

TM

Tempurity™ System User's Guide

Tempurity Version 2.0

Table of Contents

| | |
|---|-----------|
| Table of Contents | 2 |
| Introduction | 6 |
| About Tempurify™ | 6 |
| The Networked Robotics Mission..... | 6 |
| Tempurify Components..... | 6 |
| Tempurify Architecture | 6 |
| Tempurify Regulatory..... | 7 |
| About this Document..... | 7 |
| Tempurify™ System Requirements | 8 |
| Tempurify Server™ Computers | 8 |
| Tempurify Monitor™ Computers | 8 |
| NTMS4i Network Hardware | 8 |
| NTMS4p Network Hardware | 8 |
| Direct Data Collection from Scientific Instruments (Direct Connections)..... | 8 |
| Data Collection from Digital and Analog Probes (Sensors) | 8 |
| An Overview of the Tempurify System | 9 |
| Connecting to Tempurify: An Overview..... | 9 |
| Tempurify System Software | 11 |
| How it Works - The Tempurify System Architecture | 12 |
| Parallel Monitoring: Redundant Data Collection and Monitoring for High Value Biologics | 13 |
| Networked Robotics' NTMS Network Hardware | 13 |
| Configuring Networked Robotics' Hardware for Data Collection | 16 |
| Power the NTMS4 | 16 |
| Connect to the Network..... | 16 |
| Wireless Networking..... | 18 |
| Extending Connections | 18 |
| The NTMS Configuration Wizard | 20 |
| Downloading the NTMS Configuration Wizard | 20 |
| Run the NTMS Configuration Wizard | 20 |
| Viewing and Setting the NTMS's IP Address..... | 22 |
| Why is a Gateway Address Not Required? | 22 |
| Setting the WiFi Access Data | 22 |
| Viewing and Setting the Interface, Instrument, or Sensor Type..... | 22 |
| Physically Connect the NTMS to your Data Source – An Example Direct Connection and an Example Sensor | 23 |
| Example of a Direct Data Connection Data Source: Thermo Fisher Scientific® Revco and Compatible Ultracold (-80°C) Freezers..... | 23 |
| Example of a Sensor Data Source: Networked Robotics TPL3 Digital Temperature Probe in Refrigerators/ Freezers/ Incubators/ Ovens/ Rooms | 24 |
| Placing Digital Temperature Probes in Glycerine Solutions | 25 |
| Extensions..... | 26 |
| Monitoring via Standard Network Wall Plates | 26 |
| Testing Data Collection through the Network Manually | 27 |
| The Ping Command..... | 27 |
| The Telnet Command..... | 28 |
| The Tempurify Server | 30 |
| Dedicated vs Shared Use Computers as Tempurify Servers | 30 |

| | |
|---|-----------|
| Downloading the Tempurity Server Software | 30 |
| The Tempurity Server Status Icon on the Windows Taskbar..... | 31 |
| Server Running | 32 |
| Server Stopped | 32 |
| Starting and Stopping the Tempurity Server using the Taskbar | 33 |
| Starting and Stopping the Tempurity Server using Windows..... | 34 |
| The Tempurity Server Configuration Utility | 35 |
| Configuring Monitored Devices | 36 |
| Custom Monitored Device Types | 39 |
| Configuring the Server Identity | 41 |
| Enabling E-mail and Text Message Alarm Notifications | 41 |
| Testing the Ability to Send Mail | 42 |
| Microsoft Exchange Servers and Testing the Ability to Send Mail..... | 43 |
| Using Gmail as your Alarm Notification Mail Server | 44 |
| Enabling Voice Alarm Notifications..... | 44 |
| Editing Tempurity Server Configuration Files Manually | 45 |
| Configuration Histories and Restoring Previous Configurations | 45 |
| Setting the Windows Options on your Tempurity Server Computer | 46 |
| Tempurity System Data..... | 46 |
| Measurement Interval..... | 46 |
| Time of Data Collection | 46 |
| Units | 46 |
| Location..... | 47 |
| Data Retention | 47 |
| Data Backup..... | 47 |
| Accuracy..... | 47 |
| Value Alarms | 48 |
| Communication Alarms | 48 |
| The Tempurity Monitor Client..... | 50 |
| Distributed Alarm Notification | 50 |
| Dedicated vs Shared Use Computers as Tempurity Monitors | 50 |
| Running the Server and the Monitor on the Same Computer | 50 |
| Downloading and Installing the Monitor | 50 |
| Starting the Tempurity Monitor | 54 |
| Stopping the Tempurity Monitor | 54 |
| Connection Status to the Tempurity Server | 55 |
| Main Monitor Screen | 55 |
| Alarm Status Icons | 57 |
| Alarm Window | 58 |
| Monitored Device Information Window | 58 |
| Graphs..... | 59 |
| Exporting Data to Other Applications | 63 |
| Statistics | 63 |
| Alarm Notifications | 65 |
| Defining an Alarm Notification Group | 66 |
| Choosing Alarm Notification Types and Entering Alarm Notification Addresses | 66 |
| Test Alarm Notifications..... | 67 |
| Alarm Notification Groups are Mapped to the Tempurity Server for which they were Created..... | 68 |
| Alarm Notification History | 68 |
| Storage and Transfer of Alarm Notification Groups..... | 68 |
| Monitor Restart..... | 69 |
| E-mail to Text Gateways | 69 |

| | |
|--|-----------|
| Time Delay in Receiving Alarm Notifications | 70 |
| Monitoring Multiple Tempurity Servers from a Single Computer | 70 |
| Regional Versions of the Tempurity Monitor | 71 |
| Hardware Upgrades – Changing the Function of your NTMS Hardware | 73 |
| When to Upgrade your Firmware | 73 |
| Downloading the Hardware Upgrade Wizard | 73 |
| Running the Hardware Upgrade Wizard | 73 |
| Time Zones and Time Accuracy | 75 |
| System Operations..... | 77 |
| Redundancy | 77 |
| Large Scale Power Outages | 77 |
| Safety | 78 |
| Periodic Testing..... | 78 |
| Regulatory Use..... | 79 |
| Suggestions for Operation | 79 |
| Index | 80 |
| Appendix A: Glossary of Key Tempurity System Terms | 82 |
| Appendix B: USP Temperature Storage Definitions | 83 |
| Appendix C: File Locations | 84 |
| Appendix D: Networked Robotics' NTMS4 Hardware FCC Certification | 85 |
| Appendix E: Configuring your PC for Use as a Tempurity Server or Monitor | 86 |
| Appendix F: Tempurity System Specifications..... | 88 |
| Appendix G: Networked Robotics' Hardware Architecture for Handling the Physical Diversity in Data Collection..... | 89 |

Customer Support Information

Networked Robotics Corporation
1-877 FRZ TEMP

www.NetworkedRobotics.com

1-877 GLP TEMP

Copyright

Information in this document is subject to change without notice. The temperatures used in the examples are fictitious and are not actual temperatures recorded from any organization. No part of this document may be reproduced or transmitted in any form or by any means without the express written consent of Networked Robotics Corporation.

©2010-2017 Networked Robotics Corporation All Rights Reserved. Printed in the USA

Tempurity System User Manual Tempurity Version 2.0

This document and the associated online and printed documentation are the property of Networked Robotics Corporation and are loaned to the user under the terms of the license agreement. Unauthorized copying or use of the software or any associated materials is contrary to the proprietary rights of Networked Robotics Corporation and is a violation of state and federal law. This material must be returned to Networked Robotics Corporation upon demand.

Networked Robotics Corporation

825 Chicago Avenue

Suite F

Evanston, IL 60202

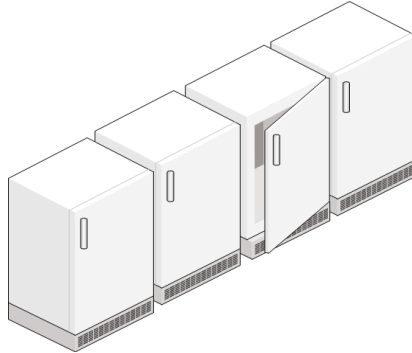
Trademarks

The Networked Robotics NR logo is a trademark of Networked Robotics Corporation.

LinkSys is a registered trademark of Cisco-LinkSys Corporation California. Microsoft, Windows, Windows XP, 7, 8, 10, Exchange, and the Windows logo are registered trademarks of Microsoft Corporation in the United States and/or other countries. Gmail is a registered trademark of Google Inc. Corporation. Sprint PCS is a registered trademark of Sprint Communications Company L.P. US Telecom Inc. T-Mobile is a registered trademark of Deutsche Telekom Ag. Corporation. Cingular is a registered trademark of Cingular Wireless LLC. Verizon is a registered trademark of Verizon Trademark Services LLC. Nextel is a registered trademark of Nextel Communications, Inc. Forma is a registered trademark of Thermo Fisher Inc. Corporation. Revco is a registered trademark of Thermo Fisher Inc. Kelvinator is a registered trademark of Electrolux Home Products, Inc.

Other product names mentioned may be service marks, trademarks, or registered trademarks of their respective companies and are hereby acknowledged.

Introduction



About Tempurity™

The Tempurity System is the most powerful system on the market for achieving compliance with United States Food and Drug Administration and other quality regulations. Environmental conditions are critical to the quality of biologics, food, and compounds. By enabling centralized data collection from environmentally-sensitive scientific equipment and sensors that are anywhere on your network, the Tempurity System enables you to confirm the integrity of your organization's key assets.

The Networked Robotics Mission

Networked Robotics' mission is to enable network-based real-time data collection from diverse sources with regulatory-compliant hardware and software. Our systems are designed and documented for use in United States Food and Drug Administration (FDA) Good Laboratory Practices (GLP) and Good Manufacturing Practices (GMP) Environments.

Tempurity Components

The system is comprised of both advanced software and unique new network hardware. All Tempurity Software can be easily downloaded and used on computers running the Windows operating system. Unique Networked Robotics hardware collects and integrates data from diverse data sources.

Tempurity Architecture

The peer-to-peer architecture of Tempurity means that the system is flexible to a degree that has not been achieved by monitoring systems to-date. Tempurity components can be rapidly installed anywhere, and can be quickly configured to communicate with other Tempurity components. The Tempurity architecture is "distributed" because pieces of the system run on multiple, networked computing devices that communicate with each other.

The Tempurity architecture improves monitoring capability by increasing access to mission-critical information. It enables a high degree of redundancy, and decreases the barriers of connection-time. Key benefits of the Tempurity System distributed architecture are:

- 1) Data can be collected from instruments and sensors that are anywhere on the network. Networked Robotics hardware "learns" to talk to new sensor and instrument types through downloadable firmware.
- 2) Any Windows computer can collect data subject to hardware, operating system requirements, and network infrastructure. The system is infinitely redundant.
- 3) Using an instantly downloadable tool, running permanently in the background of your computer, any computer on the network can watch data and when needed implement alarm notifications to anyone, anywhere.

Tempurity Regulatory

A suite of customer-facing regulatory documents for the operation of the system in regulated environments is available from Networked Robotics. These include documents for calibration, installation qualification and self-validation.

Networked Robotics operates under a set of internal procedures designed for the development of products for use in FDA-regulated laboratories.

Regulatory information is available from Networked Robotics. This manual focuses on the operational characteristics of the system.

About this Document

For the most up-to-date information on the Tempurity System hardware and software you may wish to consult the Networked Robotics web site at www.NetworkedRobotics.com. The web site can be considered to be the main source of information for the Tempurity System and is expected to be updated more frequently than this manual.

This manual can be downloaded from the "[Download](#)" section of the web site. See also the Tempurity [Quickstart Guide](#) and documentation for individual interface and sensor hardware products.

Tempurity™ System Requirements

The following describes in brief the minimum hardware requirements that are necessary to run the Tempurity System. See our [Requirements web page](#) for more current information.

Tempurity Server™ Computers

- BIOS options that support automatic recovery after power failure or power backup
- Most hardware designed to run Windows

Tempurity Monitor™ Computers

- 1024 x 768 screen resolution or greater
- Most hardware designed to run Windows including Windows tablets
- This computer must be connected to a network that can access the Tempurity Server Computer
- BIOS options that support automatic recovery after power failure are recommended but not required

NTMS4i Network Hardware

- An Ethernet TCP/IP network (10 Megabit or autosensing connection)
- Standard 115-Volt, 60 Hertz AC power outlet for each NTMS4 hardware device. Adapters are available for use outside of the United States.

NTMS4p Network Hardware

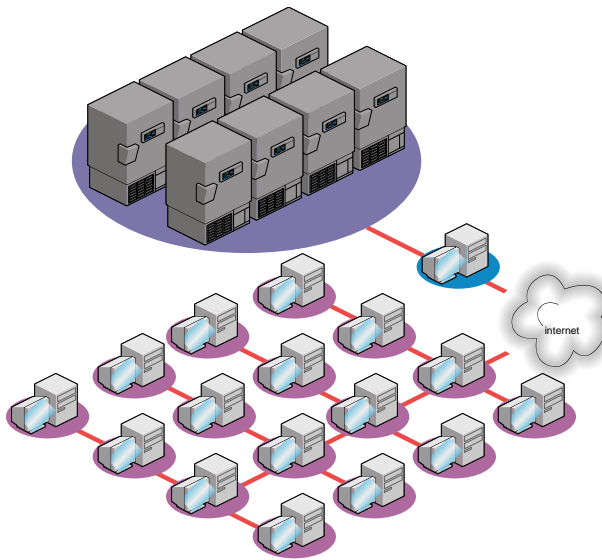
- An Ethernet TCP/IP network (100 Mbit or less)
- Or a Wi-Fi network - 2.4 GHz WiFi 802.11 (b,g,n) (150 Mbit/s)
- Standard 115-Volt, 60 Hertz AC power outlet for each NTMS4p hardware device. Adapters are available for use outside of the United States.

Direct Data Collection from Scientific Instruments (Direct Connections)

- The Tempurity System collects scientific information by communicating directly with the digital outputs of major brands of incubators, cryofreezers, ultracold -80°C freezers, refrigerators, shakers and incubated shakers by speaking to each instrument in its own individual machine language. The list of instrument types and brands to which the Tempurity System can communicate directly continues to grow. See the Networked Robotics web page for current information.

Data Collection from Digital and Analog Probes (Sensors)

- The Tempurity System also collects scientific information via networked sensors. The list of Networked Robotics digital probe types and other sensors that are supported by the Tempurity System continues to expand. Probes are now available for temperature, humidity, CO₂, pressure, voltages and electric currents of several types, alarm contacts and others. Almost any analog sensor is supported including those for light, position, rotation, and many other physical parameters. See the Networked Robotics web page for recent information.




An Overview of the Tempurty System


Connecting to Tempurty: An Overview

The major steps to follow for a new Tempurty System installation are as follows: Use the downloaded programs shown by the black-and-white tool icons, which can be obtained from the "[Download](#)" section of the Networked Robotics web site:


1) Set up the Networked Robotics NTMS4 Network Device(s)


- A. Download the NTMS Configuration Wizard  to any PC
- B. Configure the network addresses in each NTMS4 for use on your network
- C. Configure the 4 physical data acquisition ports on each NTMS4 for the type of instrument
- D. Physically connect the scientific instrument(s) or sensor(s) to the NTMS4's data port(s)
- E. Test network data collection

2) Set up the Tempurty Server

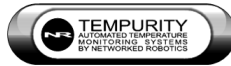
- A. Download and install the Tempurty Server software
- B. Run the Tempurty Server Configuration Utility  to specify data collection from the network addresses in (1) above and set alarm threshold criteria
- C. Start the Tempurty Server to initiate data collection

3) Set up the Tempurty Monitor Client(s)

- A. Download and install the Tempurity Monitor(s)  on the appropriate computer(s) (can be the same as the Tempurity Server) and enter the network address of the Tempurity Server(s) to watch
 - B. Create alarm notification groups and enter alarm notification addresses
 - C. Review data and alarm history as needed
- 4) **Set BIOS, Firewall, and Windows parameters on both Server and Monitor Computers**




to ensure that the Tempurity System is accessible and always running  **Windows^{XP}**

- 5) **Periodically Review and Test System Configuration and Functionality**



All software and configuration utilities can be downloaded from the Networked Robotics web site.

Tempurify System Software

The figure below shows the three main components of the Tempurify System software running simultaneously on a single computer. The NTMS Configuration Wizard , shown in the center is used to set up Networked Robotics hardware and thus to enable network-based data collection from freezers, refrigerators, incubators, and cryofreezers. The Tempurify Server Configuration Utility , shown on the lower left, is used to initiate network data collection and storage to a single computer. The Tempurify Monitor , shown on the upper right, is used to view any data in real-time and to initiate the sends of alarm notifications. Each component can be run on the same, or on different computers. Network security factors apply.

A Tempurify Server is like a web page. A Tempurify Monitor is like a web browser. Any Tempurify Monitor can connect to any Tempurify Server wherever it is in the world. However unlike a webserver-browser connection –the Tempurify Server streams data constantly in real-time to every Tempurify Monitor that is connected to it.

Tempurify-Monitor-running and Tempurify-Server-running computers must be able to communicate with each other through the network, and Server computers must be able to communicate with Networked Robotics' NTMS hardware. For fully distributed operation network ports 3010 and 80 must be open on the firewall of the Tempurify Server computer. Port 3010 allows remote Tempurify Monitors to see the information from the server. Port 80 allows alarm notifications to be initiated when an alarm condition is detected.

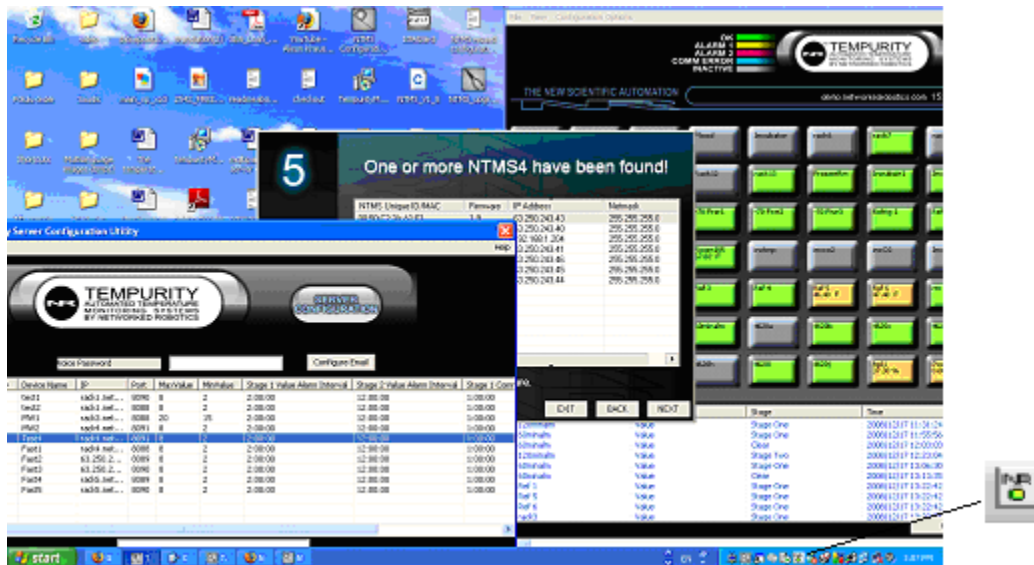



Figure 1: The 3 Main Software Components of the Tempurify System Running Simultaneously on a Single Computer

The three components are obtained from the "[Download](#)" section of the Networked Robotics web site via three separate downloads. Download by clicking on the relevant tool and then install each program as needed by clicking on the downloaded file.

The NTMS Configuration Wizard is run by clicking directly on the icon for the downloaded file. After it has been installed, the Monitor is invoked by clicking on the icon in the Windows taskbar, usually at the bottom right of your screen. After installation, the Server Configuration Utility, which is used to initiate automatic data collection and logging, is invoked in the programs list under "Start->All Programs>TempurityConfig".



The NR icon in the Windows Taskbar at the lower right  indicates that this is a computer on which the Tempurity Server software is started and is running for data collection.

How it Works - The Tempurity System Architecture

The figure below shows schematically the network-distributed architecture of Tempurity System components. The Tempurity Server (2) sends commands to Networked Robotics NTMS hardware units (1) requesting data. The NTMS units in turn query scientific instruments and sensors in each of their unique data languages. (See the section on the NTMS hardware.)

The primary function of the Networked Robotics hardware is integration. Networked Robotics hardware speaks the unique data language of diverse instruments and sensors. The network messages to NTMS devices requesting data are in a simple, common form, but the format of messages from the NTMS to each instrument or sensor are necessarily of many diverse types because it must speak the language of each machine or sensor type.

The data values that are returned to the Tempurity Server (2) by the NTMS are tagged with a time (a universal or time-zone irrelevant time) and stored.

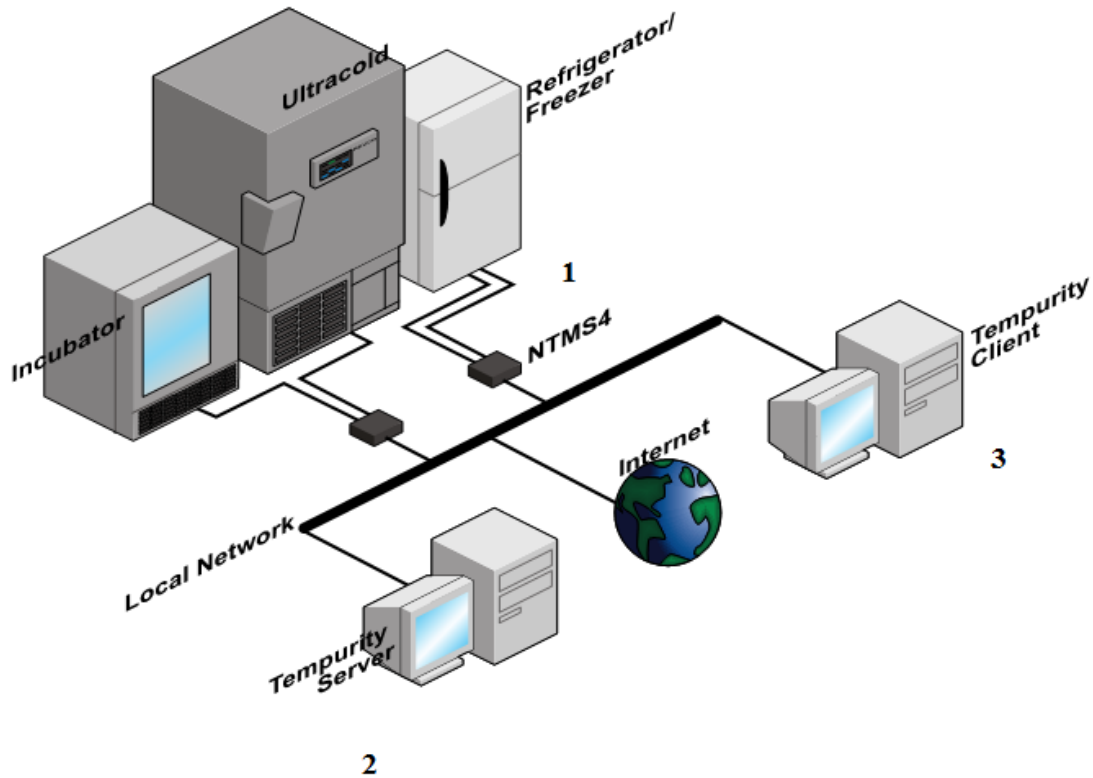
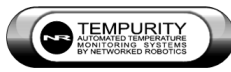


Figure 2: Network-Distributed Tempurity System Components

The Tempurity Server (2) watches the data streams from the monitored devices to see if data values that are collected meet the conditions that would initiate an alarm condition. Tempurity Monitors (3) are constantly in contact with the server, watching remotely for the development of alarm conditions. If such an event occurs they determine who should be notified and how. The process is initiated by the Monitor Client (3) however it is the Server (2) that implements the sending of these messages through an e-mail server or other means to the outside world.

