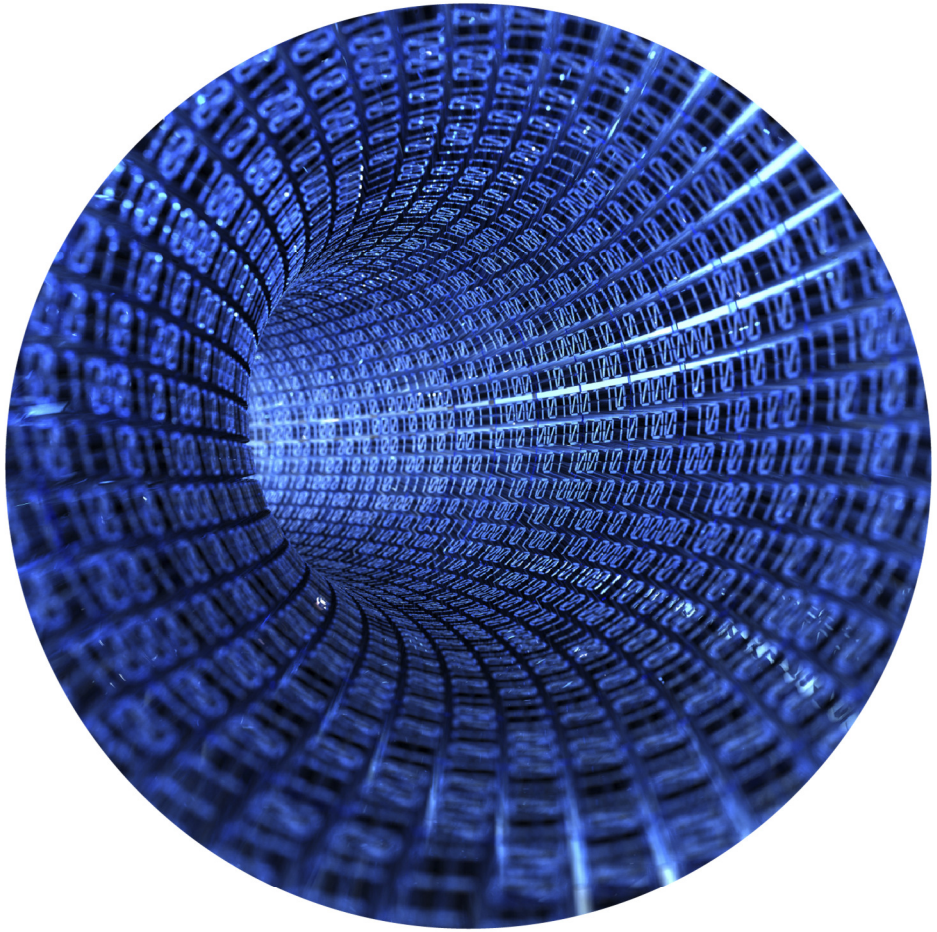
digicentral XML

Administration Guide



V3.00 onwards

Table of contents

digiCentral XML Manager Windows® Software

Minimum Recommended PC Specification

Processor: Intel P4 1.4GHz, AMD Athlon 1.4 GHz
Memory: 512Mbytes
Hard disk: 40 Gbytes
Video Resolution: 1024 x 768
Operating Systems: Windows 7 SP1, Windows 10

Software is available by download or on memory stick only.

1. **Run the setup.exe either from the supplied memory stick or from your download. It will run automatically and a dialog box will appear, click Next. Approve the software licence to commence with the install. Click Next when prompted.**
2. **Finally leave the box labelled 'Launch digiCentral Configuration Manager' ticked and click 'Finish'.**
3. **Now refer to the section entitled 'digiCentral Configuration Manager' on page 5.**

Please note that the software suite within this install consists of two products; digiCentral XML Mananger and digiCentral Configuration Manager which is a Service.

Times shown and recorded in both software is in UTC.

digiCentral Configuration Manager

Services: The core of digiCentral is essentially a Windows Service. You can change the security credentials for the Service and whether the Service is started automatically when the server is restarted.

