

Tinytag connect



User Manual
Tinytag Explorer Connect Software Included

Contents

Introduction	2
Getting Started	4
1.1 What You Need	4
1.2 Software Installation & Setup	5
1.3 USB Receiver Hardware Installation	7
1.4 Ethernet Receiver/LAN Logger Hardware Setup	8
1.5 Ethernet Receiver/LAN Logger Software Setup	9
1.6 Tinytag Connect Gateway Software Setup	12
1.7 Connecting to a System from Another Computer	15
1.8 Enabling the Tinytag Connect Navigation Pane	16
1.9 Radio Logger Setup	17
1.10 Using a Tinytag Connect Device	18
1.11 Logger Icons	19
System Information	
2.1 System Components	22
2.2 System Overview	23
2.3 Gateway Configurations	27
2.4 Data Logging	30
2.5 Data Transmission	31
2.6 Alarm E-Mails	32
2.7 Exporting Data	33
2.8 Modbus	36
2.9 Power	39
2.10 Troubleshooting	42
Radio	
3.1 Radio Specification	44
3.2 Positioning & Mounting Instructions	45
3.3 Installation	47
3.4 System Configurations	49
3.5 Receiver Configurations	51
3.6 Mesh Network Behaviour	53
3.7 Radio Configuration	57
3.8 LED Flash Patterns	60
Ethernet/LAN	
4.1 Mounting Instructions	62
4.2 Alarms	63
4.3 LED Flash Patterns	65
Appendix	
a System Requirements	66
b Software Licence	67
c Regulatory Compliance	67
d Approvals	67
e Further Information	67

Introduction

This guide explains how to set up and run a Tinytag Connect system.

It covers the installation of a system, an overview of how it works and then specific information on the different types of logger the system supports (radio and LAN connected products).

All users are advised to run the latest version of the Tinytag Explorer software. The latest version of the software can be downloaded from:

www.tinytag.info/support

Getting Started

1.1 What you need

To use a Tinytag Connect system you will require the following:

- A copy of the Tinytag Explorer Connect software CD
- A Tinytag Connect activation code (this can be found inside the front cover of this manual)
- A Tinytag Connect device (Radio receiver, loggers and/or LAN logger)
- Associated probes and cables
- Associated power supplies (if required)

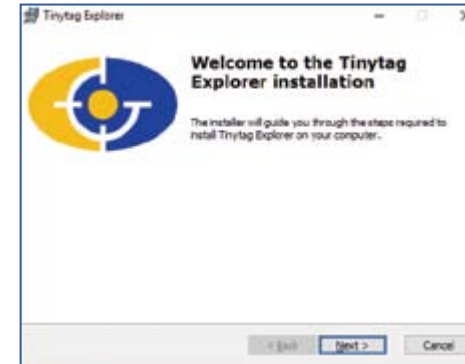
You will also need a computer to run the system; it is recommended that the software be run on a server if possible.

For further information on system configurations, please see the System Information section of this document.

1.2 Software Installation & Setup

For information on system Requirements refer to the Appendix.

Warning! To install Tinytag Explorer, you will need to have Windows Administrator Access rights on the server or computer you are using.



- Place the Tinytag Explorer CD into the CD drive of your PC. The Tinytag Explorer Installer will run automatically after a few seconds and present you with a Welcome screen. If Tinytag Explorer Installer does not run automatically, open Windows Explorer, navigate to your CD drive and double-click **tinytag.msi**.
- Click **Next** to start the installation.
- Review the software's licence agreement and if you accept the terms click **I accept the terms in the Licence Agreement**, then **Next**.
- You will then be asked where you want to install the software (we recommend you use the default installation path) and whether you would like a shortcut for the software to be created on your desktop. Once you have made your choices, click **Next**, then **Install**.
- The software will then install automatically (you may be prompted by Windows to confirm your agreement to the installation). When you see the Installation Complete screen, click **Finish**.
- Once the installation is complete, you will be asked to restart your computer. Click **Yes** to do this.

Starting Tinytag Explorer Connect

To start Tinytag Explorer, click on the desktop icon for the software:



If you didn't create a desktop icon when installing the software, you can start the software by going to:

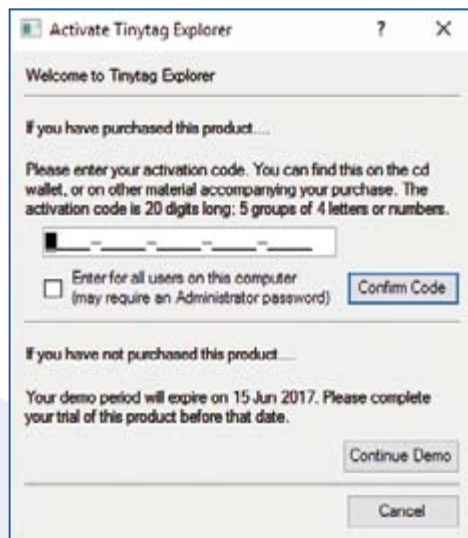
Start >> All Programs >> Tinytag Explorer >> Tinytag Explorer

Activating Tinytag Explorer Connect

The first time you run Tinytag Explorer you will be prompted to activate the software.

Enter the activation code into the box provided and choose whether you want it to be applied to all the user accounts on the computer.

Next click **Confirm Code** and you will see a message to confirm that the code has been accepted.



The activation code for Tinytag Explorer can be found on the inside front cover of this manual. It is a set of 20 characters split up into 5 blocks of 4. If you have lost or misplaced your activation code, please contact your supplier

You may need Windows Administrator access rights to activate the software for all user accounts. If you do not have Administrator access rights, leave the box unchecked and the software will only be enabled for the current user account.

1.3 USB Receiver Hardware Installation

Plug the USB cable supplied with the receiver into a USB port on your computer.

Depending on the version of Windows you are using, you should see a message to say that Windows has detected and is installing a new device.

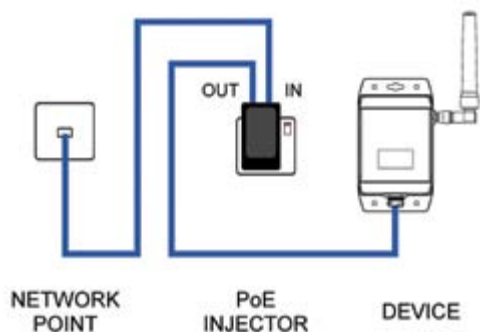
When the installation is complete, plug the cable into the receiver and turn the receiver on.

The receiver should then be located so that it is within range of one or more data loggers (an elevated position may help).

Now go to Section 1.6: Tinytag Connect Gateway Software Setup

1.4 Ethernet Receiver/LAN Logger Hardware Setup

Ethernet receivers and LAN loggers are Power over Ethernet (PoE) devices. If a PoE plug-in injector is supplied, the device should be connected up using Ethernet cables (not supplied) as shown below:



Once connected, turn the device on.

Locate and make a note of the MAC address on the back of the device being installed, this will be needed later.

If the device is being used in a location where moisture or dust is present, the supplied waterproof RJ45 shroud should be fitted over the Ethernet connection.

To fit this, thread the Ethernet cable through the shroud, plug the cable into the device and then screw the shroud into the device.



1.5 Ethernet Receiver/LAN Logger Software Setup

To install a Tinytag Plus Radio Ethernet Receiver or LAN Logger:

On the computer that will run the Master Gateway, install and activate the Tinytag Explorer Connect software, as previously described.

Browse the Tinytag Explorer CD and locate the **LAN** folder

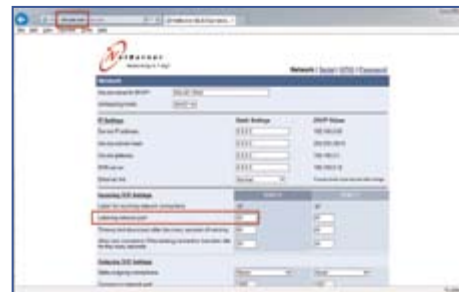
Run the program **VirtualCommPort.exe** and follow the instructions in the onscreen prompts

Run the program **IPsetup.exe**. Devices are listed by their MAC address in the **Select a Unit** section.



Highlight the required device and click on the **Launch Webpage** button.

Make a note of the IP address of the device (from the URL of the web page).



Make a note of the **Listening network port** number for **PORT 0**.

Run the Virtual Comm Port software (this is called **NB Virtual Comm Port** and can be found on the Windows Start Menu under **NetBurner NNDK**) and click **Add**.



Set **Select serial port** to COM100 (if installing more than one device, increment the port number for each successive device used).



In the **Remote host name/port** fields type the IP address of the Ethernet device and the Listening network port number (as previously determined) and click **Add** and **Apply**. The device is now ready to use.

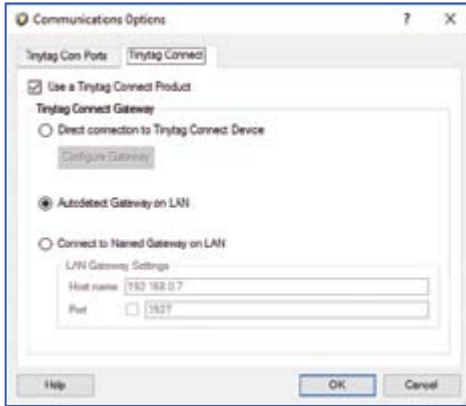


1.6 Tinytag Connect Gateway Software Setup

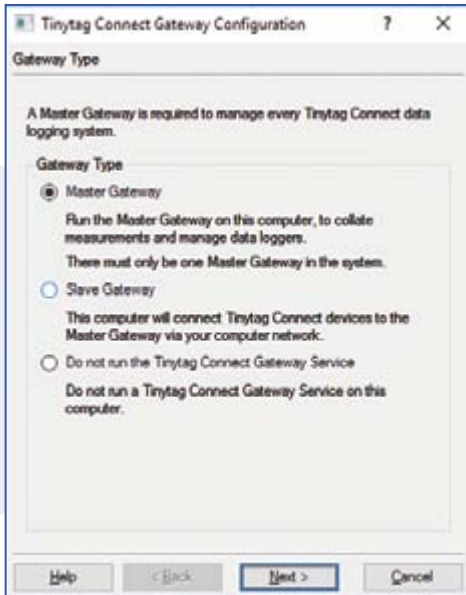
Configuring a Master Gateway

With the receiver or logger plugged into the computer or network, start Tinytag Explorer and go to **Options** and **Communication Options**.

Next, click on the **Tinytag Connect** tab and select **Use a Tinytag Connect Product**, then select **Direct connection to Tinytag Connect Device** and click on the **Configure Gateway** button.