Parallel Monitoring: Redundant Data Collection and Monitoring for High Value Biologics

Highly redundant monitoring is possible because of our distributed architecture. You can create as many Tempurity Servers and Monitors as you wish. Tempurity Servers can redundantly collect from our network hardware and thus from all of your monitored devices. Tempurity Monitors can redundantly connect to Tempurity Servers. You can have as many of our network hardware units, Tempurity Servers, and Tempurity Monitors as you wish.

Networked Robotics' NTMS Network Hardware

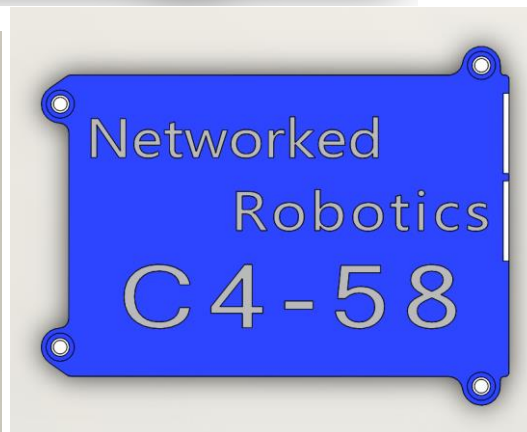
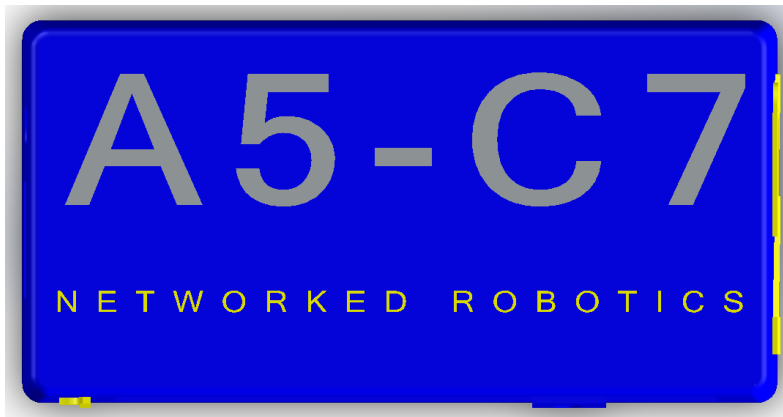
The Networked Robotics NTMS4 series (Network Telemetry Monitoring System) are network devices that are designed to collect data from diverse data sources. Most commonly these are environmental data sources such as the temperatures from ultracold (-80°C) freezers, liquid nitrogen freezers, standard freezers, refrigerators, cold boxes, incubators, or rooms via either direct data connections to those types of instruments (In effect data is collected indirectly from the instrument's own sensors) or via Networked Robotics' proprietary sensors.

Networked Robotics hardware must be configured in a process similar to that of configuring other types of network devices; the units must be set to run in your company's network environment, and each of the connected data ports on the NTMS must be configured for data collection from the type of scientific instrument or sensor from which values will be collected.

Both the NTMS4i and NTMS4p versions of the NTMS are shown below.

On the NTMS4i the data ports are on the left side of the NTMS with data port 1 the leftmost jack. The network connector has a silver rim and is the rightmost jack when facing the unit.

On the NTMS4p the data ports are numbered vertically with port one being the top left, port two under than, port three on the top right and port four on the bottom right.



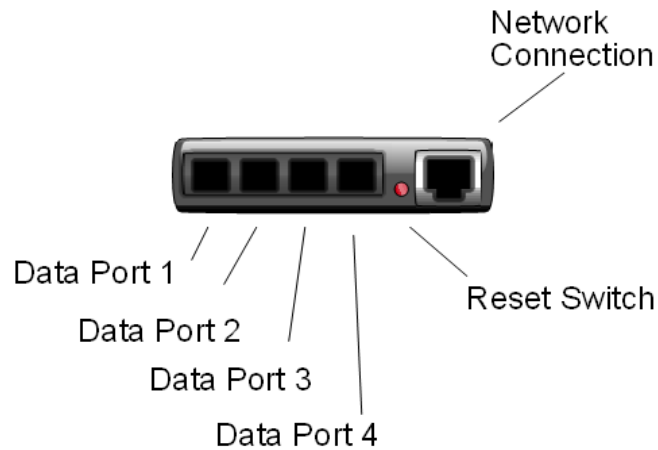


Figure 3: The Networked Robotics NTMS Hardware


Each of the NTMS4's four data ports can be used to communicate with any supported monitored device. Any combination of these instrument and sensor connections may be implemented on any of the four data ports. For example all four could be configured to collect temperature from standard refrigerators via Networked Robotics' TPL3 digital temperature probes (Networked Robotics Product #30002), or two data ports could collect temperatures from probes in standard refrigerators, the third could collect temperature via a direct connection to the serial port of a Thermo-Revco compatible ultracold freezer (Networked Robotics Product #30004), and the fourth could collect temperature, carbon dioxide, oxygen, and humidity via a direct connection to a Thermo Forma Incubator (Networked Robotics Product #30018) freezer. Monitored device types may report several parameters simultaneously (e.g. temperature, humidity, CO₂, O₂, voltage, alarm status) all through a single NTMS data collection port depending on which interface is used.

Each Networked Robotics NTMS is labeled with a unique ID. The Unique ID will be important for tracing connectivity to instruments or sensors during operation.

It should seldom be needed, but the reset switch on the NTMS4i unit sets the unit to factory defaults. To reset, unplug the unit and then depress the switch with a pen or paperclip while plugging in the unit.

For a list of Networked Robotics interface and sensor products, see the Networked Robotics product page on our web site at <http://www.networkedrobotics.com/checkout.htm>.

Configuring Networked Robotics' Hardware for Data Collection

In order to enable network data collection, you will configure the Networked Robotics NTMS hardware through your network using the NTMS Configuration Wizard  software. You will connect the instrument or sensor to the NTMS, and first test network data collection through the operating system before configuring the Tempurity System software.

In most cases it is best to immediately connect the NTMS to the network where it will be used, near the monitored scientific instrument or sensor and configure it there, however in some cases, such as when the NTMS needs to be put in a difficult-to-get-to or unsafe location or to configure wireless parameters, you may want to briefly plug it into a nearby network port in your office, configure and test it, and then move it to the network at the monitored location.

Power the NTMS4


The NTMS4i

When you plug the power into the NTMS you will see that the three LEDs on the left side of the unit are active. The yellow LED is the "link" light. It indicates that the NTMS is connected properly to the network. After powering up, the yellow light will blink once to indicate that the firmware is operating properly. The green light will flicker when connected to an active network. The red and green lights indicate data communication via the network.

The NTMS4p

Use the included micro-USB power supply to power up the unit. The orange light should be go on. The green light will blink as data transfer is initiated.

Connect to the Network

The figure below, reproduced from the first panel displayed in the NTMS Configuration Wizard , shows how the NTMS4i is connected to your network. In this figure the network switch is shown in the same room as the NTMS. In many cases the network switch, shown below in blue, will be mounted in a network closet in your facility, and you will be connected to it via the same standard wall plates and jacks used to connect personal computers to your network.

The NTMS4p, when connected via a wired connection is connected in the same way.

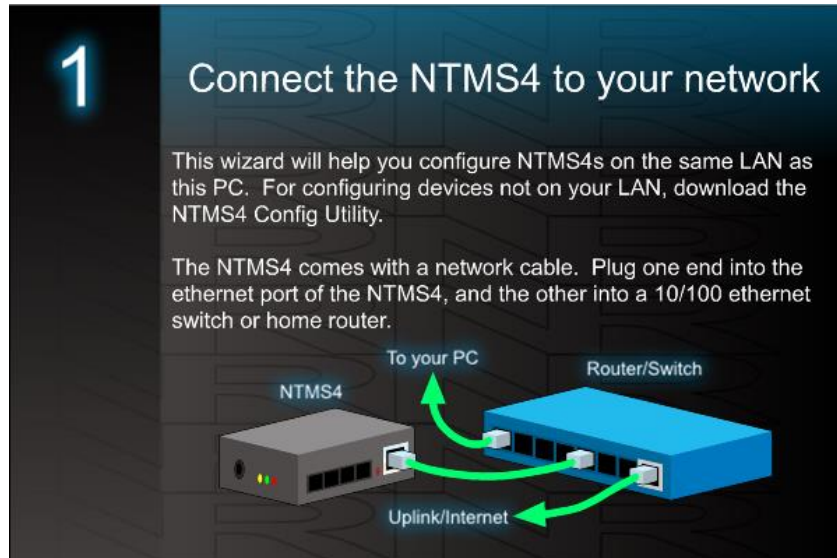


Figure 4: How to Connect the NTMS4 to your Network

In some cases it may be appropriate to first connect the NTMS unit directly to a Windows computer. (You are creating a two-node network), configure the NTMS IP address using the NTMS Configuration Wizard software, and then move the unit to your organization's network at the monitored site. This is required when first setting up the NTMS4p for use on wireless networks.

This temporary connection to the PC can be implemented with either: 1) a CAT5 crossover cable or 2) a switch/hub and two standard CAT5 Ethernet cables. Make sure that the NTMS Configuration Wizard has been downloaded to your PC before you disconnect it from the internet.

Option 1: Connect to your PC with a Crossover Cable

Try a standard CATx cable first. In many cases, depending on your computer hardware, a standard CATx cable will work fine. If it doesn't work you will need a crossover cable.

A crossover network cable can be purchased at any electronics store such as Best Buy. Crossover cables use the same RJ-45 plugs as regular Cat-5 Ethernet cables, although they have different internal wiring.

Connect the crossover network cable directly from your computer's network port to the NTMS4's network socket (the silver connector). Ensure that the NTMS is on.

Option 2: Switch or Hub

If you don't have a crossover cable you can connect your computer to a switch or hub with a standard network cable, and then connect the NTMS to the same switch or hub with another standard network cable, the NTMS4 is a 10 Mb/s device. It should be used on 10/100 switches on 10 Mb-or-less hubs.

Figure 5: Methods of Setting up a Two-Node Network for Configuration

Wireless Networking

You can use a wireless network to collect data – either directly with the NTMS4p or indirectly with the NTMS4i. The Tempurity System requires 24-hour access to the network, so your wireless network must be extremely reliable, secure, and seldom interrupted in order to consider it for network data collection using the Tempurity System. In general Networked Robotics recommends the use of wired networking for the monitoring of critical or high-value samples or applications.

NTMS4p

The Networked Robotics NTMS4p connects to standard Wi-Fi networks. (802.11.n)

The NTMS4p should be plugged into a wired network and configured with the NTMS Configuration Wizard with the appropriate Wi-Fi account and password for the wireless router. Once this is accomplished it can be rebooted and/or moved to the appropriate location for wireless network data collection and it can be configured and tested with all Networked Robotics and standard networking tools.

NTMS4i

The NTMS4i uses intermediate devices to accomplish wireless data collection. A Networked Robotics NTMS is connected via CAT5 to a wireless access point or bridge.

Some institutions mix methods, installing the NTMS in a wired fashion where available, and in a wireless fashion in rooms without any extant wired networking capability. This is perfectly acceptable.

Methods of installation, testing, and data collection are the same with wireless network as they are with wired networking.

Extending Connections

Scientific instruments and sensors can be installed more than 300 ft from Networked Robotics NTMS units. Every Networked Robotics interface can be extended using standard CAT5 cable, or in some cases, 6-pin phone cable using the simple, standard RJ45 coupler included with your interface. See the hardware manual for your Networked Robotics product for details. An extension to the Networked Robotics TPL3 digital temperature probe is shown below. The same method can be used to extend connections for all Networked Robotics products.

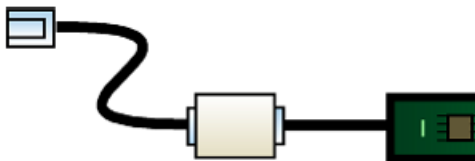


Figure 6: Use RJ45 couplers for Extensions

The NTMS Configuration Wizard




Once you have established network connectivity to your NTMS, you will run the NTMS Configuration Wizard software. The Configuration Wizard scans your network for any Networked Robotics NTMS devices, and lists them according to their Networked Robotics Unique ID and their current IP address. You will select the appropriate unit to configure by double-clicking on one of the units that were returned by the Wizard's search. Then enter the appropriate network and interface settings.

The NTMS Configuration Wizard is an important tool for managing the Tempurity System. It allows you to map a logical address, the IP address (the address used in the Tempurity System software for data collection) to the specific NTMS unit, the physical address, as shown by its Unique ID that is used to collect data from a specific instrument or sensor.

Downloading the NTMS Configuration Wizard

You can download the NTMS Configuration Wizard at www.networkedrobotics.com/download. The Wizard software can be downloaded directly to your computer and executed by clicking on the

black and white tape measure icon of the downloaded file .

Run the NTMS Configuration Wizard

A series of screens will be displayed to help you ensure that the NTMS is connected to the network properly. Then the program will scan your local network for any Networked Robotics hardware. The discover function of the Wizard finds any NTMS units on the current subnet. A subnet commonly includes the collection of all network devices on a floor or within a single building, but the definition of a subnet in your facility is determined by your network administrator.

The below shows an example of a single unit returned by the discovery function of the Wizard. Double click on the spreadsheet-style line showing the NTMS to be configured.

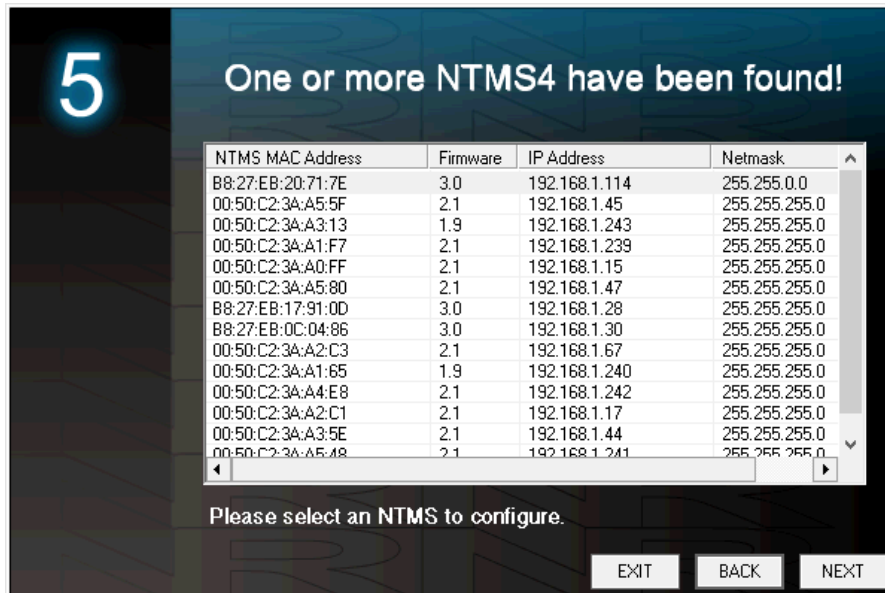


Figure 7: NTMS Units Returned by the Wizard's Discovery Function

NTMS MAC Address/Unique ID

The NTMS MAC Address shown in the table is the same as the Networked Robotics Unique ID as labeled on the side of your hardware. The numbers are always unique. No two network devices will have the same Networked Robotics Unique ID/ MAC address. The screenshot above shows both NTMSp and NTMS4i units on the same local network. NTMS4p units start with B8 27 EB. NTMS4i units start with 00 50 C2 3A.

Default IP

The default IP address of a new NTMS is 192.168.1.44 for NTMS4i and 192.168.1.28 for NTMSp units. Be aware that there is a potential for IP address conflict when several new units are connected to the network at once. Each must be distinguished with a *unique* IP address before data collection or standard network connectivity testing tools like “Telnet” or “Ping” (see below) can be used. Duplicate IP addresses will create unpredictable results.

NTMS Discovery does not always mean that Data Collection can Occur

The visibility of the device in the Wizard can create a misleading impression; just because a unit shows up in a NTMS Configuration Wizard discovery scan does not mean that Tempurity System data collection can occur. Both the ability to successfully test network data collection manually using “Telnet” and “Ping” and data collection through the Tempurity System are only enabled after you have provided an IP address and subnet mask that is appropriate for your company's network. Appearance in the list does not verify that network parameters have been set up correctly for your institution.

Viewing and Setting the NTMS's IP Address

Enter the static IP address that is appropriate for your company's network at the monitored site. Enter the appropriate Subnet Mask (Netmask) for that location as well. The Tempurity System can collect data from any local or remote network source over a local or wide area network. If you are unsure what values to use check with your network administrator.

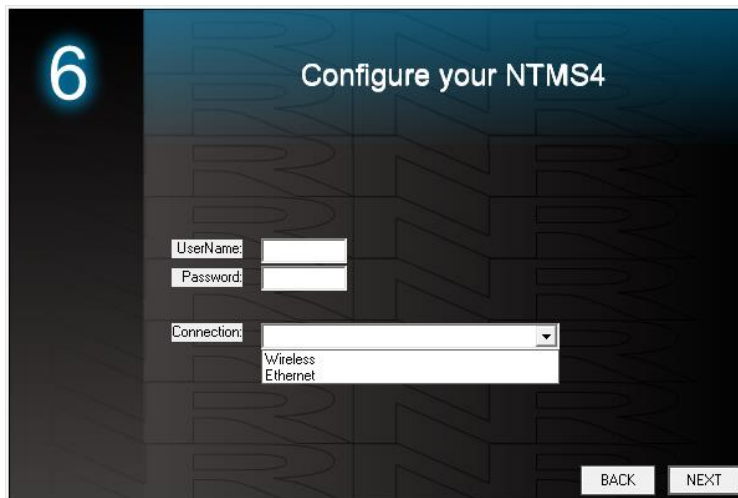
Why is a Gateway Address Not Required?

NTMS4i units do not require a gateway address because they cannot initiate outbound network packets. They respond only to inquiries from Tempurity Servers.

Setting the WiFi Access Data

This screen below is relevant to NTMS4p devices. You must click on a NTMS4p unit and then click on the WiFi button. Enter the Username or Network Name of the wireless router. Enter the access password or security key. Choose wireless and click "Next".

The NTMSp must hold the current wireless access data internally, otherwise when a power interruption occurs it will not be able to reconnect to the wireless network. Therefore the NTMS Configuration Utility needs to be run to update the access data for all NTMS units before the password is changed.



The screenshot shows a configuration utility window titled "Configure your NTMS4" with a large number "6" in the top left corner. The window contains three input fields: "UserName:" with a text box, "Password:" with a text box, and "Connection:" with a dropdown menu. The dropdown menu is open, showing "Wireless" and "Ethernet" options. At the bottom right, there are "BACK" and "NEXT" buttons.

Figure 8: Entering WiFi Access Data

Viewing and Setting the Interface, Instrument, or Sensor Type

Each connected NTMS data port must be configured for the type of instrument or sensor from which data collection will occur.

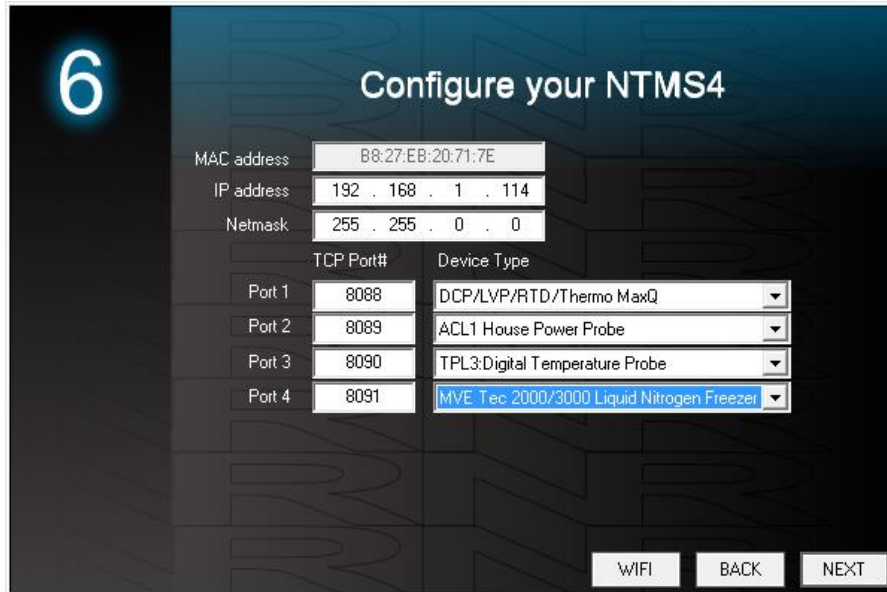


Figure 9: Configuring the Interface Type of the Connected Instrument or Sensor for each Physical Data Port of the NTMS

The figure above shows the simple pull-down list used to set the instrument or sensor type. Check the hardware manual for each Networked Robotics interface or probe product in order to determine the appropriate item to select.

