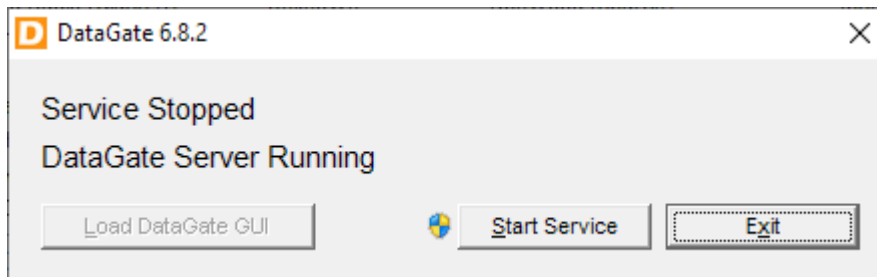
Figure 21 – DataGate already running

This screen indicates whether the DataGate service is started or stopped, and whether the DataGate COM server is running. A button is provided to start or stop the service. This button may raise a User Account Control window to confirm that the user has permission to control the service state.

If the existing instance of DataGate is shut down, the "Load DataGate Server" button will become enabled. This is a shortcut to start the DataGate GUI.

3.2 Service Operation

When the DataGate service starts, it attempts to load a DataGate COM server. If this request fails (due to permission or installation problems, or because DataGate has not been licensed) the service will immediately stop. If DataGate is already running, the service will periodically attempt to start a new instance. In this way, DataGate will automatically be started by the service when any existing instance is closed.

Likewise, if the DataGate COM server process is closed by a user (through Task Manager or the command line), the service will automatically restart it to ensure DataGate remains enabled.

3.3 Closing DataGate

When running as a service, DataGate can be closed by stopping the service.

When running as a Windows application, DataGate can be closed using the File/Exit menu. A warning screen is shown, prompting the user to confirm the closure, as follows.
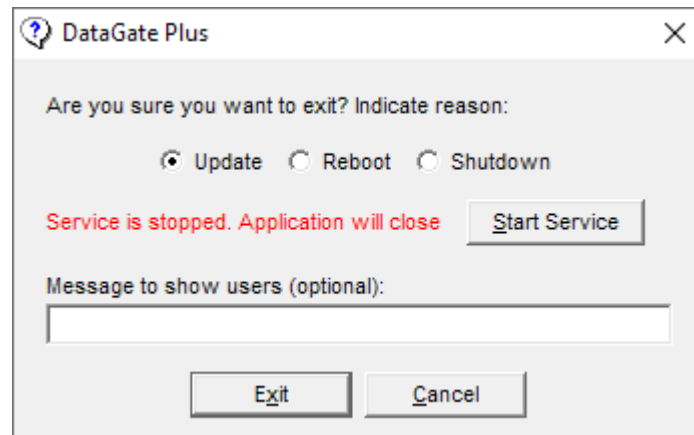
Figure 22 – Closing DataGate

A reason for the closure can be selected, which will be shown to any logged in Web Clients before the application closes. An optional message can also be used to add detail if desired.

A red warning is shown if DataGate detects that the DataGate service is currently stopped. In this case, DataGate will close and not get restarted by the service. If the service is running, a message is shown to indicate that DataGate will get restarted in the background once the GUI closes. A button is provided to quickly start or stop the service, if required.

DataGate will also close when instructed to by the operating system (such as when the system is being shut down).

When closing down, DataGate waits for database records and open files to be written, and for web connections to be gracefully closed. If all database records cannot be written before closure, DataGate keeps a record in a temporary file. These records will get loaded and written to the database when DataGate next starts.

4.0 Screen Layout

Figure 23 shows the main DataGate window. At the top is a toolbar, providing quick access to asset functions. Under this is an asset list, showing a complete list of configured assets. At the bottom of the window is a log list box showing recent data communications and information. Along the bottom edge of the window is a status bar, showing the data storage location and current connection states.
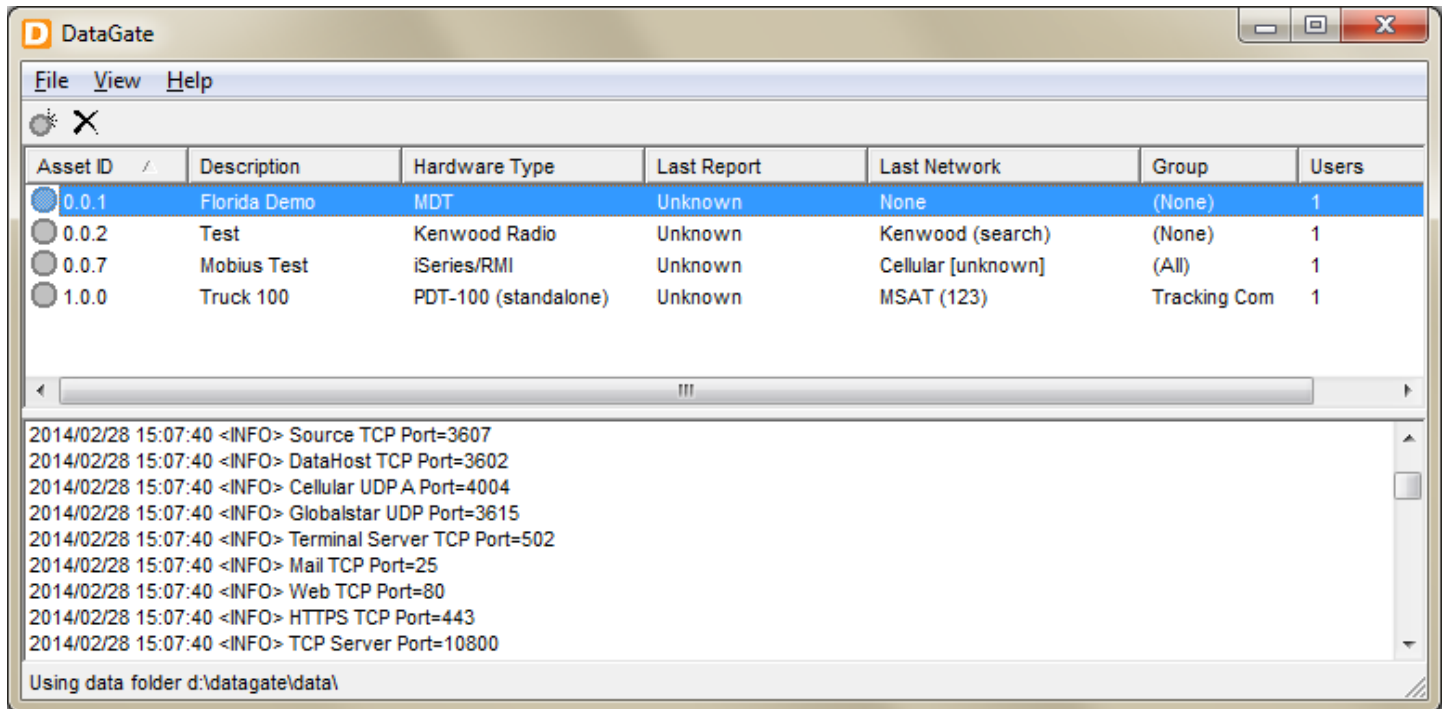
Figure 23 – Main DataGate GUI window

4.1 Toolbar

The toolbar provides quick access to add and delete assets. These functions are also accessible using the Insert and Delete keys on the keyboard, or by right-clicking on the asset list. The following functions are available:

Add Asset   Add a new asset.
Delete Asset   Delete currently selected asset.

4.2 Asset List

This list shows all assets configured on the server. See section 9.1 for more information. Unlicensed assets will be shown in red text.

4.3 Log List

The data communications log shows all data transmitted to and received from assets, as well as other information such as connection messages. When the program is started, it will load data files, connect to databases (if enabled), and attempt to open all configured IP sockets.

5.0 Main Menu

5.1 File Menu

Export Settings   Export settings for use with DataGate .NET.
Exit: Exit program.

5.2 View Menu

Partners: Configure data sharing partners (optional feature may not be available).
Groups: Shows a list of groups that users and assets can be assigned to (see section 7.0).
Users: Show the list of users allowed to connect to this DataGate. Users may connect using a web browser (see section 10.0), or via third-party interfaces.
Terminal Clients: Show the connections available for third-party applications needing to send/receive raw data to/from mobile assets (see section 11.0).
Data Sources: Open the list of Data Sources (see section 12.0).
Pager/Driver Details: Shows a list of pager/driver IDs and assigned names (see section 12.2).
Open Today's Log: Opens the DataGate log file created today.
Open HTTP Log: Opens the HTTP log created today (if enabled).
Open Email Log: Opens the email log created today (if enabled).
Options: Access DataGate options (see section 7.0).

5.3 Help Menu

The Help menu provides a link to the DataGate About screen, which shows the software version number and user information (see Figure 24).
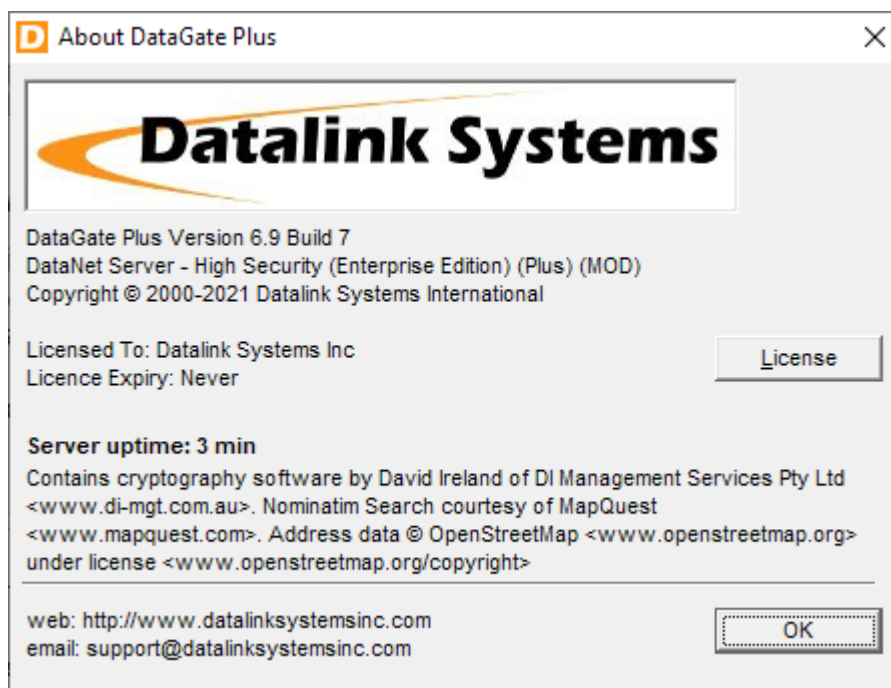
Figure 24 – DataGate About screen

Clicking on the "License" button opens the license window. See section 6.0 for more information on licensing.

This screen includes a server uptime counter, showing how long the DataGate application has been running. The exact start time can be revealed by hovering the mouse over the counter value.

6.0 Licensing

DataGate is licensed on a per-server basis. The license defines which DataGate features are enabled (see section 1.1 for information on DataGate versions), and the maximum number of users and assets allowed to be configured.

Each user can log in from a single browser at a time.

Assets are split into three classes: Class A (MDT, iSeries, Smartphone, SatMate, PotsDock, Caitland, Iridium Extreme, and Airlink devices), Class C (Mobius), and Class B (all other devices).

Note: Spare Class A licenses will automatically be assigned to Class B devices if all Class B licenses are in use. For example, a server with 10 Class A and 10 Class B licenses can support up to 10 Class A devices, or up to 20 Class B devices (depending on how many Class A licenses are in use).

If the number of assets or users configured in the DataGate exceeds the licensed maximum, these will be shown in red text, and will be non-functional until the license limits are increased, or some assets or users are deleted.

6.1 License Details

Figure 25 shows the DataGate License window, accessed through the Help/About menu.
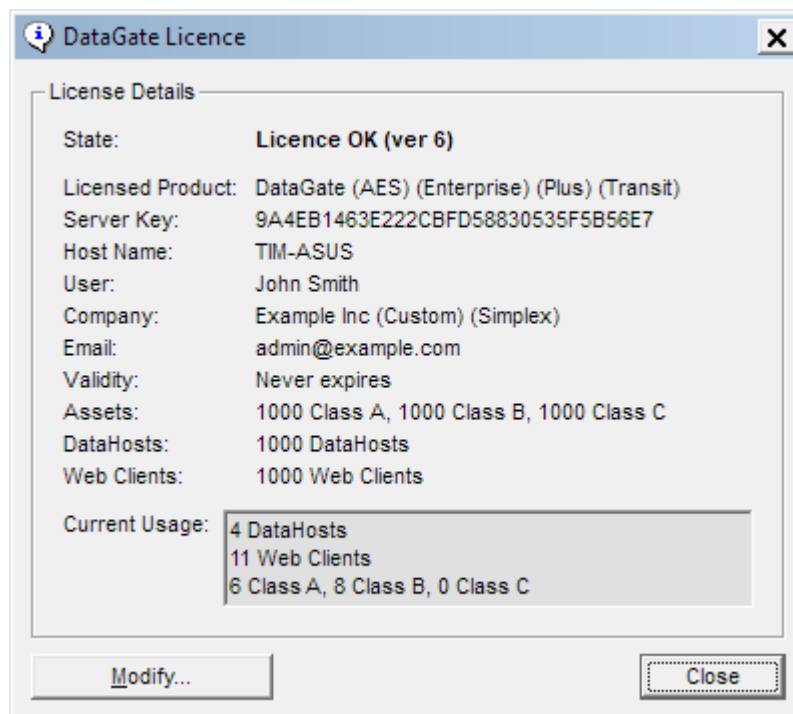
Figure 25 – DataGate License screen

The following details are shown:

State:	Indicates whether license is valid or not.
Licensed Product:	Describes product this license applies to.
Server Key:	Server identifier. Used to match the license to a specific machine.
Host Name:	Windows host name. This is also used to match the license.
User:	Contact name.
Company:	Company name. If the license allows a custom web interface, this entry will show "(Custom)" after the name. See section 18.3 for details on modifying the web page.
Email:	Email address of user. The licensing server may send messages to this address when a license is modified. This address will also receive messages when major server updates are available (unless opted out).
Validity:	Expiry date of license. Some licenses are time limited. DataGate will generate alerts when the license is due to expire.
Assets:	Shows how many assets the DataGate can support. Assets are divided into three classes (each class has a different license cost).
Web Clients:	Maximum number of Web Client users allowed.
Current Usage:	Lists the number of users and assets currently in use by the server.

6.2 Updating the License

Contact Datalink to modify the number of licensed assets or users, or to extend the validity period. When the license server has been updated, a notification email will be sent to the address listed in the license. License requests may take up to 24 hours to be processed.

Once this message has been received, click on the "Modify..." button in the License window to open the License Request form (see Figure 2). For systems that are connected to the Internet, use the "Send Request" button to update the license automatically.

Otherwise, select "Manual Entry" to open the screen shown in Figure 26.

Figure 26 – Manual License Entry

Copy the license request link to a computer with Internet access, and navigate to the address to send the request. If the license is enabled, a license key will be returned. Copy and paste this key into the key section, then click "Update" to confirm.

6.3 License Validity Period

Licenses may be defined with an expiry date, with automatic extension when the software checks in. In this case, DataGate will automatically attempt renewal prior to expiry. It is therefore recommended to allow DataGate to contact the Datalink licensing server as required.

6.4 Moving DataGate to a new PC

If DataGate is moved to a new PC, you will be prompted to request a new license key. New licenses will be granted subject to a review.

7.0 Options

The View/Options menu brings up the main options screen for the DataGate software. Many options are available, separated into several tabs.

Note: Clicking the Default button (where available) will load the default options for the currently selected tab.

7.1 Unicode Settings

The DataGate graphical user interface does not currently support Unicode data entry. If you need to include any Unicode characters in the settings, this can be done by directly editing the datagate.ini file in a Unicode-aware text editor (such as Windows Notepad). When saving the file, make sure you select Unicode character encoding.

　　　　　　　　　　　　　www.datalinksystemsinc.com

7.2 General

7.2.1 Configuration
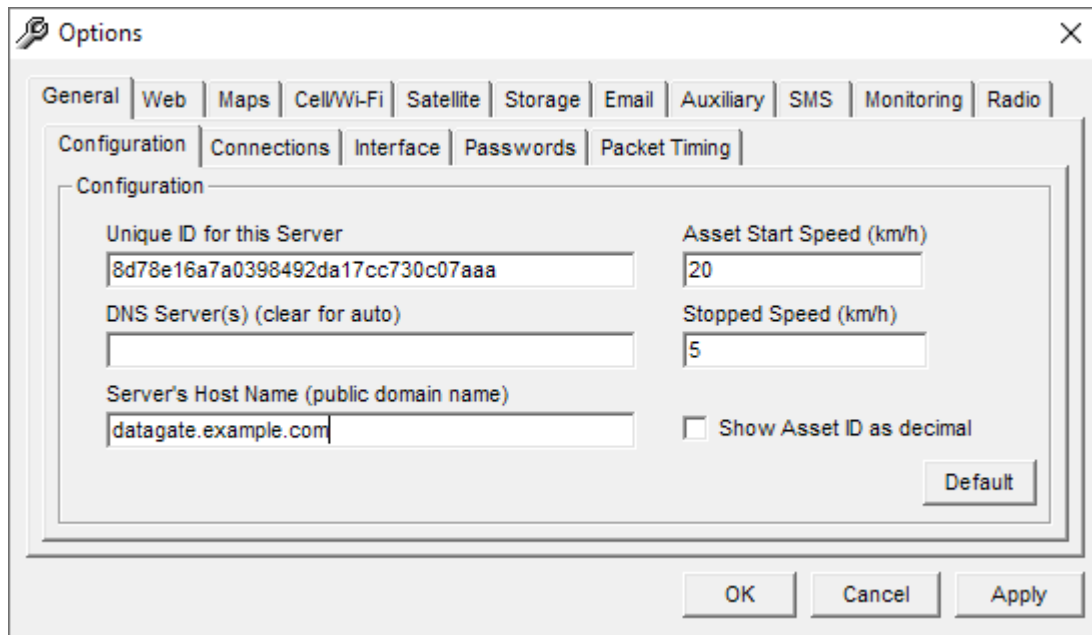
Figure 27 – Connection Options

Unique ID:	Each DataGate can be assigned a unique identifier.
Asset Start Speed:	Speed at which assets are assumed to be in motion. This setting is used to detect vehicle use outside of work hours.
DNS Server(s):	DataGate uses DNS when sending emails. Enter DNS addresses here, or leave blank (recommended) to use the DNS servers configured in Windows.
Stopped Speed:	Speed at which assets are assumed to be stopped. Used to trigger address lookups if Nominatim search enabled and asset speed is equal to or less than this limit. Also used to change WebGate icons.
Server's Host Name:	Enter the host name assigned to this server. This name will be used by the web and email servers. If using TLS for secure web or email communications, you should update DataGate's TLS certificate when changing this host name. Create a new TLS certificate (see section 7.3.2) if using a self-signed certificate, or obtain a new certificate if using a trusted provider.
Show Decimal ID:	By default, DataGate displays asset IDs using a dotted triplet notation, with three values ranging from 0 to 255 separated by a period. For example, (0.0.1) or (50.1.255). Selecting this option will cause DataGate to display IDs as a single number, ranging from 1 to 16777215. DataGate will recognise both forms of ID when entered by a user.

7.2.2 Connections
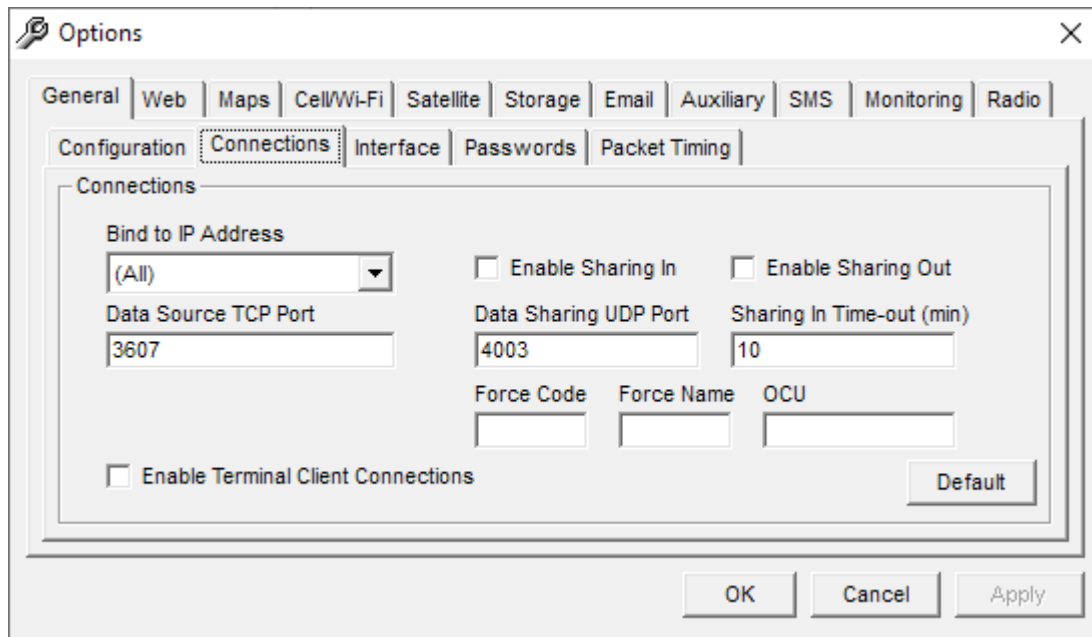
Figure 28 – Connection Options

Bind to IP Address: If a PC has more than one network connection, DataGate can bind to a specific IP address, allowing the other address(es) to be used by other programs. By default, DataGate binds to all available adapters.

Data Source TCP Port: Port for Source connections.

Enable Terminal Clients: This option must be enabled in order for Terminal Clients to connect to the DataGate.

Sharing In/Out: Optional settings for configuring sharing with external partners.

7.2.3 Interface
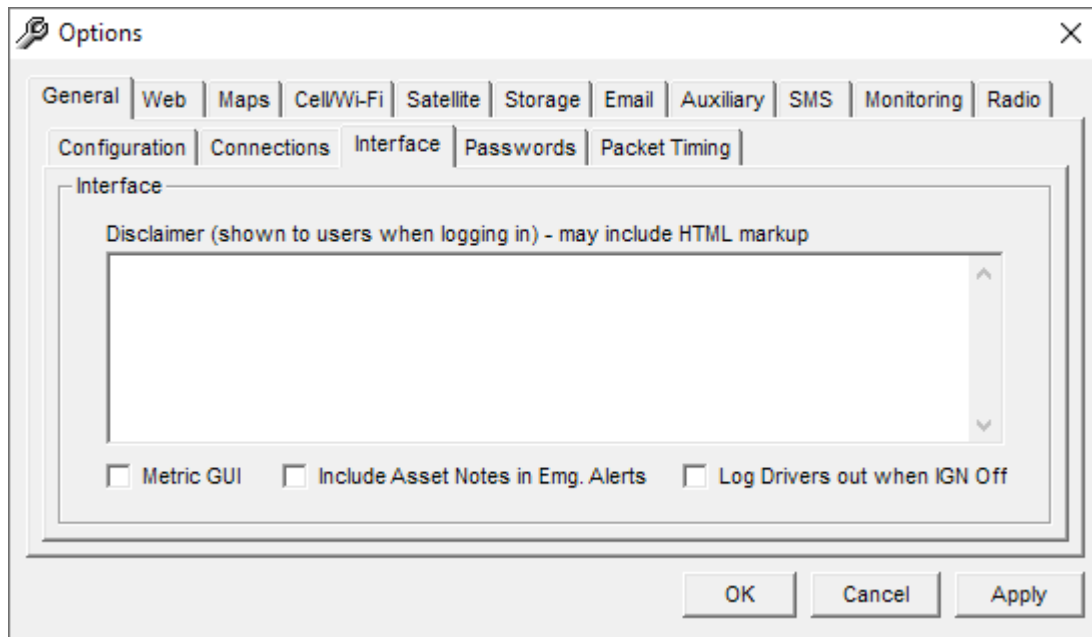
Figure 29 – Interface Options

Disclaimer:	Message to show to users before logging in. Users must agree to this disclaimer before proceeding. This field can contain HTML formatting, such as Bold.
Metric GUI:	GUI will use metric units.
Include Asset Notes:	When enabled, this option includes data from an asset's notes field in emergency alerts generated by that asset.
Log Out Drivers:	Automatically log an asset's driver out when the asset sends an IGN off event.

7.2.4 Passwords
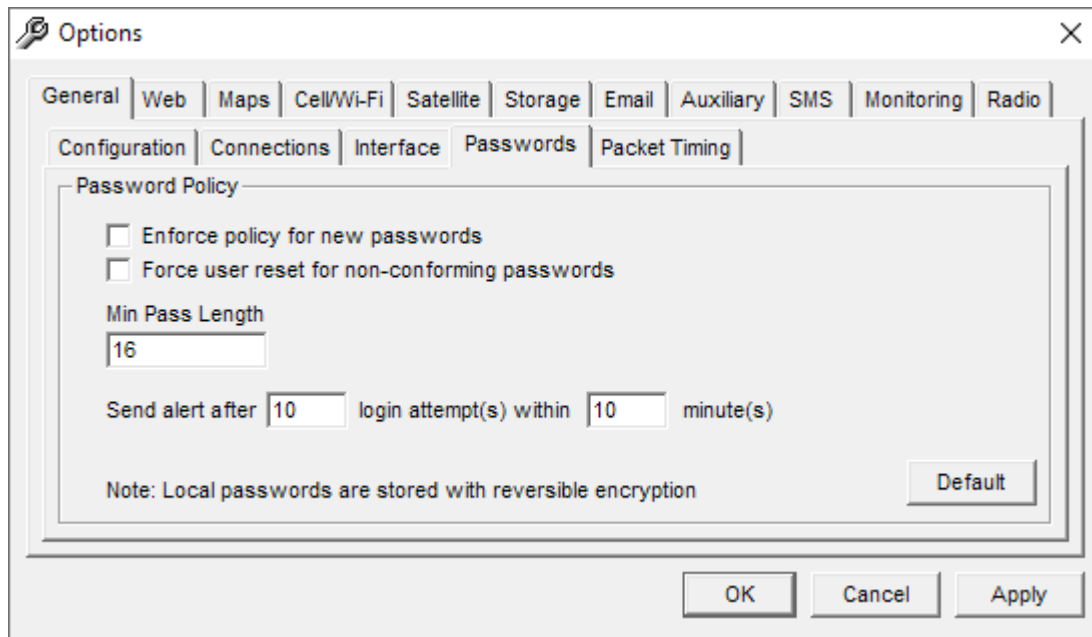
Figure 30 – Password Options

Enforce policy:	If enabled, user passwords must be at least as long as the minimum password length. This only applies when setting a new password.
Force reset:	This option forces users to change their passwords when logging in, if they are shorter than the minimum length. This applies to WebGate users only.
Min Pass Length:	The minimum allowed password length. It is highly recommended to use at least 8 characters, and preferably 14 or more to increase security. Research shows that increasing a password length adds more security than adding complexity requirements (where passwords must use mixed case, numbers, and special characters). Complex passwords are also hard to remember, compared with a password made up of multiple dictionary words.
Send Alert:	Generate alerts if multiple failed login attempts are detected within a certain time.

7.2.5 Packet Timing
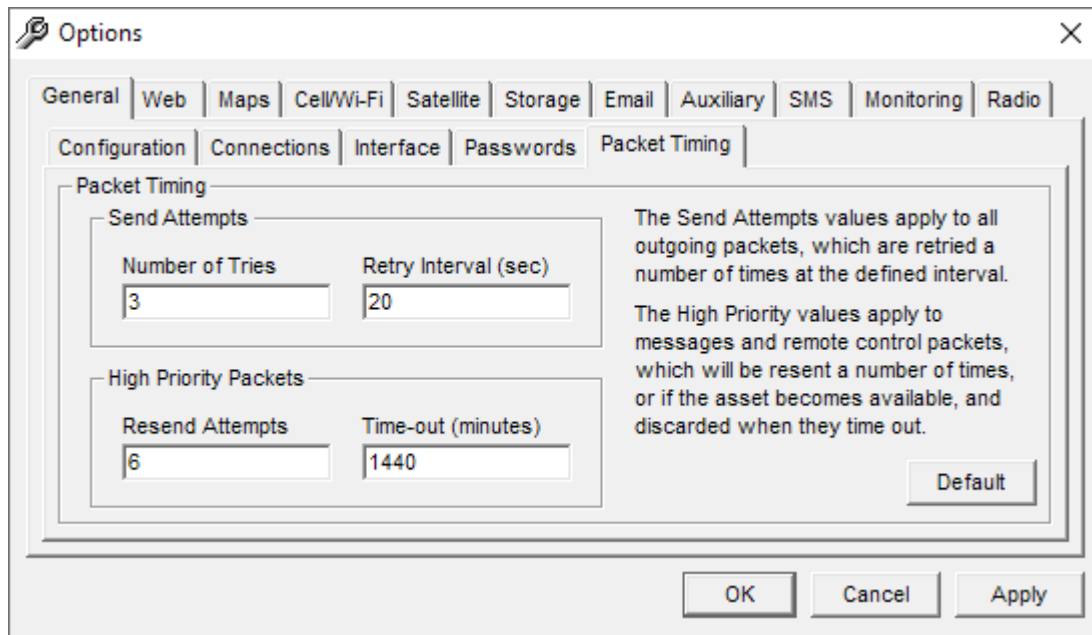
Figure 31 – Packet Timing Options

Number of Tries:	The maximum number of transmissions during send attempts. Low priority packets will give up if there is no response from the asset after this many tries.
Retry Interval:	The time between transmissions when sending over most networks. Some networks have their own timing that is controlled internally.
Resend Attempts:	High priority packets are kept in the buffer if the initial send attempt fails. This value sets the number of resends made. Each resend will use the number of tries and retry interval from above. Resends use an exponential timer with an increasing gap between resends. The exact timing will depend on both the number of attempts and time-out values.
Time-out:	High priority packets time out after this period. Note that packets will also time out immediately if a resend attempt fails after the asset reports in to the server.

The above timing is used for packets generated through the web page and XML interfaces. Packets queued via email use default email retry timing and the time-out value provided in settings (see section 7.8.3). Packets queued via the database use default retry timing and the time-out value provided in the database record.

7.3 Web

7.3.1 Web Features

See section 16.0 for a description of these features.
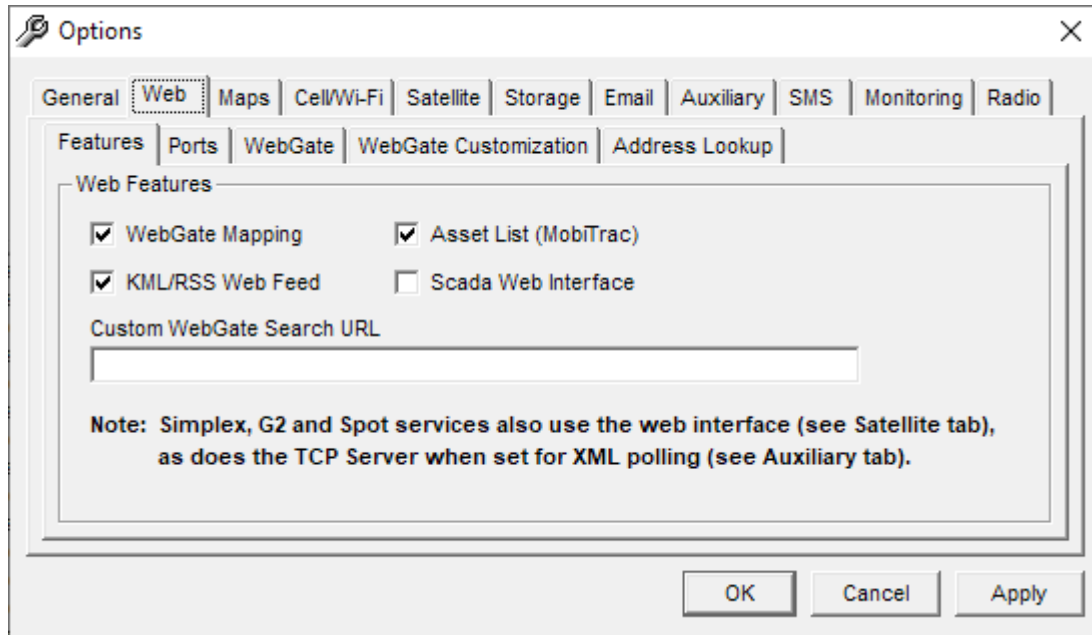
Figure 32 – Web Features

WebGate Mapping:	Enables the DataGate web mapping page (WebGate), accessible by Web Client users.
Asset List:	The asset list provides a comma separated variable (CSV) list of asset locations, and is used primarily by smartphone applications. This is accessible by adding "/list" to the web address.
KML/RSS Web Feed:	Allows Web Clients to log in and download a KML list or GeoRSS feed of asset locations. These lists are accessed by adding "/kml" or "/rss" to the web address.
Scada Web Interface:	Provides a means for terminal clients to log in and set their IP address for secure access to remote devices.
Custom Search URL:	Enter an optional URL if you want to use a custom address lookup service for WebGate. This service must return the search results in a JSON format. Contact Datalink for more information.

7.3.2 Web Ports
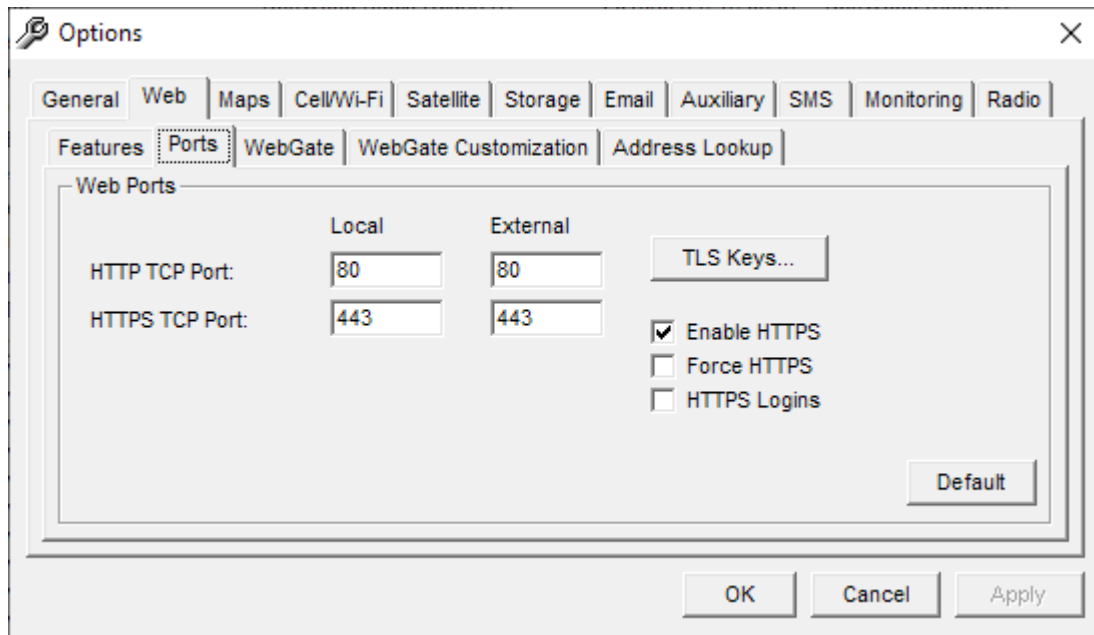
Figure 33 – Web Ports

HTTP TCP Port:	Port assigned to the web server. The local port will be opened by DataGate. The external port is used when DataGate has to redirect users to other pages, and should be set to the port used to access DataGate from an external connection. This will depend on how your external routers and firewalls are configured. Use port 80 if you want users to be able to access the server without adding a port number to the URL.
HTTPS TCP Port:	Port for HTTPS (secure) web communications. See note above about local vs. external ports. Use port 443 if you want users to be able to access the server without adding a port number to the URL.
Bus Ports:	Secondary ports for public bus interface (Transit edition only). These ports will only serve the public bus web page. The primary ports can also serve the bus page if using a separate domain name (see section 7.3.7).
TLS Keys:	Click here to edit the private key and public certificate used for secure web and email connections. See section 15.5.
Enable HTTPS:	Select to enable HTTPS. See section 15.0.
Force HTTPS:	If enabled, web requests will be redirected to the secure port.
HTTPS Logins:	Force users to login via an HTTPS page. After login, they will be redirected to the non-encrypted site.

7.3.3 WebGate Options
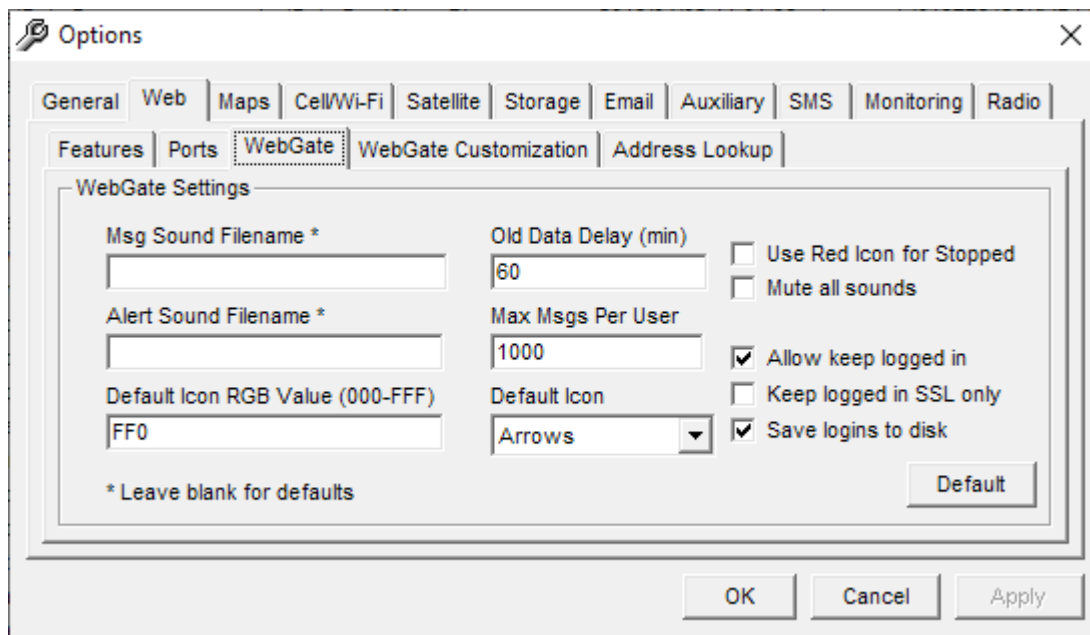
Figure 34 – WebGate Options

Sound Filenames:	Programmable WebGate sound files. Enter the full path to the files, excluding the file extension. DataGate will search for files with the extensions OGG, MP3 and WAV. Ideally, provide all three formats to ensure the sounds play in most browsers. DataGate searches for the files at start up, and also whenever the settings are updated.
Old Data Delay:	Delay period after which asset icons will change color to indicate old data on WebGate.
Max Msgs per User:	This setting limits how many messages will be buffered for each web user. When this limit is exceeded, the oldest messages will be removed from the user's message list. Note that these messages are still available when running a historical report.
Use Red Icon:	Option to change the stopped icons to red. When disabled, stop icons will be dark green.
Mute all sounds:	If enabled, the WebGate page will not play any sound effects.
Allow keep logged in:	When enabled, WebGate users will have the option to keep their sessions logged in, even if their browser is closed.
SSL only:	Allow users to keep logged in only when using SSL (https).
Save logins to disk:	This option causes DataGate to save WebGate sessions (for users who have chosen to keep logged in) to disk when closing. These sessions will be available when the server restarts.
Default Icons:	Select the default icon type and color for assets in WebGate that do not have a custom icon defined. The first character of the color defines the red value, the second is green, and the last is blue. Each character can have a value from 0-9 or A-F. For example, 000=Black, 888=Grey, F00=Bright Red, etc.

7.3.4 WebGate Customization
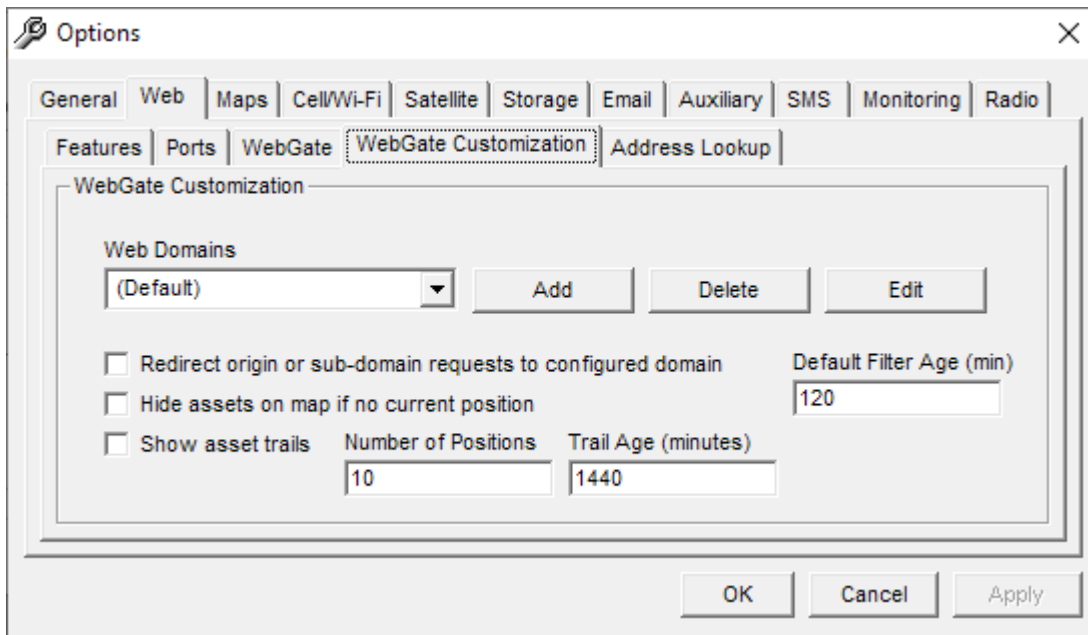
Figure 35 – WebGate Customization Options

Web Domains:	The DataGate web interface can be customized based on the domain name used to access the web page. This is useful if providing services to multiple companies, each wanting their own logos. The (Default) domain settings will be applied when any other domain name is used.
Add:	Add a new domain name. Each domain name should have a DNS A record pointing to the DataGate server IP address.
Delete:	Delete the selected domain.
Edit:	Edit domain specific options. See next section for details.
Redirect:	If enabled, any incoming web requests that do not match one of the configured web domains will be redirected to that domain. This is useful to ensure a user always accesses the same browser cookies (and therefore web settings) when logging in. For example, if a web domain is set to "www.example.com", requests to "example.com" or "xyz.www.example.com" will be redirected to "www.example.com"
Hide assets on map:	This option causes assets to disappear off the WebGate map if they do not have a valid position. Under normal usage this option should be disabled, as the asset's previous location is still of value.
Show asset trails:	When enabled, WebGate will show a line attached to each asset showing previous positions. The number of positions to show and trail age can be set.
Default filter age:	Assets will be hidden automatically when their report age exceeds this threshold. Leave blank to disable. This setting can be overridden using the filter age setting on the WebGate screen.

