RFM220
ISDB-Tb Measurement Demodulator

User Manual

071-2896-00

Tektronix

RFM220
ISDB-Tb Measurement Demodulator

User Manual

This document supports software version 1.0.

www.tektronix.com

071-2896-00

Tektronix

Contacting Tektronix

Tektronix, Inc.
14150 SW Karl Braun Drive
P.O. Box 500
Beaverton, OR 97077
USA

For product information, sales, service, and technical support:

- In North America, call 1-800-833-9200.
- Worldwide, visit www.tektronix.com to find contacts in your area.

This warranty is for the hardware.

Warranty

Tektronix warrants that this product will be free from defects in materials and workmanship for a period of one (1) year from the date of shipment. If any such product proves defective during this warranty period, Tektronix, at its option, either will repair the defective product without charge for parts and labor, or will provide a replacement in exchange for the defective product. Parts, modules and replacement products used by Tektronix for warranty work may be new or reconditioned to like new performance. All replaced parts, modules and products become the property of Tektronix.

In order to obtain service under this warranty, Customer must notify Tektronix of the defect before the expiration of the warranty period and make suitable arrangements for the performance of service. Customer shall be responsible for packaging and shipping the defective product to the service center designated by Tektronix, with shipping charges prepaid. Tektronix shall pay for the return of the product to Customer if the shipment is to a location within the country in which the Tektronix service center is located. Customer shall be responsible for paying all shipping charges, duties, taxes, and any other charges for products returned to any other locations.

This warranty shall not apply to any defect, failure or damage caused by improper use or improper or inadequate maintenance and care. Tektronix shall not be obligated to furnish service under this warranty a) to repair damage resulting from attempts by personnel other than Tektronix representatives to install, repair or service the product; b) to repair damage resulting from improper use or connection to incompatible equipment; c) to repair any damage or malfunction caused by the use of non-Tektronix supplies; or d) to service a product that has been modified or integrated with other products when the effect of such modification or integration increases the time or difficulty of servicing the product.

THIS WARRANTY IS GIVEN BY TEKTRONIX WITH RESPECT TO THE PRODUCT IN LIEU OF ANY OTHER WARRANTIES, EXPRESS OR IMPLIED. TEKTRONIX AND ITS VENDORS DISCLAIM ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. TEKTRONIX' RESPONSIBILITY TO REPAIR OR REPLACE DEFECTIVE PRODUCTS IS THE SOLE AND EXCLUSIVE REMEDY PROVIDED TO THE CUSTOMER FOR BREACH OF THIS WARRANTY. TEKTRONIX AND ITS VENDORS WILL NOT BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES IRRESPECTIVE OF WHETHER TEKTRONIX OR THE VENDOR HAS ADVANCE NOTICE OF THE POSSIBILITY OF SUCH DAMAGES.

[W2 – 15AUG04]

This warranty is for the software media.

Warranty

Tektronix warrants that the media on which this software product is furnished and the encoding of the programs on the media will be free from defects in materials and workmanship for a period of three (3) months from the date of shipment. If any such medium or encoding proves defective during the warranty period, Tektronix will provide a replacement in exchange for the defective medium. Except as to the media on which this software product is furnished, this software product is provided “as is” without warranty of any kind, either express or implied. Tektronix does not warrant that the functions contained in this software product will meet Customer's requirements or that the operation of the programs will be uninterrupted or error-free.

In order to obtain service under this warranty, Customer must notify Tektronix of the defect before the expiration of the warranty period. If Tektronix is unable to provide a replacement that is free from defects in materials and workmanship within a reasonable time thereafter, Customer may terminate the license for this software product and return this software product and any associated materials for credit or refund.

THIS WARRANTY IS GIVEN BY TEKTRONIX WITH RESPECT TO THE PRODUCT IN LIEU OF ANY OTHER WARRANTIES, EXPRESS OR IMPLIED. TEKTRONIX AND ITS VENDORS DISCLAIM ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. TEKTRONIX' RESPONSIBILITY TO REPLACE DEFECTIVE MEDIA OR REFUND CUSTOMER'S PAYMENT IS THE SOLE AND EXCLUSIVE REMEDY PROVIDED TO THE CUSTOMER FOR BREACH OF THIS WARRANTY. TEKTRONIX AND ITS VENDORS WILL NOT BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES IRRESPECTIVE OF WHETHER TEKTRONIX OR THE VENDOR HAS ADVANCE NOTICE OF THE POSSIBILITY OF SUCH DAMAGES.

[W9b – 15AUG04]

IMPORTANT

READ BEFORE OPERATING EQUIPMENT

This software is provided under license from Tektronix, Inc. Retention of this program for more than thirty (30) days or use of the program in any manner constitutes acceptance of the license terms.

CAREFULLY READ THE ENCLOSED SOFTWARE LICENSE AGREEMENT. If you cannot agree to the license terms, promptly contact the nearest Tektronix Field Office for return assistance.

TEKTRONIX SOFTWARE LICENSE AGREEMENT

THE PROGRAM, OR PROGRAMS, ENCODED OR INCORPORATED WITHIN EQUIPMENT, IS FURNISHED SUBJECT TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. RETENTION OF THE PROGRAM FOR MORE THAN THIRTY DAYS OR USE OF THE PROGRAM IN ANY MANNER WILL BE CONSIDERED ACCEPTANCE OF THE AGREEMENT TERMS. IF THESE TERMS ARE NOT ACCEPTABLE, THE UNUSED PROGRAM AND ANY ACCOMPANYING DOCUMENTATION SHOULD BE RETURNED PROMPTLY TO TEKTRONIX FOR A FULL REFUND OF THE LICENSE FEE PAID. (FOR INFORMATION REGARDING THE RETURN OF PROGRAMS ENCODED OR INCORPORATED WITHIN EQUIPMENT, CONTACT THE NEAREST TEKTRONIX SALES OFFICE.)

DEFINITIONS. "Tektronix" means Tektronix, Inc., an Oregon corporation, or local Tektronix' legal entity that is supplying the equipment.

"Program" means the Tektronix software product (executable program and/or data) enclosed with this Agreement or included within the equipment with which this Agreement is packed.

"Customer" means the person or organization in whose name the Program was ordered.

LICENSE. Customer may:

1. Use the Program on any number of machines at any one time;
2. If the Program is provided in connection with a floating-user license, the Program may be used on multiple machines provided that the user is authorized, and the total number of users at any one time does not exceed the total number of licensed concurrent users;
3. Modify the Program or merge it with another for use on one or more machines by authorized users; and
4. Copy the Program for archival or backup purposes. The Program may be copied onto multiple machines for use by authorized users.

Each copy of the Program made by Customer must include a reproduction of any copyright notice or restrictive rights legend appearing in or on the copy of the Program as received from Tektronix.

Customer may not:

1. Transfer the Program to any person or organization outside of Customer or the corporation of which Customer is a part without the prior written consent of Tektronix, except in connection with the transfer of the equipment within which the programs are encoded or incorporated;

2. Export or reexport, directly or indirectly, the program, any associated documentation, or the direct product thereof, to any country to which such export or reexport is restricted by law or regulation of the United States or any foreign government having jurisdiction without the prior authorization, if required, of the Office of Export Administration, Department of Commerce, Washington, D.C. and the corresponding agency of such foreign government;

3. For object-code Programs only, reverse compile or disassemble the Program for any purpose; or

4. Copy the documentation accompanying the Program.

For Programs designed to reside on a single-machine and support one or more additional machines, either locally or remotely, without permitting the Program to be transferred to an additional machine for local execution, the additional machines shall be considered within the definition of "single machine".

Title to the Program and all copies thereof, but not the media on which the Program or copies may reside, shall be and remain with Tektronix or others for whom Tektronix has obtained a respective licensing right.

Customer shall pay when due all property taxes that may now or hereafter be imposed, levied or assessed with respect to the possession or use of the Program or this license and shall file all reports required in connection with such taxes.

Any portion of the Program modified by Customer or merged with another program shall remain subject to these terms and conditions.

If the Program is acquired by or for an agency of the U.S. Government, the Program shall be considered computer software developed at private expense and the license granted herein shall be interpreted as granting Customer restricted rights in the Program and related documentation as defined in the applicable acquisition regulation.

THE PROGRAM MAY NOT BE USED, COPIED, MODIFIED, MERGED, OR TRANSFERRED TO ANOTHER EXCEPT AS EXPRESSLY PERMITTED BY THESE TERMS AND CONDITIONS.

UPON TRANSFER OF ANY COPY, MODIFICATION, OR MERGED PORTION OF THE PROGRAM, THE LICENSE GRANTED HEREIN IS AUTOMATICALLY TERMINATED.

TERM. The license granted herein is effective upon acceptance by Customer, and shall remain in effect until terminated as provided herein. The license may be terminated by Customer at any time upon written notice to Tektronix. The license may be terminated by Tektronix or any third party from whom Tektronix may have obtained a respective licensing right if Customer fails to comply with any term or condition and such failure is not remedied within thirty (30) days after notice hereof from Tektronix or such third party. Upon termination by either party, Customer shall return to Tektronix or destroy, the Program and all associated documentation, together with all copies in any form.

LIMITED WARRANTY. Tektronix warrants that the media on which the Program is furnished and the encoding of the Program on the media will be free from defects in materials and workmanship for a period of three (3) months from the date of shipment. If any such medium or encoding proves defective during the warranty period, Tektronix will provide a replacement in exchange for the defective medium. Except as to the media on which the Program is furnished, the Program is provided "as is" without warranty of any kind, either express or implied. Tektronix does not warrant that the functions contained in the Program will meet Customer's requirements or that the operation of the Program will be uninterrupted or error-free.

In order to obtain service under this warranty, Customer must notify Tektronix of the defect before the expiration of the warranty period. If Tektronix is unable to provide a replacement that is free from defects in materials and workmanship within a reasonable time thereafter, Customer may terminate the license for the Program and return the Program and any associated materials for credit or refund.

THIS WARRANTY IS GIVEN BY TEKTRONIX WITH RESPECT TO THE PROGRAM IN LIEU OF ANY OTHER WARRANTIES, EXPRESS OR IMPLIED. TEKTRONIX AND ITS VENDORS DISCLAIM ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. TEKTRONIX' RESPONSIBILITY TO REPLACE DEFECTIVE MEDIA, OR REFUND CUSTOMER'S PAYMENT IS THE SOLE AND EXCLUSIVE REMEDY PROVIDED TO THE CUSTOMER FOR BREACH OF THIS WARRANTY.

LIMITATION OF LIABILITY, IN NO EVENT SHALL TEKTRONIX OR OTHERS FROM WHOM TEKTRONIX HAS OBTAINED A LICENSING RIGHT BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR CONNECTED WITH CUSTOMER'S POSSESSION OR USE OF THE PROGRAM, EVEN IF TEKTRONIX OR SUCH OTHERS HAS ADVANCE NOTICE OF THE POSSIBILITY OF SUCH DAMAGES.

THIRD-PARTY DISCLAIMER. Except as expressly agreed otherwise, third parties from whom Tektronix may have obtained a licensing right do not warrant the program, do not assume any liability with respect to its use, and do not undertake to furnish any support or information relating thereto.

GENERAL. This Agreement contains the entire agreement between the parties with respect to the use, reproduction, and transfer of the Program.

Neither this Agreement nor the license granted herein is assignable or transferable by Customer without the prior written consent of Tektronix.

This Agreement and the license granted herein shall be governed by the laws of the state of Oregon.

All questions regarding this Agreement or the license granted herein should be directed to the nearest Tektronix Sales Office.

ADDITIONAL LICENSE GRANT FOR VIDEO TEST SEQUENCES. The Software Product may include certain test patterns, video test sequences and video clips (together “Video Test Sequences”). If so, the following terms describe Your rights to the Video Test Sequences:

You may use, copy and modify the Video Test Sequences and display or distribute copies of individual Video Test Sequences in connection with Your video testing activity.

You are not licensed to do any of the following:

1. You may not distribute the collection of Video Test Sequences, except in connection with the sale of original equipment containing the Video Test Sequences, without prior written permission from Tektronix.
2. You may not permit third parties to distribute copies of the Video Test Sequences.
3. You may not sell, license or distribute copies of the Video Test Sequences on a standalone basis or as part of any collection, product, or service where the primary value of the product or service is the Video Test Sequences.

You must indemnify, hold harmless, and defend Tektronix from and against any claims or lawsuits, including attorneys' fees, that arise from or result from the use or distribution of Video Test Sequences as modified by You.

You must include a valid copyright notice on Your products and services that include copies of the Video Test Sequences.

Table of Contents

List of Figures

List of Tables

General Safety Summary

Review the following safety precautions to avoid injury and prevent damage to this product or any products connected to it.

To avoid potential hazards, use this product only as specified.

Only qualified personnel should perform service procedures.

To Avoid Fire or Personal Injury

Use proper power cord. Use only the power cord specified for this product and certified for the country of use.

Ground the product. This product is grounded through the grounding conductor of the power cord. To avoid electric shock, the grounding conductor must be connected to earth ground. Before making connections to the input or output terminals of the product, ensure that the product is properly grounded.

Observe all terminal ratings. To avoid fire or shock hazard, observe all ratings and markings on the product. Consult the product manual for further ratings information before making connections to the product.

Power disconnect. The power cord disconnects the product from the power source. Do not block the power cord; it must remain accessible to the user at all times.

Do not operate without covers. Do not operate this product with covers or panels removed.

Do not operate with suspected failures. If you suspect that there is damage to this product, have it inspected by qualified service personnel.

Avoid exposed circuitry. Do not touch exposed connections and components when power is present.

Use proper fuse. Use only the fuse type and rating specified for this product.

Do not operate in wet/damp conditions.

Do not operate in an explosive atmosphere.

Keep product surfaces clean and dry.

Provide proper ventilation. Refer to the manual's installation instructions for details on installing the product so it has proper ventilation.

Terms in This Manual

These terms may appear in this manual:

WARNING. *Warning statements identify conditions or practices that could result in injury or loss of life.*

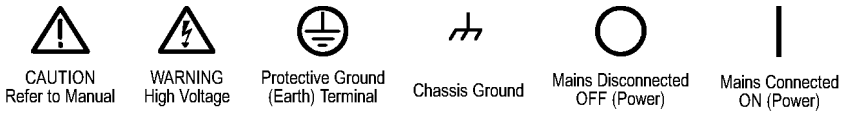
CAUTION. *Caution statements identify conditions or practices that could result in damage to this product or other property.*

Symbols and Terms on the Product

These terms may appear on the product:

- DANGER indicates an injury hazard immediately accessible as you read the marking.
- WARNING indicates an injury hazard not immediately accessible as you read the marking.
- CAUTION indicates a hazard to property including the product.

The following symbol(s) may appear on the product:



Compliance Information

This section lists the EMC (electromagnetic compliance), safety, and environmental standards with which the instrument complies.

EMC Compliance

EC Declaration of Conformity – EMC

Meets intent of Directive 2004/108/EC for Electromagnetic Compatibility. Compliance was demonstrated to the following specifications as listed in the Official Journal of the European Communities:

EN 61326-1 2006. EMC requirements for electrical equipment for measurement, control, and laboratory use.

- CISPR 11:2003. Radiated and conducted emissions, Group 1, Class A [1] [2] [3]
- IEC 61000-4-2:2001. Electrostatic discharge immunity
- IEC 61000-4-3:2002. RF electromagnetic field immunity [3]
- IEC 61000-4-4:2004. Electrical fast transient / burst immunity
- IEC 61000-4-5:2001. Power line surge immunity
- IEC 61000-4-6:2003. Conducted RF immunity
- IEC 61000-4-11:2004. Voltage dips and interruptions immunity

EN 61000-3-2:2006. AC power line harmonic emissions

EN 61000-3-3:1995. Voltage changes, fluctuations, and flicker

European contact.

Tektronix UK, Ltd.
Western Peninsula
Western Road
Bracknell, RG12 1RF
United Kingdom

1 This product is intended for use in nonresidential areas only. Use in residential areas may cause electromagnetic interference.

2 Emissions which exceed the levels required by this standard may occur when this equipment is connected to a test object.

3 For compliance with the EMC standards listed here, high quality shielded interface cables should be used.

Australia / New Zealand Declaration of Conformity – EMC

Complies with the EMC provision of the Radiocommunications Act per the following standard, in accordance with ACMA:

- CISPR 11:2003. Radiated and Conducted Emissions, Group 1, Class A, in accordance with EN 61326-1:2006.

Australia / New Zealand contact.

Baker & McKenzie
Level 27, AMP Centre
50 Bridge Street
Sydney NSW 2000, Australia

Safety Compliance

EC Declaration of Conformity – Low Voltage

Compliance was demonstrated to the following specification as listed in the Official Journal of the European Communities:

Low Voltage Directive 2006/95/EC.

- EN 61010-1: 2001. Safety requirements for electrical equipment for measurement control and laboratory use.

Additional Compliances

- IEC 61010-1: 2001. Safety requirements for electrical equipment for measurement, control, and laboratory use.

Equipment Type

Test and measuring equipment.

Safety Class

Class 1 – grounded product.

Pollution Degree Description

A measure of the contaminants that could occur in the environment around and within a product. Typically the internal environment inside a product is considered to be the same as the external. Products should be used only in the environment for which they are rated.

- Pollution Degree 1. No pollution or only dry, nonconductive pollution occurs. Products in this category are generally encapsulated, hermetically sealed, or located in clean rooms.
- Pollution Degree 2. Normally only dry, nonconductive pollution occurs. Occasionally a temporary conductivity that is caused by condensation must be expected. This location is a typical office/home environment. Temporary condensation occurs only when the product is out of service.
- Pollution Degree 3. Conductive pollution, or dry, nonconductive pollution that becomes conductive due to condensation. These are sheltered locations where neither temperature nor humidity is controlled. The area is protected from direct sunshine, rain, or direct wind.
- Pollution Degree 4. Pollution that generates persistent conductivity through conductive dust, rain, or snow. Typical outdoor locations.

Pollution Degree

Pollution Degree 2 (as defined in IEC 61010-1). Note: Rated for indoor use only.

Installation (Overvoltage) Category Descriptions

Terminals on this product may have different installation (overvoltage) category designations. The installation categories are:

- Measurement Category IV. For measurements performed at the source of low-voltage installation.
- Measurement Category III. For measurements performed in the building installation.
- Measurement Category II. For measurements performed on circuits directly connected to the low-voltage installation.
- Measurement Category I. For measurements performed on circuits not directly connected to MAINS.

Overvoltage Category

Overvoltage Category II (as defined in IEC 61010-1)

Environmental Considerations

This section provides information about the environmental impact of the product.

Product End-of-Life Handling

Observe the following guidelines when recycling an instrument or component:

Equipment recycling. Production of this equipment required the extraction and use of natural resources. The equipment may contain substances that could be harmful to the environment or human health if improperly handled at the product's end of life. To avoid release of such substances into the environment and to reduce the use of natural resources, we encourage you to recycle this product in an appropriate system that will ensure that most of the materials are reused or recycled appropriately.

This symbol indicates that this product complies with the applicable European Union requirements according to Directives 2002/96/EC and 2006/66/EC on waste electrical and electronic equipment (WEEE) and batteries. For information about recycling options, check the Support/Service section of the Tektronix Web site (www.tektronix.com).

Restriction of Hazardous Substances

This product is classified as Monitoring and Control equipment, and is outside the scope of the 2002/95/EC RoHS Directive.

Preface

This manual describes how to install and operate the Tektronix RFM220 ISDB-Tb Measurement Demodulator.

Product Documentation

The following table lists the other documents supporting the RFM220 demodulator. These manuals are available on the Tektronix Web site at www.tektronix.com/manuals.

Table i: Product documentation

Item (Tektronix part number)	Purpose
RFM220 User Manual (071-2896-XX)	Provides installation and operational information (this document)
RFM220 Specifications and Performance Verification Technical Reference (077-0565-XX)	Provides complete product specifications and a procedure for verifying the operation of the instrument
RFM220 Declassification and Security Instructions (077-0567-XX)	Provides instructions for removing your proprietary information from the instrument
RFM220 Software License Notices Reference (001-1581-XX)	Provides the software licenses that cover the RFM220 software

Naming Conventions

This document uses the following naming conventions when referring to the different components of the RFM220 system:

- RFM220 ISDB-Tb Measurement Demodulator. This is the hardware component of the system and is referred to as either “RFM220 instrument” or just “instrument.”
- RFM220 Aggregator application. This is the software application that collects data from monitored RFM220 instruments and is referred to as either “RFM220 Aggregator” or just “Aggregator.”
- RFM220 Client application. This is the software application that displays the monitoring data collected by the Aggregator and is referred to as either “RFM220 Client” or just “Client.”
- RFM220 Device Setup utility. This is the software application that allows the user to set the instrument network parameters, reset the instrument, or upgrade the instrument firmware and is referred to as the “Device Setup utility.”

Related Products

Tektronix also offers the following related products:

MTM400A DTV Monitor

The MTM400A DTV Monitor provides a complete solution for multilayer, multichannel, remote monitoring to DVB, ATSC, DCII, and ISDB-T/Tb standards with content-checking support for MPEG-2 and H.264/AVC. Optional RF measurement interfaces provide a powerful and cost-effective solution for monitoring DVB-T transmitter sites or DVB-S/S2 uplinks and downlinks. An in-depth, real-time MPEG analysis option allows diagnostics to be performed on live broadcast signals without having to use deferred-time analysis of captured streams.

Refer to the *MTM400A DTV Monitor Quick Start User Manual*, Tektronix part number 071-2492-XX.

IPM400A DTV Monitor

The IPM400A DTV Monitor is a powerful solution for remote monitoring of IP video national and regional headends. The IPM400A simultaneously verifies both IP and TS integrity on all IP Video flows (sessions) on a GbE link. It is ideal for monitoring networks which carry both Multi-Program Transport Streams (MPTS) or Single-Program Transport Streams (SPTS), at either constant bit rate (CBR) or variable bit rate (VBR). An in-depth, real-time MPEG analysis option allows diagnostics to be performed on live payload without having to use deferred-time analysis of captured streams.

Refer to the *IPM400A DTV Monitor Quick Start User Manual*, Tektronix part number 071-2698-XX.