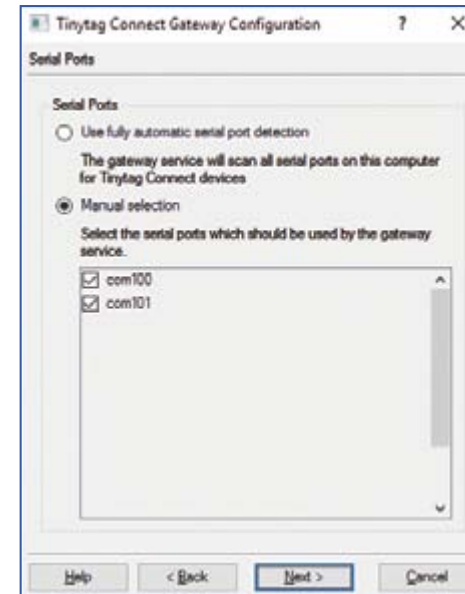


Select **Master Gateway**, then **Next**



Serial Port Set Up

Choose the **Use fully automatic serial port detection** option (recommended) or, if using LAN loggers, select the serial ports configured previously from those listed in the Manual selection section and click **Next**.



E-Mail Alarm Notifications

Tinytag Explorer can be set to send e-mail alerts when user defined logger alarm limits are exceeded (the user account that the system is working on must have a properly configured e-mail account for this to work).

To set the address e-mails are sent to, click the **Report alarms by email** box and then enter the SMTP address for your e-mail server and the recipient's e-mail address.

You can enter multiple e-mail addresses by separating them with a semi-colon.

You can set the system to send automatic e-mail reminders every 24 hours by checking the **Send a reminder email every 24 hours** box.

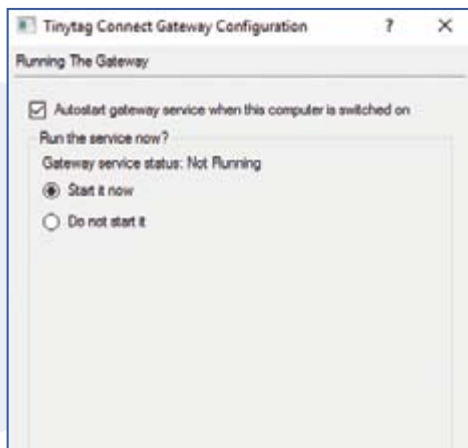
Click **Next**



Running the Gateway

To start the Connect Gateway running, every time the computer is started (recommended), check the **Autostart gateway service when this computer is switched on** box. This will automatically start the gateway service running, and maintain the network, in the event of an unexpected reboot.

To start the radio service, check the **Start it now** box, then **Finish**.

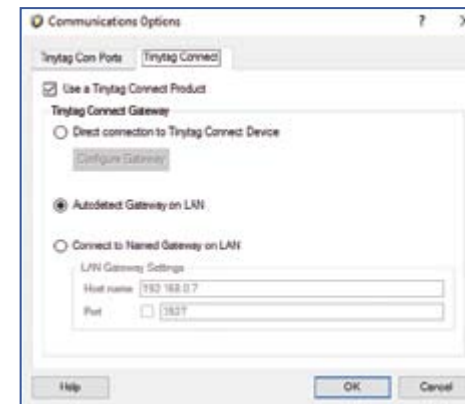


1.7 Connecting to a System From Another Computer

If the computer you have installed the Master Gateway on is connected to a LAN, you can view data and configure the system remotely from another computer on the same network.

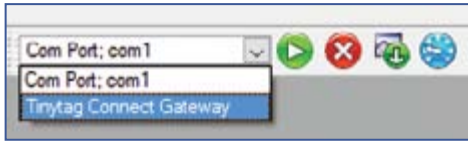
To connect to an existing system from another computer, install Tinytag Explorer on the remote computer and go to **Options** and **Communication Options**. Select the **Tinytag Connect** tab, **Use a Tinytag Connect Product** and then **Autodetect Gateway on LAN**.

If the auto-detection doesn't work, you can specify the address of the computer the Master Gateway is running on in the **Connect to Named Gateway on LAN** option. To do this, enter the **Host name** and **Port**.



1.8 Enabling the Tinytag Connect Navigation Panel

On the Tinytag Explorer Connect toolbar you will now see a new drop-down menu. Select the **Tinytag Connect Gateway** option.



A navigation panel will then appear on the left-hand side of the screen and after a few moments the receiver or any LAN logger(s) connected to the system will start listing.

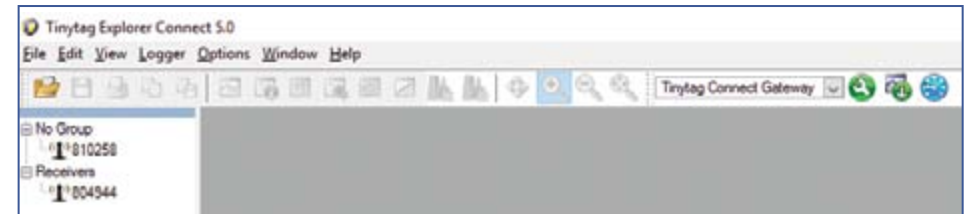


1.9 Radio Logger Setup

Once Tinytag Explorer has been installed and the receiver set up, data loggers can be turned on.

To minimise the time necessary for the units to connect, start turning on the loggers closest to the receiver first and then work outwards.

To turn a logger on, press and hold the switch on the unit until you see its LED light green. The LED on the unit will then flash red until the logger has found its place in the mesh network, at which point it will then start to flash green.



In most cases loggers will find their place in the network and be listed in the navigation pane in Tinytag Explorer within a few minutes, but depending on the size and complexity of the network, it may take a little time for all loggers to be listed.

Be patient whilst the meshing process is taking place!

If a logger doesn't show up after a few minutes, the system should be left to configure itself; moving or resetting loggers during the initial meshing will slow the process. For some large or complex installations it may be necessary to wait an hour or more for the initial connection of loggers to the system.

For more information on radio installation see section 3.3

1.10 Using a Tinytag Connect Device

To work with a Connect device, right click on it and select an option from the menu that appears.



Configure



Use this to change a device's settings

Get Data



Use this to view data from a device

Current Readings



Use this to view what a device is currently reading. Further information on these and other options can be found in the Tinytag Explorer Help file by going to **Help** and **Contents**.

1.11 Logger Icons

The navigation pane in the Tinytag Explorer Connect software allows the user to see the status of any logger at a glance. The icon for a given logger or receiver can indicate whether the device is in contact with the system, whether the device is transmitting data, whether an alarm is active and its battery status.

The table below is a guide to what these icons mean.

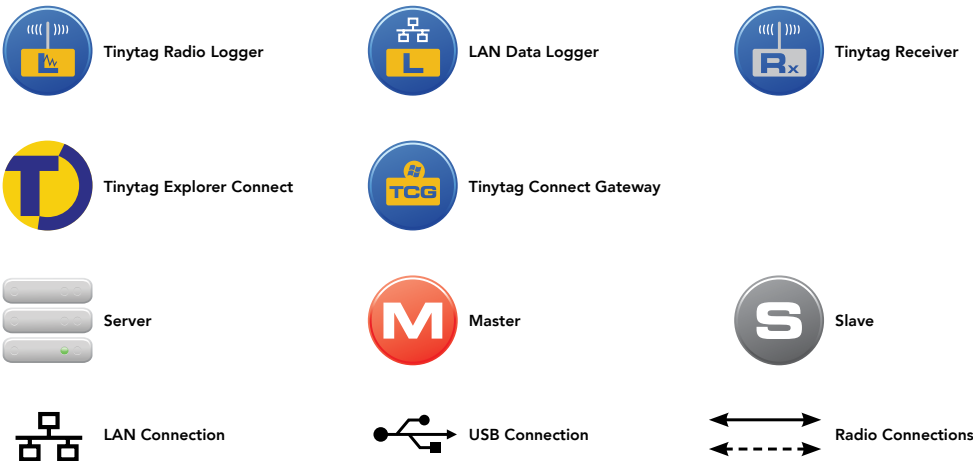
Radio	LAN	Status
 (Solid)	 (Solid)	Good Communications
 (Radio Waves Flashing)	 (Flashing)	Downloading Data
 (Flashing)	 (Flashing)	Alarm Active
 (Flashing)		Updating Device Settings
 (Flashing)		Low Battery
 (Solid)	 (Solid)	Out of Contact
 (Flashing)		Problem*

*The device connected to the system is not being recognised, check you are running the latest version of the Tinytag Connect software. If in doubt, please contact your supplier or Gemini Technical Support (contact details can be found at the end of this manual).

System Information

2.1 System Components

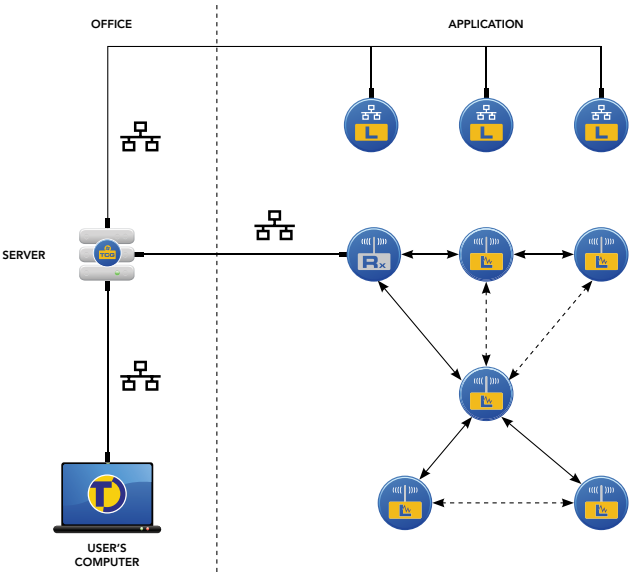
Below is a key to the components used in the Tinytag Connect system that you will see in various places throughout this manual.



2.2 System Overview

Introduction

A Tinytag Connect system can be made up of a combination of radio and/or LAN connected data loggers, but every system has the same core components; the Tinytag Connect Gateway, that manages the collection of data from the loggers; the Tinytag Explorer Connect software, which allows users to view the data and configure their loggers and the data loggers themselves (additionally, in radio systems, a receiver is required to forward data from loggers to the Connect Gateway).



Both the Tinytag Connect Gateway and the Tinytag Explorer Connect software are installed at the same time from the Tinytag Explorer CD.

Tinytag Connect Gateway



The Tinytag Connect Gateway is a Windows service which runs in the background on a computer. The Connect Gateway manages data from loggers connected to it and makes this data available for viewing in Tinytag Explorer.

There are two types of Connect Gateway; a Master Gateway, which runs and manages a system, and a Slave Gateway, which is used to forward data from USB receivers or remote sites to a system's Master Gateway. Every system must have a Master Gateway, but Slave Gateways are optional and only need to be installed in specific circumstances.

For more information on Slave Gateways, see section 2.3: Gateway Configurations

On a networked system, it is preferable for the Master Connect Gateway to be installed on a server, as they usually run continuously and are routinely backed up, but it can also be installed on a PC if required (in this instance, the computer ideally needs to be left running continuously).

Master Connect Gateways can also be installed on stand-alone computers, if required, using a USB radio receiver to connect to a radio network. This type of configuration is preferable if a system needs to be run on a computer that is separate from existing IT infrastructure.