7.3.5 Configure Domain

Figure 36 – Domain Configuration

Some of these customization options are only available when the DataGate "Custom" licensing option has been purchased.

Domain Host Name: Enter fully qualified domain name, excluding http prefix.

Web Title Style: CSS styling for title bar background image.

Web Page Background: Enter CSS style information that will be applied to the body element of WebGate dialog pages (login, disclaimer, password change, etc). For example, "background:url(http://example.com/back.jpg) #888;background-size:cover;" will set the background image to cover the background, and add a default background color in case the image cannot be shown.

Login Support Info: This message is displayed on the login page. It can also include HTML formatting. It is recommended to add an email link to allow users to contact the DataGate support staff. For example, "Contact Support for assistance". To provide your own formatting, enclose the text in a <div> tag with inline style information. For example, "<div style='...'>Support Message</div>".

Web Page Title: Set a custom title for the web interface.
Page Description: This information is placed inside a <META> tag.
Extra Header Tags: Add any extra tags here, such as Google Analytics scripts.
Custom Link: This link is shown on the WebGate web page under the user menu. It may be used for any purpose, but the intention is to provide a support link for users to find assistance.
Custom Link URL: Enter the fully qualified URL for the support link.
Logo Link: Optional link to follow if a user clicks on the web page logo.
Custom Logo: Select a .png file to display at the top of the web page.
Custom Touch Icon: Icon used by some devices when bookmarking the page.
Custom Favicon: Small .ico file displayed on the browser tab for this page.

See section 18.4 for details on custom icons.

7.3.6 Address Lookup
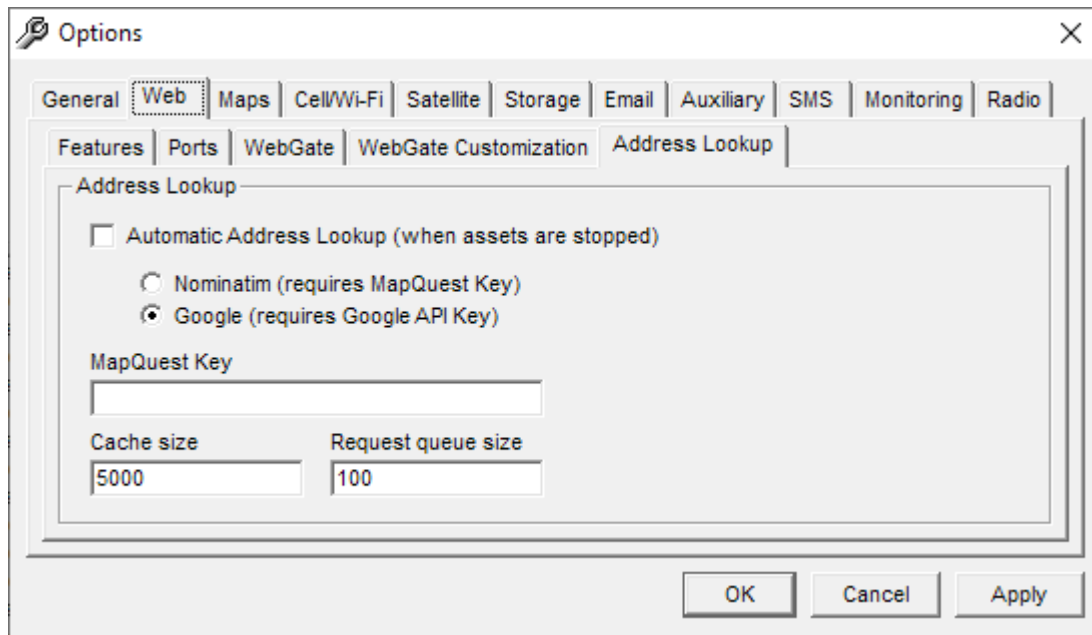
Figure 37 – Address Lookup Options

Automatic Lookup:	When enabled, DataGate will attempt to look up street addresses for any location where an asset's speed is less than or equal to the stopped speed. These queries are sent over the Internet to either the free MapQuest search engine or Google map servers.
MapQuest Key:	Obtain a key from MapQuest to allow MapQuest address lookups.
Cache size:	Number of addresses to keep in memory. DataGate will search this cache before sending a lookup request. The cache is populated at startup by querying the history database.
Request queue:	Limits the number of requests to queue at startup.

* Address lookup vendors may require the purchase of licenses for access to their address data. Please check their license terms of use before enabling lookups in DataGate.

7.3.7 Public Bus Interface (Transit Edition)

Figure 38 – Address Lookup Options

Web Page Title:	Public bus web interface title.
Page Description:	Description placed in web page <META> tag.
Domain Names:	Enter one or more domain names to be used for the public bus interface. DataGate will check the host name inside HTTP requests on the primary web port, and serve the bus page when one of these domain names is detected. Note that the separate bus web port will always serve the bus page.
Links to External Sites:	Enter one or more links that will show on the public bus page under the Information section. Enter the link name, a colon, and the full URL of the link (including http/https protocol). Separate multiple links with a comma.
Min/Max Zoom:	Enter optional minimum and maximum zoom limits for the bus page.
Live Interval:	Enter minimum update interval for the bus page (in seconds).
Extra Header Tags:	Extra header tags for the public page. This is useful for adding Google Analytics links or similar.
Message Box:	Optional message to show every time the page is loaded. This is intended for short-term warnings, such as service disruptions.

7.4 Maps
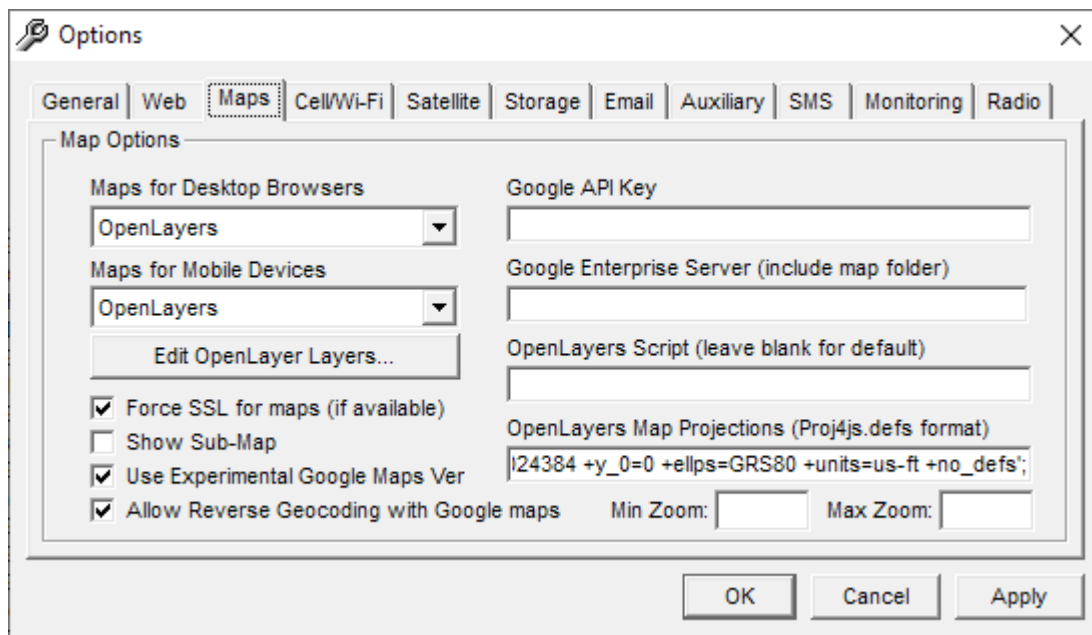
Figure 39 – Map Options

Maps for Desktop:	Selects the type of map to show users on desktop browsers.*
Maps for Mobile Devices:	Selects the type of map to show users on mobile devices. Some maps (such as Bing) do not operate well with touch input.*
Edit OpenLayer Layers:	Control which layers are shown when using OpenLayers. See section 22.0 for details.
Force SSL:	Force browsers to use an SSL connection to map servers. SSL will always be used if a user logs in to WebGate using HTTPS.
Show Sub-Map:	Display a small secondary map on the mapping web interface. This is useful in applications where two zoom levels are required.
Use Experimental Ver:	Enable this option to use the latest Google maps version.
Allow Reverse Geocoding:	When enabled, the WebGate address lookup feature will use the Google API. If disabled, or non-Google maps are being used, DataGate performs address lookups using the free Nominatim web service provided by MapQuest.
Google API Key:	Optional API key for Google maps.
Google Enterprise:	Optional API location if using Google Enterprise maps.
OpenLayers Script:	Optional script location for OpenLayers.
OpenLayers Projections:	Optional projection descriptions. These may be required if using custom OpenLayers layers with non-standard projections. Separate multiple entries with a semicolon. Example: `Proj4js.defs['EPSG:26910']='+proj=utm +zone=10 +ellps=GRS80 +datum=NAD83 +units=m +no_defs';`
Min/Max Zoom:	Limit zoom levels for Google maps.

* Map vendors may require the purchase of licenses for access to their map data. Please check their license terms of use before enabling the maps in DataGate.

7.5 Cell/Wi-Fi

7.5.1 UDP
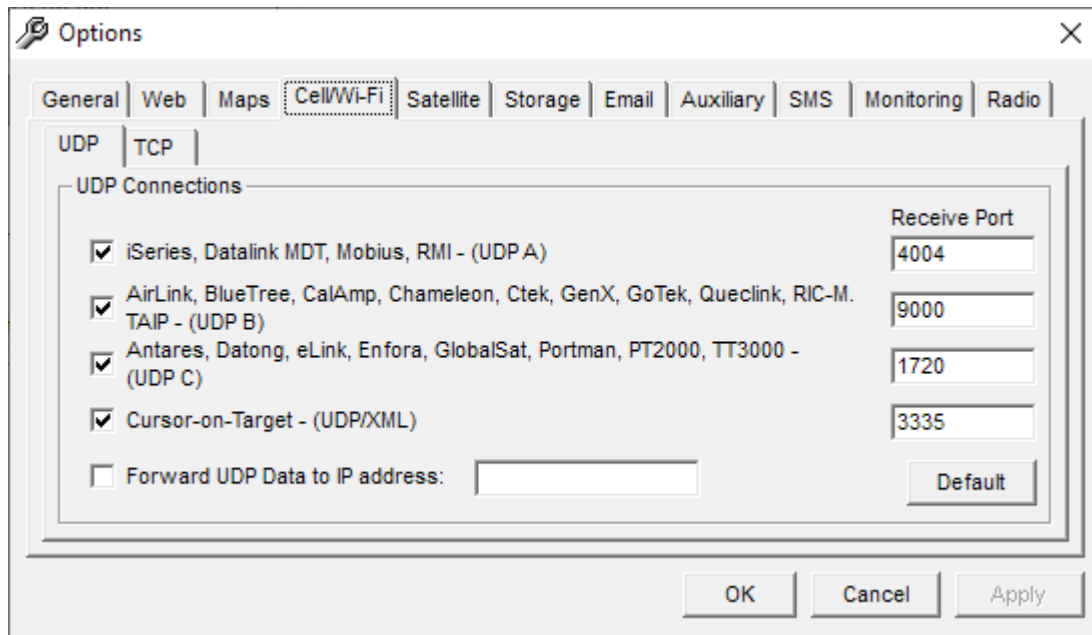
Figure 40 – Cell/Wi-Fi UDP Options

UDP A:	Enables data from Datalink hardware devices (UDP).
UDP B:	Enables data from AirLink, BlueTree, CalAmp, Chameleon, Ctek, GenX, GoTek, Queclink, RIC-M, and TAIP modems (UDP).
UDP C:	Enables data from Antares, Datong, eLink, Enfora, GlobalSat, Portman, PT2000, and TT3000 modems (UDP).
UDP/XML:	Enabled data from Cursor-on-Target modems (UDP).
Receive Ports:	UDP ports used to listen for data. Transmit ports are not defined, as these are set dynamically when data from an asset is received. This allows data to flow through a NAT server.
Forward UDP Data:	If enabled, all incoming cellular/NMEA UDP packets will be forwarded to the specified IP address. Data will be forwarded to the same port number used to receive the data. This option allows data to be used by a backup or secondary server.

7.5.2 TCP
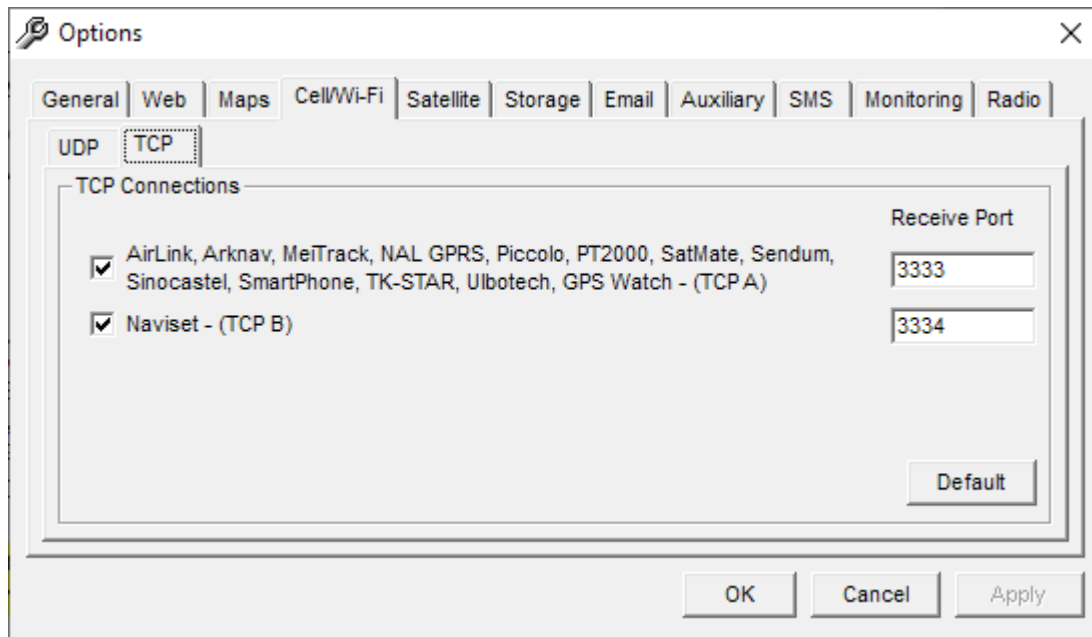
Figure 41 – Cell/Wi-Fi TCP Options

TCP A:	Enables data from AirLink, ArkNav, MeiTrack, NAL GPRS, Piccolo, PT2000, SatMate, Sendum, Sinocastel, SmartPhone, TK-STAT, Ulbotech and GPS Watch modems over TCP connections.
TCP B:	Enables data from Naviset modems (TCP).
Receive Ports:	TCP ports used to listen for data. Transmit ports are not defined, as these are set dynamically when data from an asset is received. This allows data to flow through a NAT server.

7.6 Satellite

7.6.1 Globalstar Duplex
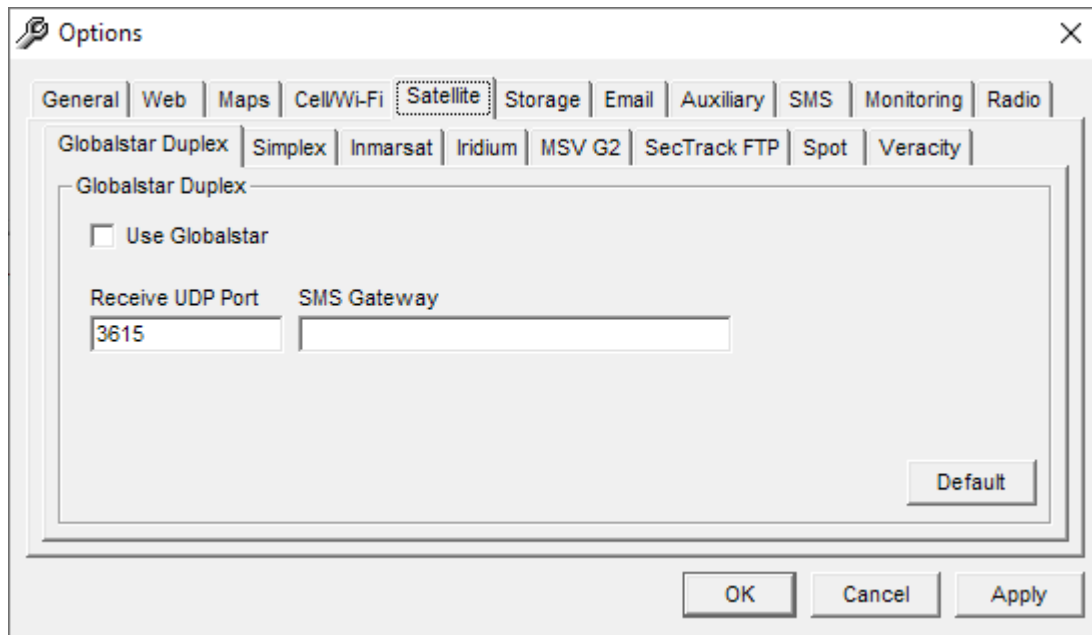
Figure 42 – Globalstar Options

Use Globalstar: Enables IP data from Globalstar duplex modems.
UDP Port: UDP port used to listen for data.
SMS Gateway: SMS gateway address for sending messages to wake up modems.

7.6.2 Simplex
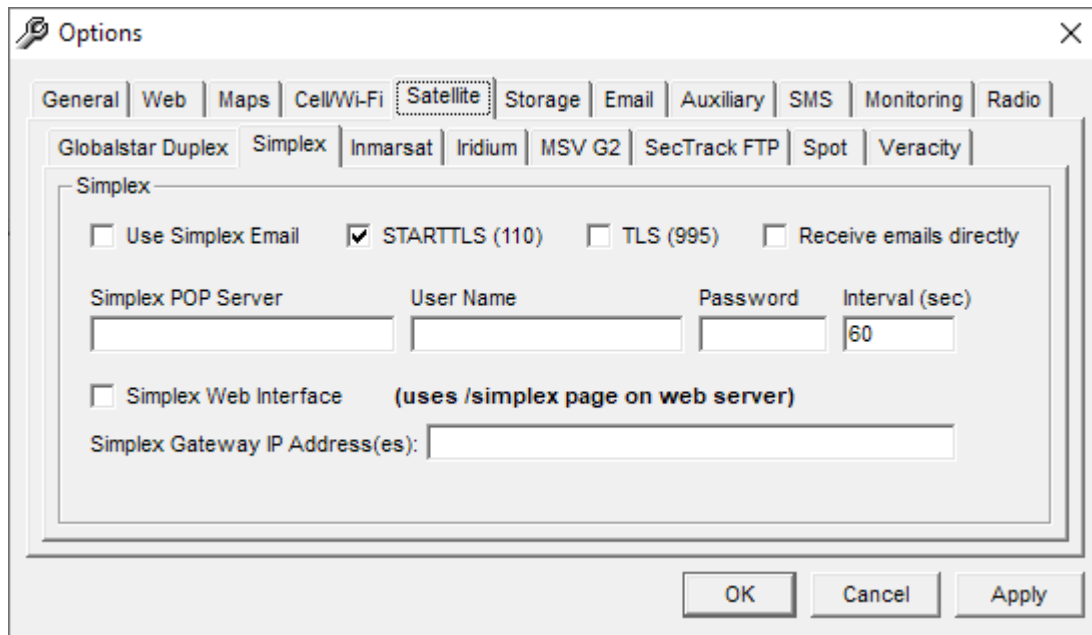
Figure 43 – Simplex Options

Use Simplex Email:	Receive Simplex data via email. This is normally achieved by using DataLink's PlexGate server as a proxy gateway to translate Globalstar XML data into email addresses. PlexGate is useful where a single XML connection is available, but data needs to be sent to multiple DataGates.
Use STARTTLS:	Use STARTTLS to upgrade to a secure mail connection.
TLS:	Check emails using TLS via a secure port.
Receive emails directly:	Enterprise versions can receive emails directly. Emails addressed to the user name defined here will be parsed as simplex data.
POP Server:	External email server that will collect emails.
User Name:	Name for POP access, or user name for receiving emails directly.
Password:	POP password. When supported by the POP server, DataGate will encrypt the password when logging in (even with TLS disabled).
Interval:	Update period for mailbox checks.
Simplex Web Interface:	DataGate accepts Simplex data via a built-in web service using the /simplex web page, e.g. http://datagate.example.com/simplex. This address must be given to Globalstar when setting up connections. DataGate can accept both DTD and XSD formatted data.
Gateway IP Addresses:	Enter one or more IP addresses which will be allowed to send simplex data to DataGate. These may be individual addresses or network ranges (such as 192.168.0.0/24). Enter * to accept any address.

7.6.3 Inmarsat
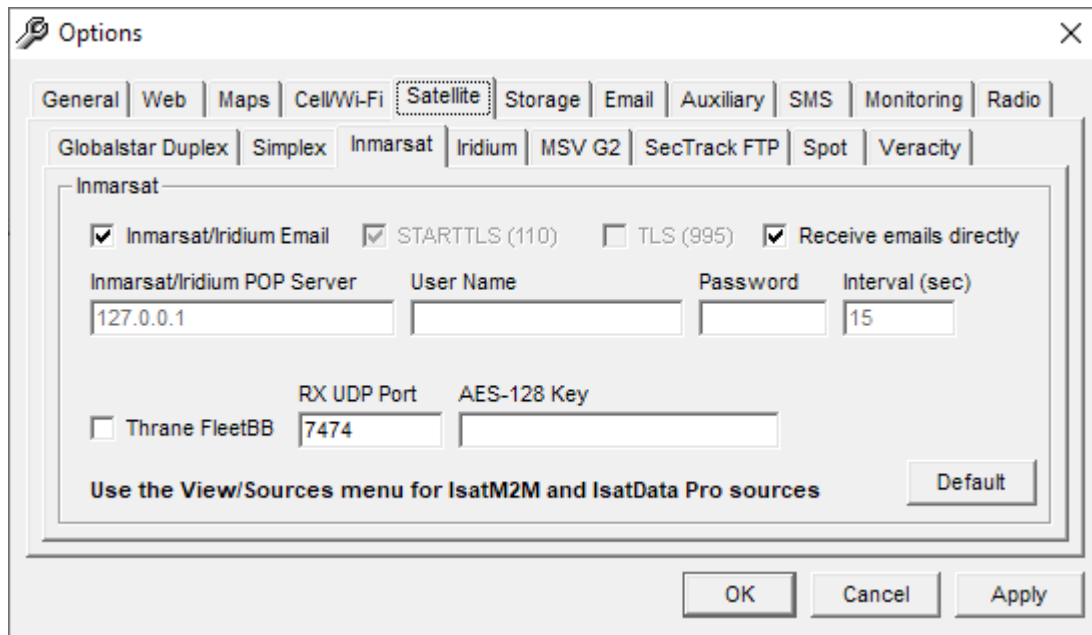
Figure 44 – Inmarsat Options

Use Inmarsat/Iridium:	Inmarsat data (except IsatM2M) and Iridium SBD data can be received by email.
Use STARTTLS:	Use STARTTLS to upgrade to a secure mail connection.
TLS:	Check emails using TLS via a secure port.
Receive emails directly:	Enterprise versions can receive emails directly. Emails addressed to the user name defined here will be parsed as simplex data.
POP Server:	External email server that will collect emails.
User Name:	Name for POP access, or user name for receiving emails directly.
Password:	POP password. When supported by the POP server, DataGate will encrypt the password when logging in (even with TLS disabled).
Interval:	Update period for mailbox checks.
Thrane FleetBB:	Thrane&Thrane Fleet Broadband data can be accepted using a UDP port.
UDP Port:	Port for Fleet Broadband data.
AES-128 Key:	AES key used to decode data from Fleet Broadband devices.

7.6.4 Iridium
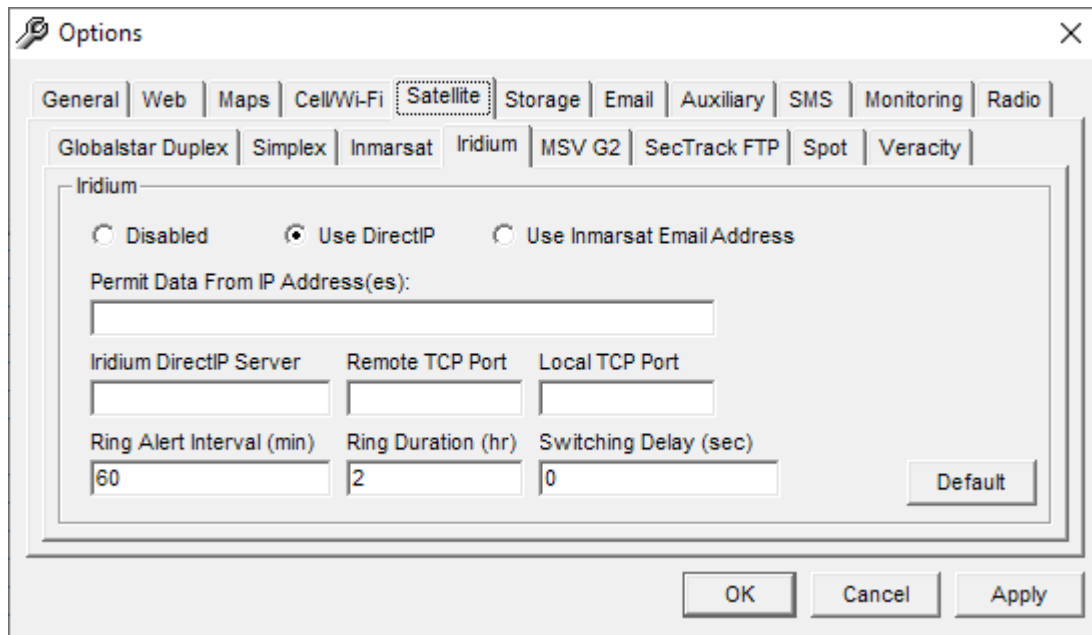
Figure 45 – Iridium Options

Use DirectIP:	DirectIP allows the Iridium gateway to connect directly to DataGate when it has SBD packets to send.
Use Email:	Optionally, Iridium SBD packets can be received via email, using the same account set under the Inmarsat settings.
Permit Addresses:	Enter one or more IP addresses which will be allowed to send SBD data to DataGate. These may be individual addresses or network ranges (such as 192.168.0.0/24). Enter * to accept any address.
DirectIP Server:	DataGate will connect to this server when sending SBD data to modems.
Ports:	Ports used to send and receive data.
Ring Alert Interval:	If non-zero, DataGate will periodically send Ring Alert packets to assets that have not responded to sent packets. This ensures that assets will pick up waiting data if they were turned off or out of coverage when the data was first sent. Ring alerts are sent at the programmed interval for up to the Ring Duration period.
Ring Duration:	Ring alerts will be sent for this period, or until an asset has downloaded any waiting data from the Iridium data queue.
Switching Delay:	Use this setting to delay switching to satellite networks when sending data to multi-network devices. This can be useful if your devices are using a lower-cost network that does not allow mobile-terminated data. It gives the devices time to connect to DataGate so that data can be exchanged over the cheaper route. Note that this will increase the packet timeouts when sending data.

7.6.5 MSV G2
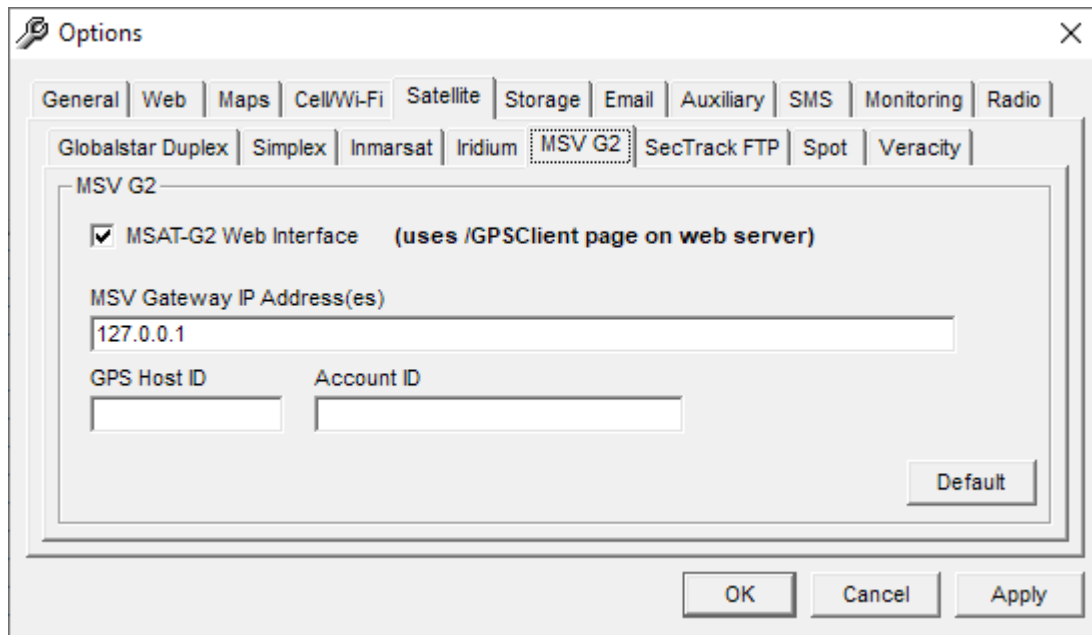
Figure 46 – MSV G2 Options

Use MSV-G2:   DataGate accepts G2 data via a built-in web service using the /gpsclient web page, e.g. http://datagate.example.com/gpsclient. This address must be given to MSV when setting up connections.

Gateway Addresses: Enter one or more IP addresses which will be allowed to send G2 data to DataGate. These may be individual addresses or network ranges (such as 192.168.0.0/24). Enter * to accept any address.

**Host/Account ID:**   Enter the IDs provided by MSV when setting up the account.

7.6.6 SecTrack
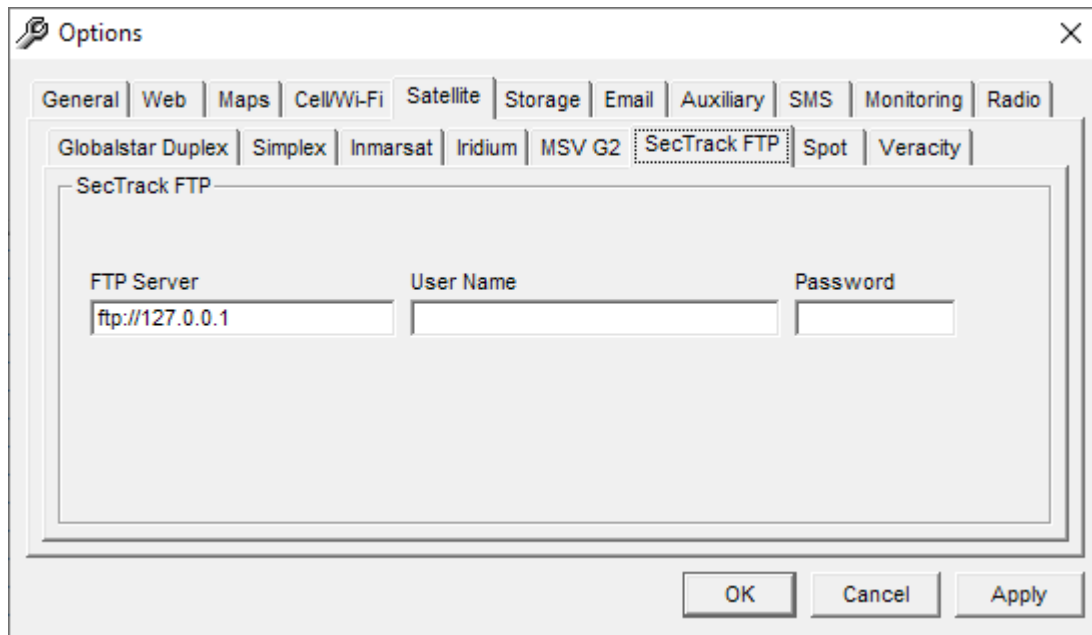
Figure 47 – SecTrack Options

FTP Server: Enter the FTP server where SecTrack data will be sent.
User Name/Password: Settings for logging in to FTP server.

7.6.7 Spot
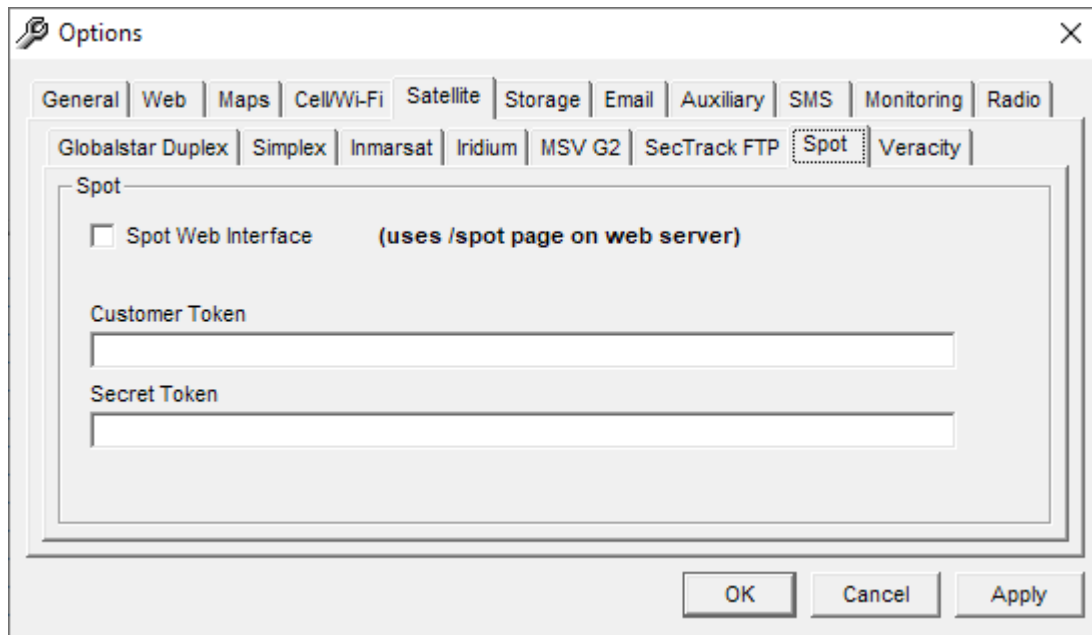
Figure 48 – Spot Options

Spot Web Interface: Globalstar Spot data is accepted via a built-in web service using the /spot web page, e.g. http://datagate.example.com/spot. This address must be given to Globalstar when setting up connections.

Tokens: A customer and secret token must be entered to authenticate communications. These are provided by Globalstar when setting up the account.

7.6.8 Veracity
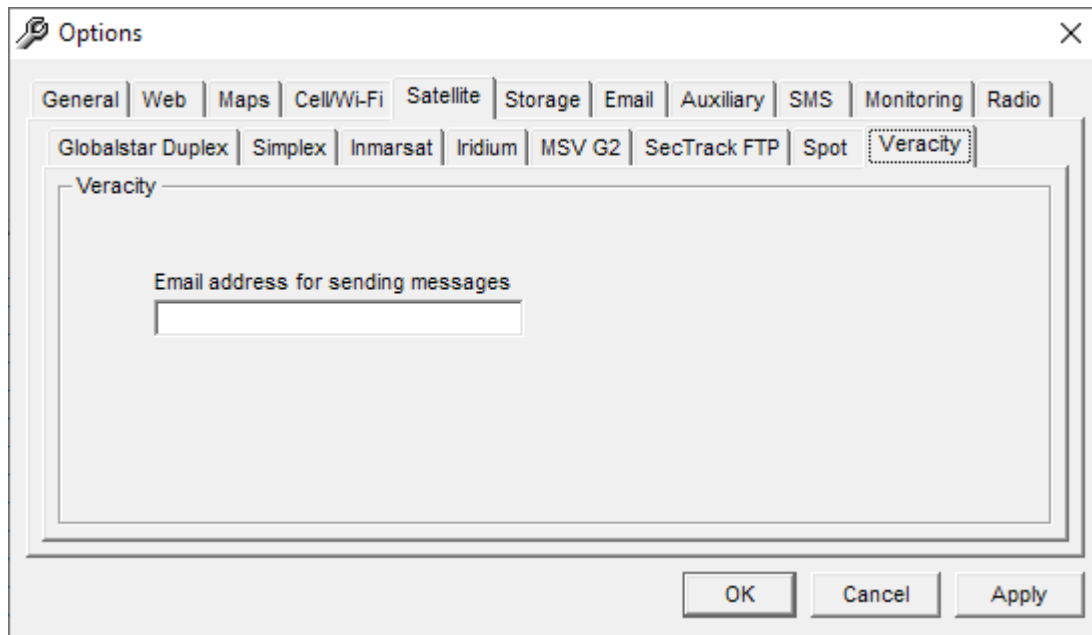
Figure 49 – Veracity Options

Email address: Outgoing messages to Veracity modems will be sent to this email
                            address.

7.7 Storage

7.7.1 Primary Storage
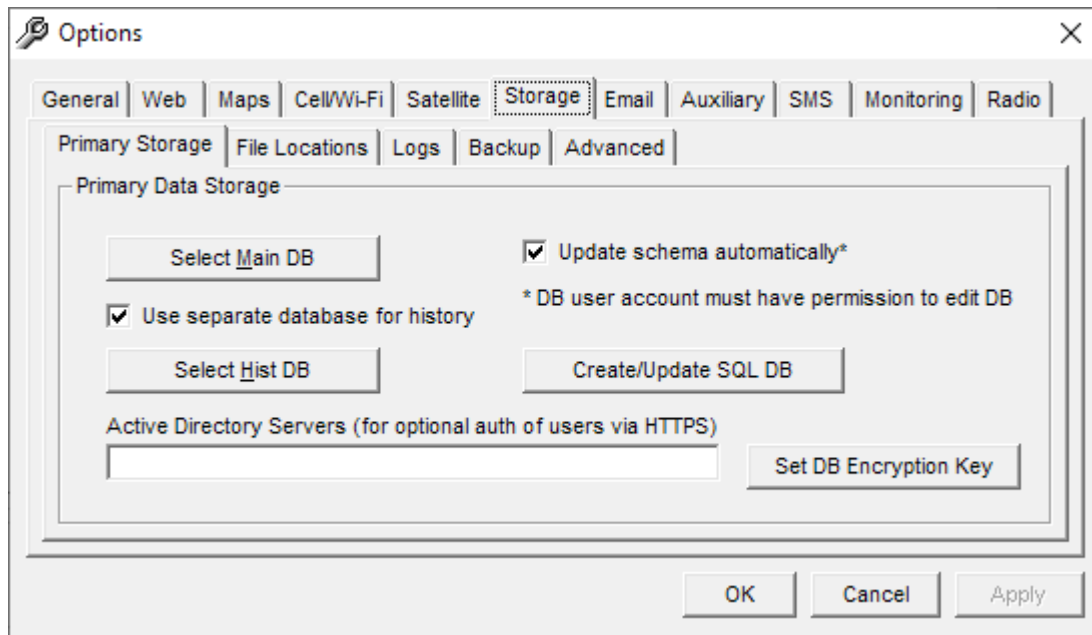
Figure 50 – Primary Data Storage Options

Select Databases:	Clicking on these buttons opens the standard Windows database properties window, where the database provider and connection parameters can be entered. See section 20.0 for details.
Use separate database:	When enabled, DataGate will use a second database for historical data. This makes archiving easier, and reduces the time taken to back up the main database.
Update Schema:	If enabled, DataGate will automatically update the database tables when connecting to a database with an old schema. Note that some schema updates may take a long time with a large database. In some cases the schema update will fail due to lack of memory or a database becoming too large. In this case you may need to archive some history data to allow the update to succeed.
Create/Update SQL DB:	Use this link to automatically create and update SQL Server databases. The database login must have permission to create databases and/or edit tables. See section 0 for details.
Active Directory:	DataGate can optionally authenticate logon attempts by querying an Active Directory. Enter one or more server addresses separated by a comma, or leave blank to use the default domain controller. See section 10.1.1 for details on enabling AD lookup for each user.
Set DB Encryption Key:	Clicking this button opens the database encryption key screen shown in Figure 51. By default, DataGate encrypts sensitive database records (such as user passwords) using a built-in encryption key. When a custom key is set, DataGate will use this key instead, which will prevent your encrypted fields being read by another DataGate installation (unless it also uses the same key).

Note that the key is stored in the DataGate ini file after encryption with the built-in encryption key, so this file should be kept secure.