The list of supported interfaces changes as new instruments and sensors are supported by Networked Robotics hardware. You require access to both the most recent NTMS Configuration Utility and the most recent NTMS firmware to support the latest instrument and sensor interfaces. Both can be obtained from the "[download](#)" section of the Networked Robotics web site.

Physically Connect the NTMS to your Data Source – An Example Direct Connection and an Example Sensor

Each scientific instrument or sensor is connected differently. The details of how to connect each interface are described in the individual Networked Robotics hardware manuals which are included with each interface or sensor product and are available online. Examples of the two broad classes of connections are given here: direct data connections using a [Thermo Revco Ultracold Freezer Interface](#) (Networked Robotics Product Number #30004) as an example and sensors/probes using The Networked Robotics [TPL3 digital temperature probe](#) (Networked Robotics Product Numbers #30002 and #30012) as an example.

Example of a Direct Data Connection Data Source: Thermo Fisher Scientific® Revco and Compatible Ultracold (-80°C) Freezers

The following diagram shows how some types of ultracold freezers can be connected to the Tempurity System. The system connects to the freezer's data port in order to collect the temperatures as they are reported by the ultracold's own internal temperature sensor. When using a direct connection, the value collected and stored by the Tempurity System is the same as the value shown on the instrument's front panel.

The figure below shows the connection from NTMS to the ultracold freezer. Cat5 patch cable is used to connect the NTMS hardware to an interface adapter (DB-9 to RJ-45) that connects to the serial port of the ultracold.

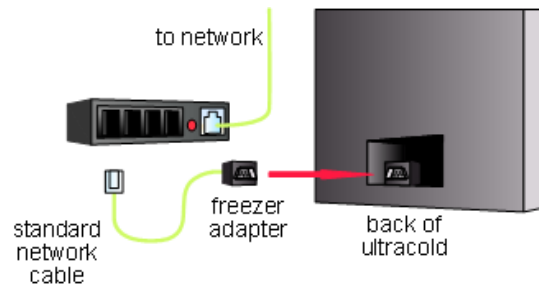


Figure 10: Method of Direct Connection to an Ultracold (-80°C) Freezer

Direct connections require that the instrument be powered on and working properly in order to acquire data. If the instrument is unplugged from wall power, the Tempurity System will issue a communication alarm for the monitored device. See Networked Robotics interface hardware manuals for specific connection instructions.

Example of a Sensor Data Source: Networked Robotics TPL3 Digital Temperature Probe in Refrigerators/ Freezers/ Incubators/ Ovens/ Rooms

Networked Robotics' proprietary TPL3 digital temperature probes are used to record the interior temperatures of refrigerators, freezers, some ultracold freezers, and other instruments. In these kinds of scientific instruments the probes are usually installed through the seal of the refrigerator or freezer door on the hinge side. The door must be open to install the probe.

Networked Robotics probes are constructed of ultra-thin wires that will ensure the integrity of the door's rubber seal. Make sure that the probe wire is installed flat and not twisted as it runs through the seal.

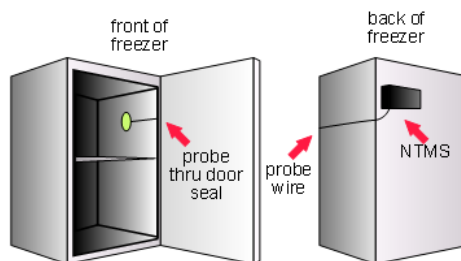


Figure 11: Method of Installation for collecting temperature from a Refrigerator using a Networked Robotics TPL3 Digital Temperature Probe

Some incubators have smaller openings between the instrument and the door. This makes probe insertion difficult. It may be helpful to remove the probe's dual-lock adhesive backing before inserting the probe through the hinge space. Add new dual-lock to the probe before affixing it to the interior wall of the incubator.

Do not install Networked Robotics TPL3 probes in ovens that reach temperatures of higher than 120°C. Networked Robotics RTD probes (Networked Robotics Product Number #30014) are appropriate for such high temperatures.

Probe Positioning

The location of the TPL3 or TPL3U probe within the device will have an effect on the temperature reading. Usually lower placement of probes results in colder readings. There can be temperature gradients of 5 degrees C or more in a full-sized refrigerator. In the devices of some manufacturers the temperatures near the cooling coils may be lower than the temperature at other locations within the refrigerator.

Networked Robotics recommends that probes be positioned $\frac{1}{4}$ of the way from the top of a refrigerator or freezer about one foot deep, if possible, on the door-hinge side wall. Placing the probe on the hinge side reduces the degree of fluctuation in temperature measurement caused by opening the door.

Probe Installation

The Networked Robotics TPL3 probe head includes a dual-lock strip that is designed to attach to an opposite dual-lock strip on the wall of the freezer. The wall of the freezer must be dry to apply. Use a paper towel to dry the region where the probe will be mounted. In some cases it may be necessary to warm the wall with a gloved hand for 15 or 20 seconds before the probe is affixed. The warmer and dryer the interior wall, the more likely that the dual-lock will adhere permanently. If the probe does not attach, remove the old dual-lock strip and try again.

The probe is not designed to be installed in environments where frost covers the interior wall of the device.

To remove the Networked Robotics TPL3 probe from the freezer wall, use a slight twisting motion while pulling the probe away from the wall of the freezer. Unplug the probe from the NTMS' RJ-45 temperature jack.

The Networked Robotics TPL3U probe is frozen directly to the wall of an ultracold freezer using a glycerin/water solution. See the TPL3 digital temperature probe hardware manual for details.

Placing Digital Temperature Probes in Glycerine Solutions

Many regulated customers will have a requirement for using temperature probes in glycerine for standard refrigerators and freezers. Use of glycerine solutions dampens the response time to temperature fluctuations. Some regulatory standards require the use of temperature probes in

glycerine, citing that appropriate volumes be used that reflect the mass of any at-risk material. Networked Robotics TPL3 digital probes are fully waterproof and can be used in these solutions indefinitely.

Extensions

You can extend any connection from your scientific instrument or sensor to your NTMS with standard CAT5 or 6-pin phone cable using the standard RJ-45 coupler provided with most interfaces. The instrument or sensor can be placed 300ft or more away from the NTMS. See your specific hardware manual for details.

Monitoring via Standard Network Wall Plates

The sensors or direct connections responsible for the monitoring of refrigerators, freezers, and other instruments can be plugged directly into the same wall plates that are commonly used to provide network to your personal computers.

Normally personal computers are connected to the network through the CAT5 wiring in your building that all meet in a network closet located somewhere on your floor or building. In the network closet there's a panel (shown below right) called a patch panel that allows connections to the wall plate in your office. Common connections are network or phone.

You can use this infrastructure to collect data for Tempurity.

In this case the NTMS units to which these sensors are connected are mounted in racks or shelves in a network closet. Each data port of the NTMS as shown below right is connected or "patched" to an RJ45 jack on one of your standard network wall plates.

The figure below shows an example of a room temperature monitoring application. The Networked Robotics TPL3 probe is plugged in directly to a wall plate which in turn is connected through the building's CAT5 infrastructure to an NTMS (the link between the wall plate and the patch panel is not shown). Temperature is being measured from 3 other rooms or labs, which are not shown in the figure below. In this case the NTMS unit is installed in a network closet, and connected to the probe via the building's CAT5 infrastructure.

For facilities that have advanced network infrastructure this method makes it very easy to connect a large number of monitored devices in just a few hours.

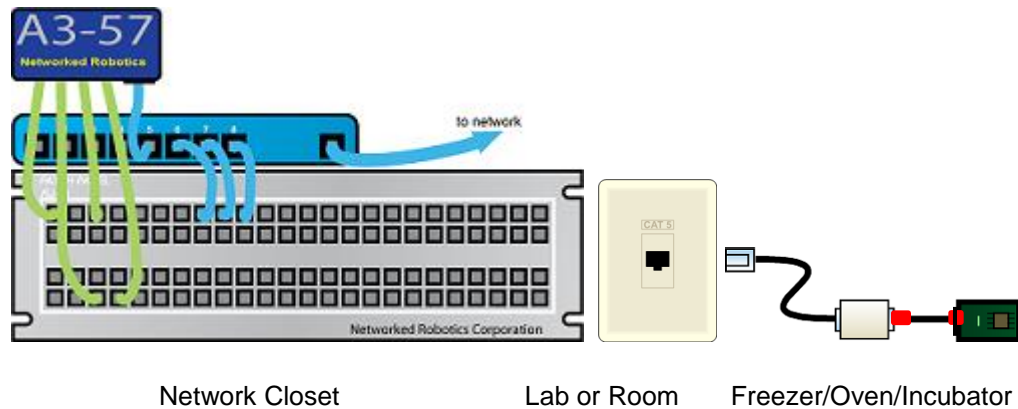


Figure 12: A Networked Robotics TPL3 digital temperature probe used for Measuring Room Temperature as Installed in a Standard Network Wall Plate.

Testing Data Collection through the Network Manually

Once the instrument or sensor is physically connected to an NTMS we recommend that you test the ability to acquire remote data manually. We recommend that you do this before configuring this monitored device for automatic data collection through the Tempurity System software. By assuring that basic network connectivity and network data collection are possible BEFORE Tempurity System configuration, you help to identify the source of connection problems early in the connection process.


To test manually you will use some common operating-system-resident network testing commands.

“Ping” and “Telnet” commands are available on Windows XP computers by default, but must be manually enabled in Windows Vista and Windows 7. On these operating systems use “Control Panel → Programs and Features → Turn Windows Features on or off” and check “Telnet” to enable this feature.

The Ping Command

Ping is used in order to confirm basic, network-device-to-network-device connectivity. Make sure that your NTMS is connected to your network. From any computer go to the Windows command prompt via “Windows Start → Run → Enter *Cmd*” and then at the black screen type

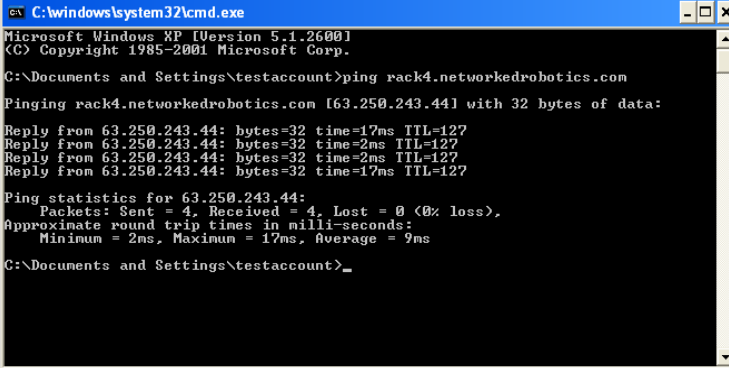
“Ping *IPaddress*”

where “*IPaddress*” is the same IP address you entered for the device in the NTMS Configuration Wizard. 

If the NTMS responds to the ping) proceed with the connection, otherwise, examine your configuration. A high ping-time is not indicative of a Networked Robotics hardware failure, but ping errors do suggest such a failure.

If the ping does not respond at all then there is a failure in basic network connectivity. This indicates the kind of problem that your network administrator would have in connecting any other kind of network device to your network. Was the right IP address configured for this region of the

network? Is there a firewall blocking the message? Your Network administrator may be helpful in analyzing the problem.



```
C:\windows\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\testaccount>ping rack4.networkedrobotics.com

Pinging rack4.networkedrobotics.com [63.250.243.44] with 32 bytes of data:

Reply from 63.250.243.44: bytes=32 time=17ms TTL=127
Reply from 63.250.243.44: bytes=32 time=2ms TTL=127
Reply from 63.250.243.44: bytes=32 time=2ms TTL=127
Reply from 63.250.243.44: bytes=32 time=17ms TTL=127

Ping statistics for 63.250.243.44:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 17ms, Average = 9ms

C:\Documents and Settings\testaccount>_
```

Figure 13: A Successful Ping Response


The Telnet Command

If the Ping responds, go a step further and use the Windows-based “Telnet” utility from any PC. The use of “Telnet” tests the ability to obtain measurements through remote network data collection from the instrument or sensor.

From Windows choose “START”, then “RUN”, and then type “CMD” and return. At the black screen type

“Telnet” *IPaddress Port*,

where *IP* is the same IP address you used in the “Ping” command above, and *Port* is the network TCP port address (defaults are 8088 to 8091 for the physical data ports 1 through 4 of an NTMS)

as selected by your use of the NTMS Configuration Wizard . If you are successfully connected through the network you will see only a blank screen.

Type the command character that is indicated by your monitored device type as specified in your interface hardware manual. For example, a capital “T” for any temperature type of monitored device. The resultant temperature and the associated checksum value will be returned. For other types of monitored device a different command character will be entered, for example “H” for humidity. See your Networked Robotics interface or sensor hardware manual for details. An error will be returned if the NTMS does not sense a successful connection to the instrument or sensor.

If a data value is returned, you can now safely configure the Tempurity Server for data collection knowing that proper physical connectivity has been established.

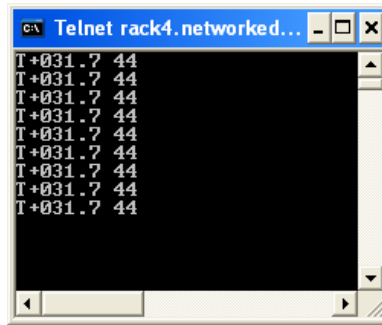


Figure 14: A Successful Response to Several Temperature Requests through Telnet

The flowchart below is designed to help you identify connectivity problems:

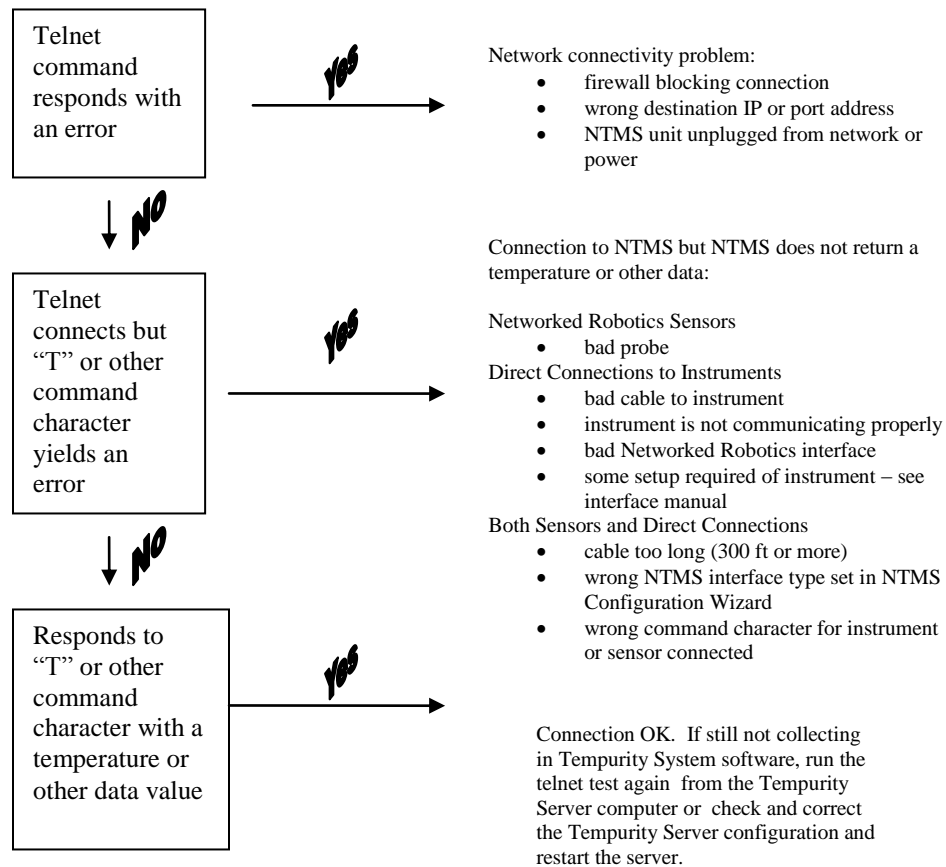


Figure 15: Flow Chart for Testing Network Data Collection

Once measurements can be collected manually through the network, you can be sure that the instrument is connected properly and that this monitored device can be configured for automatic data collection through Tempurity.

The Tempururity Server



The Tempururity Server's function is to collect temperatures and other kinds of data from each monitored device at the scheduled time interval and to store that data on the Tempururity Server computer. The server program responds to requests from all Tempururity Monitor clients and sends alarm notifications to the outside world. The software runs in the background on your computer and has no direct user interface, however the Tempururity Server Configuration Utility, indicated by the black-and-white wrench icon, writes information to files that specify the operation of the Server. The information in these files is loaded into the server program every time it is restarted.

Dedicated vs Shared Use Computers as Tempururity Servers

In general, Tempururity Server computers need not be dedicated to the Tempururity System however some software conflicts with Tempururity System operation. The more application software loaded on your machine the more likely it will be that such a conflict exists. Therefore keep your other applications to a minimum on Tempururity Servers. Make sure that those other applications are not automatically downloaded.

Tempururity Servers are sensitive to downtime. Scheduled maintenance that is required for other applications will temporarily suspend data collection and alarm notification. In general a Tempururity Server should not share a computer with an application that requires any down-time, generates very high network traffic, could generate an excessive CPU load, or automatically updates. The Tempururity Server software will conflict with any web server or web hosting software such as *Internet Information Services* and *Apache*. (Any software that uses TCP port 80)

Downloading the Tempururity Server Software

The Tempururity Server can be downloaded and installed from the Networked Robotics web site

from  at <http://www.networkedrobotics.com/download/>

You may also want to download the Tempururity Monitor  from the same location.

See the section of this manual on the Tempururity Monitor

You must have an account with "Administrator" access in order to install the Tempururity Server. Major versions of Tempururity components cannot be mixed; Version 1 Servers must be used with Version 1 Monitors and Version 2 Tempururity Servers must be used with Version 2 Tempururity Monitors.

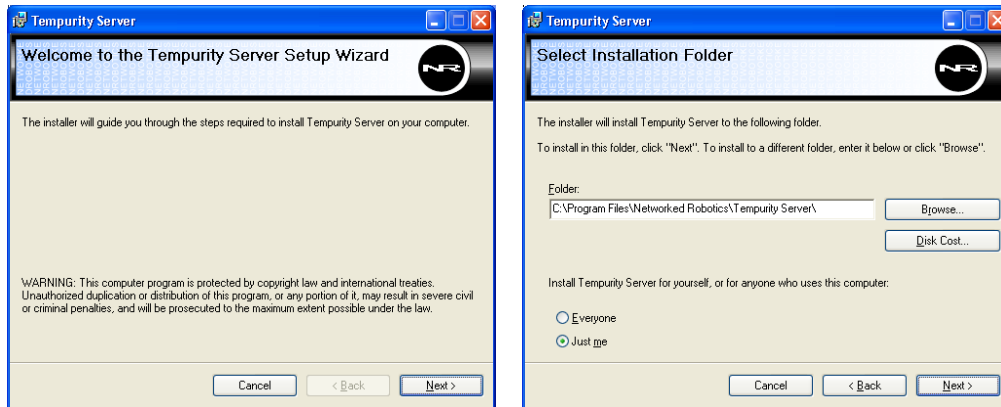


Figure 16: Tempurity Server Software Installation

If a previous version of the Tempurity Server is installed you may need to uninstall the previous version using the Windows “add/remove programs” option of the control panel as shown in the figure below.

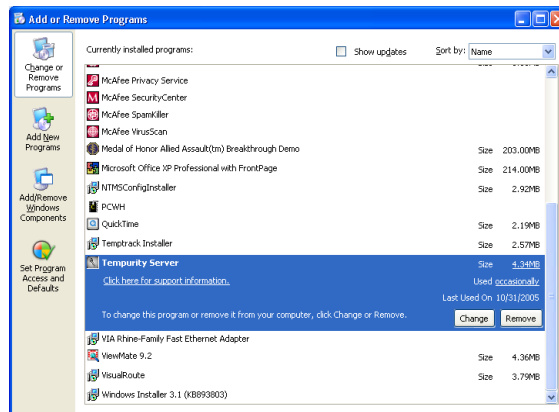



Figure 17: Uninstalling the Previous Version of the Tempurity Server Software

When the Tempurity Server software is installed, an icon will appear in the Windows taskbar. Although the icon is displayed as green after installation, “monitored devices” must be configured manually in the Tempurity Server Configuration Utility  before data can be acquired.

The Tempurity Server Status Icon on the Windows Taskbar

The Tempurity Server status icon in the Windows Taskbar is automatically displayed whenever a user is logged into Windows. The taskbar shows at-a-glance whether the Tempurity Server is running and thus that data collection is possible. It also allows an easy way to start, or stop data collection.

If you are connecting to a Tempurity Server computer through remote desktop, the taskbar is usually not visible. You will need to use "Control Panel-> Administrative Tools->Services" to see the status of the Tempurity Server as described below.

Server Running

When the Tempurity Server is running you will see the following icon in the taskbar:



The server may or may not be collecting temperatures and other data if the taskbar icon is green. To see whether data collection is occurring, you will need to view the Tempurity Monitor where green icons indicate that data is being collected as expected. The taskbar icon indicates only whether the server software is operating and has no relevance to the collection status of any of the monitored devices.

Under conditions of normal network connectivity Tempurity Monitors that are connected to this Server show the Server's name in white characters as in the "localhost" that is displayed in the screenshot below. "Localhost" is the network name for "this computer that we are on".



Figure 18: Tempurity Monitor Connected to Tempurity Server

Server Stopped

When the Tempurity Server is stopped, the Tempurity Taskbar icon shows:



All of the Tempurity Monitors that are connected to this Server will always show the Server name in red as indicated in the screenshot below. When the Tempurity Server is stopped, no data collection can occur and all connected Tempurity Monitors are unable to initiate Alarm Notifications. No Alarm Notifications can be sent when the Tempurity Server is stopped.

When a Tempurity Server is stopped, all of the Tempurity Monitor displays, status icons and graphs, for this server are essentially “frozen”, showing the last-known alarm statuses. When the Server is restarted, the Monitor is able to automatically reconnect and obtain real-time data once again.