QAM400A DTV Monitor

The QAM400A DTV Monitor provides a complete solution for remote real-time monitoring of cable broadcast signals. The comprehensive QAM RF and SI/PSI and PSIP confidence-monitoring capabilities provide a powerful and cost-effective solution for monitoring HFC (hybrid fibre-coaxial) cable headends. An in-depth, real-time MPEG analysis option allows diagnostics to be performed on live ATSC signals without having to use deferred-time analysis of captured streams.

Refer to the *QAM400A DTV Monitor Quick Start User Manual*, Tektronix part number 071-2784-XX.

RFM300 DTV Monitor

The RFM300 DTV Monitor provides a complete solution for remote real-time DTV monitoring of ATSC signals. The comprehensive 8VSB RF and PSIP confidence-monitoring capabilities provide a powerful and cost-effective solution for monitoring DTV transmitter sites, including contribution and distribution feeds at local and national operation centers for FCC compliance. An in-depth, real-time MPEG analysis option allows diagnostics to be performed on live ATSC signals without having to use deferred-time analysis of captured streams.

Refer to the *RFM300 DTV Monitor Quick Start User Manual*, Tektronix part number 071-2700-XX.

VQS1000 Video Quality Software

VQS1000 is a Video Quality Software application for single ended objective QoE analysis of video and audio content. It is designed for use with all current Tektronix IP Video and DTV Monitor probes using private backhaul video and audio and audio. It can also be used standalone for file analysis. Combined with physical transport alarms from the Tektronix probes, operators can determine if the source of a problem is in the content (for example, over-compression) or in network distribution layers.

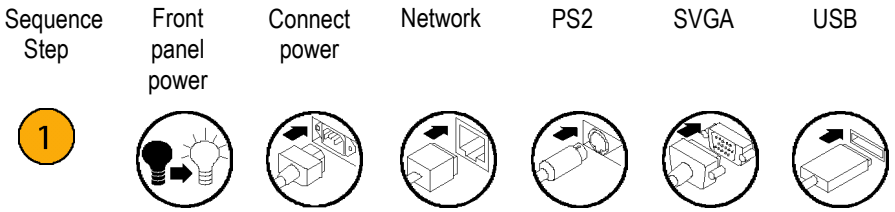
Refer to the *VQS1000 Video Quality Software Quick Start User Manual*, Tektronix part number 077-0489-XX.

Firmware and Software Upgrades

Updates to the RFM220 system firmware and software are released to the Tektronix Web site when problems are fixed or when new product features are introduced. (See page 51, *Upgrading Instrument Firmware*.) To check for firmware or software upgrades, go to the Tektronix Web site (www.tektronix.com/products/video-test).

Conventions Used in This Manual

The following icons are used throughout this manual.



Getting Started

Product Description

The Tektronix RFM220 ISDB-Tb Measurement Demodulator provides the means to measure and monitor signal performance for signals conforming to the Brazilian and Japanese ISDB-Tb terrestrial Digital TV standard.

The RFM220 demodulator can measure MER in real time, commonly considered a key figure for qualifying a transmitting system. The input to the RFM220 demodulator can be an RF signal or an ASI stream. The software interface displays measurement traces, signal spectrum, and constellation and lets you configure and control the instrument using a local or remote Ethernet connection.

Installed at a transmission site, the RFM220 demodulator can continuously monitor in real-time the essential signal performance figures such as input level, MER, shoulder levels, and error rate ratio. The ASI output on the RFM220 demodulator can output either the ASI input signal or the RF demodulated signal to feed an external video/audio decoder or a transport stream analyzer such as the Tektronix MTS400A MPEG Test System.

The RFM220 demodulator can be used as a standalone RF monitoring solution or used in conjunction with a Tektronix MTM400A DTV monitor to provide combined RF and TS monitoring. (See page 75, *Connecting to an MTM400A DTV Monitor*.)

Figure 1: RFM220 ISDB-Tb Measurement Demodulator

Key Features

- Demodulator
  - Single RF input
  - Single ASI input
  - Automatic transmission mode recovery
- Measurement probes
  - Full band input level
  - Channel input level
  - Left and right shoulder
  - Signal to Noise Ratio (SNR)
  - Carrier Frequency Offset (CFO)
  - Coarse MER
  - Fine MER per Layer
  - BER, PER
  - TS monitoring possible when the RFM220 output signal is fed to a TS analyzer such as the Tektronix MTM400A DTV Monitor
- Measurement data
  - Recovery transmission mode (from TMCC)
  - SFN window (5 main echoes)
- Measurement displays
  - Spectrum response
  - Coarse and overall Constellation pattern
  - Fine Constellation pattern per layer
  - Delay profile
- Clock and synchronization signal management
  - Internal 10 MHz but possibility to correct measures with external reference
- Control and management
  - Control via HTTP/Ethernet using the RFM220 software
  - Alarm management via SNMP

System Overview

The following illustration shows the block diagram of the RFM220 system, which consists of the following components: RFM220 instrument, RFM220 Aggregator application, and RFM220 Client application.

The RFM220 instrument(s) that will be monitored and the PCs running the RFM220 Client application must be connected to the same Ethernet network as the PC or server running the RFM220 Aggregator application.

The RFM220 system can be used as a standalone RF monitoring solution or used in conjunction with a Tektronix MTM400A DTV monitor to provide combined RF and TS monitoring.

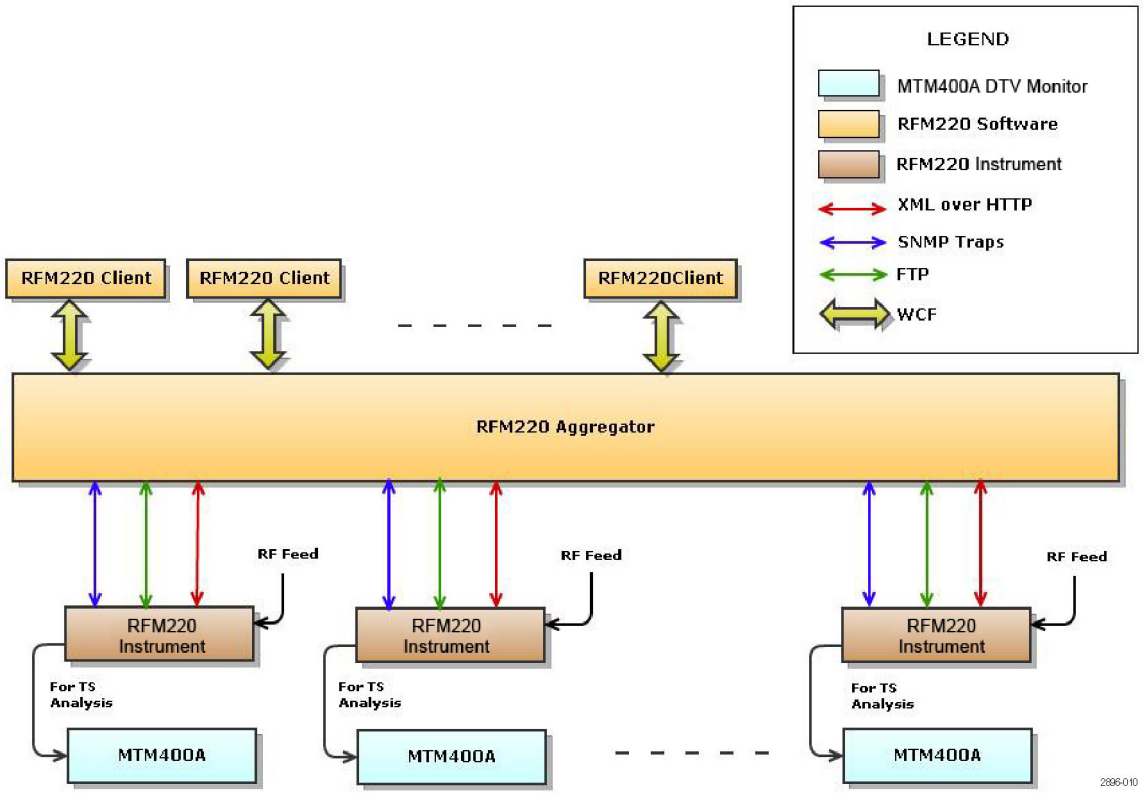


Figure 2: RFM220 system block diagram

RFM220 instrument. The RFM220 instrument is the hardware component of the system. ASI and RF signals that are connected to the instrument are monitored remotely by the RFM220 Aggregator. SNMP traps are sent to the RFM220 Aggregator when signal measurements exceed the user-defined limits, which are set using the RFM220 Client.

An individual RFM220 instrument can be monitored by only one RFM220 Aggregator at a time. Multiple RFM220 Clients can view the monitoring data for a single RFM220 instrument at a time by connecting to the RFM220 Aggregator that is monitoring the instrument.

RFM220 Aggregator applicaton. The RFM220 Aggregator application collects and stores data from RFM220 instruments and makes the data available to RFM220 Clients that connect to the Aggregator.

The RFM220 Aggregator can reside on a PC or on a network server. The typical RFM220 system installation will have the RFM220 Aggregator installed on a network server, where it can be accessed by remote PCs with the RFM220 Client application installed.

The RFM220 Aggregator can be configured to collect data from up to ten RFM220 instruments at a time. Only one RFM220 Aggregator should connect to an individual RFM220 instrument at a time. Multiple RFM220 Clients can connect to the RFM220 Aggregator at a time.

The RFM220 Aggregator configuration can be changed using the Configuration.xml file, which controls communications between the RFM220 system components (instrument, Aggregator, Client). The file can be updated dynamically, meaning that it can be updated while the RFM220 Aggregator is running.

RFM220 Client application. The RFM220 Client application allows the user to view the monitoring data collected by the RFM220 Aggregator application.

The data available for viewing includes event logs, metrics of signal parameters, device information such as the firmware version installed in the RFM220 instrument, and various graphs. You can view the data from any RFM220 instrument that the RFM220 Aggregator is monitoring. Multiple RFM220 Clients can be connected at the same time to a single RFM220 Aggregator.

MTM400A DTV Monitor (TS monitoring). All RF-related monitoring of the input signal is performed by the RFM220 system. If you also want to perform TS-related monitoring of the input signal, you can route the output signal from the RFM220 instrument to a TS analyzer such as the Tektronix MTM400A DTV Monitor. (See page 75, *Connecting to an MTM400A DTV Monitor*.)

RFM220 Device Setup utility. The RFM220 Aggregator software includes the RFM220 Device Setup utility. This utility allows the administrator of the RFM220 system to connect to a RFM220 instrument to perform the following tasks:

- View and change the network settings
- View and change the secondary trap address and port number (for use with an NMS system)
- Restart the instrument
- Reset the instrument settings back to the default values
- Upgrade the instrument firmware
- View the type of instrument and the installed hardware and firmware versions

User Profiles and Roles

The RFM220 system uses two user profiles to control software access: Administrator and User. Each user profile has different roles for supporting the RFM220 system.

Administrator. The Administrator profile has the following roles:

NOTE. *Although some of the administrative functions listed below can be performed by any user, it is recommended that the person who is assigned the role of RFM220 system administrator be the one responsible for these tasks.*

- Configuring the RFM220 Aggregator and making sure the correct RFM220 Client software is installed on all user PCs.
- Configuring the network settings for each RFM220 instrument and ensuring that each instrument is monitored by only one RFM220 Aggregator.
- Assigning passwords to the Administrator and User profiles.
- Ensuring that the correct set of RFM220 Clients are connecting to the correct RFM220 Aggregators
- Configuring the alarm thresholds and other measurement parameters.
- Configuring the channel plans and tuning the RFM220 instrument to a specific channel and frequency.
- Upgrading the instrument firmware and the Aggergator and Client software as needed.

User. The User profile has the following role:

- Viewing the measurement status of the signal connected to the RFM220 instrument and generating error log reports.

NOTE. *A person logged in under the User profile is not be able to change the RFM220 system configuration.*

Supported ISDB-Tb Modes

The RFM220 demodulator supports the ISDB-Tb modes listed below:

Table 1: Supported ISDB-Tb modes

Item	Description
Transmission modes	Multi-carrier (OFDM)
Bandwidth	6 MHz
FFT (carrier spacing)	Mode 1 (4 kHz), Mode 2 (2 kHz), Mode 3 (1 kHz)
Mapping	QPSK, 16QAM, 64QAM
Time interleave	From 0 to 32
Guard intervals	1/4, 1/8, 1/16, 1/32
FEC	1/2, 2/3, 3/4, 5/6, 7/8
Hierarchical mode	Single layer, 1+12 layer, layered A+B, layered A+B+C

Before Installation

Unpacking the Instrument

Unpack the instrument and check that you have received all of the standard accessories. (See Table 2.)

Table 2: Standard accessories

Accessory	Tektronix part number
Certificate of Compliance	001-1180-XX
RFM220 Software and Documentation CD	063-4352-XX
RFM220 User Manual	071-2896-XX
Power cord – Brazil	N/A

Installation Process

The process for installing and starting the RFM220 system includes the following steps:

CAUTION. *To prevent installation problems, the person assigned as the RFM220 system administrator should perform these initial system-setup tasks. (See page 5, User Profiles and Roles.)*

1. Install the RFM220 instrument and power the instrument on.
   (See page 8, *Hardware Installation*.)
2. Install the RFM220 software.
   (See page 12, *Software Installation*.)
3. For each RFM220 instrument that you intend to monitor, reset the instrument settings back to the factory-default state and configure the network settings.
   (See page 18, *Configuring the Network Settings of a RFM220 Instrument*.)
4. Edit the Configuration.xml file for the RFM220 Aggregator.
   (See page 22, *Configuring the RFM220 Aggregator*.)
5. Configure the Windows firewall settings.
   (See page 31, *Configuring the Windows Firewall*.)
6. Start the RFM220 Aggregator application.
   (See page 35, *Starting the RFM220 Aggregator*.)
7. Start the RFM220 Client application.
   (See page 38, *Starting the RFM220 Client*.)

Operating Considerations

Electrical

The following table lists the electrical operating requirements for the RFM220 instrument. The complete electrical operating requirements are listed in the *RFM220 Specifications and Performance Verification Technical Reference*.

Table 3: Electrical operating requirements

Requirement	Specification
Temperature, operating	+5 °C to +40 °C, 30 °C per hour maximum gradient, temperature of the intake air at the front and sides of the instrument
Altitude, operating	0 to 3,000 m (9,800 ft.)
Source voltage	100 to 240 V_{AC} 50/60 Hz, fluctuations must not exceed ±10% of the nominal rate voltage
Power consumption	0.6 A, 100-240 V, 50/60 Hz, single phase
Peak inrush current	1 A peak at 240 V_{AC}, 50 Hz
Fuse rating	Mains fuse is 2 A, 250 V, delay fuse; internal (not operator replaceable). Refer servicing to qualified service personnel.
Overvoltage category	II (as defined in IEC61010-1)
Pollution degree	2 (as defined in IEC61010-1), rated for indoor use only

Software

For the best operating performance, Tektronix strongly recommends that you install the RFM220 Aggregator and the RFM220 Client applications on separate computers. The Microsoft .NET Framework 3.5 software needs to be installed on the computer hosting the RFM220 Client.

Ethernet Network

The RFM220 instruments that will be monitored and the PCs running the RFM220 Client application need to be connected to an Ethernet network which has access to the PC or server running the RFM220 Aggregator application.

Hardware Installation

Air Flow

The RFM220 demodulator chassis is cooled by drawing air in from the left side of the instrument and exhausting it out the right side of the instrument. (See Figure 3.)

CAUTION. *To prevent damage to the instrument from overheating, do not block the left or right side of the instrument. Leave at least two inches of clearance on each side.*

Figure 3: Chassis air flow

Rackmounting

The RFM220 demodulator chassis is designed to be a transportable platform. If you need to install the instrument into an equipment rack, use one of the following two methods:

- Use appropriate hardware to secure the front face plate of the instrument to the rack, restraining the cantilevered mass of the instrument. (See Figure 7.)
- Use a rack shelf to support the instrument.

Figure 4: Securing the instrument in an equipment rack

Connecting Signals to the Instrument

The external connectors are all located on the rear panel of the instrument. (See Figure 43.) Refer to the *RFM220 Specifications and Performance Verification Technical Reference* for more detailed information about each connector and the associated signal requirements.

NOTE. *The 1PPS In connector is not used. Do not connect a signal cable to this connector.*

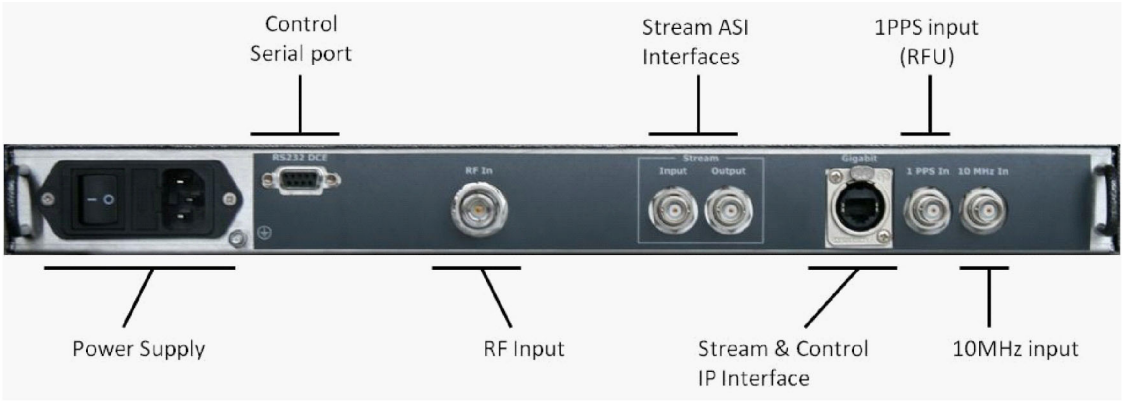


Figure 5: RFM220 rear panel

After you install the RFM220 demodulator in the desired location, connect the power cord that was provided with the instrument to the power connector on the rear panel. Connect the power cord plug to a properly grounded electrical outlet.

CAUTION. *To be sure of compliance with specified EMC standards and directives, use only high quality shielded cables with this product. Equipment performance can be affected. Typically, the cables are braid and foil types that have a low impedance connection to shielded connectors at both ends.*

The following table describes the signal requirements for each connector.

Table 4: External connectors

Connector	Description
RF input	Connector: N type, 50Ω Standard: ISDB-Tb Input frequency range: 170-230 MHz / 470-862 MHz Bandwidth: 6 MHz Input amplitude range: –90 dBm to –30 dBm Maximum input level: 0 dBm
Stream input (ASI)	Connector: BNC, 75Ω Transport stream rate: 50 Mbps maximum Data format: Accepts both Burst and Packet mode DVB-ASI format; 188/204 bytes
Stream output (ASI)	Connector: BNC, 75Ω Transport stream rate: Same as ASI input Mode: Packet Format: 188/204 bytes
10 MHz clock input	Connector: BNC, 50Ω Frequency: 10 MHz Level: -15 dBm to +15 dBm
Gigabit (LAN/IP interface)	Connector: 10/100/1000 Base-T; RJ-45 Use only good quality screened cable; Cat 6 Data rate: 100 Mbps maximum (2 streams) Packet type: IPv4 Mode: Half/full duplex Protocols: IEEE802.3, RTP/UDP/IP, IPv4, ARP
RS-232 port	Connector: Sub-D9 female Baud rate: 57600 bps Standard: RS-232 Other: No parity, 8 bits data, 1 bit stop
1 PPS In	This connector is not used. ⚠ ***CAUTION.*** *Do not connect a signal cable to the 1 PPS In connector.*

Network Installation

The typical RFM220 system will have the RFM220 Aggregator installed on a network server where it can communicate with RFM220 instruments on the network and be accessed by network PCs that have the RFM220 Client application installed.

In this case, the network server that runs the RFM220 Aggregator must have two network ports that are dedicated for RFM220 system communications:

- Control port. This port connects to the network to which the RFM220 instruments are connected. You will enter the IP address of the Control port in the "SNMPConfiguration" section of Configuration.xml file. (See page 22, *Configuring the RFM220 Aggregator*.)
- Corporate port. This port connects to the network to which the PCs running the RFM220 Client application are connected. You will enter the IP address of the Corporate port in the "ClientCommunication" section of Configuration.xml file. (See page 22, *Configuring the RFM220 Aggregator*.)

The RFM220 Aggregator software includes the RFM220 Device Setup utility that allows users to configure the network parameters of the RFM220 instrument. Since the RFM220 instrument does not support DHCP service, you must assign the instrument a specific IP address. (See page 18, *Configuring the Network Settings of a RFM220 Instrument*.)

NOTE. *If necessary, contact your local network administrator for help in entering the correct network parameters.*

If you lose or cannot remember the IP address of a RFM220 instrument, you can recover the IP address using an RS-232 command. (See page 77, *Recovering the IP Address*.)

Powering the Instrument On and Off

The RFM220 demodulator has a rear-panel power switch located next to the power cord connector. (See Figure 5 on page 9.)

To power on the instrument, connect the power cord to your local power source, and then use the rear-panel switch to power on the instrument. The front-panel Power On LED will light up.

To power off the instrument, use the rear-panel switch to power off the instrument and then remove the power cord from the power source.

Software Installation

The RFM220 software consists of two applications and one utility:

CAUTION. *For the best operating performance, Tektronix strongly recommends that you install the RFM220 Aggregator and the RFM220 Client applications on separate computers. The RFM220 Aggregator and RFM220 Client computers must be connected to the same Ethernet network as the RFM220 instruments that will be monitored.*

- RFM220 Aggregator. This application collects data from the RFM220 instrument and makes it available to the RFM220 Client application. The Aggregator can be configured to collect data from multiple RFM220 instruments at a time. The RFM220 Aggregator will typically be installed on a network server where it can be accessed by PCs running the RFM220 Client.
- RFM220 Client application. This application allows the user to display the data that the RFM220 Aggregator has collected from any of the RFM220 instruments that it is monitoring. The RFM220 Client will typically be installed on PCs connected to the same network as the server running the RFM220 Aggregator.
- RFM220 Device Setup. This utility allows the user to set the IP address parameters for a RFM220 instrument. This utility is installed as part of the RFM220 Aggregator software.