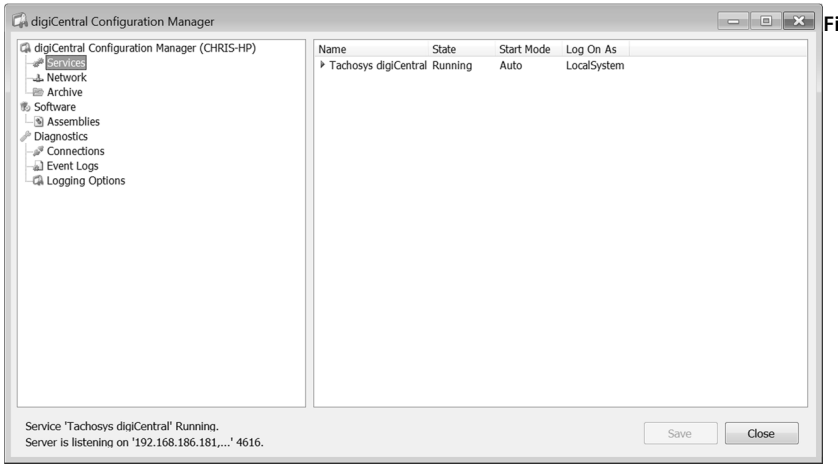


Fig 1.

Network: By default digiCentral automatically uses your machines first IP address. Ensure your digiCentral server is using a Fixed IP address as if you are on a local network this is the IP address your Tachosys devices will use so it should not be able to vary. Likewise if you are using an external IP address this IP will be used in your firewall settings. By default the Port is set to 4616 but you may change this provided remote devices are set to the same Port address. You can force connections on the server to close for unrecognised data to avoid denial of service attacks, see Fig 2 below for details of the default settings.

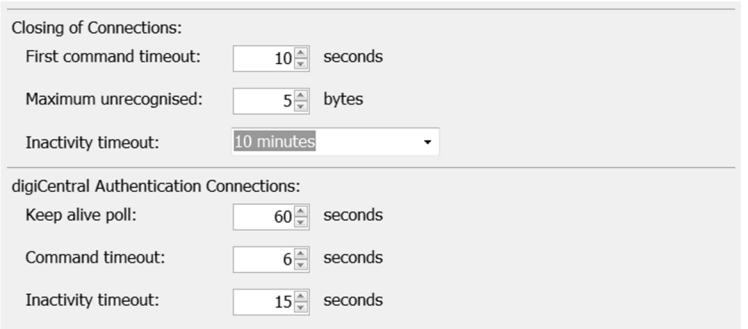


Fig 2.

digiCentral Configuration Manager - Cont.

You will need Start the Service under Services to view the following settings.

Archive: This option allows you to define file locations, for Driver Card and Vehicle Unit files and Log files for troubleshooting. The tick box headed 'Place downloaded files into the sub-folder of the Driver or Vehicle' will by default create a directory for each Driver and each Vehicle for which files are uploaded. Untick this option if you want all uploaded files to reside in a single directory.

Please make a note of the Archive Folder or create a chosen location as this is where all your uploaded files will reside. There is no shortcut in the software to the Archive Folder.

Connections: View currently connected devices.

Event Logs: The Event Log is a set of text files providing detailed information for fault finding and debugging.

Logging: By default digiCentral creates a detailed log for each day. In the case of very busy servers the log file can grow to very large sizes so will need management. Older files should be removed if no longer required.

Please note that this Service must be running for digiCentral XML to function.

digiCentral XML Manager.

This is a separate application found in Start - All Programs - Tachosys -.

Devices: When a Tachosys device tries to connect to digiCentral a record is automatically created in the Devices section.

To see your new device you may need to click the 'Refresh' option at the top of the XML Manager window and find the Serial Number. Double Click on the appropriate row entry and you will see the Edit Device window. You may apply a Group Name to devices which may relate to a customer, depot or global location.

When you allocate a Group Name to a device this will mean that all data that passes via this device will end up in an archive folder with that location name. This helps to logically group data.

A Driver or Vehicle will be allocated the Location associated to their first presentation of a card or vehicle file. You can subsequently move a Driver or Vehicle to another Location but earlier files will remain in their original archive folder.

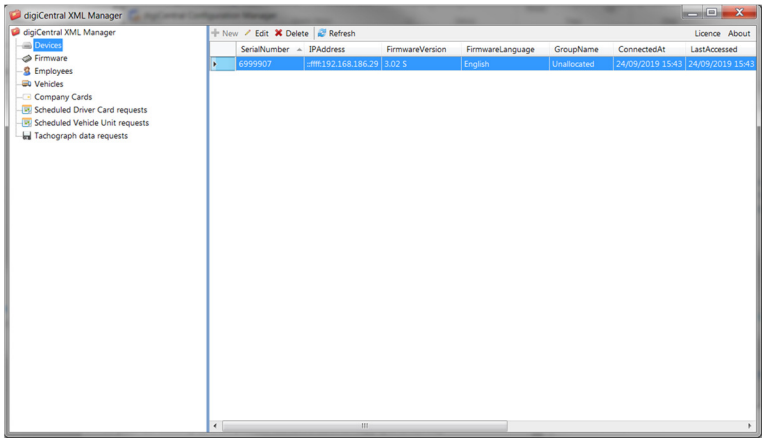


Fig 3.

digiCentral XML Manager - Cont .