7.7.2 Database Encryption Key
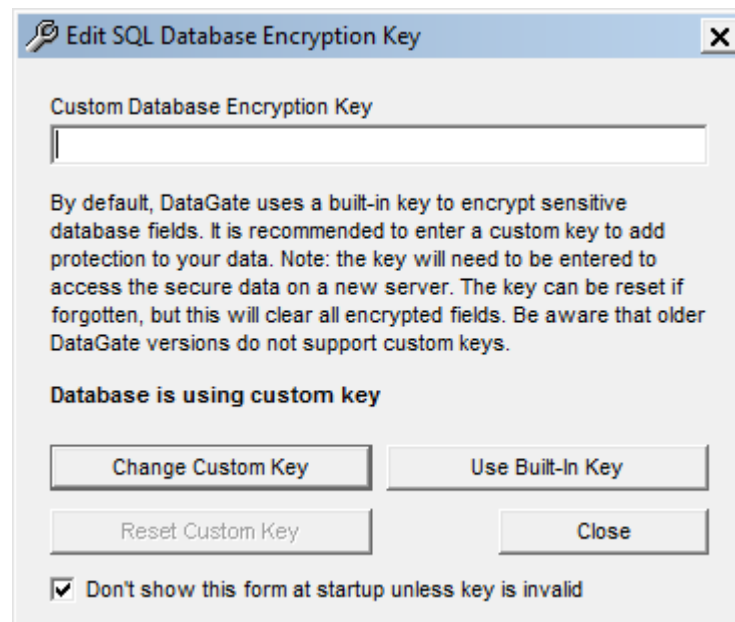
Figure 51 – Edit Database Encryption Key

Change Custom Key:	Saves the new key. If the database is currently open, all encrypted database records are rewritten with the new custom key. If the database is not open, the key is checked to confirm it matches the key used to encrypt the database.
Use Built-In Key:	Clears the custom key. If the database is currently open, all encrypted database records are rewritten with the built-in key. Use this option if you want the database to be readable by an older DataGate version without custom key support.
Reset Custom Key:	In the event that the custom key is forgotten, use this option to force the key to be reset. Note that all encrypted records will be cleared.
Don't Show form:	Prevents this form showing at start-up when no key is set.

7.7.3 File Locations
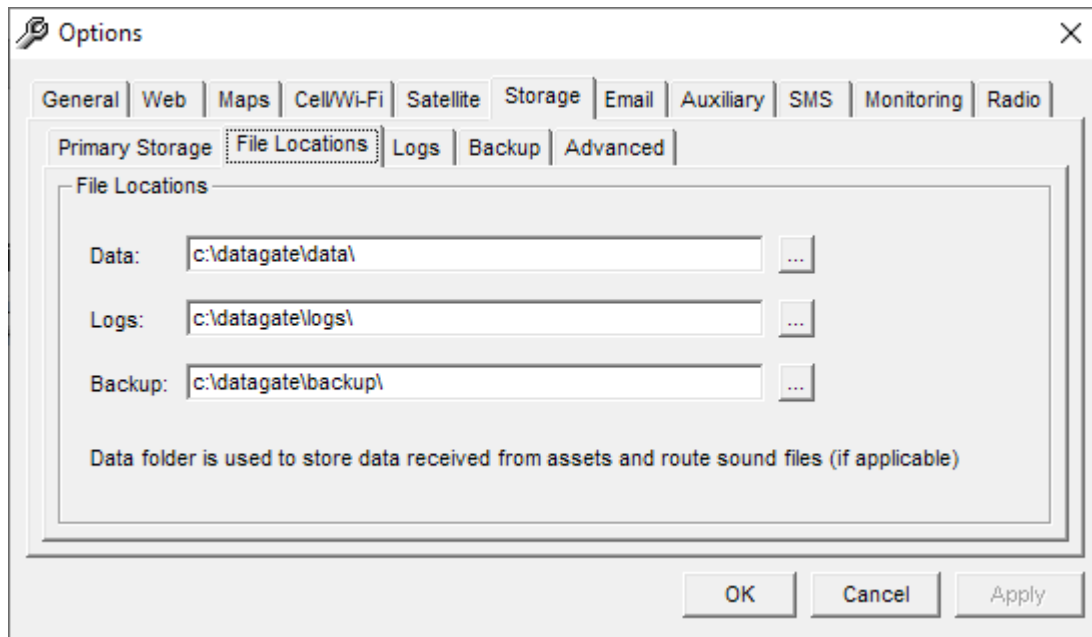
Figure 52 – File Location Options

Data File Location:	DataGate uses this folder to store data from assets.
Logs Location:	DataGate log files are written here.
Backup Location:	DataGate will generate daily data file backups (if primary storage is set to files). Backups are also made when updating data files from one version to another.

7.7.4 Logs
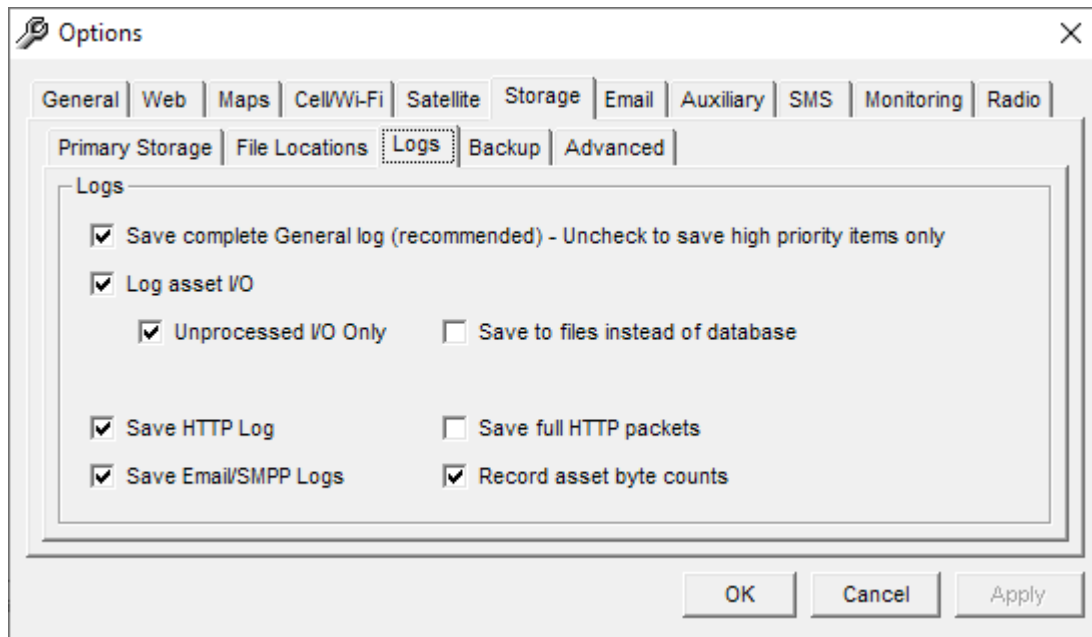
Figure 53 – Log Options

Save Complete Log:	If active, DataGate saves a complete record of the log listing window (recommended). Otherwise, only alerts, errors, and warnings are saved.
Log Asset I/O:	DataGate can save a copy of all data sent to and received from assets (recommended). This is useful if you need to play back data at a later stage. If primary storage is set to files, this data will be stored in the log folder. Otherwise it is written into the database itself.
Unprocessed Only:	If enabled, only unprocessed data will be saved. This data will include unknown packets or data from unlisted device IDs. Selecting this option will reduce the size of the database, but will prevent accessing processed raw data via historical reports in WebGate.
Save to files:	When enabled, asset I/O will be saved to file instead of database. This may speed up the parsing routines, improving performance on a heavily loaded server. Using this option prevents accessing raw data via historical reports in WebGate.
Save HTTP Log:	This option causes DataGate to save a copy of data sent and received on its web interface. The log includes the entire contents of received requests, but only the header of replies.
Save Full HTTP:	Logs will contain full HTTP packets. If disabled, the logs will contain packet headers only.
Save Email/SMPP Log:	Save logs relating to email and SMPP (SMS) messages.
Record byte counts:	When enabled, DataGate keeps track of the data used by each asset.

7.7.5 Backup
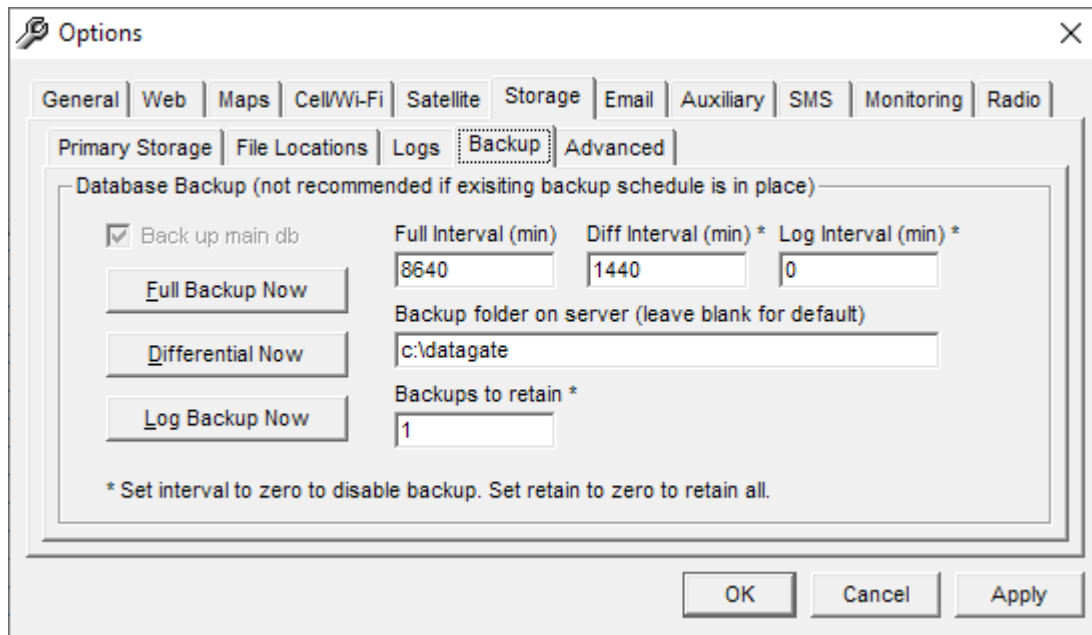
Figure 54 – Backup Options

Back up main db:	DataGate can be set to periodically back up the SQL database. This is only recommended if no other back up schedule exists, otherwise the log sequences can be disrupted.
Full Interval:	Number of minutes between full backups. If the log interval is non-zero, a log backup will also be performed. Each full backup starts a new backup file (and log file, if required).
Diff Interval:	Minutes between differential backups. This interval must be shorter than the full interval. Set to zero to disable differential backups.
Log Interval:	Minutes between log backups. Log backups are only available when the database is set to the "Full" recovery model. For databases using the "Simple" model, set this value to zero to disable log backups. Frequent log backups are recommended (in full mode), as they allow the database to automatically truncate the transaction log.
Backup Folder:	This is the folder where the backups will be saved. Note that this location is on the SQL Server machine. Leave blank to use the database default location.
Backups to Retain:	Number of full backups to retain. Once this number of backups has been performed, the oldest will be overwritten.

Use the Backup Now buttons to perform an immediate backup.

The backup filenames will be in the form:

Full/Differential:	*backup_folder*\datagate_backup_x.bak
Log:	*backup_folder*\datagate_log_backup_x.trn

where x is a sequence number from 1 to *backups_to_retain*.

7.7.6 Advanced
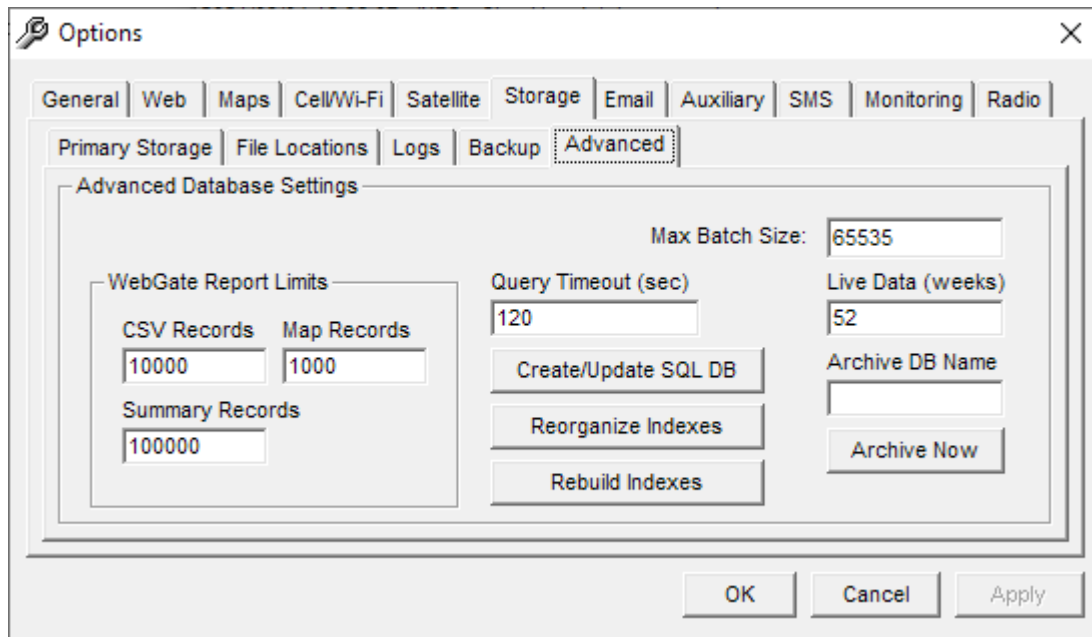
Figure 55 – Advanced Options

Max Batch Size:	Maximum size for batched queries.
CSV Records:	Maximum number of records to return in a WebGate historical report (when running a CSV report).
Map Records:	Limits the number of records returned for WebGate map reports (Map/KML). This limit should be smaller than the CSV limit, as there is more processing involved when displaying points on a map.
Summary Records:	Maximum number of records for summary reports.
Query Timeout:	Sets the timeout for SQL queries sent to database. Large or busy databases may need longer timeouts to allow queries to complete.
Archive DB Name:	Name of database to use for archiving. This database must exist on the database server being used to store history data.
Live Data:	Number of weeks of data to keep in the main history table when archiving data.
Archive Now:	Automatically move old data from the history and raw data tables to the archive database. This will also delete any message links pointing to archived data. Note that archiving large amounts of data at one time may fail due to the size of temporary tables required.
Create/Update SQL DB:	Use this link to automatically create and update SQL Server archive databases. The database login must have permission to create databases and/or edit tables. See section 20.3 for details.
Reorganize/Rebuild:	Shortcuts to reorganize or rebuild the database indexes. Do this periodically to reduce index fragmentation.

7.8 Email

7.8.1 General
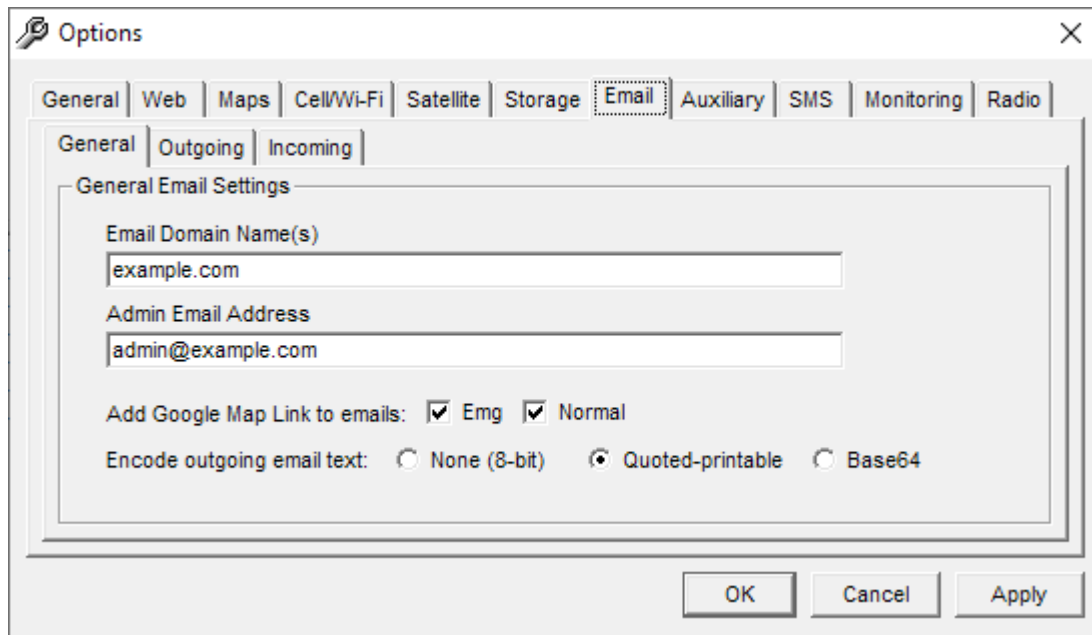
Figure 56 – General Email Options

Domain Names:	This is a list of domains or IP addresses for which the DataGate will accept incoming messages (used by Enterprise version only).
Admin Email Address:	Address where DataGate will send messages when it encounters any errors or alerts. Leave blank to disabled admin emails.
Add Google Map Link:	Select whether alert emails will contain an embedded Google Map link pointing to the asset location (when available). This option can be applied to both high priority and standard messages.
Encode Email Text:	Choose how email text is encoded. None (8-bit) should be acceptable in most cases.

7.8.2 Outgoing
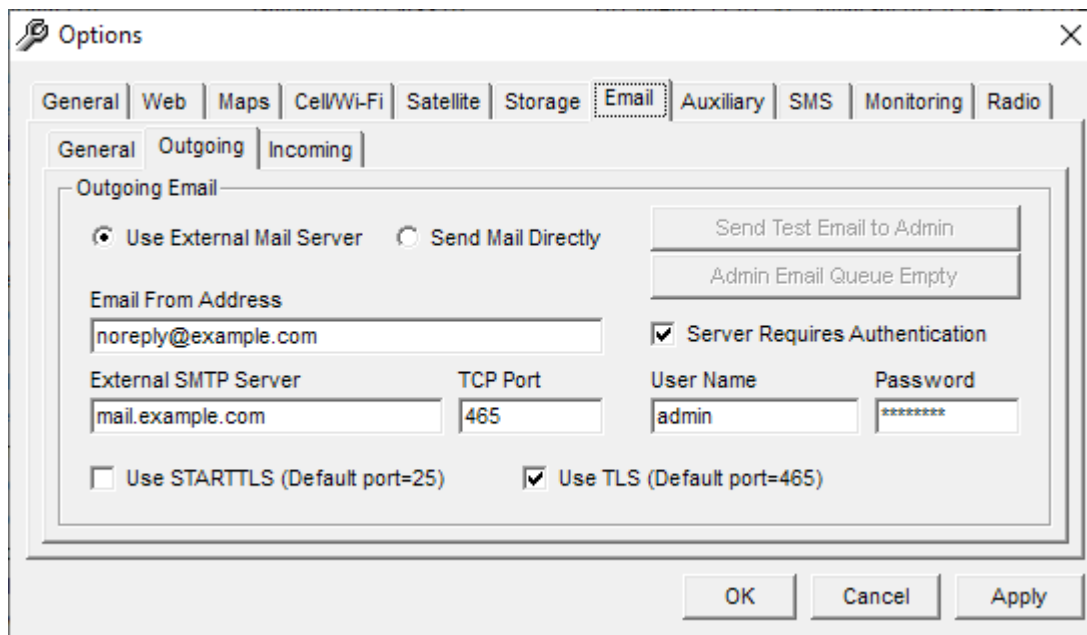
Figure 57 – Outgoing Email Options

Use External Server:	If selected, DataGate will use an external email server to send email.
Send Directly:	DataGate can also send email directly. This gives DataGate more control when sending mail, but messages a more likely to get rejected if the server's settings or DNS records are incorrect.
Email From Address:	Address to send email from. If using an external server it is recommended to use a valid account on that server. If sending directly, this address should use the email domain name assigned to your DataGate server. See section 14.0.
Email Test:	Send a test email to the admin address. This button will only be active when any changes to the address have been applied.
Clear Queue:	Delete any admin emails waiting to be sent.
External SMTP Address:	If using the external server option, enter the email server address.
TCP Port:	Port used to connect to the server. Standard port is 25 for unencrypted or when using STARTTLS, but 587 is a common alternative. Port 465 is standard for TLS connections.
Authentication:	Use this option to authenticate with the mail server before sending mail. This may be required by some servers to prevent open relaying of mail.
User Name/Password:	Settings for authenticating with server.
Use STARTTLS:	Encrypt the connection when sending email. This option upgrades a plain text connection to SSL, and generally uses port 25 or port 587.
Use TLS:	This option uses TLS for the entire connection, and generally uses port 465.

7.8.3 Incoming
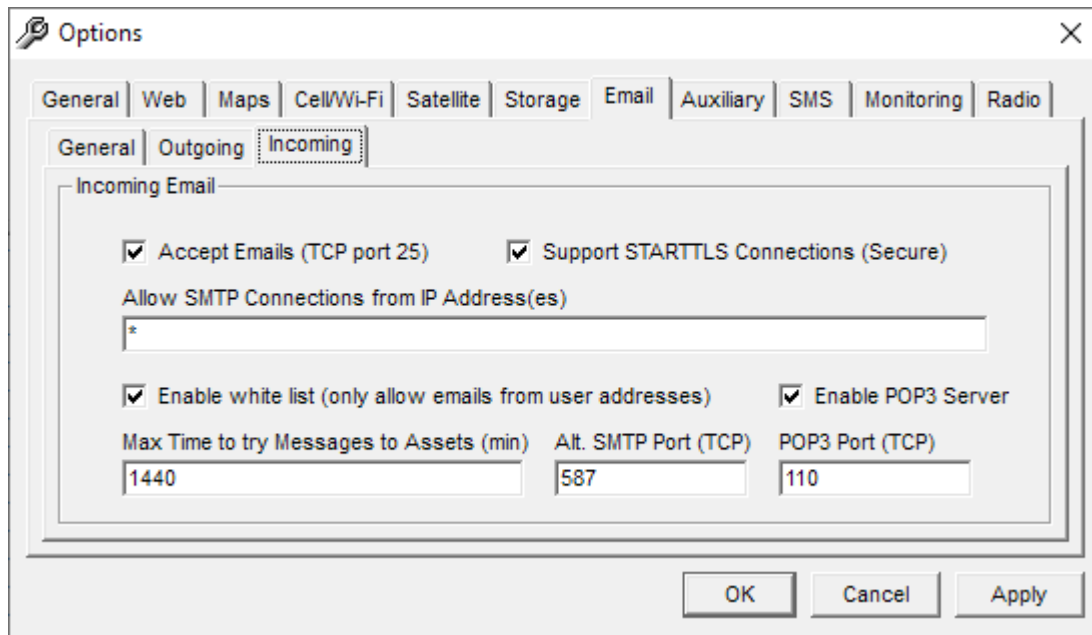
Figure 58 – Incoming Email Options

Accept Emails:	Enterprise versions of DataGate can accept emails on TCP port 25. See section 14.0.
Support STARTTLS:	Allow remote servers to encrypt the connection when sending emails to the DataGate. Also enables encryption for POP3 connections.
Allow SMTP From:	Enter one or more IP addresses which will be allowed to send emails to DataGate. These may be individual addresses or network ranges (such as 192.168.0.0/24). Enter * to accept any address.
Enable White List:	When enabled, this option will reject any incoming messages unless the sender's address is assigned to one of the DataGate users. This white-listing process is explained in section 14.3.
Enable POP3 Server:	Enterprise versions of DataGate contain a POP3 server to hold messages to users. Users can log in to this server to download waiting messages from assets.
Max Time to try Msgs:	Time limit for sending messages received from an email source to an asset. If this time expires before the message is sent, a delivery failure is returned to the original sender.
Alternate SMTP Port:	Second port for incoming SMTP connections.
POP3 Port:	Port used for POP3 server.

7.9 Auxiliary

Figure 59 – Auxiliary Options

TCP Server:	DataGate can accept connections from third-party applications using a TCP connection. Data is then exchanged in the selected format.
Format:	Format of TCP data. If DataGate XML is selected, DataGate will use its built-in web server, accepting data on its /xml page.
External IP Address:	Enter one or more IP addresses which will be allowed to connect to DataGate's TCP server. These may be individual addresses or network ranges (such as 192.168.0.0/24). Enter * to accept any address.
Listening TCP Port:	Port for TCP connections. Note that XML polling is handled through DataGate's web server, using the ports defined under the Web tab.
Push to Web Service:	When enabled, DataGate will connect to an external web service to pass device data via XML or JSON packets.
Format:	Format for XML/JSON data. DataGate supports some generic and custom formats. New formats can be defined if required.
Web Service Address:	Destination address for web service connections.
User/Password:	User ID and password included in web service XML packets. Also used to authenticate incoming XML-based TCP connections.
Send SNMP Alerts:	DataGate can be configured to send SNMP alerts when high priority alerts occur. This allows existing SNMP servers to detect and process the alerts.
Community Name:	Used in SNMP packets.
SNMP Server:	Destination address for SNMP.
Send Test Trap:	Send a test SNMP trap.
Send data from all:	If enabled, all asset data will be pushed to the external web service. Otherwise, assets are only included if enabled on the Asset Properties page.

Pager Message Files: Enter a folder name, optionally including a filename with or without wildcards. DataGate will monitor this location for message files. See section 19.1.

DataGate will buffer data for external TCP and web service connections until sent. The amount of buffered data is shown at the bottom of this screen. A "Clear Queue" button is provided to clear the data buffer, if required.

Note: when using a database for primary storage, DataGate will search for unsent packets at startup, and buffer them for sending to the web service. This ensures that all data is passed to the external server, even if DataGate is restarted.

7.10 SMS (Enterprise Version Only)

7.10.1 Config
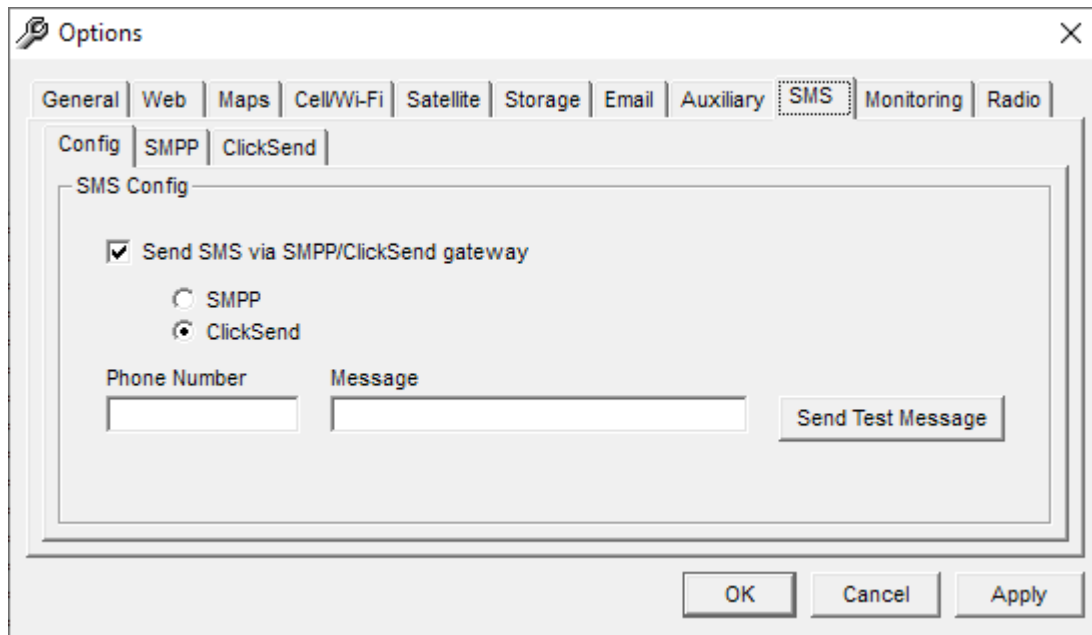
Figure 60 – SMS Config

Send SMS: If enabled, DataGate can send/receive SMS messages using an external SMPP or ClickSend gateway. SMS messages are generated when sending remote configuration commands to certain assets, and also when sending alert emails to addresses without an "@" or domain part. Incoming SMS messages are used by some devices to send data to the server. Select whether to enable SMPP or ClickSend connections.

Phone/Message: Provides a simple interface for sending test SMS messages.

7.11.1 SMPP

Figure 61 – SMPP Options

Debug:	Include detailed information in log.
User Name/Password:	Used for logging in to SMPP server.
System Type/TON/NPI:	Connection details.
Server ID:	Phone number or code that the server can be reached using.
Gateway address:	SMPP server address.
Port:	Connection port.
Msg Rate:	Limits message rate for sending messages to server.
Data Coding:	Coding parameter for sending messages. Defaults to '0', but can be changed if SMPP gateway does not encode messages correctly.
GSM:	Select to encode outgoing messages as 7-bit GSM. Default uses 8-bit Latin ASCII characters.

7.11.2 ClickSend

Figure 62 – ClickSend Options

Debug: Include detailed information in log.
API Username/Pass: Used for logging in to ClickSend server.
Msg Rate: Limits message rate for sending messages to server.
From Number: Define the from address for messages. This may require purchasing
                              a dedicated number through ClickSend.

7.12 Monitoring
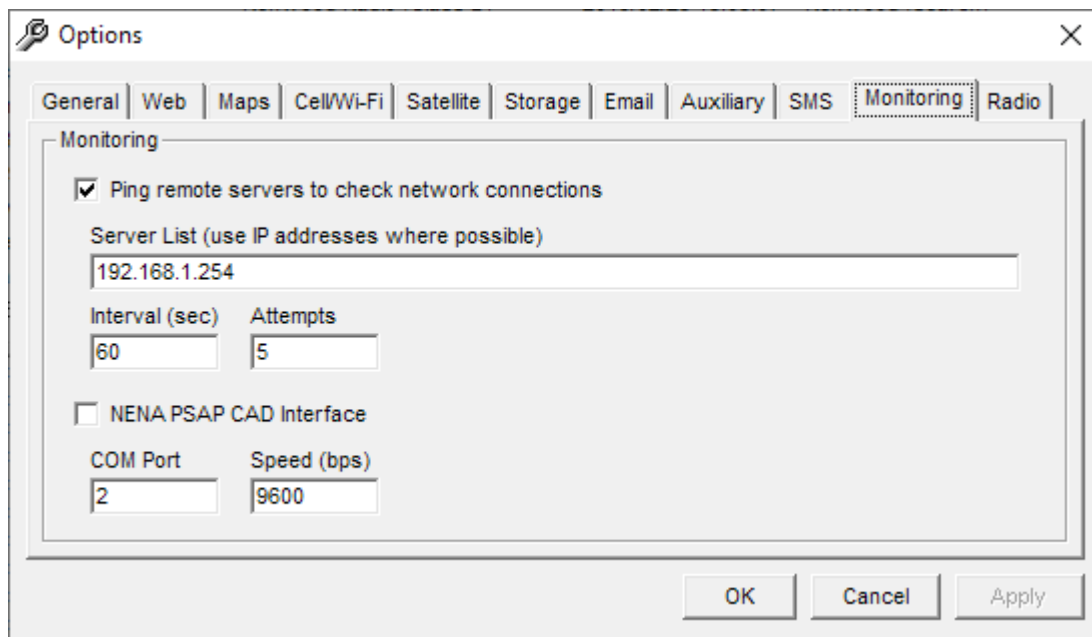
Figure 63 – Monitoring Options

Ping remote servers:	When enabled, this option causes DataGate to periodically send a ping to the listed servers. An alert is generated if there is no response from any address.
Server List:	List of server names or IP addresses to check. Separate multiple servers with a space, comma or semicolon.
Interval:	Seconds between checks.
Attempts:	An alert is generated after if the packet fails for this many attempts.
NENA PSAP Interface:	Experimental interface to PSAP connection to obtain address information for emergency dispatch consoles.

7.13 Radio
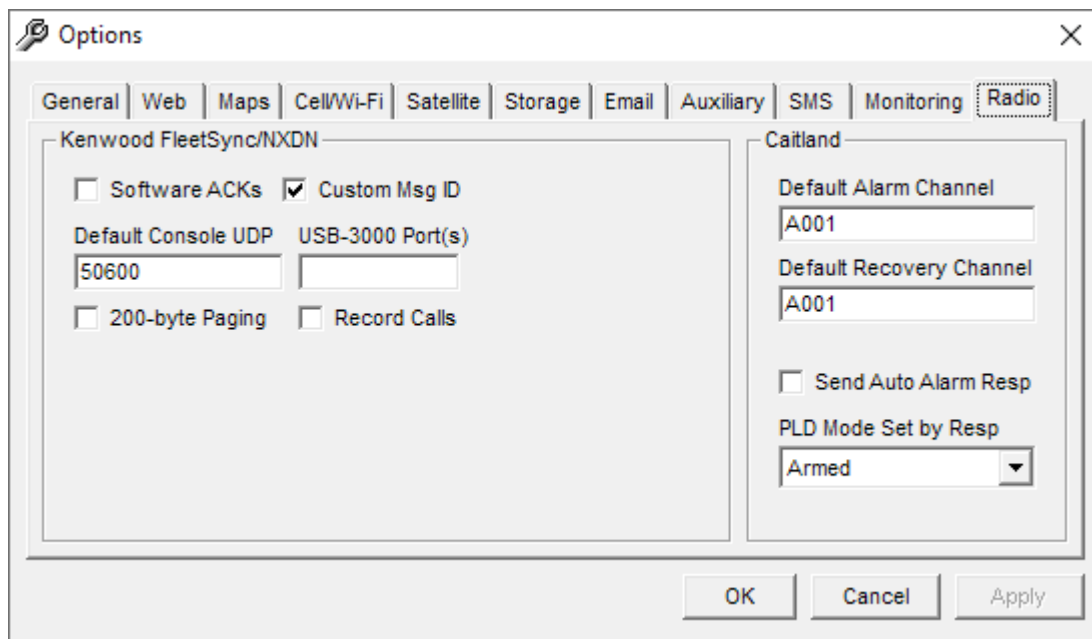
Figure 64 – Radio Options

Software ACKs:	When sending data to an iSeries device over Kenwood networks, request ACKs from the device. This increases reliability, but adds extra traffic on the network. When disabled, DataGate relies on the ACKs provided by the radios themselves.
Custom Msg ID:	When enabled, DataGate includes a message ID in text messages sent to radios. This allows radios with special firmware to reply to specific messages. This is especially useful when sending email messages to radios, in which case the responses are sent as replies to the original email.
Default Console Port:	Default UDP port number for receiving Kenwood IP console data.
USB-3000 Port:	Select virtual COM ports used for decoding Kenwood voice calls.
200-byte Paging:	When enabled, DataGate will send messages to Kenwood NXDN radios with up to 200 characters, instead of the standard limit of 100 characters. This requires special repeater firmware.
Record Calls:	Save incoming voice call data to disk. This data is currently saved as raw encoded data. Future development will allow decoding by using a USB-3000 dongle.
Default Channels:	Channel assignments for Caitland devices. These channels will be presented as defaults to the user when sending commands.
Automatic Response:	When enabled, DataGate will automatically ACK alarms sent via Caitland RFU devices.
PLD Mode:	Mode to set Caitland PLDs in when sending alarm response.

8.0 Groups

DataGate allows users, assets, geofences, drivers, data sources and points of interest to be assigned to groups, simplifying asset/user assignment. Multiple levels of grouping are supported, allowing separation of customers, their departments and sub-departments.

As well as these user-defined groups, two special predefined groups exist:

Unassigned: Assets cannot be assigned to any users.
                      Users cannot be assigned any assets.
Root: Top parent group.

Users can only be assigned assets in their group or subgroups, and cannot access users, geofences, drivers, and points of interest in parent groups.

Data sources can only handle data for assets in their group or subgroups.

Assets, Users and Groups are automatically moved to their parent group if the group is deleted.

Note that administrator users may be assigned Sys Admin access. These users will have access to all assets and users in their group and subgroups. Sys Admin users belonging to the Root group can also access the Unassigned group.

8.1 Group List

Use the View/Groups menu on the main screen to open the Group List window. Groups may be added and deleted using the insert and delete keys, or the buttons on the toolbar.

Figure 65 – Group List

Note that the Unassigned and Root groups cannot be deleted or renamed.

8.2 Group Properties

Double-click on a group in the Group List to open the properties window.
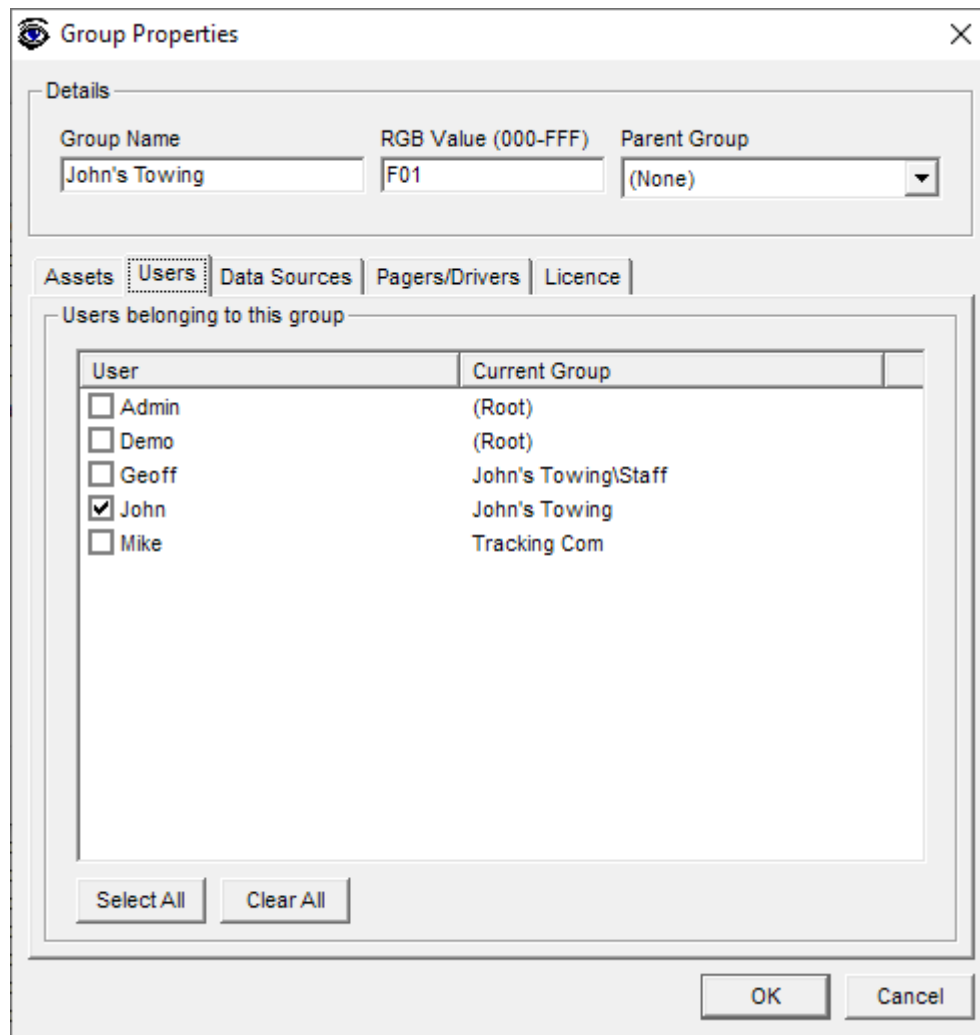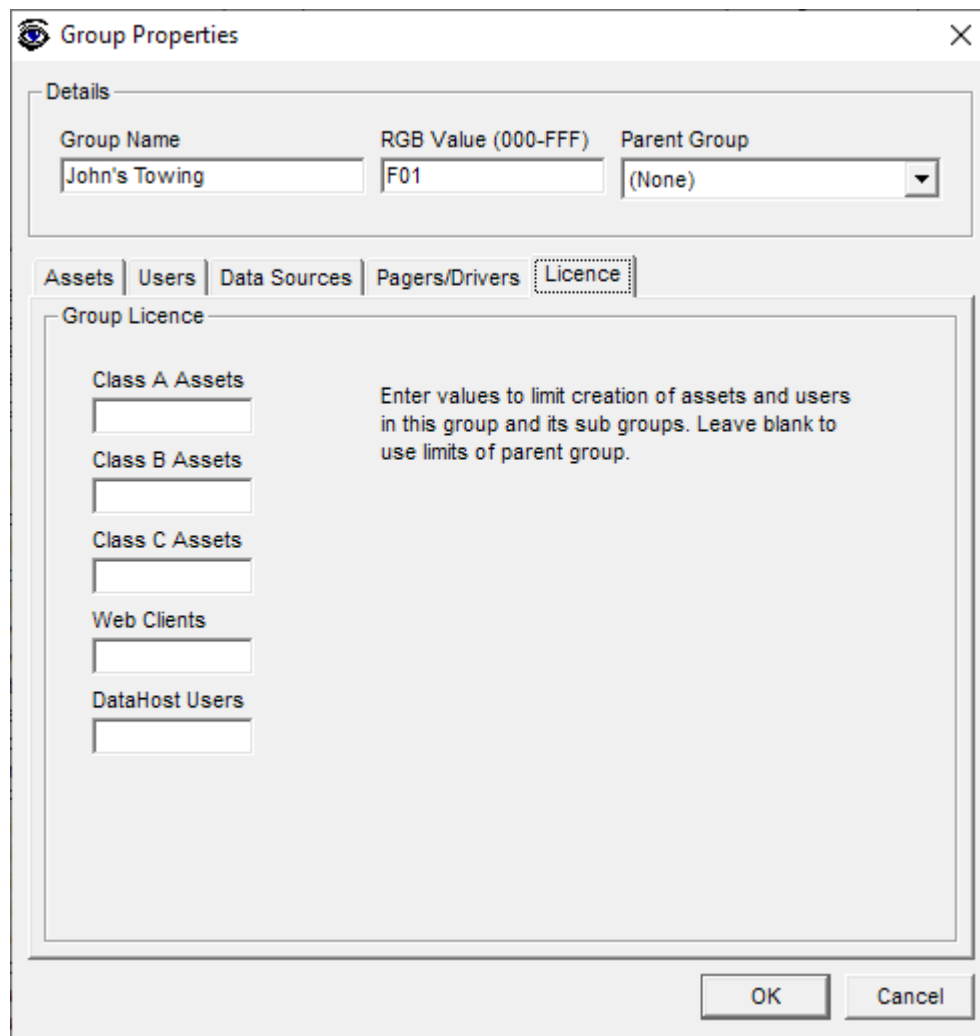
Figure 66 – Group Properties

Each group can be assigned a name and parent group. Set the parent group to (None) to create a top level group, or select a parent group to create a sub-group. A custom color can also be defined for this group (see section 18.1.1).