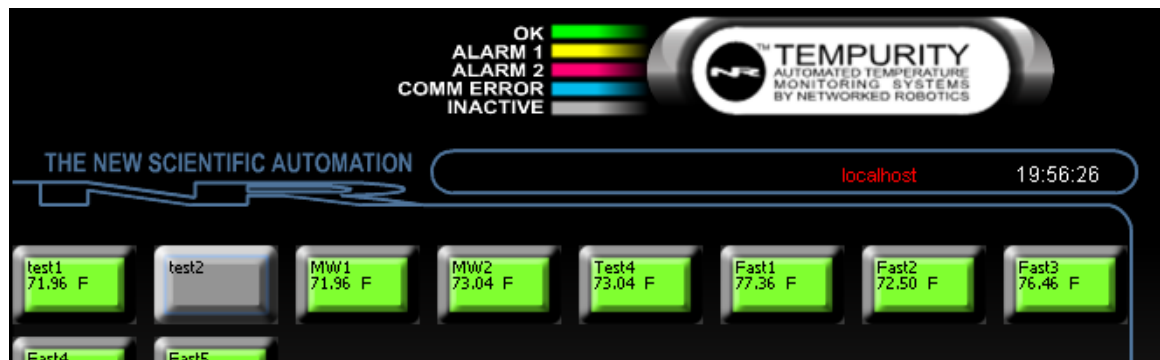


Figure 19: Tempurity Monitor Connection to the Tempurity Server is Lost

Starting and Stopping the Tempurity Server using the Taskbar

You can initiate or halt data collection by starting or stopping the Tempurity Server program by clicking on the Tempurity Server icon in the Tempurity Taskbar. The server must be restarted every time that there is a configuration change that needs to go into effect. While usually the restart is handled in the Tempurity Server Configuration Utility, there are times where it is convenient to use the Taskbar for this purpose.

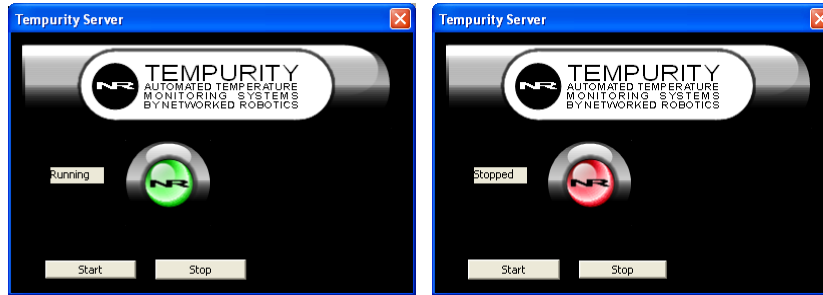


Figure 20: Starting and Stopping the Server through the Taskbar Icon

Starting and Stopping the Tempurity Server using Windows

You can start and stop the Tempurity Server through Windows as well as by using the Tempurity Taskbar Icon. Choose “Start→ Control Panel → Administrative Tools → Services” then scroll to the line for “Tempurity Server”. Right-click on this line. You will be able to start, stop, and restart as needed. The same method can be used on the Tempurity Monitor service, however depending on Windows operating system multiple instances of the Tempurity Monitor (Monitor0, Monitor1, Monitor2 etc.) can run on a single computer whereas only one Tempurity Server runs on a single computer (The Tempurity Server can run under Windows Virtual Machine, in which case more than one Tempurity Server can run on a single physical computer).

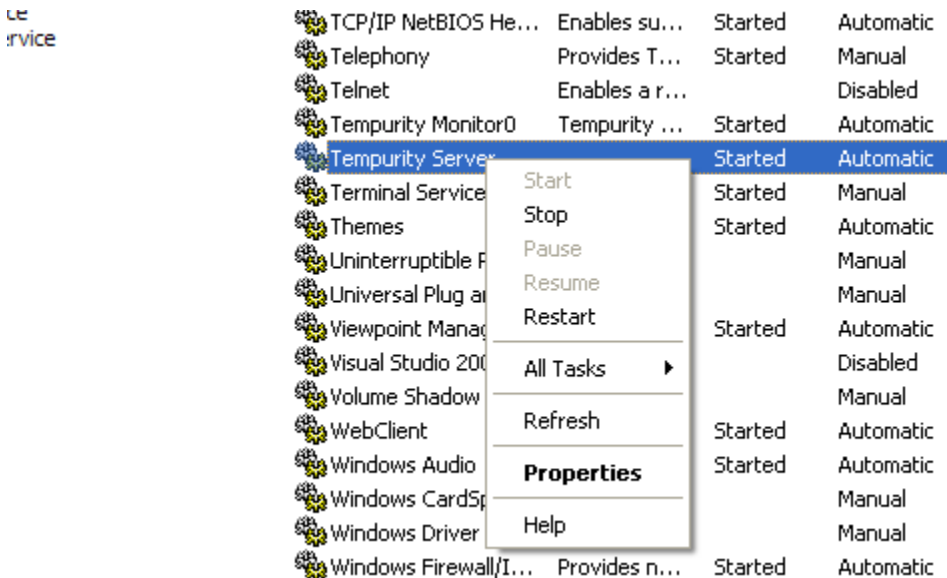


Figure 21: Starting and Stopping the Tempurity Server through Windows

The Tempurity Server Configuration Utility

The Tempurity Server must be instructed on the network source from which to collect data and must be given the alarm definition criteria that will indicate under what combination of circumstances an alarm condition will be issued. These parameters are entered through the Tempurity Server Configuration Utility.

Open the Tempurity Server Configuration Utility. The program's icon is a wrench as shown below. You



can invoke the program by "Start→Programs→ Tempurity Server→Tempurity Configure".

The first time you run the program no monitored devices will be defined. You will need to manually add each monitored device, making sure to enter the appropriate network, Id, and alarm criteria.

The main display of the Tempurity Server Configuration Utility is shown below. In the example below 11 monitored devices are identified and are thus are enabled for network data collection.

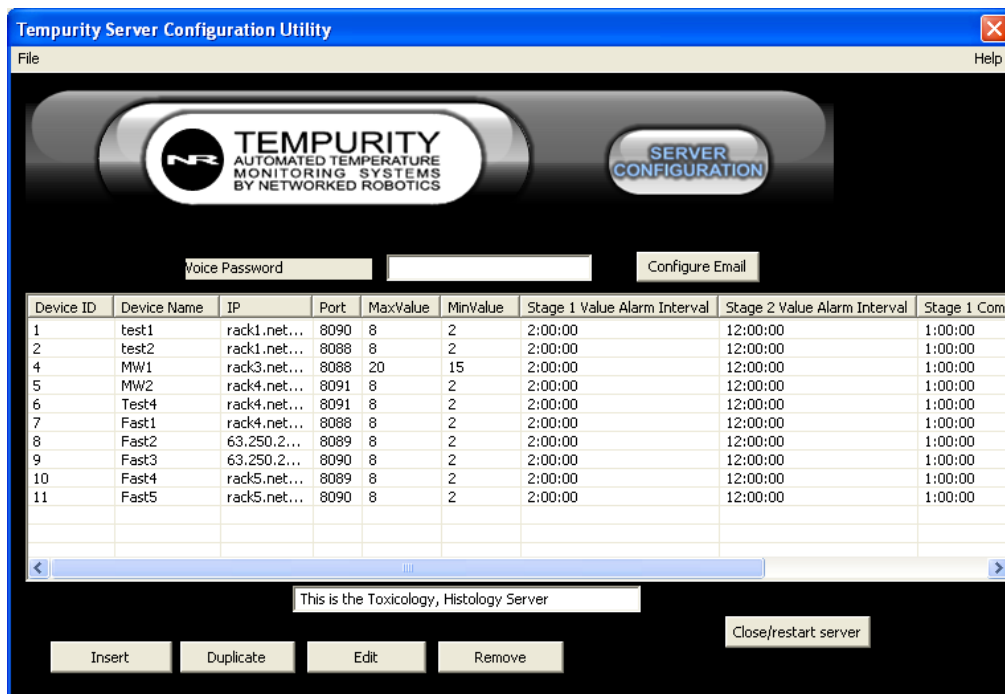


Figure 22: The Main Tempurity Server Configuration Utility screen.

Configuring Monitored Devices

The following buttons are used to manage the list of monitored devices:

| | |
|------------|--|
| Insert: | Adds a new monitored device to the end of the table |
| Duplicate: | Adds a new monitored device to the end of the table, but fills as defaults in each field the current settings for the device highlighted |
| Edit: | This is used to change the settings for the selected monitored device |
| Remove: | Removes the selected monitored device |

On the Menu Bar under the "File" option are:

| | |
|--------------------|--|
| Save: | Saves the settings to the configuration files |
| Revert: | Loads the currently saved settings from the configuration files, thus overwriting all recent but unsaved changes. Note that once you save a new configuration you can no longer revert to the old settings unless you manually reload the history files. |
| Clear All Entries: | Clears all monitored devices. Does not take effect until "Save" is selected. |

When you double-click on a single line showing a monitored device the following data-entry screen is shown.

This screen requires you to provide ID, network source, and alarm criteria for a single monitored device.

In Tempurity terminology a monitored device is really a data stream and not a physical entity. For example a Networked Robotics Forma® incubator interface can collect temperature, humidity, carbon dioxide, and oxygen concentration from a single interface and thus from a single network address. For this kind of connection four Tempurity System monitored devices are created, one for each parameter. Each Networked Robotics hardware manual provides instructions on how to configure this screen.

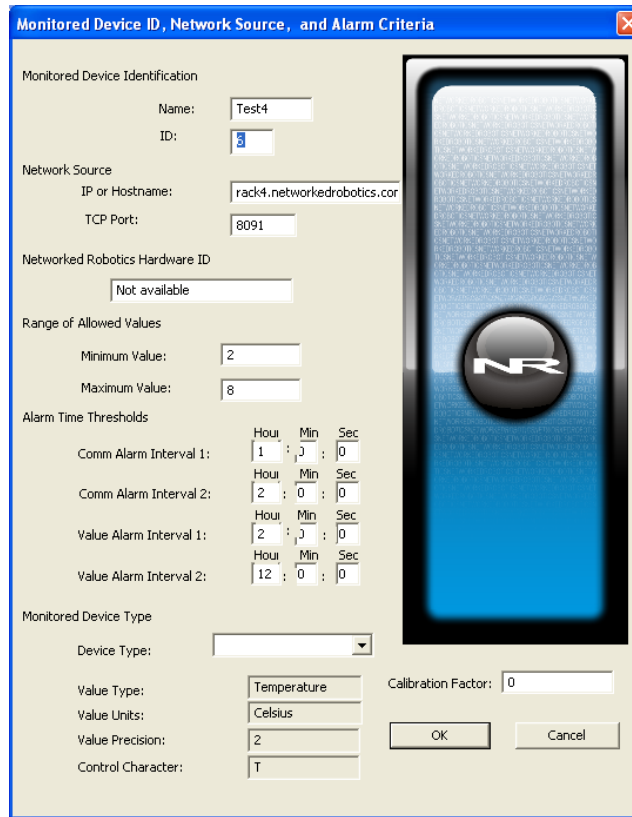


Figure 23: Configuring a Tempurity System Monitored Device

The following table provides an explanation of each field:

| Variable Name ¹ | Explanation | Legal Values |
|----------------------------|---|------------------------------|
| Monitored Device Name | Unique name for the monitored device. This is your organization's name for the freezer. Usually this name will be labeled on the front of each refrigerator or freezer. | String (1-9 characters long) |
| Monitored Device ID | Unique number for the monitored device. Data will be stored by filename under this number. | Number between 1 and 999 |

| | | |
|--------------------------------|--|--|
| IP or Hostname | IP address or hostname of the Networked Robotics' NTMS to which the monitored device is connected. | Legal IPV4 address or hostname as defined in DNS Server A - record |
| Port | The network TCP port address to which the monitored device is connected. These port addresses are selected when you use the NTMS Configuration Wizard to set the network parameters of the NTMS hardware, but by default physical port 1 is 8088, port 2 is 8089, port 3 is 8090, and port 4 is 8091 | Number between 0 and 65535 |
| Networked Robotics Hardware ID | This entry field is free-form but is meant to hold the Unique ID of the particular NTMS from which data is collected. See the yellow and black side label on the NTMS. | |
| Stage 1 Value Interval | Time out-of-range in hours, minutes and seconds required to trigger a stage 1 alarm. Seconds are allowed in this field but alarm resolution is about 10 minutes. It is not recommended to choose a value less than 10 minutes. | Positive Integer |
| Stage 2 Value Interval | Time out-of-range in hours, minutes and seconds to trigger a stage 2 alarm. Seconds are allowed in this field but alarm resolution is about 10 minutes. It is not recommended to choose a value less than 20 minutes. | Positive Integer |
| Stage 1 Comm Alarm Interval | Time out-of-data-communication in hours, minutes and seconds that is required to trigger a first stage communication alarm. Communication alarms usually occur 10 minutes after this specified interval. It is not recommended to choose a value less than 10 minutes. | Positive integer |
| Stage 2 Comm Alarm Interval | Time out-of-data-communication required in hours, minutes and seconds in order to trigger a second stage communication alarm. Communication alarms usually occur 10 minutes after this specified interval. It is not recommended to choose a value less than 20 minutes. | Positive integer |
| Minimum Value | Data Value in default units. If the data value drops below this value for the alarm interval time, it will trigger an alarm. This minimum value should be less than the maximum value. | Integer |
| Maximum Value | Data Value in default units If the temperature goes above this value for the alarm interval time, it will trigger an alarm. The high temperature should be higher than the Low Temp parameter. | Integer |

| | | |
|-----------------------|---|---|
| Monitored Device Type | Examples are "Temperature", "Humidity", "Volts", and "Custom". These are predefined in the Tempurity Configuration Utility Software. To choose a unique type such as "Flood" or "Door" choose "Custom". | |
| Value Type | If this is a custom type, you can enter whatever you want here, otherwise it is filled in for you automatically based on the Monitored Device Type. | |
| Value Units | If this is a custom type you can enter whatever you want here, otherwise the units are filled in for you based on the Monitored Device Type that you selected. | Practically speaking, keep this to 9 characters or less, longer are OK, but will sometimes be displayed incompletely. |
| Value Precision | The number of decimal places stored in the data file. | Should be no more than 3. |
| Command Character: | The Command Character is sent to the NTMS to request data. Command characters are consistent among monitored device types. Every temperature source is "T". Every humidity source is "H". See the individual hardware manual for your interface, which lists the available types and thus command characters for a particular physical interface. | A single character supported by the instrument and sensor to which you are connected. |
| Calibration Factor | The calibration factor is a constant value that is added or subtracted from the network-collected measurement. Both the actual reading and calibration-corrected values are stored in the data file but only the corrected values are displayed. | |

Figure 24: Tempurity Server Configurable Variables

Custom Monitored Device Types

The ability to define Custom Monitored Device Types is a powerful feature of the Tempurity System designed to enable the monitoring of any parameter.

As an example, take a custom monitored device of type "Flood" that detects the presence or absence of water. In this case the Networked Robotics DCP Probe (Networked Robotics Product #30008) is connected to a Waterbug® Flood sensor. Since the Networked Robotics DCP probe/Waterbug can only detect a flood or noflood condition, and not for example water level, the detection of a flood condition is unitless.

The following shows how a custom monitored device of type "Flood" is created. Command character is "T" in this case, because the default Networked Robotics Dry Contact Probe command character is "T", as indicated in the hardware manual for the DCP.

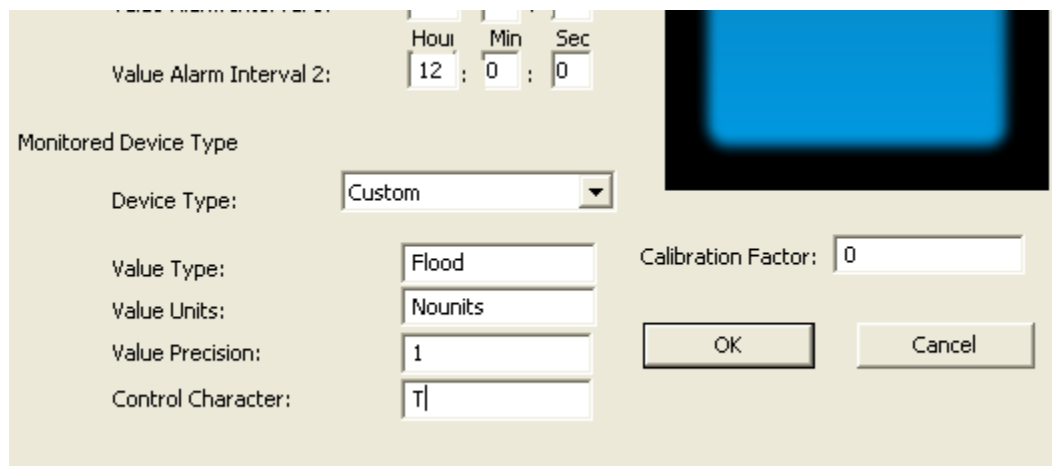
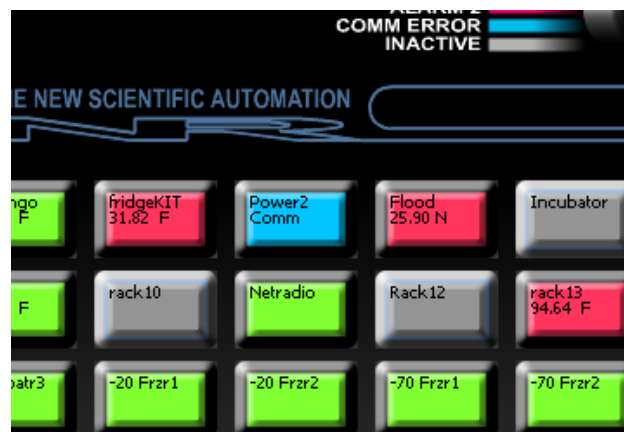


Figure 25: Defining a Custom Monitored Device of Type "Flood"

The following shows how the "Flood" monitored device type looks in the Tempurity Monitor:



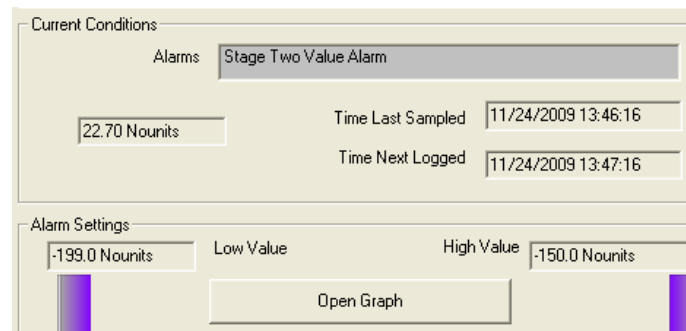


Figure 26: Tempurity Monitor Screens for a Custom Monitored Device with the Type of “Flood” and units “Nounits”

Configuring the Server Identity

The data-entry field shown below the monitored device table is designed to be an indicator or reminder of the Tempurity Server's function. It is the most useful in organizations that are running multiple Tempurity Servers simultaneously because it makes it easier for an operator configuring a list of monitored devices to distinguish one Tempurity Server from another. The field's only function is to display a saved message to users of the Server Configuration Utility.

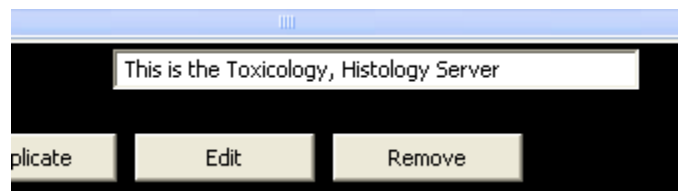


Figure 27: Free-form Entry Field to Describe this Tempurity Server

Enabling E-mail and Text Message Alarm Notifications

In version 2 of the Tempurity System alarm notifications are implemented by Tempurity Server computers. The Monitor client sends a message to the server computer which in turn communicates with the SMTP mail servers that are responsible for sending the message.

In version 2 of the Tempurity System all non-voice alarm notifications are sent to a mail server by the Tempurity Server. The process of configuring Tempurity's mail parameters is similar to that of configuring the mail parameters in a mail client like Microsoft Outlook. An SMTP mail server must be entered and tested in the Tempurity Server Configuration Utility in order for e-mail and text alarm notifications to be sent.

Usually, authentication information, a username and password, will be sent to the mail server through an authenticated SMTP protocol. This authentication allows the mail server to trust the

request to send mail. Some mail servers allow usernames and passwords to be encrypted using the SSL protocol.

The screen below must be completed and tested fully (except when using Exchange mail servers) in order for alarm notifications to be sent by Tempurity. The figure below shows example settings that could be used to send Tempurity alarm notifications through a Gmail mail server and account.

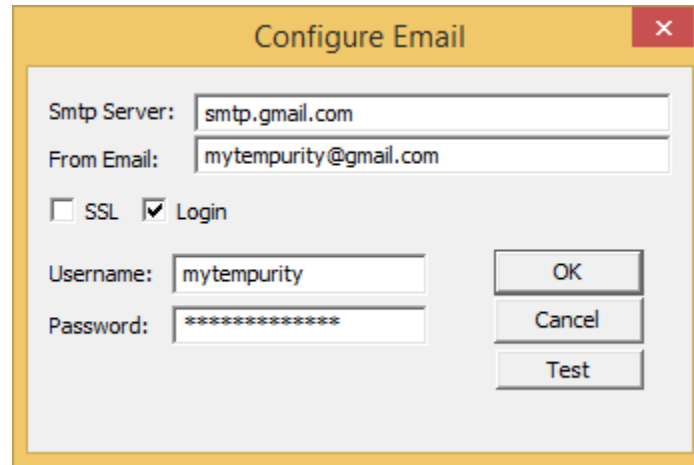


Figure 28: Configuring E-mail Alarm Notifications

| | |
|---------------|---|
| Smtip Server: | The network address (IP or domain name) of the mail server that you are logging into |
| SSL: | Encrypts the username and password. Must be supported by the mail server you have selected |
| Login: | Uses authenticated SMTP to initiate the sending of a mail message. You must provide a username and password to use this feature |
| From E-mail: | The mail account from which Tempurity alarm notifications will be sent |
| Username: | Usually the part of the mail address before the “@” sign. Your mail account name. |
| Password: | The password to that mail account |

Testing the Ability to Send Mail

Once mail server parameters have been entered you should test them from the Tempurity Server before defining any alarm notification groups in any Tempurity Monitors. To do this click on the “Test” button in the E-mail Configuration dialog. Then enter the “To” address of the test e-mail and a short descriptive message. Click the “Send” button. An hourglass may appear as the e-mail test can take a minute or more. If the test returns an error, check your entries and try again. If the test is successful, any Tempurity Monitors with network access to this server will be able to send mail and text message and voice alarm notifications.