The Connect Gateway is configured to start running when the computer is turned on, and stores data from loggers in individual files using a proprietary file format. The gateway then makes the data it is managing available for viewing on any networked computer running the Tinytag Explorer Connect Software.

As well as making data available for viewing in Tinytag Explorer, data can also be exported from the Connect Gateway directly using either the Modbus protocol, or in csv files via a http link.

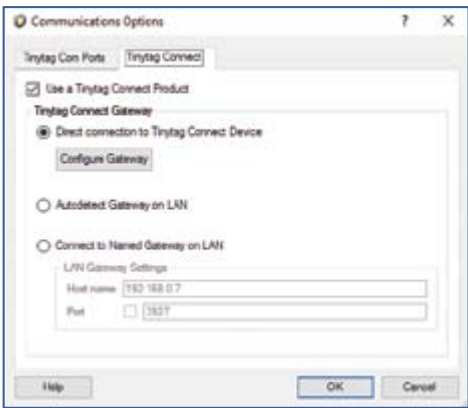
The Connect Gateway can also be configured to send e-mail alerts when a property goes out of specification.

The Tinytag Connect Gateway is configured through the Tinytag Explorer Connect software.

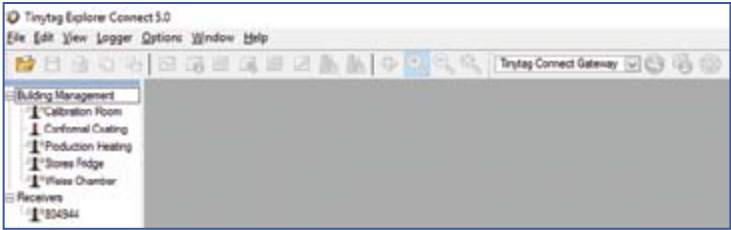
Tinytag Explorer Connect Software

Tinytag Explorer is the software that is used to view data from and work with all Tinytag products. The Connect version of the software provides extended functionality, allowing users on the same network to view data from the system on their own computer.

The Connect version of the Tinytag Explorer uses a different activation code from the standard version of the software to enable Connect functionality. This activation code adds a **Tinytag Connect** tab to the **Options >> Communication Options** dialog box which allows the user to configure the Tinytag Connect Gateway Service.



Tinytag Explorer Connect also has a navigation pane that shows the status of individual data loggers, allowing users to see at a glance the status of their system and whether there are any issues, such as an alarm or low battery, that need to be addressed.



The software presents data in graphs, but it can also be viewed in a table of readings and summary views detailing the logger's settings, daily min/max and average data are also available. Graphical data from the software can be easily exported as an image, for use in presentations and report writing, and in a table for further analysis in third-party spreadsheets or databases.

The software also allows data from non-Connect data loggers to be combined into the same graph as data from a Connect system, using the software's overlay feature.

Loggers

Every Connect system requires at least one data logger to collect the actual data.

Data loggers are electronic devices that record data using different types of sensors. By default, they transmit this data to the Connect Gateway as it is recorded, but they also hold a copy of the data locally in case problems arise.

If the logger cannot see the Connect Gateway for any reason, it will record data locally until the problem is resolved and the data can be transmitted.

Radio loggers connect to the Connect Gateway via a receiver that is either connected to the Gateway via a LAN connection, or directly into the computer running the system via USB. Radio loggers talk to each other to form a mesh network. The advantage of a mesh network is that it is robust and can route data around obstacles.

For more information on mesh network behaviour, see section 3.6: Mesh Network Behaviour

LAN loggers connect to the Connect Gateway across a LAN connection.

Receivers

Receivers are a radio system's point of contact with the Connect Gateway. They collect information from loggers and forward it to the Connect Gateway and they send configuration information to the loggers from the Connect Gateway. Additionally, receivers also manage the flow of data in a mesh network and, in the event of a power failure to the Connect Gateway, they will keep the mesh network together allowing faster reconnections and transmission of data when power is restored.

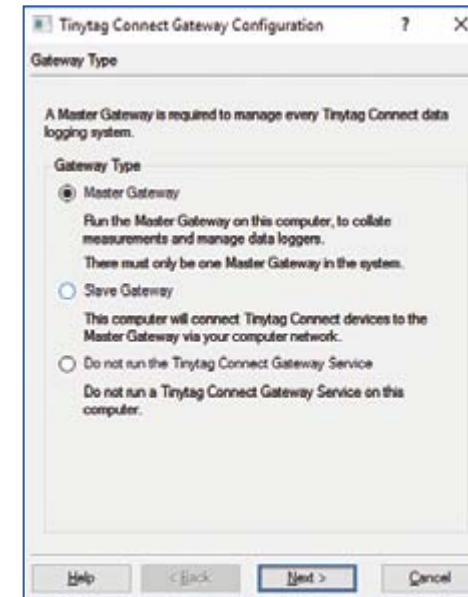
Receivers can be used in a variety of configurations. These are described in a later chapter.

For more information on receiver configurations, see section 3.5: Receiver Configurations

2.3 Gateway Configurations

Introduction

There are two types of Connect Gateway; a Master Gateway, which runs a system, and a Slave Gateway, which can be setup to forward data to a Master Gateway from another computer.



Every system must have a Master Gateway, but Slave Gateways are optional and are generally used to make a system more flexible.

Slave Gateways

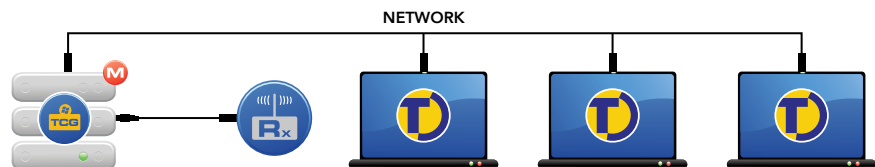
Slave Gateways are typically used where:

- Data is being collected from more than one site that are all connected on the same company LAN. For example, a company may have three sites; a head office and two satellite sites, and monitoring is required at all three. In this example, it is preferable to have a Master Gateway running on a server at the head office, with a computer at each satellite site running a Slave Gateway. The Slave Gateways then forward data from their local networks onto the Master Gateway, allowing anyone running Tinytag Explorer Connect to see data from all three sites.
- If USB receivers are being used, they have to be plugged directly into a computer and that computer has to run a Slave Gateway to get the data back to the system's Master Gateway.

The Slave Gateway relays data between any connected radio receivers or LAN loggers and the Master Gateway. No data is stored locally and it is a very lightweight program.

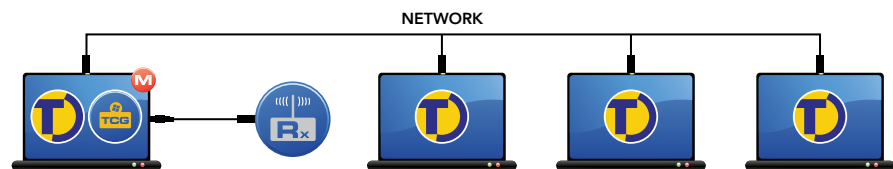
Common Configurations

Server



A Tinytag Connect Master Gateway is installed on a server, with a receiver for a radio network, or a number of LAN loggers, connected to it. The Connect Gateway then makes data available to other users on the same network for viewing in the Tinytag Explorer Connect software. This is the recommended configuration for a system because servers are usually on all of the time and they are also backed-up regularly, making the system more robust.

Dedicated Computer



Basically the same as the Server configuration, but with the Master Gateway running on a computer. This configuration might be used when only a few users in a large company need to work with a system. A receiver or a number of LAN loggers are connected to a computer and any computers on the same network, with a copy of Tinytag Explorer Connect installed, can also work with the system.

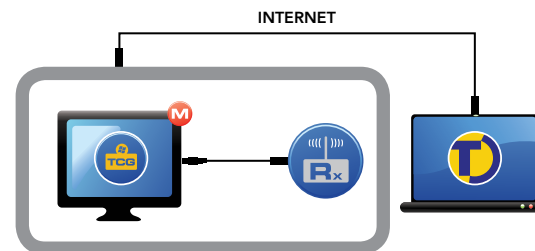
Standalone



The Connect Gateway is run on a non-networked, stand-alone computer with a USB receiver collecting data from a radio network. Although this prevents remote access to data by other users, this configuration allows a system to be kept separate from other IT infrastructure, which can sometimes be desirable. This configuration does not support LAN loggers.

Off-Site/Remote Access

The Connect Gateway is installed on a computer with internet access at a remote site and the user works with the data remotely using VPN access to the computer.



General

Ideally a Tinytag Connect Gateway should be left running continuously to allow it to collate data from loggers as it is being recorded. No measurements will be lost if the computer is shut down for up to 2 weeks (if using the default 10 minute logging interval the loggers are set for when supplied), however this will affect battery life and there will be a delay in displaying new measurements, due to the need to collect the saved data, when the system is restored. If a Connect Gateway is shut down, it will determine what data a logger holds that it hasn't stored and arrange for it to be transmitted (this ensures that no data is permanently lost).

For best performance, ensure the **Autostart service when the computer is turned on** box is checked when setting up a Gateway (this should already be selected on new installations). This ensures that the Tinytag Connect Gateway will start running as soon as a computer is turned on; reducing the delay in fetching the data the gateway hasn't downloaded. Enabling this option also ensures a Tinytag Connect system will start running again in the event of a power cut.



2.4 Data Logging

No stopping

Tinytag Connect data loggers will start logging as soon as they are switched on. They do not need to be 'launched'. It is possible to change the configuration of a logger (logging interval, channels labels, groups, etc.) without stopping the logging process.

Time zones

Tinytag Connect data loggers store a timestamp with every measurement. This timestamp is traceable to GMT.

Note that Tinytag Explorer will display this timestamp in your local time zone. This means that timestamps displayed on the graph or readings view will be different for users in different time zones, or will change when users move in and out of daylight savings time.

Timestamps are not affected in any way by the time zone of the user who installed or configured the data logger.

Current Readings

If a logger has a good connection with the Connect Gateway, live readings will be shown in black and readings will update every few seconds.

If communications with a logger are poor, or the logger is out of contact with the system, the last logged values will be shown in grey.

The update interval of live readings will be extended when viewing readings from multiple devices (or if multiple users are viewing current readings simultaneously).

Note: The Current Readings feature in Tinytag Explorer has been designed as a diagnostic tool to check loggers are working correctly, and to aid troubleshooting a system that is having problems. Extensive use of this feature will affect battery life in radio loggers due to the extra radio activity so it is not recommended for day-to-day use.

2.5 Data Transmission

Data Organisation

Every measurement is written to memory and transmitted to the Connect Gateway as soon as it is taken. Every measurement transmission carries the logger serial number and a measurement sequence number, therefore it is impossible for measurements to be mixed up between devices or recorded in the wrong order.

The Connect Gateway uses these sequence numbers to control retransmissions. If the sequence numbers are not consecutive then it requests a retransmission to cover the gap.