Asset, User, Source, Driver lists are provided to make quick group assignments. Note that group assignments can also be made from the corresponding Asset/User/Source/Driver properties screens.

8.3 Group Licensing

Figure 67 – Group Licence

Each group can be assigned limits on the generation of assets and users. This is useful when granting Sys Admin rights to users in sub-groups – allowing them to create their own users and assets.

9.0 Assets

9.1 Asset List

The asset list on the main screen shows all assets configured on the DataGate. It includes the Asset ID, Description, Hardware Type, Last Report time, Last Network used, Group, and number of Users that have access to this asset. The list can be sorted by clicking on the desired column header.

Each asset is shown with an icon, which provides a quick indication of the asset status, as follows:

- 🟢 Recent asset report (<1 hour)
- 🔴 Older asset report (>1 hour and <24 hours)
- ⚪ Old asset report (>24 hours)
- 🔍 Last attempt to contact asset failed (device off or out of range)

Assets may be added and deleted using the insert and delete keys, or the buttons on the toolbar.

9.2 Asset IDs

DataGate assets are identified by Asset IDs. These IDs are assigned when assets are added to the DataGate, and cannot be changed once created. By default, each ID consists of three numbers separated by dots. Each number can range from 0 to 255, giving a range of IDs from 0.0.0 to 255.255.255. Address 0.0.0 is reserved but all other combinations are valid. Alternatively, DataGate can display IDs as a single number, ranging from 1 to 16777215. Section 7.2.1 shows how to set this option.

Use the following equations to convert from one form of ID to another:

Given a dotted ID (A.B.C) then the decimal ID = (A * 65536) + (B * 256) + C
For example, ID (5.100.7) = (5 * 65536) + (100 * 256) + 7 = 353287.

Given a decimal ID X then the dotted ID (A.B.C) can be calculated:
A = Integer value of (X / 65536) rounded down
B = Integer value of ((X – (A * 65536)) / 256) rounded down
C = X – (A * 65536) – (B * 256)

For example, for decimal ID 353287:
A = Int(353287 / 65536) = 5
B = Int((353287 – (5 * 65536)) / 256) = 100
C = 353287 – (5 * 65536) – (100 * 256) = 7
Giving dotted ID (5.100.7)

When entering IDs, DataGate will accept IDs in either format, but will always display the ID based on the current ID format setting.

Note that automatic IDs are supported when adding assets via WebGate. In this case the first part of the ID is based in the user's group, while the rest uses the next available number.

9.3 Asset Properties

Double-click an asset in the asset list to open the Asset Properties window. This window is divided into several tabs, listed below. At the bottom of the window is a button labelled "Asset Same As", which allows the transfer of all asset settings from another asset, excluding asset-dependent settings such as Description and modem IDs.

9.3.1 General

This tab provides general asset information and settings (see Figure 68).

Figure 68 – General Asset properties

Description:	A user-friendly name for the asset. In Enterprise DataGate versions this name can also be used as the email address for the asset (e.g. test@example.com). If the description is not valid as an email address, and emails are enabled, a warning will be shown. In that case, the Asset ID can be used as an email address instead (e.g. 0.0.7@example.com).
Group:	Each asset can be assigned to a group. Note that this can also be defined under the Group Properties screen. See section 7.0 for more information about groups.
Asset Tag:	User configurable text assigned to this asset.
Hardware Type:	Type of asset hardware. The DataGate supports many different hardware devices, and Datalink is committed to adding further devices as required.
Store History:	Select whether to keep this asset's historical data in the database.

Forward to Ext:	If enabled, reports from this asset will be sent over DataGate's external TCP/UDP and web service connections. This option will be unavailable if there are no external connections set up, or if the external connections have been configured to send data from all assets (see section 7.9).
Accept Emails:	Enterprise versions of DataGate can convert incoming emails into text messages to send to an asset.
Device:	Device type. This will show firmware variations, if available.
Firmware Version:	Version of asset firmware, if available.
Current Driver:	Name of driver logged into asset, if available.
GPS Status:	Current GPS status.
Usage Counts:	Counters showing the amount of data sent and received for this asset.

9.3.2 Modems

Use this tab to configure the asset modem(s). Each hardware type will have different options available. Figure 69 shows the settings for a device that is capable of using multiple networks at once.
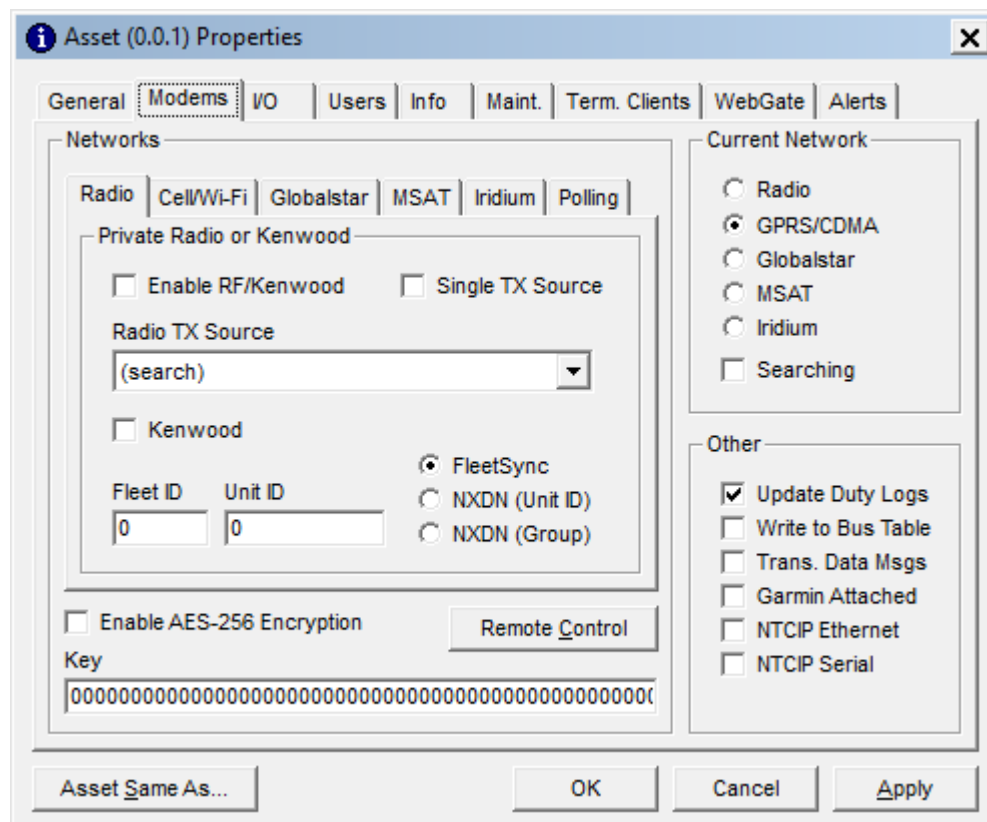
Figure 69 – Asset Modem Properties

| **Networks:** | Choose which networks this asset can operate on. Each network will have settings to identify the device, such as a network address or ID. Some networks may also have multiple Data Sources available. This screen allows the selection of the source used to transmit data, and controls whether the asset can send on multiple |

	sources (for example, in a radio network operating over a wide area).
AES-256:	The DataGate-256 edition supports AES-256 encryption, which certain devices support for secure communications. AES keys are entered as 64 hexadecimal characters (0-9 or A-F).
Current Net:	Set the current network. This will be tried first when sending data to the asset. The searching option indicates that DataGate has lost contact with the asset, and will try each enabled network when it has data to send.
Update Duty Logs:	Write duty log information from this asset to the database. This is only used in specific applications with a custom database.
Write to Bus Table:	Store location in the bus table (for third-party app).
Trans Data Msgs:	If checked, incoming transparent data messages will be forwarded to users as text messages. Normally such messages are sent to terminal clients only.
Garmin Attached:	Certain devices can connect to Garmin devices for messaging purposes. Enable this setting to allow outgoing messages.
NTCIP:	Option for iSeries hardware to connect to NTCIP highway signs. Select whether the sign is connected to the iSeries hardware via direct serial port, or a serial to Ethernet converter. When these options are enabled, DataGate formats messages as required by the NTCIP standard. WebGate will also show an option to request the current sign message.
Remote Control:	See next section for details

9.3.2.1 Remote Control

Certain asset types allow remote configuration of network settings. These settings are accessed by clicking on the "Remote Control" button on the Modems tab of the Asset Properties screen.

Note: the settings must be entered correctly, or else the asset may send data to the wrong PC, or may not be able to connect to the network.
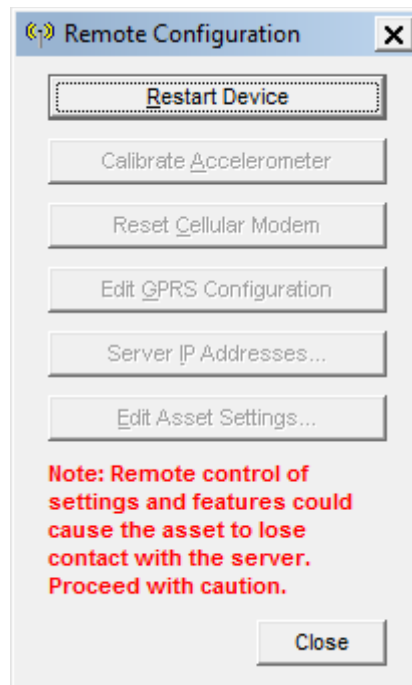
Figure 70 – Remote Configuration

Restart Device:	Reboot the device to make sure new settings are used.
Calibrate Accel:	Put the accelerometer into calibration mode.
Reset Cell Mode:	Restart the cell modem. Useful when IP address has been changed.
Edit GPRS Config:	Update GPRS connection information.
Server IP Addresses:	Set the IP addresses used to connect to DataGate. This allows the device to be moved to a different server. Note that the device will continue to listen to the current IP address for server IP address changes (in case an error is made).
Edit Asset Settings:	Remote control of individual asset settings.

9.3.3 Input/Output

This tab provides configuration options for asset input and output pins. Each hardware type will have different numbers of inputs and outputs available for use. Figure 71 shows an example asset.
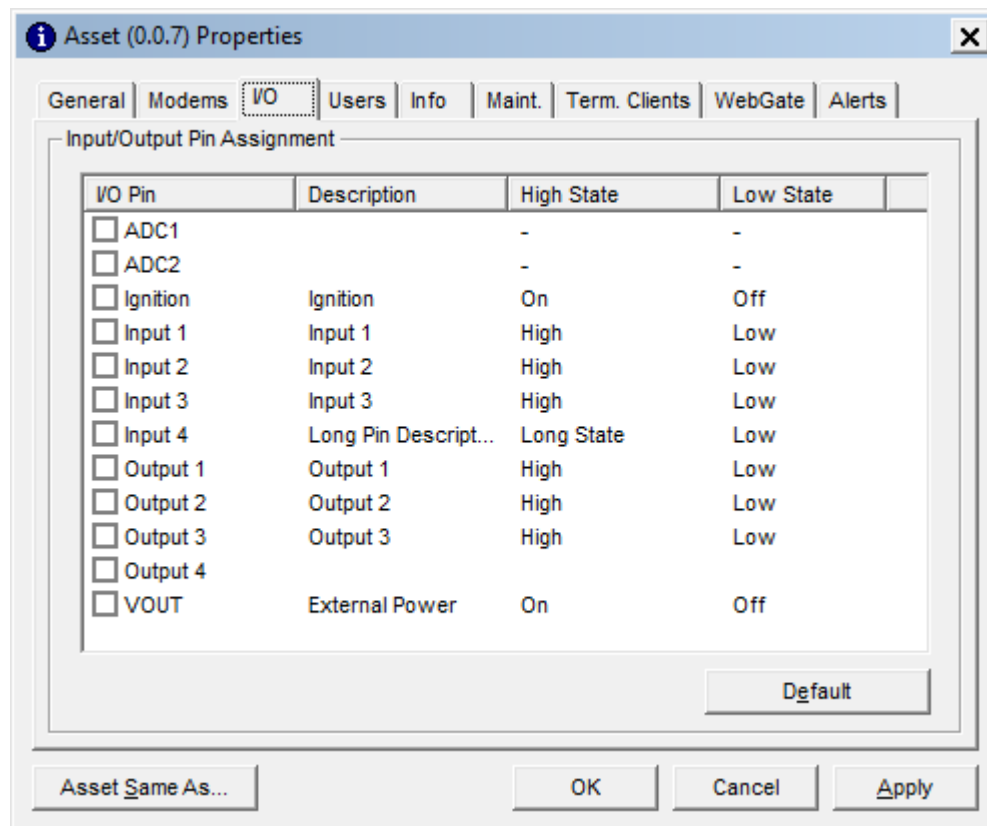
Figure 71 – Asset I/O Properties

Each pin can be enabled or disabled by clicking the checkbox next to the pin name. Double-click a pin name to edit the pin settings.

9.3.3.1 Digital Pin Properties

Figure 72 shows the Pin Properties window when editing a digital (ON/OFF) pin. This provides the following settings:

Figure 72 – Digital Pin Properties

Pin Description:	The pin will be identified using this name.
High State:	Friendly name for the high (or open) state.
Low State:	Friendly name for the low state.
RGB Value:	Assign an optional icon color to change this asset's icon in WebGate when the input is in the high or low state. Note that the "Custom Color" option under asset web properties must be enabled for these settings to take effect. See section 18.1.1 for details about setting icon colors.
Msg Triggers:	Control whether pin changes (going high or low) will cause a message to be generated. High priority messages will trigger alerts for Web Clients, and also generate email alerts if enabled.

9.3.3.2 ADC Properties

Figure 73 shows the Properties window for ADC (analog) pins. This provides the following settings:

Figure 73 – ADC Pin Properties

Description:	The pin will be identified using this name.
Units:	This optional text will be added after the value.
Decimal Places:	Enter how many decimal places to include in the value.
Scale Factor:	Factor to multiply the raw value by. Most assets produce raw values representing the mV reading on the input pin.
Offset:	Amount to add to the raw value <u>after</u> the scale factor is applied.
High Priority:	If enabled, any ADC events sent by the asset will generate high priority alerts.

Example:

Description: "Current"
Raw Value: "1234"
Units: "mA"
Decimal Places: "1"
Scale Factor: "0.01"
Offset: "10"

Calculated Value: (1234 * 0.01) + 10 = 22.34

Displayed Value: **Current=22.3 mA**

9.3.3.3 Users

This tab provides a way of assigning each asset to one or more users (see Figure 74). Any assigned client will receive data from this asset, and be able to send data back to the asset (if enabled). Note: this link between user and asset can also be modified in the User Properties window. Use the "Users Same As" button to quickly copy the links from another asset.
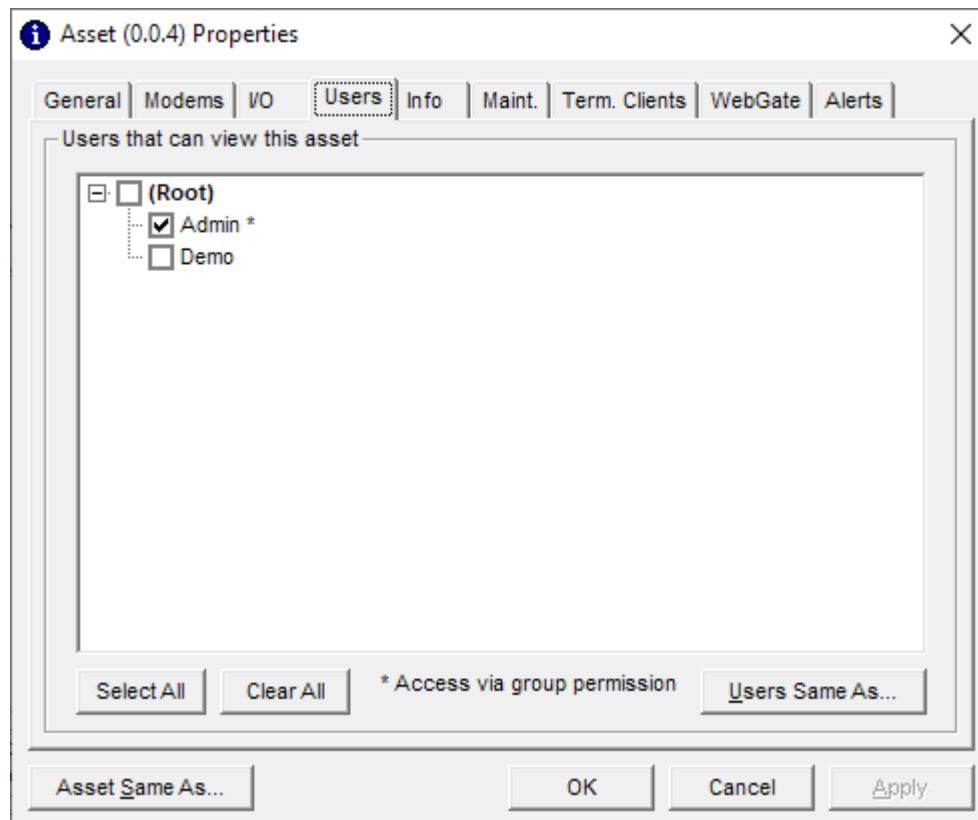
Figure 74 – Asset User Links

Only users belonging to the same group or parent groups of the asset will appear. Click on the group name to quickly toggle all users of that group on or off. Note that users who have been assigned full access to a group will always have access to all assets in that group, and therefore cannot be unchecked in this list.

9.3.4 Asset Info

This page allows extra information to be assigned to each asset.
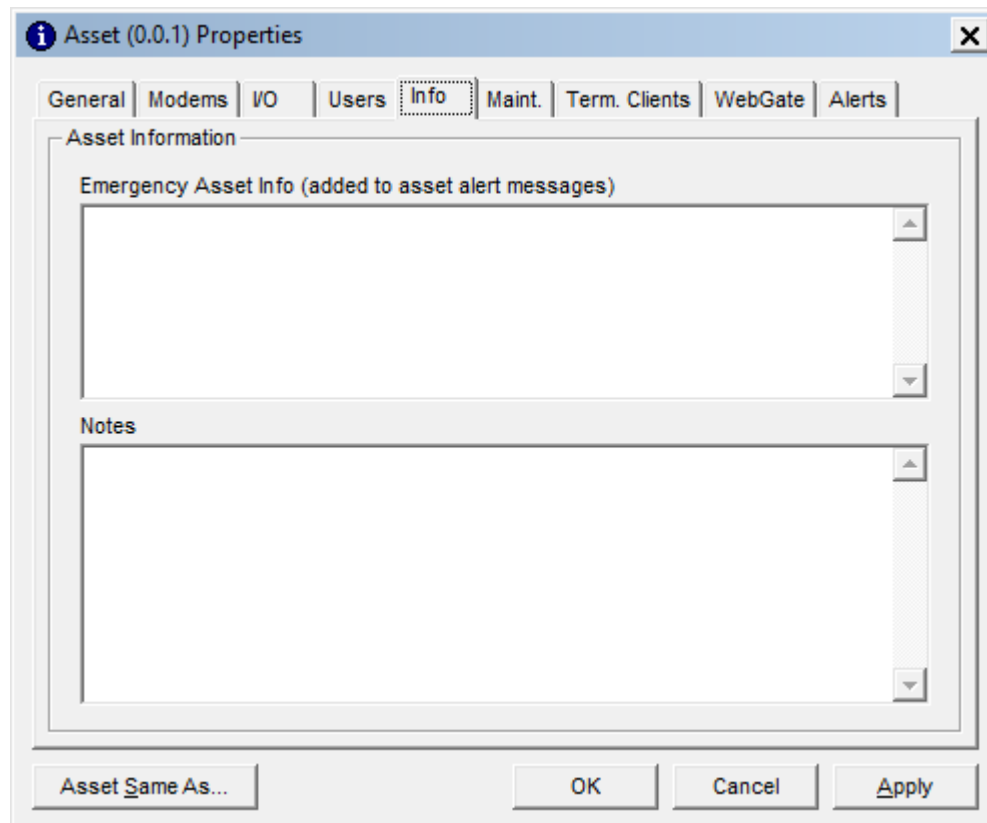
Figure 75 – Asset Emergency Info

Emergency Info: Emergency information can be assigned to each asset. These details will be appended to any alert messages or emails generated by this device.

Notes: Use this field to store any information relating to this asset, such as vehicle details, SIM card IDs, etc. Note that this information will be attached to alerts generated by this asset if enabled under DataGate options. This section can also contain custom message text for SPOT modems, which will be displayed to users when a custom message event is received. Custom messages are defined as CUSTOM=<message>.

9.3.5 Asset Maintenance

The DataGate keeps track of distance travelled and engine hours for each asset. These values are obtained directly from the asset (for devices that transmit this information over the air), or calculated using GPS locations and IGN pin changes.

Click on the "Update" button to manually set the Odometer and Engine Hours values. This is useful if a device is transferred to a new vehicle.

Figure 76 – Asset Maintenance

Click "Add Alert" to add a maintenance reminder. Triggers can be set for one or more of the following parameters: odometer, engine hours, time interval, and can be one-off or repeating alerts.

The Idle Fuel Use value is used to produce idle fuel usage estimates in certain reports.

9.3.6 Terminal Clients

Similar to the Users tab, this tab (Figure 77) links an asset with certain Terminal Clients. Only the selected clients will be able to communicate transparent data with this asset.
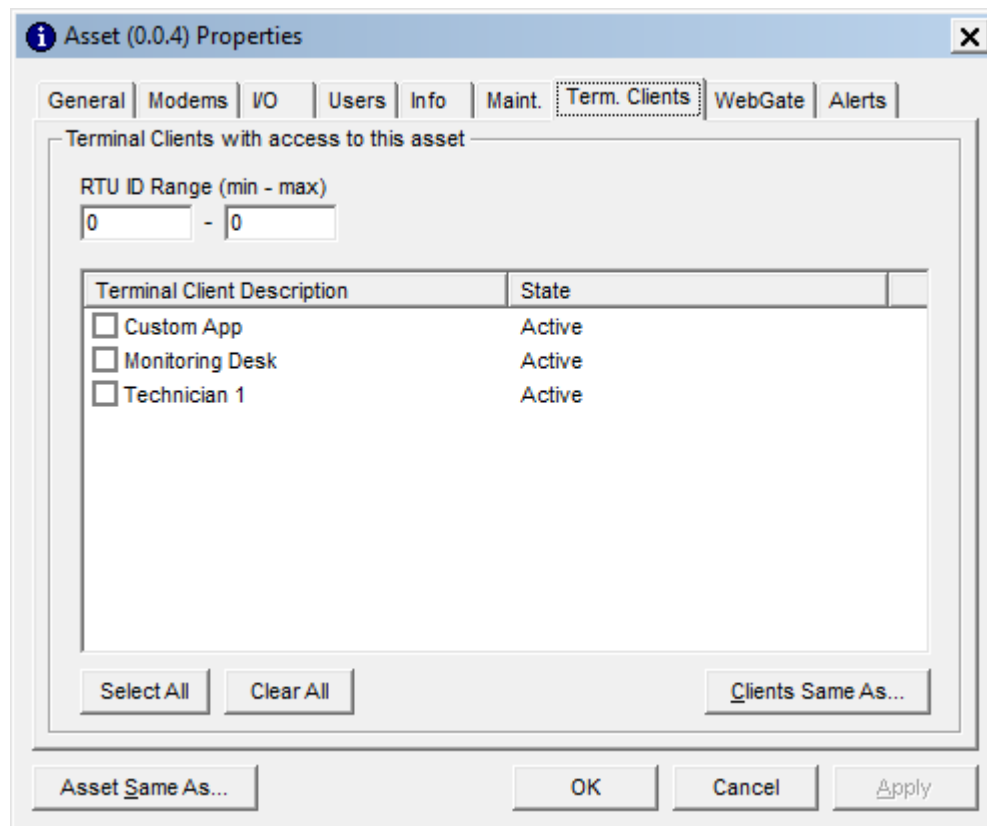
Figure 77 – Asset Terminal Client Links

    RTU ID: ID (or range of IDs) of third-party unit (RTU) attached to transparent port on mobile device. This enables a terminal client to connect to the RTU.

9.3.7 Asset WebGate Settings

This tab (Figure 78) allows you to modify how this asset will appear in WebGate.
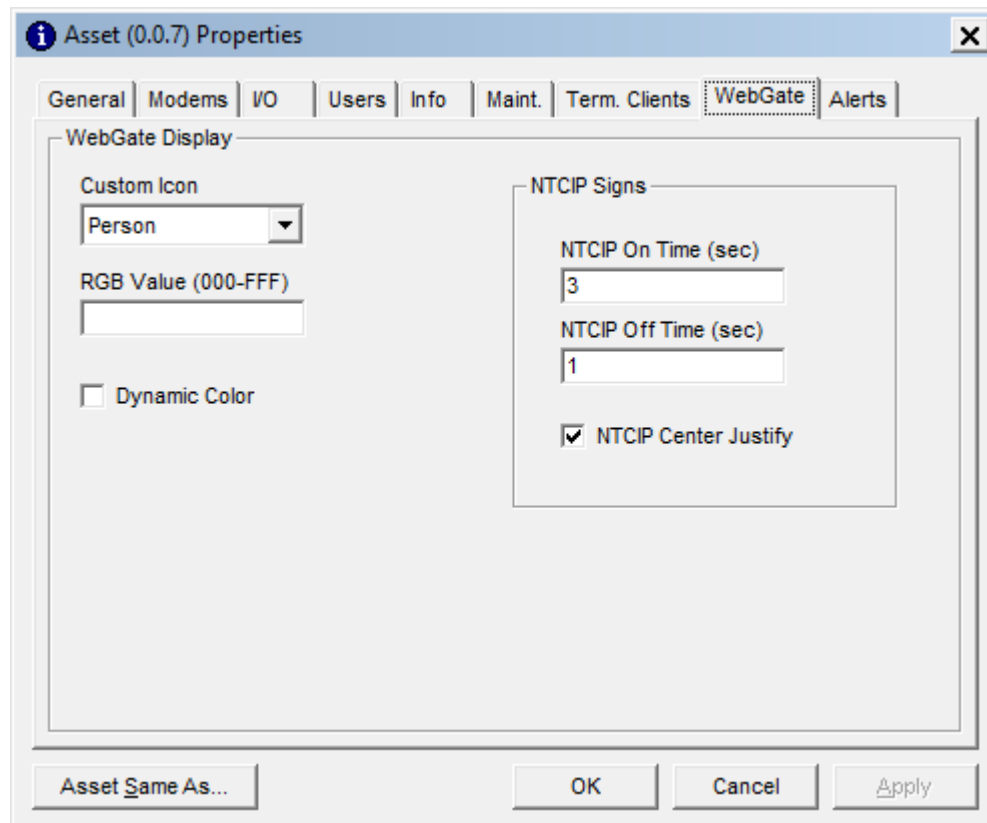
Figure 78 – Asset WebGate Settings

Custom Icon:	The default WebGate asset icons are defined under the main DataGate options. Use this setting to choose a custom icon for this asset.
RGB Value:	Define the asset's default icon color. Leave blank to use the server or group default color. See section 18.1.1 for details.
Dynamic Color:	When selected, the icon color will change based on asset status (Kenwood status values, digital input states and SmartPhone alert status). If not selected, the icon will use the default color.
NTCIP Settings:	For assets attached to NTCIP highway signs, these settings control the default on and off times for displaying multiple pages, as well as horizontal justification.

9.3.8 Asset Alerts

This tab provides access to asset alert settings.

Figure 79 – Asset Alerts

Timeout:	Send alert to users if this asset stops reporting for the set period.
Speed:	Send alert if asset reports a speed exceeding this limit. This option is intended for assets that do not have built-in speed alerts.
Data Warning:	If these values are non-zero, a warning email will be sent when the asset exceeds these usage limits (in bytes for Land/Sat data, and number of messages for SMS). The left-hand values are daily limits, while the right-hand values are monthly limits. Daily and monthly totals are reset at the start of each day or month based on local server time.
Working Hours:	Enter the normal working hours for this asset. If asset motion is detected outside these hours, an alert will be generated.
Time Zone:	Enter a reference time zone and daylight time setting for this asset. This is used to calculate the actual working and alarm hours. If no zone is set, DataGate will default to the local server time zone.
Temperature:	Send alerts if the asset's temperature sensors go out of range. Set the low and high points to the same value to disable the alerts. This option is intended for assets that do not have built-in temperature alerts.
Alarm Hours:	To limit temperature alarms to certain working hours, enter the start and end hours along with the days of the week when alarms are enabled. Temperature alarms occurring outside these hours will be ignored.
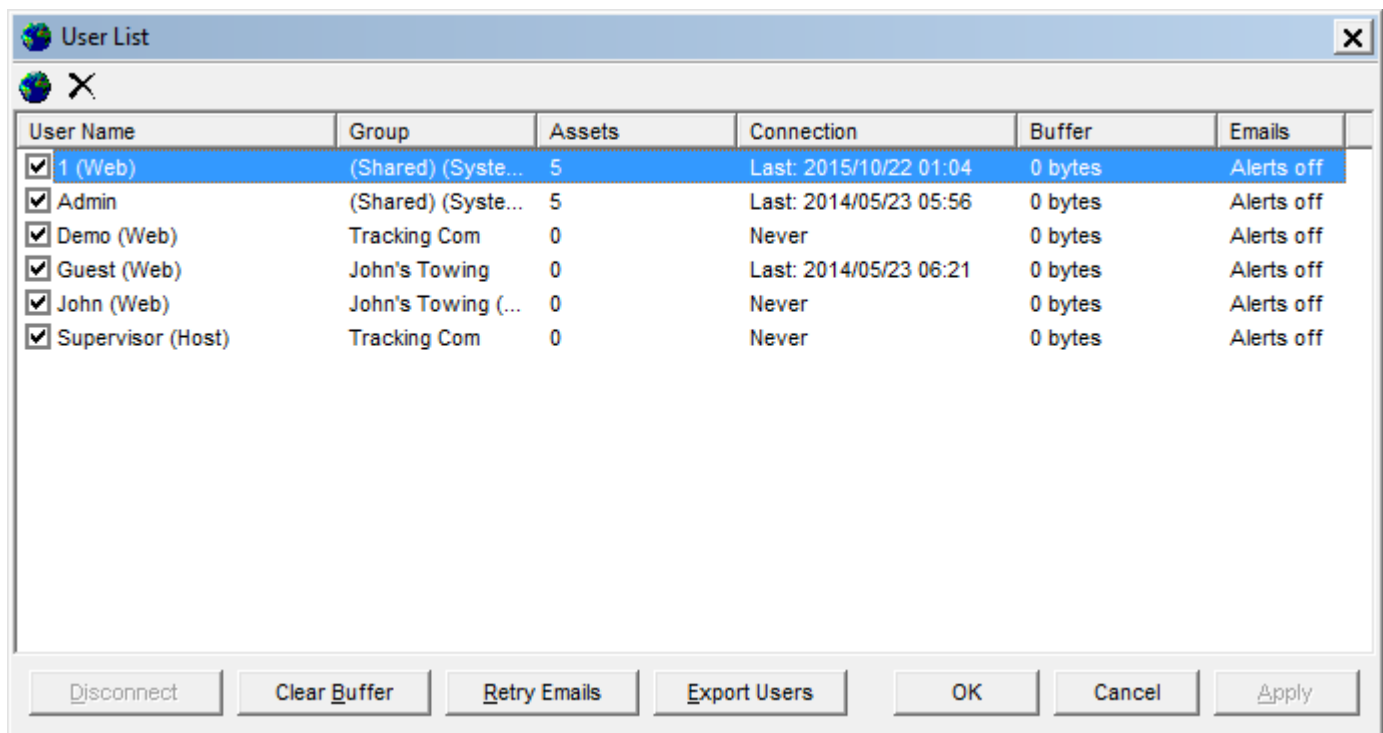
10.0 Users

The User List screen (Figure 80) shows a listing of all DataGate users. Each item shows the user name, group, assets assigned, connection and buffer details, and number of emails in the buffer.

Each user account can be activated or deactivated using the checkbox next to its name.

Users can be configured with or without Web Client access. Web Clients log in to the built-in DataGate web server (WebGate) via a web browser. Web Clients also have access to the KML and CSV listings. See section 18.0 for more information about end-user connections.

User accounts without Web Client access cannot log in to DataGate, but can be configured to receive alerts on the Alerts/Emails tabs. Such users can also be used as groups when parsing pager files (see section 19.1) or receiving group emails (see section 14.3).

User Name	Group	Assets	Connection	Buffer	Emails
☑ 1 (Web)	(Shared) (Syste...	5	Last: 2015/10/22 01:04	0 bytes	Alerts off
☑ Admin	(Shared) (Syste...	5	Last: 2014/05/23 05:56	0 bytes	Alerts off
☑ Demo (Web)	Tracking Com	0	Never	0 bytes	Alerts off
☑ Guest (Web)	John's Towing	0	Last: 2014/05/23 06:21	0 bytes	Alerts off
☑ John (Web)	John's Towing (...	0	Never	0 bytes	Alerts off
☑ Supervisor (Host)	Tracking Com	0	Never	0 bytes	Alerts off

Buttons: Disconnect | Clear Buffer | Retry Emails | Export Users | OK | Cancel | Apply

Figure 80 – User List

Users may be added and deleted using the insert and delete keys, or the buttons on the toolbar.

The following buttons are provided at the bottom of the window:

Disconnect: Force Web Client offline
Retry Emails: Try sending any waiting emails now.
Export Users: Exports the user list to a local file.

10.1 User Properties

Double-click a user in the user list to open the User Properties window. This window is divided into three tabs, listed below. At the bottom of the window is a button labelled "User Same As", which allows the transfer of all User settings (except password) from another user.

10.1.1 Configuration

This tab provides general User settings (see Figure 81).

Figure 81 – User Properties - Configuration

User Name: User name for login and identification.
Group: Set which group this user is assigned to. Note that this can also be defined under the Group Properties screen. See section 7.0 for more information about groups.
New Password: Enter text here to change a user's password. This is always case sensitive. Passwords are stored encrypted on the server. The maximum password length is 16 characters.

Force Change:	Force Web Clients to change their passwords at next login.
Use Active Directory:	If enabled, DataGate will authenticate this user by querying an Active Directory server (configured under Data Storage settings – see section 7.7.1). This option requires the user to log in via a secure HTTP connection. Unsecured HTTP logins are disabled. When AD lookup is enabled for a user, that user's local password is deleted.
Connection Type:	A Web Client can connect via the DataGate web server, and also has access to KML and CSV listings used for Google Earth and mobile phone applications. Users configured without Web Client access cannot log in to DataGate, but can be configured to receive alerts on the Alerts/Emails tabs. Such users can also be used as groups when parsing pager files (see section 19.1) or receiving group emails (see section 14.3).
Web Timeout:	If enabled, Web Clients will automatically be logged off after 10 minutes of inactivity. A warning will be shown on their web page to allow them to continue the connection. When this option is disabled, user sessions stay active as long as the browser is kept open.
Permissions:	Using the web interface, admin users are able to edit the configuration of assets they have access to, as well as user configuration for users in any group they have full access to. Admin and Supervisor users with full access to a top level group can create sub-groups, and are able to assign assets to users in any group they have full access to, as well as move assets and users within those groups. Sys Admin users have full access to all assets and users (even those in the unassigned group), including adding and deleting items. They can also access system logs. **Note that users can only edit other users with lower permission levels**.
LAN Only:	Limits user to logging in from a local (private) IP address.
Geofence Editing:	Allow web clients to edit geofence areas.
History Retrieval:	Enable historical reports for web clients.
Polling:	Allow users to request current asset locations.
Set Outputs:	If enabled, users can set asset output pins remotely.
Send Msgs:	Allow users to send messages to assets.
Remote Ctrl:	If active, users have the ability to send commands and modify asset settings.
Maintenance:	Allow users to edit maintenance alerts.
Asset Name Changing:	Allow users to remotely change asset names. This will affect the name shown to all users with access to this asset.
Hot Pursuit Mode:	Web clients can activate a hot pursuit mode, which automatically polls the asset every 10 seconds for 5 minutes.
Cancel Alarms:	If enabled, users can cancel asset alarms.
Set Driver:	When enabled, users can assign drivers to assets.

10.1.2 Assets

Use this tab to select which assets will be visible to this user (see Figure 82). Note: this link between User and asset can also be modified in the Asset Properties window. Selecting a group name toggles access to all assets in that group. When a group name is selected, this user will automatically get access to any new assets assigned to that group. **Admin and Supervisor users will also be able to view/edit other user accounts in any group for which the group name is selected. This includes creating and editing sub-groups and drivers belonging to these groups, and editing asset/user/driver assignments. Admin users can also edit user configuration.**
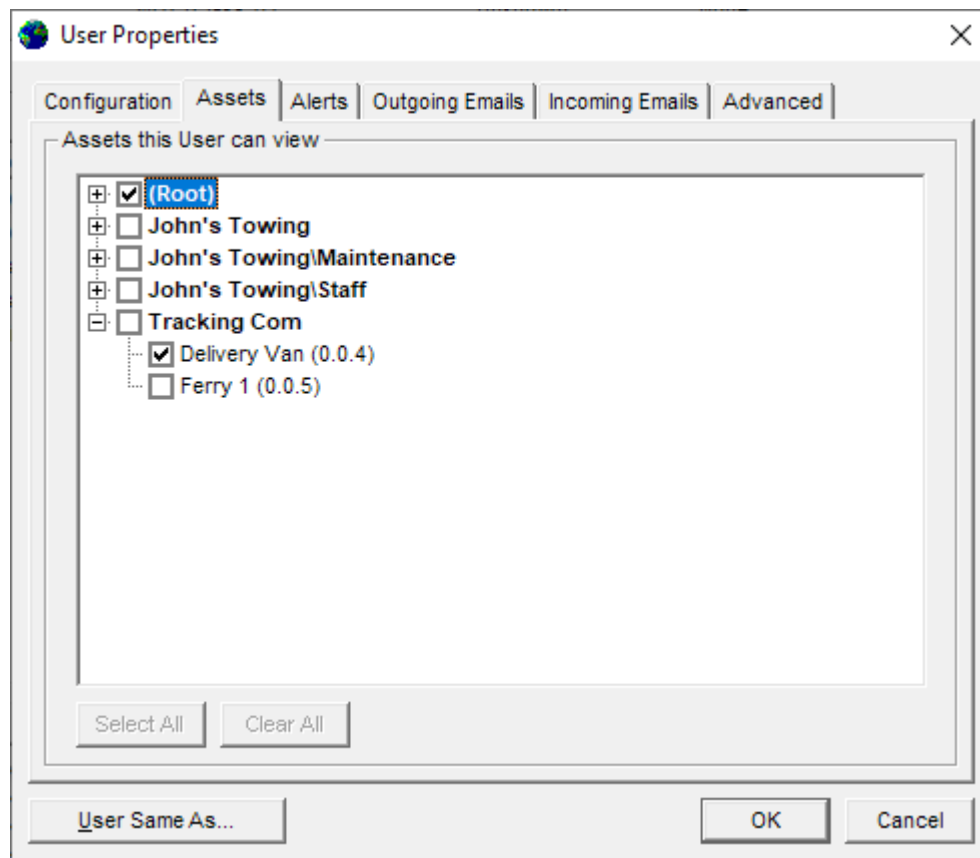
Figure 82 – User Properties - Assets

Select All: Quickly select all assets.
Clear All: Remove all check marks.

Only assets in the users group or sub-groups will appear here.