Is Your Institution Blocking Outbound Mail?

Some institutions block outbound mail. To find out whether this is true at your site for this machine go to the command prompt in Windows and type:

Telnet smtp.gmail.com 25

(Note that the Telnet client must be turned on at Control Panel – Programs – Programs and Features – Turn Windows Features on and Off – Select Telnet Client.) Then bang on the keyboard a bit. If any kind of response is received your institution allows connections to external mail servers. If an error is received on Telnet initiation then mail is blocked.

Microsoft Exchange Servers and Testing the Ability to Send Mail

There are some limitations in the ability of the Tempurity System to test connections to Microsoft Exchange mail servers. The server-side Test function will always fail when the mail server you are connecting to is a Microsoft Exchange® mail server. Despite the failure of the server-side test system Tempurity is capable of sending alarm notifications if the address and login parameters have been entered appropriately. To test a connection to Exchange, you will have to test your settings using the Tempurity Monitor. Make sure that the Monitor Name setting in the Tempurity Monitor is exactly 10 characters. Then define an alarm notification group and ensure that the message is received. If the alarm notification is not received, check the entry of the "Configure Email" parameters in the Tempurity Server Configuration Utility.

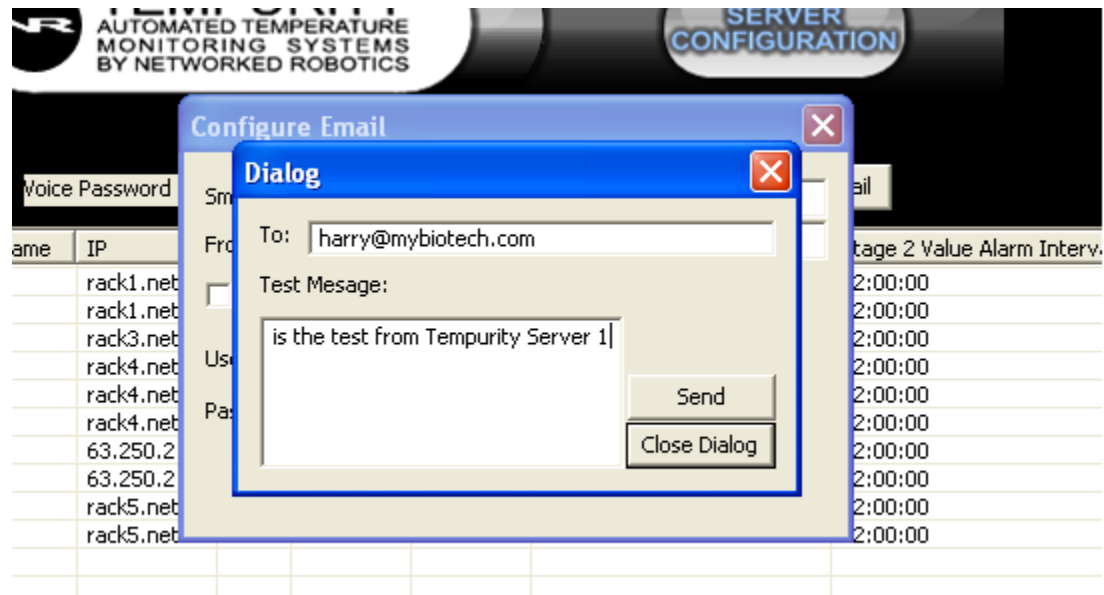


Figure 29: Testing the Ability of the Tempurity Server to Send Alarm Notifications

If the test is not successful, and you are sure that you have entered the SMTP information correctly, try using a Gmail or other mail server and account. Networked Robotics can provide a mail account if needed for temporary testing.

Using Gmail as your Alarm Notification Mail Server

Networked Robotics recommends the use of a Gmail for sending Tempurity System alarm notifications. Gmail is a reliable, standard interface that is easily used as a Tempurity System alarm notification engine. From your Gmail account you will be able to track all sends of alarm notifications by logging in and viewing the "Sent" folder.

The appropriate e-mail configuration parameters for Gmail are shown in the screenshot above.

You must register for a Google account in order to use Gmail.

Important: To use Gmail as a Tempurity Sender you must Enable the "Less Secure Apps" Setting!

Login to your Gmail account and then go here.

<https://www.google.com/settings/security/lesssecureapps>

or

Go to the "[Less secure apps](#)" section in My Account.

Next to "Access for less secure apps," select **Turn on**. (**Note to G Suite users:** This setting is hidden if your administrator has locked less secure app account access.)

You can also use SSL to connect to a Gmail mail server if desired.

Enabling Voice Alarm Notifications

Voice alarms are an alarm notification type in which a robotic voice speaks the alarm notification message.

Networked Robotics must specifically authorize voice alarm notifications from Tempurity Servers.

In order to enable voice alarm notifications at your site two things are required:

- 1) A voice password obtained from Networked Robotics, which must be entered into the Tempurity Server Configuration Utility
- 2) Networked Robotics must authorize your Tempurity Server(s) externally-known IP address or addresses.

Voice passwords are obtained from Networked Robotics Corporation. The external address of your Tempurity Server(s) must be provided to Networked Robotics and enabled by Networked Robotics for voice sends. To find the relevant external address, from your Tempurity Server computer go to a website such as:

<http://whatismyipaddress.com/>

Send the request to enable voice alarm notifications to support@networkedrobotics.com.

Networked Robotics recommends the use of multiple alarm notification types for communicating alarm conditions. In the current implementation of voice alarm notifications, your phone is called up to three times, after which the system stops making attempts. Networked Robotics recommends using e-mail or text alarm notification types in conjunction with voice alarm notifications. In this way a persistent record is made of the alarm condition that could be missed with just a voice call. Voice alarms currently cannot be used with phones that are on extensions or require other than a 10-digit phone number.

Once your voice password is entered, and your external address is registered with Networked Robotics. Test voice alarm notifications by defining an Alarm Group in the Tempurity Monitor with at least one alarm notification address with type "Voice".

Editing Tempurity Server Configuration Files Manually

The set of text files that define Tempurity Server operation are called configuration files. These are created by the Tempurity Server Configuration utility and can be found in the Tempurity\configs directory. The absolute location of the directory is listed in the appendix.

Editing configuration files manually is not recommended, but some advanced users may consider this option with caution.

One possible option is to change the data collection period which is set by default to 1 minute. To do this, use an editor like notepad to change the "logInterval=60" to the appropriate data collection period in seconds. Data collection periods other than the default were not tested as part of the Tempurity System regulatory validation and should be used at your own risk.

The low limit of reliable data collection period depends heavily on the characteristics (speed, CPU, memory, other applications) of your server computer.

Configuration Histories and Restoring Previous Configurations

Tempurity Server configuration files are stored in a history directory whenever changes are made. The history directory is created for any single date on which changes are made and can hold one configuration. This means that only the last changes on any given day are stored. Earlier configurations made on that day are not stored.

To retrieve a configuration we recommend manually making a backup of the configuration directory (see Appendix C for location of files). Then copy the files in the history directory to the "Config" directory (the active configuration files). Confirm the proper configuration using the Tempurity Server Configuration Utility and then restart the Tempurity Server to restart data collection.

Setting the Windows Options on your Tempururity Server Computer

In order to assure that data collection occurs constantly, it is important that you change the Windows settings on the Tempururity Server computer.

The most important settings are those having to do with power loss recovery. You should set your Windows power scheme to "Power Always On", and set your PC's BIOS to "Restore on AC Power Loss" or equivalent. These settings assure that when power is interrupted, and then restored, processing, and thus data collection resumes automatically. Appendix F describes these changes in more detail, including a full list of recommendations for setting your PC for use as a Tempururity Server or Monitor.

Tempururity System Data

The following describes the data that is collected and stored by the Tempururity Server.

Measurement Interval

The system collects temperatures and other data at approximately 1-minute intervals by default. The collection period may vary by a few seconds. If a communication failure occurs, the program will try again at one-minute intervals until another several minutes have passed. If no measurement is successfully made at this time, a communication error has occurred and the icon for this monitored device on the main monitor screen will turn blue.

Measurement target times are independent, each device is on a different time schedule. The target measurement times can shift relative to other monitored devices, and to the initial measurement schedule over time as communications interruptions and the latency mentioned above shifts target data collection times.

Although the data measurement period can be changed from the default of one minute, (see above) this capability is not recommended.

Systems that are CPU-overloaded may have higher-than-normal measurement latencies. The discrepancy between target and actual measurement times can be 10 seconds or more on such systems.

Time of Data Collection

Tempururity stores each collected value with a Universal Time. The Universal Time on February 13, 2009 at 23:31:30 was 1234567890. Universal Time is time-zone independent. See Wikipedia on [Unix Time](#) for more information. Times displayed in the Tempururity Monitor are all displayed in local time.

Units

Data is always saved in default units. For Temperature this is Celsius, for humidity it is percent relative humidity. Temperature can be viewed in the Tempurity Monitor in either Celsius or Fahrenheit, and all messages are sent in the selected scale.

Location

Temperature and other data are stored in Windows text files on the Tempurity Server. Data files are stored in subdirectories based on the monitored device's numeric ID and the date. There will be a time-value data file for each monitored device for each day that on which any data is collected. A data file might not be created for a given day if a persistent communication error exists for the monitored device on that day or days.

Each time-value data file has an associated Cyclic Redundancy Check (CRC) file which is used to verify the validity of the data collected on that day.

Appendix C lists the location of the Windows text files that store Tempurity System data.

Data Retention

There are no mechanisms for deleting data through the Tempurity System. If you wish to delete information, you must delete the data files through the operating system.

Networked Robotics does not recommend deleting any data files at any time, especially in regulated environments.

Data Backup

Tempurity Data should be backed up using your normal Windows file backup procedures, ensuring that the backup procedure covers the files specified in the "Location" heading listed above. Regulated customers will want to include backup procedures as part of a comprehensive written monitoring procedure. Consider using built-in disk redundancy, redundant Tempurity Servers, or automatic network-based backup procedures.

Accuracy

The accuracy of any data acquired by the Tempurity System is based on the accuracy of the specific sensors or instrumentation connected to the Networked Robotics NTMS network hardware. You must reference the manufacturer's product documentation for accuracy information.

The Networked Robotics TPL3 digital temperature probe is based on the Dallas/Maxim DS18B20Z integrated circuit. The Dallas chips show the highest accuracy at physiological temperatures and the lowest near the low range of -80C. See the Networked Robotics TPL3 manual for a detailed accuracy chart. Temperatures from DS18B20Z integrated circuits report to a precision of .1 degrees Centigrade.

Value Alarms

Tempurity System value alarms are defined by the parameters of value, and time. Out-of-range conditions are not considered to have generated alarm conditions until the measured value has been continuously out-of-range for the time indicated by the Stage One time threshold parameter (for a yellow alarm) or for the Stage Two time threshold parameter (for a red alarm). These alarm threshold parameters can be defined for each individual monitored device. For example, if desired, an incubator temperature could be set to a 1-hour yellow Stage One alarm time, and a refrigerator to a 2-hour yellow Stage One alarm time threshold. These alarm time thresholds are defined via the Tempurity Server Configuration Utility.

Even a single in-range measurement will reset the alarm time-out-of-range counters in the software. When this occurs, the device must once again be continuously out-of-range for the Stage One time threshold period before an alarm will be generated. Note that a device that is cycling in and out of range may never trip a Tempurity temperature alarm despite being out-of-range for a considerable percentage of the day. This can occur when the monitored device is cycling such that the tip of the temperature cycle is just within normal range.

Alarm conditions are recognized based on their alarm time thresholds at the time that the data was acquired. It should not be assumed that at the time of a historic alarm that the current alarm time thresholds were in force. The applicable alarm criteria in force on the indicated date can be recovered from configuration history files if needed.

Communication Alarms

Monitored devices that don't respond to server requests for temperature or other kinds of data will eventually elicit a communications alarm. A communication alarm, sometimes referred to in this manual as a communication error, may have several causes. The alarm may be due to a planned interruption of network service by the network administrators or an unexpected failure of your organization's network components such as routers or switches.

Because the Tempurity Server must get a response from a monitored device within a defined time period, an intermittently-functioning network may sometimes cause an increased frequency in this type of error. A router that is intermittently functioning may also be the cause of frequent communication alarms.

Other causes of communication errors:

- Temperature or other probe failure or disconnection
- NTMS hardware failure or disconnection
- Freezer or other Instrument failure (direct connections only) or disconnection
- A loss of power or an unplugged power cable to a direct-connected instrument or NTMS

If a monitored device is in a Stage One alarm, and then moves to a communication error state, the Stage One alarm will wait to clear and will wait to move to a Stage Two alarm until at least one more temperature measurement is acquired for that monitored device. When the temperature value is received, if it is out-of-range, the "missing" data is assumed to have been continuously out-of-range. Communication errors resolve automatically when the conditions causing them, such as an unplugged temperature probe, are reversed.

The two types of alarms, communication and value, are linked. You cannot selectively enable alarm notifications for value alarms without also enabling them to the same alarm notification addresses for communication alarms. However communications alarms and temperature alarms can be configured to have different time thresholds. There are four time thresholds defined for Tempurity alarms, stage one and two communication alarm thresholds, and stage one and two temperature time thresholds. These are entered separately into fields of the Tempurity Server Configuration Utility for each monitored device.

The Tempurity Monitor Client



The Tempurity Monitor application is used to view temperatures and other data and to initiate the sends of alarm notification messages such as e-mail or text messages. The Monitor may run independently on any computer on the network, however it must have network access to at least one Tempurity Server. Tempurity Monitors are Read-only in the sense that they do not modify network-collected data. Essentially a Tempurity Monitor's job is to enhance the distribution of the server-collected data.

Distributed Alarm Notification

The Tempurity System is fundamentally different from other monitoring systems in that alarm notifications are configured and executed in the client software. Many customers will prefer to run only one Monitor – on the same computer as the Server, but the Monitor can run on many different computers simultaneously. An unlimited number of “watching” computers, Tempurity Monitors, can be constantly running in the background and monitoring a Tempurity Server for alarms in its population of monitored devices. Each monitor is under the control of its user who can define destination e-mail and text messages independently. There are only two requirements to this highly distributed architecture 1) the Monitor must have network access to the Server and 2) the Monitor must be on all the time.

Dedicated vs Shared Use Computers as Tempurity Monitors

The Tempurity Monitor software needs to run in the background of your computer at all times. It does not use a significant amount of either CPU or network resources, and is not affected by most other software. It maintains an active connection to the Tempurity Server over which data is streamed constantly but at low bandwidth by modern standards.

Running the Server and the Monitor on the Same Computer

The most common computer for a Tempurity Monitor will often be the Tempurity Server. This is the more traditional approach to temperature monitoring. Placing both Tempurity Monitor and Tempurity Server on the same machine allows centralized management of the monitoring process. Enter a server address of 'localhost' when the Tempurity Monitor prompts for a server address.

Downloading and Installing the Monitor

The Tempurity Monitor client software can be downloaded from the Networked Robotics web site at <http://www.networkedrobotics.com/download>.

Installation requires administrative access to the computer on which you are installing the software.

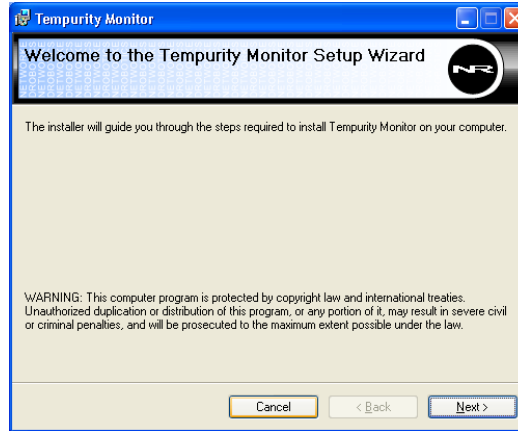


Figure 30: Installation of the Tempurity Monitor (some Windows Operating Systems)

During the download process you may either open directly (start the download) or save the download file to your disk. Click on the downloaded file and respond to the prompts. If you have previously installed the program you may need to uninstall it using “Windows→Start→Control Panel→ Add/remove Programs” before installing the new version.

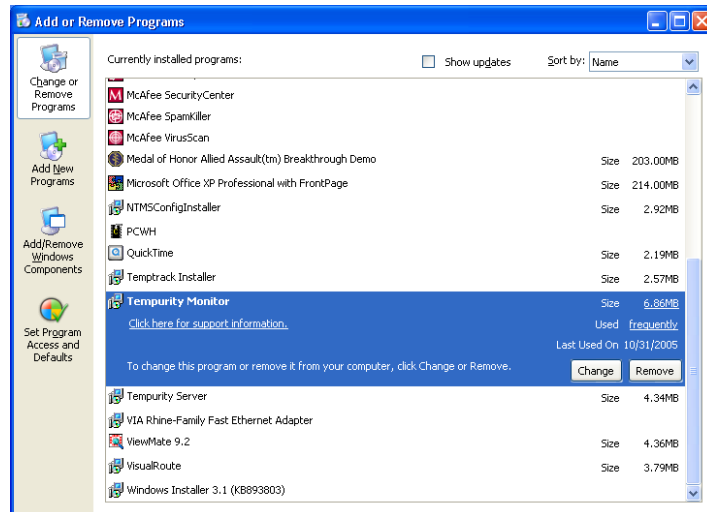


Figure 31: Uninstalling the Last Version of the Tempurity Monitor

The Monitor installer will ask a few questions including confirmation of legal agreement and other common installation options. The screen below appears with the following options:

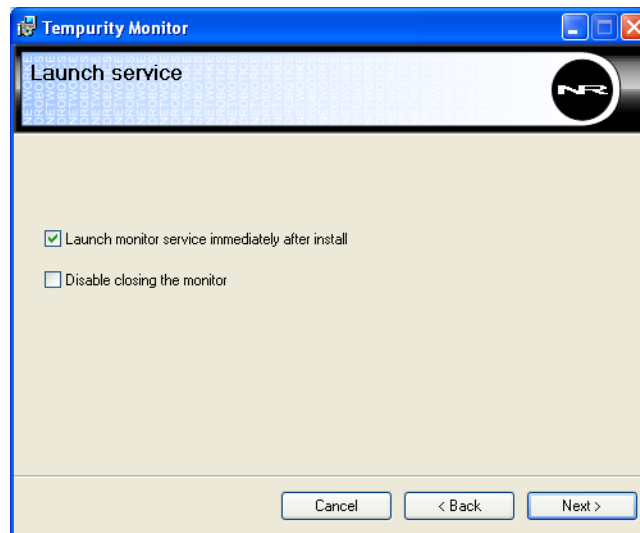


Figure 32: Service Options when Installing the Tempurity Monitor (Some Windows Operating Systems)

Launch Monitor service immediately after install

The default is to start the Tempurity Monitor immediately. If you uncheck this option, you will need to start the Tempurity Monitor manually using the “Administrative Tools->Services” option of the Control Panel. Leave this setting checked unless you are an advanced user.

Disable closing the Monitor

This option, if checked, prevents manually closing the Tempurity Monitor. The Tempurity Monitor, by default, allows users to close it with the standard “X” in the red box at the top right of a Windows screen. But if you do this, it stops the ability for this computer to send alarm notifications permanently. This is often an unintended action. To prevent this, check the box next to “Disable closing the Monitor” so that the program will always be running. Be aware that if the box is checked, the only way to stop the Monitor is through the “Administrative Tools->Services” option of the Control Panel as shown in Figure 16.

The Main Tempurity Monitor Installation Options are presented in a subsequent installation screen:

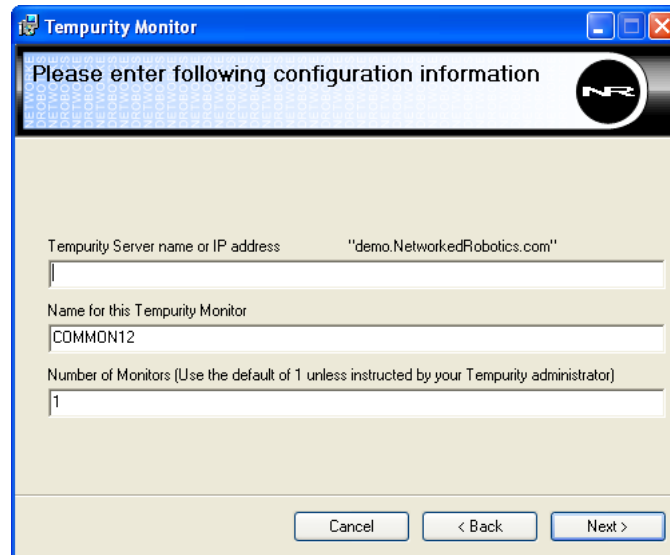


Figure 33: The Main Configuration Options when Installing the Tempurity Monitor (Some Windows Operating Systems)

Tempurity Server Name

The Tempurity Server name is the network address, either an IP address or host name of the computer running the Tempurity Server software. Examples of possible Tempurity Server names are given below.

Examples of Tempurity Server names:

| | |
|----------------------------|--|
| demo.networkedrobotics.com | The Networked Robotics computer at the network address indicated by this domain name must be defined in a DNS server A-record) |
| tempurity.mycompany.com | This same as above, but a computer in Mycompany. |
| 10.45.67.21 | The computer at this IP address. Should be a static IP address |
| "Localhost" | This computer that we are on now, same as below but textual rather than numeric |
| 127.0.0.1 | This computer that we are on now. This is called the loopback address |

Tempurity Monitor Name

There can be many Tempurity Monitors in an organization. When an alarm notification is sent, it is tagged with the name of the specific Tempurity Monitor that initiated it. The default is the Windows name for this computer.

If the Tempurity Server has been configured to use a Microsoft Exchange® mail server, you must use any 10-character Tempurity Monitor Name. This only applies to Tempurity Servers that are configured to send alarm notifications via Exchange mail servers.

Number of Tempurity Monitors

Consider setting this option to more than one monitor only in the case where you want this computer to watch several Tempurity Servers simultaneously. These servers can be at any organization, anywhere on the internet as long as you have network access. The Tempurity Server name needs to be entered manually within the Tempurity Monitor software's "Configuration Options" for additional Monitors.