Computer Requirements

To communicate with the RFM220 instrument, you need to install the RFM220 software on a client PC or server. The following table lists the required platform requirements.

Table 5: RFM220 Aggregator platform requirements

Characteristic	Description
Processor	Minimum: Commonly available dual-core system; for example, Intel Core 2 Duo CPU @ 2.66 GHz or similar Preferred: Commonly available quad-core system; For example, Intel Xeon CPU E5420 @ 2.5 GHz or similar
Operating System	Minimum: Microsoft Windows XP Pro or Windows 7 Preferred: Windows 7 with 64 bits
Disk Space	Minimum: 120 MB free disk space
RAM	4 GB
Ethernet	Dual 1 Gigabit interfaces

Table 6: RFM220 Client platform requirements

Characteristic	Description
Processor	Minimum: Commonly available dual-core system: For example, Intel Pentium D CPU @ 3.2 GHz or similar
Operating System	Microsoft Windows XP Pro or Windows 7
Disk Space	120 MB free disk space
RAM	4 GB
Ethernet	1 Gigabit interface
Display	1024 x 768 pixel or higher resolution
Installed Software	Microsoft .NET Framework 3.5 with Service Pack 1

Windows 7 Requirements

Installation privileges. To install the RFM220 software on Windows 7 systems, you must log on to the computer with administrative privileges.

Microsoft .NET Framework 3.5 feature requirements. If the RFM220 software is installed on a computer running Windows 7, the RFM220 software will not operate properly (for example, trend graphs will not be displayed) unless the WCF HTTP and Non-HTTP Activation features in the Microsoft .NET Framework 3.5 software are enabled.

Before you install the RFM220 software on a Windows 7 computer, open the Windows Features dialog and verify that the Microsoft .NET Framework 3.5 features are checked as shown below.

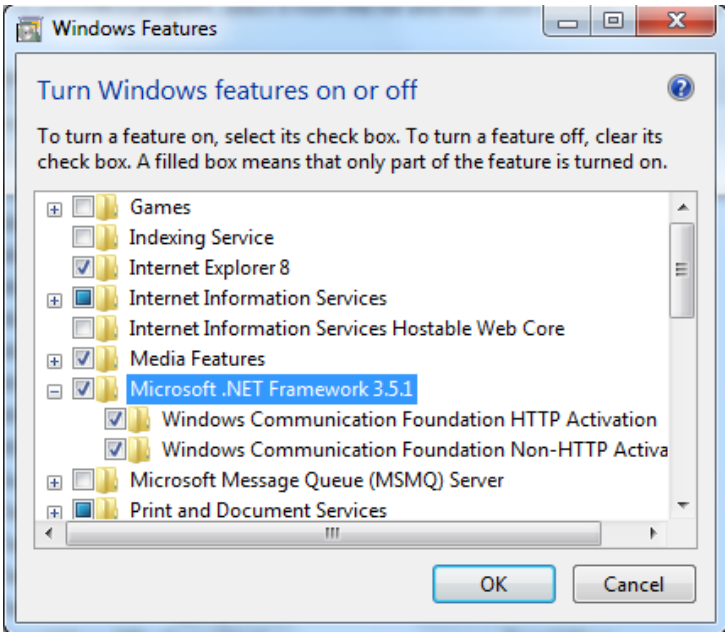


Figure 6: Enabling the WCF HTTP and Non-HTTP activation features

Installing the RFM220 Software

Perform the following procedure to install the RFM220 software on your client PC:

1. Insert the *RFM220 Software and Documentation CD* into the CD drive of your client PC.
2. When the CD browser opens, click the **Install Software** button. Windows Explorer opens the directory containing the software installation files on the CD.
3. Copy the software installation files to a location on the hard drive of your computer.
4. Start the software installation process as follows for the operating system on your PC or server:
   - Windows 7 systems. Right-click the **setup.exe** file and select **Properties**. If necessary, select **Full Access** and then close the Properties dialog. Right-click the **setup.exe** file again and select **Run as Administrator**.
   - Windows XP systems. Double-click the **setup.exe** file.
5. When the RFM220 InstallShield Wizard welcome screen opens, click **Next** to continue.

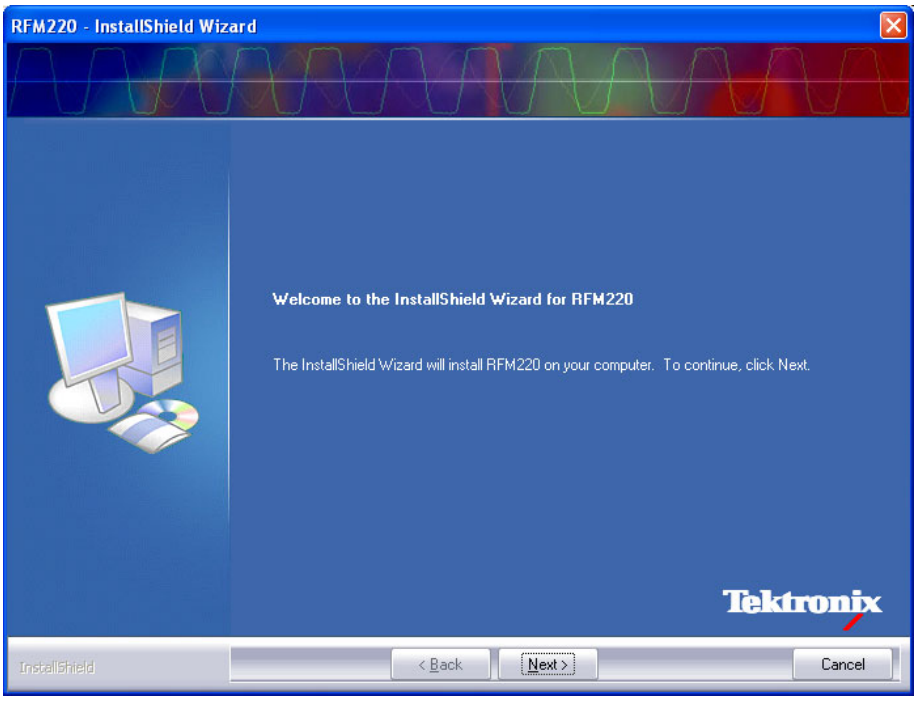


Figure 7: Initial RFM220 InstallShield display

6. The next screen displays the software license agreement. Click **Print** to print out a copy of the license agreement. After you read the license agreement, click **I accept the terms of the license agreement**, and then click **Next** to continue.

7. The next screen lets you select which applications to install. Select which application(s) you want to install, and then click **Next** to continue.

CAUTION. *For the best operating performance, Tektronix strongly recommends that you install the RFM220 Aggregator and the RFM220 Client applications on separate computers.*

- To install the RFM220 software on a PC or server that will be dedicated to running only the RFM220 Aggregator application, select only **RFM220 Aggregator**.
- To install the RFM220 software on a PC that will be used as a client to access the RFM220 Aggregator application located on another PC or server, select only **RFM220 Client**.
- To install both the RFM220 Aggregator and the RFM220 Client applications, select both **RFM220 Aggregator** and **RFM220 Client**.

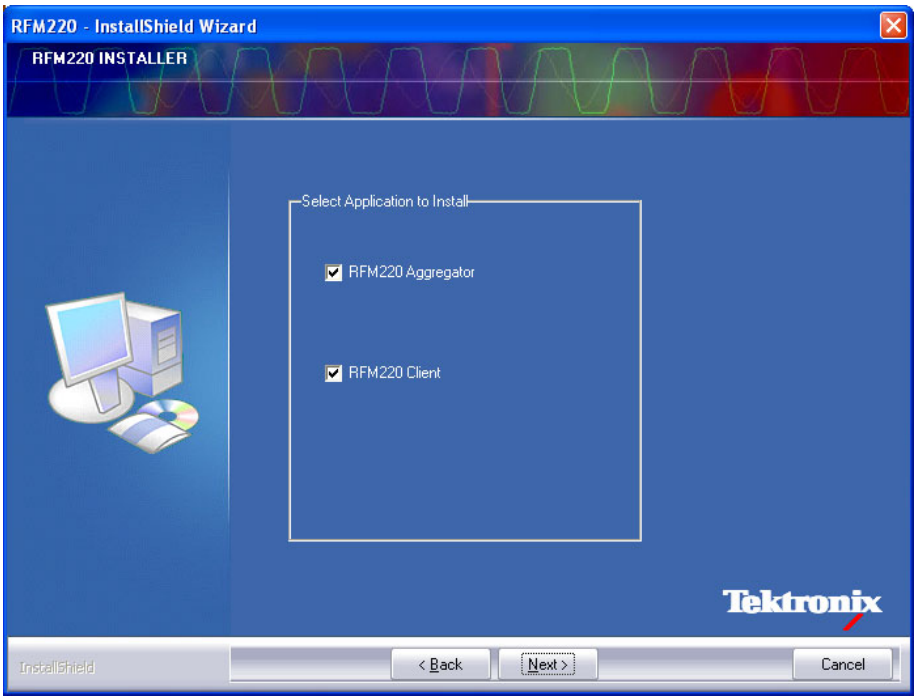


Figure 8: Selecting the applications to install

8. The next screen lets you select where to install the RFM220 software. If you want to install the software to a location other than the default location, click **Browse** and then navigate to your desired location. Click **Next** to continue. The default location of the software installation is here:
   - Windows 7 systems: C:\Program Files (x86)\Tektronix\RFM220
   - Windows XP systems: C:\Program Files\Tektronix\RFM220
9. The next screen gives you a chance to change your installation settings. Click **Back** to change your settings or click **Install** to proceed with the software installation.

10. As the software installs, a progress bar shows the progress of the installation.

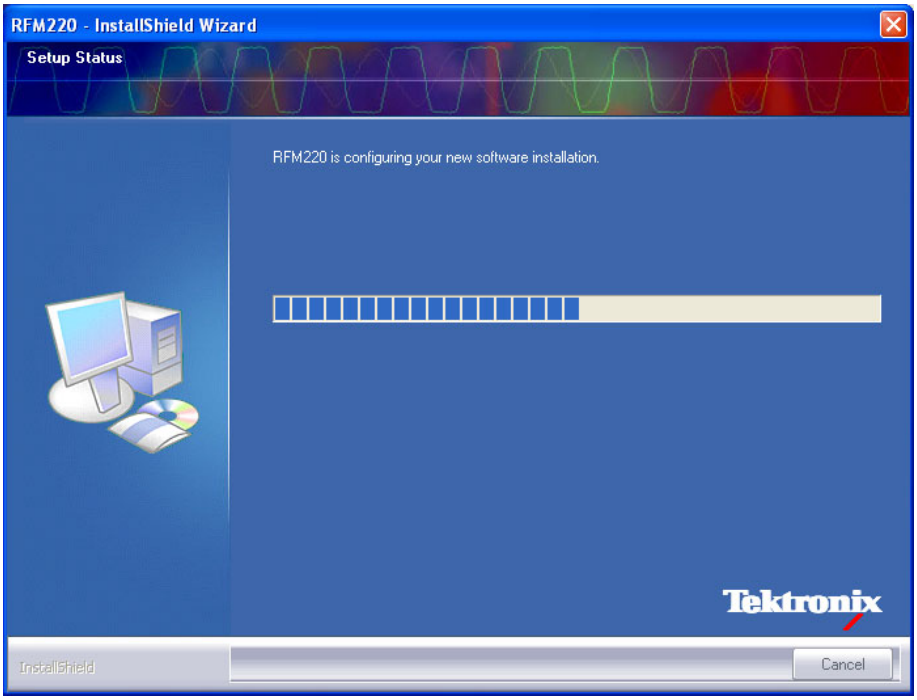


Figure 9: Installing the software

11. When the software installation is complete, click **Finish** to exit the InstallShield Wizard.

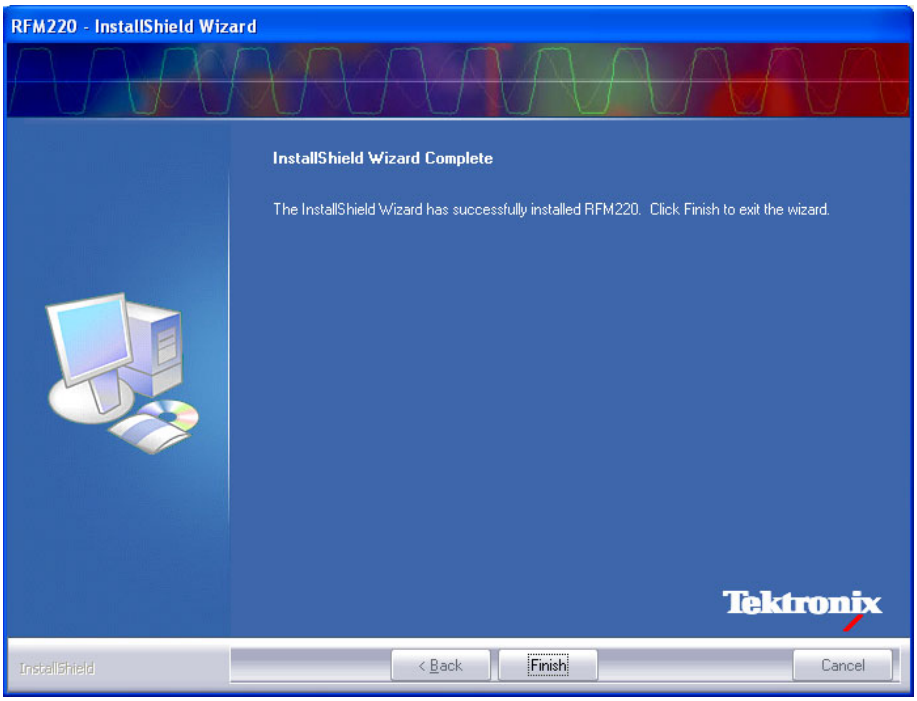


Figure 10: Final InstallShield screen

12. After the software is installed, shortcut icons will appear on your desktop for the RFM220 Aggregator and/or RFM220 Client applications you installed. The RFM220 Aggregator, RFM220 Client, and RFM220 Device Setup applications are also listed in the Start menu under All Programs > Tektronix.

    You can copy the RFM220 Device Setup shortcut from the Start menu to your desktop. The shortcut icons for all three RFM220 applications are shown below.

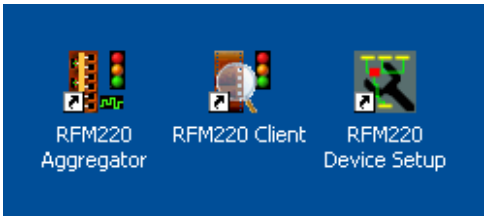


Figure 11: RFM220 shortcut icons

Configuration

Configuring the Network Settings of a RFM220 Instrument

In order for the Aggregator to monitor a RFM220 instrument, the instrument must be on the same network as the computer hosting the Aggregator. In order for the RFM220 Client to communicate with an Aggregator, the Aggregator and Client computers must be on the same network. The RFM220 instrument and the Client computers should also be connected to the same network subnet, if present.

The RFM220 Aggregator software includes the RFM220 Device Setup utility that allows you to configure the network parameters of a RFM220 instrument. Since the RFM220 instrument does not support DHCP service, you must assign the instrument a specific IP address.

NOTE. *If necessary, contact your local network administrator for help in entering the correct IP address parameters.*

If you lose or cannot remember the existing IP address of a RFM220 instrument, you can recover the IP address using an RS-232 command. *(See page 77, Recovering the IP Address.)*

First time operation. If the network settings of the RFM220 instrument have not been changed from the factory-default settings, perform the following steps to prepare the instrument for use on your local network:

NOTE. *This procedure is for first-time operation only. If you have already changed the network settings of the RFM220 instrument from the factory-default settings, perform the changing network settings procedure.* *(See page 49, Changing Network Settings.)*

For this procedure, you will need a PC or laptop that is not connected to your local network.

1. Install the RFM220 Aggregator software on a PC that is not connected to your local network.
2. Connect an Ethernet cable between the Gigabit port on the RFM220 instrument and the Ethernet port on the PC.
3. If necessary, power on the instrument.
4. Set the following network parameters on the PC:
   - IP address type: Static
   - IP address: 192.168.0.100
   - Subnet mask: 255.255.255.0
   - Gateway: Leave this field empty
5. Open a command prompt on the PC, and then ping the default IP address of the RFM220 instrument: 192.168.0.209. If the ping fails, check your network settings, your connections to the network, and then try to ping the instrument again.
6. If the instrument responded to the ping, then locate the RFM220 Device Setup utility that was installed on your PC:
   - Windows 7 systems:
     C:\Program Files (x86)\Tektronix\RFM220\RFM220 Aggregator\RFM220DeviceSetup.exe
   - Windows XP systems:
     C:\Program Files\Tektronix\RFM220\RFM220 Aggregator\RFM220DeviceSetup.exe

NOTE. *If you installed the RFM200 Aggregator software to a location other than the default location, your path to the RFM220 Device Setup utility will be different than the path shown above.*

7. Start the RFM220 Device Setup utility as follows for the operating system on your PC or server:
   - Windows 7 systems. Right-click the **RFM220DeviceSetup.exe** file and select **Run as Administrator**.
   - Windows XP systems. Double-click the **RFM220DeviceSetup.exe** file.
8. In the RFM220 Device Setup dialog, enter 192.168.0.209 in the Device IP Address box, and then click **Connect**.
9. After the RFM220 Device Setup utility connects to the instrument, the current network settings and device information fields are displayed.

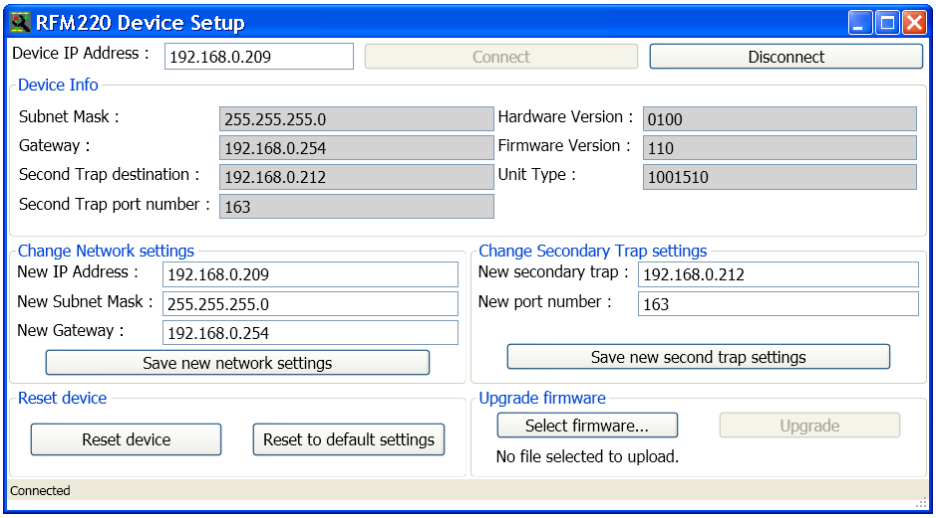


Figure 12: RFM220 Device Setup dialog showing initial connection

NOTE. *Always work with your local network administrator to properly set these values.*

Make a note of the network settings you assign the instrument for later reference.

10. In the Change Network Settings fields, enter the network settings that are appropriate for your network, and then click **Save new network settings**.

11. If you will be using an Network Management System (NMS) to monitor SNMP traps sent by the RFM220 system, perform the following steps. Otherwise, leave these fields blank and go to step 12.

    a. Enter the IP address of the PC or server hosting the NMS system in the New secondary trap box.

    b. Enter the port number that will receive SNMP traps on the PC or server hosting the NMS system in the New port number box.

    c. Click **Save new second trap settings**.

CAUTION. *If you enter a secondary trap destination, you need to ensure that the secondary trap port number is added to the Windows Firewall exceptions on the PC or server hosting the NMS system. This enables the NMS system to receive traps from the RFM220 system.*

If you click Save new second trap settings, you must enter a valid IP address and port number for the secondary trap destination. You will receive an error message if a valid IP address is not entered.

12. Remove power from the instrument, connect the instrument to your network, and then reapply power.

13. On a PC that is connected to the same network as the instrument and has the RFM220 Aggregator software installed, use the RFM220 Device Setup utility to connect to the instrument using the new IP address.

14. In the RFM220 Device Setup dialog:

    a. Click **Reset to default settings**.

    b. Click **Reset device**.

15. Close the RFM220 Device Setup dialog.

Configuring the RFM220 Aggregator

The RFM220 Aggregator is configured using the Configuration.xml file, which contains various user-defined parameters that control the communications between the three components of the RFM220 system: instrument, Aggregator, and Client. Consult with your local network administrator before setting these parameters.

Configuration change requirements. The Configuration.xml file can be updated dynamically. This means that after the file has been initially set up during the installation process, the file can be updated while the Aggregator is running. The Aggregator will automatically load the parameters from the updated Configuration.xml file when changes to the file are saved.

CAUTION. *The RFM220 software will not work properly if you have more than one RFM220 Aggregator monitoring an RFM220 instrument at a time. The Aggregator can communicate with multiple instruments at a time, but an individual instrument can only communicate with one Aggregator at a time.*

In the case where more than one Aggregator has connected to an RFM220 instrument, only the last Aggregator to connect to the instrument will receive SNMP trap messages from the instrument.

The RFM220 system requires the Configuration.xml file in order to operate. It is recommended that you backup this file to a safe location. A copy of the default file is located on the RFM220 Software and Documentation CD that was shipped with the product.

After a configuration change, the Aggregator requires approximately 2 minutes to reconfigure for each instrument listed in the Configuration.xml file. To prevent software problems, you should wait at least 2 minutes after saving a change for each instrument listed in the file before you make additional changes to the Configuration.xml file. For example, if 5 instruments are listed in the file, you should wait 10 minutes before making additional changes.

File structure. The Configuration.xml file contains four sections of communication parameters. The default file contains comment sections, which describe the various parameters. The following illustration shows the structure of the file with the comment sections removed.