10.1.3 Alerts

The Alerts tab controls which events this user will be notified about (see Figure 83). Alerts can be displayed in WebGate (see below) or sent as emails. See section 10.1.4 for user email settings.
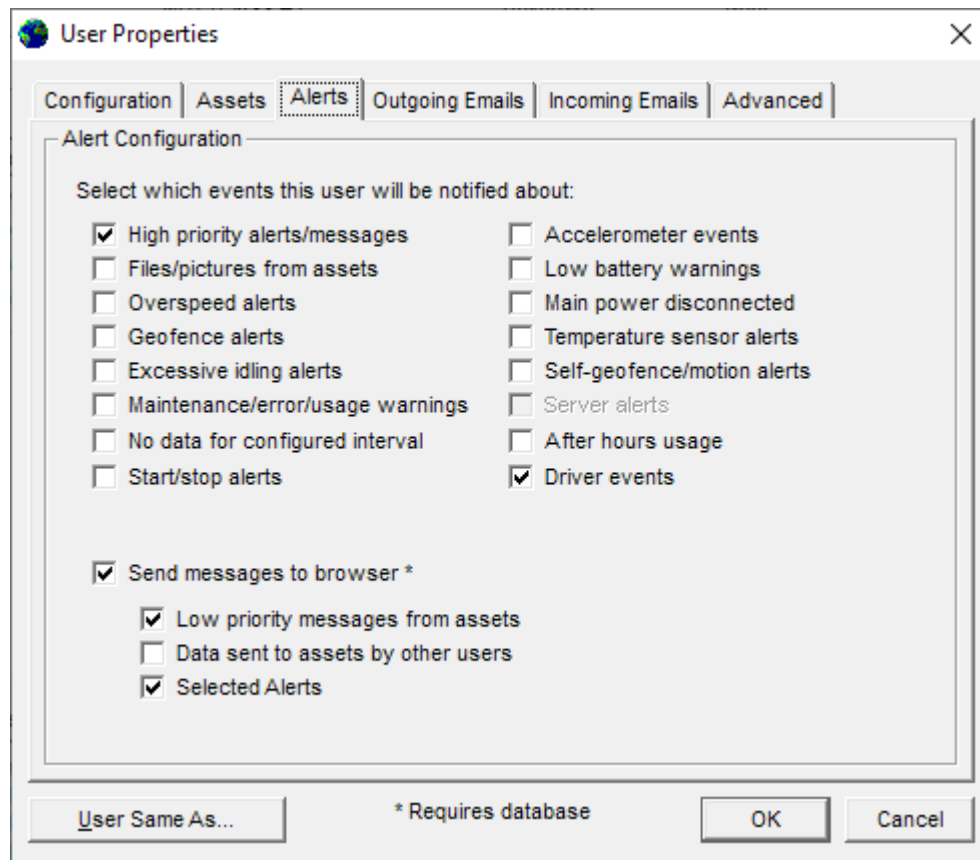
Figure 83 – User Properties - Alerts

Alerts can be generated upon the following triggers:

High priority:	These include high-priority input changes and geofence crossings, pager/emergency alerts from assets, and engine monitoring alerts.
Files/pictures:	Any files or camera pictures received from assets will be sent as an attachment.
Overspeed:	Occurs when assets send a high speed warning.
Geofence:	Includes waypoint reports from assets, and low priority geofence crossings.
Excessive idling:	Sent by assets when engine running with no movement.
Maintenance:	Includes maintenance alerts, error indications from assets, and asset usage warnings.
No data:	Alerts can be generated when an asset stops reporting for a specified period (as set under Asset Properties).
Start/Stop:	Generate alerts when assets send start and stop reports.
Accelerometer:	Heavy braking, fast acceleration, hard cornering and tilt angle alerts.
Low battery:	Alerts occur when assets report low battery conditions.
Main power:	Generate an alert when main power is removed from an asset.
Temperature:	Send alerts when temperature sensor reports high or low values.

Self-geofence: Includes self-geofence and tow alerts (motion with ignition off).
Server alerts: Generates alerts when server error or alert logs are generated.
After hours: Alerts are generated if an asset moves outside of its programmed work hours.
Driver events: Includes driver logging events.

Use the options at the bottom of the window to enable messages and alerts in WebGate:

Show messages panel: Enable this option to display the messages panel for this user in WebGate. Note that the panel is automatically hidden if there are no messages to display. If no other display options are enabled, the panel will only show packets sent to assets by this user. If not using a database for primary storage, the messages panel will be limited to showing outgoing packets.
Messages from assets: Show all messages from assets in the browser.
Data sent to assets: Show messages and remote commands sent to assets by other users.
Selected alerts: Include all alerts selected at the top of this window.

10.1.4 Outgoing Emails

To enable email alerts for this user, enter one or more email addresses, then select the types of messages to be sent. Buttons are provided to send a test email and clear any waiting emails. The checkbox next to each email address defines whether it is active. Inactive addresses will not be sent any alerts, but will still be used for the sender white-listing feature (see section 14.3).

Note: if an address is entered without an '@' character or domain, it will be treated as an SMS destination and sent to the SMS gateway configured under DataGate settings (if enabled). SMS emails are automatically formatted in a shortened format to fit within a 160 character limit.

Adding an asterisk (*) to the end of an email address will cause DataGate to send emails in the shortened format used for SMS addresses. This is useful if using an email to SMS gateway.

See section 14.5 for information about using the built-in POP3 server. A button is provided to clear POP3 emails for this user.

Figure 84 – User Properties – Outgoing Emails

Selected alerts:	Send emails when any of the alerts selected on the Alerts tab occur.
Low priority messages:	Generate emails for low priority messages from assets.
GPS positions:	All incoming GPS reports will be sent as an email containing a NMEA GPS string.
Data sent to assets:	Send emails when messages or commands are sent to an asset.
Send daily reports:	Emails a daily summary and/or trip report to the user.

Forward Simplex data: If the DataGate license permits, DataGate can forward incoming Simplex data to this email address.

Stopped Speed/Time: Settings used for generating daily trip reports.

The user's time zone is shown at the bottom of the window. This zone is automatically set when the user logs in, and is used to format email timestamps to the user's local time.

Note: enabling the "Low priority", "GPS reports" or "Data sent" options may generate a large volume of messages.

10.1.5 Incoming Emails

DataGate can check external email accounts and download messages. These messages will be processed in the same way as emails sent directly to DataGate, and sent out to matching assets.
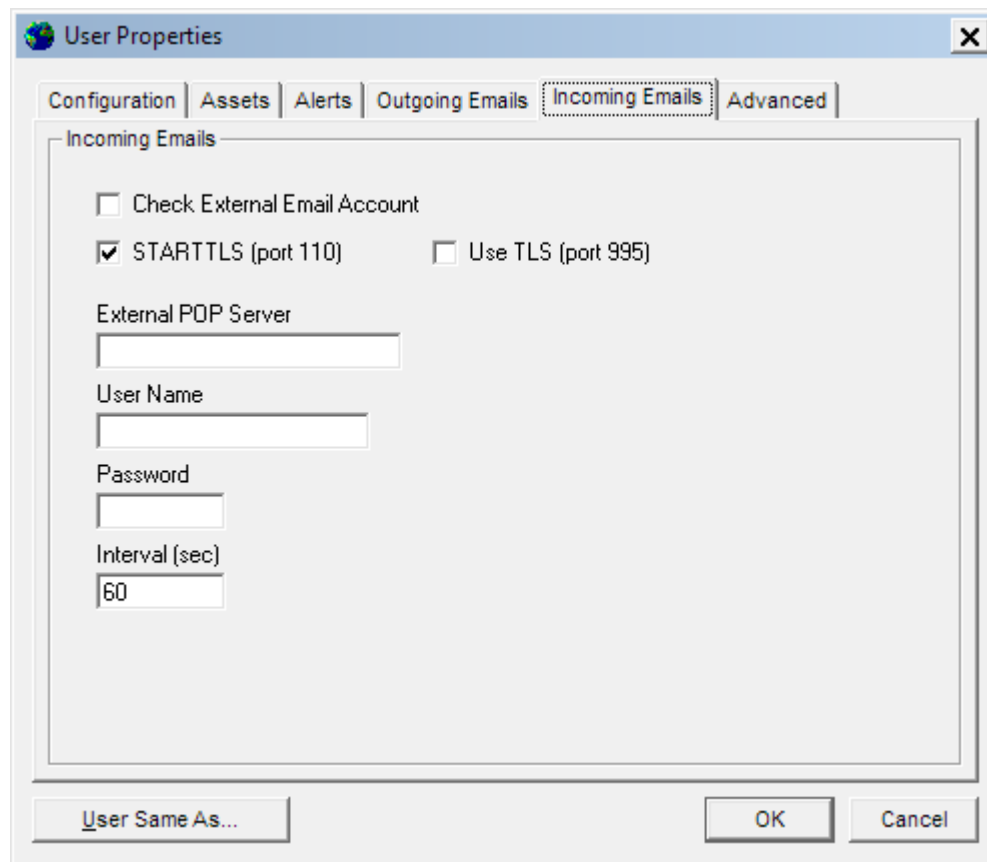
Figure 85 – User Properties – Incoming Emails

Check External Email:	Check an external email account for email messages.
STARTTLS:	Upgrade to TLS when checking emails.
TLS:	Use TLS to connect to a secure port.
External POP Server:	Address of external POP server.
User Name:	User name to log in as.
Password:	User password.
Interval:	Interval for checking emails.

10.1.6 Advanced

The Advanced tab contains settings for a browser custom link and display options (see Figure 86). The browser custom link is shown on the WebGate user menu when this user logs in. This link is hidden if either the Link Name or URL settings are blank.

Figure 86 – User Properties - Advanced

Link Name:	Enter the name of the link to appear on the WebGate user menu. When a user selects this link, the custom URL will open in a new page. Setting the link name to "FleetNet" will hide the URL, which is recommended for FleetNet hours of service links.
URL:	This sets the destination for the custom link. For best results, enter the fully qualified name starting with http:\\ or https:\\.
Options:	For web clients, set how speed, distance and degree values are displayed.
Hide asset trails:	Hide asset trails for this particular user.
Public Web Page:	If enabled, this user's assets are available via a public web page. Use the "Generate Page" button to create a unique page ID, or enter a 32 hexadecimal (0-9 and A-F) character string. The public page uses a simplified layout, showing basic information only.

11.0 Terminal Clients

The Terminal Client List screen (Figure 87) shows a listing of all configured Terminal Clients. Each client has a name, and various connection related details. A client connects to the DataGate using a TCP/IP connection, and can then transmit and receive raw data to and from selected assets. A Client can be activated or deactivated using the checkbox next to its name.
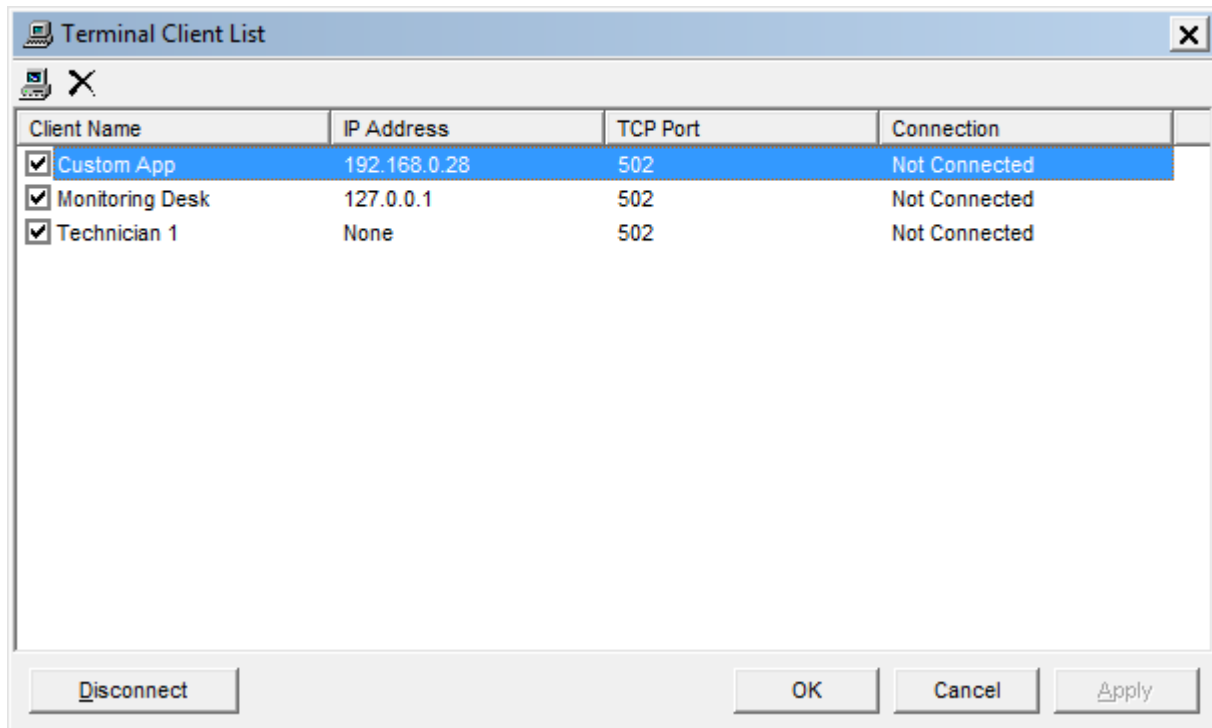
Figure 87 – Terminal Client List

Terminal Clients may be added and deleted using the insert and delete keys, or the buttons on the toolbar.

A Disconnect button is provided at the bottom of the window to force a client offline.

11.1 Terminal Client Properties

Double-click a Terminal Client in the client list to open the Terminal Client Properties window. This window is divided into several tabs, listed below. At the bottom of the window is a button labelled "Client Same As", which allows the transfer of all Terminal Client settings from another client.

11.1.1 Connection

This tab controls how the client connects to the DataGate (see Figure 88).

Figure 88 – Terminal Client Properties - Connection

Client Name:	A "friendly" name for this client.
IP Address:	IP address from where client connects. The DataGate will only allow this client to connect from this IP addresses.
Local Port:	TCP/IP port to which this client connects.
Dynamic IP:	If active, the client must first log in to the DataGate web interface to update his/her IP address.
User Name:	Name used to log in to the web interface.
Password:	Password for web interface.
Connect to Client:	If data is received from an asset while the client is disconnected, DataGate can attempt to connect to the client using the remote port setting.
Buffer Packets:	If active, DataGate will buffer packets and retry if necessary. In most cases it is better to uncheck this option and let the client control retries.
Timeout:	How long to leave connection open if no data is transmitted or received.

11.1.2 Routing

The Routing tab controls how data is routed to and from assets (see Figure 89).
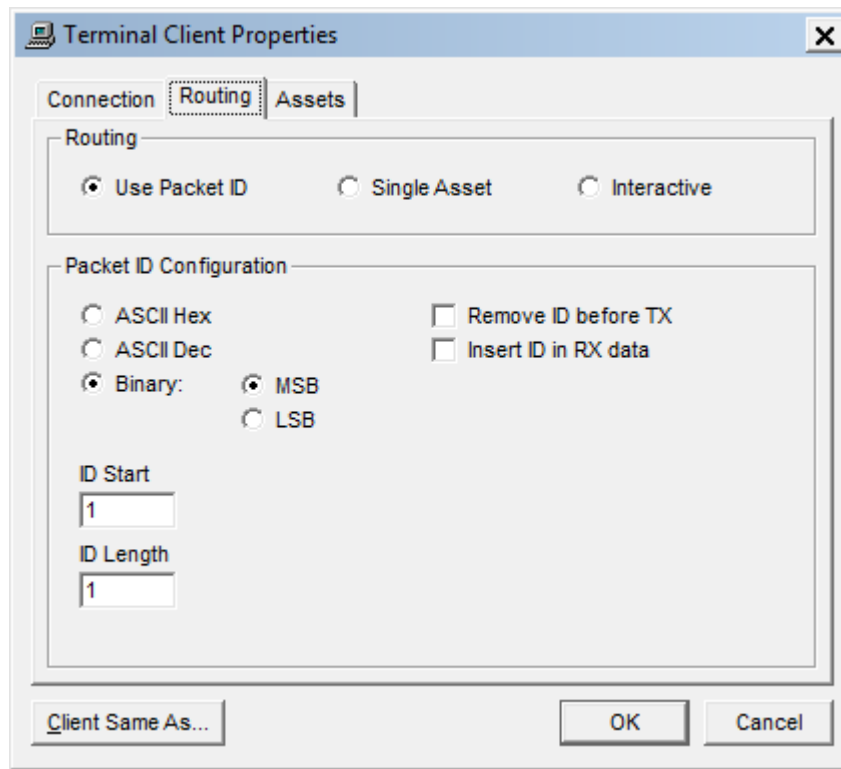
Figure 89 – Terminal Client Properties – Routing

There are three main options:

Use Packet ID: DataGate looks inside the data packets, and decodes an ID. This ID is then matched with the RTU ID of an asset.
Single Asset: The client only connects to one asset.
Interactive: The DataGate prompts the client for an RTU ID upon connection. This ID is then matched as above.

When using the Packet ID option, the following settings are available:

ASCII Hex: ID is encoded as a hexadecimal ASCII string, e.g. "F01B".
ASCII Dec: ID is a decimal ASCII string, e.g. "1052".
Binary: ID is a binary number. Data can be stored with most or least significant byte first.
Remove ID: This removes the ID from the packet before sending the data to the asset.
Insert ID: An ID is added to data from an asset before it is sent to the client.
ID Start: Position of first ID byte in packet (first byte is position 1).
ID Length: Length of ID in number of bytes.

11.1.3 Assets

Use this tab to select which assets will be accessible by this Terminal Client (see Figure 90). Note: this link between Client and asset can also be modified in the Asset Properties window.
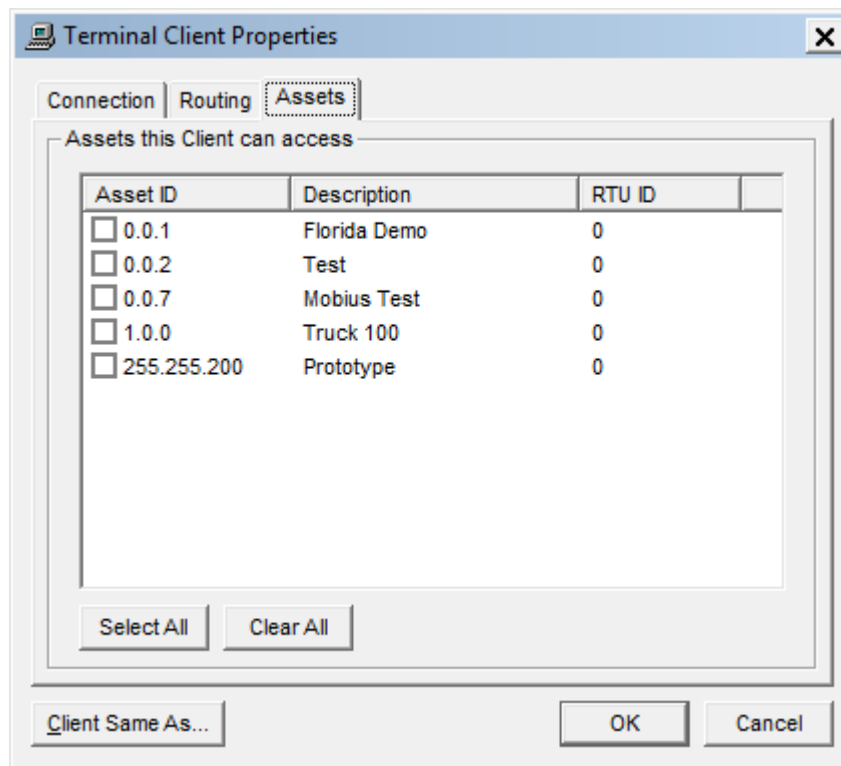
Figure 90 – Terminal Client Properties - Assets

Select All: Quickly select all assets.
Clear All: Remove all check marks.

Note: when using the Single Asset method of routing, you may only select one asset from this list.

12.0 Data Sources

The Data Sources window (Figure 91) shows a listing of all available data sources. Data sources are required for networks that cannot send data directly to DataGate, require some extra processing, or allow multiple sources. Other networks, such as Iridium and GPRS, use IP or email addresses for communication, so assets can connect directly to DataGate without a source set up.
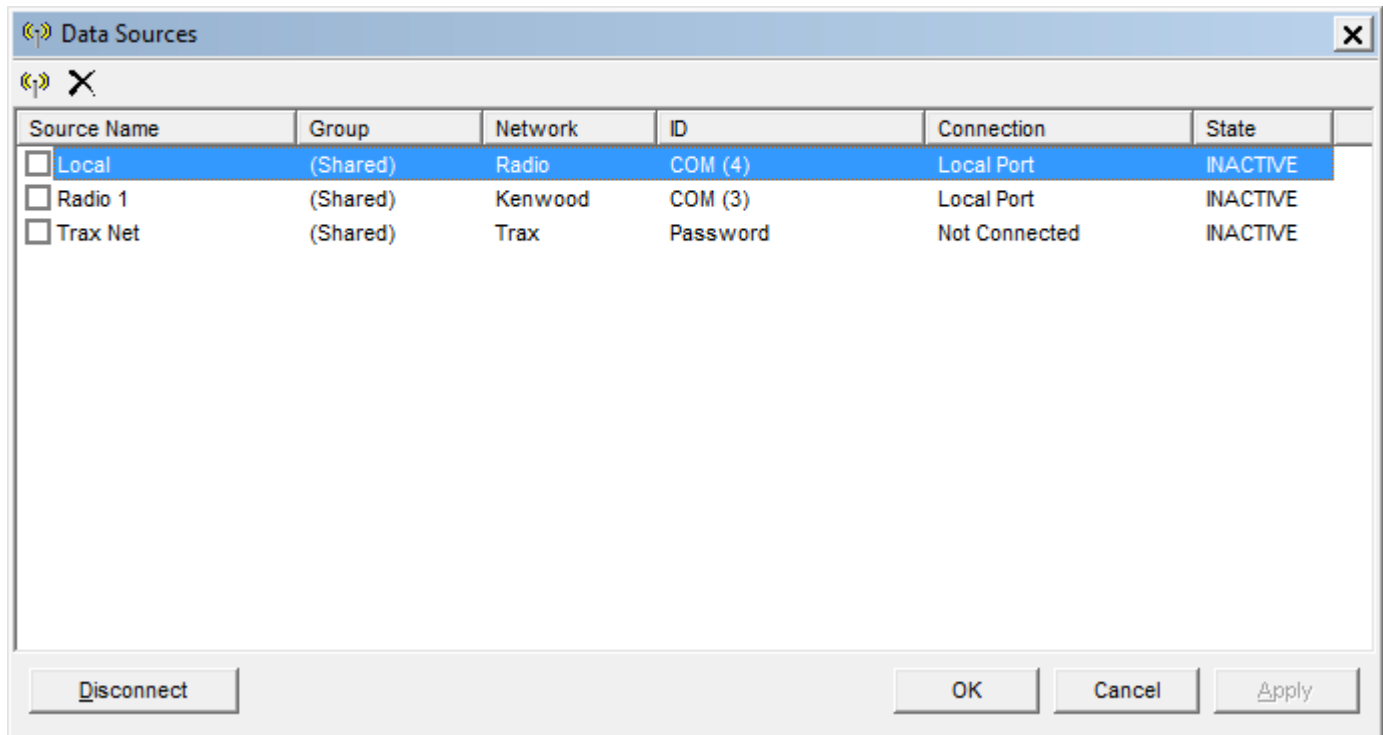
Figure 91 – Data Sources

Sources may be added and deleted using the insert and delete keys, or the buttons on the toolbar. To edit a source's settings, double-click it on the list to open the properties window (Figure 92).
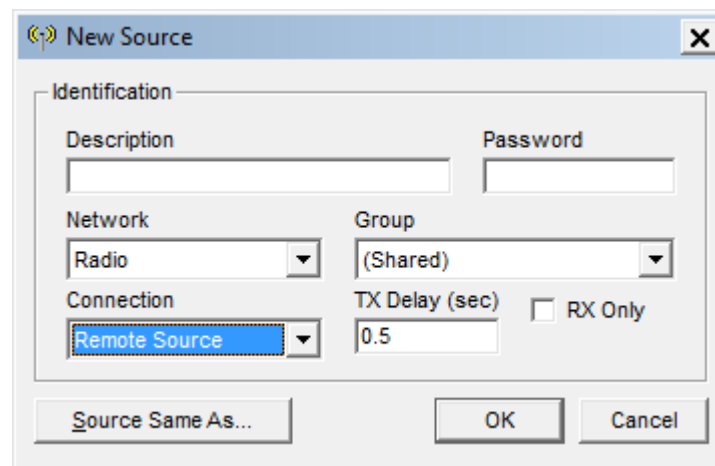
Figure 92 – Source Properties

Each source is configured with some or all of the following settings:

Description: Name for this source.

Password: Remote sources use a password when connecting to DataGate.

Network: Network type. Identifies the network this source is connecting to.

Group: Each source can be assigned to a DataGate group. If assigned to a group other than (All), the source will only be used by assets in that group.

Connection: Defines how this source connects to DataGate. Most sources are limited to "Remote Source" connections, where an external program connects via a TCP connection using a password for authentication. These external source programs are available for download from Datalink Systems. Radio and Kenwood sources have other options – see below.

ACK Delay: Certain RF networks have an ACK Delay setting, where DataGate will delay sending data to the network after receiving data. Set this delay high enough that the remote radio has time to switch back to receive mode before the DataGate sends data. It is also used as a delay for Kenwood Console connections between long data message attempts.

RX Only: RF networks can be configured for RX Only operation. In this mode, DataGate will accept incoming data from the source, but will not attempt to transmit.

Debug: RF network connections support a debug mode, where all incoming and outgoing data is written to the DataGate log.

Note: multiple sources can be configured for each network type. This allows DataGate to communicate with several separate networks or channels at once.

12.1 Radio Connections

Radio networks, including Kenwood, ICOM and Hytera, support other source connection types:

1) Local COM Port. DataGate can connect directly to a local COM port to communicate with a base radio.
2) Serial to Ethernet. In this case, the base radio can connect directly to DataGate via a serial to Ethernet adapter. This may eliminate the need for a standalone PC at the base radio.
3) IP Console (Kenwood NXDN only). DataGate connects directly to a repeater as a console.
4) Radio via USB (Hytera only). DataGate connects to a base radio over USB.
5) Repeater (Hytera only). Hytera repeater connects directly to DataGate over IP.

Note that these connection options are only available if using files for primary storage, or database version >= 3.

12.1.1 Local COM Port Connections

The Local COM properties screen is shown in Figure 93. In this mode, DataGate can connect directly to a base radio attached to one of the server's COM ports. Enter the desired port number and COM settings to match those programmed into the radio.

Figure 93 – Local COM Port

12.1.2 Serial to Ethernet Connections

Figure 94 shows the Serial to Ethernet properties screen.

Figure 94 – Direct IP

This mode requires the use of a serial to Ethernet box to connect the radio's COM port to DataGate. The Source Properties should be set as follows:

1) Under the remote IP address setting, enter the IP address of the serial to Ethernet box, assuming it has a static IP address. If the adapter is running behind a firewall/router, this address will be the router address. Using a static address provides security, as DataGate will only accept connections from that address. If the box has a dynamic address, enter * to allow connections from any address.
2) Choose a local TCP port that the device will connect to. The combination of remote IP address and port should be unique, allowing DataGate to distinguish between sources connecting from the same address. Note that a port can only be used once if the remote address is set to *.

The serial to Ethernet box should be configured as follows:

1) Set the box to act as a TCP client (it will make an active connection to the server). Enter the IP address of the DataGate server, and use the TCP port assigned under the source settings.
2) Set the box to connect on power on.
3) Configure the serial settings to match the base radio. This is normally 9600,N,8,2 for Kenwood networks, but may have been modified in the base radio settings.

12.1.3 ICOM/Kenwood/Hytera Settings

When using a connection option other than "Remote Source" with ICOM/Kenwood/Hytera networks, the source properties screen includes Status Message programming (see Figure 95).

Figure 95 – Kenwood Status Message Programming

Status messages sent from mobile radios are received as a numeric code. DataGate can translate these codes into text using a lookup table. For example, Status ID 1 might be assigned "Job complete". Status codes can also be hard-coded as IGN on/off or PWR on/off events.

High priority status messages will be treated as alerts. Each status also has an optional color code. See section 18.1.1 for details about setting icon colors.

The Status Timeout interval is used to prevent duplicate status messages being generated when the same code is received within this time period.

For Kenwood Local COM Port and Serial to Ethernet connections, the properties screen also has an option for the Kenwood PC Interface Version (1 or 2), which must match the setting in the radio.

Note that when using a Kenwood source with connection type set to "Remote Source", the status messages and status timeout settings are set within the remote source program.

Figure 96 – Kenwood IP Console

When using IP Console mode (Figure 96), various options are available to configure the connection to the repeater.

Repeater IP Address:	IP address of the Kenwood NXDN repeater or gateway.
Remote UDP Port:	UDP port that repeater is listening on.
Local IP Address:	Local address to use when sending and receiving messages. A drop-down box provides any local addresses detected by DataGate. This address will be used when the radio network sends data to the server, so it must be visible to the repeaters.
Auto:	If the local IP address changes, DataGate will automatically select the closest match. This will help if a VPN connection is being assigned a dynamic IP address.
Local UDP Port:	Port used to receive data. Each IP Console source must have a unique local UDP port to allow simultaneous connections. Be aware that ports in the range 50000-56000 can be used by some DNS server software.
RAN:	RAN code for conventional networks.
System ID:	System ID of trunking network.
Site ID:	Site ID of trunking network.
Console SUID:	The console subscriber ID DataGate will connect as.
Conventional:	Select conventional, as opposed to a trunking network.
Regional:	Indicates whether this system is configured as a regional trunking system.
Very narrow band:	Channel bandwidth.
Encyption Keys:	Encryption keys used to unscramble data. Up to 64 keys can be defined.

Figure 97 – Hytera Sources

When setting up Hytera sources (Figure 97), the following settings are required:

Radio/Repeater IP Address: For repeater connections, this should be the IP address of the repeater, as seen by DataGate. For USB connections, use the base radio's radio-to-radio IP address, such as 10.0.0.1.

Local IP Address: For repeaters, select the local network address you wish to listen on. For USB connections, select the local IP address of the base radio connection, such as 192.168.10.2.

Repeater ID: For repeaters, enter the repeater ID to use as a source address when sending data to mobile radios.

12.2 Inmarsat Settings

DataGate can connect directly to a Skywave Inmarsat gateway to send and receive IsatM2M data. Multiple sources can be configured, allowing separate control station IDs to be used.

Figure 98 – Inmarsat Source
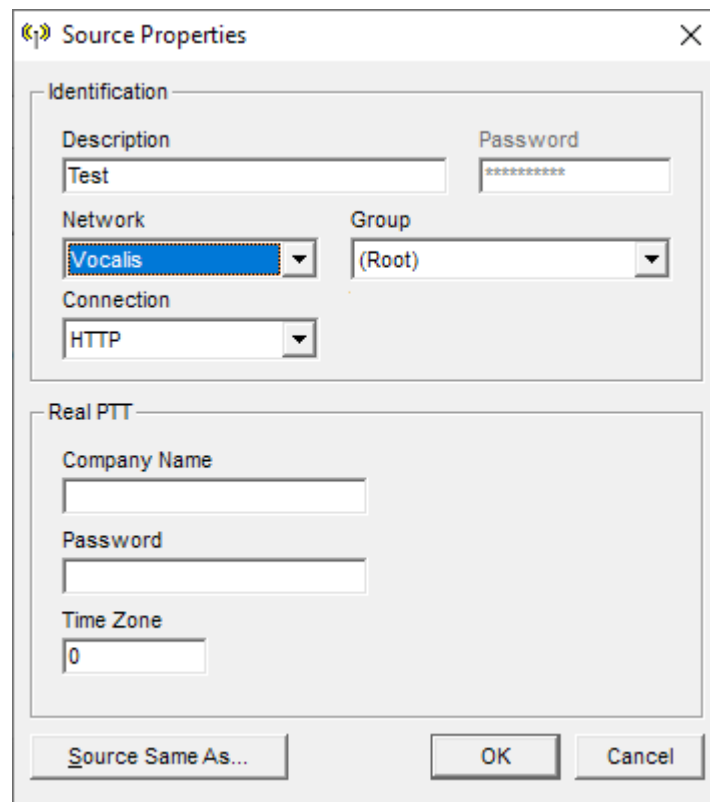
Control Station ID:	This ID is used when logging in to the IsatM2M server.
Password:	Code used when logging in to IsatM2M.
Server URL:	URL of the IsatM2M server. Both HTTP and HTTPS connections are supported. Enter the full URL, including port (such as https://example.com:5102/xml/dapi-xml1)

12.3 Vocalis GPS API

Figure 99 – Real PTT Source Options

Company Name: Company name defined in the Vocalis portal.
Password: GPS API password assigned to this company account.
Time Zone: Time zone (hours relative to GMT) used by the Vocalis server.

13.0 Pager/Driver Details

The Pager/Driver Details window (Figure 100) shows a listing of pager devices and driver names.

Pagers may be two-way Sentry devices or one-way T-PASS units designed for lone-worker security. Each pager has a unique ID, and is normally assigned to a particular worker. This window allows the system operator to assign "friendly" names (such as the worker's name) to each ID. These names will be attached to incoming messages from the Sentry devices, providing end-users with additional information.

The list of drivers is used when assigning drivers to assets via WebGate (if the user has been assigned the "Set Driver" permission). This list is also used when displaying each asset's current driver on the WebGate screen. Certain asset types allow drivers to log in via a terminal. DataGate will use the driver list to match driver IDs to driver names.
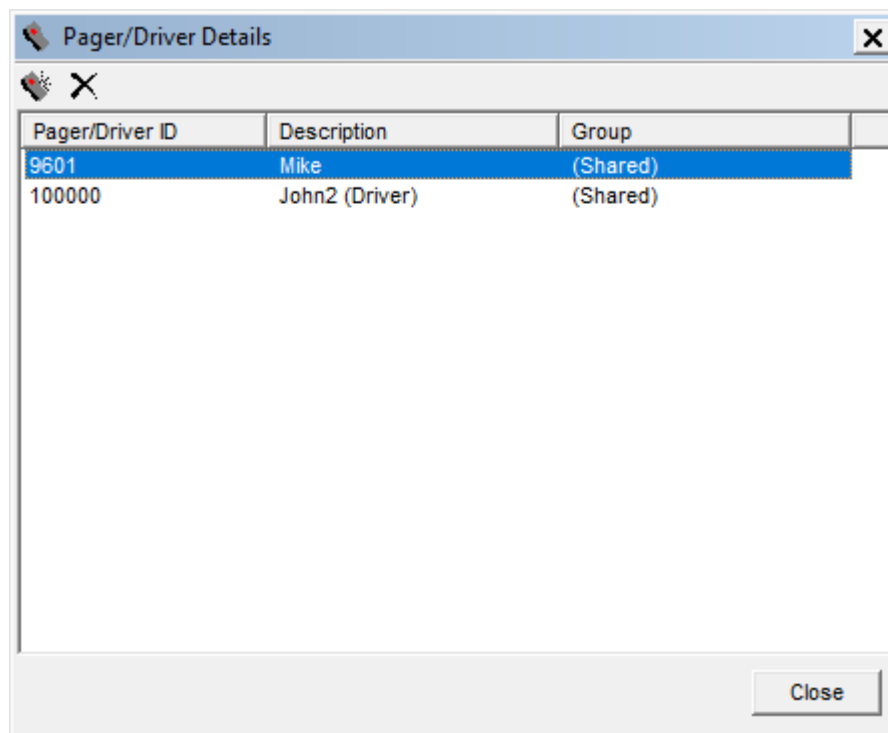
Figure 100 – Pager Details

Items may be added and deleted using the insert and delete keys, or the buttons on the toolbar.

Note that pagers and drivers can be assigned to groups. This allows each customer/department to keep their information private.

Select an item from the list to modify its settings. Figure 101 shows the Pager/Driver Properties screen.

Figure 101 – Pager/Driver Properties

ID:	This value identifies the pager or driver. For pagers, this is the ID assigned to the device. For drivers, the ID uniquely identifies that person, and can be used as a log in code.
Description:	Friendly name to be shown to users.
Pager/Driver:	Select whether this is a pager or driver entry.
Group:	Assign this record to a specific group. Only users with access to this group will be able to edit this record.
iButton/Tag ID:	Certain assets allow drivers to log in using an iButton or RFID tag. Use this field to assign an iButton or Tag ID to a driver.
Driver's Email Address:	Enter an optional email address for this driver. When set, users can send messages to the driver from the WebGate screen. These messages are forwarded by DataGate to the driver's email address.
Copy messages:	When checked, the driver will be sent emails when messages are sent to any asset which the driver is logged in to.
Info:	Add any extra information about this pager/driver. This information will be included in pager alert messages.

14.0 Email Settings

In order for DataGate to send emails directly, or to receive emails (Enterprise version), there are a few extra configuration steps:

1) Assign a fully qualified domain name to the DataGate server, such as datagate.example.com. The DNS record for this domain name should point to the server's IP address. For example, `datagate.example.com A 192.168.0.1`.
2) The reverse DNS record for the server's IP address should point to the domain name used in step one. For example, `1.0.168.192.in-addr.arpa PTR datagate.example.com`. This can normally be modified by a request to your ISP.
3) Create a new (or choose an existing) domain name that will be used to send/receive email, e.g. example.com. DataGate will use this domain to construct email addresses.
4) Assign an MX record to this email domain. This record must point to the DataGate domain name. For example, `example.com MX datagate.example.com`. This means that any email for example.com will be processed by the DataGate machine. This step may be skipped if the email domain name matches the DataGate domain.
5) Create an SPF DNS record to indicate which server is allowed to send email for this domain. The "a" and "mx" values will normally match the DataGate domain name. For example, `v=spf1 mx a:datagate.example.org mx:datagate.example.com -all`.
6) Create a DMARC DNS record to enforce server IP address checks and message header alignment. This record should be assigned to host "_dmarc" at your domain. For example, `_dmarc.example.com`. The record itself contains the DMARC version, policy, and address for sending reports. For example, `v=DMARC1; p=none; rua=mailto:reports@example.com`. Start with policy set to none to check messages are being delivered OK. Switch to a policy of quarantine or reject once message delivery has been confirmed.
7) On the Configuration tab of DataGate's General options, enter the host name from step 1.
8) On the Outgoing tab of Email options, select "Send Directly".
9) Make sure the "Email From Address" uses the mail domain from step 3. For example, noreply@example.com.

If you want DataGate to receive emails (Enterprise version), then the following steps should also be taken:

10) Enable the "Accept Emails" option on the Incoming Email tab.
11) On the General Email tab, set the "Domain Name(s)" settings to match any domain names or IP addresses you want to accept email for. This should include the domain from step 3. For example, example.com. Emails addressed to any other domains will be rejected.
12) DataGate will always accept email addressed to its From address or to the postmaster account. These emails are forwarded to the admin email address.

14.1 Asset Emails (Enterprise Edition)

The Enterprise version of DataGate allows emails to be sent to and from assets with DataGate acting as an email gateway. To enable this functionality, the server must first be configured to send and receive emails as shown in the previous section.

Asset email addresses are automatically generated for each asset that has the "Accept Emails" option enabled (set under Asset Properties). This address consists of the asset description (if valid as an email address) or Asset ID (in dotted or decimal format). For example:

Asset ID	Description	Email Address
0.0.1	truck100	truck100@example.com or 0.0.1@example.com or 1@example.com
0.0.2	truck<200>	0.0.2@example.com or 2@example.com

In this example the second asset description is not valid as an email address as it contains <> characters. In this case the asset ID must be used.

14.2 Valid Email Addresses

In order for a description to be valid for use in an email address, it should adhere to the following rules:

- Must not contain two periods in a row (..)
- Must not start or end with a period (.)
- Must not contain unprintable characters
- Must not contain any of the following characters: " ( ) , : < > @ [\ ]

DataGate will also reject emails to addresses that are valid for multiple assets. For example:

Asset ID	Description	Email Address
0.0.1	100	100@example.com or 0.0.1@example.com or 1@example.com
0.0.100	Service 1	0.0.100@example.com or 100@example.com
0.0.101	0.0.1	0.0.1@example.com or 0.0.101@example.com or 101@example.com

In this case, the addresses 100@example.com and 0.0.1@example.com can apply to multiple assets, and will therefore be rejected. It is recommended to limit the use of asset descriptions that match asset ID formats.

14.3 Group Emails

In order to send a single email to multiple assets, DataGate can accept emails to special alias addresses representing groups of assets. This alias uses a special address: usergroup.name@example.com, replacing "name" with the description of a DataGate user account.

For example:

User Description	User Group Email Address
Admin	usergroup.admin@example.com

Note that the user description must be valid for inclusion in an email address.

When DataGate receives such emails, it will forward the message to ALL assets the named user has access to, providing the assets can accept messages and have the "Accept Email" option enabled.

14.4 Email Address White-Listing

When the "Only allow emails from user addresses" option is enabled under the Incoming Email settings screen, emails to assets will only be accepted if the email "From Address" or credentials used to send email match an address defined for one of the DataGate users assigned to that asset. This reduces the possibility of spam email being sent over the network. If emails need to be sent from an unlisted address, the address will first need to be added to one of the users under the User Properties screen.

For group emails, the "From Address" or credentials must match an address defined for the named user account.

Alternatively, incoming emails can be filtered by IP address, which is useful if all valid emails will always be sent from a known list of servers.

14.5 POP3 Server (Enterprise Edition)

DataGate (Enterprise) has a built-in POP3 server that can be enabled under email options. When turned on, an internal email address is created for each user. This address will consist of the user name '@' DataGate's email domain name. For example, user "Admin" on a server whose email domain is "example.com" will be assigned an email address admin@example.com. Entering this address under the user's email settings will cause alerts to be buffered in DataGate's database. The user can then use a standard email client to connect to DataGate and download the messages.

Users should configure their email clients with the following account settings:

Account Type: POP3
Incoming Server: IP address or domain name of the DataGate server
User Name: the user's WebGate name
Password: the user's WebGate password
Connection Security: use STARTTLS if enabled in DataGate
Authentication: encrypted password (plain password also supported over TLS)
Leave messages on server: ideally disabled, or set for a few days

These internal accounts can also be used when sending messages to assets. By setting the "From Address" to this internal account, any replies from the asset will be buffered internally.

15.0 Secure Web/Email Connections

DataGate supports secure web and email connections using the TLS standard.

Incoming web connections support TLS 1.2, with RSA key exchange, AES 128/256 encryption, and SHA1/SHA256 hashing.

Email and outgoing web connections support TLS 1.0, with RSA key exchange, AES 128/256 encryption, and SHA1 hashing.

Web browsers and email servers not supporting these cipher suites will be unable to establish an encrypted connection.

These secure connections require a private key and public certificate, which can be obtained from a trusted authority (see next section). For testing, DataGate will generate its own key and self-signed certificate upon install, which will allow secure communications but will cause a certificate warning message to display when users access the web page.

A new self-signed certificate and key can be generated by DataGate at any time using the button on the TLS Keys window, accessible from the View/Options/Web/Ports menu. This will overwrite any existing key and certificates. Remember to update your certificates if changing the address of the server.

15.1 OpenSSL

We recommend using the OpenSSL toolkit to generate keys and certificate requests, or to convert certificate file formats. This toolkit is available on the Internet as a free download. Links to setup distribution files can be found at https://wiki.openssl.org/index.php/Binaries. We have tested with Windows binaries from https://slproweb.com/products/Win32OpenSSL.html.

Download and install OpenSSL files to an easily accessible folder such as c:\openssl.