If the Connect Gateway is aware of a gap in the data from a logger when it is viewed in Tinytag Explorer then it will ask the user whether they want to see the data so far, or wait until the gap has been filled in.

Data can be transferred from multiple loggers simultaneously. It will prioritise loggers that Tinytag Explorer is waiting for, and loggers that are nearly complete.

If the data gap cannot be filled in because too much time has passed (approximately two weeks in the default configuration) and the logger has overwritten its memory then Tinytag Explorer will leave a gap on the graph.

Radio data is transferred at approximately 6kb per minute.

2.6 Alarm E-Mails

When configuring the system, alarm notification e-mails can be enabled. When an alarm is triggered, an e-mail will be sent to the address(es) provided during setup, detailing the logger and probe that triggered the alarm.

If an alarm is configured, the logger samples the parameter every few seconds. If an alarm value is exceeded, an alarm indicator will be transmitted to the Connect Gateway immediately, and this will show up in Tinytag Explorer straight away.

However, the Connect Gateway does not send an alarm e-mail warning immediately; it delays for five minutes in case another logger should raise another alarm so that it can deliver all the alarm warnings in one e-mail.



The screenshot shows the 'Tinytag Connect Gateway Configuration' window with the 'Alarm Notifications' tab selected. The 'Report alarms by email' checkbox is checked. Under 'Email Settings', the 'SMTP Server' is 'mail.gemini-data.com', 'Login Name' is 'connect@...', 'Login Password' is masked with asterisks, and 'Port' is '25'. The 'Use TLS' checkbox is unchecked. The 'Recipient Email Addresses' field contains 'help@gemini-data.com' with a note '(use a semicolon to list multiple recipients)'. At the bottom, there is an unchecked checkbox for 'Send a reminder email every 24 hours' and navigation buttons: 'Help', '< Back', 'Next >', and 'Cancel'.

2.7 Exporting Data

The data stored by the Connect Gateway is held in propriety format data files that have a .jf extension, that open directly in Tinytag Explorer. Data from a Connect system can also be accessed directly from the gateway using the Modbus protocol or in CSV files over http.

Modbus

The Connect Gateway provides a standard Modbus over TCP interface, providing read-only access to a data logger's configuration and instantaneous measurements (instantaneous measurement means the last logged measurement received from the logger).

Modbus may be a convenient option for software which uses Tinytag Connect loggers as part of an industrial process control or SCADA system.

For more details about Modbus, see section 2.8: Modbus

CSV Files

Connect data loggers transmit measurements as they are recorded and these are collated and stored by the Connect Gateway. The Connect Gateway provides access to historic logged measurements for third party software by downloading CSV files over http.

The URLs for these files are listed on the Connect Gateway interface page and there is one CSV file per logger.

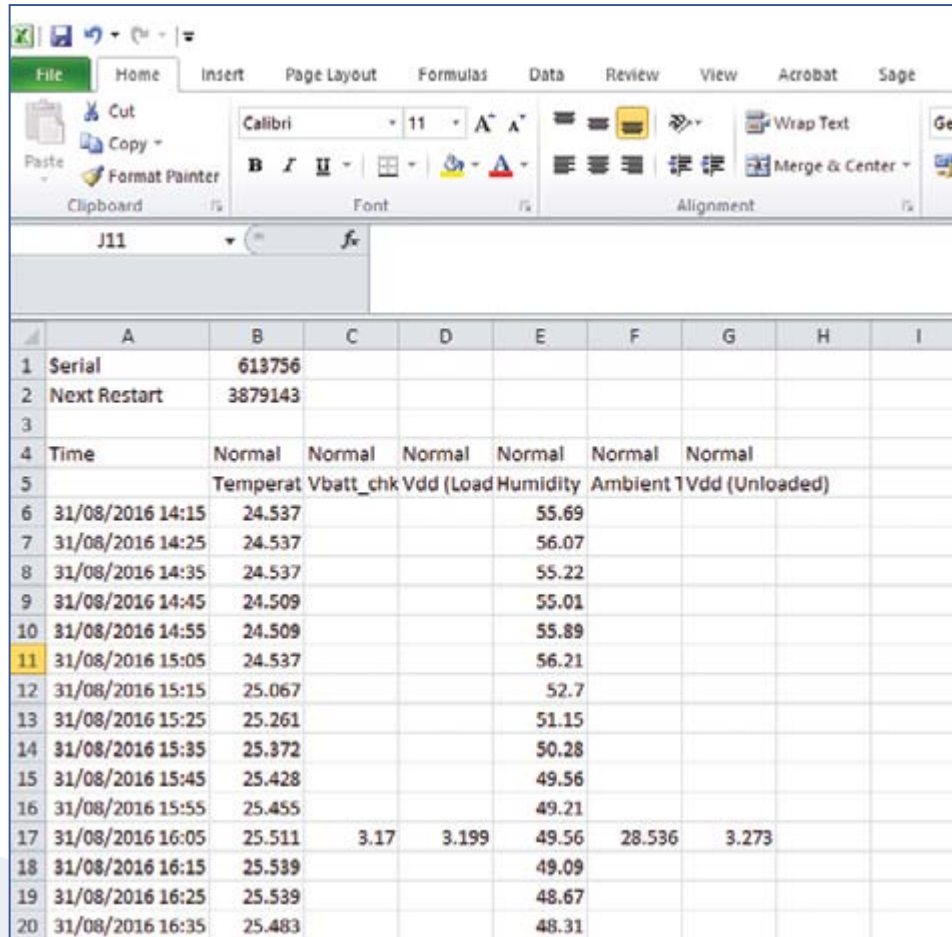
To access these files, click on the **Tinytag Connect Gateway Status: Connected** message in the bottom right corner of Tinytag Explorer. The pop-up panel that appears should say **Connection Established to Tinytag Connect Gateway**. Clicking on the blue **Tinytag Connect Gateway** text will open the gateway's interface page in your default web browser.

The **Exports** tab at the top of the page lists all files available to download by the serial number of the device. There are two columns for each logger; the left-hand column is raw data that opens directly in Tinytag Explorer. The right-hand column will download the data as CSV file.

CSV export files are generated when the link is opened; they do not exist as separate files that are updated as recordings are received by the gateway. The data held in these files is a snap-shot of the data recorded to the point when the link was opened.

The following example was downloaded from:

http://hostname:3927/Exports/all_readings/613756.csv



	A	B	C	D	E	F	G	H	I
1	Serial	613756							
2	Next Restart	3879143							
3									
4	Time	Normal	Normal	Normal	Normal	Normal	Normal		
5		Temperat	Vbatt_chk	Vdd (Load	Humidity	Ambient	TVdd (Unloaded)		
6	31/08/2016 14:15	24.537			55.69				
7	31/08/2016 14:25	24.537			56.07				
8	31/08/2016 14:35	24.537			55.22				
9	31/08/2016 14:45	24.509			55.01				
10	31/08/2016 14:55	24.509			55.89				
11	31/08/2016 15:05	24.537			56.21				
12	31/08/2016 15:15	25.067			52.7				
13	31/08/2016 15:25	25.261			51.15				
14	31/08/2016 15:35	25.372			50.28				
15	31/08/2016 15:45	25.428			49.56				
16	31/08/2016 15:55	25.455			49.21				
17	31/08/2016 16:05	25.511	3.17	3.199	49.56	28.536	3.273		
18	31/08/2016 16:15	25.539			49.09				
19	31/08/2016 16:25	25.539			48.67				
20	31/08/2016 16:35	25.483			48.31				

The first few lines of this file is a header which consists of:

- Various properties, name and value in the first two columns, for example 'Serial' and 'Next Restart'.
- A blank line.
- Two rows of titles for measurement columns. For example "Maximum" and "Temperature". For loggers that do not support maximum and minimum readings, this row will contain "Normal" rather than "Maximum".

Measurements are in the subsequent rows after the header.

The first column contains the time stamps. Timestamps always use GMT time, and are written in ISO format (yyyy-mm-dd hh:mm:ss), but may be presented differently in the program you use to open the file based on your Windows preferences. The second and subsequent columns contain measurements.

Note:

- Measurements are listed in time order.
- If there is a gap because of a communications delay then measurements will be held back until the Connect Gateway has been able to fill the gap in. (i.e. guaranteed to preserve time order)
- Multiple users can access the CSV data without interfering with each other.

Note: In rare cases, it is possible that one row of measurements is split between consecutive transfers. The last line of one transfer will contain half of the expected measurements. The first line of the next will contain the same timestamp, and the other half of the measurements. This will happen if the transfer is started part way through the Connect Gateway receiving measurements from the logger.

Exporting Incremental Data

The CSV files linked from the **Exports** page will always create a file containing every measurement, which is inefficient and cumbersome for systems which need to keep up to date by tracking new measurements as they arrive. In order to download only new measurements it is necessary for a custom software solution to keep track of the Next Restart value from its previous download, and add this to the URL which is downloaded. For example, the measurements received after the snapshot shown above can be downloaded from:

http://hostname:3927/Exports/all_readings/613756.csv?restart=3879143

Note: This URL – ending in "?restart=3879143" – does not appear anywhere in the Connect Gateway web pages. It must be generated by the software solution which wants to perform incremental transfers.

Proprietary Connect Gateway Protocol

The Connect Gateway supports a simple text-based proprietary network protocol which provides read-write access to logger configuration. This is the protocol used by Tinytag Explorer to access the Connect Gateway.

2.8 Modbus

Properties and Registers

The Modbus protocol provides read/write access to numbered 16-bit registers. Connect loggers natively use numbered properties which are somewhat similar to Modbus registers.

The Connect Gateway automatically translates between these two systems. The translation primarily involves changing data types. Modbus registers are always 16-bit integers, while Connect logger properties have high-level data types. For example, the logger description is a length limited string. Logging interval is a 32-bit integer.

This property-to-register mapping is generated automatically. Different types of device have different properties; therefore they may have different registers too.

Devices

The web view in the Connect Gateway site includes a **Devices** tab which contains an index of all devices currently or recently connected to the Connect Gateway, with links to a page showing detail for each individual device. Near the top of these device detail pages is a link labelled Modbus Registers which links to a page showing:

- Which logger properties are exposed as Modbus registers
- Which Modbus address is used for each property
- How many Modbus registers are used for each property. For example, 32-bit properties will be spread over two 16-bit registers.

Expected Values

The **Modbus** tab on the Connect Gateway web view shows the current value of every register on every device.

The **Properties** tab shows the equivalent in high-level data types.

Unit Identifiers

The Modbus protocol supports up to 254 devices, identified by a unit identifier. Unit identifiers are automatically assigned to device serial numbers.

The unit identifier of each device is shown on the **Modbus** tab page of the Connect Gateway interface. These values are stored under the Tinytag Explorer program files, in json format, in the file:

```
\\Program Files\\Tinytag\\Tinytag Explorer\\var\\storage\\units.db
```

It is possible to manually adjust the assignment of unit identifiers to serial numbers by stopping the Connect Gateway, editing this file, and restarting.