- Client Communication contains the settings used by the RFM220 Aggregator for communications with connected RFM220 Clients.
- SNMP Configuration contains settings that are used by the RFM220 Aggregator to receive to alarm notifications (SNMP traps) from monitored RFM220 instruments.
- Diagnostic Log contains settings that control which event messages will be logged into the Aggregator.Log file. This file contains log messages at the Aggregator level and is intended to be used only as a diagnostic aid.

NOTE. *There is a separate DiagnosticLog setting in the Devices section of the file for limiting which event messages appear in the RFM220 Client display and in the log file for each monitored RFM220 instrument.*

- Devices contains the communication settings for each of the RFM220 instruments that will be monitored by the RFM220 Aggregator.

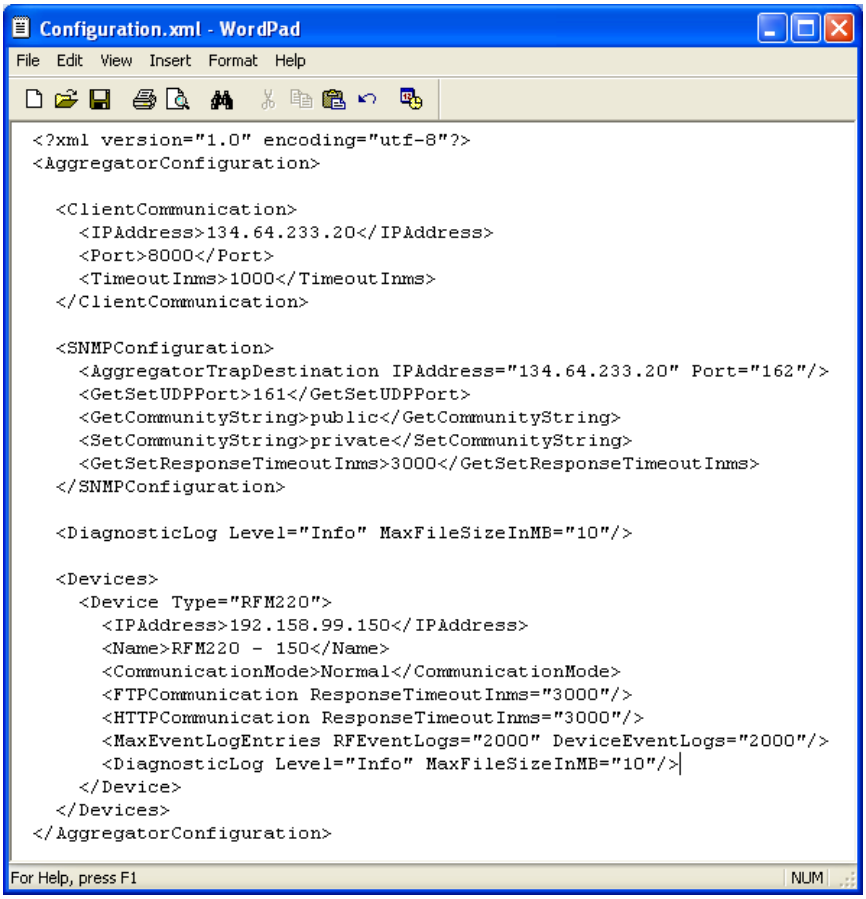


Figure 13: Structure of the Configuration.xml file

Procedure. Perform the following steps to edit the Configuration.xml file (See Figure 13 on page 23.):

CAUTION. *Read the requirements for making configuration changes before you edit the file. (See page 22, Configuration change requirements.)*

1. Before you edit the Configuration.xml file, use the RFM220 Device Setup utility to configure the network settings of the RFM220 instrument(s) that will be monitored by the RFM220 Aggregator. (See page 18, *Configuring the Network Settings of a RFM220 Instrument*.)
2. Use Wordpad, Notepad, or an XML editor to open the following file:
   - Windows 7:
     C:\Program Files (x86)\Tektronix\RFM220\RFM220 Aggregator\Configuration.xml
   - Windows XP systems:
     C:\Program Files\Tektronix\RFM220\RFM220 Aggregator\Configuration.xml

NOTE. *If you installed the RFM220 software to a location other than the default location, the path to your Configuration.xml file will be different.*

3. Edit the Client Communication parameters, which control the communications between the RFM220 Aggregator and connected RFM220 Clients.

```
<ClientCommunication>
  <IPAddress>134.64.233.20</IPAddress>
  <Port>8000</Port>
  <TimeoutInms>1000</TimeoutInms>
</ClientCommunication>
```

   a. Change the IPAddress parameter to match the IP address of the network interface on the PC or server to which all RFM220 Clients will connect. This PC or server should be running the RFM220 Aggregator and be connected to the same network as all of the PCs running the RFM220 Client.

CAUTION. *For the best operating performance, Tektronix strongly recommends that you install the RFM220 Aggregator and the RFM220 Client applications on separate computers. In the case where you need to run the Aggregator and Client applications on the same PC or server, you can enter "localhost" for this parameter instead of the IP address.*

However, entering localhost limits access to the RFM220 Aggregator to only the RFM220 Clients that are installed on that PC or server. It is recommended that you use the IP address instead of localhost since that will allow RFM220 Clients to access the RFM220 Aggregator from PCs other than the one hosting the Aggregator.

b. Change the Port parameter to match the port number on the PC or server running the RFM220 Aggregator that you will use to communicate with RFM220 Clients. You should change this value only if your PC or server is already using port 8000 for communication with other devices.

NOTE. *You will need to add this port number to the Windows firewall exceptions on the Aggregator PC or server to prevent communication problems between the Aggregator and any connected RFM220 Clients.* *(See page 31, Configuring the Windows Firewall.)*

The Aggregator will display the message "An attempt was made to access a socket in a way forbidden by its access permissions" if it detects communication conflicts with another device. In this case, change the value of this parameter to an unused port number.

c. Change the TimeoutInms parameter value as needed, based on the performance of your network. This is the amount of time in milliseconds after which communications with an RFM220 Client will time out and a communication error message will be displayed.

4. Edit the SNMP Configuration parameters, which are used by the RFM220 Aggregator to receive to alarm notifications (SNMP traps) from the RFM220 instruments. These settings are global in nature; they are applied to all RFM220 instruments that are monitored by the RFM220 Aggregator.

```
<SNMPConfiguration>
  <AggregatorTrapDestination IPAddress="134.64.233.20" Port="162"/>
  <GetSetUDPPort>161</GetSetUDPPort>
  <GetCommunityString>public</GetCommunityString>
  <SetCommunityString>private</SetCommunityString>
  <GetSetResponseTimeoutInms>3000</GetSetResponseTimeoutInms>
</SNMPConfiguration>
```

NOTE. *The RFM220 Aggregator supports two trap destinations. The first destination is always set by the RFM220 Aggregator to itself so that it can record all alarms. The second destination is set for any other listener, such as an NMS (Network Management System), that needs to monitor alarms raised by the RFM220 instruments.*

a. Change the AggregatorTrapDestination IPAddress parameter to match the IP address of the PC or server on which the RFM220 Aggregator is installed. This is the Control IP address.

CAUTION. *To prevent communication problems, do not use "localhost" as the Aggregator Trap Destination IP address. This address must be the IP address of the PC or server on which the RFM220 Aggregator is installed.*

b. Change the AggregatorTrapDestination Port parameter to match the port number on the Aggregator PC or server that will be used to receive SNMP traps from monitored RFM220 instruments. You should change this value only if your PC or server is already using port 162 for communication with other devices. The RFM220 Aggregator will display an error message if it detects communication conflicts with other devices.

NOTE. *You will need to add the Aggregator Trap Destination and Get/Set UDP port numbers to the Windows firewall exceptions on the Aggregator PC or server to prevent communication problems between the RFM220 Aggregator and any connected RFM220 Client.* *(See page 31, Configuring the Windows Firewall.)*

---

c. Change the GetSetUDPPort parameter to match the port number on the Aggregator PC or server that will be used for UDP communications with the RFM220 Clients. You should change this value only of your PC or server is already using port 161 for communication with other devices. The RFM220 Aggregator will display an error message if it detects communication conflicts with other devices.

d. Change the GetCommunityString and SetCommunityString parameter values as desired. These values should not need to be changed unless required by your network.

e. Change the GetSetResponseTimeoutInms parameter value as needed, based on the performance of your network. This is the amount of time in milliseconds after which Get and Set command communications with a monitored RFM220 instrument will time out and a communication error message will be displayed.

5. Edit the Diagnostic Log parameters that control which event messages will be logged into the Aggregator.Log file. This file contains log messages at the Aggregator level and is intended to be used as a diagnostic aid.

NOTE. *There is a separate DiagnosticLog setting in the Devices section of this file for limiting which event messages appear in the log files for a specific device.*

```
<DiagnosticLog Level="Info" MaxFileSizeInMB="10"/>
```

   a. Change the DiagnosticLog Level parameter value to control which events are logged into the Aggregator.Log file. The possible values for this parameter are listed below. When this parameter is set to a value other than Off, the selected message level and the levels that are above the selected level will be logged. For example, if Info is set as the logging level, all messages for Info and Error will be logged. If Verbose is set as the logging level, all messages for Error, Info, Debug, and Verbose will be logged. Entering the value Off turns off the logging function. Entering the value All enables logging of all messages.

      Off
      Error
      Info
      Debug
      Verbose
      All

   b. Change the DiagnosticLog MaxFileSizeInMB parameter value as needed to increase or decrease the maximum file size in megabytes for the Aggregator.Log file.

6. Edit the Devices parameters, which are used to govern the communications for each of the RFM220 instruments that will be monitored by the RFM220 Aggregator.

```
<Devices>
  <Device Type="RFM220">
    <IPAddress>192.158.99.156</IPAddress>
    <Name>Sample RFM - 156</Name>
    <CommunicationMode>Normal</CommunicationMode>
    <FTPCommunication ResponseTimeoutInms="3000"/>
    <HTTPCommunication ResponseTimeoutInms="3000"/>
    <MaxEventLogEntries RFEventLogs="10000" DeviceEventLogs="10000"/>
    <DiagnosticLog Level="Info" MaxFileSizeInMB="10"/>
  </Device>
</Devices>
```

   a. Do not change the Device Type parameter value from RFM220. This parameter is for future use.

   b. Change the IPAddress parameter to match the IP address of the RFM220 instrument that will be monitored by the RFM220 Aggregator.

CAUTION. *The RFM220 software will not work properly if you have more than one RFM220 Aggregator application monitoring an RFM220 instrument at a time. The Aggregator can communicate with multiple instruments at a time, but an individual instrument can communicate with only one Aggregator at a time.*

   c. Change the Name parameter to the device name, if any, that is associated with the RFM220 instrument that will be monitored by the RFM220 Aggregator. The name you enter here will appear in the Client Login dialog to help you select a particular RFM220 instrument when the Aggregator is monitoring multiple RFM220 instruments.

   d. Change the CommunicationMode parameter value from Normal to Secure if you want communications between the RFM220 Aggregator and the RFM220 instrument CRC'd and verified at both ends.

   e. Change the FTPCommunication ResponseTimeoutInms parameter value as needed, based on the performance of your network. This is the amount of time in milliseconds after which FTP communications with a monitored RFM220 instrument will time out and a communication error message will be displayed.

   f. Change the HTTPCommunication ResponseTimeoutInms parameter value as needed, based on the performance of your network. This is the amount of time in milliseconds after which HTTP communications with a monitored RFM220 instrument will time out and a communication error message will be displayed.

   g. Change the MaxEventLogEntries RFEventLogs parameter value as needed to increase or decrease the maximum number of entries in the RF Event log.

h. Change the MaxEventLogEntries DeviceEventLogs parameter value as needed to increase or decrease the maximum number of entries in the Device Event log.

i. Change the DiagnosticLog Level parameter value to control the amount of logging that occurs for the RFM220 instrument. The possible values for this parameter are listed below. When this parameter is set to a value other than Off, the selected message level and the levels that are above the selected level will be logged.

For example, if Info is set as the logging level, all messages for Info and Error will be logged. If Verbose is set as the logging level, all messages for Error, Info, Debug, and Verbose will be logged. Entering the value Off turns off the logging function. Entering the value All enables logging of all messages.

Off
Error
Info
Debug
Verbose
All

j. Change the DiagnosticLog MaxFileSizeInMB parameter value as needed to increase or decrease the maximum file size in megabytes of each event log.

7. If you want the RFM220 Aggregator to monitor more than one RFM220 instrument at a time, edit the Configuration.xml file as follows:

   a. Duplicate the Device Type parameters in the Devices section of the Configuration.xml for each RFM220 instrument you want to monitor. The following figure shows a Configuration.xml file with two Device sections, which allows the RFM220 Aggregator to monitor two instruments.

   b. For each Device Type section you duplicate, repeat step 5 to edit the Devices parameters for the additional RFM220 instrument.

```
<Devices>
  <Device Type="RFM220">
    <IPAddress>192.158.99.150</IPAddress>
    <Name>RFM220 - 150</Name>
    <CommunicationMode>Normal</CommunicationMode>
    <FTPCommunication ResponseTimeoutInms="3000"/>
    <HTTPCommunication ResponseTimeoutInms="3000"/>
    <MaxEventLogEntries RFEventLogs="2000" DeviceEventLogs="2000"/>
    <DiagnosticLog Level="Info" MaxFileSizeInMB="10"/>
  </Device>
  <Device Type="RFM220">
    <IPAddress>192.158.99.152</IPAddress>
    <Name>RFM220 - 152</Name>
    <CommunicationMode>Normal</CommunicationMode>
    <FTPCommunication ResponseTimeoutInms="3000"/>
    <HTTPCommunication ResponseTimeoutInms="3000"/>
    <MaxEventLogEntries RFEventLogs="2000" DeviceEventLogs="2000"/>
    <DiagnosticLog Level="Info" MaxFileSizeInMB="10"/>
  </Device>
</Devices>
```

Figure 14: Partial Configuration.xml file showing the file structure for monitoring two RFM220 instruments

Configuring the Windows Firewall

Network communications between the RFM220 system components (instrument, Aggregator, and Client) may be inhibited unless the RFM220 Aggregator application and the communication ports that you configured in the Configuration.xml file are set as exceptions in the Windows Firewall settings of the PC or server running the RFM220 software. Perform the following steps to set the Windows firewall exceptions:

1. Use the Start menu on your computer to open the Control Panel.
2. Double-click **Windows Firewall** to open the Windows Firewall dialog shown below.

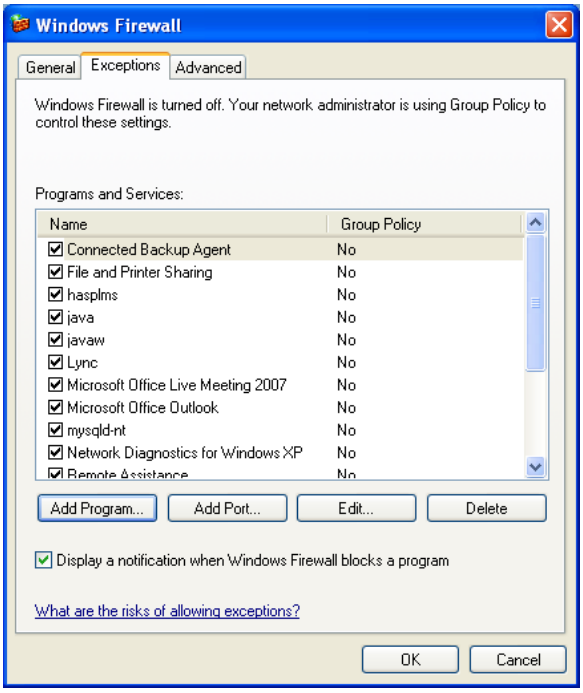


Figure 15: Windows Firewall dialog

3. Add the RFM220 Aggregator application to the firewall exceptions:

   a. In the Windows Firewall dialog, click **Add Program**.

   b. In the Add a Program dialog, select **RFM220 Aggregator** from the Programs list, and then click **OK** to close the Add a Program dialog.

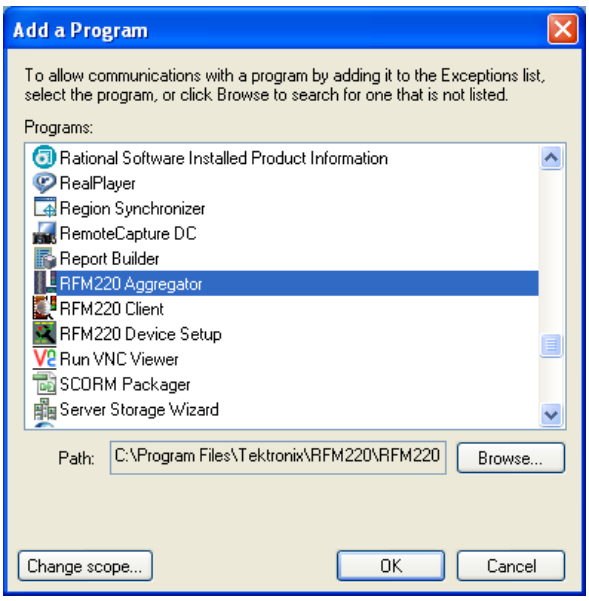


Figure 16: Adding the RFM220 Aggregator to the Windows firewall

4. Add the Client Communications port to the firewall exceptions:

   a. In the Windows Firewall dialog, click **Add Port**.

   b. In the Add a Port dialog, enter **RFM220 Aggregator** in the Name box.

   c. In the Port number box, enter the port number you entered in the Client Communication section of the Configuration.xml file. The default port number is 8000.

   d. Select **TCP**, and then click **OK** to close the Add a Port dialog.

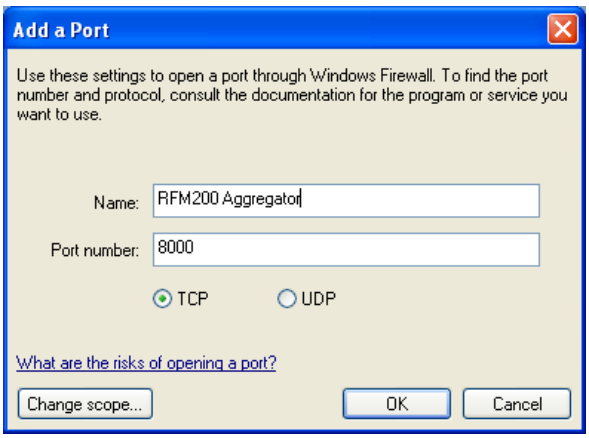


Figure 17: Adding the Client Communications port to the Windows firewall

5. Add the SNMP Configuration ports to the firewall exceptions:

   a. In the Windows Firewall dialog, click **Add Port**.

   b. In the Add a Port dialog, enter **RFM220 Aggregator** in the Name box.

   c. In the Port number box, enter the AggregatorTrapDestination Port number you entered in the SNMP Configuration section of the Configuration.xml file. The default port number is 162.

   d. Select **UDP**, and then click **OK** to close the Add a Port dialog.

   e. Repeat steps a through d for the GetSetUDP Port number you entered in the SNMP Configuration section of the Configuration.xml file. The default port number is 161.

   f. If you used the RFM220 Device Setup utility to configure a secondary SNMP trap address and port number to support an NMS system, repeat steps a through d using the network name of the PC or server hosting your NMS system and the port number you assigned to receive traps.

NOTE. *You will also need to add the secondary trap destination port number to the firewall exceptions on the computer hosting the NMS system.*

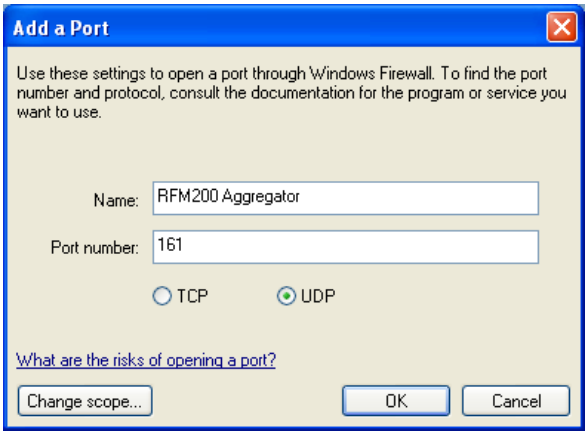


Figure 18: Adding the Client Communications port to the Windows firewall

6. In the Windows Firewall dialog, click **OK** to accept the changes and close the Windows Firewall dialog.

Starting the RFM220 Software

Starting the RFM220 software is a two step process. You must first start the RFM220 Aggregator application and then start the RFM220 Client application.

CAUTION. *The RFM220 instrument must be powered on and connected to the same network as the PC/server on which the RFM220 Aggregator and Client applications are installed.*

Windows 7 Privileges

Before you start the RFM220 software on a Window 7 system, ensure the following:

- The user who is logged onto the computer has Full Access privileges for the RFM220 applications.
- Start the RFM220 applications using the "Run as administrator" command.

Setting Full Access privileges. Perform the following steps to set access privileges for the RFM220 software on a Windows 7 system:

1. Right click the RFM220 Aggregator or RFM220 Client icon on your desktop and select **Properties**.
2. Select the **Security** tab in the Properites dialog.
3. Select **SYSTEM** in the list of groups and user names, and then set the full access permissions. (See Figure 19.)
4. Select **Administrators** in the list of groups and user names, and then set the full access permissions.
5. Select **Users** in the list of groups and user names, and then set the full access permissions.
6. Click **OK** to save the changes and close the Properties dialog.