Firmware: From time to time devices may need to be upgraded to add functionality or to eradicate undesirable features. A .BIN file can be supplied by your reseller or Tachosys and can be allocated to a specific device or devices. It is important to ensure you are applying the appropriate firmware to a device. The update is picked up by the device when it next connects to digiCentral.

Employees: The first time a Driver Card file is presented to digiCentral a new Employee entry is created. Use the Refresh button at the top of the screen to ensure you are looking at all current entries. You can manually name the driver by double clicking on the entry.

Vehicles: The first time a Vehicle Unit file is presented to digiCentral a new Vehicle entry is created. Use the Refresh button at the top of the screen to ensure you are looking at all current entries. **N.B. You must assign a Company Card to each Vehicle that will be performing remote download.**

Company Cards: For use with digiDL remote download devices. Create a Company Card record for each of your Company Cards. A unique key is generated for each card and this key is then used within 'digiCentral Authenticate' our Company Card hosting application (see page 9 to setup Authentication).

Scheduled Driver Card Requests: This setting is for use with digiDL remote download products only and will place individual download tasks against each driver record and pass these to whichever vehicle tachograph the particular Driver Card(s) is next inserted into. Set the Default schedule to your requirement.

Scheduled Vehicle Unit Requests: This setting is for use with digiDL remote download products only and will allow you to set a global or individual download Schedule for each vehicle together with the data types (TREPS) required. Set the Default schedule to your requirement.

Tachograph Data Requests: Displays remote download tasks that have been generated for devices and their current status.

digiCentral XML Manager - Cont .

Remote Authentication of a Company Card - digiDL

Company Card(s) can be hosted on any PC running our digiCentral Authenticate Configuration software. For each Company Card which is hosted you will need to create a record (see Page 8 - Company Cards). Then in turn you will need to associate each Vehicle Record (see Page 8 - Vehicles) with the appropriate Company Card. The party who is setting up a Company Card for hosting will need the unique Key which is generated when a Company Card record is created in digiCentral XML Manager.

Installing digiCentral Authenticate Windows® Software

Minimum Recommended PC Specification

Processor: Intel P4 1.4GHz, AMD Athlon 1.4 GHz
Memory: 512Mbytes
Hard disk: 40 Gbytes
Video Resolution: 1024 x 768
Operating Systems: Windows 7 SP1, Windows 10

Installing the digiCentral Authenticate Windows® Software

1. Download the software from Tachosys.com - Software Downloads.
2. Double click on the downloaded executable and approve the installation
3. Choose your preferred language and click OK.
4. You will receive a welcome message, simply click 'next'.
5. Read the terms of the Licence Agreement then click on the 'I accept the terms in the Licence agreement' option and then click 'next'. If you choose to not accept the terms the installation will be terminated.
6. Choose the folder in which you wish the software program files to be installed. The default folder is the standard location for Windows® programs. Click 'Next'.
7. Click 'Install' to begin the actual installation. This may take several minutes.
8. Finally leave the box labelled 'Launch digiCentral Authenticate Configuration' ticked and click 'Finish'.
9. Now refer to the section entitled 'digiCentral Authenticate Configuration' on page 10.

We strongly recommend you use either the Tachosys digicard card reader or our WiFi based solution digicard AUT.