It is also possible to clear the current assignments by stopping the Connect Gateway, deleting this file, and restarting. This may be necessary at sites where more than 254 devices have been used and decommissioned, because the unit identifiers will remain reserved for the decommissioned devices.

Function Codes

The Connect Gateway supports only Modbus function code 0x03: Read Holding Registers.

32-bit Values

All values wider than 16 bits are mapped onto multiple 16 bit registers.

The request packet for function code 0x03 (Read Holding Registers) includes a byte containing the “quantity of registers” to be read. This is interpreted as the number of 16-bit words which should be transferred.

For example, when requesting the 32-bit value starting at address 50688, this “quantity of registers” byte should contain the value 2. The response will contain the content of two registers: four bytes.

Freshness

Most registers have a corresponding register containing the number of seconds since the property was refreshed from the device. Some properties are refreshed daily, others are never refreshed. Properties containing ‘current measurements’ are updated every time a measurement is received from the device.

These registers will contain the value 0xFFFF if some error occurred in processing that property. The maximum normal value (for example, if the property was refreshed more than 65535 seconds ago) is 0xFFFE.

Device Connection

No Modbus interaction is possible until a device is fully connected. That is, when the device leaves the Connecting group in Tinytag Explorer Connect’s Navigation pane, and the device’s state is listing as HAPPY in the **Devices** tab of the Connect Gateway interface.

It is not possible to read any registers from a device which is not yet fully connected. The Connect Gateway will return an Illegal Data Address error code.

At this point, the Current Readings registers may not yet have been refreshed, and will all contain 0xFFFF. For the floating point registers, this corresponds to NaN. These registers will be refreshed when the first measurement is received, at the next logging interval.

Missing Properties

The Connect Gateway will return an Illegal Data Address error code if the requested property has not been fetched, or is missing from the device. This should not happen under normal circumstances, but may occur if:

- Requesting a register corresponding to a diagnostic/debugging property, and the Connect Gateway is not in a diagnostic mode.
- The device does not contain an expected property. The device's characteristics are inconsistent with its driver in the Connect Gateway. This may happen if using prototype devices, or a pre-release version of the Connect Gateway.

The device detail page can be used to confirm exactly which properties have been received by the Connect Gateway.

Concurrent Connections

The Connect Gateway enforces a limit of no more than 4 concurrent Modbus TCP connections.

There is no additional limit to concurrent Modbus transactions.

TCP connections are closed after being idle for 10 seconds.

Modsak

Modsak is a third party Modbus diagnostic tool, available at:

<http://www.wingpath.co.uk/modbus/modsak.php>

Gemini Data Loggers is a user of Modsak, but does not endorse or support this product.

The **Device State** page in the Connect Gateway interface contains a download link for a Modsak configuration file. When opened, this configures Modsak to show most registers from that device, and, when you press the Start button, it continuously polls for new values.

Note that Modsak cannot format Modbus registers as text strings; therefore these registers are omitted from the download Modsak configuration line.

Also note that Modsak does not distinguish signed and unsigned values: all numbers are formatted as signed in Modsak, which may or may not be correct.

2.9 Power

All Tinytag Radio and LAN data loggers and receivers are fitted with alkaline batteries that are widely available and cheap to replace. These batteries are either the main source of power for the device, or provide back-up power in the event of the devices primary power source going down.

Radio Data Loggers

Radio data loggers are battery powered devices with an option for being mains powered, through a plug-in power supply, if required.

When powered from batteries the loggers can be easily moved and relocated as monitoring requirements change. The battery life of a logger, when set to the default ten minute logging interval it is supplied with, will be typically a year.

When powered from the mains, the batteries in the logger are used as a back-up should the power to the logger fail. If this happens, the batteries will keep the logger recording and transmitting (if the computer running the system is also affected by the power cut, the loggers will record data locally until the problem is resolved, the data will then be transmitted).

Plus Radio data loggers and the USB receiver are fitted with 2 x C (LR14) 1.5V batteries.

Ultra Radio data loggers are fitted with 2 x AA (LR6) 1.5V batteries.

Ultra Radio Receivers

Ultra Radio USB receivers are mains powered devices that are powered through a plug-in power supply.

This receiver also has back-up batteries that will allow it to maintain the radio mesh network it is a part of in the event of a problem with the power supply from the computer.

Ultra Radio receivers are fitted with 2 x AA (LR6) 1.5V batteries.

Plus Radio USB Receivers

Plus Radio USB receivers are powered from their USB connection.

They are also fitted with batteries that will allow the receiver to maintain the radio mesh network it is a part of in the event of a problem with the power supply from the computer.

Plus Radio USB receivers are fitted with 2 x C (LR14) 1.5V.

LAN Data Loggers and Ethernet Receiver

Plus Radio Ethernet receivers and LAN data loggers are Power over Ethernet (PoE) devices.

A plug-in PoE injector (part number ACS-0041) is supplied with all LAN data loggers and the Plus Radio Ethernet Receivers. If a number of LAN devices are going to be used, an Ethernet hub that provides PoE should be considered.

LAN data loggers and the Ethernet Receiver are also fitted with back-up batteries to keep them recording in the event of PoE failure.

LAN data loggers and Ethernet receivers are fitted with 2 x AA (LR6) 1.5V batteries.

Lithium Batteries

If a longer battery life or a wider temperature operating range is required, lithium battery versions of the Plus Radio products can be supplied.

Mains Power

Mains powered Tinytag devices should only be used with Tinytag power supplies.

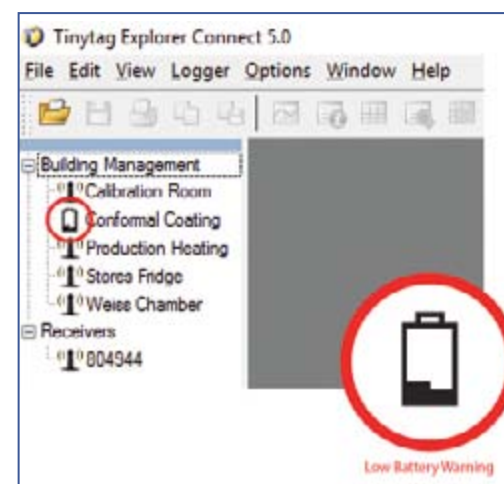
Ultra Radio loggers and receivers should only be used with the ACS-0005 power supply
Plus Radio loggers should only be used with the ACS-0044 power supply

Low Power Warnings

Tinytag Explorer Connect displays a low battery flashing icon in its navigation pane when the battery voltage of a device is below a critical threshold.

Battery voltage in alkaline powered devices can be temperature dependent. If used outside, on very cold nights, when batteries start to go flat it is possible that loggers will show a low battery warning, but then recover during the day when the temperature rises again. This may continue for several weeks before the low battery indicator remains on.

Low battery warnings are not included in the systems e-mail alerts.



The Effect of the Mesh Network (Radio Only)

The battery life of radio loggers is typically 12 months in an average sized radio system (when loggers are set to record on the default ten minute logging interval they are supplied with).

The effect on battery life of the mesh network primarily depends on the number of radio messages that a logger will hear. Battery life will be slightly shorter if:

- A network has a large number of loggers
- Loggers are set to record at a fast logging interval
- Loggers are close to a receiver in a large system where there are a lot of loggers that are not in direct contact with a receiver.

Battery life will be significantly shorter if the Current Readings feature in Tinytag Explorer is used regularly for long periods.

Interference from other devices using a close frequency may also have an impact on battery life.

2.10 Troubleshooting

Tinytag Explorer Status Bar Flashes Red (Connect Gateway Status: Not Connected)

The connection between Tinytag Explorer and the Connect Gateway has been broken. Click on the Status Bar and press the Connect button. This may be either a computer network connection or a software connection within the same computer.

If it cannot connect, check that the Connect Gateway is running. If it is on another computer, check that computer is not turned off and it is connected to the LAN. If it is running on the same computer then maybe the service has not started, check the Master Gateway section of this manual for details on how to get the service running again.

Note that this indicator shows Connected as soon as Tinytag Explorer has connected to the Connect Gateway. This does not indicate that the Gateway Service has connected to a receiver or any loggers.

Firewall Configuration

Tinytag Explorer needs to be able to communicate with the Connect Gateway. They connect using TCP and UDP which allows them to run on different computers. This connection will be under the control of any firewall running on these computers.

The Tinytag Explorer installer automatically configures the Windows Firewall to allow this connection, so most likely no action is necessary.

Any third party firewall will need to be configured to permit the following connections:

UDP port 3927: For autodetection
TCP port 3927: For all other communications

Radio

3.1 Radio Specification

Different radio frequencies are used for different countries:

- 869.8MHz Used in the EU. Devices using this frequency can be identified by their part number ending –A. Older part numbers which do not have a single letter part number suffix also use this frequency.
- 917.8MHz Used in Australia. Devices using this frequency can be identified by their part number ending -B.

Naturally, parts using different frequencies cannot interoperate.

The radio uses FSK modulation, with +/-32 kHz deviation.

The transmission power is <5mW in EU & <3mW in Australia.

Typical range in free space:

- Ultra Radio 100m
- Plus Radio 200m

These frequencies will easily penetrate most internal or external walls; however the range may be reduced.

Indoors the range is quite variable. It is usually reduced to between 30% and 80% of full range. However it will sometimes be increased, maybe up to double the nominal range, due to reflections off other buildings, steel roofs, etc. This variability works to the advantage of the mesh network because the majority of loggers will be able to relay their information via the one logger with the extra-long range.

The radio system works well both indoors and out. The frequencies will usually penetrate steel-walled rooms to a degree, through door seals, windows, ventilation etc. Even though the radio waves cannot penetrate a metal wall (whether a fridge, or corrugated iron shed), the signal will probably still get through gaps around door seals and other openings.

These frequencies are very slightly absorbed by water. Wet walls are not a problem, but the signal will not get through a room filled with shelves full of fruit, for example.

3.2 Positioning & Mounting

Antenna Orientation

Ideally the antenna should be oriented vertically. Most of the energy is emitted perpendicular to the antenna.



Ultra Radio products can be wall mounted or placed flat on a surface, such as a shelf or a table top. They should be oriented as shown below, and not with the logger and antenna both mounted vertically.

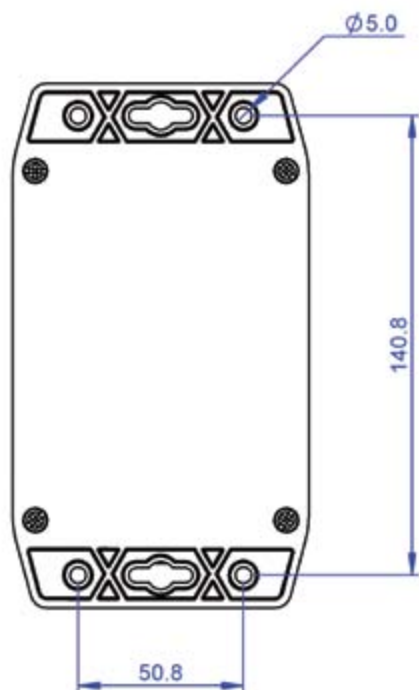


The radio is affected by line of sight. Please note that “line of sight” means that of the antenna – not your line of sight while standing over a logger on the floor.