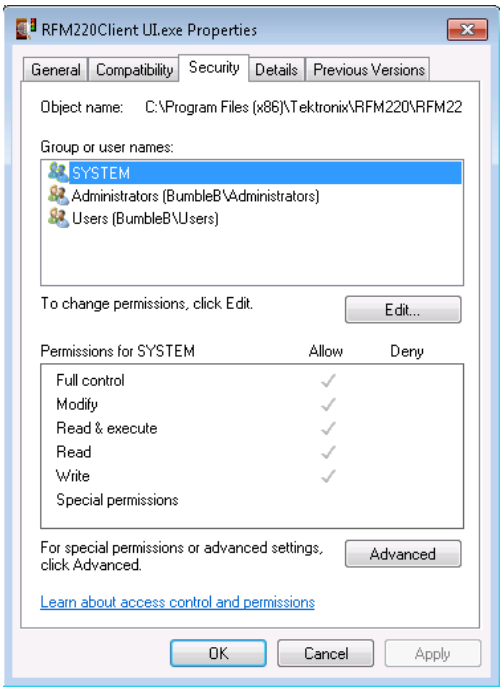


Figure 19: Setting full access privileges

Starting the RFM220 Aggregator

Perform the following steps to start the RFM220 Aggregator application:

1. Before you start the Aggregator application, perform the following tasks on the PC or server where you installed the RFM220 Aggregator application:
   a. Use the RFM220 Device Setup utility to configure the network settings of the RFM220 instrument(s) that the Aggregator will monitor. (See page 18, *Configuring the Network Settings of a RFM220 Instrument*.)
   b. Configure the Configuration.xml file as necessary for your installation. (See page 22, *Configuring the RFM220 Aggregator*.)
   c. Configure the Window Firewall to support network communications. (See page 31, *Configuring the Windows Firewall*.)
2. Start the RFM220 Aggregator as follows for the operating system on your PC or server:
   - Windows 7 systems. Right-click the **RFM220 Aggregator** icon on your desktop and select **Run as Administrator**.
   - Windows XP systems. Double-click the **RFM220 Aggregator** icon on your desktop.

3. The RFM220 Aggregator window displays messages as the application initializes. When the initialization is complete, you will see the message "Aggregator is ready." (See Figure 20.)

CAUTION. *To prevent communication problems with the RFM220 system, wait until you see the message "Aggregator is ready" in the Aggregator window before you use the RFM220 Client to connect to the Aggregator.*

During the initialization process, the Aggregator sets trap destinations, disables some alarms, and establishes communications with each RFM220 instrument that the Aggregator is configured to monitor. The initialization process must complete before monitoring data is valid.

The Aggregator initialization process takes approximately 70 seconds for each RFM220 instrument that the Aggregator will monitor. For example, if the Aggregator is configured to monitor 10 instruments, it will take approximately 11-12 minutes for the initialization process to complete.

The Aggregator continously monitors the Configuration.xml file. Whenever the file is edited and saved, any changes that were made to the file will immediately change the Aggregator configuration.

After a configuration change, the Aggregator requires approximately 2 minutes to reconfigure for each instrument listed in the Configuration.xml file. To prevent software problems, you should wait at least 2 minutes after saving a change for each instrument listed in the file before you make additional changes to the Configuration.xml file. For example, if 5 instruments are listed in the file, you should wait 10 minutes before making additional changes.

The Aggregator will display the message "An attempt was made to access a socket in a way forbidden by its access permissions" if it detects conflicts with another device on a communication port. In this case, you will need to edit the Configuration.xml file to change the configured port to an unused port number.

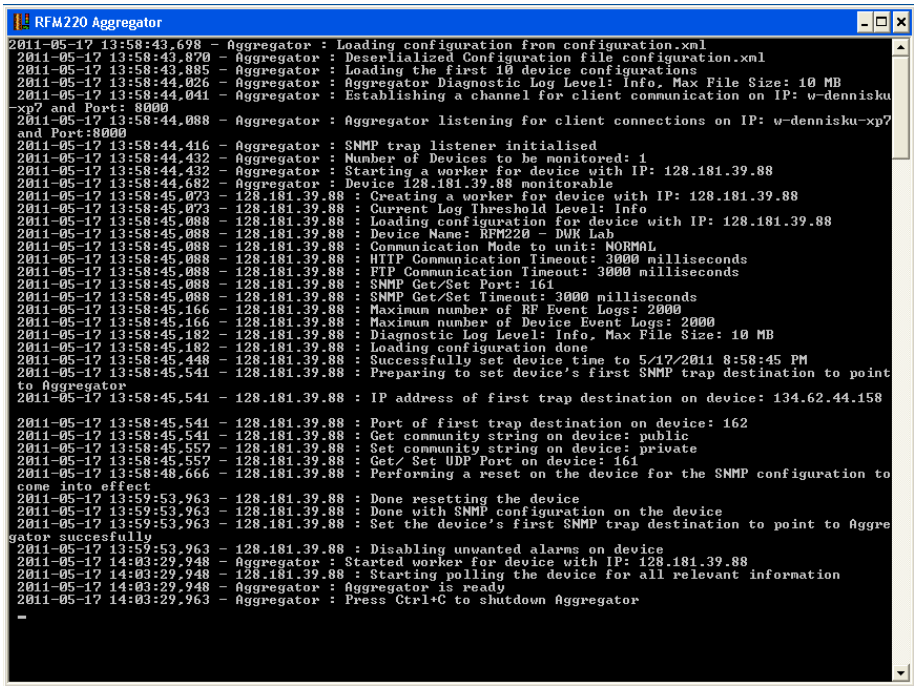


Figure 20: RFM220 Aggregator window

4. After the Aggregator initialization completes, you can deselect and minimize the RFM220 Aggregator window to ensure that the Aggregator application is not accidently closed.

⚠ ***CAUTION.*** *When you close the RFM220 Aggregator window, the Aggregator will no longer be able to collect data from the monitored RFM220 instrument(s) and all existing trend data will be lost.*

When the RFM220 Aggregator window is selected on the PC or server desktop, pressing Ctrl-C will close the RFM220 Aggregator application. To ensure that no trend data is lost, deselect or minimize the RFM220 Aggregator window after the application initializes.

5. Leave the PC or server on and the RFM220 Aggregator application running for as long as you want the Aggregator to collect data from the RFM220 instruments it is monitoring.

Starting the RFM220 Client

The RFM220 Aggregator must already be running before a RFM220 Client can connect to the Aggregator. Perform the following steps to start the RFM220 Client application:

1. On the PC where you installed the application, start the RFM220 Client as follows for the operating system on your PC or server:
   - Windows 7 systems. Right-click the **RFM220 Client** icon on your desktop and select **Run as Administrator**.
   - Windows XP systems. Double-click the **RFM220 Client** icon on your desktop.

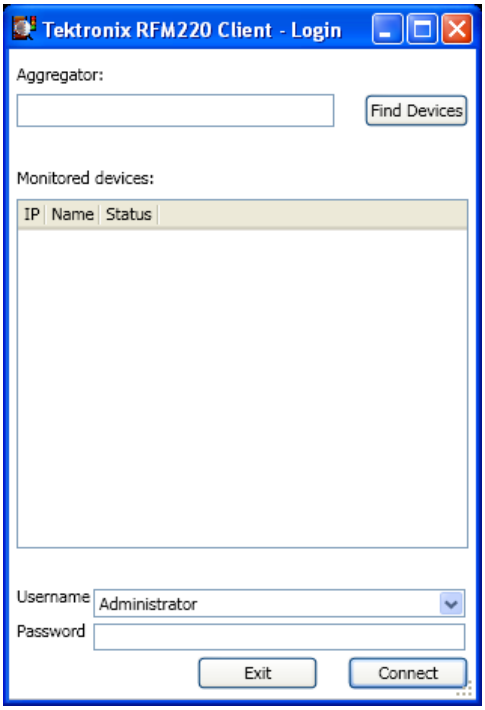


Figure 21: Initial RFM220 Client login window

2. In the RFM220 Client Login window, enter the IP address or device name of the PC or server hosting the RFM220 Aggregator.

NOTE. *For first-time operation, the Aggregator box is blank. In future logins, the last IP address or device name that you used to connect to a RFM220 Aggregator will be displayed.*

If the Configuration.xml file has been updated since the last time you logged on to the instrument to change the port number used by the Aggregator for Client communications, you will need to add the new port number to the Aggregator IP address. For example, if the IP address of the Aggregator is 128.94.1.36 and the new port number is 8001, then enter 128.94.1.36:8001 in the Aggregator box.

CAUTION. *When you use the RFM220 Client to connect to a RFM220 instrument, the software does a version check to verify that the firmware version installed in the instrument and the software versions of the RFM220 Aggregator and RFM220 Client are all compatible.*

If they are not compatible, an error message will be displayed and you will not be able to connect to the RFM220 instrument until the software or instrument firmware is upgraded to a compatible version.

3. After you enter the IP address or device name in the Aggregator box, click **Find Devices**. The IP addresses, device names, and status for all of the RFM220 instruments being monitored by the selected Aggregator will be displayed in the Monitored Devices list.

NOTE. *If a RFM220 instrument is added to the Aggregator after you click Find Devices, you must click Find Devices again to see the additional instrument in the monitored devices list.*

The following illustration shows a device name being used to connect to a RFM220 Aggregator, which is monitoring two RFM220 instruments.

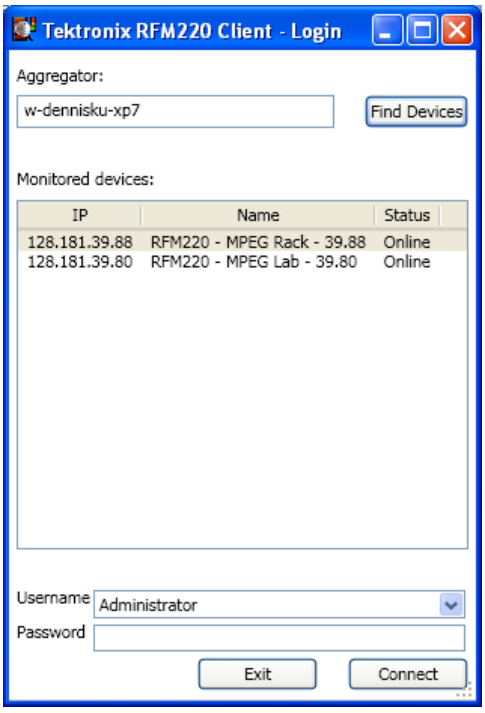


Figure 22: RFM220 Client login window showing two monitored devices

4. Select the RFM220 instrument from the Monitored Devices list to which you want to connect. The selected device will be highlighted.

NOTE. *The monitored devices list includes a status column, which lists the status of the monitored device: Online or Offline. Offline devices are currently unavailable to the RFM220 Aggregator. (See page 55, Online and offline monitoring.)*

5. Select a user name from the drop-down list: Administrator or User.

NOTE. *Two user types are provided: Administrator and User. The Administrator has full operating privileges. The User can view all data but cannot change alarm parameters or perform other administrative tasks. (See page 5, User Profiles and Roles.)*

6. Enter the appropriate password. The default password is **tek** for the Administrator user type. There is no default password for the User.

7. Click the **Connect** button. For first-time operation, the RFM220 Client appears as shown below with no log entries and the LED indicators in the Metrics pane grayed out. This indicates the default state of all tests being disabled.

   The RFM220 Client will show log events and metrics data after tests are enabled and alarms are configured. (See page 60, *Alarm Configuration*.)

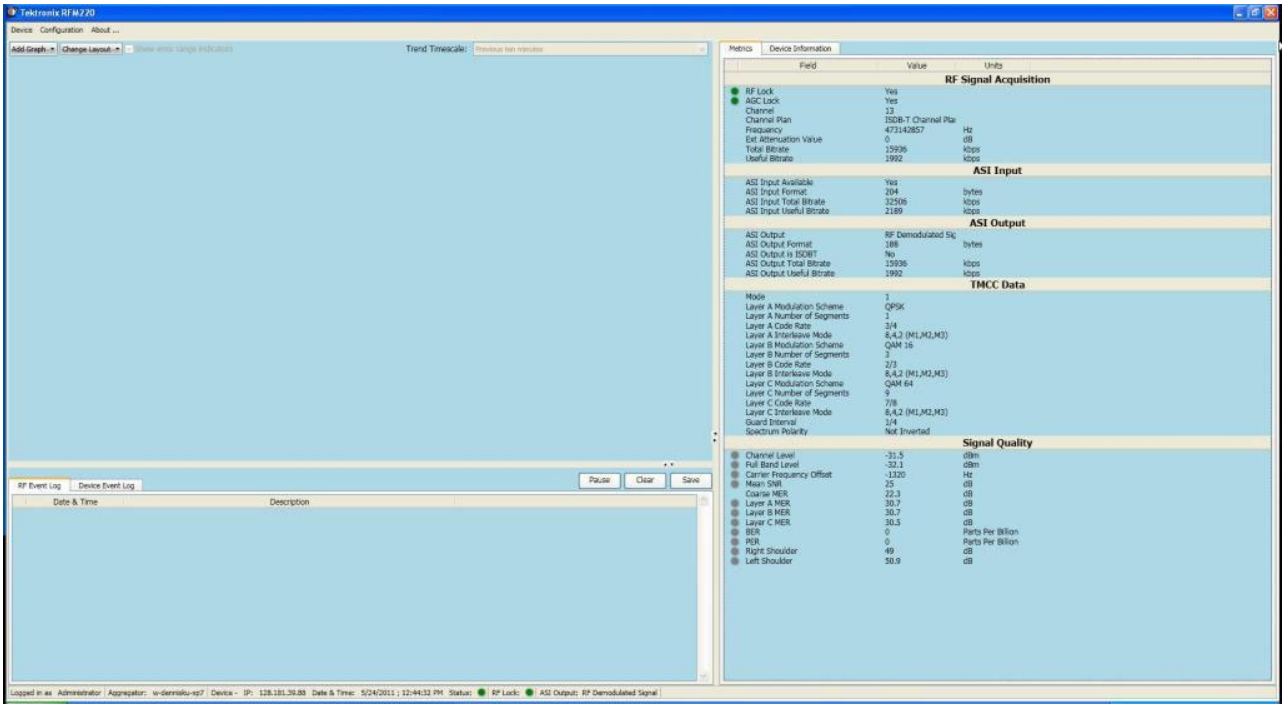


Figure 23: Initial RFM220 Client application window

Operating Basics

This section provides the basic operating information for each component of the RFM220 system:

- RFM220 instrument
- RFM220 Aggregator application
- RFM220 Client application
- RFM220 Device Setup utility

RFM220 Instrument

Installation Considerations

Network installation. If you are operating the RFM220 system on a local Ethernet network, the RFM220 instrument(s) to be monitored must be connected to the same network as the PC or server hosting the RFM220 Aggregator application.

Non-network installation. If you are operating the RFM220 system without an Ethernet network, you must directly connect the Ethernet port on the RFM220 instrument to the Ethernet port on the PC or server hosting the RFM220 Aggregator and Client applications.

(See page 8, *Hardware Installation*.)

Network Settings

The RFM220 instrument is shipped with a default IP address (192.168.0.209). Use the RFM220 Device Setup utility to change the network settings of a RFM220 instrument so that it can operate on your network.

(See page 18, *Configuring the Network Settings of a RFM220 Instrument*.) (See page 47, *RFM220 Device Setup*.)

If you lose or cannot remember the IP address of a RFM220 instrument, you can recover the IP address using an RS-232 command. (See page 77, *Recovering the IP Address*.)

Front Panel

The front panel has three LED indicators.

Figure 24: Front panel LED indicators

Alarm Status. This red LED has three states:

- Off. Indicates there is no critical error.
- Blinking. Indicates an input failure (no signal).
- On. Indicates one of the following errors has occurred: temperature, internal failure, hardware failure, or software failure.

Ready Status. This green LED has three states:

- Off. Indicates there is no input signal (AGC KO).
- Blinking. Indicates that the input signal is OK, but that no measurements are possible (AGC KO, Carrier KO, or MPEG KO).
- On. Indicates that the input signal is OK, the measurements are OK, and the output stream is available.

Power On. This green LED has two states:

- On. Indicates that the instrument is powered on.
- Off. Indicates that the instrument is powered off.

Rear Panel

Power switch. The power switch is located on the left side of the instrument rear panel. The power cord must be connected to a power source and this switch turned on before the instrument will operate. The front-panel Power On LED turns on to indicate when power is applied to the instrument.

Signal connectors. All of the signal connectors are located on the rear panel. (See page 9, *Connecting Signals to the Instrument*.)

CAUTION. *To prevent operating problems, do not connect a signal cable to the 1 PPS In connector.*

Figure 25: RFM220 rear panel

RFM220 Aggregator

The RFM220 Aggregator application collects data from monitored RFM220 instruments and makes it available to be viewed by connected RFM220 Client applications. The RFM220 Aggregator can be configured to monitor up to 10 RFM220 instruments. (See page 18, *Configuration*.)

Installation Considerations

The typical RFM220 system installation will have the RFM220 Aggregator installed on a network server, where it can be accessed by network PCs with the RFM220 Client application installed. In this case, the network server that runs the RFM220 Aggregator must have two network ports that are dedicated for RFM220 system communications:

- Control port. This port connects to the "Control" network of the RFM220 instruments, which is the network to which the RFM220 instruments are connected.
- Corporate port. This port connects to the "Corporate" (public) network where users can use the RFM220 Client application to access the RFM220 Aggregator.

With this installation scenario, you need to edit the "ClientCommunication" section of the Configuration.xml file to enter the "Corporate" IP address of the server running the RFM220 Aggregator, and also edit the "SNMPConfiguration" section of file to enter the "Control" IP address of the server.

If you do not have a local network, the RFM220 Aggregator and Client applications must be installed on the same PC or server, and the Ethernet port on the RFM220 instrument must be directly connected to the Ethernet port on the PC or server hosting the RFM220 applications.

Operating Considerations

For the RFM220 system to operate properly, you need to observe the following operating conditions for the RFM220 Aggregator:

CAUTION. *The RFM220 system will not operate as designed unless the following operating requirements for the RFM220 Aggregator are observed.*

- For best system performance, install the RFM220 Aggregator and Client applications on separate computers. The computers must meet the minimum requirements. (See page 13, *Computer Requirements*.)

  Although the RFM220 Aggregator can monitor up to 10 instruments and can have multiple RFM220 Clients connected at the same time, system performance diminishes as more instruments are monitored and as more RFM220 Clients connect to the Aggregator and display graphs.

- For best system performance, the logging level should be set at Info in the Configuration.xml file unless there is a specific signal problem or RFM220 system problem you are investigating.

- Only one Aggregator should monitor an RFM220 instrument at a time. The Aggregator can communicate with up to 10 instruments at a time, but an individual instrument can communicate with only one Aggregator at a time.

NOTE. *In the case where more than one Aggregator has connected to an RFM220 instrument, only the last Aggregator to connect to the instrument will receive SNMP trap messages from the instrument.*

- The Aggregator requires access to the Configuration.xml file in order to operate. This file sets the parameters that control the communications between the different components of the RFM220 system. You must configure this file before you can operate the RFM220 system. (See page 22, *Configuring the RFM220 Aggregator*.)

  If the Configuration.xml file is lost or deleted, the Aggregator will not be able to start or operate. The default location of the Configuration.xml is as follows. The location will be different if you installed the Aggregator software to a location other than the default location.

  - Windows 7:
    C:\Program Files (x86)\Tektronix\RFM220\RFM220 Aggregator\Configuration.xml
  - Windows XP systems:
    C:\Program Files\Tektronix\RFM220\RFM220 Aggregator\Configuration.xml

  A replacement copy of the default file is located on the *RFM220 Software and Documentation CD* that was shipped with the product. It is recommended that you save a backup copy of the Configuration.xml file after you configure your system.

- On Windows 7 systems, the user who has logged on as the Administrator must have Full Access privileges.

- The RFM220 Aggregator must be started and fully initialized before a RFM220 Client can connect and view valid data from a monitored RFM220 instrument.

  The Aggregator initialization process takes approximately 70 seconds for each instrument that the Aggregator will monitor. For example, if the Aggregator is configured to monitor 10 instruments, it will take approximately 11-12 minutes for the initialization process to complete. When the Aggregator is fully initialized, the message "Aggregator is ready" is displayed, as shown near the bottom of the following illustration.

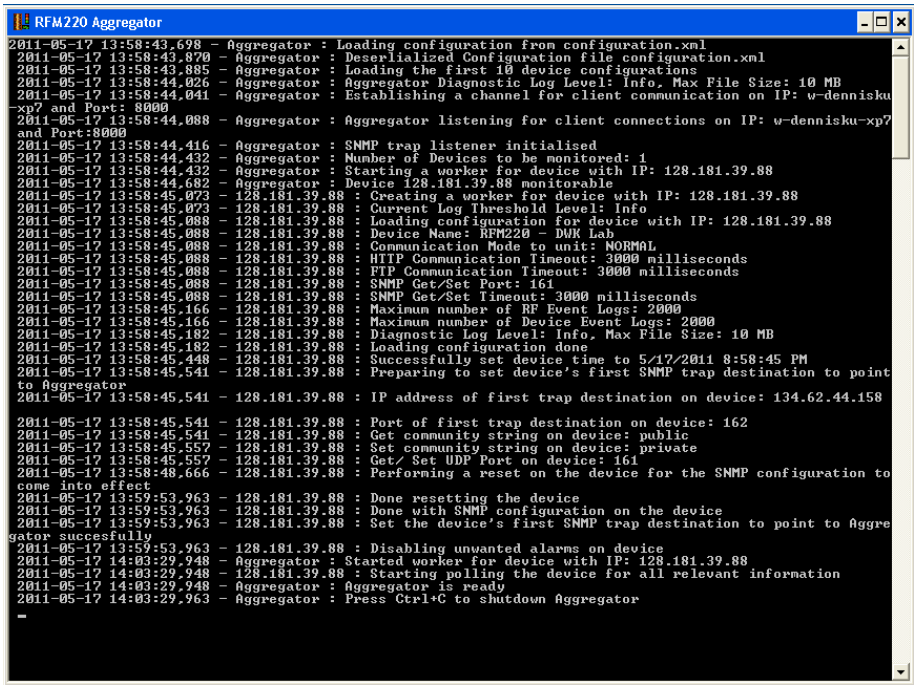


Figure 26: RFM220 Aggregator application window

- Once the Aggregator is started, the application should be left running for as long as you want to collect data from the RFM220 instruments.

  The Aggregator collects and stores trend data from the instruments that it is monitoring. As long as the Aggregator stays running, the trend data remains available for all of the instruments that the Aggregator has monitored since it was started. However, all trend data will be lost when the Aggregator application is closed or shut down. Press Enter or Ctrl-C to close the RFM220 Aggregator.

- The Aggregator will display the message "An attempt was made to access a socket in a way forbidden by its access permissions" if it detects conflicts with another device on a communication port. In this case, you will need to edit the Configuration.xml file to change the configured port to an unused port number. (See page 86, *Communication port conflicts*.)