15.2 Creating a Certificate Request

Once OpenSSL is installed, create a folder to store your configuration and key files, such as c:\openssl\keys.

Run openssl.exe in the c:\openssl\bin folder to load an OpenSSL command prompt.

Now, issue the following command:

```
req –new –nodes –keyout c:\openssl\keys\private.pem –out c:\openssl\keys\server.csr
 –newkey rsa:2048
```

You will be prompted to enter the details to appear on the certificate. Note: set the common name field to the exact fully qualified domain name that will be used to access your server, e.g. datagate.example.com.

During this process an RSA private key will be generated and saved in the private.pem file. This example produces a 2048 bit key, but longer keys can also be created. To enable the key to be imported, it is created without password protection (-nodes option).

Note: keep the private key file secure, as the server security depends on this key remaining secret. After importing the key into DataGate, It is recommended to encrypt and back up the key, then delete the key file.

The resulting server.csr file contains the Certificate Signing Request that can be sent to a signing authority (do not send the private.pem file!). The authority will respond with a public certificate containing the server's public key. They may also send intermediate certificates to form a chain back to a trusted root certificate.

15.3 Converting Existing Certificates

If you already have a certificate available, this can be exported into .pem format, which can then be imported into DataGate.

If the certificate is installed in Windows, load the Certificate Manager from a command prompt:

```
certmgr.msc
```

Right-click on the certificate you want to export, and then click on All Tasks/Export to open the Certificate Export Wizard. You will need to export the private key too, which requires entering a password to protect the key file. Save the file to disk in PKCS #12 format, using a folder such as c:\openssl\keys. In the example below, the certificate is saved as cert.pfx.

Run openssl.exe and enter the following commands to convert the .pfx file to .pem format:

```
pkcs12 –in c:\openssl\keys\cert.pfx –out c:\openssl\keys\key.pem –nodes -nocerts
pkcs12 –in c:\openssl\keys\cert.pfx –out c:\openssl\keys\cert.pem -nokeys
```

When prompted, enter the password used when creating the .pfx file. These commands give you two files: key.pem containing the private key, and cert.pem containing the public certificate.

15.4 Intermediate Certificates

Intermediate certificates are used to identify signing authorities when a chain of authorities have been used. There certificates may be supplied as individual .pem files, or as a single .p7b file (in the example below, as chain.p7b), which can be converted using openssl.exe as follows:

```
pkcs7 -in c:\openssl\keys\chain.p7b -out c:\openssl\keys\chain.pem -print_certs
```

This creates a file named chain.pem, containing all the certificates in the chain. Each certificate will start with `-----BEGIN CERTIFICATE-----`, and end with `-----END CERTIFICATE-----`.

Use a text file editor such as Wordpad to combine your public certificate and chained certificates into one file. Note that the order is important. The first certificate must be the server certificate, followed

by the next authority, and so on until the root certificate is reached. It is not necessary, or recommended, to include the root certificate in this chain.

15.5 Loading Certificates into DataGate

The private key and public certificate (or chain) files can now be imported into DataGate. Use the View/Options/Web/Ports menu to access the TLS Keys screen (see Figure 102), and then import the private key and public certificates. DataGate will encrypt and store the private key internally, after which you should encrypt and backup the raw key file before removing it from the server.
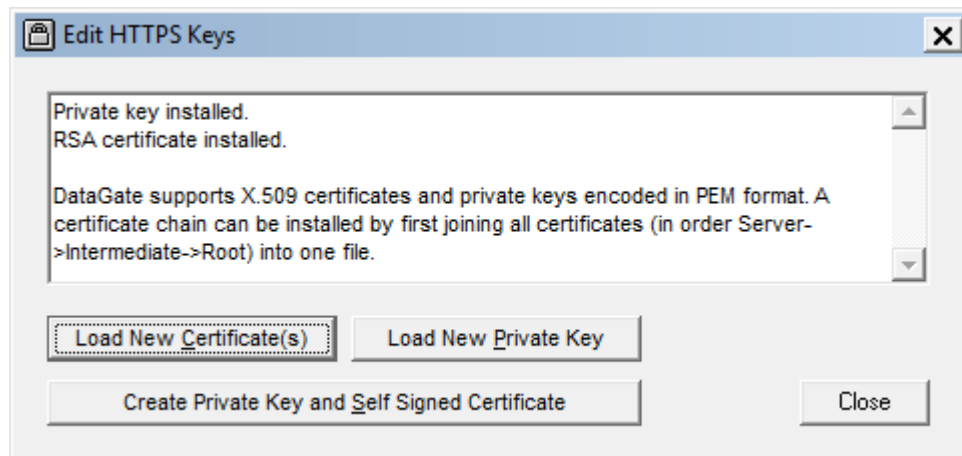
Figure 102 – HTTPS Keys

16.0 Web Server

DataGate has a built-in web server that supports user interaction and asset data transfer. The web interface can be accessed by browsing to the DataGate server address (IP address or domain name) and specifying the port if changed from the default (80), e.g. http://datagate.example.com, or http://datagate.example.com:81 (port changed to 81). If using HTTPS, replace http with https in the address, e.g. https://datagate.example.com.

The following pages are accessible if enabled under Web settings (see section 7.3):

/   Main web page.
Displays mapping login dialog for Web Clients (see section 18.1).
Provides a link to Scada login page for Terminal Client users.
Provides a Blackberry Mobitrac download page for Blackberry devices.

/fleetnet   Users are directed to this page when accessing their FleetNet hours of service link.

/gpsclient MSAT-G2 web service for receiving G2 satellite data. This service only accepts connections from IP addresses listed under the MSAT-G2 options.

/kml   KML listing. Used by Web Clients to download a listing of current asset locations. This can be used as a Network Link in Google Earth, ArcGIS Explorer and other mapping programs. The connection uses HTTP authentication to identify the user.

/list   Comma separated variable (CSV). Web Clients can connect to download a listing of current asset information. This is used by Mobitrac mobile phone applications. The connection uses HTTP authentication to identify the user. See section 16.1 for details.

/rss   GeoRSS feed. Used by Web Clients to access a listing of current asset locations. The connection uses HTTP authentication to identify the user.

/scada   Scada login page. Terminal Clients can log in to update their IP addresses.

/simplex   Globalstar Simplex web service for receiving satellite data (POST). This service only accepts connections from IP addresses listed under the Simplex options. Simplex data can also be sent to the root domain (/).

/spot   Spot web service for receiving Spot satellite data. Only requests using the correct Spot customer and secret tokens will be accepted.

/xml   XML web service allows an external server to request asset locations and send msgs.

/xml?wsdl XML web service definition file

Most user pages require HTTP authentication using password hashing (plain-text passwords are never sent). If further security is required then HTTPS encryption should be enabled.

DataGate also provides an optional public web page available per user. This can be accessed without a login, but requires knowledge of the unique web page address. The page can be set via the User Properties page (see section 0), where a random 32-character hex address is generated. For example, this address might look like:

http://datagate.example.com/d3a7efc041bcfea61d9284ffed886c97

16.1 CSV List Page

This page provides a simple CSV listing showing the current state of a user's assets. Any unknown or unsupported values will be blank. Note that this page will only show the latest information for each asset, and provides no way to access historical data.

The HTTP response will include the following custom headers:

"x-sequence" contains an integer value representing the sequence number of the most recent asset update (such as x-sequence: 123). Note that DataGate resets the sequence number to zero when restarting, and then increments it for each data packet received.

"x-ref" contains an integer value identifying this server instance. This value will change each time the server restarts, and is used to identify when the sequence value has reset.

"x-list" indicates whether the list contains all available assets (x-list: Full) or only updates (x-list: Update).

By default, the server will always return a full list of assets. However, if the x-sequence and x-ref values are included in the query (using "sequence" and "ref" parameters) DataGate will only return data for assets that have changed since that sequence. For example, http://datagate.example.com/list?sequence=123&ref=4589 requests assets that have changed since sequence 123, using reference 4589. If the requested sequence is greater than the current server sequence, or the reference does not match, DataGate will return a full list. DataGate will also return a full list if any assets are added or removed from this user's account.

A "wait" parameter can also be specified, which will cause the server to wait for up to the specified time (in seconds) before sending a response. The response will be sent as soon as any new asset data is available. This enables fast asset update rates without unnecessary http polling. For example, http://datagate.example.com/list?sequence=123&wait=30 will cause the server to wait for up to 30 seconds for new asset data. If no data is available at the end of the wait period, an empty response will be returned. The resolution of the timer is 10 seconds, with a maximum value of 10 minutes. Due to internal timing, the actual wait interval will be 0 to 10 seconds longer than that requested.

Including a "selfID" parameter causes DataGate to exclude asset data for the smartphone asset with a modem ID (normally IMEI/UDID) that matches this parameter. This is useful where an application is acting as an asset as well as a client, as it prevents the client displaying itself on the map.

When data is returned, the response begins with a header line showing the included fields. Newer versions of DataGate may add fields onto the end of this list, but the existing order will not change. The current field list is as follows:

Asset_ID,Description,Last_Report_GMT,Last_GPS_GMT,Latitude,Longitude,Heading,Speed_KPH,Network,GPS_State,Heading_Deg,Altitude_Metres,Motion,Cell_ID,Cell_LAC,RSSI_dBm,Cell_Advance_Metres,IGN,Input_1,Input_2,Input_3,Input_4,Output_1,Output_2,Output_3,Output_4,Sensor_1,Sensor_2,Batt_Percent,Batt_Volts,Temp_C,VOUT,Driver,Odo,Hours,Today_Land,Today_Sat,Today_SMS,This_Total,This_Sat,This_SMS,Last_Total,Last_Sat,Last_SMS,Group,Alert,Site_Number

See Appendix A for a description of these fields.

16.2 Terminal Clients

Simple TCP/IP connections can be used to send and receive transparent data to/from certain assets. See section 11.0 for more information on setting up Terminal Clients.

17.0 Third-Party Interfaces

Third-party software can connect to DataGate to download asset information.

17.1 Database

Historical data will be stored in the DataGate database (if enabled). This can be read by external software for display in other programs. The database also provides support for sending messages and job dispatches to assets. See Appendix D for database details.

17.2 TCP Server

DataGate can be configured to output asset data packets on TCP connections. DataGate acts as a TCP server, and will accept connections on the TCP Server port from programmable IP addresses. Various output formats are available:

17.2.1 Text Output

When using the NMEA, Pipe, CSV and SANAV formats, DataGate will generate lines of text each time an asset reports. This data is buffered until a TCP connection is made, at which time it is sent one line at a time as follows:

<SEQ>;<DATA><CR><LF>

<SEQ> = Alternates between "0" or "1"
<DATA> = Line of text as described in following sections
<CR> = Carriage return (0x0D)
<LF> = Line feed character (0x0A)

The connected client must acknowledge each line of text by responding with:

<SEQ><CR><LF>

Where <SEQ> must match the <SEQ> value sent by the server.

Heartbeat packets must be sent approximately every 10 seconds to keep this TCP connection alive. The heartbeat packet is:

H<CR><LF>

Note that the TCP text buffer is cleared when the server is restarted, and therefore this interface is not recommended where all data needs to be monitored. XML Polling or Push to Web Service may be more suitable in this case.

The following formats for the <DATA> element are available:

17.2.1.1 NMEA

ID=<ID>&RMC=<RMC>,<Battery>,<Network>

<ID> = Asset ID as integer (e.g. 1234)
<RMC> = RMC GPS string (e.g. $RMC...*30)
<Battery> = Battery level as voltage or percentage (e.g. 12.5V or 55%)
<Network> = "Sat" or "Cell"

17.2.1.2 Pipe

?<ID>|<Date>,<Lat>,<Lon>,<Knots>,<Heading>,<Altitude>,<Data>

<ID> = Asset ID
<Date> = Report date (e.g. 2016/07/10 17:30:02)
<Lat><Lon> = Latitude and Longitude in decimal degrees (e.g. -123.12345)
<Knots> = Speed in Knots
<Heading> = Heading in degrees
<Altitude> = Altitude in metres
<Data> = Transparent data received from asset, encoding as hexadecimal (e.g. 414243)

17.2.1.3 CSV
The CSV format outputs data using comma separated variables. Fields containing commas or quotes will be output inside quote characters.

<ID>,<Last_Report_GMT>,<Network>,<Last_GPS_GMT>,<Motion>,<GPS_OK>,<Latitude>,<Longitude>,<Speed_KPH>,<Heading_Deg>,<Altitude_Metres>,<Cell_ID>,<Cell_LAC>,<Cell_RSSI_dBm>,<Input_1>,<Input_2>,<Input_3>,<Input_4>,<Output_1>,<Output_2>,<Output_3>,<Output_4>,<IGN>,<Sensor_1_Hex>,<Sensor_2_Hex>,<Batt_Volts>,<Batt_Percent>,<Temp_C>,<Temp2_C>,<Event_ID>,<Event_Str>,<Priority>,<Msg_ID>,<Trip_ID>,<Trip_State>,<Host_ID>

See Appendix A for a description of these fields. If any fields are unavailable, they will be left empty.

17.2.1.4 SANAV

imei=<IMEI>&RMC=<RMC>,<Battery>,<Network>

<ID> = Asset ID as integer (e.g. 1234)
<RMC> = RMC GPS string (e.g. $RMC...*30)
<Battery> = Battery level as voltage (in millivolts) or percentage (e.g. 3700mv or 55%)
<Network> = "I-POLL" (satellite) or "G-POLL" (cellular)

17.2.2 DataGate XML

With DataGate XML enabled, DataGate provides a web service which can be used by clients to monitor and send messages to assets. This web service is located at the /xml page accessible via the standard DataGate web interface. For example, http://datagate.example.com/xml

DataGate supports two main formats: MultiSpeak and DataGate messages. Both formats use SOAP XML packets transported over HTTP.

17.2.2.1 DataGate XML SOAP Packets

Each request made to DataGate must contain a single SOAP envelope, made up of a header and body. The header must contain a DataGateRequestHeader object, including username and password fields. DataGate searches its user list for a matching user, and then allows the client to access any asset assigned to that user account.

If the request is successful, DataGate will return a SOAP envelope with header and body. A DataGateResponseHeader object will contain version information about the DataGate, as well as sequence and instance values to allow clients to detect new data and server restarts.

The web service description file (.wsdl) can be obtained by adding a "wsdl" parameter to the xml request. For example, http://datagate.example.com/xml?wsdl

Appendix E includes sample XML packets and a description of the various methods and responses.

17.3 Push to Web Service

DataGate can push data to an external web service using HTTP POST packets. Data can be formatted in various ways, depending on customer requirements. The default format uses SOAP XML packets conforming to the schema found at http://www.datalinksystemsinc.com/datagate1.xsd.

Each packet contains a single SOAP envelope, made up of a header and body. The header contains a DataGateHeader object, which holds information about the DataGate server along with programmable username and password fields. The body has an AssetEventNotification object, which contains one or more events and a transaction ID.

Each event holds information about the asset that generated the data, along with various location, network, and telemetry fields. Network and event IDs are the same as those used for other external connections (see Appendix B and Appendix C).

Appendix E includes a sample XML packet.

17.4 Web Connections

Third parties can also use one of the web pages listed in section 16.0 to download live asset information. This is limited to GPS location data, and does not provide historical reporting capabilities.

18.0 End-User Access

18.1 Web Client Interface (WebGate)

DataGate includes several built-in web pages that a Web Client can log in to. This web interface is referred to as the WebGate Tracking System. The WebGate manual is available at http://www.datalinksystemsinc.com/support/webgate.pdf
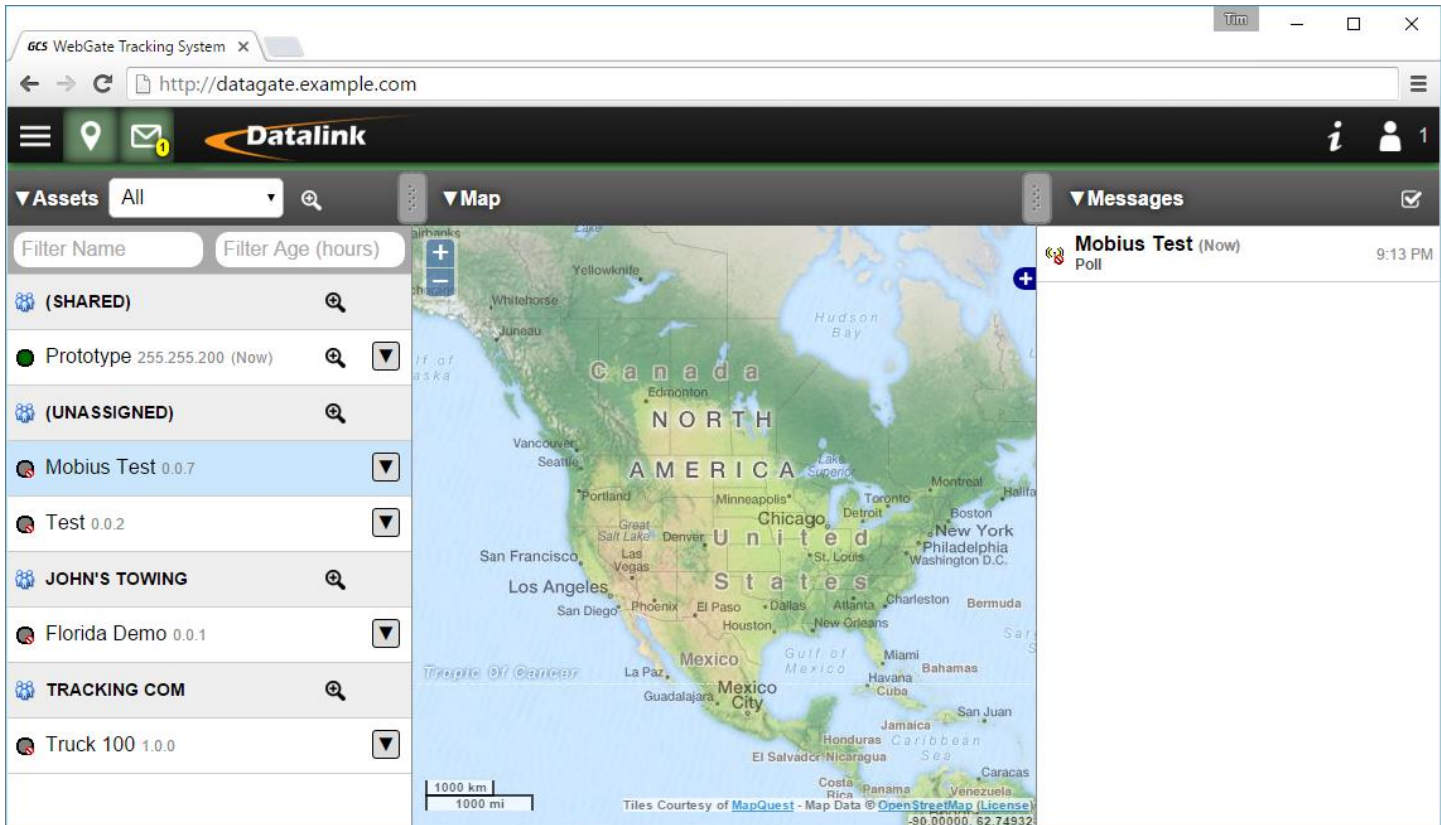
Figure 103 – WebGate Interface

If enabled under DataGate settings, a "Keep me logged in" option is available. When selected, DataGate will keep this user's session in memory, even if the browser is closed or network link is lost. By default, sessions are not saved when the server restarts, but this can be enabled under settings.

If the keep logged in option is disabled or not checked, a user's session will automatically expire if closed for more than 10 minutes. WebGate administrators can also force sessions to close if there is no user activity for 10 minutes. In any case, users can force a session to expire by logging out.

Note that a DataNet Scada Interface link will appear on the main page, if the Scada web link is enabled under web options (see section 7.3.1). This link allows Terminal Clients to set their dynamic IP address.

When viewing this main page on a Blackberry device, a link will be shown for downloading the Mobitrac application. Mobitrac allows users to view asset locations directly on their Blackberry devices, and is also available for iPhone/iPad devices.

Unless disabled under the DataGate Web options, the WebGate page automatically plays sounds when certain events occur. An alert sound is played when high priority messages are received, and a message sound is played for low priority messages. These two sounds can be customized under the web options. If any high priority messages are unread, or the server connection is lost, the web page will beep every minute to warn the user.

18.1.1 Custom Icon Colors

WebGate displays assets using small circular icons by default. The default color of these icons is set under the WebGate options screen (see section 7.3). Colors can also be set based on group assignment (see section 8.2), or by setting a custom color under asset setting (see section 9.3.7).

Icon colors can also be dynamic, based on the most recent status report for Kenwood devices (see section 12.1.3), alarm status for Smartphone apps, or a digital input state (see section 0).

Custom colors are entered as three hexadecimal numbers (0-9 or A-F), representing red, green and blue primary levels, with zero representing the minimum, and F the maximum value. Here are some examples:

000 = Black
F00 = Bright Red
F80 = Bright Orange
FF0 = Bright Yellow
0F0 = Bright Green
00F = Bright Blue
FFF = White
444 = Dark Gray
888 = Medium Gray
CCC = Light Gray

To add more red, increase the first character (up to a maximum of F). To reduce the amount of red, decrease the first value (down to a minimum of 0). Likewise, adjust the green level with the second character, and blue level with the third character.

As of DataGate version 6.2 build 33, two custom colors can be defined by using six characters, where the first three characters represent the first color, and the next three represent the second color. For example, red and blue would be defined as F0000F. Note that if you wish to use black as a second color, it must be entered second. For example, black and white would be defined as FFF000.

When two colors are defined, WebGate will alternate the colors every 0.5 seconds (this rate is customizable in datagate.ini file). One possible use of this feature is to generate red/blue flashing icons when a police car has its warning lights on.

18.2 Tablet/Smartphone Access

WebGate is accessible by most modern browsers, including touch-enabled phones and tablets. The screen layout dynamically changes as the screen size changes. On large screens the asset list, map and messages list can all be displayed at the same time. If space permits, the asset properties box is

also shown. As screen size is reduced, the page will allow only assets or messages to be selected (as well as map). On the smallest screens, the user must select between assets, map, and messages.

18.3 Security Concerns

DataGate can serve web pages via standard (http) or secure (https) connections. Secure connections reduce the chance of malicious users obtaining passwords or session IDs, as well as protecting asset locations and configuration data from eavesdropping.

Non-secure (http) traffic is not protected from eavesdropping. Although passwords are encrypted before transmission, it is possible for a malicious user to obtain session IDs by intercepting http traffic. These sessions IDs could be used to impersonate an existing connection. To prevent this, it is recommended to force all web connections to use secure (https) connections (see section 7.3.2).

With https enabled, it is highly recommended to set up a server certificate (see section 15.0). Without a certificate, users will see a security warning each time they try to connect over an https connection, making it difficult to determine whether they are communicating with the actual server.

When using default settings, WebGate sessions stay active while users' browsers are kept open (and the network link is ok). Sessions expire 10 minutes after a browser is closed, or the network connection is lost. To improve security, a user option is available to force the user's browser to log off after 10 minutes of inactivity (see section 10.1.1 for details on user options).

In any case, sessions expire immediately when a user logs out of WebGate. Users should be instructed to log out whenever they leave their PC accessible to third parties.

For cases where session capture is less likely (such as when DataGate is only accessible via a local network, or connections are forced to use https), a DataGate option allows users to stay logged in, even when their browsers are closed or the network connection drops. In this case, a user's browser will automatically continue the existing session when the network reconnects, or the user resubmits an existing WebGate page. A cookie is also stored in the user's browser to record the session ID, allowing a user to reconnect when opening a new connection to the server. This new connection will trigger a prompt for the user to confirm logging in using the stored session.

The DataGate options control whether this "Keep logged in" option is available on all or only secure (https) connections. Another option allows session IDs to be stored to disk when DataGate is closed. This allows users to reconnect without having to log back in after a server restart.

18.4 Custom Web Logo/Title

The DataGate license has an option to enable customizing the WebGate logo, background and title text. To check whether this feature is enabled for your license, look at the Company entry on the DataGate License screen (see section 6.1), which will show "(Custom)" if enabled. Contact Datalink to discuss pricing.

The custom values can be assigned based on the domain name used to access DataGate, allowing different logos and text for different customers. See section 7.3.5 for settings. Three custom logo formats can be defined:

Logo	Used at the top left of the WebGate screen. Image should have an alpha blended (transparent) background, with a height of at least 40 pixels. This image is placed on top of the blended grey title bar, so it should be designed to be shown with a dark background. Higher resolution images will give better results on high-dpi screens, but could cause problems with older browsers (such as IE6).
Favicon	This icon is displayed in the browser address bar or on browser tabs containing a WebGate page. The file should contain 48x48, 32x32 and 16x16 PNG images. Adding a 256x256 PNG image may be useful if users are pinning the WebGate site to their home screen/desktop.
Touch icon	Used by browsers where a higher resolution icon is required, such as when pinning the web page to the home screen. This icon should be 144x144 pixels. Higher resolutions should also work (although the filename must stay the same), if required in the future.

19.0 Data Files

DataGate settings are stored in a file named "datagate.ini". The location of this file is specified in one of the following registry keys:

HKEY_LOCAL_MACHINE\SOFTWARE\DataNet\DataGate\DataDir (on 32-bit machines)
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\DataNet\DataGate\DataDir (64-bit)

The default location of this file is in the data folder specified during installation (normally \DataGate on the system drive). Older DataGate versions placed this file in the program files directory. If this file cannot be found, default settings will be used.

Data, log, and backup files are stored in user-defined directories, which can be modified from the Options menu. When changing directories, all existing data files (excluding logs and backups) will be copied to the new directory (leaving the old files as a backup). However, if the new directory already contains data files, a prompt will be displayed to either keep or overwrite the existing files.

The following files are written (unless disabled in the options menu):

Log Files: These files contain a record of DataGate activity, including web and email connections. They are written to the Logs folder in the format yyyymmdd.log, http_yyyymmdd.io, and email_yyyymmdd.io, where yyyymmdd is the date in server local time.

Device I/O: A record of raw asset data sent and received. Saved to the Logs folder in the format yyyymmdd.io, where yyyymmdd is the current date in GMT time. The data is unprocessed, allowing network byte counts to be performed. The DataNet Reporter program can be used to extract valuable information from these files. Only written when primary storage is set to Files, or if the option to save logs to files is enabled. Another DataGate option limits these logs to unprocessed data only.

Backup Files: Each time DataGate starts up, and also once per day, it makes a backup of its data files in the Backup folder. The file format is yyyymmddHHMM_prefix_name.dat, where name is the original data file name, yyyymmdd is the local server date, HHMM is the local server time, and the prefix indicates the backup type (Auto or Startup).

Temp Files: DataGate may keep queued database queries and session data in the Data folder using files with a .bak extension.

Data Objects: When DataGate receives files from assets, it saves a copy in the Data folder.

19.1 Pager Message Files

For interfacing with pager message systems, or any software that delivers messages via files, DataGate has a simple file monitoring feature. A certain location (as set under Auxiliary options – see section 7.9) is monitored for new files. This location can be a simple folder name (where all files in the folder will be processed as messages), or may also include a file name or wildcards (where only matching files are processed).

DataGate loads the files and searches for the correct format, as follows:

ID="Name"
ISGROUP="Yes" or "No"
MESSAGE: "Text"

If ISGROUP is set to "No", then DataGate searches its asset list for a description that matches the "Name" field. If a match is found, DataGate constructs a message to that asset, using the "Text" field as the message body.

If ISGROUP is set to "Yes", then DataGate searches its user list for a description that matches the "Name" field. If DataGate finds a match, it constructs a message to each asset that the user has access to, as well as all SMS/email addresses assigned to that user, using the "Text" field as the message body.

If the file format is incorrect or a match cannot be made, no message is generated.

The file is deleted once DataGate has finished processing it.

20.0 SQL Database Reference

20.1 SQL Server Log In

Open the SQL Server Management Studio to access the database server. When the utility starts, you will be prompted to enter the server log in information (see Figure 104). Under Server name, start with a single period to access the local machine, or enter a server name to access another machine. If SQL Server was installed as a named instance, follow the server name with a slash (\) and the instance name. For example, if an instance is named "DATAGATE", then the server name will be ".\DATAGATE".
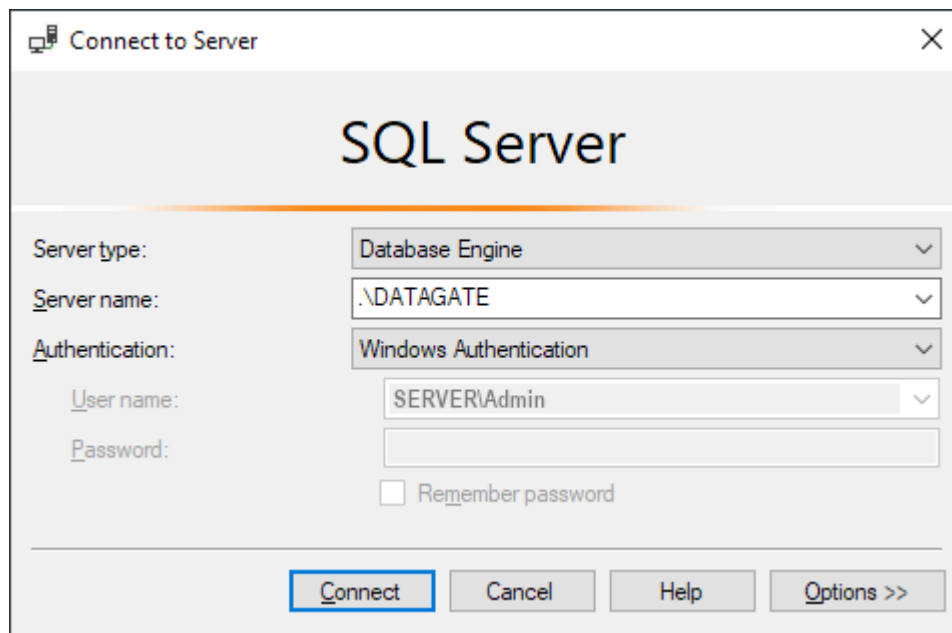
Figure 104 – Logging in to SQL Server

Select Windows Authentication for authentication, which will use the currently logged in user account to provide log in settings.

If using mixed authentication mode, you can enter the system administrator username (sa) and password assigned during installation.

Figure 105 shows the Management Studio window. The Object Explorer panel provides links to various database server properties.

Figure 105 – SQL Server Management Studio

Otherwise, the databases can be set up manually as follows:

To create a new database in SQL Server Management Studio, right-click on Databases in the object explorer and select "New Database". This opens the New Database wizard (see Figure 106).

Enter a database name. For security purposes, it may be beneficial to change the database owner to the "sa" user. By default, the owner will be set to the currently logged in user.

It is recommended to create the DataGate databases through the DataGate GUI (see section 7.7.1).
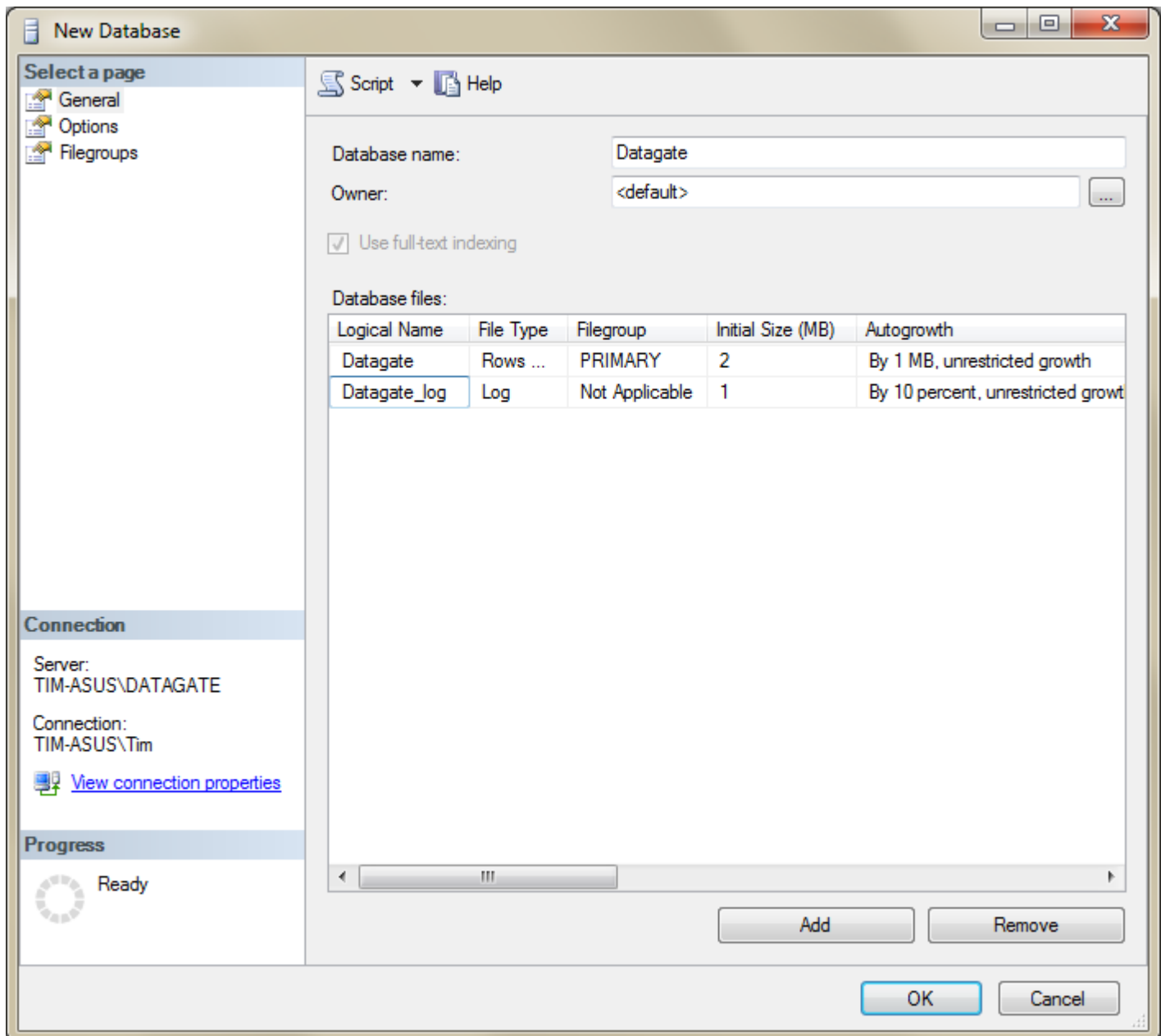
Figure 106 – New SQL Server database

Next, it is optional to go to the options page and change the recovery model to Full. The Full model allows a database to be recovered to a particular point in time, assuming the necessary database backups are available. The Simple model provides increased performance, but restore points will be limited to the previous backup times.

The online SQL Server manuals provide detailed information about these choices.

It is recommended to use a SQL Server Maintenance Plan to back up and maintain the database (requires full version of SQL Server). Otherwise, DataGate provides a simple backup system for the SQL database (see section 7.7).
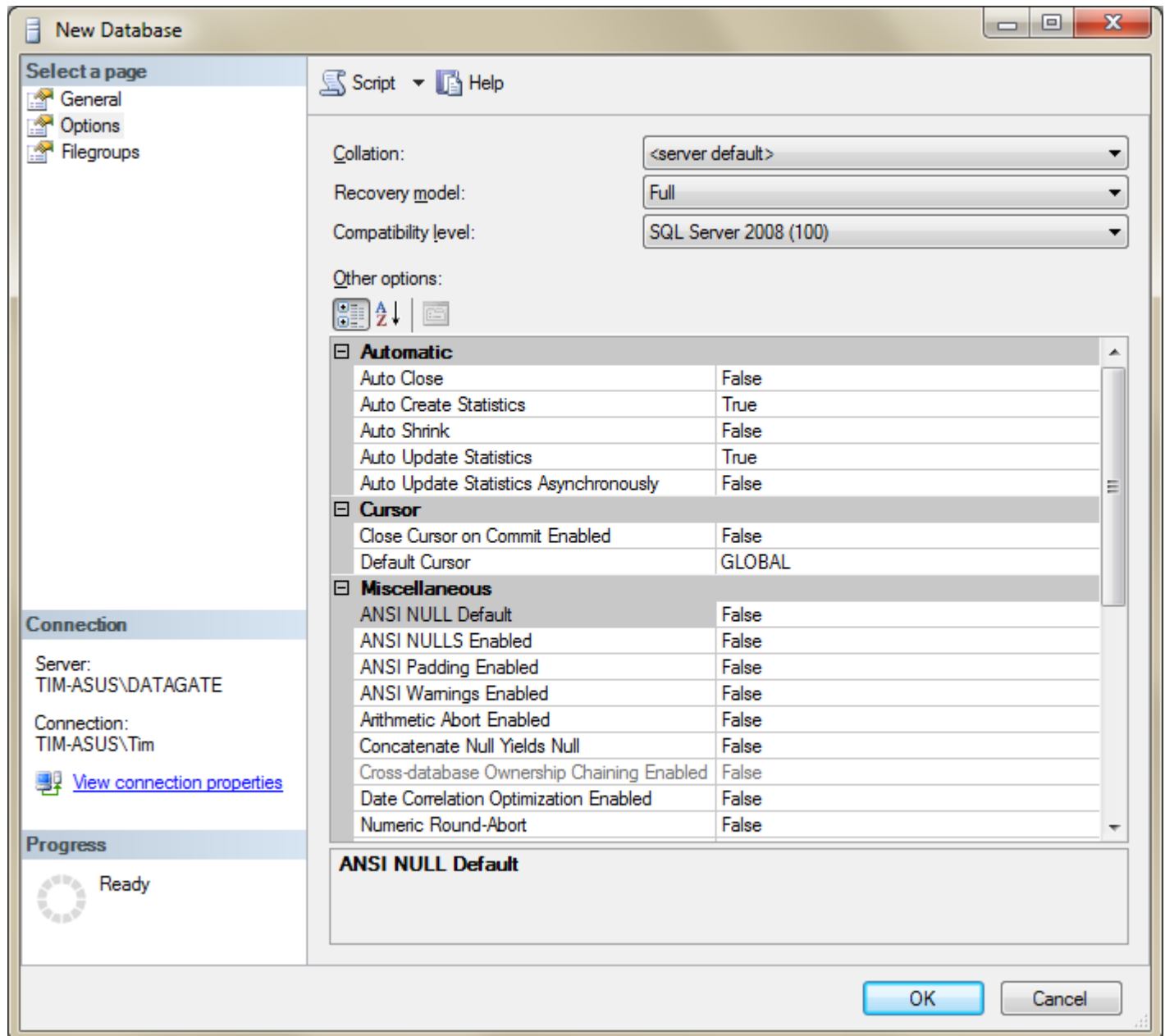
Figure 107 – Database options

20.1.1 SQL Server Logins

Once the database has been created, you need to edit user logins to allow access to the database. Look under the Security/Logins section of the Object Explorer to see the current login accounts (see Figure 108).
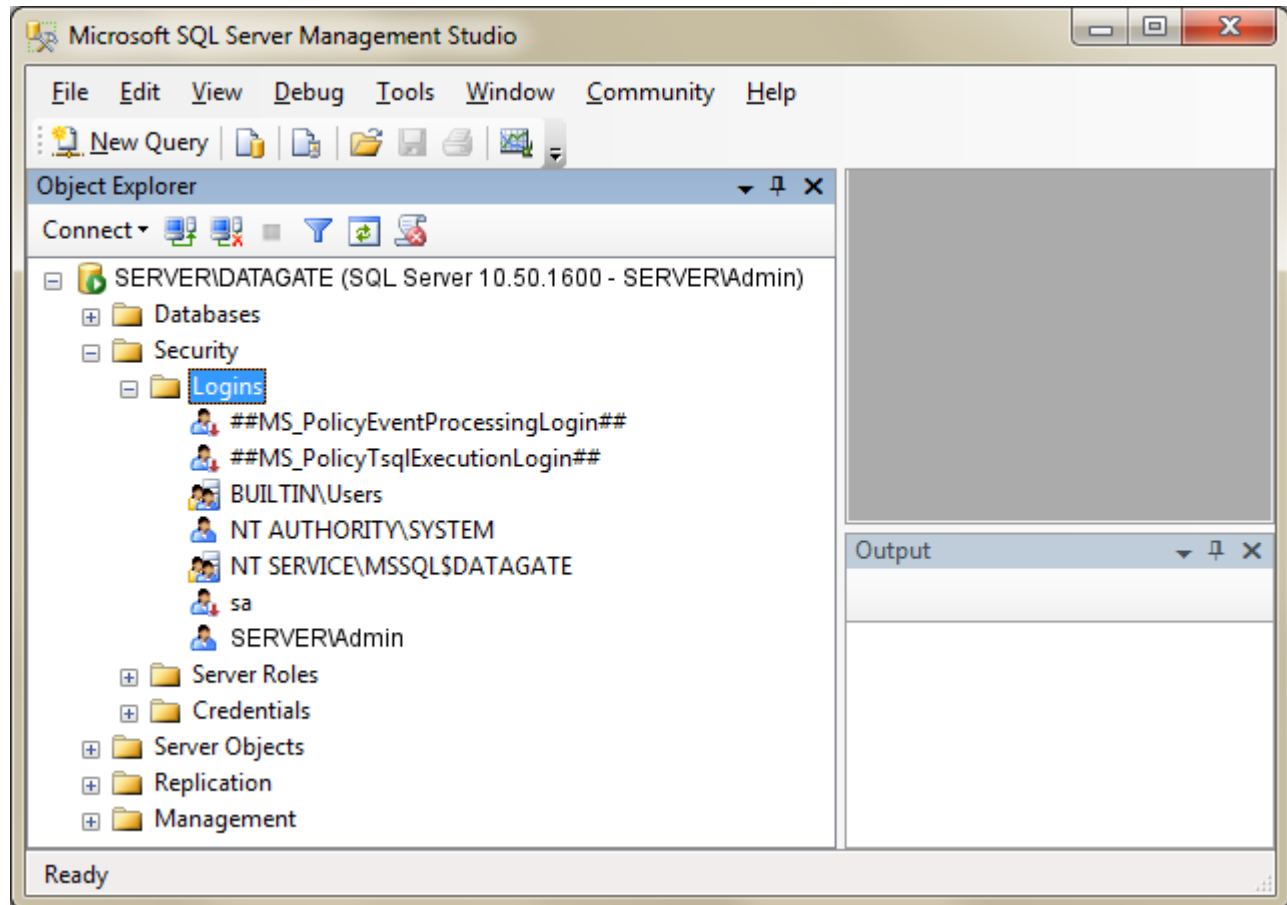
Figure 108 – SQL Server logins

If DataGate is going to connect as any of these existing logins, then you do not need to add any new users. However, if DataGate will be running under a different user account, or you want it to log in using a different username in mixed authentication mode, you will need to add it here.