Starting the Tempurity Monitor

The monitor automatically starts after the installation procedure is run. If you have entered a valid Tempurity Server name in the installation process you will see red or green icons for the monitored devices as defined in the server you selected and as shown in Figure 32 below. If the connection indicator status is red as in Figure 31 you may have entered an incorrect Tempurity Server name. To enter a valid name, choose "Configuration Options" from the menu bar. Enter the appropriate name and click OK. If you still are not able to connect there may be a firewall or other network connectivity issue preventing network access to that Tempurity Server. Check that the server software is running on the indicated computer.

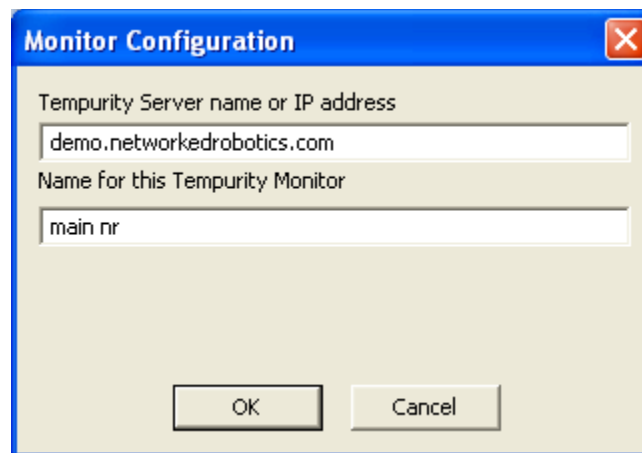


Figure 34: Monitor Configuration Screen

Stopping the Tempurity Monitor

Do not close or stop the Tempurity Monitor if you have activated any alarm notification groups. The monitor must be running in order to initiate alarm notifications. If you have accidentally closed the monitor you must restart it with the procedures shown in Figure 16, or by reinstalling the Tempurity Monitor software. Consider reinstalling using the "Disable Closing the Monitor" installation option. If this option is selected the program can not be manually closed and thus can not be manually stopped.

Connection Status to the Tempurity Server

If the Tempurity Server name or IP address, shown next to the Monitor's local time, is shown in white characters, the Monitor has made a proper connection to a Tempurity Server. If the name is shown in red characters, a connection has not been established. It sometimes takes as long as a minute for a Tempurity Monitor to connect to a Tempurity Server.

If this is the first time that you are connecting this Monitor to a Tempurity Server, and the server name is shown in red, it is likely that no monitored device icons will be displayed. The screen will be blank except for the heading. Check that you have entered an appropriate server name and that the Tempurity Server is running at the network address indicated. Make sure that the firewall on the server is open on port 3010.

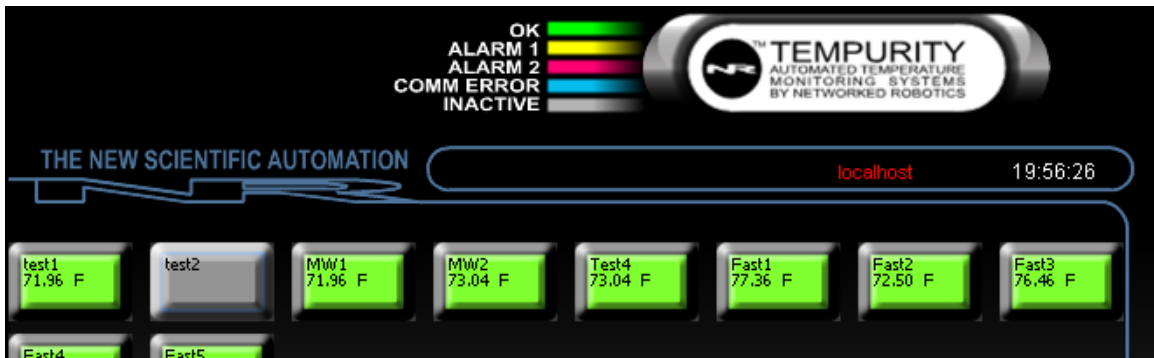


Figure 35: Connection Status to Tempurity Server

If you see a Tempurity Monitor with an unexpectedly red server name, the Tempurity Monitor is unable to connect to the Tempurity Server. No alarm notifications are possible from this Monitor and steps must be taken to identify and correct the problem. Check your network status and the status of the Tempurity Server. When the adverse conditions are reversed, no manual intervention is needed, the Monitor will regain its ability to communicate with the server, and the server indicator will once again be displayed in white characters.

Main Monitor Screen




The main monitor screen shows an at-a-glance view of the status of each of the monitored devices connected to the Tempurity Server. The status is indicated by a) color and b) text descriptions.



Figure 36: The Tempurity Monitor Main Screen

The table below shows the progression of the visual display of the icon over time as monitored devices report out-of-range values (Value Alarms), or do not report values as expected (Communication Alarms). The lower the entry in the table, the longer the monitored device has been out-of-expected performance.

Value Alarms

| Condition | Icon | Value Displayed? | Alarm Notifications |
|------------------------|---|------------------|---------------------|
| • Normal |  | No | No |
| • Out-of Range |  | Yes | No |
| • Out-of-Range Stage 1 |  | Yes | Yes |
| • Out-of-Range Stage 2 |  | Yes | Yes |

Communication Alarms





| Condition | Icon | Alarm Notifications |
|------------------|---|---------------------|
| • Normal |  | No |
| • Not Collecting |  | No |
| • Stage 1 Comm |  | Yes |
| • Stage 2 Comm |  | Yes |

Figure 37: Alarm Visualization in the Tempurity Monitor

Alarm Status Icons

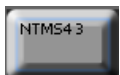
The alarm status on the main Monitor screen is represented by the following colored icons:



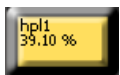
Green – The monitored device is operating within the proper range. A value on this icon indicates an out-of-range condition, but it has not persisted for long enough to generate an alarm condition of yellow or red.



Blue – Data cannot be obtained. The device may or may not be within the allowable data range. Anytime data has ceased to be collected as expected, the icon will be blue.



Gray – No device is present. This occurs when the monitored device ID was configured for data collection but has not collected at least one value since the Tempurity Server was last started. If even a single data value was collected, and then no further data came in, the icon would be blue, not gray.



Yellow – A Stage One alarm exists for this monitored device. The value of the last measurement will be shown.



Red – A Stage Two alarm exists for this device. The value of the last measurement is shown.

“Comm” indicates that a communication error exists for a monitored device. The Tempurity Server has collected at least one measurement, but is not currently collecting. Note that devices indicated as gray on the monitor may also be suffering from an inability to collect temperatures or other kinds of data. When the Tempurity Server starts, it must be able to make a network connection to the indicated network address. If it cannot collect values, the monitor icon for that device remains gray. When the connectivity problem is corrected, the device will change from gray to green status. If a subsequent communication error occurs the monitor icon will show as a blue communication error rather than a gray inactive indication.

Alarm Window

The alarm window of the main monitor screen shows a list of the Communication, Stage One, and Stage Two alarms that have occurred within the last year starting January 1 of the current year. It also shows the time, if any, that these alarms cleared. Usually there will be a clear event for every alarming monitored device however there are some possible exceptions such as when a reconfiguring of high and low value thresholds occurs.

The alarm window display can be toggled on or off using the option on the ‘View’ menu as shown below.

The data in this file is held in an alarm file. See Appendix C for details.

The alarm window can be cleared using the “View->Display Alarms” option from the Monitor menu bar.

Monitored Device Information Window

Detailed information about the current status of the monitored device may be obtained by clicking on the representative icon for any monitored device. The screen shows the time of the next reading, a real-time graph of the temperatures in the previous two hours, the time of the last reading, the last temperature recorded and the alarm status. The IP address and the port address of the monitored device are also displayed.

If this window is left open, this graph will be updated in real-time every minute.

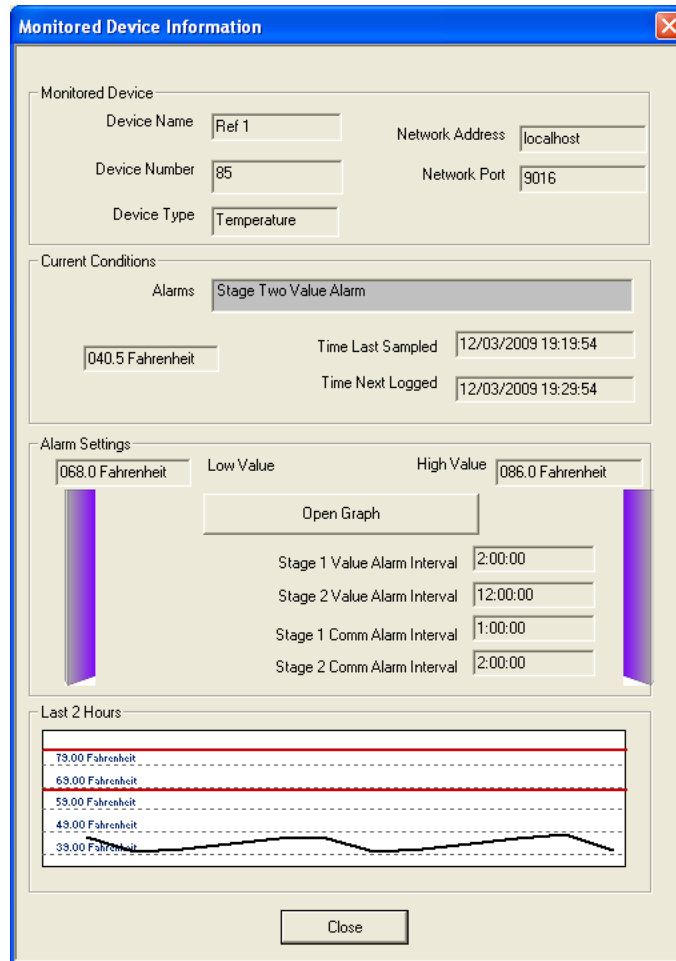


Figure 38: Monitored Device Information

The window shows the parameters that were set for this monitored device in the Tempurity Server Configuration Utility. It also shows the last-collected measurement and the data acquisition schedule.

Graphs

Graphs of this monitored device's data can be generated by clicking on the "Open Graph" button. As Figure 35 shows, graphs can also be obtained from the menu bar of the main monitor screen.

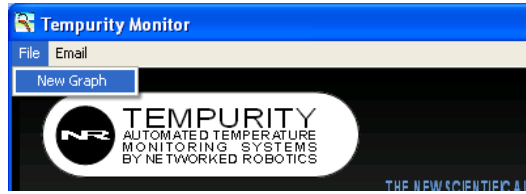


Figure 39: Method of Graphing from the Monitor

Figure 36 below shows a graph of a temperature kind of monitored device type.

The graph will autoscale by default. The autoscale may be overridden by entering maximum and minimum Y axis values. Any time interval can be selected by entering a time period manually or by scrolling with the arrow buttons. Zoom in or out to see data at the desired granularity.

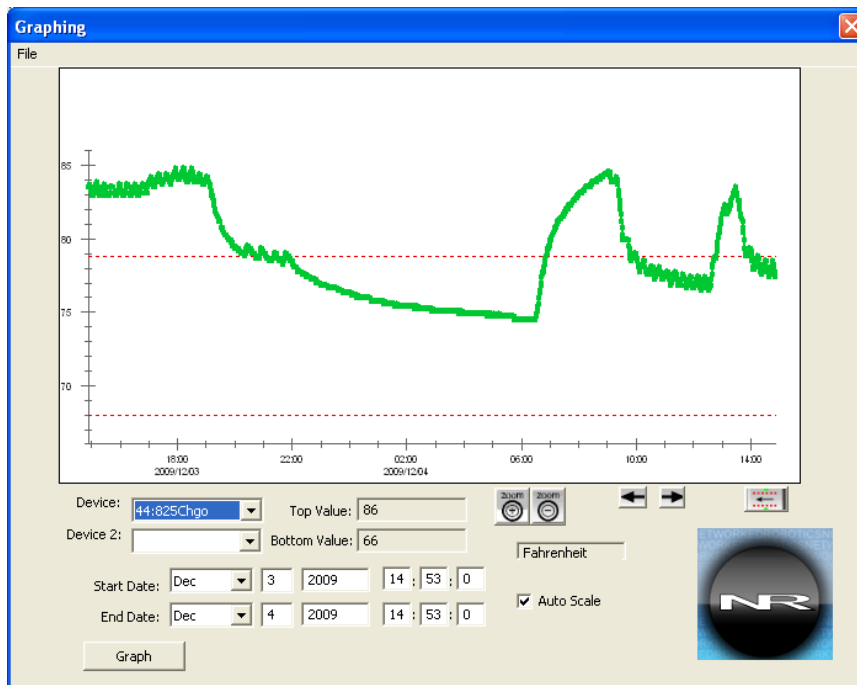







Figure 40: An Example Graph from a Monitored Device of Type Temperature

| Setting | Definition |
|----------|--|
| Device | The graph of the selected monitored device |
| Device 2 | Plots a second monitored device |

| | |
|---|---|
| Top Value | The temperature or other data high value limit |
| Bottom Value | The temperature or other data low value limit |
| Auto Scale | The Top Value and Bottom Value will be automatically set based on the measurements in the selected time range |
|  | Zooms into a shorter time range |
|  | Zooms out to a greater time range |
|  | Moves forward the current time interval |
|  | Moves backwards the current time interval |
|  | Zooms to the last out-of-range value recorded |
| Graph | Draws a graph with the given settings |

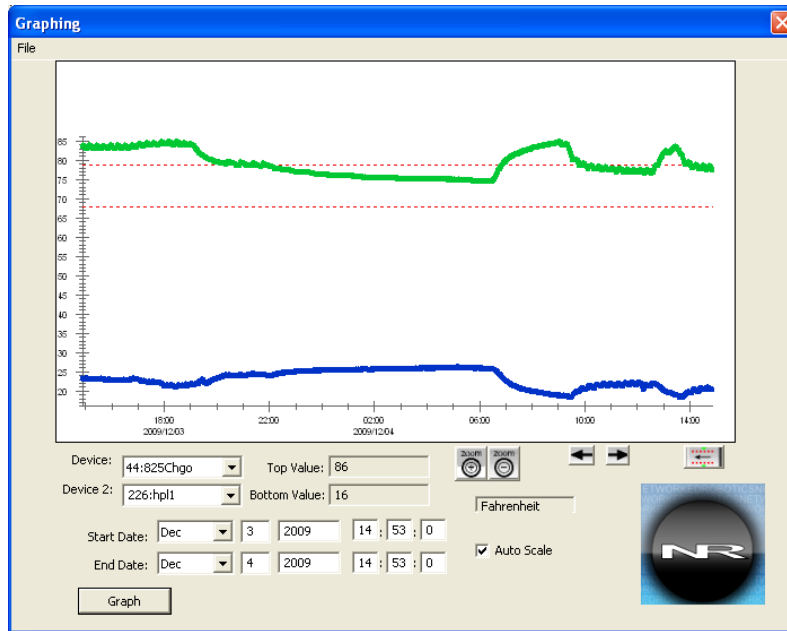


Figure 41: An Example Graph showing a Simultaneous Plot of Relative Humidity and Temperature from Two Monitored Devices

The 'File->View Data' menu option allows you to view the numeric values in the selected date and time range of the graph. This numeric data can be copied and pasted into other applications e.g. Microsoft Excel.

| Local Time | Humidity (%RH) |
|---------------------|----------------|
| 2009/11/19 17:23:40 | 41.90 |
| 2009/11/19 17:24:40 | 41.90 |
| 2009/11/19 17:25:40 | 41.90 |
| 2009/11/19 17:26:41 | 41.90 |
| 2009/11/19 17:27:42 | 41.90 |
| 2009/11/19 17:28:42 | 41.90 |
| 2009/11/19 17:29:43 | 41.90 |
| 2009/11/19 17:30:44 | 41.90 |
| 2009/11/19 17:31:44 | 42.00 |
| 2009/11/19 17:32:44 | 42.00 |
| 2009/11/19 17:33:45 | 42.00 |
| 2009/11/19 17:34:46 | 42.00 |
| 2009/11/19 17:35:47 | 42.00 |
| 2009/11/19 17:36:48 | 42.00 |
| 2009/11/19 17:37:50 | 42.00 |
| 2009/11/19 17:38:51 | 42.00 |
| 2009/11/19 17:39:51 | 42.00 |
| 2009/11/19 17:40:52 | 42.10 |
| 2009/11/19 17:41:53 | 42.00 |
| 2009/11/19 17:42:54 | 42.10 |
| 2009/11/19 17:43:55 | 42.10 |
| 2009/11/19 17:44:55 | 42.10 |
| 2009/11/19 17:45:57 | 42.10 |
| 2009/11/19 17:46:58 | 42.10 |
| 2009/11/19 17:47:58 | 42.10 |
| 2009/11/19 17:48:58 | 42.10 |
| 2009/11/19 17:49:58 | 42.10 |
| 2009/11/19 17:50:59 | 42.10 |
| 2009/11/19 17:51:59 | 42.10 |
| 2009/11/19 17:53:00 | 42.10 |
| 2009/11/19 17:54:01 | 42.10 |

Figure 42: Tempurity System Numeric Data

Exporting Data to Other Applications

One way to export data is to click on the “Copy” button as shown in Figure 37, which moves all the measurements in the date range that you selected for the graph to the copy buffer.

Then Paste the data into the other application. When pasting into Microsoft Excel® you may need to use the “Text to Columns” feature to split the time and the measured value into separate columns.

Another way to export data is to create a comma-separated value (.CSV) file. Choose the “File->Export Data” option from the graph. The .CSV file holds 3 values for each measurement: universal time, local time, and the measurement and its units. Some users will want to delete the universal time column, because its unique format is hard to read without special converting software.

Large time ranges will be difficult to export because of the large number of data points. At the default measurement interval, Tempurity stores a little more than 10,000 data points per week for each monitored device. You may want to consider exporting small data ranges and reducing the quantity of data via another application.

Statistics

Simple statistics are available using the “File->Statistics” option from the graph to describe the data in the time range specified by the current graph. The below shows the statistics window operating on a range of data that includes one out-of-range event as seen in the data graph below left.

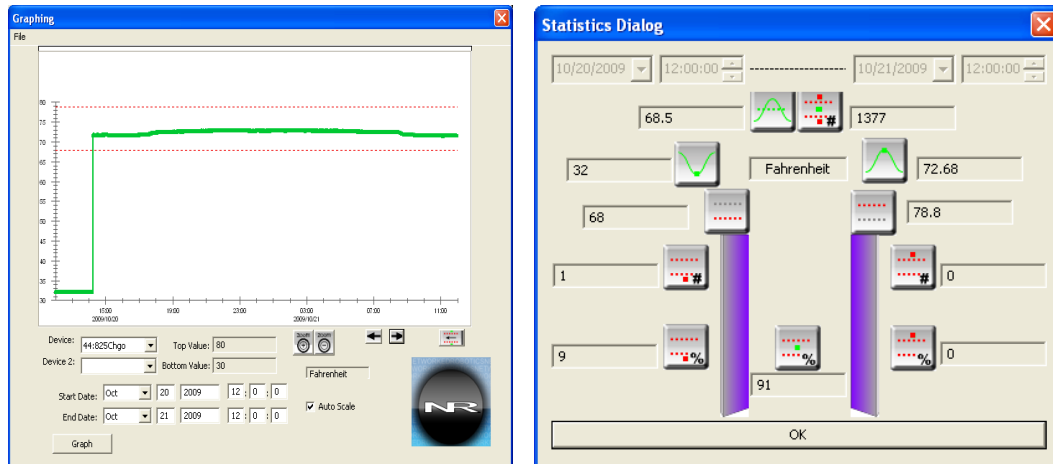


Figure 43: Statistics Windows and Statistics for an Example Data Range

Each statistical calculation is indicated by an icon as described below:

Allowed Data Value Range



Current High Value Limit



Current Low Value Limit

Max, Min, and Mean



The maximum recorded data value in this time range



The minimum recorded data value in this time range



The mean recorded data value in this time range. The number of data points in this time range is also shown.

Number of Events High or Low



The number of events where data was higher than allowed



The number of events where data was lower than allowed

Percentage of Points In or Out-of-Range



The percentage of recorded data points that were in-range



The percentage of recorded data points that were higher than the high value limit



The percentage of recorded data points that were lower than allowed

An “event” is defined as an instance where the data was out-of-range to any level and then returned to normal. The difference between an alarm and an “event” is that alarms are bound by alarm time criteria. Events are not bound by these criteria. Any out-of-range case will be an event no matter how long it lasts. Like the other statistics, events are only counted for the time period selected by the graph's time range.

Alarm Notifications

The Tempurity System is capable of sending messages through the internet when alarm conditions are found to have arisen in any of the monitored devices. In Tempurity System terminology, these messages are called “alarm notifications”. There are different kinds of alarm notifications such as E-mail, Text message, Robotic Voice, Pager, etc.

An Alarm Notification Group is a list of people and their contact information (phone numbers, e-mail, etc) that will be contacted when there's a problem with any of a specified list of monitored devices.

The Tempurity Monitor continuously talks to the Tempurity Server to see whether any alarms have been found. If so, and if an Alarm Notification Group has been defined that references the errant monitored device, alarm notifications are sent. The Tempurity Server sends these alarm notifications but the send is triggered by the Tempurity Monitor.