- The RFM220 Aggregator maintains all of the log and settings files in the following directories on the PC or server where the Aggregator is installed:
  - Windows 7:
    C:\Users\<user ID>\AppData\Local\Tektronix\RFM220\RFM220 Aggregator\Logs

    C:\Users\<user ID>\AppData\Local\Tektronix\RFM220\RFM220 Aggregator\Settings
  - Windows XP systems:
    C:\Documents and Settings\<user ID>\Local Settings\Application Data\Tektronix\RFM220\RFM220 Aggregator\Logs

    C:\Documents and Settings\<user ID>\Local Settings\Application Data\Tektronix\RFM220\RFM220 Aggregator\Settings

  Since the trend data and log entries are lost when the Aggregator is shut down, it is recommended that the RFM220 system administrator backup the log and settings files before the Aggregator is stopped. The administrator should also ensure that no log files are present in the Logs folder when the Aggregator is restarted. (See page 70, *Event Logs*.)
- When you use the RFM220 Client to configure the alarm settings, you should leave enough range between the Active and Clear thresholds to account for minor signal fluctuations. To prevent an SNMP alarm storm from overloading the Aggregator, If the error band is too narrow and the signal has a lot of fluctuations, a large number of SNMP traps will be generated and can overload the Aggregator.

RFM220 Device Setup

The RFM220 Device Setup utility dialog shown below is used by the RFM220 system administrator to perform the following tasks:

- Configuring the network settings of RFM220 instruments so they can operate on the local network
- Configuring a secondary trap destination for use with an NMS system
- Resetting a RFM220 instrument or resetting the instrument back to the default settings
- Upgrading the instrument firmware
- Viewing the hardware and firmware versions of the RFM220 instrument

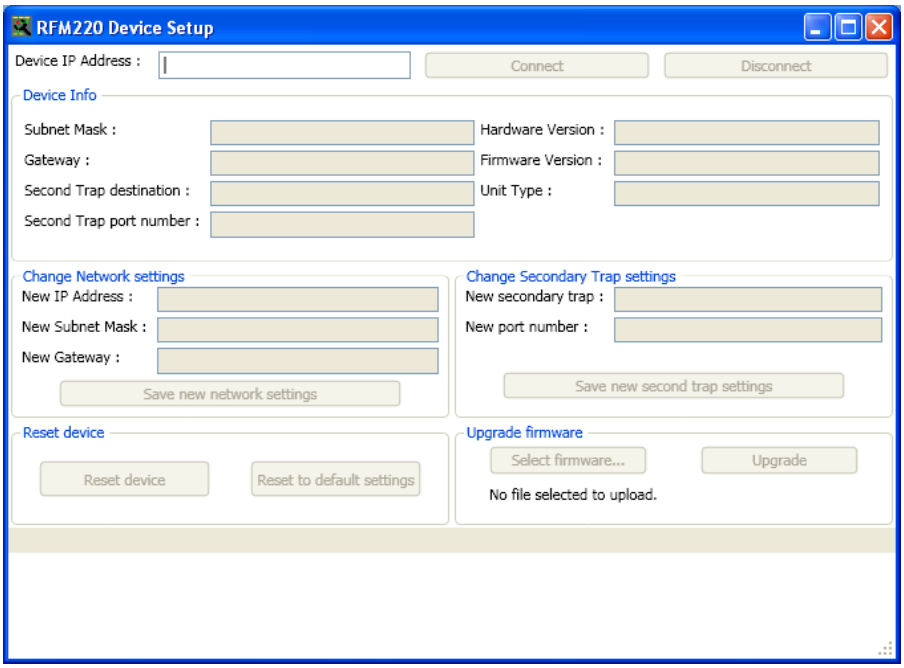


Figure 27: RFM220 Device Setup dialog

Performing RFM220 System Maintenance

The procedure for using the Device Setup utility to setup the RFM220 system is described in the *Software Installation* section of this manual. (See page 18, *Configuring the Network Settings of a RFM220 Instrument*.)

If you need to perform maintenance on a RFM220 instrument, such as changing the IP address, resetting the device, or upgrade the firmware, perform the following steps:

CAUTION. *To prevent false errors from being reported in the event logs, perform the following steps during system maintenance. If an instrument being monitored by a RFM220 Client is taken offline, the LED indicator for RF Lock in the Status bar will blink red and the Metrics pane will be grayed to indicate that the data is no longer valid.*

All trend data and log entries for the RFM220 instrument is lost when the instrument is removed from the Configuration.xml file. You should back up the following files before you perform instrument maintenance:

Windows 7 systems:
C:\Users\<user ID>\AppData\Local\Tektronix\RFM220\RFM220 Aggregator

Windows XP systems:
C:\Documents and Settings\<user ID>\Local Settings\Application Data\Tektronix\RFM220\RFM220 Aggregator

1. Notify users that they need to disconnect their RFM220 Client from the RFM220 instrument that will be removed from the system.
2. Delete the RFM220 instrument from the Configuration.xml file.
3. Use the Device Setup utility to perform maintenance on the instrument as required. After you perform the maintenance, be sure reset the instrument to the default settings and then reset the instrument.
4. Add the RFM220 instrument back into the Configuration.xml file.
5. Use the RFM220 Client to set the alarm configuration parameters for the instrument.
6. Use the RFM220 Client to select the correct channel plan and channel number, retune the channel input frequency, compensate for an external attenuation if one exists, and set the left and right shoulder distances.
7. Notify users that the instrument has been returned to the RFM220 system.

Changing Network Settings

This procedure assumes that you have already installed the RFM220 instrument on your network and have powered the instrument on. For first-time operation, perform the first-time operation procedure. (See page 19, *First time operation*.)

Perform the following steps to configure the network settings of a RFM220 instrument. You should always work with your network administrator to correctly set these values.

CAUTION. *If you change the network settings of a RFM220 instrument, you must reset the instrument before you use the Aggregator to start monitoring the instrument.*

1. On the PC or server where the RFM220 Aggregator is installed, locate the RFM220 Device Setup utility that was installed in the following directory:
   - Windows 7 systems:
     C:\Program Files (x86)\Tektronix\RFM220\RFM220 Aggregator\RFM220DeviceSetup.exe
   - Windows XP systems:
     C:\Program Files\Tektronix\RFM220\RFM220 Aggregator\RFM220DeviceSetup.exe

NOTE. *If you installed the RFM200 Aggregator software to a location other than the default location, your path to the RFM220 Device Setup utility will be different than the path shown above.*

2. Start the RFM220 Device Setup utility as follows for the operating system on your PC or server:
   - Windows 7 systems. Right-click the **RFM220DeviceSetup.exe** file and select **Run as Administrator**.
   - Windows XP systems. Double-click the **RFM220DeviceSetup.exe** file.
3. In the RFM220 Device Setup dialog, enter the current IP address of the RFM220 instrument in the Device IP Address box, and then click **Connect**.

   If you cannot locate the IP address of the instrument, you can recover the address using an RS-232 command. (See page 77, *Recovering the IP Address*.)

4. After the RFM220 Device Setup utility connects to the RFM220 instrument, the current network settings and device information fields are displayed.

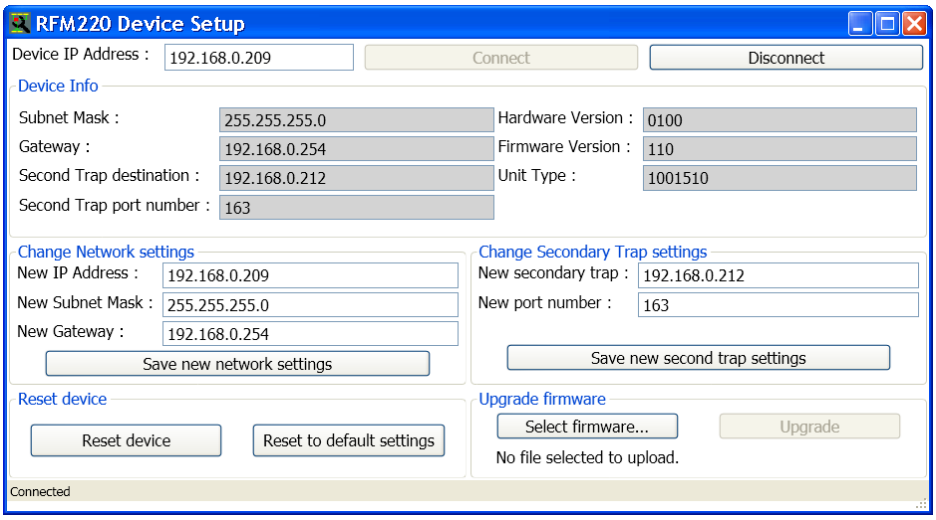


Figure 28: RFM220 Device Setup dialog

5. Enter any desired changes for the network settings and then click **Save new network settings**.

⚠ ***CAUTION.*** *If you change the IP address of a RFM220 instrument, you must reset the instrument as described in the following steps before you use the Aggregator to start monitoring the instrument.*

After changing the network settings, the RFM220 Device Setup utility will not be able to access the instrument for a while if the instrument is on different subnet than the computer hosting the RFM220 Device Setup utility.

If you enter a secondary trap destination, you need to ensure that the secondary trap port number is added to the Windows Firewall exceptions on the PC or server hosting the NMS system. This enables the NMS system to receive traps from the RFM220 system.

If you click Save new second trap settings, you must enter a valid IP address and port number for the secondary trap destination. You will receive an error message if a valid IP address is not entered.

---

6. If you want an NMS system to also monitor the SNMP traps sent by the RFM220 system, enter the secondary trap and associated port number in the appropriate boxes and then click **Save new second trap settings**. If you are not using an NMS system, leave the secondary trap fields blank.
7. Click **Reset to default settings** to reset the RFM220 instrument back to the default settings.
8. Click **Reset device** to reset the RFM220 instrument.

9. Click **Disconnect** to disconnect the RFM220 Device Setup utility from the RFM220 instrument.
10. If you are configuring multiple RFM220 instruments, repeat steps 3 to 9for each instrument.
11. Close the RFM220 Device Setup utility dialog.

Resetting Instruments and Instrument Settings

The Device Setup utility provides the following selections for resetting RFM220 instruments:

- Reset device. Use this selection to reset the RFM220 instrument to which you are connected. Measurement settings are not affected.

NOTE. *You need to reset the instrument if you change the network settings of a monitored instrument.*

- Reset to default settings. Use this selection to reset the various instrument settings back to their default values.

Upgrading Instrument Firmware

Tektronix occasionally releases product firmware and software updates to introduce new features or to fix product problems. If a instrument firmware update is available, perform these steps:

CAUTION. *Before upgrading the instrument firmware, following the steps for performing RFM220 system maintenance. (See page 48, Performing RFM220 System Maintenance.)*

1. Download the upgrade firmware to the PC or server hosting the Aggregator.
2. Remove the instrument from the Configuration.xml file.
3. Use the Device Setup utility to connect to the instrument.
4. Click **Select firmware**, and then browse to the location of the upgrade files.
5. After you select the firmware files, click **Upgrade** to start the upgrade process.

CAUTION. *While the instrument is being upgraded, do not power down the instrument. If the instrument is powered down during an upgrade, the firmware will likely be corrupted, which will require the instrument to be returned to Tektronix for repair.*

6. After the upgrade is complete, click **Reset device** to reset the instrument.
7. Add the upgraded instrument back into the Configuration.xml file.

RFM220 Client

The RFM220 Client application allows you to view the data that the RFM220 Aggregator application has collected from the RFM220 instrument(s) that the Aggregator is monitoring.

Installation Considerations

The typical RFM220 system installation will have the RFM220 Aggregator installed on a network server, where it can be accessed by network PCs with the RFM220 Client application installed.

You can run the RFM220 Client application from any PC or server that is on the same Ethernet network as the PC or server on which the RFM220 Aggregator application is running. In situations where multiple Aggregators are installed, you can use the RFM220 Client to access any Aggregator running on the network.

The RFM220 Client can connect to only one Aggregator at a time and can view data from only one monitored RFM220 instrument at a time.

Multiple RFM220 Clients can establish network connections to the RFM220 Aggregator and request for data for a particular device.

NOTE. *The performance of the RFM220 Aggregator diminishes as more RFM220 Clients are connected and as more graphs are selected to be displayed by the RFM220 Clients.*

For best system performance, install the Aggregator and Client applications on separate computers and limit the number of graphs that each RFM220 Client opens at a time to six.

Improving Performance

Windows 7 systems. On Windows 7 systems, the RFM220 software is more responsive when the Visual Effects settings are changed as follows:

1. Use Windows Explorer to navigate to the following file: C:\Windows\System32\SystemPropertiesPerformance.exe
2. Double-click **SystemPropertiesPerformance.exe** to open the Performance Options dialog.
3. Select the **Visual Effects** tab, and then click **Adjust for best performance** as shown below.
4. Verify that all of the boxes are unchecked in the Custom list, and then click **OK** to save the changes and close the Performance Options dialog.

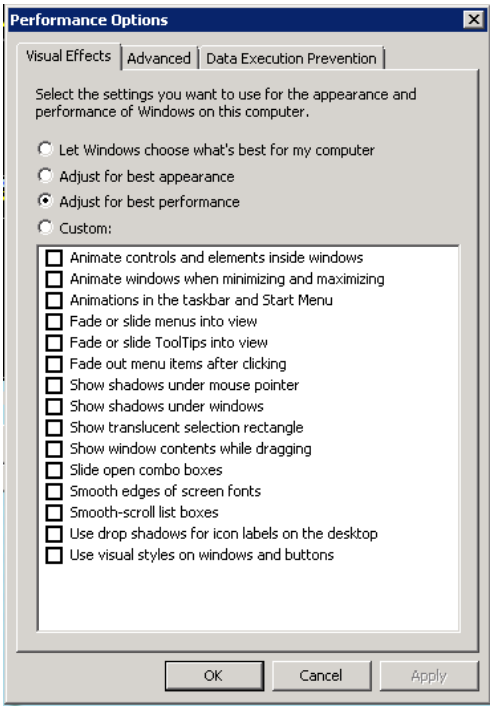


Figure 29: Setting the Windows 7 visual effects

Windows XP systems. On Windows XP systems, the RFM220 software is more responsive when the display effect settings are changed as follows:

1. Use the Start menu to open the Control Panel.
2. Double-click **Display** to open the Display Properties dialog.
3. Select the **Appearance** tab, and then click **Effects** to open the Effect dialog.
4. In the Effects dialog, select the settings as shown in the following illustration, and then click **OK** to accept the changes.

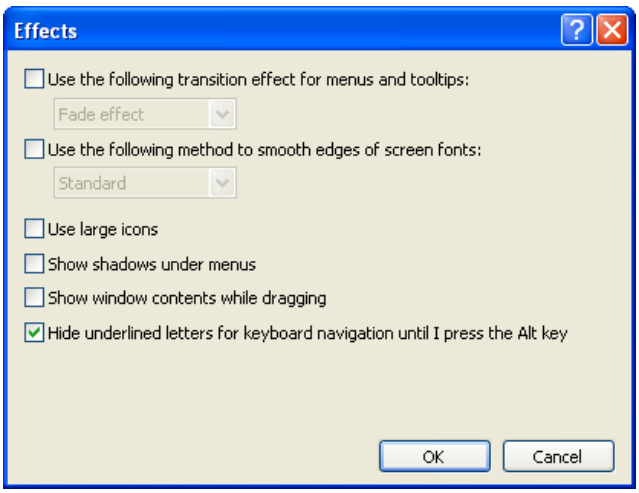


Figure 30: Setting the Windows XP display effects

General Operating Information

User types. The RFM220 Client application allows you to log into an RFM220 instrument using one of two user types:

- Administrator. Log in as Administrator for unrestricted access to full operating privileges such as setting measurement thresholds.
- User. Log in as User when you need to only view the measurement data or to generate log reports.

CAUTION. *To operate the RFM220 software on Windows 7 systems, the user who has logged on must have Full Access privileges.*

Each user type has a different role for supporting and using the RFM220 system. Some functions of the Client application, such as using the Configuration menu, are only available to a user logged in as the Administrator. (See page 5, *User Profiles and Roles*.)

Passwords. The default password for each user type are as follows:

- Administrator: tek
- User: none (blank)

A user must be logged in as the Administrator to change the passwords. Select Change Password in the Configuration menu to open the Change Password dialog box. You can use the dialog box to change the password for both user types.

NOTE. *The passwords are used for software access only. They do not provide security for the monitoring data or for the instrument hardware.*

Error indicator color codes. The RFM220 Client uses colored LEDs to indicate the status of signal measurements and device events. Use the Alarm Configuration dialog box to enable/disable tests, and to categorize error levels and set measurement limits for each test. (See page 60, *Alarm Configuration*.)

Table 7: Error indicator color codes

Item	Description
	Red indicates that a test categorized as Critical has failed or that a threshold limit on a Critical test has been crossed.
	Amber indicates that a test categorized as a Warning has failed or that a threshold limit on a Warning test has been crossed.
	Blue indicates that a test categorized as Information has failed or that a threshold limit on a Information test has been crossed.
	Green indicates that a test has not failed or that a threshold limit has not been crossed.
	Gray indicates that a test is disabled.

Date and time displays. When the Aggregator is started, it pushes the UTC time into each instrument listed in the Configuration.xml file. All of the times that are shown in the RFM220 Client displays (for example, in the event log entries and in the Status bar), are the times reported by the RFM220 instrument in terms of the time on the RFM220 Client computer, including taking into account the local time zone and daylight savings time settings.

Changes to the time zone or daylight savings time settings that occur on the RFM220 Client computer after the RFM220 Client has been started, will be automatically accounted for in the time displays on the RFM220 Client.

NOTE. *There may be a small discrepency in the time displayed on the RFM220 Client computer and the time displayed in the RFM220 Client. This is caused by small time drifts in the RFM220 instrument that occur after the instrument receives the UTC time from the RFM220 Aggregator.*

Online and offline monitoring. In the RFM220 Client Login dialog, the monitored devices list includes a status column, which lists one of the following as the status of the monitored device: (See Figure 22 on page 39.)

- Online. Indicates that the device is an RFM220 instrument and that it is available to the Aggregator.
- Offline. Indicates that the device is an RFM220 instrument and that it is turned off or otherwise unavailable to the Aggregator.

NOTE. *Since trend data and log entries are stored by the RFM220 Aggregator for as long as it remains running, you can still connect to an offline RFM220 instrument if that instrument was ever monitored by the Aggregator. In this case, you will be able to view trend data and event log entries for the offline device that was collected in the past while the device was online and being monitored by the Aggregator.*

Display Elements

The RFM220 Client window has the following primary display elements:

- Title bar. Lists the name of the product: Tektronix RFM220.
- Menu bar. Provides access to the various menu commands. Click on a menu name to access the commands under that menu. The menu commands are described on the following pages.
- Status bar. Displays the status of various parameters. (See page 62, *Status Bar*.)
- Graphs pane. Displays the graphs you select from the pull-down list. Controls allow you to change the graph layout, show error range indicators, and change the trend time scale of a graph. (See page 66, *Graphs*.)
- Metrics pane. Displays the metrics of the measurement results and information about the selected device (RFM220 instrument).(See page 72, *Device Metrics*.)
- Logs pane. Displays information about RF events (signal measurements) and device (RFM220 instrument) events. Control buttons allow you to pause, clear, or save the event log. (See page 70, *Event Logs*.)
- Pane Controls. Allows you to completely collapse or expand the pane boundaries. You can adjust the pane sizes by dragging and dropping the pane boundaries.

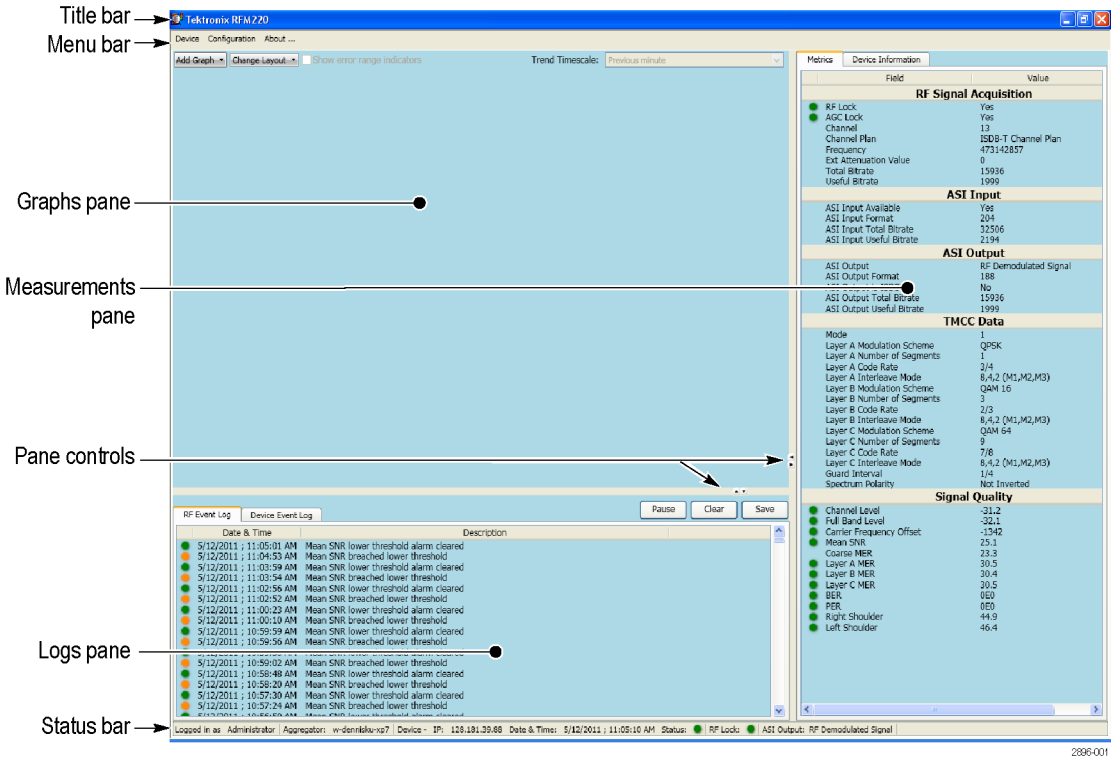


Figure 31: RFM220 Client window elements

Device Menu

The Device menu provides the following selections to enable you to connect or disconnect from an RFM220 instrument or to connect to another Aggregator.