digiCentral Authenticate Configuration

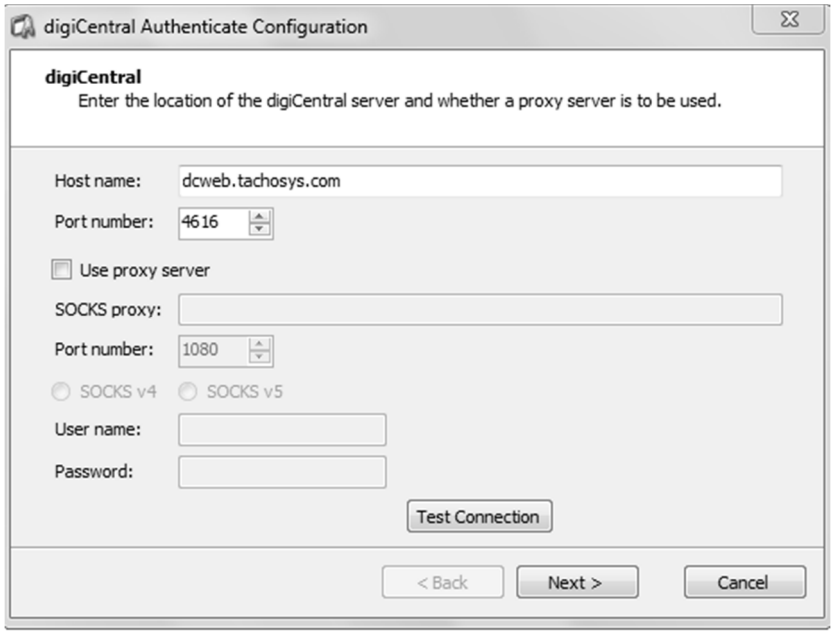


Fig 4

digiCentral Authenticate allows you to publish your Company Card online to facilitate the remote download of your vehicle(s) Digital Tachograph. The publication in this case can be either a different PC on the same network or the same PC which is running digiCentral XML Server. digiCentral Authenticate runs as a service on your PC in the background so the connection to the Company Card is always live provided the service is running.

The settings for digiCentral Authenticate are simple (see Fig 4.) enter the digiCentral Host Name. In this case it will be the IP address of your digiCentral XML Server. In general the Port Number should be left at its default of 4616 unless you are running a customised installation. If your network uses Proxy Server then you will need to activate these settings and add the appropriate entries for your network. The 'Test Connection' button will return a 'Test Successful' message if your settings are correct. Click the 'Next' button when your settings are confirmed.

digiCentral Authenticate Configuration- Cont.

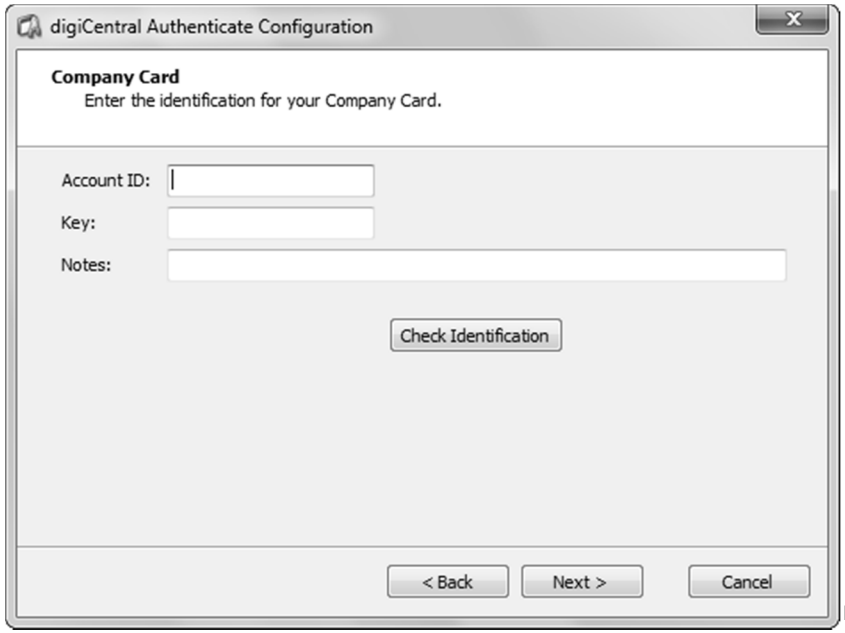


Fig 5

Please note that in order for digiCentral Authenticate to be able to publish a Company Card there must be a corresponding entry already on the appropriate digiCentral XML Server. This entry generates the Key to enter into digiCentral Authenticate.

Account ID: In the case of digiCentral XML Server this field is not used to match with the digiCentral server entry so it can consist of the company card number or your company name or depot name for instance.

Key: this is a unique key generated by the digiCentral XML Server. You can find this key in digiCentral XML Manager under Company Cards. If there are no entries you will have to add one by following the instructions on pages 7 and 8.

Notes: this field can be used to describe the company card. This can be helpful to identify a Company Card in an extensive list.