Defining an Alarm Notification Group

To define an alarm notification group, choose “E-mail and Text Messaging” from the menu bar. Create an alarm notification group name. You may want to define groups by area of responsibility, “Tox”, “QA”, or “Gene Tox” for example. Individual freezers can be assigned to each alarm group

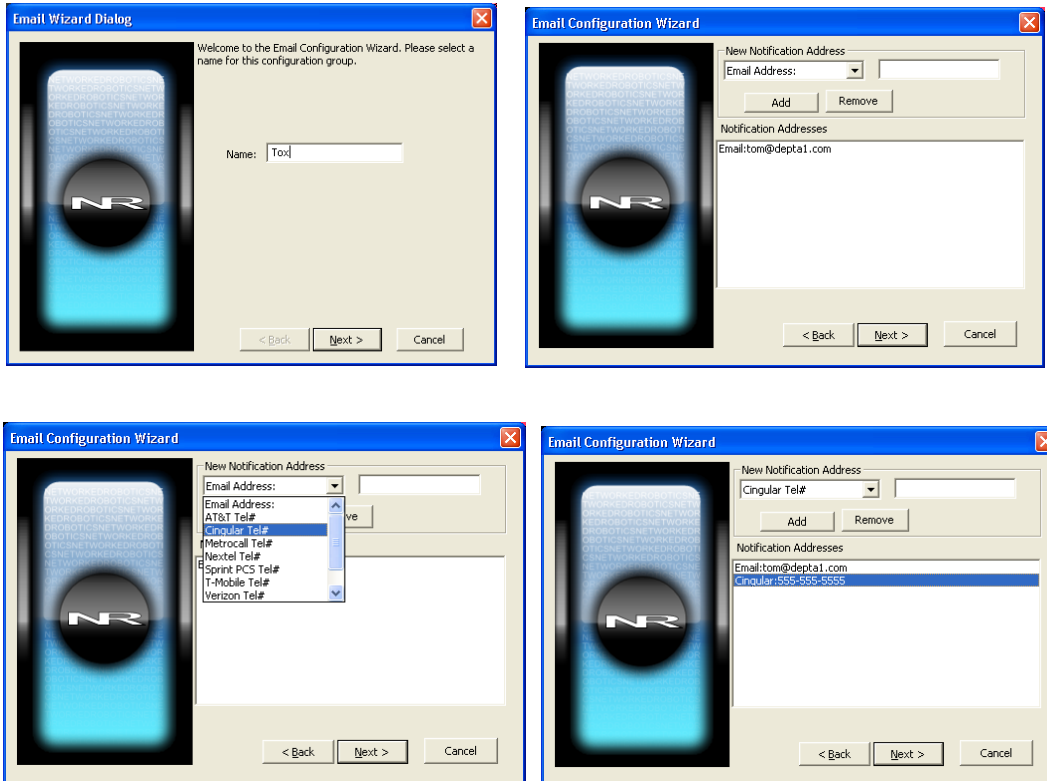


Figure 44: Creating an Alarm Notification Group

Choosing Alarm Notification Types and Entering Alarm Notification Addresses

The above shows the process of defining alarm notifications. First an alarm group is defined. Then added to it are alarm notification addresses, a list of people and their e-mail addresses or phone numbers. Then the user selects the monitored devices, the freezers, refrigerators, etc. that this group of people cares about and at what stage (Stage 1 or Stage2 or both) they want to be notified.



Figure 45: Selecting the Monitored Devices of Interest for this Group

The options are to select or clear all Stage One or Stage Two alarms, select or clear all alarms, or select individual monitored devices with individual alarm stages.

Note that communication alarms cannot be selected independently of temperature and other value alarms. If a notification is selected when a monitored device is in temperature alarm state, notification will also be sent when a communication alarm exists for that same device.

The time thresholds for these two events are different however, as specified in the Tempurity Server Configuration utility. For example, if the Stage One value threshold is 1 hour, and the stage 1 communication threshold is 4 hours, and if that device stops responding to the Tempurity Server at 45 minutes after out-of-range values began, a notification will be sent 4 hours and 10 minutes after temperatures stopped being received. The communication alarm supersedes the temperature alarm in this case and an alarm notification was not sent at the 1 hour mark as would be the case if out-of-range values had continued to arrive.

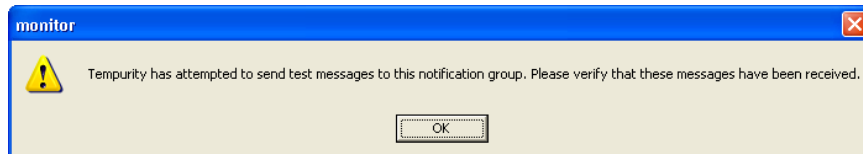


Figure 46: Test Messages are Sent to the Addresses in your Alarm Notification Group

Test Alarm Notifications

Test alarm notification messages are always sent after you have configured the alarm notification group. The program will not be able to recognize whether the entered e-mail or other notification address that you entered is valid. Therefore always check that the alarm notification test e-mail or text message was received as expected.

You can test existing alarm notification groups by simply highlighting a group in the first panel of the alarm notification wizard and clicking on the "Test" button.

E-mail addresses and phone numbers change. Networked Robotics recommends that you test your alarm notification groups on a monthly basis.

Alarm Notification Groups are Mapped to the Tempurify Server for which they were Created

If you change the network name or address of the Tempurify Server that is being watched by this Tempurify Monitor (see options in Figure 30) then your alarm notification groups will seem to disappear. That's because alarm notification groups "belong" to the Tempurify Servers under which they were created. If you change the watched Tempurify Server back to the original, you will once again see the alarm notification groups that you created for that server.

The current version of Tempurify does not recognize equivalence in network names. So "localhost" and "127.0.0.1" will appear to be two different servers with two different sets of alarm notification groups even though they are equivalent network names. The same would apply to a domain name like "tempurify1.mycompany.com" and "10.34.56.29". You should use a consistent name for your Tempurify Server.

Networked Robotics recommends the use of domain names rather than IP addresses to reference the network address of Tempurify Servers. One reason for this is that if the IP address of the Tempurify Server changes – alarm notification groups will need to be reentered or reloaded as below if you use and IP address, but this would not be required if you were using a domain name.

Alarm Notification History

You can use the "Sent" folder of the e-mail account you configured as the sending account in your Tempurify Server (see Figure 23) in order to view a record of the e-mail and text message alarm notification types. No such record is available for voice alarm notifications.

Storage and Transfer of Alarm Notification Groups

The Tempurify Monitor acts as an extension to your Windows operating system. It stores all the information for alarm notification groups in the Windows Registry by the watched Tempurify Server name, as entered in the Monitor configuration (See Figure 30).

If you have a detailed list of alarm notification groups, you can transfer them from one Tempurify Monitor to another by exporting and importing registry keys. Use "Start->Run->Regedit" then navigate to *Hkey_Users->Tempurify Monitor->Monitor*. If you do a registry Export of this branch of a tree, and a subsequent import of the registry file into another computer on which the Monitor is running, the Monitor will inherit the alarm notification groups specified. The figure below shows the registry organization. Since the Monitor was installed many Tempurify Server names were defined, each with their own alarm notification groups. Server names shown in the figure range from "1" through "192.168.1.106" to "D".

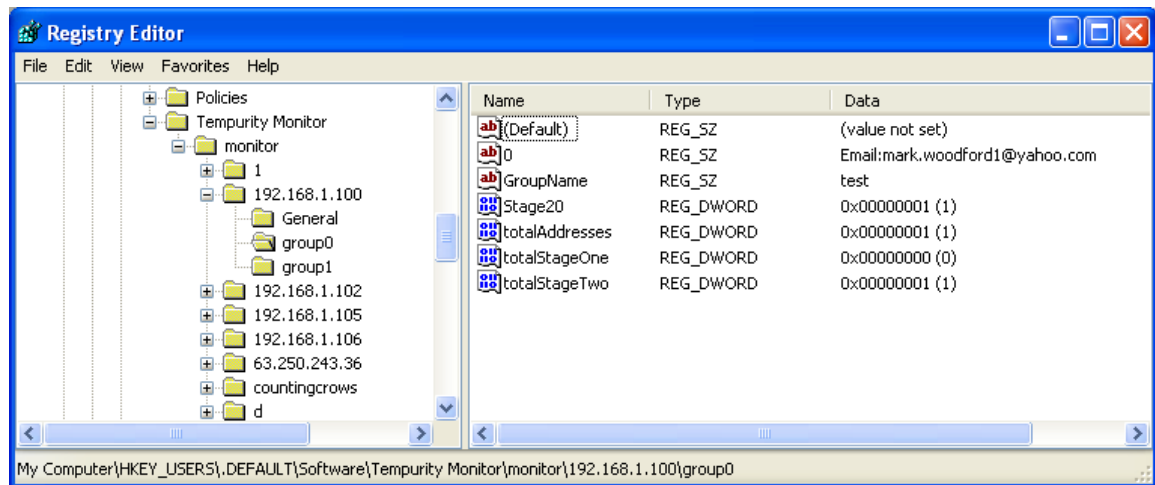


Figure 47: Storage of Tempurity Monitor Alarm Notification Groups in the Registry

Monitor Restart

When the Tempurity Monitor is restarted, for example if the PC reboots or if the Monitor is manually restarted using “Control Panel->Administrative Tools->Services” alarm notifications will be sent for any monitored devices currently in an alarm state.

This means that there are cases where you may receive more than one alarm notification for any alarm stage.

E-mail to Text Gateways

The Tempurity System uses E-mail as the means of sending a text message to a cell phone.

The software does this by sending an e-mail to the E-mail-to-Text gateway provided by the cell phone provider. When you choose a particular cell phone service provider or pager, the Tempurity System formats the e-mail into the form required by the selected provider's text message gateway.

Because implementation of e-mail to text gateways is controlled by the major cell phone service providers, the format of e-mail message for a particular gateway changes from time-to-time.

If the format of a gateway no longer works for a particular service provider, it could be that the format has changed. Use the internet or call the cell phone company to find the e-mail format for provider's e-mail-to-text gateway. You can send text alarm notifications to those recipients using an Alarm Notification Type of “E-mail” by providing an E-mail address that complies with the e-mail address for the gateway.

Several companies have more than one gateway format, often as the result of mergers or acquisitions in their industry. Some of the most common gateways are listed below. We recommend that you try the lowest number first for any particular vendor. For example T-Mobile 2 is the lowest of the possible T-Mobiles.

At the time of this writing here are some of the gateways for cell phone providers:

If the user has a text-message or SMS-enabled phone, you can send them a message via Internet e-mail. Here is a list of known e-mail addresses: (replace *number* with the recipient's 10 digit wireless phone number. Some of these may differ from the format of alarm notification types in Tempurity.

ATT Wireless *number*@txt.att.net

Cingular *number*@cingular.com (must be logged in)

Nextel *number*@messaging.nextel.com

Sprint (PCS) *number*@messaging.sprintpcs.com

T-Mobile *number*@tmomail.net

US Cellular *number*@email.uscc.net

Many providers now allow users to set up their own e-mail alias for text messaging. Please check with your provider for details.

Check with your cell phone provider for any updates to these addresses.

These e-mail addresses must be accessible from the SMTP Mail server that you selected for use with Tempurity in the Tempurity Server Configuration Utility. Some corporate mail servers are set to block some kinds of mail. Check with your mail administrator if test e-mail or text messages are not received.

Time Delay in Receiving Alarm Notifications

The time that it takes for an alarm notification to reach its destination is variable. It depends on the characteristics of corporate e-mail systems and other mail servers, on the speed of the e-mail to text gateways of cell phone providers, on whether a cell phone is out-of-tower-range and other factors that are sometimes beyond the control of either customer organizations or Networked Robotics. Individual cell phone providers may have response times that are highly variable especially during periods of internal maintenance. If you suspect that an alarm notification is reaching you late, contact the e-mail or text messaging provider that you use. Alarm notifications are usually tagged with the time that the provider sent the message, not the time that it was sent to the provider by Tempurity.

Monitoring Multiple Tempurity Servers from a Single Computer

A single computer running several instances of the Tempurity Monitor can watch the status of as many as 30 different Tempurity Servers, each with their own alarm notification groups, in parallel. These servers can be in different companies, states, or countries.

To monitor multiple Tempurty Servers from a single computer, at install time just set the number of Tempurty Monitors to the number of Servers you wish to watch. Enter the unique Tempurty Server address into each instance of the Tempurty Monitor. Alarm groups and their corresponding alarm notification addresses are independent in each instance of the Monitor.



Figure 48: Running Multiple Instances of the Tempurty Monitor

When you want to restart instances of the Monitor through Windows, you can do it through Control Panel->Administrative Tools -> Services". Each Monitor is labeled with a unique number for example Monitor0, Monitor1, Monitor2, etc.

Regional Versions of the Tempurty Monitor

On Windows XP Only Currently.

The Tempurty Monitor is designed to run in the same written language that your Windows computer uses. In Windows this setting is found in the "Regional and Language-> Regional Options->Standards and Formats" option of the Windows Control Panel.

Currently supported languages include French, German, Italian, Portuguese, Dutch, Chinese, and Japanese. Other languages will run in English.

Although the Tempurty Monitor program automatically runs in the language of your computer, the installation procedure always runs in the specific language version that you select from the Networked Robotics download page. If you download the French version of the Tempurty Monitor, but your Windows options have set your PC as Spanish, the installation of the Monitor will proceed in French but the Tempurty Monitor will run in Spanish.

Certain features may not be available in foreign language versions, for example the synthesized speech in voice alarm notifications is optimized for English and may be difficult to understand in regional versions. Certain items are not translated, for example Tempurity Server network names and IP addresses are constant in all languages at present.

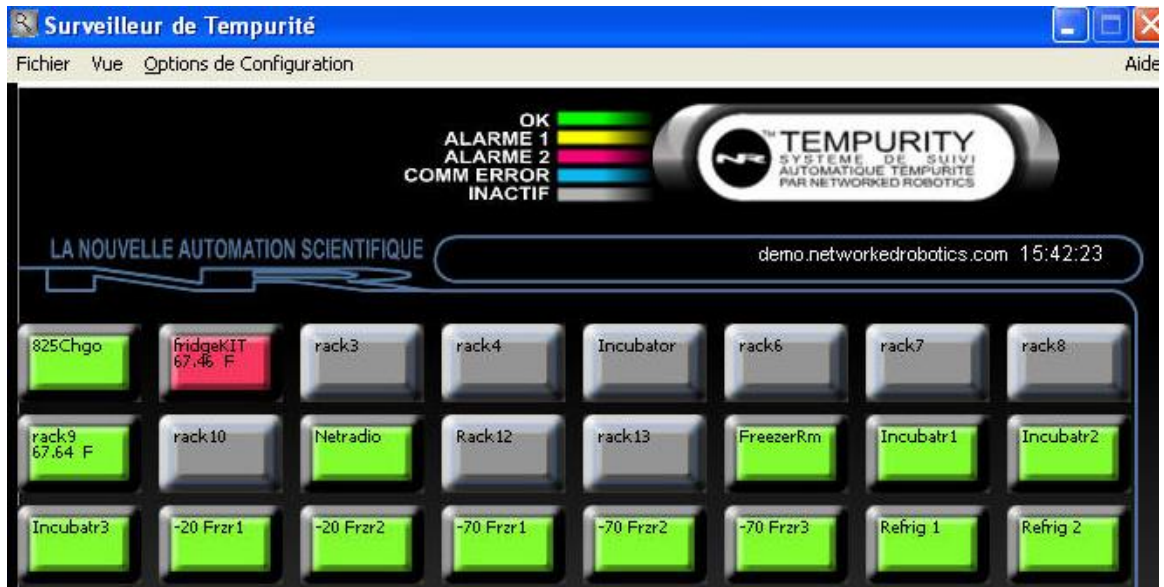


Figure 49: French Language Version of the Tempurity Monitor

Hardware Upgrades – Changing the Function of your NTMS Hardware



You can change the functionality of your Networked Robotics hardware by changing the firmware resident in the unit. The upgrade is easily made from any networked PC.

When to Upgrade your Firmware

NTMS Firmware should be changed when it is necessary to connect to new kinds of instruments and sensors that are not supported by the version of the hardware you purchased. Some firmware enhancements are quality-related; they provide fixes for known problems.

Scans returned by the NTMS Configuration Wizard show the firmware version resident in each NTMS. You can use this utility as the basis for determining whether any units require firmware upgrades. As a general rule, Networked Robotics does not recommend updating units with no specific need for enhanced functionality.

Older (2006 and older) Networked Robotics NTMS units do not support firmware upgrades.

Any changes to NTMS firmware that support new instrument interfaces or sensor types that you plan to connect to usually also require the downloading of a new version of the NTMS Configuration Wizard



software as described in detail above. The new NTMS Configuration Wizard will support the ability to configure your NTMS for data collection from the new device type.

Downloading the Hardware Upgrade Wizard

Download the Hardware Upgrade Wizard from the “Hardware Upgrades” subsection of the download section of the Networked Robotics web site. The downloaded file comes as a zipped package of several files including the Upgrade Wizard, the Networked Robotics firmware file with a .NRF extension, and release notes. You'll need to use a tool like WinZip® to unzip and use the files. Once unzipped, click on

the NTMS Upgrade Wizard program  as indicated by the pliers icon.

Running the Hardware Upgrade Wizard

The upgrade can be done from any PC on the same local area network as the NTMS that you wish to change. The Firmware Upgrade Wizard runs in a similar manner to the NTMS Configuration Wizard. It scans your network for any Networked Robotics hardware. From the returned list you will double-click

on the unit you wish to upgrade, choose a .NRF (Networked Robotics Firmware) file to load, and then wait for the process to finish. It should take about 3 minutes depending on the speed of your network.



Figure 50: The Introductory Panel of the NTMS Upgrade Wizard

If a network failure or power failure occurs during the firmware upgrade process you need to power cycle the NTMS and start over.

If the NTMS does not perform as expected with the new version, you can run the NTMS.

Time Zones and Time Accuracy

The Tempurify System is designed to operate in an environment in which temperatures and other kinds of data can originate in many world time zones. Any computer, anywhere, can view the data collected by Tempurify Servers. The system has features that facilitate the data interpretation from data sources (Tempurify Servers) in multiple geographical regions.

The Tempurify Server stores each data collection time in universal time format. When a Tempurify Monitor Client displays alarm times, graphed data or numeric data, these measurements are shown in the appropriate local time based on the Windows Operating System setting of the Tempurify Monitor computer's time zone.

An example of the global time-related features of Tempurify follows:

A temperature measurement was collected from a Tempurify Server based in New York at 3:00 pm US EST. The temperature showed a spike of 0°C over a baseline of -20°C. A stage 1 alarm was issued at that time recognizing the out-of-range condition. Assume that each Windows Monitor client has their correct time zone specified in the Windows Date and Time option of the Windows control panel, if a Tempurify Monitor client reviews that temperature spike from Denver at Mountain Standard Time, it will appear on graphs and in the data view option as having occurred at 1:00 pm. If a Monitor client in London connects to that same Tempurify Server in New York and views the data, that same 0°C temperature spike will be plotted as having occurred at 8:00 PM.

The Windows time zone defined on the server computer does not affect the time displayed by any client. If the Tempurify Server computer time zone is changed there will be no consequences to the data collection times viewed by any Monitor Client in any time zone. However, if you change the Windows time of day setting on that same server, this will be reflected in the observed record for all connected Monitors in all time zones. For example if you change the server's time of day from 10:12 to 10:14, this two-minute change will be reflected in the subsequent data observed by all Monitors.

The Main Monitor Screen's time display, shown in white numbers, is not related or dependent on time zone. A visual tool only, it shows the *local time of the client computer* in white numbers. This is the Tempurify Monitor computer's Windows system time and is unrelated to the Tempurify Server's time or time zone. It is not attached to any collected data or any alarm notifications issued by Tempurify.

For all Tempurify Server computers we recommend that you connect to a time synchronization server, a computer on the network who's job is to issue the correct time to other computers. You can automatically synchronize your Tempurify Server by clicking on the Windows time, usually at the bottom right of the Start bar. Choose "internet time" and the "automatically synchronize" option (See figures below). This will set your Tempurify Server computer's time with the network time server and thus will always be accurate.

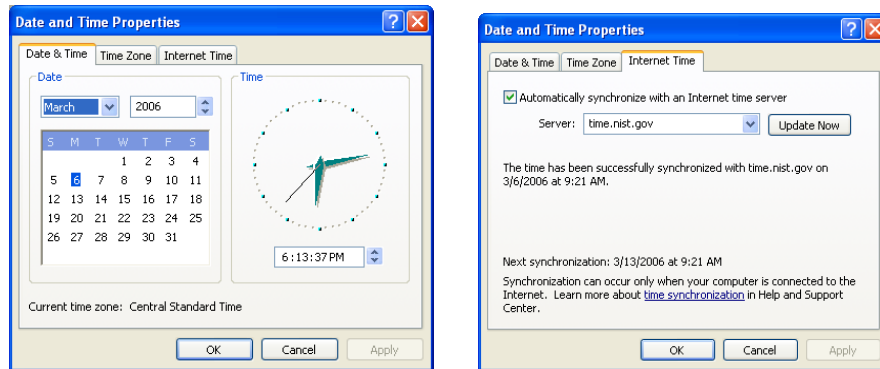


Figure 56: Setting a Network Time Server

System Operations

Redundancy

The Tempurity System allows greater reliability through the use of redundant processes. You can download and configure multiple Tempurity Servers that collect temperatures from exactly the same population of monitored devices simultaneously.

The figure below shows one strategy for redundancy called “near-far”. Two Tempurity Servers and two Tempurity Monitors have been implemented. The Tempurity Monitor at site A, shown in blue, watches its local Tempurity Server also shown in blue. The site B Tempurity Server, shown in green, collects temperatures from the monitored devices at site A; the site B Tempurity Monitor also watches its local Tempurity Server. At least one location will survive any negative event that causes large-scale power or network failure. In this way communication alarm notifications are guaranteed to be sent.

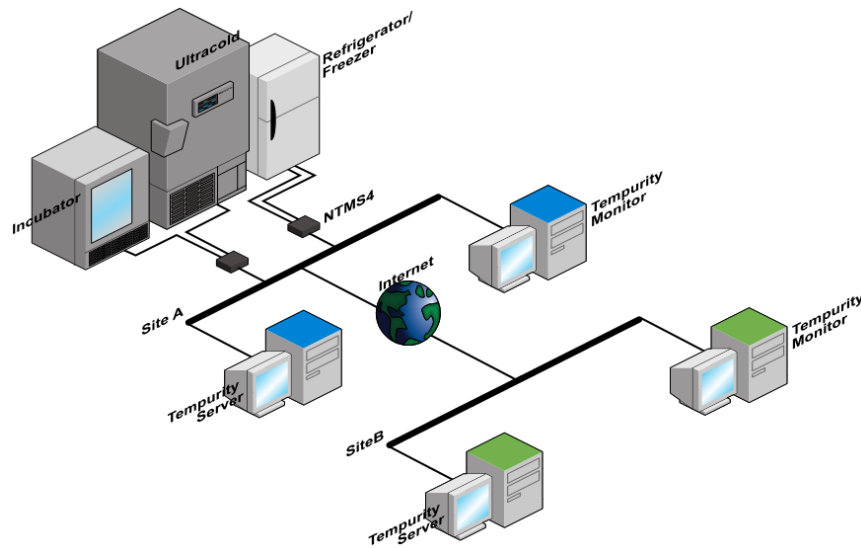


Figure 57: A Strategy for Utilizing Redundant Tempurity Components

Large Scale Power Outages

You need to avoid a bit of a Catch22 in Tempurity System operations. On the one hand if there's a power failure then the outside world needs to know about it because freezers will be affected, on the other hand the system that tells the outside world that there's a problem, Tempurity, needs power. So how do we resolve this discrepancy?