Connect. Displays the RFM220 Client Login dialog. Use this dialog to connect to a different RFM220 instrument that is being monitored by the Aggregator to which you are connected or to connect to a different Aggegator that is running on the network. (See page 38, *Starting the RFM220 Client*.)

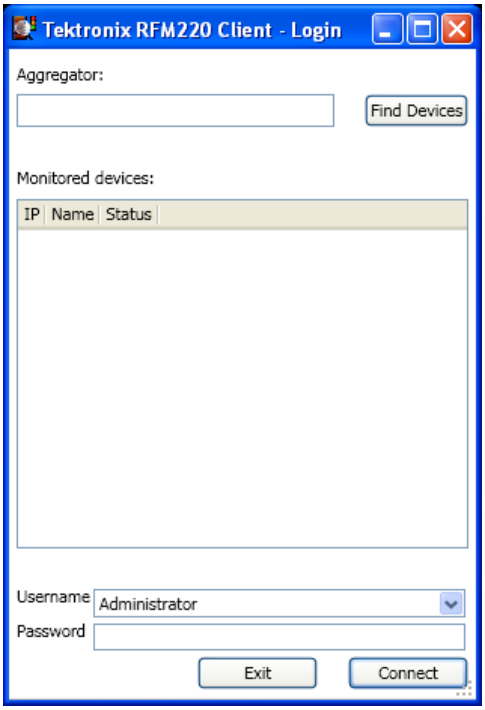


Figure 32: RFM220 Client login window

Exit. Saves your settings and closes the RFM220 Client application.

Configuration Menu

The Configuration menu provides the following selections to enable you to configure the channel plan, enable/disable tests and set alarm thresholds, or to change user passwords:

NOTE. *A user must be logged in as the Administrator to select any of the items in the Configuration menu. (See page 5, User Profiles and Roles.)*

Edit Settings. Displays the Edit Settings dialog shown below. Use this dialog to configure the channel plan for your input signal.

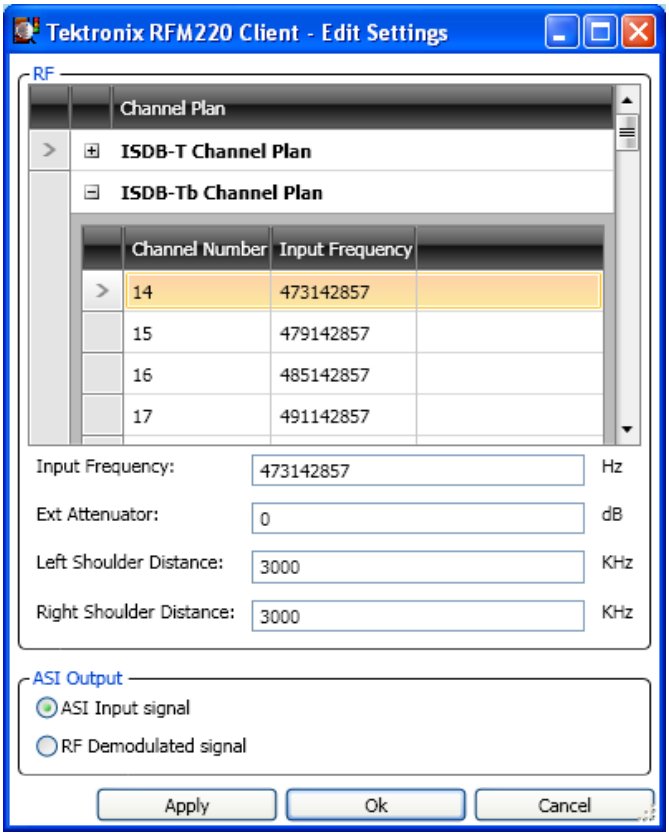


Figure 33: Edit Settings dialog

The Edit Setting dialog allows you to perform the following tasks:

- Configure the channel plan by setting the following parameters:
  - Channel Number. Select which channel will be monitored from either the ISDB-Tb or ISDB-T channel plans. Select the appropriate plan and channel number for the input signal you intend to monitor.
  - Input Frequency. Enter the frequency for the selected channel. You can set the channel frequency to any number between 170–862 MHz in Hertz. If you set the input frequency to a custom value that does not match the frequency of any of the channels in the selected Channel Plan, the Channel Plan selected is set as None and Channel Number list is made empty.
  - Ext Attenuator. Enter the dB value of any external attenuator that is connected to the input signal. This allows the RFM220 system to compensate for the attenuator and adjust the measurement thresholds for reporting signal errors.
  - Left and Right Shoulder Distance. Enter the distance (in kHz) for the left and right shoulders. This allows the RFM220 system to compensate for the shoulder distance on the input signal. The default value is 3150 kHz.
- Configure which signal will be output from the ASI output connector of the RFM220 instrument. You can select either the ASI input signal or the RF demodulated signal.

After you make any desired changes, click **Apply** to apply the changes. Click **OK** to apply the changes and close the dialog box.

Alarm Configuration. Displays the Alarm Configuration dialog shown below. Use this dialog to enable/disable tests and set alarm measurement parameters. After you make any desired changes, click **Apply** to apply the changes. Click **OK** to apply the changes and close the dialog window.

Information about how to set the measurement thresholds is provided later in this manual. (See page 63, *Alarm Thresholds*.)

CAUTION. *To prevent an SNMP alarm storm from overloading the Aggregator, you should leave enough range between the Active and Clear threshold to account for minor signal fluctuations. If the error band is too narrow and the signal has a lot of fluctuations, a large number of SNMP traps will be sent to the Aggregator.*

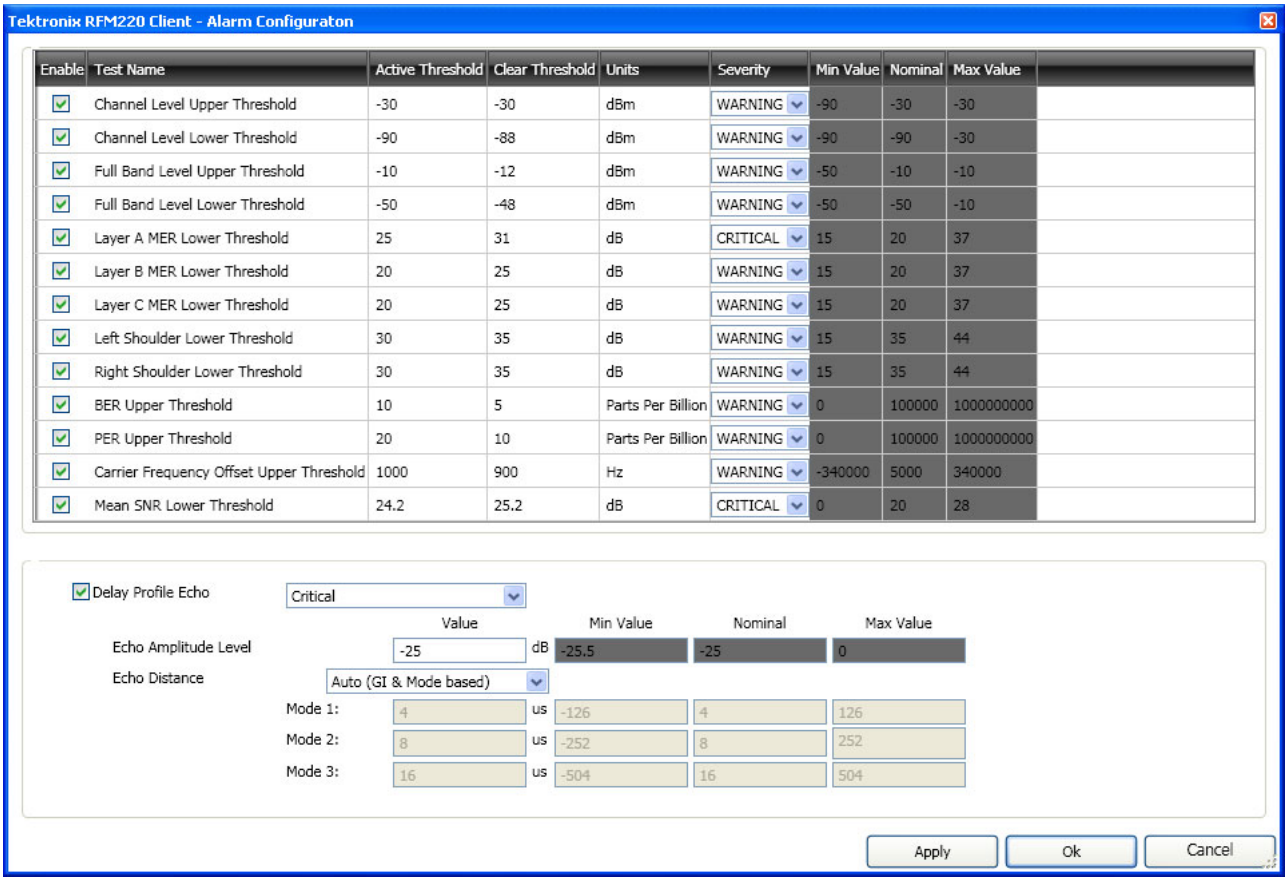


Figure 34: Alarm Configuration dialog

Change Password. Displays the Change Password dialog shown below.

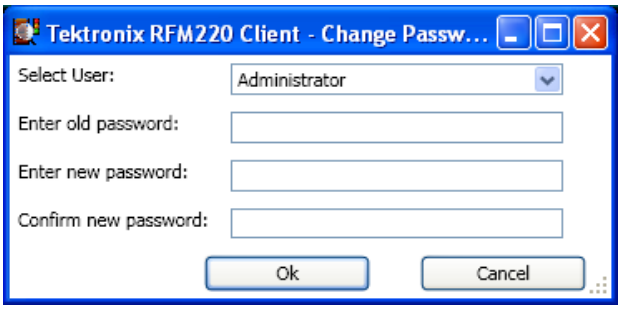


Figure 35: Change Password dialog

Select the user type (Administrator or User) of the password you are changing, and then enter the old password and the new password. Click **OK** to save the new password and close the Change Password dialog.

About Menu

Displays the About window shown below, which contains information about the RFM220 hardware and software versions.

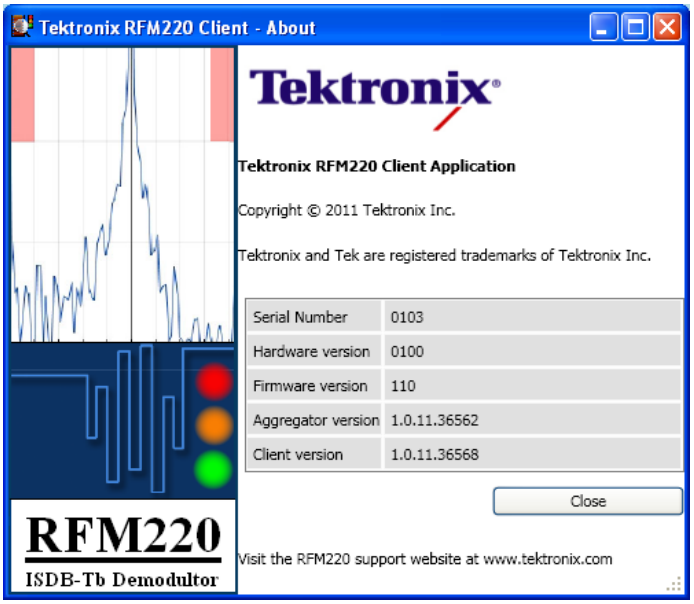


Figure 36: About window

Status Bar

The Status bar appears at the bottom of the Client display and provides the following information:

- Logged in as. Lists which user type (Administrator or User) was used to login to the RFM220 system. Each user type has different roles. (See page 5, *User Profiles and Roles*.)
- Aggregator. Lists the IP address or network name that was used to connect to the Aggregator in the RFM220 Client Login dialog.
- Device. The device section lists the following information:
  - IP. This is the IP address of the RFM220 instrument to which you are connected.
  - Date & Time. This is the current date and time of the RFM220 instrument to which you are connected. The time displayed here and in the event logs may vary from the time displayed on your computer. (See page 55, *Date and time displays*.)
  - Status. This colored LED indicates the current status of the instrument. Green indicates the instrument is online and red indicates the instrument is offline. When an instrument is offline, the Metrics display grays out to indicate that the displayed signal parameters are no longer valid.
- RF lock. Displays a colored LED to indicate whether the RFM220 instrument is locked to the frequency of the input signal:
  - Green indicates that the instrument is locked to the input signal.
  - Red indicates that the instrument is not locked to the input signal.
- ASI Output. Lists which signal is being output from the ASI ouput connector on the RFM220 instrument (ASI Input Signal or RF Demodulated Signal). Use the Edit Settings dialog to change which signal is output. (See page 58, *Edit Settings*.)

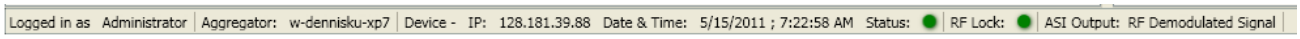


Figure 37: Status bar

Alarm Thresholds

Select Alarm Configuration from the Configuration menu in the RFM220 Client, the Alarm Configuration dialog opens as shown below. Use this dialog to enable/disable tests and set alarm measurement parameters.

NOTE. *When you enable/disable tests or change measurement thresholds, information messages are entered in the Device Event log. The messages are color-coded blue to indicate they are information-only messages. (See page 55, Error indicator color codes.) (See page 70, Event Logs.)*

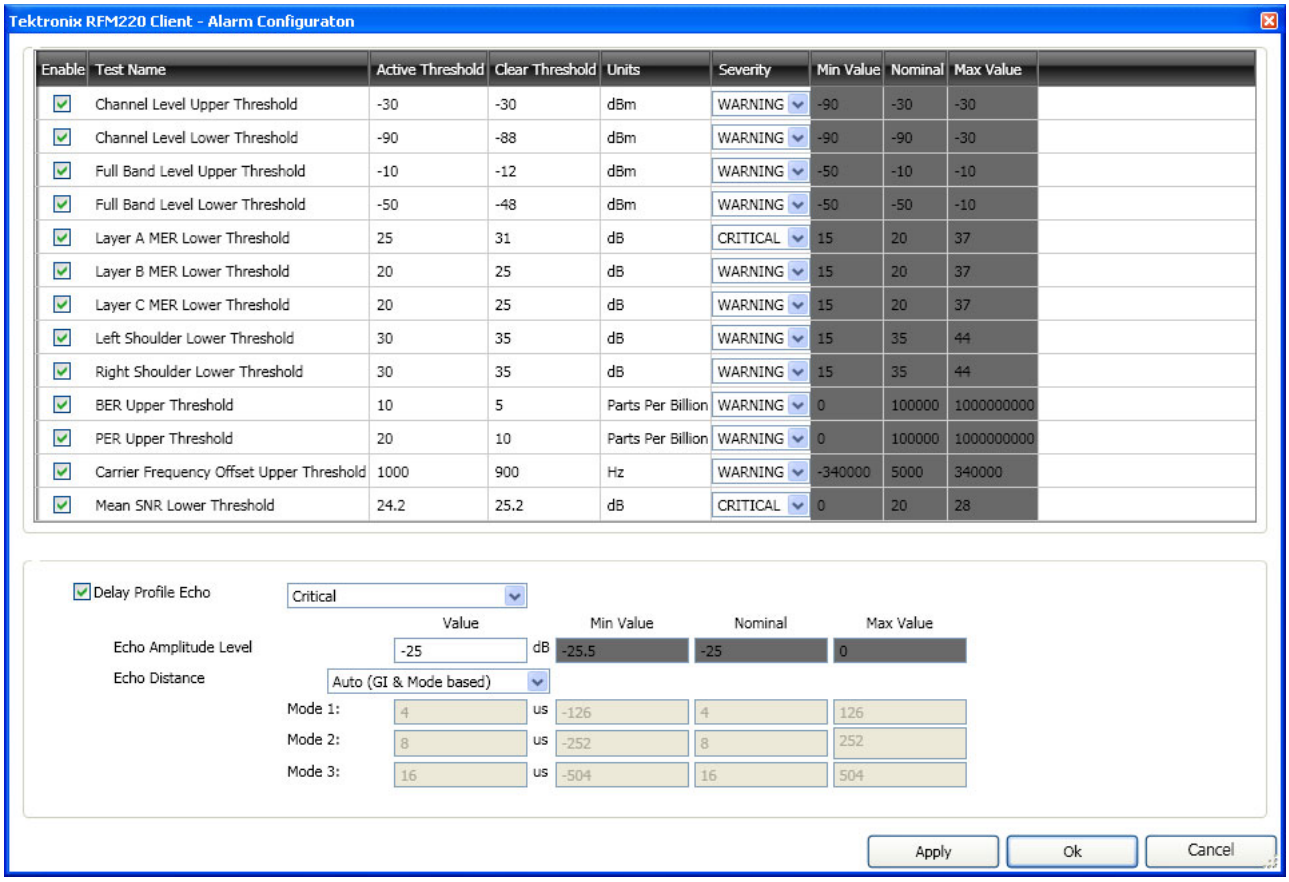


Figure 38: Alarm Configuration dialog

The Alarm Configuration dialog allows you to perform the tasks listed below. After you make any desired changes, click **Apply** to apply the changes and then click **OK** to save the changes and close the dialog window.

- Enable/disable tests. Click the box next to the test names to enable or disable tests. Enabled tests are indicated by a check mark. Disabled tests are indicated by a gray LED in the Metrics pane.
- Set the Active threshold. Click in the Value field and enter the measurement threshold for each test. When this threshold is exceeded, an error message will be generated. The Min/Max Value columns list the threshold ranges for each test. The Nominal column lists the recommended value for the test.

NOTE. *When there is a change in the Alarm state, for example, when the measurement value crosses the Active threshold or when it crosses the Clear threshold, SNMP traps are generated and sent to the Aggregator and to the secondary trap destination intended for your NMS System (if you used the Device Setup utility to configure the secondary trap destination).*

- Set the Clear threshold. Click in the Value field and enter the measurement threshold for each test. When this threshold is crossed by a test that is in an active error condition, an error-cleared message will be generated.
- Set the Severity level. Set the error-reporting severity level for each test by picking from the drop-down list: Critical, Info, or Warning. Color codes are assigned to the status LEDs based on the severity levels that are configured here. (See page 55, *Error indicator color codes*.)
- Configure the Delay profile echo parameters. Enable or disable the Delay Profile Echo measurement to set parameters such as amplitude level and distance for echo-related time distortions. If the echo distance is set to User Defined, you can set the distance limits for modes 1 ,2 and 3. Alarms occur if the echo amplitude is higher than the Amplitude level you set and if it is outside of the set region. If the echo distance mode is set to Automatic, alarms are generated based on the Mode and Guard Interval.

NOTE. *The Delay Profile alarm is a software alarm, unlike the other alarms which are SNMP alarms. Therefore, alarms generated by the Delay Profile alarm will not be sent to the secondary trap destination that is intended for your NMS System.*

Measurement Thresholds

The following table shows the default active and clear thresholds for each test along with the maximum and minimum values for each test. The nominal value is the normally expected value for the test.

CAUTION. *To prevent an SNMP alarm storm from overloading the Aggregator, you should leave enough range between the Active and Clear threshold to account for minor signal fluctuations. If the error band is too narrow and the signal has a lot of fluctuations, a large number of SNMP traps will be sent to the Aggregator.*

Table 8: Alarm measurement thresholds

Test name	Active threshold	Clear threshold	Minimum value	Nominal value	Maximum value
Channel (input) level upper threshold	-30 dBm	-32 dBm	-90 dBm	-30 dBm	-30 dBm
Channel (input) level lower threshold	-90 dBm	-88 dBm	-90 dBm	-90 dBm	-30 dBm
Full band level upper threshold	-10 dBm	-12 dBm	-50 dBm	-10 dBm	-10 dBm
Full band level lower threshold	-50 dBm	-48 dBm	-50 dBm	-50 dBm	-10 dBm
Layer A MER lower threshold	20 dB	22 db	15 dB	20 dB	37 dB
Layer B MER lower threshold	20 dB	22 db	15 dB	20 dB	37 dB
Layer C MER lower threshold	20 dB	22 dB	15 dB	20 dB	37 dB
Left shoulder lower threshold	35 dB	37 dB	15 dB	35 dB	44 dB
Right should lower threshold	35 dB	37 dB	15 dB	35 dB	44 dB
BER (Bit Error Rate) upper threshold	100,000 parts per billion	10,000 parts per billion	0 parts per billion	100,000 parts per billion	1,000,000,000 parts per billion
PER (Packet Error Rate) upper threshold	100,000 parts per billion	10,000 parts per billion	0 parts per billion	100,000 parts per billion	1,000,000,000 parts per billion
Carrier frequency offset upper threshold	5,000 Hz	4,000 Hz	-340,000 Hz	5,000 Hz	340,000 Hz
Mean SNR lower threshold	20 dB	22 dB	0 dB	20 dB	28 dB
Delay profile echo	-25 dB	NA	-25 dB	-25 dB	0 dB

Compensating for an external attenuator. If your input signal has an external attenuator, you need to adjust the alarm thresholds to compensate for the attenuator.

Graphs

The Graphs pane is where measurement graphs are displayed and controlled.

CAUTION. *The graphs will not display properly if the resolution of your computer monitor is less than 1024 x 768 pixels.*

NOTE. *The performance of the RFM220 Aggregator diminishes as more RFM220 Clients are connected and as more graphs are selected to be displayed by the RFM220 Clients. For best system performance, install the Aggregator and Client applications on separate computers and limit to six, the number of graphs that each RFM220 Client opens at a time.*

Figure 39: Graphs pane

Selecting Graphs

Use the drop-down list of the Add Graph menu to select/deselect graphs to display. You can select multiple graphs to display. Selected graphs are indicated by a check mark.