Plus Radio Mounting Points

The logger can be wall mounted or placed on its back on a flat surface, such as a shelf.

The logger's back-plate has mounting holes, as shown.



Ultra Radio Mounting Bracket

If wall mounting an Ultra Radio data logger, remove the two indicated screws from the rear of the logger and use them to screw the mounting clip onto the back of the logger.

The bracket to hold the logger on a wall has two 3mm diameter holes, 32mm apart.



3.3 Installation

Introduction

This section describes best practice for installing a radio system.

Note that deviating from this process will not cause any significant problems; at worst it may take a little longer for all the loggers to connect to the system.

Receiver First

The first step in setting up a system should be placing the receiver. It should ideally be in a location where it will be within range of as many loggers as possible (an elevated position may help).

Configure and start the Connect Gateway.

Check using Tinytag Explorer that:

1. Tinytag Explorer has been able to connect to the Gateway Service, and
2. The receiver is listing in the navigation pane.

If working correctly, the receiver should be listing in Tinytag Explorer within a few minutes.

Do all of this before powering up any loggers.

Nearby Loggers Next

The first loggers to be switched on should be those nearest to the receiver.

These loggers should be within direct range of the receiver; they should connect at full performance within a few minutes.

When turning on a logger, do not hold it by its antenna. A logger sends its first transmission within a few seconds of switching on, and this should prompt the Connect Gateway to start its connection process. If your hand is around the antenna then this first transmission may not get through. In this case (or if the receiver does not catch this first transmission for some other reason) the Connect Gateway will start connecting on the next logging interval (which, as supplied, will be after 10 minutes).

Distance Order

Power up the remaining loggers, starting with those closest to the receiver – this order will minimise the time necessary for them all to connect.

In most cases these loggers should establish a preliminary place in the mesh and connect within a few minutes, otherwise the full meshing process will allow them to connect after 30 minutes.

Be Patient

It can sometimes take a while for a network to establish itself.

If a logger is not listing in Tinytag Explorer it may be tempting to reboot it or move it to another location. Rather than helping, doing this may actually slow the connection of the logger; it is better to be patient and give the system some time.

If a logger hasn't signed in after a couple of hours, that would be the time to try rebooting the unit or moving it to another location.

Transplanting a Network to a New Location

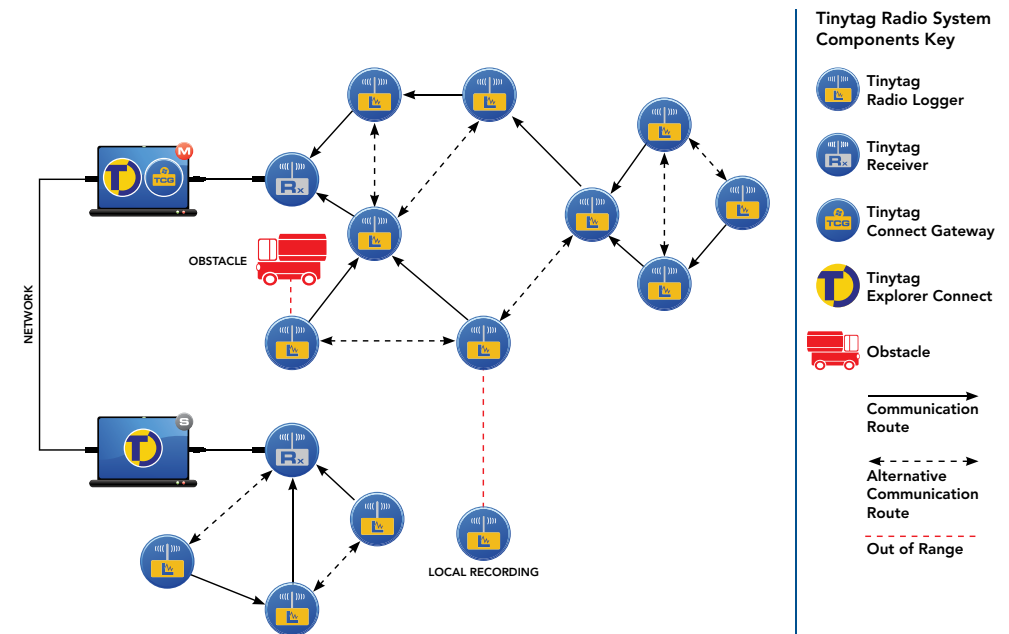
If moving a complete network to a new location, the following steps should be carried out:

- Set the loggers to a 2 minute logging interval to speed up the connection process (this can be adjusted to a longer logging interval once the system has configured itself in its new location).
- Assuming the existing data is no longer required; clear the loggers of historical data before turning them off (this means the system won't be trying to download old data whilst trying to configure itself).
- Power down all devices (including receivers) before starting over in the new location, as detailed previously.

3.4 System Configurations

Mesh Network

All devices in a radio system participate in a mesh network.



Mesh networks are ideally suited to data logging because they have the following characteristics:

1. Robustness. The mesh network allows information to be routed around obstacles. For example a van parked in front of a data logger will not cause a problem, because that logger will be able to transmit its information to the receiver via another device. The mesh will adapt to moving obstacles – it is self-healing.
2. Low set-up costs. In general it is possible to deploy loggers in an application and they "just work". The system will be able to automatically establish a mesh which connects all devices. This avoids the "radio survey" step which is necessary for point-to-point radio links.

Several advantages are unique to the Tinytag Radio mesh network:

1. All devices are capable of meshing. Some mesh network systems from other vendors differentiate between “mesh routing hubs” (which are often mains powered, and may need to be placed with some care) and non-meshing “transmitters”. The Tinytag solution is more robust because having a larger number of mesh-capable devices will allow it to form a more effective mesh. The number of redundant routing options is a key parameter that will be discussed later.
2. All devices can be reconfigured remotely. This is possible because all devices “listen” across the mesh network.
3. All devices are loggers, and data will not be lost due to momentary interruptions to the mesh network (a van driving in front of the logger) or temporary interruptions (a van is parked in front of the logger overnight). This capability also relies on devices being able to “listen” across the mesh, because that enables the Connect Gateway to request retransmissions.

3.5 Receiver Configurations

Most installation will only need the one receiver, but in some cases multiple receivers might be a benefit.

Receivers can be connected directly to the computer running either type of gateway in two ways; either across a network, using an Ethernet connected receiver, or directly, using a USB cable.

The default configuration of the Connect Gateway will automatically scan all com ports to find any receivers attached to the system, but if Ethernet receivers are being used it is best to specify these manually.

Multiple Receivers

Multiple receivers can provide:

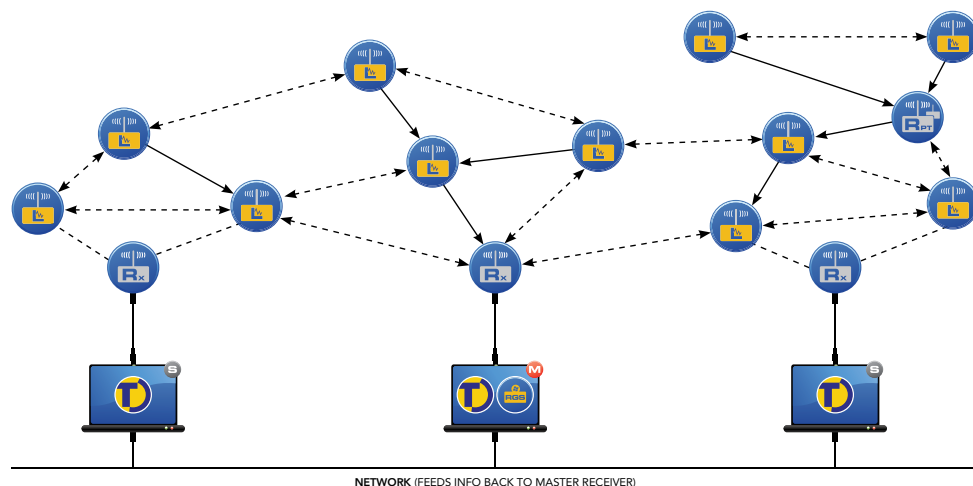
Redundancy The radio system will continue to function if one receiver fails.

Range Consider a radio system covering two warehouses, but the radio link between each warehouse is unreliable when all doors are closed overnight. It may be appropriate to locate one receiver in each warehouse.

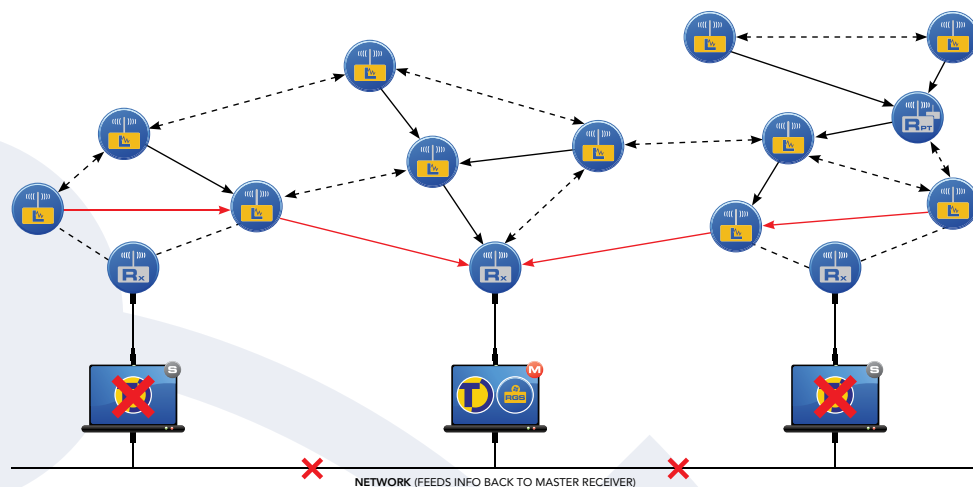
Capacity Having multiple receivers can improve capacity because they can share traffic. It is better to locate the two receivers at opposite ends of a large warehouse containing many radio devices. Each radio logger will find a mesh to its nearest receiver. For this traffic sharing to occur, they must not be within radio range of each other. If the two receivers in the warehouse were adjacent then they would both hear all traffic.

Receiver Configurations

There is a minor difference to the behaviour of a receiver depending on whether it is connected to Master or Slave Gateway. A receiver that loses contact with the Master Gateway (maybe because the computer has shut down) will continue to maintain the mesh network centred on that receiver. This ensures that the mesh is ready for use as soon as the computer running the Connect Gateway reboots.



A receiver that loses contact with a Slave Gateway will cease to maintain its local mesh, and other radio devices will switch over to another receiver within an hour.