Use the 'Check Identification' button to verify the settings before continuing.

digiCentral Authenticate Configuration- Cont.

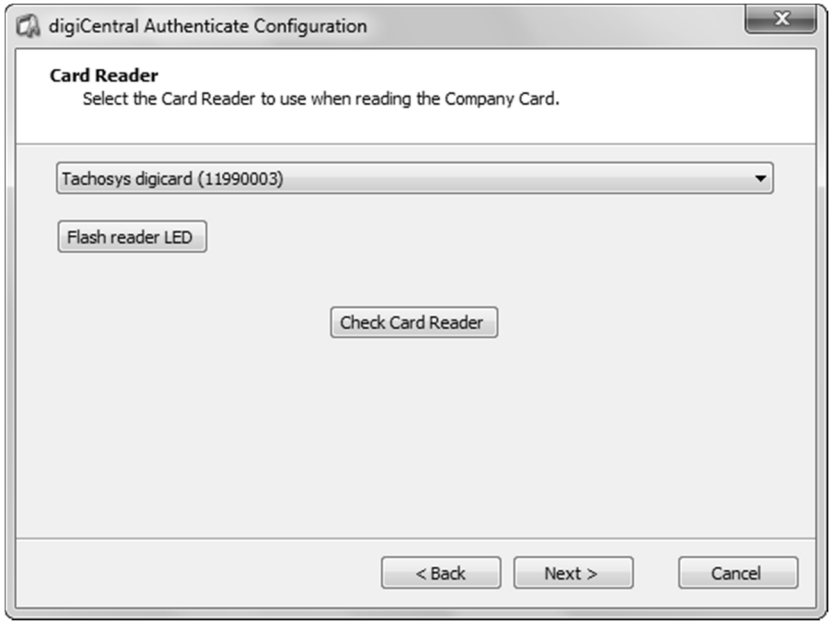


Fig 6

Next you will need to select the card reader that will be used to read the company card that you configured in the previous step.

Connect your chosen card reader to the PC. Select the card reader from the drop down menu and, with the company card inserted, click 'Check Card Reader' to confirm the configuration. The Company Card chip should be closest to the LED of the Tachosys digicard card reader when inserted.

If digiCentral Authenticate is being used in conjunction with a Tachosys digicard card reader (digicard), you can use the 'Flash reader LED' option to locate the specific card reader. This is particularly useful when using multiple card readers.

After successfully checking the reader, click 'Next'.

The final page will confirm the configuration and clicking 'Finish' will complete the installation. You will then be taken to the main digiCentral Authenticate Configuration menu.

Adding Company Cards to reduce contention

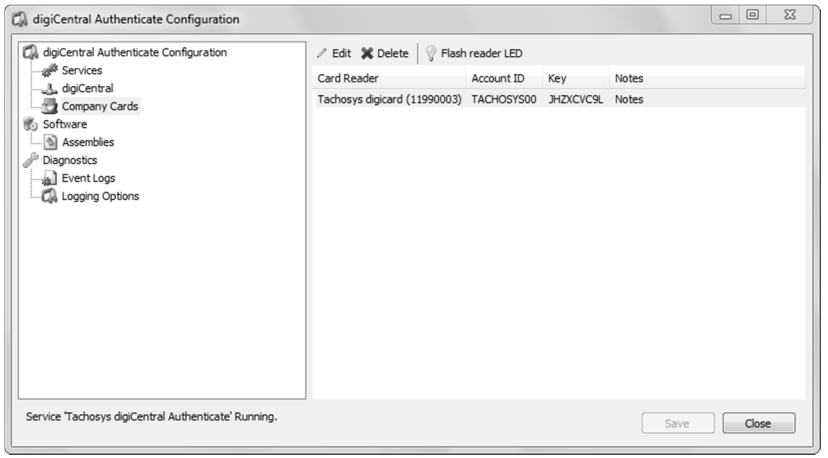


Fig 7

You can add additional Company Cards if you feel there is contention for Authentication in a busy environment. You must first add additional card readers, one card reader for each Company Card.

Open up the digiCentral Authenticate Configuration application under; Start–ALL Programs - Tachosys. Click on 'Company Cards', then select the card reader you want to configure and either double click the reader or click the 'Edit' button above. Enter the Account ID, Key and Notes where appropriate, as supplied by your service provider or digiCentral server manager. Click 'Check Identification' to verify the settings, followed by 'Apply' and 'OK' to finish the configuration.

When you have configured all your card readers, click the 'Save' button in the bottom right of the main window.