To add a user, right-click on Logins in the object explorer and select "New User".

For Windows authentication mode, set the login name to match the desired Windows user account.

If using mixed authentication mode, you may enter a new username and password to allow connection to the server independently of the Windows account in use. Note: deselect the "Enforce password policy" option to prevent login issues.

To change user permissions, double-click on the user name in the logins section. This will open the Login Properties window, as shown in Figure 109.
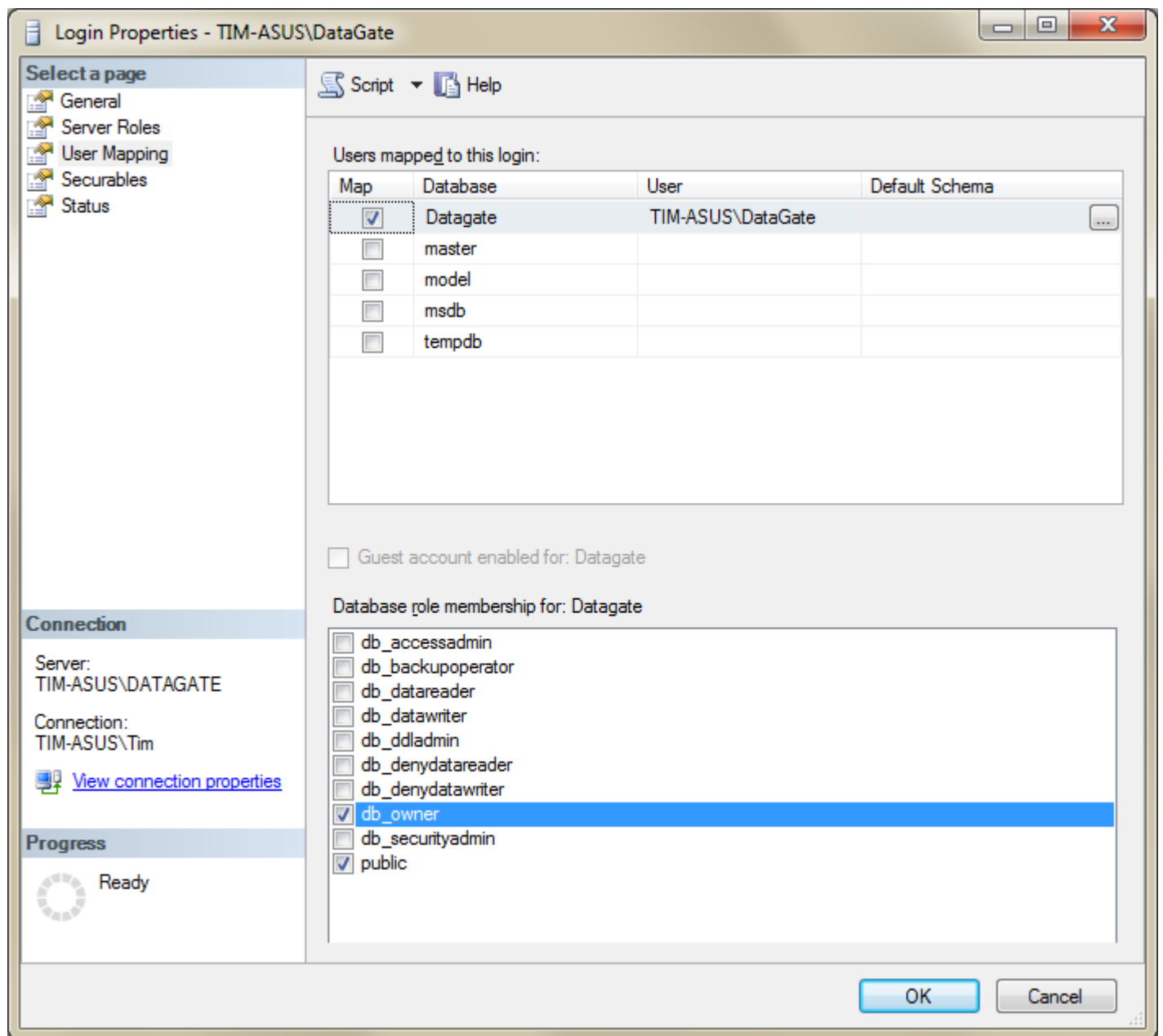
Figure 109 – SQL Server login properties

Under the User Mapping page, select the DataGate database, and then choose db_owner under role membership. This user will be allowed complete access and control over the database.

20.2 Automated Database Creation and Updating

The Primary Storage options (see section 7.7.1) include a button to create or update the database. Clicking this button opens the screen shown in Figure 110.
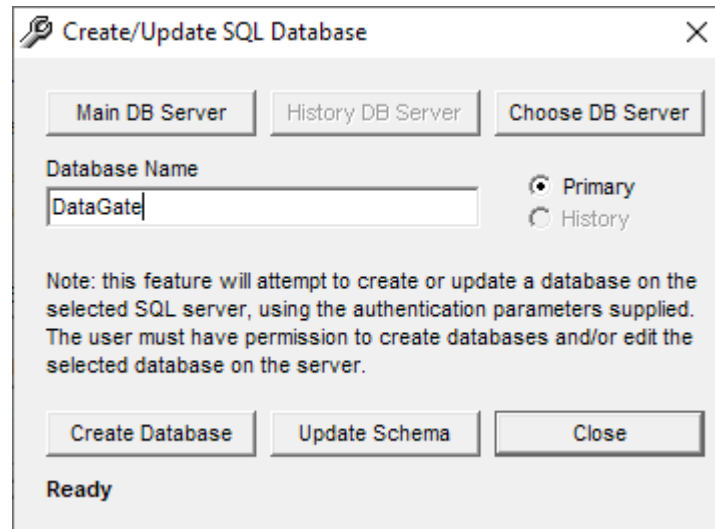
Figure 110 – Create/Update SQL Database

20.2.1 New Database

When setting up a new database, select "Choose DB Server" to set up the database connection. This will open the Windows Data Link Properties window. See section 20.4 for details on configuring the connection.

Note that the selected database user must have permission to create databases.

After testing the connection, close the Data Link Properties window to return to DataGate. Now enter a database name and click on "Create DataBase" to create a database on the configured database server.

When closing the database options form, DataGate will check if you want to update the database settings to point to the new database. Select Yes to proceed, and then Apply to enable the database.

20.2.2 Updating Existing Database

To update a currently configured database, use the Main/History DB Server buttons on the Create/Update SQL Database form to select the correct server settings. The database name should match the existing database. Select "Update Schema" to check and update the database to the latest schema. If automatic schema updates are enabled under DataGate settings then this step should not be required.

Note that the database user assigned in the database connection properties must have permission to modify the database.

20.3 Archive Database Creation and Updating

Figure 111 shows the archive database setup page, accessible from the Advanced Storage options page (see section 7.7.6). This connection uses the same connection settings as the primary database. Enter a database name, and then click on the buttons to create and/or update the database.
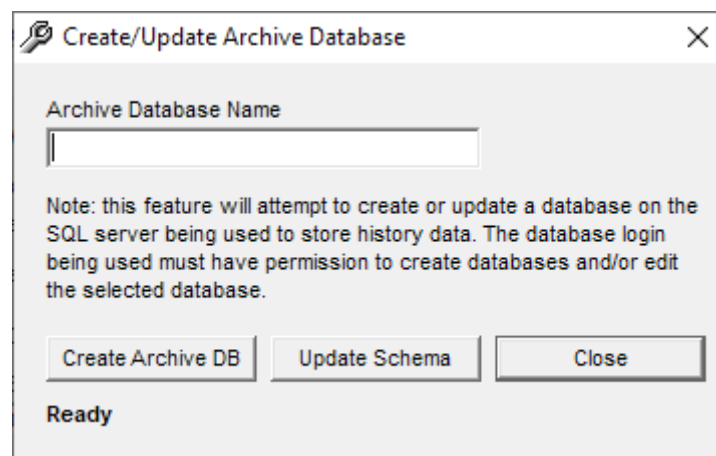
Figure 111 – Create/Update Archive Database

The archive database uses a special schema with identity columns and unnecessary tables removed.

20.4 Database Connection Properties

When configuring database connections, DataGate will display the standard Windows data link properties screen, as shown in Figure 112.
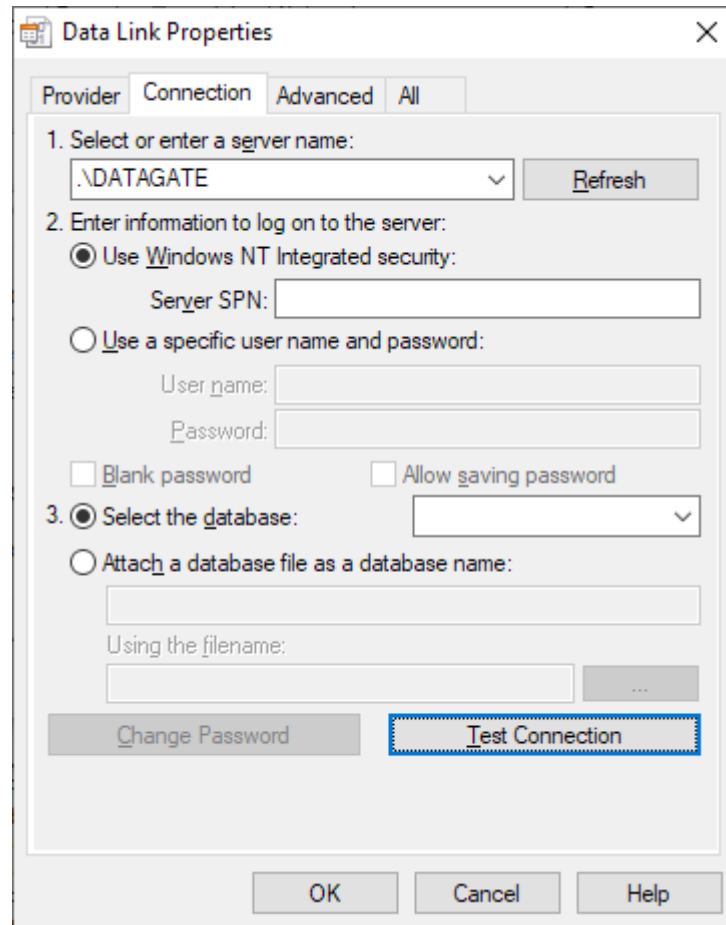
Figure 112 – Database Properties

The first step is to specify the database provider on the Provider tab. For SQL Server, select "SQL Server Native Client". For other databases, select the appropriate OLE DB provider from the list.

Next, enter the database server name on the Connection tab. For a database running on the local machine, use a single period (.) to specify the server. Otherwise, use a DNS name or IP address. If the database has been installed as a named instance, add a backslash (\) followed by the instance name, such as ".\DATAGATE".

DataGate can log in to the server in two ways: using Windows integrated security, or by specifying a user name and password.

Integrated security uses the credentials of the Windows user account that DataGate is running under. To use this option, make sure DataGate is running under the correct user account, and that this user has the necessary permissions in the database server. If running DataGate as a service, ensure that the service is set to run under an account with the necessary database permissions.

If the database server has been set up in mixed authentication mode, then it will also accept a log in using specific user names and passwords. In this case, the user has to be configured in the database server, and given the necessary permissions. Select the "Allow saving password" option and deselect "Blank Password" to allow DataGate to save an encrypted copy of the password.

Finally, select the desired database on the server. This can be left blank if the database has not yet been created, or if you want to use the default database (configured under the database server's options).

Use the "Test Connection" button to test the connection.

Note: in some situations (depending on client and database version) the database password is not saved when closing the database properties screen. You can check this by re-opening the database properties screen to see if the password field is populated. If the password has not been saved, the "Blank Password" checkbox will be selected instead. In this case you should re-enter the password, then switch to the "All" tab to adjust the following two parameters:

-    Set "Persist Security Info" to True
-    Open the "Integrated Security" option and click on "Reset Value"

21.0 Managing SQL Server Data

21.1 Importing Historical Data into SQL Server

If you migrate your data from one database platform or schema to another, you may want to move any historical data from the old to the new location. SQL Server provides an Import and Export Data feature, available from the Windows Start menu. On 64-bit machines you may need to run the 32-bit version, which supports more data source types (such as Microsoft Access).

The first step in the process is to select the data source.
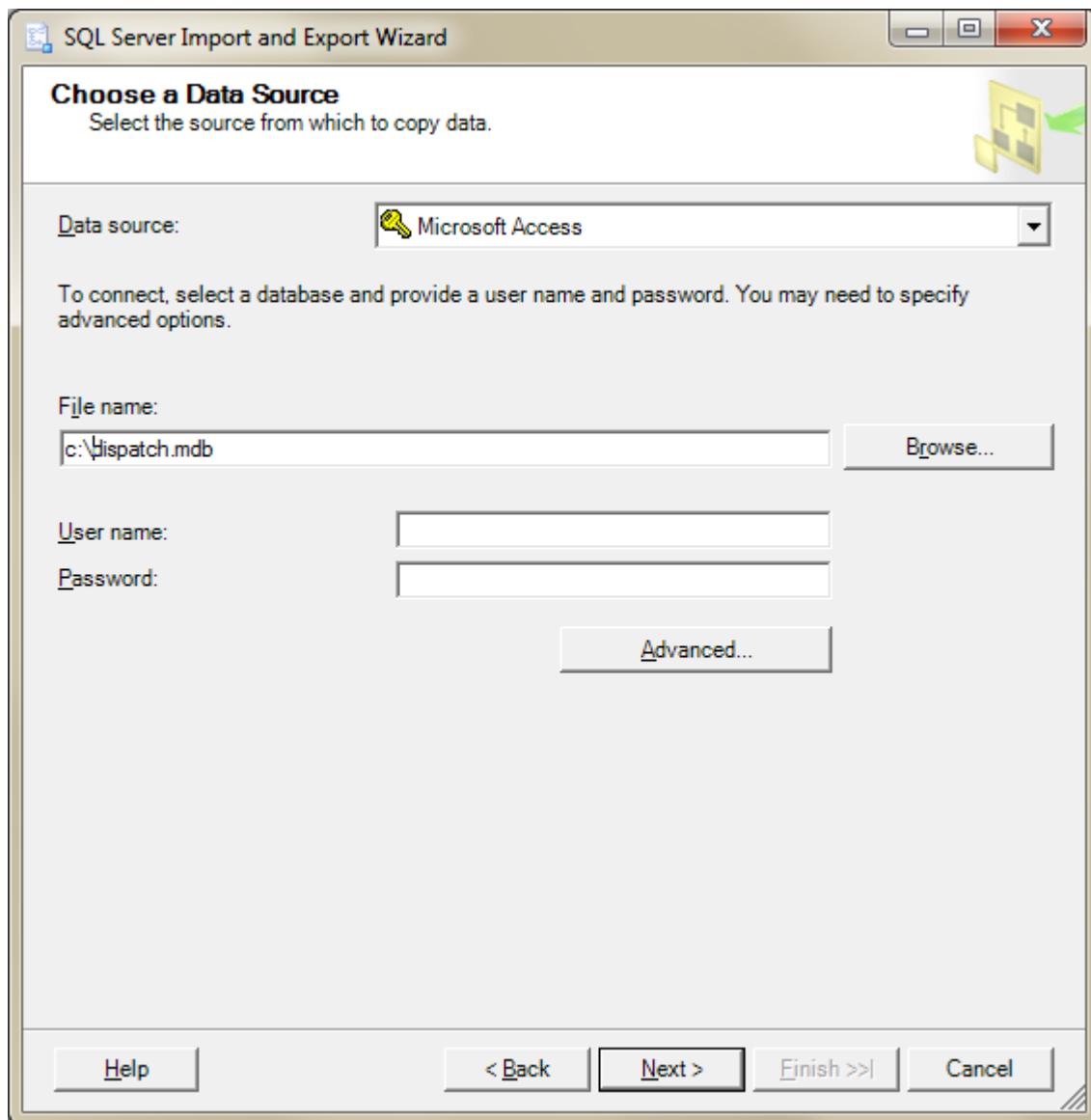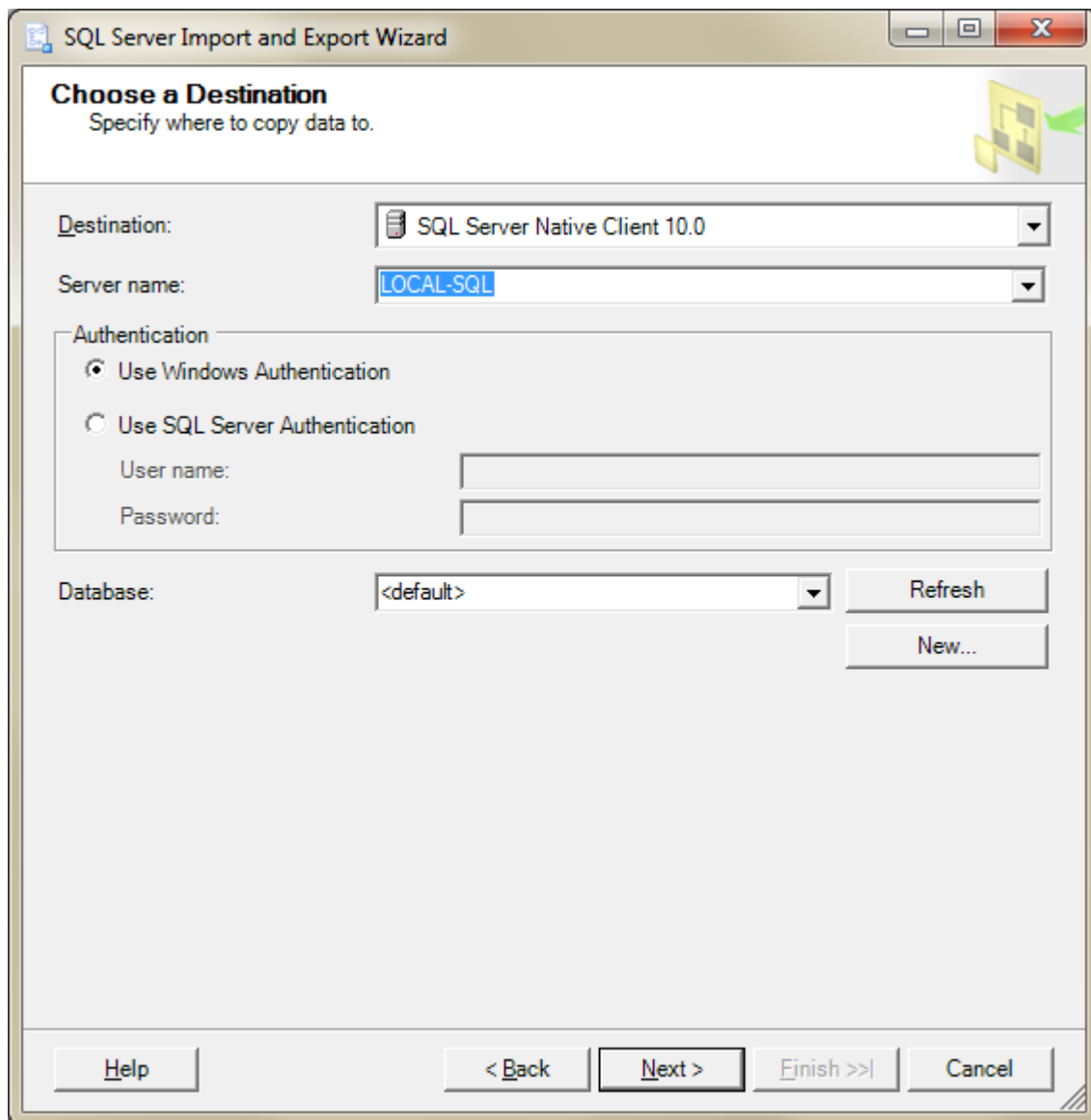
Figure 113 – Import Data Source

Select the source type and file location, and set the user name and password, if required.

The next step is to select the destination. This should point to your new SQL database. Select "SQL Server Native Client", and then enter you server name and authentication settings. Finally, choose the database into which you want the data to be imported.

Figure 114 – Import Data Destination

At the next step, select the "Copy data" option.
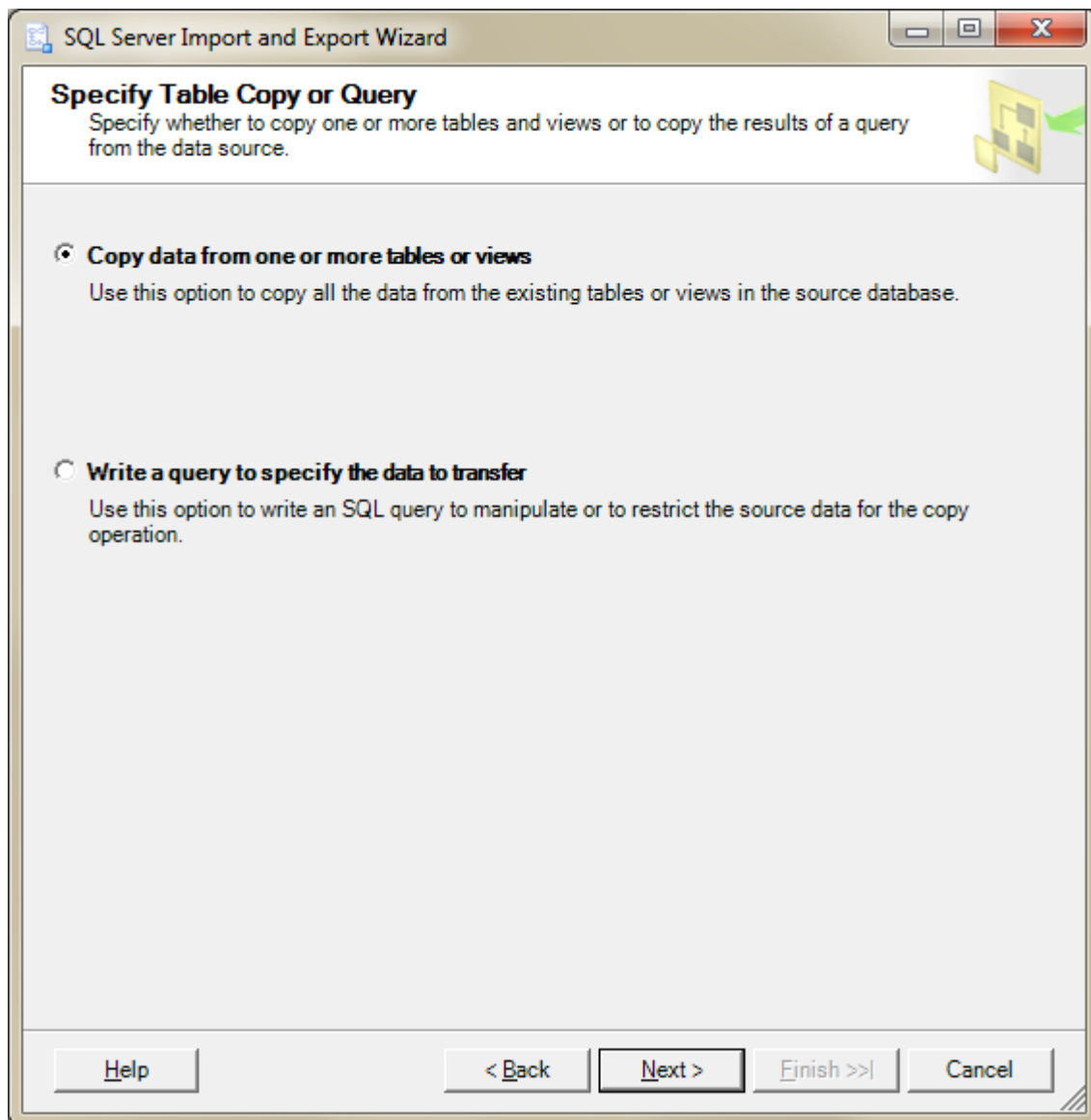
Figure 115 – Import Action

This step selects the source and destination tables. Select the History table in both the source and destination databases.
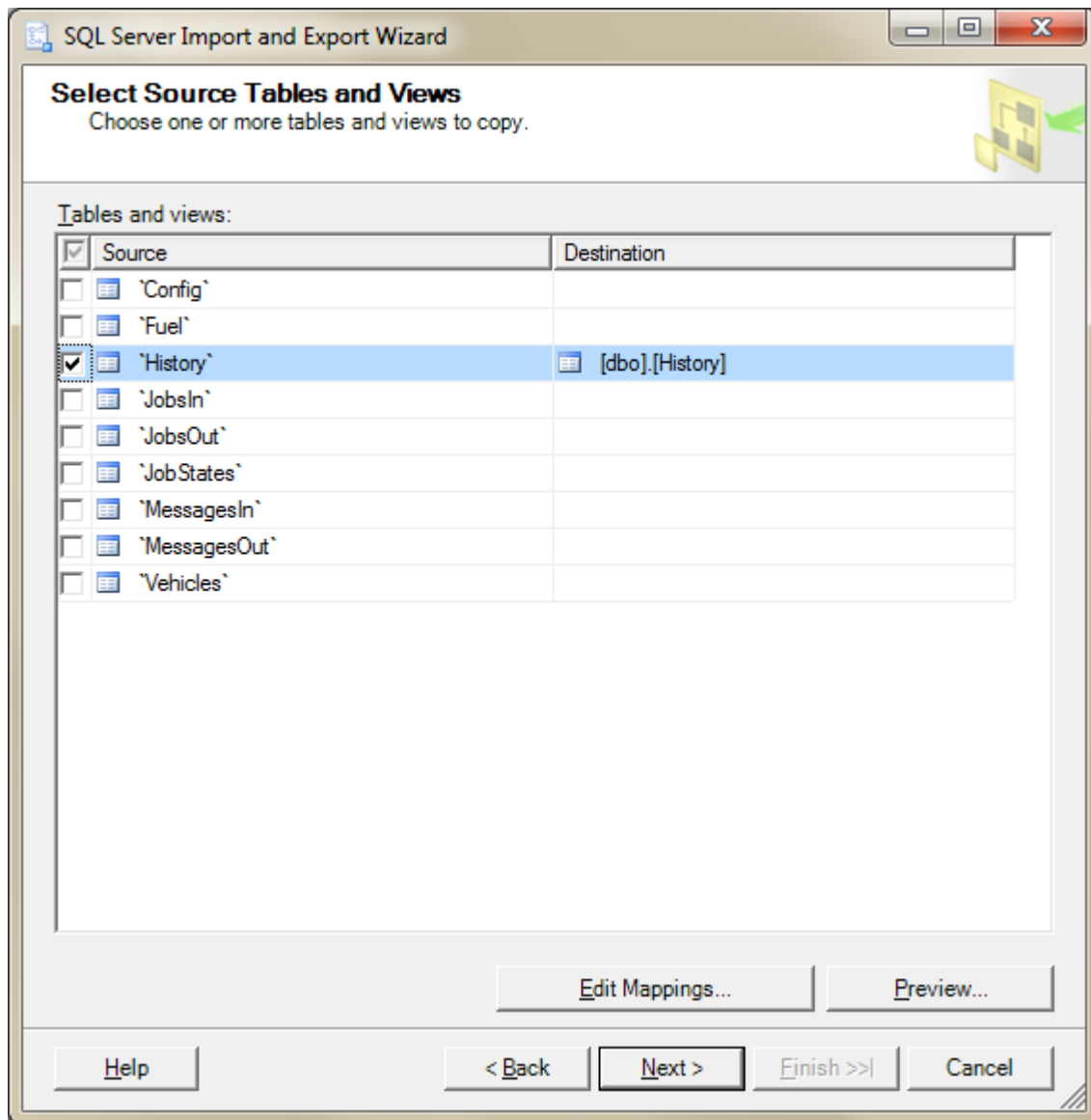
Figure 116 – Import Table

Before moving to the next step, click on "Edit Mappings" to set which fields to import.

Select "Append rows" then edit the mappings under the Destination column to ensure data is imported into the correct place. The HistoryID column should be ignored, as the new database will automatically generate these IDs. Some field names may have changed from the old to the new schema, so match them as shown below. For example, DeviceID maps to AssetID, while GPSDate maps to PacketTime. If any fields do not match, or are of the wrong type, select <ignore>. The EventData field used in the Dispatch schema is incompatible with the new schema, and cannot easily be imported.

Figure 117 – Import Column Mappings

Click OK to close this screen and return to the wizard.

This step shows a review of how the data will be mapped, and will highlight any potential incompatibilities.
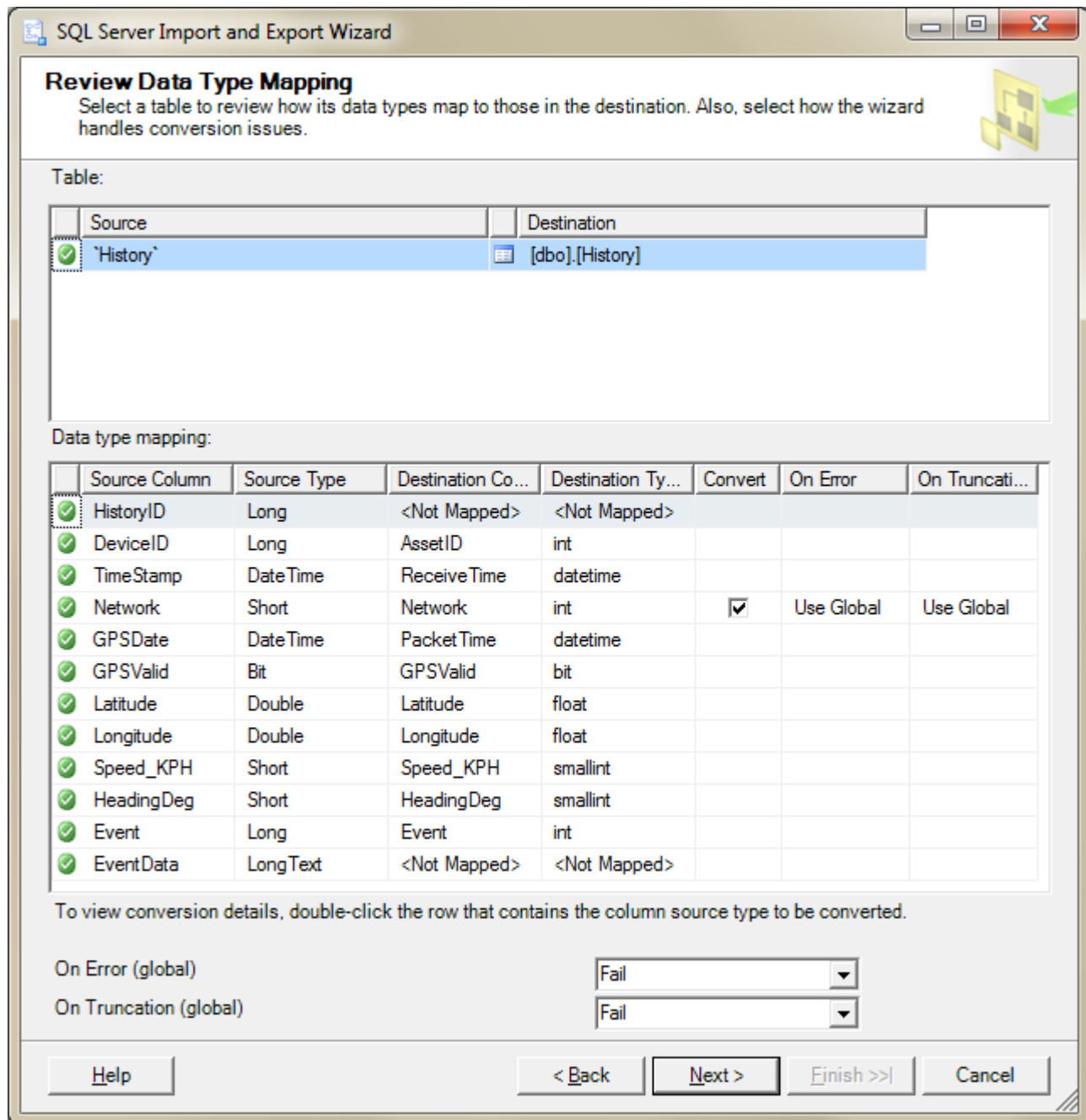
Figure 118 – Import Review

You can select whether to ignore or cancel the transfer when errors occur. Errors may occur whenever a type conversion is required.

Depending on your SQL Server version, you may have the option to save the import package. Otherwise, you can now run the package to begin importing data.
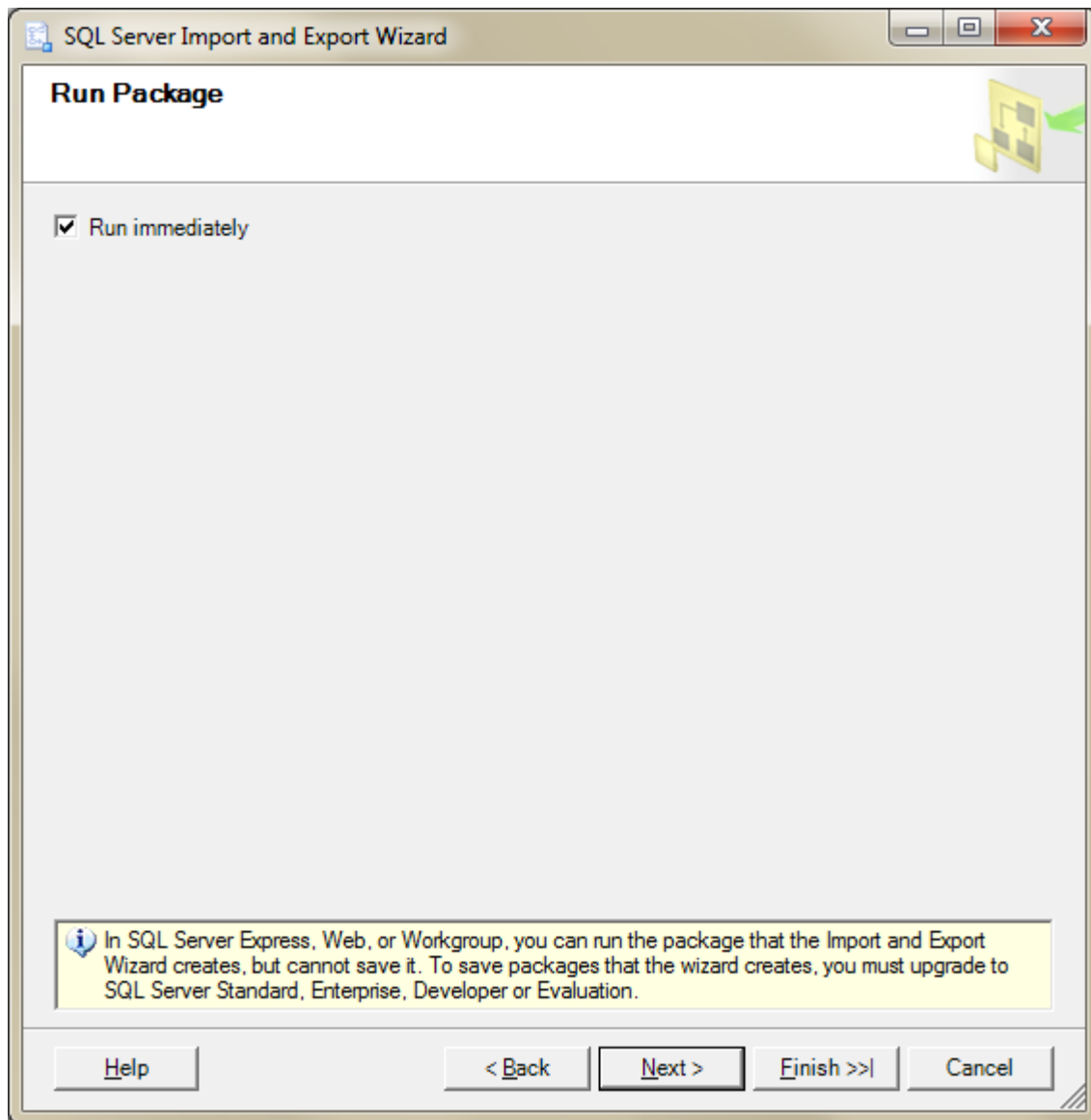
Figure 119 – Run Import Package

The import wizard now runs the package to import the data. The results panel shows whether the process succeeded or failed, and how many rows were transferred.
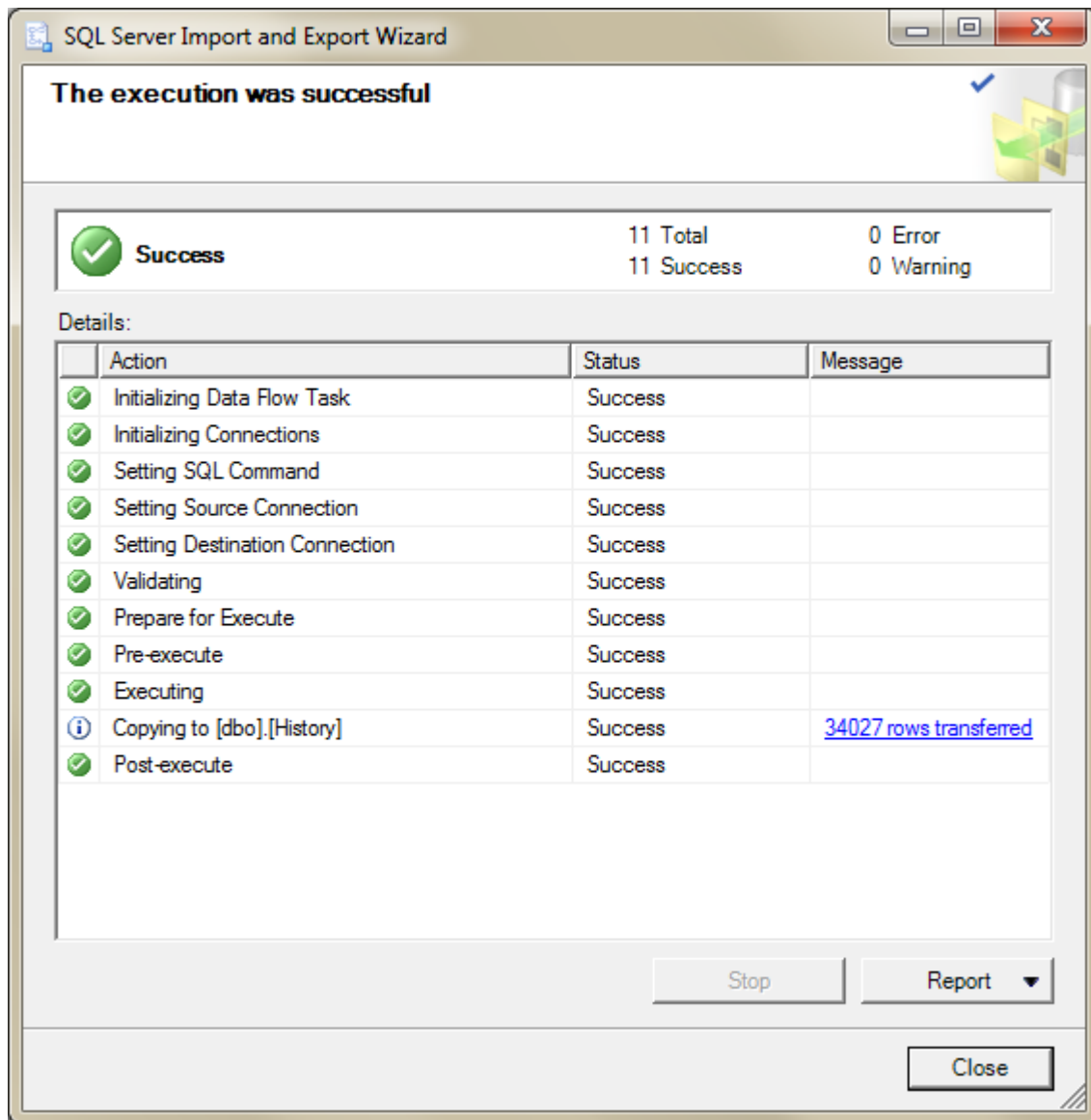
Figure 120 – Run Import Package

21.2 Archiving SQL Server Data

If using a database to store history data, the History table will continually increase in size until you manually archive its contents. Some free database servers (including SQL Server Express) have limitations on database size, so archiving can be critical to ongoing database usage.

It is recommended to use DataGate's built-in archiving feature (see section 7.7.6). Otherwise, the following steps describe how to perform manual archiving:

The simplest way to archive this data is to set up a new database into which the data will be moved, and then run two queries to move then delete the data, as follows:

1) Follow the steps in section 2.7 to create a new database, or use the built in database creation feature (see section 0). We will only be using the History table for archiving, but it will need to be modified to allow data to be inserted. By default, the HistoryID column will be an Identity value. This must be modified to set Identity = false, as we do not need to generate new Ids in this table.

2) Use SQL Server Management Studio to run the following two queries:

First, move x records from the current database into the archive database. In this example we are moving 10 million records from the "datagate" database into the "archive" database.

```
insert into [archive].[dbo].history
select top (10000000) * from [datagate].[dbo].history order by historyid
```

Second, delete those x records from the current database.

```
delete [datagate].[dbo].history where historyid in (
select top (10000000) historyid from [datagate].[dbo].history order by historyid)
```

Note: you should check how many records are transferred in the first step, and make sure you only delete that many records in the second step to prevent data loss.