3.6 Mesh Network Behaviour

Switching On a Device

When a device is first switched on it will send new measurements downstream as soon as it has any radio contact with another device. If there is a mesh established this should happen within a few minutes. When the Connect Gateway sees the first of these measurements it knows that the new logger exists. At this point it should quickly determine the identity of the logger, and begin collating measurements and requesting retransmissions if any measurements are lost.

Moving a Device

When a device is moved from one place in the mesh to another it may take between 30 and 60 minutes to work out its new place in the mesh. This meshing process works on a 30 minute cycle. After being moved the logger may not fully adapt until after one whole cycle.

Starting the Connect Gateway

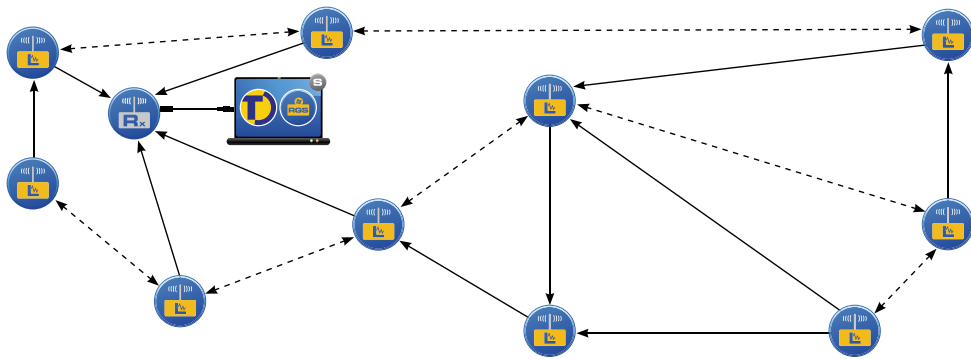
When the Connect Gateway is first started it needs to wait for a packet of data to arrive from each logger before it knows which loggers are present in the mesh. This is another process which will take up to one logging interval for each logger. An exception is loggers which had previously established a direct connection to the receiver (that is, not via any other mesh devices) within the last 4 days. It will probe these loggers immediately to see if they still exist within direct range. This again assumes that there is a well-established mesh; in particular, that the receiver is not just being switched on at the same time.

Switching On the Receiver

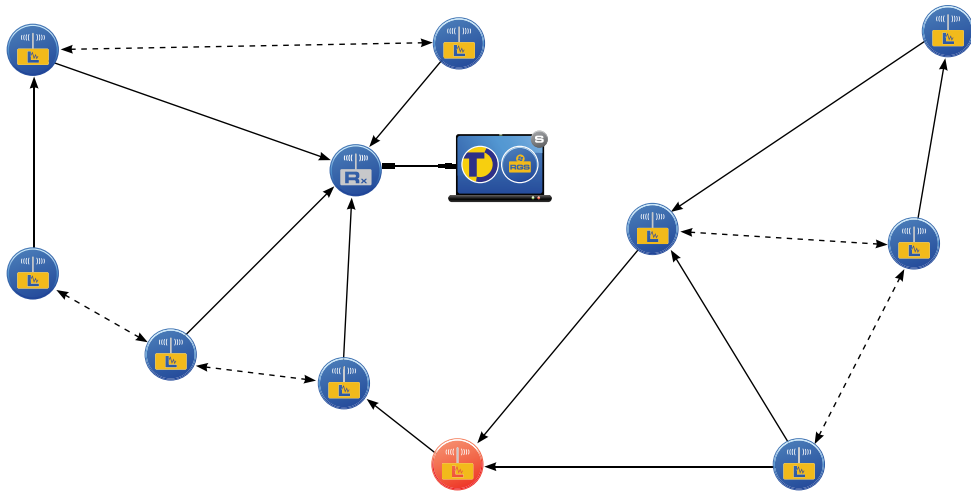
Receivers need to find their place in the mesh exactly like a logger. This adds an extra 30 minutes on to the "Starting the Connect Gateway" scenario. If the Connect Gateway is being shut down, possibly overnight, it is desirable to avoid this delay by leaving the receiver running.

Redundant Routing

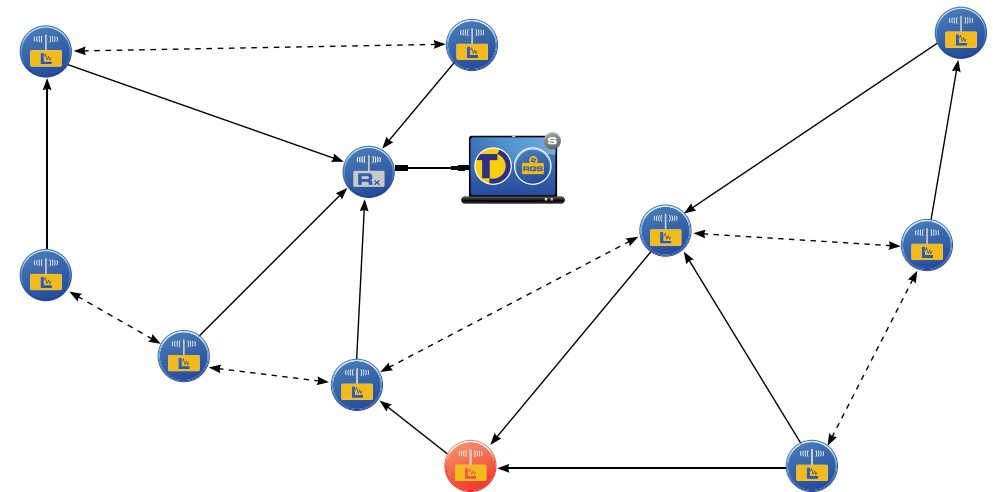
The best way to ensure reliable communications is to provide redundant routing options. Every device should have at least two other devices in front of it, but preferably more. Very often a radio device will find that an individual packet is not being received by its chosen downstream neighbour, either due to a momentary obstacle or momentary radio interference. Tinytag radio mesh devices can respond to this very quickly by immediately switching to the second best downstream route. It is not a problem even if this is a sideways hop – the information still gets through with a few seconds delay. In this way the mesh is constantly adapting to changing radio interference patterns to ensure reliable delivery. However this strategy only works if every node has at least two possible devices in front of it. A device with only one possible route is very much more fragile. In most cases this redundancy is easy to achieve – just scatter plenty of loggers within the measurement area, and locate the receiver so that it is within range of plenty of loggers.



(a) Good – plenty of redundant routing options for all devices.



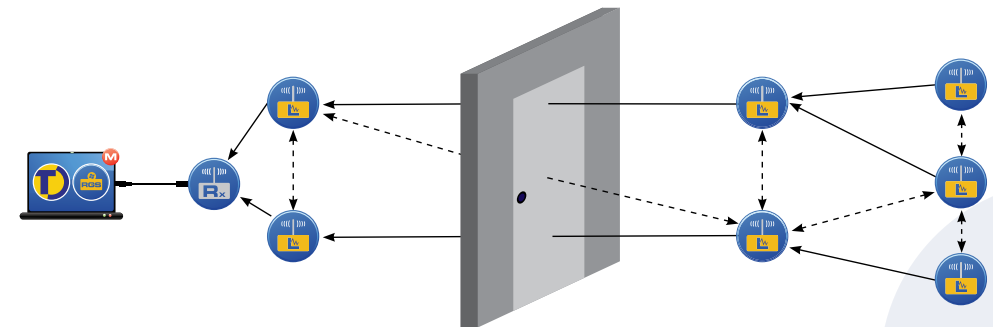
(b) Not Good – the red logger has only one place to send its data, so everything upstream of there (to the right) will not be reliable.



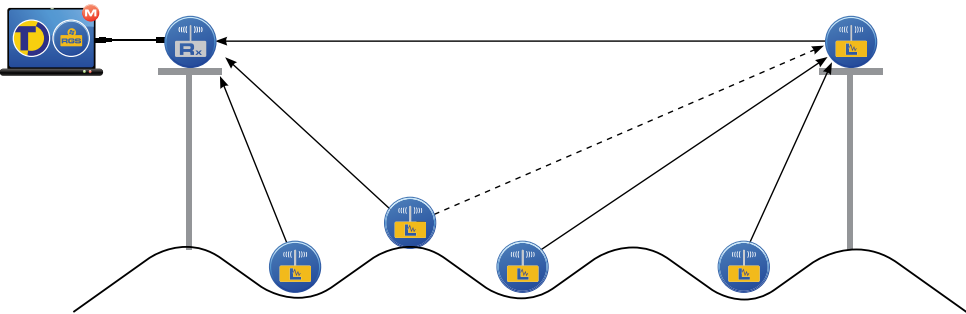
(c) Modifying the position of the red logger, so it has more than one place to send its data, will improve the range and therefore the reliability of the communications.

In some cases it can be beneficial to add or move a device to improve redundancy:

1. If there is a radio restriction, for example a narrow doorway through a thick steel wall, then it is good to have a pair of devices on either side of the doorway (better than just a single device on either side).



2. In some cases it is not possible to provide a clean radio path for loggers that are physically close to each other, perhaps because they are at ground level on an undulating ground. In this case it may be possible to elevate a small fraction of the loggers so that they can overlook the others. The majority of loggers will need to relay via the elevated minority. If it is not possible to move the logger in this way, it may be possible to install an extra logger to act as a repeater. The network is affected by the number of redundant routing options (the number of peer loggers within range of each other):



The network is affected by the number of redundant routing options (the number of peer loggers within range of each other):

Number of Peer Loggers Within Range	Effect
1	A single point of failure. Not ideal.
2-3	A mesh with alternative routes. Good.
4-15	A dense mesh. Ideal.
15-20	More peers than it needs. Could reduce range to increase battery life, but probably not worth it.
20+	Reducing range (by adjusting sensitivity, then transmit power) will increase battery life, and can help if the system will not form a robust mesh automatically.

Repeaters

Repeaters are not generally required because of the way the mesh network handles data. In some applications, however, where distance or obstacles make a repeater necessary (either to gain distance or improve the robustness of the mesh) an extra data logger can be used to relay data.

3.7 Radio Configuration

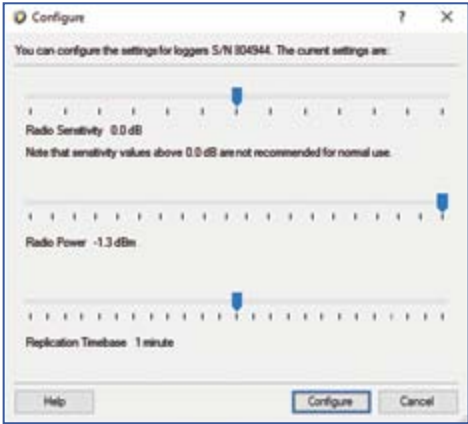
Adjusting the Radio Range

This section details how the Radio Range can be adjusted for each logger in the mesh network by changing the values of the parameters in the Radio Configuration program. Reducing the radio range can be beneficial when there are 20 or more loggers within range of each other, as this situation can make the mesh network less robust.