Please note that the program runs as a Service. Changes will not come into effect until you STOP and START the Service or you next reboot the PC. You may Stop and Restart the service by clicking on Services and then Right Click the Service entry and select Stop. Right Click the Service and then select Start. You will be prompted to Stop and Start the service whenever a change is made.

You may delete a card entry by highlighting it and selecting the Delete button.

Please note that when a Vehicle is associated with a Company Card the vehicle must have been locked to a Company Card at least in the same number series or the Authentication will fail or the Vehicle File will have no data.

Software Firewalls and Security .

When digiCentral is installed an entry should be created within the Windows Firewall to allow digiCentral to receive and send data. Digicentral uses a custom Port, 4616, for all communication. If for some reason your digiCentral was unable to allow access for 'Tachosys digiCentral' you will need to enable this access (see Fig 8.) Tick the Tachosys digiCentral entry and click OK. If you are using a third party firewall product you will need to make a similar exclusion for either the digiCentral application or specifically for Port 4616.

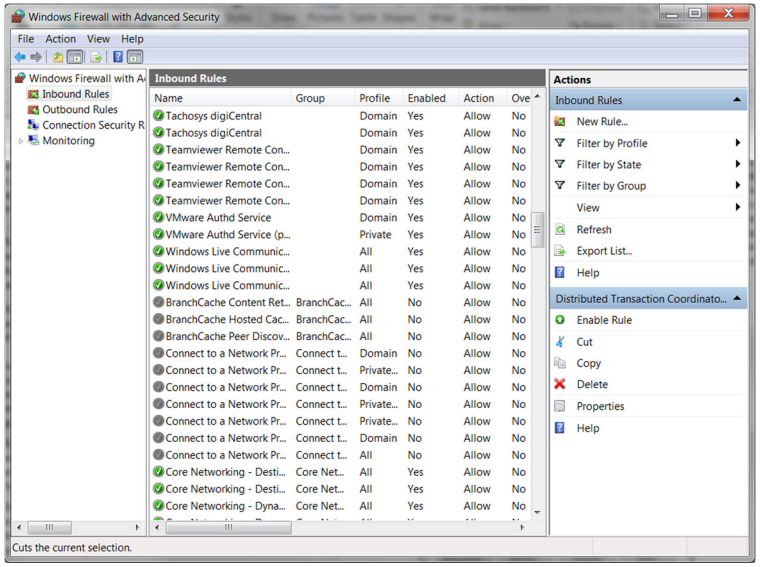


Fig 8.

Web Hosting

digiCentral allows you to accept connections from any Tachosys device using the Internet. You can place digiCentral on your existing Windows based web server or expose a separate PC to the Internet via your Hardware Firewall. Simply ensure you direct all traffic for Port 4616 to your digiCentral server.

You may also use a specific Host Name such as 'MyTachoData.YourServer.com'. This would be defined on your local or remote DNS server. This host name can then be used in all your remote devices. This has the advantage of ensuring that you do not need to change settings in remote devices should your Internet IP address change.

Hardware Firewalls

If you are using Tachosys products in remote locations or as part of an Extranet you will need to make sure that your hardware firewalls allow Port 4616 to pass through to the digiCentral server.

Most connection problems are likely to relate to data packets from the remote Tachosys device being blocked by a hardware firewall either at the remote location or the server location.

Other connection problems are likely to relate to the IP settings on the server or the remote device. It is imperative that both the server and the remote device have a valid IP address, Subnet Mask and Gateway appropriate to the network on which they reside.

On an Extranet careful consideration of how data on Port 4616 will pass through Routers and Hardware Firewalls should be taken.

Troubleshooting

1. Ensure that you have assigned the correct host name or IP address for your digiCentral Server in your remote devices.

2. Ensure that you are using the correct Subnet Mask and Gateway in the Server and Host Devices.

3. Make sure that Port 4616 is not being blocked by a firewall; either a corporate hardware firewall or a PC software firewall.

4. If you have changed the Port Number on which digiCentral listens then make sure that the remote devices are using the same Port. We strongly recommend you do not use a common Port such as 21, 25, 80, 8080 or 110.

4. Make sure that all Vehicles performing remote download have the appropriate Company Card associated with them.

digicentral

TACHO-SYS

Albion House

48 Albert Road North

Reigate, Surrey

United Kingdom

Phone: +44 (0) 208 687 3900

Fax: +44 (0) 208 687 3919

E-mail: info@tachosys.com