The situation in the case of a large-scale power outage can be complicated. In general several monitored devices will not be able to transmit temperature and other data and thus will enter a communication alarm state. In this case alarm notifications will still be sent to the outside world as long as a minimum infrastructure is still powered up.

To make sure that this infrastructure is available you will either need to use redundant servers from another , unaffected, site as described above, or use uninterruptible power supplies (UPS) to backup your Tempurity Server computer and the path to the outside world. By “path” we mean any routers or switches or other network equipment that the Tempurity Server needs in order to get to the outside world. If you are using a mail server the “path” means the network routers and switches to your internal mail server, the mail server itself, and the routers and switches needed to get from the mail server to the outside world. Note that if you use an external mail server like Gmail for alarm notifications then it eliminates the need to power-protect a company-internal mail server.

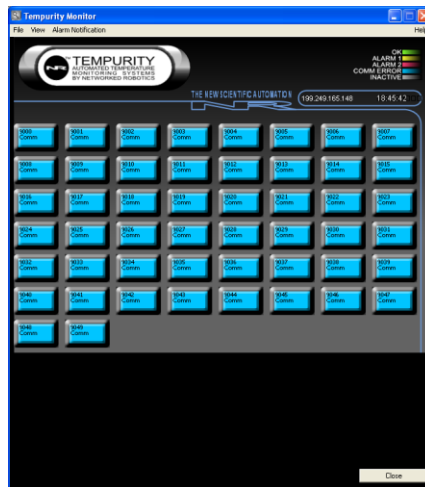


Figure 58: Tempurity Monitor Display under Conditions of Large-Scale Communication Failure

Safety

The contents of scientific refrigerators and freezers are often hazardous. Recognize safety concerns. Use appropriate protective equipment before opening any scientific device containing scientific samples. Be aware of any procedures that need to be followed in the event of a hazardous material spill. The contents of the refrigerator or freezer should always be labeled and sealed to prevent accidents. Protective gloves should be worn when working inside scientific refrigerators and freezers.

Periodic Testing

Test alarm notification groups periodically. Tempurity System alarm notifications are based on the operating capability of large telecommunications companies. These companies are often merging and sometimes change their capabilities and requirements.

Some regulated customers require a calibration or recalibration procedure for the scientific instruments and sensors that provide data to Tempurity.

Regulatory Use

The Tempurity System was designed for use in FDA regulated environments, specifically for use under the United States Food and Drug Administration's Good Laboratory Practices and Good Manufacturing Practices standards.

Compliance with these standards often requires the use of corporate operating procedures for reacting to potential sample quality issues caused by the failure of refrigerators, freezers, or other equipment.

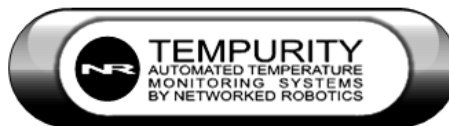
Procedures for reacting to Tempurity events will be uniquely defined by your company scientists, management, and quality assurance specialists. Some clients might define the Stage One alarm as an event designed to enable an event to be addressed by lab or facilities personnel and reserve the Stage Two alarm as an event that needs to be communicated to quality personnel. Some organizations might consider communication alarms to be equally important as temperature and other value alarms from a regulatory and quality point of view while others may wish to disregard communications alarms completely.

Suggestions for Operation

Based on our experience, the most reliable freezer monitoring depends on several overlapping methods – each with assigned human responsibility. The first line of defense is often the freezer's internal audible alarm, where nearby lab personnel can respond to the alarm and correct the problem. The second line of defense, with the advent of Tempurity's advanced distributed data, is centralized monitoring of an entire organization's samples, which might be accomplished by a facilities or security group. Hallway displays, implemented via a dedicated computer running the Tempurity Monitor, and showing the entire population of freezers for a group or department can be a third line of defense.

Monitoring freezers is sometimes assumed to be a "reactive" process. Many of our clients find that the value of Tempurity is less in the generation of alarm notifications for out-of-range conditions than in the ability to easily examine the daily cycling of the temperatures and other environmental conditions of their samples under "normal" conditions. Some customers will be able to recognize trends in temperature history that signal the need for replacement or maintenance of their freezer or incubator.

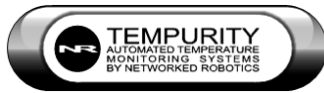
A person is still the best judge of a temperature quality problem and how to fix it. For these reasons we feel that the most powerful feature of Tempurity is the ubiquitous, fingertip-access to the temperatures and other data types from critical scientific instruments and sensors. People and processes must be appropriately employed in order to assure sample quality and these people are best served by the use of advanced tools like the Tempurity System by Networked Robotics.



Index

- Alarm, 66, 82
 - stage one, 48
 - stage one interval, 37
 - stage one time threshold, 48
 - stage two interval, 37
- Alarm criteria, 36
- Alarm file, 84
- Alarm notification definition*, 65
- time delay, 70
- Alarm Notification**, 82
- Alarm notification group
 - monitored devices, 67
 - name, 66
 - storage, 68
- Alarm Notification Group**, 82
- Alarm notification groups
 - disappearing, 68
 - testing, 67
- Alarm Notification Type**, 82
- Alarm notifications
 - periodic testing, 78
 - text gateways, 69
- Alarm Window*, 58
- Authenticated SMTP, 41
- Calibration, 78
- Calibration Factor, 37
- Client software installation**, 8
- Command Character, 37
- Communication alarm
 - comm one interval, 37
 - comm two interval, 37
 - description*, 48
 - intermittent, 48
- Configuration files
 - definition, 45
 - editing, 45
 - histories, 84
 - location, 84
 - restoring, 45
- Connectivity problems, 29
 - flowchart, 29
- Crossover cable, 17
- Custom monitored device
 - types, 39
- Data file, 84
- Data retention**, 88
- Digital temperature probe, 23
- DLL, 84
- Dry Contact Probe, 40
- DS18B20Z, 47
- Extending connections, 18
- FDA, 6
- Firewall, 28
- Firewall exceptions, 87
- Flood sensor, 40
- Flow Chart for Testing
 - Network Data Collection, 29
- Freezer, 24
- Freezer failure, 48
- Glycerin, 25
- Gmail, 44
- Google account, 44
- Graph
 - autoscale, 61
- Guaranteed alarm notification, 77
- Hallway displays, 79
- Inactive, 58
- Interface type, 23
 - Networked Robotics RTD probe, 25
 - supported interfaces, 23
 - ultracold freezer interface, 23
- localhost, 32
- Mail account name, 42
- Main monitor screen
 - blue, 57
 - gray, 57
 - green, 57
 - red, 58
 - yellow, 57
- Maximum Value, 37
- Microsoft Exchange®, 43
 - monitor name limitation, 54
- Minimum Value, 37
- Monitor Name**, 82
- Monitored **device**
 - maximum number, 88
- Monitored Device**, 82
- Monitored Device Name, 37
- Monitored Device Type, 37, 82
- Monitoring multiple Tempurify Servers, 70
- Network
 - hub, 17
 - switch, 17
- Network time server, 75
- Networked Robotics Unique ID**, 82
- NTMS, 14
 - 10 Mb/s, 17
 - data port 1, 14
 - data ports, 14
 - default IP, 21
 - distance from sensor, 18
 - FCC certification, 85
 - green led, 16
 - hardware architecture, 89
 - MAC Address, 21
 - NTMS Configuration Wizard, 16
 - Part 15 compliance, 85
 - red led, 16
 - requirements, 8
 - reset switch, 15
 - static IP, 22
 - unique ID, 15
 - yellow led, 16
- NTMS Configuration Wizard
 - downloading, 20
- Ovens, 25
- Peer-to-peer, 6
- Ping, 27
- Power options, 86
- Power outages, 77
- Precision, 37
- Probe
 - dual-lock, 25
 - installation, 25
 - positioning, 25
 - removal, 25
- Redundancy data collection*, 77
- near-far, 77
- Refrigerator, 25
- Requirements, 8
- Safety*, 78
- Screen resolution, 87
- SMTP mail server
 - Exchange, 43
- SMTP mail servers, 41

- Specifications, 88
- SSL protocol, 42
- Standard network wall plates, 26
- Standard operating procedures, 79
- Subnet, 20
- TCP port, 37
- Telnet, 27
 - successful response, 29
- Temperature data
 - backup, 47
 - cyclic redundancy check, 47
 - data files, 84
 - deletion, 47
 - events, 65
 - location, 47
 - measurement interval, 46
 - measurement period, 46
 - statistics, 64
 - time of measurement, 46
- Temperature units*, 46
- Tempurity Monitor, 70, 82
 - alarm notifications, 65
 - alarm window display, 58
 - disable close, 52
 - downloading, 50
 - installation options, 52
 - main monitor screen, 55
 - number of monitors, 54
 - read-only, 50
 - starting, 54
 - supported languages, 71
 - time display, 75
 - watching multiple servers, 70
- Tempurity Server, 34, 41, 82
 - automatic restart, 86
 - computer time, 75
 - configuration files, 45
 - Configuring Monitored Devices, 36
 - conflict with any web server software, 30
 - conflicts with web server software, 87
 - connecting through remote desktop, 32
 - dedicated, 30
 - downloading, 30
 - external IP address, 44
 - identity, 41
 - monitoring multiple servers, 71
 - name, 53
 - operating system, 88
 - recommended name, 68
 - starting and stopping through Windows, 34
 - stopped, 33
 - Tempurity Server Configuration Utility, 33
 - testing automatic restart, 86
 - testing mail server connection, 43
 - time synchronization, 75
 - uninstalling, 31
- Tempurity Server Configuration Utility, 33, 35
- wrench icon, 35
- Tempurity System
 - installation, 9
 - PC settings, 86
- Tempurity System software, 11
 - Tempurity Taskbar*, 31
- Text message
 - alias, 70
- Time zone, 87
- Time zones, 75
- TPL3U digital temperature probe
 - installation, 25
- Ultracold
 - adapter, 24
 - connection, 24
- Uninterruptible power supplies, 78
- Units, 37
- Universal time, 87
- USP definition**
 - cold**, 83
 - cool**, 83
 - excessive heat**, 83
 - freezer**, 83
 - room temperature**, 83
 - warm**, 83
- Value alarms, 48
- Voice alarms
 - enabling, 44
 - phone number, 45
- Windows
 - automatic updates, 87
- Windows XP Professional, 7
- Wireless network, 18



Appendix A: Glossary of Key Tempurify System Terms

Monitored Device – The data stream that you are watching. It is obtained from a network address that is an IP address/network port combination. Sometimes the instrument or sensor interface supports data collection of several monitored device types from a single IP address/port combination. For example both humidity and temperature are obtained from the Networked Robotics HPL1 relative humidity probe. In this case the humidity stream is a monitored device and the temperature stream is a second monitored device even though both parameters come from the same sensor.

Monitored Device Type– E.G. Relative Humidity, Co2 concentration, Temperature (not incubator, freezer, room which are considered to be instruments or sensors)

Monitor Name – Since any computer can initiate alarm notifications, alarm notification messages need to be labeled with a name that distinguishes it from other senders of alarm notifications – The Monitor Name

Alarm – A state attached to each monitored device. There are multiple stages of alarm state. In Tempurify the word “alarm” is a noun and not a verb

Alarm Notification – A message telling you that a monitored device is in alarm state. Alarm Notifications will be sent when a monitored device enters an alarm state

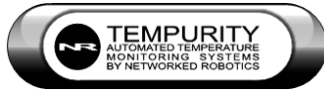
Alarm Notification Group – When a monitored device that is specified in the alarm notification group alarms, alarm notification messages are sent to the list of the intended recipients in the alarm notification group

Alarm Notification Type – e.g. E-mail, cell phone text message, automated voice to a phone

Tempurify Server – Collects data from monitored devices through the network and stores it. Defines when an alarm is occurring. Services the data feeds to any connected Tempurify Monitors and the Monitor's requests to send alarm notifications

Tempurify Monitor – Continuously watches a Tempurify Server to see if alarm conditions have been met for any Monitored Devices. The Monitor can not write regulated data. It reads data however and can distribute data visually or in the form of alarm notifications. The Tempurify Monitor is the main user interface for the Tempurify System

Networked Robotics Unique ID – The unique numeric combination labeled on the side of each NTMS unit. This is the same number as the MAC address of the NTMS hardware.



Appendix B: USP Temperature Storage Definitions

From US Pharmacopeia Quality Review No. 40, Revised 6/94

"In some USP monographs, there are specific directions for stating the temperature at which Pharmacopeial articles shall be stored. The following are storage definitions, as defined in the *General Notices* section of the *USP XXII-NF XVII*, for recommended conditions commonly specified on product labels."

Freezer

A place in which the temperature is maintained thermostatically between -20°C and -10°C (-4°F and 14°F).

Cold

Any temperature not exceeding 8°C (46 F). A refrigerator is a cold place in which the temperature is maintained thermostatically between 2°C and 8°C (36°F- 46 F).

Cool

Any temperature between 8°C and 15°C (46°F-59 F). An article that requires cool storage, alternatively may be stored in a refrigerator, unless otherwise specified by the individual USP monograph.

Room Temperature

The temperature prevailing in a working area.

Controlled Room Temperature

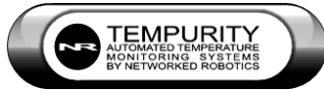
A temperature maintained thermostatically that encompasses the usual and customary working environment of 20°C to 25°C (68°F-77°F) that allows for brief deviations between 15°C and 30°C (59°F- 86 F) that are experienced in pharmacies, hospitals, and warehouses. Articles may be labeled for storage at "controlled room temperature" or at "up to 25", or other wording. An article for which storage at *Controlled room temperature* is directed may, alternatively, be stored in a cool place, unless otherwise specified in the individual monograph or on the label. (See the entire revised definition of *Controlled Room Temperature* in the *Ninth Supplement to USP XXII-NF XVII*.)

Warm

Any temperature between 30°C and 40°C (86°F-104 F).

Excessive Heat

Any temperature above 40°C (104°F).



Appendix C: File Locations

Files:

C:\Program Files (x86)\Networked Robotics\Tempurity Server\tempurity (64 bit other Windows)
Or
C:\Program Files\Networked Robotics\Tempurity Server\tempurity (32 bit other Windows)
Or
C:\Windows\System32\Tempurity (Windows XP 32 bit)

Bin- executable files
Config- configuration files
Data - Data and verification files

Configuration histories are stored in the "History" subdirectory of the Configuration folder by year and date

Alarm data is stored in the files "alarm_YYYY" where YYYY is the year that the alarms were observed

C:\Program Files\Networked Robotics
stores client executables and needed DLLs and DLL registration utility

Some needed DLL files are also stored in the Windows\System32 directory.

An Example Alarm File Record:

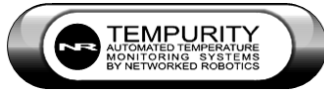
1225221944,1225221944,011, HPL1Probe, Comm,01

Times are the same and shown in Universal Time
Monitored Device ID
Monitored Device Name
Type of Alarm
Stage 1=Stage1, 2=Stage2, 3=Clear

An Example Data File Record

1258437680 +22.50 Celsius +0.00

Time of acquisition is shown in Universal Time
Data Value
Units
Correction Factor



Appendix D: Networked Robotics' NTMS4 Hardware FCC Certification



The NTMS4 version I network hardware complies with FCC Part 15 Subpart A requirements.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

The NTMS4 version R network hardware complies with FCC Part 15 Subpart B requirements.

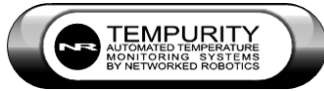
Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an output on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

The NTMS4 version P network hardware complies with 47 CFR Part 15, Subpart C for Intentional Radiators

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions. (1) This device may not cause harmful interference and 2) this device accept any interference received including interferences that may cause undesired operation. This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.



Appendix E: Configuring your PC for Use as a Tempurity Server or Monitor

Your computer system administrator is best able to tell if these changes are required. For some types of computing environments these changes would not be needed, for example Tempurity Server computers running from machine rooms with highly backed up power supplies might not need the power-related BIOS setting changes recommended below.

1) Control Panel -> Power Options

->Power Schemes Set to "Power Always On"

->Settings for "Power Always On" Power Scheme

"Turn off Hard Disks" should be set to "Never"

"System Hibernates" should be set to "Never"

"System Standby" should be set to "Never"

"Turn off Monitor" It's fine to allow the computer's monitor to turn off automatically after a given time unless this is a Tempurity Monitor computer used as a wall-mounted (eg. hallway or lab) display, meant to be always on in which case it should be set to "Never"

2) BIOS - Power Test and BIOS Setting

A Tempurity Server computer should be set to run automatically after a power fails and is then restored. When the power is restored processing should start automatically without the need for any manual intervention.

You will need to set the BIOS options of your computer. The commands to access BIOS are different on each computer model. Usually a function key is pressed during the boot sequence. You'll need to check your manual to find the proper keystrokes to enter. Once in the BIOS you'll want to look at the category:

"Power Management Setup" or equivalent

There should be a setting called "AC Power Loss Restart" or "Restore on AC Power Loss". This should be set to Yes.

Although it's not good for your computer (it *is* good for your compliance or quality program) You should test that the setting is right by yanking the power cord out of the PC or unplugging it from the wall, then plug it back in. If Windows restarts, the system is appropriate for the Tempurity System to automatically recover from a power failure.

3) Control Panel -> Windows Firewall -> Exceptions

If you want other PCs to access the Tempurity data then right click on Properties and then Advanced for Firewall click Exceptions and Add port 3010 TCP. If you want other PCs to be able to run the Tempurity Monitor and thus to initiate alarm notifications also ensure that port 80 is open on the Tempurity Server computer.

4) Control Panel->Automatic Updates

Set to "Notify me but don't download or install them"

Automatic Updates can interrupt normal PC operation at unexpected times. Install updates manually.

5) Control Panel -> Display -> Settings -> Screen Resolution

Should be set to 1024 x 768 resolution or better

6) Control Panel -> Date and Time

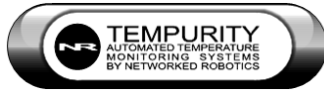
Enter the correct, date, time zone, and time

Networked Robotics recommends connection to a time server, which is the default and already set on most new PCs. The Time Zone setting does NOT matter since Tempurity data is tagged with Universal Time. However the time of day should be correct.

7) Control Panel -> User Accounts

Make sure that passwords are entered on all Windows accounts. This is required for regulatory compliance.

8) The Tempurity Server should not run web server software such as IIS or Apache. These will conflict with the Tempurity Server software and cause unpredictable results in both Tempurity and your web service.



Appendix F: Tempurity System Specifications

Maximum Number of Monitored Devices on Each Tempurity Server

56

Server Operating System

Most Windows Operating Systems – See www.NetworkedRobotics.com.

Temperature Scale

Celsius and Fahrenheit in the Monitor Client
Celsius only in the Tempurity Server Configuration

Alarm Levels

2

Data Retention

There is no capability for data deletion or modification through the Tempurity System.

Data Format

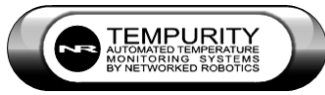
Temperatures and other data are stored in a series of Windows text files.

Network Access

Access to a properly functioning wired or wireless TCP/IP network connection is required. Switched networks are recommended for wired applications.

Power Backup

Tempurity relies on the availability of power and network to collect temperatures and other data types. UPS power should be used on Tempurity Server, Tempurity Monitor computers, internal mail servers, and the network equipment that supports outbound connections to the internet.



Appendix G: Networked Robotics' Hardware Architecture for Handling the Physical Diversity in Data Collection

Figure G1 below describes the Networked Robotics architecture for handling the physical complexity needed to acquire data from diverse instruments and sensors. The figure shows a cascading complexity, from a uniform network device, to a limited number of connector/hardware interfaces, to a wide variety of scientific instruments and sensors. Logical complexity is handled by labile NTMS firmware that can “learn” to speak the data languages of diverse scientific instruments and sensors.

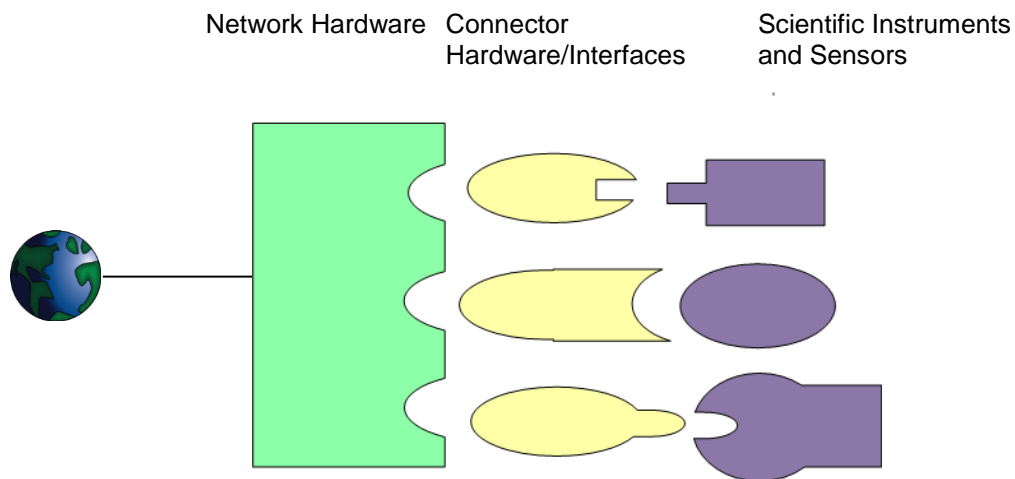


Figure G1: Networked Robotics Corporation's Architecture for Collecting Data form Diverse Instrumentation

An example of one kind of network hardware is the Networked Robotics NTMS4i.

Examples of connector/interfaces are the Networked Robotics DCP probe, the Networked Robotics Thermo-Revco® and compatible ultracold freezer interface, the Networked Robotics RTD Probe, the Networked Robotics Thermo-Cryoplus® liquid nitrogen freezer and compatible interface.

Examples of scientific instruments and sensors are the Networked Robotics TPL3 digital temperature probe, the Networked Robotics HPI1 humidity probe, Thermo-Revco® Ultracold freezers, Marvel® Refrigerators and Freezers, Lauda® water baths, Sanyo® freezers, etc.