In most cases these parameters do not need to be adjusted, and incorrect configuration may adversely affect the performance of your radio network. We therefore advise that you only use this feature following the advice of Tinytag Technical Support.

Receive Sensitivity

The primary parameter to affect radio performance is Receive Sensitivity. This parameter adjusts the threshold at which the receiver will decode a receiver signal, relative to a baseline threshold of 9dB above the noise floor.



The default value for this parameter is zero dB, and may be adjusted between -6dB and +6dB.

In the default configuration, radio range is typically 200m for Plus Radio products and 100m for Ultra Radio products.

Radio range may be reduced by reducing the sensitivity:

Change in dB	Radio Range
0dB	100% of range
-3dB	~75% of range
-6dB	~50% of range

Reducing the range in this way will have an effect on the mesh network connections established by the loggers. In some circumstances the mesh can be less robust for loggers which are within range of more than 20 other loggers.

Reducing the range can also increase battery lifetime. It is possible to reduce the total amount of radio traffic processed by one device, by allowing it to ignore irrelevant distant traffic. However, this may also have the opposite effect, if it results in increasing the number of hops required for data to reach the receiver.

The radio range may be increased by increasing the sensitivity:

Change in dB	Radio Range
0dB	100% of range
+3dB	~130% of range
+6dB	~180% of range

Sensitivity values above 0dB will adversely affect the power consumption of a device.

The higher sensitivity means that it is less able to distinguish between good signals and background noise, and will spend extra battery power decoding spurious signals.

For a device with a mains power supply this may not be a problem.

Note that this figure is a typical measurement, and not a guaranteed minimum. It may be affected by many factors including the surrounding physical environment (buildings, equipment, etc.) or other local radio transmitters.

Transmit Power

The radio range can also be adjusted by changing the transmit power. The default configuration is for devices to transmit at their maximum power. If you wish to reduce the range of a logger the transmit power may be reduced in steps with the slider control. Minimum power will result in a range of typically 10% of normal. In general it is preferable to reduce sensitivity before reducing the transmit power in order to reduce the radio range. This ensures the signal to noise ratio is maximised.

Very Slow Logging Intervals

Some of the connection timings above depend on the logging interval. The logging interval affects the time taken for a logger to connect to the Connect Gateway, because that service will normally only discover that a logger is present when it transmits a measurement.

Other information which can also trigger this connection process is transmitted hourly; therefore loggers with very slow logging intervals will still connect without unreasonable delay.

Very Fast Logging Intervals

Normally loggers will transmit every measurement as it is taken. If the logging interval is faster than 2 minutes then multiple measurements are sent in a burst. This batching process avoids radio congestion, and maximises capacity.

The Replication Timebase Parameter can be changed to adjust the interval between measurement transmissions. A data logger will not transmit measurements more frequently than between one and two multiples of the Replication Timebase.

The default value for this parameter is one minute.

Note that this parameter is different from the Measurement Interval, which can be controlled using Tinytag Explorer and is typically set to 10 minutes. Under normal circumstances, measurements are transmitted as soon as they are taken, and arrive on the computer system almost immediately.

The Replication Timebase Parameter may be increased to save battery power, at the expense of less frequent measurement updates onto the computer system.

For example, if the Measurement Interval is 10 minutes, and the Replication Timebase is 30 minutes, the radio data logger will record between three and six measurements (30 to 60 minutes) before transmitting them all back to the computer system.

This saves battery power due to reduced transmission overheads.

3.8 LED Flash Patterns

With the exception of the Ethernet radio receiver, Tinytag Radio loggers and receivers have a single LED indicator that shows the current status of the unit:

Action	LED	Status/Operation
n/a	No Indicators	Device is powered off
n/a	Red flash every 4 seconds	<p>The device is powered on and has a problem.</p> <p>Either:</p> <ul style="list-style-type: none">a) Battery is Low.b) Device has not yet established its place in the mesh network.c) An alarm indicator is signalled. <p>Check the nature of the problem using Tinytag Explorer.</p>
n/a	Green flash every 4 seconds	The device is powered on, and does not have any problems.
Press and briefly hold the on/off switch.	Green indicator shows for one second. It then briefly flashes green then red.	The device has been switched on.
Press and hold the on/off switch for 3 seconds.	Red indicator shows for one second.	The device has been switched off.

LED flash patterns for the Ethernet Receiver can be found in section 4.3

Ethernet/LAN

4.1 Mounting Points

LAN loggers can be wall mounted or placed on its back on a flat surface, such as a shelf.

The logger's back-plate has mounting holes, as shown.



4.2 Alarms

Introduction

In addition to the status LED on the front of the logger (see section 4.3, LED Flash Patterns), LAN data loggers have a built-in sounder and an external connection that changes state when the logger's alarms are active.

The external connection can be used to trigger devices such as an SMS Dialler or a purpose built indicator (light and/or sound etc.).

The external connection can also supply power to external devices.

An active alarm can be muted by pressing the button on the front of the logger.

Note that muting the internal alarm sounder will also turn off the external connection. If required, the connection should be held on (latched) by external equipment until it is explicitly acknowledged. Muting the alarm at the logger does not acknowledge or switch of the alarm in Tinytag Explorer Connect.

Cable Wiring

An output cable for the external connection is available, part number CAB-0042. This is a plug with a 1.5m cable with stripped ends, ready for wiring into a terminal block. Connection information is as follows:

Alarm Output Connections

Colour	Name	Function
Brown	Power	DC power supply from the logger (see below for details)
Green	Ground	Power-supply reference (0V) and alarm signal return
White	Signal	Alarm Indication (open-drain, pulled to Ground when an alarm is active, otherwise open-circuit). This output will continue to change state, in the event of an alarm, should the PoE supply to the logger fail.

Power Output

The power output is regulated at 11.5V \pm 0.5V from the PoE supply. The output voltage will therefore turn off if the PoE supply fails.

Example Usage

Note that if only 2 cores are used, the unused core must be insulated.

- Indicator

Wire an indicator (sound and/or light) between Power (brown) and Signal (white). The indicator must have a suitable supply voltage rating.
- SMS Dialler

Wire Signal (white) to an active-low input and Ground (green) to the Ground reference. Polarity is important! If the input does not have a pull-up then one should be provided between Signal (white) and Power (brown). A pull-up resistance between 1kΩ and 10kΩ is suggested.

WARNING



THE CABLE AND CONNECTOR MUST NOT BE CONNECTED TO ANY VOLTAGE MORE THAN 50V AWAY FROM EARTH POTENTIAL, INCLUDING MAINS VOLTAGES!

Maximum current through any pin = 200mA
Maximum voltage on the Signal output (relative to Ground) = 30V

Protection

Both the Power (brown) and Signal (white) outputs are protected with a 350mA (nominal) self-resetting fuse and a clamping diode (TVS).

The fuses will enter a high-resistance state if self-heating from the current passing through them causes heating above a threshold. Once the fault is removed the fuse will cool down and its resistance will fall (to around 1Ω). The current at which the fuse will ‘blow’ varies according to the ambient temperature. At high temperatures (70°C) it will pass at least 200mA; at low temperatures it may pass considerably more (up to 0.5A).

The switching FET on the open-drain output will switch 30V. Its ‘On’ resistance is less than 0.5Ω.

4.3 LED Flash Patterns

Ethernet Radio Receivers and LAN data loggers have two status LEDs; one to show the status of the device’s Ethernet connection (yellow/blue) and the second to show the status of the unit (green/red).

Action	LED	Status/Operation
n/a	No Indicators	Device is powered off
n/a	Red flash every 4 seconds	The device is powered on and has a problem. Either: a) Battery is Low. b) An alarm indicator is signalled. Check the nature of the problem using Tinytag Explorer.
n/a	Green flash every 4 seconds	The device is powered on, and does not have any problems.
Press and briefly hold the mute button.	Green indicator shows for one second. It then briefly flashes green then red.	The device has been switched on.
Press and hold the mute button for 3 seconds.	Red indicator shows for one second.	The device has been switched off.
n/a	Yellow indicator on constantly	The device is being powered from its Ethernet connection, but no communications have been established.
n/a	Blue (flickering)	Ethernet communications are established and on-going

Note that the yellow and blue LEDs cannot be on at the same time. If the blue LED is on (or flickering) then PoE power must be available.

Appendix

a) System Requirements

Tinytag Connect Gateway Service

The system requirements for running the Tinytag Connect Gateway Service are shown below.

Note that additional requirements apply if you are running Tinytag Explorer Connect on the same computer (see below).

Operating System: Windows 7, 8, 8.1, 10 & 11 (x86 and x64 bits versions)

Processor: 200MHz Pentium III processor or better

Memory: 512Mb

Hard Disk Space: At least 30Mb for programs, allow up to 100Mb for data

Monitor for installation: Minimum 256 colours, resolution 800 x 600

The requirements for running the Connect Gateway on an existing server are shown below.

CPU time: Negligible

Memory: 20Mb

Hard Disk Space: Typically 30Mb for programs, allow up to 100Mb for data.

The service stores a small amount of configuration information in the Windows Registry, in

HKEY_LOCAL_MACHINE/Software/Tinytag/Kola

Cached measurement data and diagnostic logs are stored in

C:\Program Files\Tinytag\Tinytag Explorer\var

These locations should ideally be included in any regular backup, which can be safely taken while the service is running.

Tinytag Explorer Connect

Tinytag Explorer Connect requires a PC with the following specification:

Operating System: Windows 7, 8, 8.1, 10 & 11 (x86 & x64 versions)

Browser: Internet Explorer 8 (or above); Firefox or Google Chrome.

Processor: 200MHz Pentium III processor or better (1.6GHz recommended).

Memory: 512Mb (1024Mb recommended for Windows 7 & above).

Hard Disk Space: At least 30Mb available hard disk space (120Mb recommended).

Monitor: Minimum 256 colours, 800 x 600 resolution or greater recommended.

The recommended options above should give the user ample performance to run other applications at the same time as Tinytag Explorer Connect.

b) Software Licence

Tinytag Explorer is supplied under a site licence which means that it can be installed on as many computers as the customer wishes at a given location (additional copies of the software are required for each additional site the software is used at).

To view the full software licence, please visit our web site here:

<http://www.tinytag.info/software>

c) Regulatory Compliance

For the specific standards our radio & Ethernet/LAN products comply with, please see individual product data sheets.

Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

d) Approvals

Gemini Data Loggers (UK) Ltd. operates a Business Management System which conforms to ISO 9001 and ISO 14001.

e) Further Information

Further information on Tinytag products, including data sheets and manuals, can be found on our web site at:

www.tinytag.info

If you should have any further questions, please contact your supplier or:

Gemini Technical Support

t: +44 (0)1243 813009

e: help@tinytag.info

Gemini Data Loggers (UK) Ltd

Scientific House, Terminus Road,
Chichester, West Sussex,
PO19 8UJ,

T: +44 (0)1243 813000

E: info@tinytag.info

www.tinytag.info

9800-0150: ISSUE 3 (26th May 2023)