In this example, the data is being sorted by the HistoryID column. This assumes that the oldest data was written to the database first. Alternatively, you may choose to sort the data by one of the timestamps in the table, such as the ReceiveTime or PacketTime columns. This will insure you are moving the oldest records, but the query may take longer to run.

Note: the archive schema must match the DataGate database schema, so you may need to update the archive database if you update the main database schema.

Also note that removing data from the history table may cause index fragmentation, which will reduce historical query speed. It is recommended to reindex or reorganize the indexes on the history table when they become fragmented.

22.0 Custom Map Layers

DataGate supports the display of custom map layers in its web interface using data provided by external mapping servers.

To enable custom maps, select "OpenLayers" under Map options (see section 7.4), and then click on "Edit Layers" to display the Mapping Layers window as shown in Figure 121.
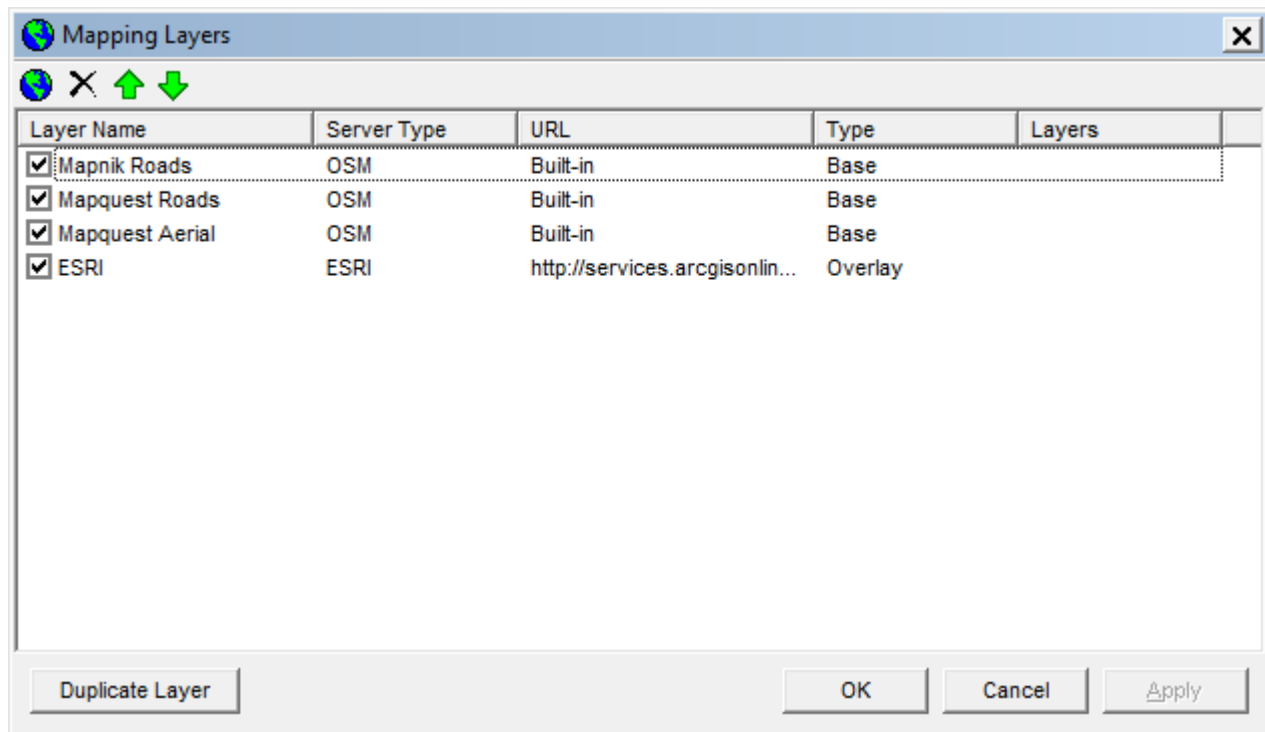
Figure 121 – Mapping Layers

Layers can be added and deleted using the toolbar or Insert and Delete keys on your keyboard. Layer order can be changed using the up and down arrows on the toolbar. Only checked layers will be shown on the web page. At least one layer must be enabled at any time. If custom layers are selected but cannot be loaded (due to map server error), DataGate will automatically enable one of the built-in layers.

By default, there are two layers built in to DataGate. These cannot be edited or deleted, but may be enabled or disabled using the list checkboxes. One layer uses OpenStreetMap (OSM) data, while the other uses an ESRI street map.

Note: these layers are provided for reference and testing purposes, and may require licensing for commercial or asset tracking use. Contact the map providers for more information.

Custom layers support ESRI and WMS maps. ESRI maps are served by ArcGIS servers, which are popular with commercial and government mapping departments. WMS servers are also popular, and include several free options such as GeoServer (http://geoserver.org).

A "Duplicate Layer" button is provided to quickly make a copy of an existing layer.

Double-click on a layer to open the Layer Properties window (Figure 122).

Figure 122 – Layer Properties

Layer Name:	Name used to reference this layer on the map.
Server Type:	Select ESRI to access ArcGIS Server maps, or WMS to access maps on a WMS server. OSM maps are currently limited to the three built-in layers.
Layer Type:	Select whether this layer is a base layer or an overlay. Only one base layer will be shown at once in the browser, whereas overlays can be toggled individually.
Server URL:	Address of map server. The URL also contains information about the particular map being requested. Do not include a trailing "/export" for ESRI servers.
Layer List:	For WMS and non-cached ESRI maps, a layer list allows you to select which map layers should be included.
Extra Parameters:	If required, extra parameters can be included in the map tile requests.
ESRI Token Server:	If the ESRI map server is secured, enter the token server URL. DataGate will attempt to obtain tokens as required. This will normally be a secure (https) address.
Username/Password:	Enter the username and password for the token server.

Ideally, you want to combine as many layers as possible into a single cached map layer. Cached maps will load much more quickly, but the data will only be as recent as the last cache update time.

Note that it is not possible to display overlays with different projections from the base layer. If possible, make sure all your map layers use the same projection.

22.1 ESRI Layers

DataGate is designed to connect to ArcGIS servers using REST services. The server URL will normally be of the form: http://example.com/arcgis/rest/services/map/mapserver

When accessing ESRI maps, the Web Client page will attempt to access the map server URL to determine the map parameters. It will then look up the map projection to allow it to transform the map data into latitude and longitude values. This process can take a few seconds when first loading the page. If the Web Client detects cached layers, it will access these directly. Otherwise, it will add /export to the URL and request the tiles as required. The maps should use an EPSG spatial reference, which the web page will load from a predefined list, including those projections defined under the View/Options/Maps menu. If an unknown reference is used, a lookup will be performed using http://spatialreference.org.

ESRI provides several base map layers. To use one of these maps, add a layer with Server Type set to ESRI and Layer Type set to Base. The Server URL can be obtained from the ESRI map services directory at http://services.arcgisonline.com/ArcGIS/rest/services. For example, the World Street Map URL is http://services.arcgisonline.com/ArcGIS/rest/services/World_Street_Map/MapServer.

Note: use of the ESRI map tiles may require a paid account. Contact an ESRI representative for more information.

22.2 WMS Layers

If you have access to map Shape files, or wish to create maps from other sources, you can use a free WMS map server to serve the maps to the Web Client.

22.2.1 GeoServer Setup

- Download and run the Windows Installer from http://geoserver.org/release/stable
- Note the username and password (default is admin/geoserver)
- Choose an available port, different from the DataGate web port (default is 8080)
- Select Install as a service
- Run "Start GeoServer" from Windows Start menu
- Run "GeoServer Web Admin Page" from Windows Start menu
- If you cannot see the admin page in a browser then check that the service is started, and port 8080 is available
- Log in to GeoServer using the admin username and password
- Go to the Data / Workspaces section
- Click on Add new workspace
- Set Name = datagate, and URI = http://www.geoserver.org/datagate
- Select Default Workspace, and Submit changes

22.2.2 Create a Map from JPEG Image

- Create a "world" file with the same name as your jpeg map, but with a .jgw extension
- Use a text editor (e.g. Notepad) to write six numbers (one per line) as follows:
  - o Pixel size X (longitude range / image width)
  - o Rotation X
  - o Rotation Y
  - o Pixel size Y (latitude range / image height)
  - o Top left position X (longitude of left side of image)
  - o Top left position Y (latitude of top side of image)
- For example, consider an image covering longitudes -100 to -98, latitudes 35 to 38, with image size 2000 x 5000 (width x height). The world file should look like:

```
0.001
0
0
0.0006
-100
38
```

- For compatibility it is recommended to use units of degrees based on the WGS 84 datum.
- Make sure the map/world filenames match and do not have spaces

22.2.3 Add a Map Source

- Create a folder in the GeoServer data directory for your map. For example, "C:\Program Files (x86)\GeoServer 2.13.0\data_dir\data\datagate"
- Copy your map files to this folder
- Go to the Data / Stores section on the GeoServer Web Admin Page
- Click on Add new store
- Select map source type. For a JPEG map, use WorldImage
- Select datagate workspace
- Choose a Data Source Name (e.g. "world")
- Browse for your map files, and Save changes
- Click on Publish to add a new layer
- The layer defaults should be OK, but you can change the layer name

22.2.4 DataGate Setup

- In DataGate, go to the View / Options / Maps menu
- Make sure OpenLayers is selected for map type
- Click on Edit OpenLayer Layers...
- Click on the globe icon to add a new layer
- Enter a layer name to appear in WebGate
- Set Server Type to WMS
- Set Layer Type to Base
- Set Server URL to http://localhost:8080/geoserver/datagate/wms. Change "localhost:8080" to point to your map server if necessary. Note that this server will need to be accessible from WebGate users' machines
- Under Layer List enter the layer name assigned in GeoServer
- Click OK to save

© 2000-2021 Datalink Systems International, Inc. | www.datalinksystemsinc.com

22.2.5 Confirm Operation

- Open a browser and load the WebGate page
- Zoom to the map area
- Click on the map layer icon (small plus sign on map)
- Select the custom map layer and ensure it displays

22.2.6 PatchMap Maps

Another example is the Canadian PatchMap map from SkyBase. To access this map, obtain the URL and API Key from SkyBase, and then add a map layer with the following settings:

1) Server Type: WMS
2) Layer Type: Base
3) Server URL: URL provided by SkyBase
4) Extra Parameters: version=1.1.1,apikey=xxxxx

23.0 Contact Information

For further support, email: support@datalinksystemsinc.com

Appendix A *CSV Fields*

The following fields are used for third-party interfaces:

Asset_ID	Asset ID
Description	Asset description
Last_Report_GMT	UTC time last packet received ("YYYY/MM/DD HH:MM:SS")
Last_GPS_GMT	UTC time packet generated by asset ("YYYY/MM/DD HH:MM:SS")
Latitude/Longitude	GPS latitude and longitude (decimal degrees)
Heading	GPS heading as compass point (N, NE, E, SE, S, SW, W, NW)
Speed_KPH	Asset speed (km/h)
Network	Network data was received on (see Appendix C)
GPS_State	GPS state (Invalid, Valid)
Heading_Deg	GPS heading (degrees)
Altitude_Metres	GPS altitude (metres)
Motion	Motion state (0=Stopped, 1=Moving)
Cell_ID	Cell ID
Cell_LAC	Cell LAC
Cell_RSSI_dBm	Cell RSSI (dBm)
Cell_Advance_Metres	Distance from cell site (metres)
IGN	IGN pin state (0=off, 1=on)
Input_X	Digital input states (0=low, 1=high)
Output_X	Digital output states (0=low, 1=high)
Sensor_X	Sensor states
Batt_Percent	Battery percentage
Batt_Volts	Battery voltage (Volts)
Temp_C	Temperature (degrees C)
VOUT	VOUT state (0=off, 1=on)
Driver	Currently logged in driver
GPS_OK	GPS state (0=Invalid, 1=Valid)
Sensor_X_Hex	Sensor states (hex encoded string)
Temp2_C	Temperature (degrees C)
Event_ID	Event ID (see Appendix B for details)
Event_Str	Event data (hex encoded string)
Priority	Data priority (0=normal, 1=high priority)
Msg_ID	Message ID
Trip_ID	Current trip ID
Trip_State	Current trip state (0=Unknown, 2=Postponed, 3=Started, 4=To Job, 5=At Job, 6=Selecting Dest, 7=To Dest, 8=At Dest, 9=Backhaul, 10=Backhaul Complete, 11=Returning, 12=Closing, 13=Paused)
Host_ID	Host ID (used to identify message source/dest)
Odo	Odometer (miles)
Hours	Engine hours (hours)
Today_Land	Bytes sent and received today over terrestrial networks *
Today_Sat	Bytes sent and received today over satellite networks *
Today_SMS	Number of SMS messages sent and received today *
This_Total	Total bytes sent and received this month *
This_Sat	Total bytes sent and received over satellite this month *

This_SMS   Total number of SMS messages sent and received this month *
Last_Total   Total bytes sent and received last month *
Last_Sat   Total bytes sent and received over satellite last month *
Last_SMS   Total number of SMS messages sent and received last month *
Group   Name of group this asset belongs to
Alert   Alert state for this asset (0=no alert, 1=alert active)

The hex encoded fields contain a string of hexadecimal numbers (0-9 or A-F), where each pair of numbers represents an 8-bit ANSI character. For example, "Hello" = "0x48656C6C6F".

* Daily byte totals are reset at midnight server time. Monthly totals are reset at the beginning of each calendar month (server time).

Appendix B   *Event Codes*

Event codes are used to describe asset events, and are used in the CSV field <Event_ID>, Push to Web Service XML packets, and database History table. Event IDs less than -1 are generated when data is sent to an asset.

The following events are supported:

-97	Message with Fields
-73	Message to External Port
-69	Remote Control
-67	Pager Message
-65	Message
-56	Take Picture
-55	Call-back Phone
-52	Garmin Control
-51	Email Message
-50	Cancel Alarm
-49	Reset Device
-48	Set Hourmeter and Odometer
-47	Reset Cell Modem
-46	Request Network Settings
-45	Set Network Settings
-44	Request String
-43	Set String
-42	Request Setting
-41	Set Setting
-38	Request IP Address
-37	Set IP Address
-34	Request Settings
-33	Set Settings
-30	Request Engine Settings
-29	Set Engine Settings
-28	Duty Log Update
-23	Job Dispatch
-11	Frame Reset
-10	Request Waypoint List
-8	Request Waypoint
-7	Set Waypoint
-6	Request Canned Message
-5	Set Canned Message
-3	Poll
-2	Set Outputs
-1	No Event
0	IO1 Change
1	IO2 Change
2-6	Pin Change (3-8)
7	IGN Change

8	Power Up
9	GSM Registration
10	GPRS Registration
11	Got IP Address
12	Timer 1
13	Timer 2
14	Timer 3
15	Timer 4
16	Distance Report
17	Overspeed
18	ADC 1
19	ADC 2
21-25	Geofence (1-5)
26	Power Save
27	GPS Status
28	RTC Alarm
29	GPS Invalid
30	Stopped
31-50	Geofence (6-25)
51	Input Event Counter
52	New SMS
58	Key Press
59	Low Battery
62	Motion Detected
63	Main Power Disconnected
71	GPS Antenna Fault
72	GPS Overspeed
73	Key Release
111	GSM Jamming
119	GPS Overspeed (alternate)
120-129	Polygon Geofence (0-9)
132-146	Polygon Geofence (10-24)
147	Firmware Updated
148	Acceleration Alert X1
149	Acceleration Alert X2
150	Motion Detected
151	Acceleration Alert Y1
152	Acceleration Alert Y2
153	Acceleration Alert Z1
154	Acceleration Alert Z2
160	Accelerometer Calibrated
161-163	Fast Acceleration
164-166	Heavy Braking
167-169	High RPM
170	Low Fuel Level
171	Idling Alert
172-174	Speed Alert
175	Low Battery

176	Engine Error
177	Entering Low Power Mode
178	IGN Change
183	Timer 9
184	Timer 10
185	OBD Discovered
186	OBD Time Out
988	Trip State Change
989	After Hours Use
990	Suntronics File
991	Picture Failed
992	Picture Received
993	File Received
994	Hold-Off Changed
995	Maintenance Warning
996	Hold-Off Alert
997	Time-Out
998	Configuration Response
999	Geofence Alert
1000	Event description is in Event_Str field
1001	Overspeed
1002	Pager NAK
1004	Power Up
1005	Reboot
1006	Power Down
1008	Input Change
1016	Stopped
1032	Started
1064	Pager ACK
1129	Overspeed End
1130	Power Down
1131	Enter Sleep
1132	Wakeup
1133	Periodic Report
1136	IGN Change
1137	AUX Change
1138-1141	Input Change (1-4)
1142	ADC1 Threshold Crossed
1143	ADC2 Threshold Crossed
1144	Alarm Test
1145	Geofence
1146	Invalid Password
1147	Tow Alert
1148	Blank Memory
1149	Angles Set
1152	Output Change
1153	Out1 Change
1154	Out2 Change

1155	Out3 Change
1156	Out4 Change
1157	VOUT Change
2048+1	IGN Changed
2048+2	AUX Changed
2048+4	In1 Changed
2048+8	In2 Changed
2048+16	In3 Changed
2048+32	In4 Changed
2048+64	ADC1 Threshold Crossed
2048+128	ADC2 Threshold Crossed
3000	Reset
3003	Swipe
3004	Internal Message
3006	Waypoint Setting
3008	Waypoint List
3010	Frame Reset
3012	Message Status
3015	Message Sent
3016	Engine Status
3021	Service
3022	Trip
3023	Driver Logged In
3024	Driver Logged Out
3026	Duty Status
3028	Engine Settings
3032	Settings
3036	IP Settings
3040	Setting Value
3042	String Value
3044	Network Settings
3050	Email Message
3064	Text Message
3066	Pager Message
3068	Waypoint
3069	Status Message
3072	External Data Message
3080	Transparent Data
4000	Stopped
4001	Started
4002	Idling
4003	Idling End
4004	Maintenance
4005	Pager Alarm
4006	False Alarm
4007	Alarm Cancelled
4008	Panic Alarm
4009	Clock Battery Low

4010	Clock Invalid
4011	Low Memory
4012	Low Disk
4013	Code Error
4014	Overspeed End
4015	Status Report
4016	Watchdog Timeout
4025	Stop Status
4026	ETA Update
4028	Fast Acceleration
4029	Heavy Braking
4030	Hard Cornering
4031	Tilt
4032	High Angle
4033	GPS Invalid
4034	Name Change
4035	Clear Stop List
4036	Geofence
4037	OBD-II Alert
4038	OBD-II Connected
4039	Low Battery
4040	Sensor Change
4041	Main Power Connected
4042	Device Plugged In
4043	Firmware Warning
4044	Power Down
4045	Wake Up
4046	GPS Antenna Fault
4047	GPS Antenna Cut
4048	Cellular Jamming
4049	GPS Jamming
4050	High RPM
4051	Low Fuel
4052	Acceleration Alert
4053	Power Up
4054	Engine Diagnostics
4055	High Coolant Temp
4056	Health Inspection
4057	Crash Alert
4058	Temperature Alert
4059	No Driver Check
4060	Fast Descent
4061	High G Force
4062	RFID Tag
4063	No Movement
4064	Diagnostics
4065	Seatbelt Violation
4066	Seatbelt OK

4067	Extreme Speeding
4068	Extreme Speeding End
4069	Fatigue Alarm
4070	GPS Jamming End
4071	Tamper
4072	Tamper End
4073	Antenna Cut
4074	Antenna OK
4075	Geozone Dwell
4076	Geozone Dwell End
4077	Cell Jamming End
4078	Invalid Driver

Appendix C   *Network Codes*

Network codes describe the network used to send or receive data. They are used in the CSV field <Network>, Push to Web Service XML packets, and database History table.

The following networks are supported:

1	Radio
3	MSAT
6	Inmarsat
7	UDP A
9	Kenwood
10	Globalstar Duplex
11	Simplex
12	UDP B
13	Iridium
14	G2
15	Trax
16	Raveon
18	Astro 25
19	Fleet Broadband
20	SMS
22	UDP C
23	TCP A
24	ICOM
25	TCP B
26	Local Serial
27	Local UDP
28	Relm
29	Hytera
30	Cursor on Target
31	HTTP
32	Shared

Appendix D *Database Tables*

The DataGate database contains several tables for storing asset and user information. A few tables can be used by third-party software to monitor asset history and send data to assets.

History	This table holds historical data. NULL values will be used where data is unavailable.
HistoryID:	Int - Automatically generated index, incremented with each new packet.
AssetID:	Int - 24-bit ID of the mobile device this packet was sent to/from. This ID is defined in DataGate, and is normally expressed as three 8-bit numbers (high byte first), such as 97279 = (1.123.255).
Sequence:	Int - Not used.
ReceiveTime:	Datetime - Time and date when packet was received by the DataGate server (UTC).
Network:	Int - Number defining which network was used to send this packet. See Appendix C.
PacketTime:	DateTime - Time and date when packet was created in remote device (UTC). If not available, the ReceiveTime value is used.
Motion:	Bit - Motion state of asset (1=moving, 0=stationary).
GPSValid:	Bit - GPS position validity (1=valid, 0=invalid/estimate).
Latitude:	Float - Latitude (decimal degrees).
Longitude:	Float - Longitude (decimal degrees).
Speed_KPH:	Smallint - Speed (km/h).
HeadingDeg:	Smallint - Heading (degrees).
Altitude:	Int - Altitude (metres).
CellID:	Int - Cellular site ID.
CellLAC:	Int - Cellular LAC.
CellRSSI:	Int - If value >= 128 then Cell Advance = (value and 63) * 550 metres. Otherwise, Cellular RSSI = value - 109 dBm.
GPSAccuracy:	Int – Accuracy estimate from GPS (metres).
Input1/4:	Bit - Input state (1=high, 0=low).
Output1/4:	Bit - Output state (1=high, 0=low).
IGN:	Bit - Ignition state (1=on, 0=off).
Sensor1/2:	Float - ADC raw values.
Battery:	Float - Battery voltage (volts).
BatteryPercent:	Tinyint - Battery percentage.
Temperature1:	Float - Temperature 1 (degrees C).
Temperature2:	Float - Temperature 2 (degrees C).
Temperature3:	Float - Temperature 3 (degrees C).
Event:	Int - Event code. See Appendix B.
EventData:	Varbinary(max) - Event details.
Priority:	Tinyint - Packet priority (1=high priority, 0=normal).
MessageID:	Int - Message identifier.
JobID:	Varchar(10) - Job/Dispatch identifier.
JobState:	Smallint - State of Job/Dispatch (0=Unknown, 1=Pre/Post Trip, 2=On Duty, 3=Roadside Inspection, 4=Driving, 5=Loading, 6=Unloading, 7=Waiting, 129=Off Duty, 130=Sleeper Berth, 131=Personal).

HostID:	Int - Host/User identifier.
Address:	Varchar(255) - Address of this location. DataGate will look up addresses when asset speed is below the global "stopped" speed, assuming Nominatim lookups are enabled.
CellSiteID:	Int - ID of cell site matching the cell ID/LAC. Set to -1 if no match.
CellSiteLat:	Float - Latitude of cell site.
CellSiteLon:	Float - Longitude of cell site.
CellSiteOrientation:	Smallint - Cell sit orientation (degrees).
DriverID:	Int – ID of driver assigned to asset when packet received.
VOUT:	VOUT state (1=on, 0=off).

Outbox	Use this table to send data to assets. Set State to zero to trigger processing.
MessageID:	Int - Message ID to allow client to track data. Set automatically by DataGate.
AssetID:	Int - ID of mobile device to send data to.
PacketType:	Int - Packet type (1=Set Outputs, 2=Poll, 64=Text Message, 1024=Clear Iridium queue). Other types are device dependent.
Data:	Varbinary(max) - Data to accompany packet. Leave blank for poll. Enter text for text message. Other types are device dependent. See DataNet Packet Structure document for iSeries packets.
MaxAttempts:	Int - Number of attempts allowed to send data. Zero specifies no limit. With each attempt, the NextSend value is increased by a larger amount, up to 24 hours between tries.
Attempts:	Int - Number of attempts taken so far.
Cancel:	Bit - Not used.
NextSend:	Datetime - Time of next attempt (UTC). Set to zero for immediate send.
SentTime:	Datetime - Time at which packet was sent (UTC).
QueueTime:	Datetime - Time at which packet was queued (UTC). Set to zero when adding record.
ResponseTime:	Datetime - Time at which response was received (UTC).
CancelledTime:	Datetime - Time at which job was cancelled (UTC).
EmailSMS:	Varchar(320) - Not used.
State:	Int - Status of transmission:

        0 – Not yet processed by DataGate.
        1 – Sending
        2 – Sent OK
        -1 – Unknown Device
        -2 – No Response
        -3 – Message Too Long
        -4 – No Outputs
        -5 – No Access
        -6 – Not Assigned
        -7 – Invalid Pager
        -8 – Invalid Packet
        -9 – Unsupported Packet
        -12 – Timeout
        -13 – Server Error
        -14 – Already Queued

-18 – Queue Full
-19 – Too many Trips
-20 – Unknown Trip
-21 – Trip already exists
-22 – Can't Cancel
-23 – Rejected
-24 – No Connection
-25 – Wrong Driver ID

Appendix E   *Sample SOAP Packets*

Here is an example packet sent from DataGate when push to web service is enabled:

```
POST /test HTTP/1.1
Host: www.example.com:80
Content-Type: text/xml; charset=utf-8
Content-Length: xxx
SOAPAction: "http://www.datalinksystemsinc.com/datagate1/AssetEventNotification"
Connection: close

<?xml version="1.0" encoding="utf-8"?>
 <soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Header>
   <DataGateHeader xmlns="http://www.datalinksystemsinc.com/datagate1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.datalinksystemsinc.com/datagate1
http://www.datalinksystemsinc.com/datagate1.xsd" Company="Datalink Systems, Inc."
AppVersion="6.8.9" AppName="DataGate Plus" Version="1.0" Pwd="test" UserID="test"/>
  </soap:Header>
  <soap:Body>
   <AssetEventNotification xmlns="http://www.datalinksystemsinc.com/datagate1">
    <Events>
     <AssetEvent objectID="6517927010000-7">
      <AssetDescription>Mobius</AssetDescription>
      <AssetID>0.0.1</AssetID>
      <RXTime>2020-08-26T21:31:41Z</RXTime>
      <GMTTime>2020-08-26T21:31:41Z</GMTTime>
      <Network>7</Network>
      <Priority>normal</Priority>
      <GPS>
       <Valid>false</Valid>
       <Latitude>34.18937</Latitude>
       <Longitude>-103.595</Longitude>
      </GPS>
      <Telemetry>
       <Speed units="mph">35</Speed>
       <Heading>285</Heading>
      <DigitalIO>
       <IGN>low</IGN>
       <Input1>low</Input1>
       <Output1>low</Output1>
      </DigitalIO>
      </Telemetry>
      <Event>
       <Number>3000</Number>
       <Description>Version 1</Description>
      </Event>
     </AssetEvent>
    </Events>
    <TransID>651792756</TransID>
   </AssetEventNotification>
  </soap:Body>
</soap:Envelope>
```

The following example shows an XML polling request sent to DataGate, and its responses. Each request must include a SOAP header with DataGateRequestHeader element. Responses will contain a DataGateResponseHeader element.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
 <soap:Header>
  <DataGateRequestHeader xmlns="http://www.datalinksystemsinc.com/Version_1.0"
   User="user" Password="pass"/>
 </soap:Header>
 <soap:Body>
  <GetAssetList xmlns="http://www.datalinksystemsinc.com/Version_1.0"/>
 </soap:Body>
</soap:Envelope>

<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
 <soap:Header>
  <DataGateResponseHeader xmlns="http://www.datalinksystemsinc.com/Version_1.0"
   Company="Datalink Systems, Inc." AppVer="6.1.10" AppName="DataGate" Version="1.0"
   Sequence="19" Instance="123"/>
 </soap:Header>
 <soap:Body>
  <GetAssetListResponse xmlns="http://www.datalinksystemsinc.com/Version_1.0">
   <Assets>
    <Asset>
     <AssetID>1</AssetID>
     <Name>Example</Name>
     <Sequence>1</Sequence>
    </Asset>
    ...
   </Assets>
  </GetAssetListResponse>
 </soap:Body>
</soap:Envelope>
```

The following examples show the SOAP body elements used in requests and responses.

Use the Ping method to check server operation:

```xml
<Ping xmlns="http://www.datalinksystemsinc.com/Version_1.0"/>

<PingResponse xmlns="http://www.datalinksystemsinc.com/Version_1.0">
 <State>OK</State>
</PingResponse>
```

GetMethods returns a list of supported methods:

```
<GetMethods xmlns="http://www.datalinksystemsinc.com/Version_1.0"/>

<GetMethodsResponse xmlns="http://www.datalinksystemsinc.com/Version_1.0">
 <Methods>
  <string>Ping</string>
  <string>GetMethods</string>
  <string>GetAssetList</string>
  <string>GetRecentPositions</string>
  <string>GetInbox</string>
  <string>GetSent</string>
  <string>DeleteMessages</string>
  <string>GetOutbox</string>
  <string>DeleteOutboxMessage</string>
  <string>SendMessage</string>
 </Methods>
</GetMethodsResponse>
```

Use GetAssetList to obtain information on all supported assets:

```
<GetAssetList xmlns="http://www.datalinksystemsinc.com/Version_1.0"/>

<GetAssetListResponse xmlns="http://www.datalinksystemsinc.com/Version_1.0">
 <Assets>
  <Asset>
   <AssetID>123</AssetID>
   <Name>Example</Name>
   <RadioID>U00001</RadioID>
   <Sequence>19</Sequence>
   <Network>Kenwood</Network>
   <LastReportTime>2016-07-14T13:55:02Z</LastReportTime>
  </Asset>
  ...
 </Assets>"
</GetAssetListResponse>
```

GetRecentPositions returns positions from all assets that have sent something since the Sequence value provided. It is expected that a client will use the Sequence and Instance values returned by the server (in the DataGateMsgHeader element) the last time this method was called. If the Sequence value is not entered, or Instance does not match the server's current Instance value, all assets with positions will be returned:

```
<GetRecentPositions xmlns="http://www.datalinksystemsinc.com/Version_1.0">
 <Sequence>10</Sequence>
 <Instance>123></Instance>
</GetRecentPositions>

<GetRecentPositionsResponse xmlns="http://www.datalinksystemsinc.com/Version_1.0">
 <Positions>
  <Position>
   <AssetID>123</AssetID>
   <Name>Example</Name>
   <Time>2016-06-10T01:30:48Z</Time>
   <Speed_MPH>0</Speed_MPH>
   <Heading>260</Heading>
   <Latitude>39.12345</Latitude>
   <Longitude>-100.42314</Longitude>
   <Valid>true</Valid>
   <Network>Kenwood</Network>
  </Position>
  ...
 </Positions>
</GetRecentPositionsResponse>
```

Use GetInbox to return all available messages received from assets. Provide a HistoryID value to limit the response to messages with higher HistoryID values. It is expected that the client will use the highest HistoryID value obtained in any previous call to this method:

```
<GetInbox xmlns="http://www.datalinksystemsinc.com/Version_1.0">
 <HistoryID>12345</HistoryID>
</GetInbox>

<GetInboxResponse xmlns="http://www.datalinksystemsinc.com/Version_1.0">
 <InboxMessages>
  <InboxMessage>
   <AssetID>123</AssetID>
   <Name>Example</Name>
   <Time>2016-05-01T23:59:49Z</Time>
   <HistoryID>12346</HistoryID>
   <Text>Message text</Text>
   <MessageID>123</MessageID>
   <Priority>High/Low</Priority>
  </InboxMessage>
  ...
 </InboxMessages>
</GetInboxResponse>
```

Use GetSent to return all available messages send to assets. Provide a HistoryID value to limit the response to messages with higher HistoryID values. It is expected that the client will use the highest HistoryID value obtained in any previous call to this method:

```
<GetSent xmlns="http://www.datalinksystemsinc.com/Version_1.0">
 <HistoryID>12345</HistoryID>
</GetSent>

<GetSentResponse xmlns="http://www.datalinksystemsinc.com/Version_1.0">
 <SentMessages>
  <SentMessage>
   <AssetID>123</AssetID>
   <Name>Example</Name>
   <Time>2016-05-02T21:39:42Z</Time>
   <HistoryID>12347</HistoryID>
   <Text>Sent Message</Text>
   <MessageID>100</MessageID>
  </SentMessage>
  ...
 </SentMessages>
</GetSentResponse>
```

The DeleteMessages method will delete all messages from the inbox and sent items with a HistoryID equal to or less than the provided value. It is expected that the client will delete messages periodically. The server will automatically delete older messages when the queue gets too long:

```
<DeleteMessages xmlns="http://www.datalinksystemsinc.com/Version_1.0">
 <HistoryID>12345</HistoryID>
</DeleteMessages>

<DeleteMessagesResponse xmlns="http://www.datalinksystemsinc.com/Version_1.0">
 <State>OK</State>
</DeleteMessagesResponse>
```

Use the GetOutbox method to return a list of messages waiting to be sent to assets. The State element indicates whether the message is being sent or has failed. Once messages have been successfully sent, they will be moved to the sent messages list:

```
<GetOutbox xmlns="http://www.datalinksystemsinc.com/Version_1.0"/>

<GetOutboxResponse xmlns="http://www.datalinksystemsinc.com/Version_1.0">
 <OutboxMessages>
  <OutboxMessage>
   <AssetID>123</AssetID>
   <Name>Example</Name>
   <OutboxID>17</OutboxID>
   <MessageID>999</MessageID>
   <State>Sending.../Send Failed</State>
   <Text>Message to asset</Text>
  </OutboxMessage>
   ...
 </OutboxMessages>
</GetOutboxResponse>
```

The DeleteOutboxMessage method removes a message from the outbox, using the OutboxID to identify the message. Include the server's Instance value, as this is required to uniquely identify each item in the outbox:

```
<DeleteOutboxMessage xmlns="http://www.datalinksystemsinc.com/Version_1.0">
 <OutboxID>17</OutboxID>
 <Instance>12345</Instance>
</DeleteOutboxMessage>

<DeleteOutboxMessageResponse xmlns="http://www.datalinksystemsinc.com/Version_1.0">
 <State>OK</State>
</DeleteOutboxMessageResponse>
```

Use the SendMessage method to queue a message to an asset. The AssetID value identifies the destination asset, while the Text value contains the message itself. Note that messages will be rejected if they are too long. The response will contain a State value, indicating whether the packet has been sent or is queued for delivery. Queued packets will appear in the outbox, and can be identified using the returned OutboxID value.

The optional Priority and MaxAge values are available from DataGate version 6.8.16. Priority tells DataGate how often to attempt delivery of this message to the asset. Priority 1 messages are tried one time only (using the last known network for this device). Priority 2 messages are tried once per network used by the device. Priority 3 messages (the default if value not provided) are tried three times per network before failure. Priority 4 messages are tried three times per network, and then retried with an increasing delay. Use MaxAge to limit how long a message will stay queued for delivery (in seconds, with a default of 86400).

```
<SendMessage xmlns="http://www.datalinksystemsinc.com/Version_1.0">
 <AssetID>123</AssetID>
 <MessageID>1000</MessageID>
 <Priority>3</Priority>
 <MaxAge>86400</MaxAge>
 <Text>Message</Text>
</SendMessage>

<SendMessageResponse xmlns="http://www.datalinksystemsinc.com/Version_1.0">
 <State>Sent/Accepted</State>
 <OutboxID>17</OutboxID>
</SendMessageResponse>
```

If any requests are unrecognised or contain invalid values, the server will return a SOAP fault similar to the following:

```
HTTP/1.1 500 Internal Server Error
...

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
 <soap:Header>
  <DataGateHeader xmlns="http://www.datalinksystemsinc.com/Version_1.0"
   Company="Datalink Systems, Inc." AppVer="6.1.10" AppName="DataGate" Version="1.0"
   Sequence="1" Instance="521883026"/>
 </soap:Header>
 <soap:Body>
  <soap:Fault>
   <faultcode>Client</faultcode>
   <faultstring>Invalid user ID or password</faultstring>
  </soap:Fault>
 </soap:Body>
</soap:Envelope>
```

Appendix F   *NXLink Quick-Start*

1) Before you install DataGate, there are a few steps required to enable email sending and receiving:

- You must have a static public IP address through which the DataGate email server can be accessed. If passing through a router or firewall, make sure TCP port 25 is directed to the DataGate machine.
- Assign a host name (Fully Qualified Domain Name) to the server, such as `datagate.example.com`. Contact your DNS provider to add an "A" record for this host name, pointing to the public IP address. For example, `datagate.example.com A 192.0.2.1`
- The reverse DNS entry for your public IP address should point to the same host name. For example, `1.2.0.192.in-addr.arpa PTR datagate.example.com`. Contact your ISP to make this change.
- Select or create a domain name that will be used for sending and receiving DataGate emails, such as `example.com`. This domain must not already be assigned to an email server. Emails sent to and received from DataGate will use this domain as the second part of the email to and from addresses. For example, demo@example.com.
- Contact your DNS provider to assign an MX record for this domain. This record must point to the DataGate host name. For example `example.com MX datagate.example.com`. When a remote machine wants to send an email to your domain, it will look up this record and connect to your DataGate.
- Make sure your ISP permits you to make outgoing connections on TCP port 25. Some providers block port 25 in an attempt to reduce spam originating from their networks. DataGate uses port 25 when sending emails from assets to remote servers. If port 25 cannot be unblocked, DataGate can be configured to use an external email server when sending email.

2) You will also need to configure your radios:

- If the base radio is located next to the server, and the server has a COM port, you may use a standard serial cable to connect the radio to the PC. Otherwise, obtain a serial to Ethernet converter to allow the radio to connect into the network. We recommend the Neteon GW-212 unit, or similar.
- Program the base radio so that its rear COM port is set to output Data + GPS. Use this rear port when connecting the radio to the server or serial to Ethernet converter.
- Assign a Fleetsync or NXDN ID to the base radio.
- In order for portable/handheld radios to reply to email messages, they require a special messaging version of firmware from Kenwood. Update your radios as required.
- Program your portable/handheld radios with a Fleetsync or NXDN ID. Enter the ID of base radio under the base settings.

3) Once this is complete, you may continue with the DataGate installation:

- Download DataGate from the Datalink Systems website at www.datalinksystemsinc.com/downloads. Install DataGate on a Windows PC. Optionally, also download and install the DataGate service, which allows DataGate to run automatically when the system boots.

- Request a license through the DataGate user interface. An Enterprise version of DataGate is required for processing emails. You will also need asset licenses for each radio you want to send messages to. Demo licenses are available. Contact Datalink Systems at this step to expedite the licensing process.
- Go to the View/Options menu in DataGate, and select the Emails tab.
- On the General tab, enter the public host name of the server (e.g. datagate.example.com). Enter the domain name you have selected for sending and receiving emails (e.g. example.com). Assign an admin email address, which will receive errors or alerts generated by DataGate.
- On the Incoming tab, uncheck the "Enable white list" option. This can be enabled later, along with the "Allow SMTP Connections from IP Addresses" option, when securing the server.
- On the Outgoing email tab modify the email from address to use your email domain (e.g. noreply@example.com).
- Click Apply to save the settings.
- Click on the "Send Test Email to Admin" button to send a test email. Check the log listing on the main DataGate screen to confirm the email is sent OK.
- Click OK to close the settings window.

4) Add remote radios to the DataGate. These radios will send and receive messages via DataGate:

- On the main DataGate screen click on the grey circle in the toolbar to add an asset. Enter an ID such as 0.0.1, and select the Kenwood Radio as hardware type. Click OK to create the asset.
- Double-click on the asset in the list. Enter a description for this asset. This name will be used as the first part of the email address for this asset. For example, an asset with description "radio1" will have email address radio1@example.com.
- Change the group to (All).
- Check the "Accept Emails to Device" option to allow sending emails to this asset.
- On the Modems tab, select the type of radio ID and enter the ID for the remote radio. Unit (individual) IDs will normally be used when sending and receiving emails.
- Click OK to save the changes to this asset.
- Repeat this process to add further assets, making sure you use unique asset IDs and descriptions. Asset IDs can be entered in the range (0-255).(0-255).(0-255).

5) Add a base radio to DataGate:

- Go to the View/Data Sources menu.
- Click on the Antenna icon in the toolbar to add a source.
- Enter a description, such as "Base Radio".
- Select the Kenwood network.
- Choose the connection type. Radios are normally connected through a local serial port or via a serial to Ethernet converter. Kenwood console connections are also supported for advanced setups.
- If using a local COM port, enter the port number and COM settings.
- If using a serial to Ethernet converter, enter the IP address of the converter. Select a port that the converter will connect to. Program the converter to connect to DataGate's IP address and selected port using a TCP client connection.

- Kenwood radios can be configured to use PC interface versions 1 or 2. The DataGate setting should match the setting in the base radio.
- Program status messages as required. These are used to translate status codes sent by the radio into text. The remote radios should also be programmed to show this text when the user selects a status code.
- Click OK to save the source settings.
- The base radio can now be connected to the DataGate.

6) Test:

- Using an external email server, send an email to one of your assets. The first part of the address will be the asset's description, while the second part will be your email domain. For example, john@example.com
- Check that DataGate shows email activity in the log listing on the main screen. It may take a few seconds for the email to be delivered by the remote system. If configured correctly, DataGate will process the email and send it to the remote radio.
- Once received on the remote radio, select the "Reply" option and send a status code back to the server. DataGate should receive this code, and then forward it as an email to the original sender.

7) Next steps:

- For security, you may want to limit who can send emails to your radios. The most secure option is to limit which IP addresses can connect to the email server. This works if all emails will originate from a known set of servers. Another option is to enable the white list feature, where emails must contain a known "from" address.
- Read the DataGate manual for details on how to configure this and other advanced server settings.