NOTE. *As you select more graphs to display, the performance of the RFM220 software will diminish.*

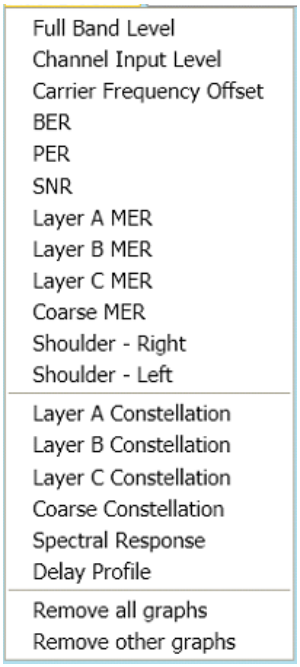


Figure 40: Add Graph menu selections

Trend graphs. All of the graphs in the Add Graph list that appear above the graph list separator are trend graphs.

The Aggregator collects and stores trend data from the instruments that it is monitoring. As long as the Aggregator stays running, the trend data remains available for all of the instruments that the Aggregator has monitored since it was started. However, all trend data will be lost when the Aggregator application is closed or shut down, or when the instrument is removed from the Configuration.xml file.

Special graphs. Constellation and spectrum graphs enable you to identify modulation problems such as amplitude imbalance, quadrature error, coherent interference, phase noise, amplitude noise, phase error and MER problems. Left and right shoulder measurements are displayed in dB to help indicate if there are spectrum mask issues.

NOTE. *Special graphs are shown properly only if the instrument is online. Special graphs for Offline instruments will show a "Loading Data" message. If a special graph is already open and showing data when an instrument goes offline, the special graph will continue to show the old data or the last graph obtained.*

If the RF input signal to the RFM220 instrument is not proper or if RF lock to the signal is lost, the Constellation graph will not show data and a "Loading Data" message will be continuously displayed. A possible cause of this problem in an inaccurately tuned channel frequency. Use the Configuration menu to edit the channel plans and tune channel frequencies. (See page 58, Configuration Menu.)

Changing the Graph Layout

Change Layout menu. Use the Change Layout drop-down list to select one of the following layouts:

- Horizontal
- Vertical
- Tiled Horizontal
- Tiled Vertical

Pane controls. Allows you to completely collapse or expand the pane boundaries. You can adjust the pane sizes by dragging and dropping the pane boundaries. (See Figure 31.)

Graph selection. Click on a graph to select it. The selected graph will have a red line around the graph.

Error range indicators. The Error Range Indicator check box is only available when a trend graph or the Delay Profile graph is seleted. When the error range indicators are displayed, the error thresholds are indicated by red areas on the graph.

Trend timescales. The Trend Timescale drop-down list is only available when a trend graph is selected. The following time scales are available:

- Previous minute
- Previous ten minutes
- Previous hour
- Previous day
- Previous week

Trend Graph Updates

Trend graph displays are updated as follows:

- The error range indicators are updated with every update cycle of the trend graphs.
- The update rate of the trend graphs depends on the time scale that is selected:
  - When “Previous minute” or “Previous ten minutes” is selected, graphs are updated every 5 seconds.
  - When “Previous hour” is selected, graphs are updated every 12 seconds.
  - When “Previous day” is selected, graphs are updated every 5 minutes.
  - When “Previous week” is selected, graphs are updated every hour.

NOTE. *When “Previous day” or “Previous week” is selected as the time scale for a graph, changes that are made to the active alarm threshold are not immediately reflected on the error range band of the graph. You can force the graph to update by closing and reopening either the graph or the application itself.*

Error Range Indicators

The error-range indicators on the graph displays correspond (See Figure 39 on page 66.) to the active alarm thresholds set in the Alarm Configuration dialog. (See page 63, *Alarm Thresholds*.)

For trend graphs, the error range indicators behave as follows:

- The error range indicators show the same value as the corresponding Active alarm threshold value for that metric.
- The presence of the upper and lower error bands depends on the presence of the upper and lower alarms for that metric. If a metric has only an upper limit, only the upper error-range band will be displayed. An error-range band will not be shown for metrics that do not have either an upper or lower value alarm.
- The error range indicators on the graphs are updated at every update cycle of the trend graphs.

Plot Lines

Most of the graphs have a Settings button in the top right corner which allows you to add or remove plot lines on the graph. You can select the following plot lines to display. By default, all plot lines are shown.

- Draw maximum. Draws a plot line for the maximum measurement.
- Draw average. Draws a plot line for the average measurement.
- Draw minimum. Draws a plot line for the minimum measurement.

Event Logs

The RFM220 Aggregator creates and stores events from monitored RFM220 instruments in log files.

Log File Location

The RFM220 Aggregator maintains all of the log files in the Application Data folder on the PC or server where the Aggregator is installed. The path to these files are as follows:

- Windows 7 systems:
  C:\Users\<user ID>\AppData\Local\Tektronix\RFM220\RFM220 Aggregator\Logs
- Windows XP systems:
  C:\Documents and Settings\<user ID>\Local Settings\Application Data\Tektronix\RFM220\RFM220 Aggregator\Logs

Log File Types

There are two types of log files in the Logs directory:

- Aggregator.log, which contains log entries that are related to the Aggregator. A user will not typically need to access this file.
- <IP address>.log, which contains the device logs for the associated RFM220 instrument being monitored. There will be a file for each RFM220 instrument that the Aggregator has monitored.

Log File Management

Backing up the log files. To prevent the loss of data, it is recommended that the RFM220 system administrator backup the log files whenever the Aggregator is stopped (for example, if the RFM220 system requires maintenance or if there is a reason to stop the Aggregator).

CAUTION. *To prevent the loss of data after the Aggregator has been shut down, the RFM220 system administrator needs to ensure that no log files are present in the Logs folder before the Aggregator is restarted.*

Saving log files. To help solve a problem with your RFM220 system, Tektronix may request a copy of your log files. If your logging has been set to a low level such as Info in the Configuration.xml file (See page 22, *Configuring the RFM220 Aggregator*.), Tektronix may request that you change the logging to a higher level such as Debug or Verbose in order to get a better diagnosis of the problem. Except in such support request cases, users are advised to set the logging level to Info.

Log size control. The size of the event logs and the length of the log entries is controlled by the Configuration.xml file used by the RFM220 Aggregator.

Preexisting Errors

Aggregator startup. When the Aggregator is first started, errors may already exist in the monitored signal. Since the Aggregator cannot know when the preexisting error started, the error is reported in the event logs with the prefix "Synchronized" to indicate that the error started prior to the Aggregator starting to monitor the signal. This type of message is also displayed when a test is enabled after the Aggregator is started.

The timestamp for these Synchronized messages is the time the error was detected by the Aggregator, not the time the error occurred.

Instrument reset. When a RFM220 instrument is reset, the alarm state for the SNR test is set to true. This is because during the instrument reset, the SNR value is set to 0. If the Aggregator is started after the instrument is reset, it will be observed that the SNR value will go below the threshold with no alarm being reported (because the alarm state is already set to true). The work-around for this situation is to first clear the SNR alarm by setting a lower value for the Clear threshold, and then later setting new Active and Clear thresholds.

RFM220 Client Logs Display

The RFM220 Client displays two types of event logs:

- RF events. All of the RF-related events are shown in the RF Event Log.
- Device events. All of the other instrument-related events are shown in the Device Event Log.

You can view the desired event log by selecting the associated tab in the Logs pane: RF Event Log or Device Event Log.

You can pause, clear, or save the selected event log by clicking the Pause, Clear, or Save buttons. Only a user logged in as the Administrator can clear the logs.

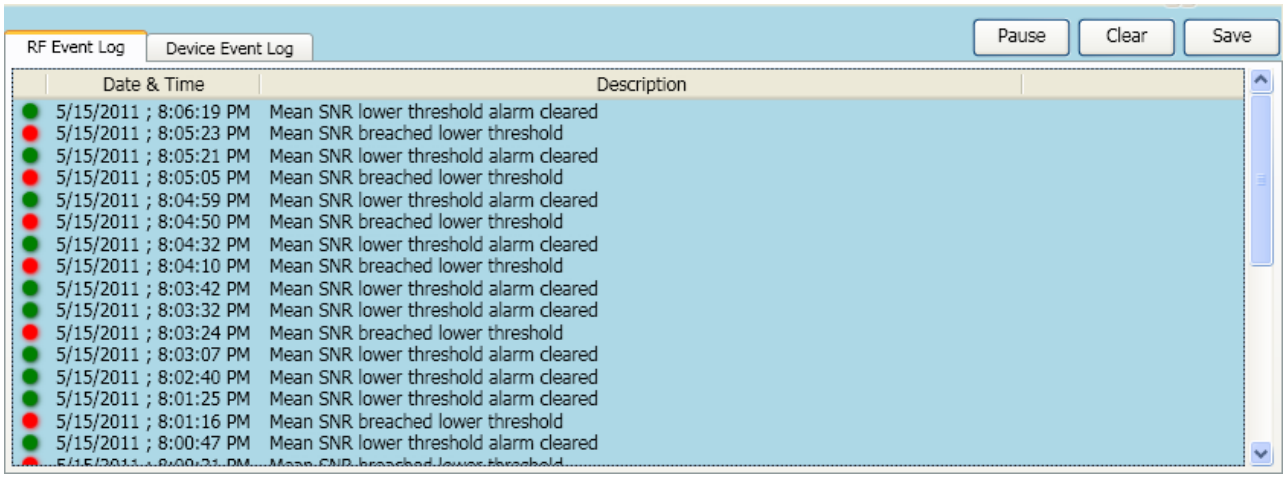


Figure 41: RFM220 Client Logs pane

Device Metrics

The Metrics pane provides two tabs to display various metrics for the signal and instrument being monitored: Metrics and Device Information.

Metrics Tab

Select the Metrics tab to display metrics for the input signal.

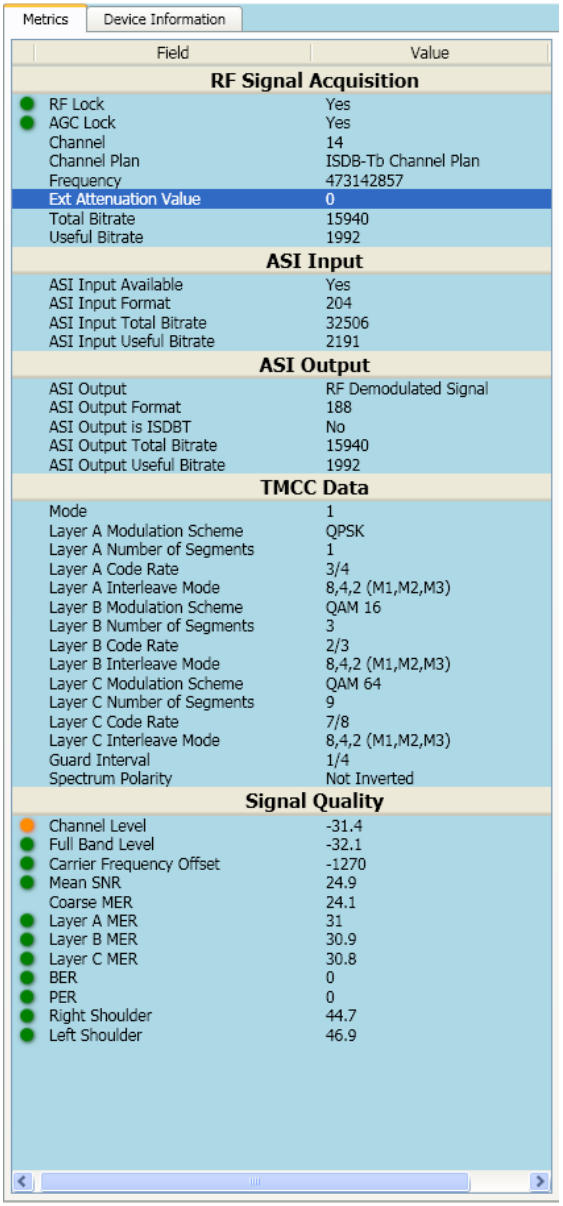


Figure 42: Metrics display

Device Information Tab

Select the Metrics tab to display metrics for the RFM220 instrument that is being monitored.

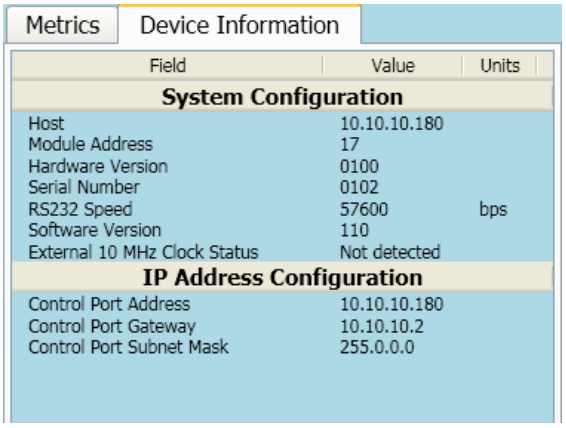


Figure 43: Device Information metrics display

LED Indicators

When SNMP alarms from a RFM220 instrument are sent to the RFM220 Aggregator, the LED indicators in the Metrics pane will change color to match the severity level of the detected error. (See page 55, *Error indicator color codes*.)

Synchronizing Alarms

If a RFM220 instrument is reset to the default settings while being monitored by an Aggregator, you need to reapply the alarm configuration settings to synchronize the alarm LED indicators on the Metrics pane with the actual state of the alarms. To reapply the alarm configuration settings, open the Alarm Configuration dialog and click Apply.

CAUTION. *If you do not reapply the alarm configuration settings after a RFM220 instrument is reset to the factory default settings, the LED indicators for some metrics will indicate an active error condition that cannot be cleared.*

Reference

Connecting to an MTM400A DTV Monitor

The RFM220 demodulator can be used as a standalone RF monitoring solution or used in conjunction with a Tektronix MTM400A DTV monitor to provide combined RF and TS monitoring.

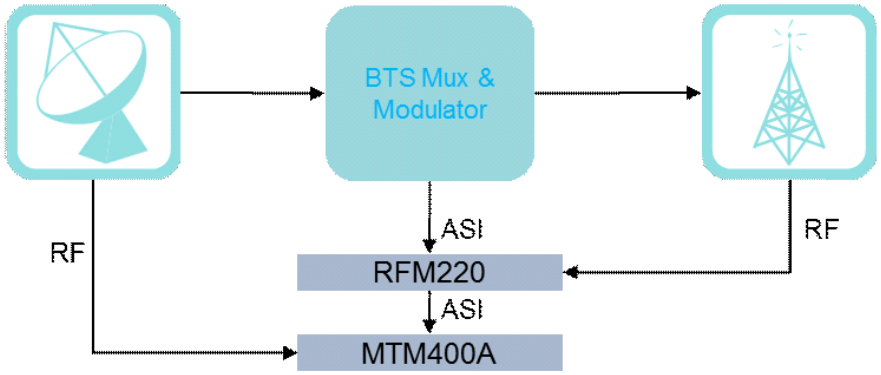


Figure 44: Combined RF and TS monitoring

If you connect both the RF and ASI inputs to the RFM220 demodulator, you can then use the RFM220 to select which signal source to output to an MTM400A or any other device that requires ASI input. This enables monitoring before and after modulation.

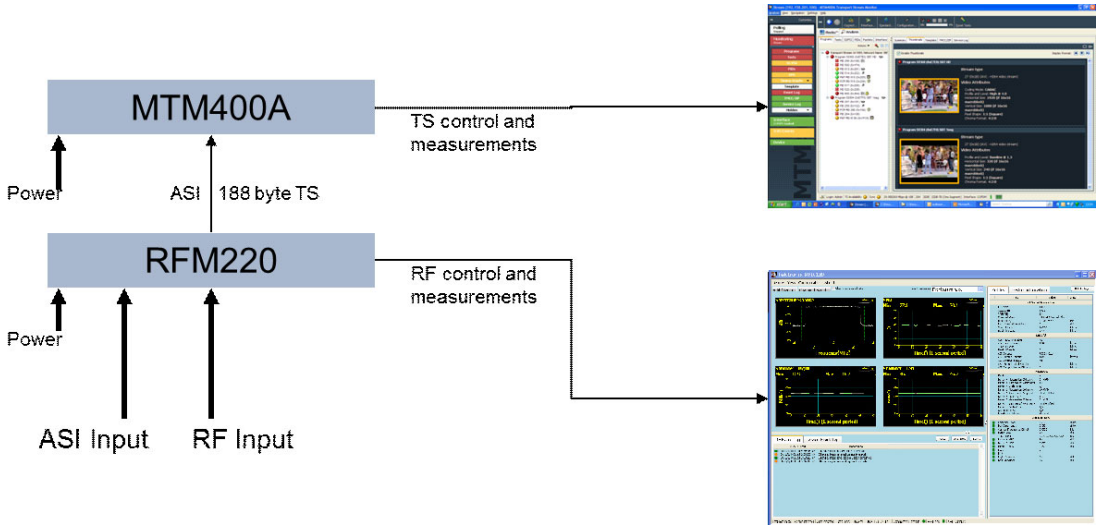


Figure 45: Outputting the RF or ASI input signal to an MTM400A monitor

TMCC Monitoring

The RFM220 demodulator will continue to monitor the RF signal quality even if the ASI input is selected for routing to the MTM400A for TS analysis. In this configuration a 204-byte BTS input can be monitored providing TMCC and IIP consistency analysis in the MTM400A in addition to monitoring the RF broadcast signal quality.

TMCC information must be monitored to ensure that receivers can demodulate the signal effectively. Errors in the TMCC information would lead to STBs not functioning properly. In addition to displaying the TMCC information on the RFM220 Client application, the MTM400A DTV monitor can be used to provide TMCC and IIP consistency testing and analysis at the Transport Stream layer. The in-depth ISDB-Tb cross-table consistency testing was developed in conjunction with Japanese broadcasters. When combined with ISDB-Tb RF metrics, the Tektronix solution represents a powerful and unique toolset for remote ISDB-Tb monitoring.

Frequency Shift Measurement

The RFM220 demodulator is able to measure the frequency shift of the input signal. To make this measurement, you must connect a 10 MHz reference signal to both the modulator equipment and to the 10 MHz In connector on the RFM220 instrument.

Recovering the IP Address

If you lose or cannot remember the IP address of the RFM220 instrument, use the procedure in this section to recover the address.

Required Equipment

You will need the equipment listed below to recover the IP address:

- PC with an RS-232 connection
- RS-232 serial cable, DB9 male to DB9 female, straight wiring (pin 2 to pin 2, pin 3 to pin 3, etc.)

Procedure

1. Connect the RS-232 cable between the RS-232 ports on the PC and the RFM220 instrument.
2. Power on both the PC and the RFM220 instrument.
3. From the Start menu on the PC, select **All Programs > Accessories > Communications > Hyper Terminal**. This opens the HyperTerminal window.

NOTE. *If this is the first time that HyperTerminal has been opened on the PC, a Location Information dialog box will open where you must enter your location parameters before the HyperTerminal application will operate.*

If the Location Information dialog box appears, fill in the location information and then click ***OK****.*

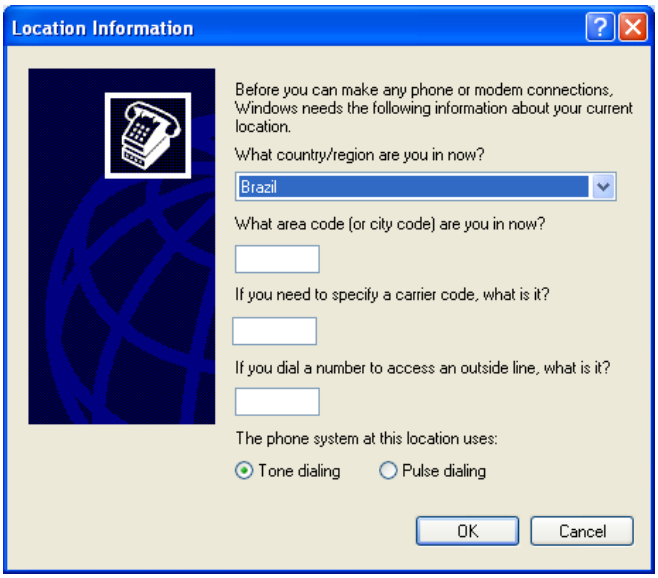


Figure 46: Entering location information for HyperTerminal

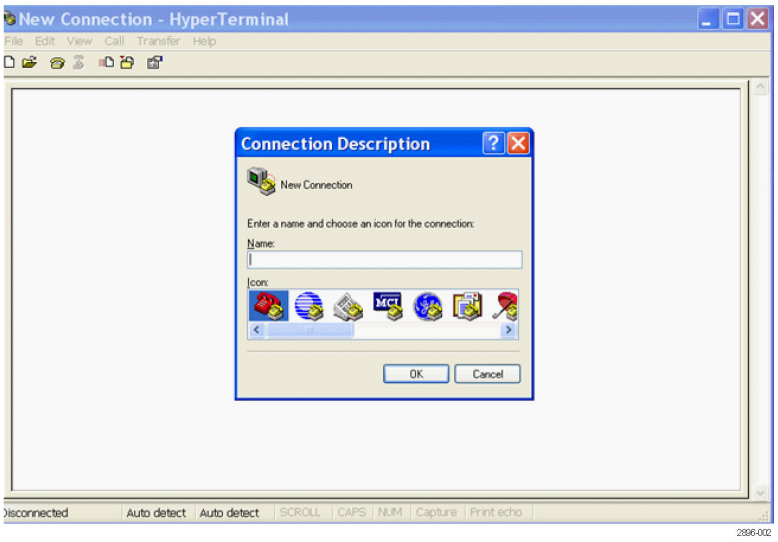


Figure 47: Entering the connection description for HyperTerminal

4. When the HyperTerminal window opens, the Connection Description dialog box appears. Enter the connection name you want to use and then click **OK**. The Connect To dialog box appears with the connection name you entered. In the example shown below, RFM220 – 150 was entered as the connection name.

Figure 48: Selecting the COM port for HyperTerminal

5. In the Connect To dialog box, use the drop-down list to select an available COM port on your PC (one not used by another device). Typically, this will be COM1. If you select a COM port that is already in use, a warning message will appear. Select another COM port until no warning message appears and then click **OK**.

6. In the COM port properties dialog box, enter the information shown below and then click **OK**.

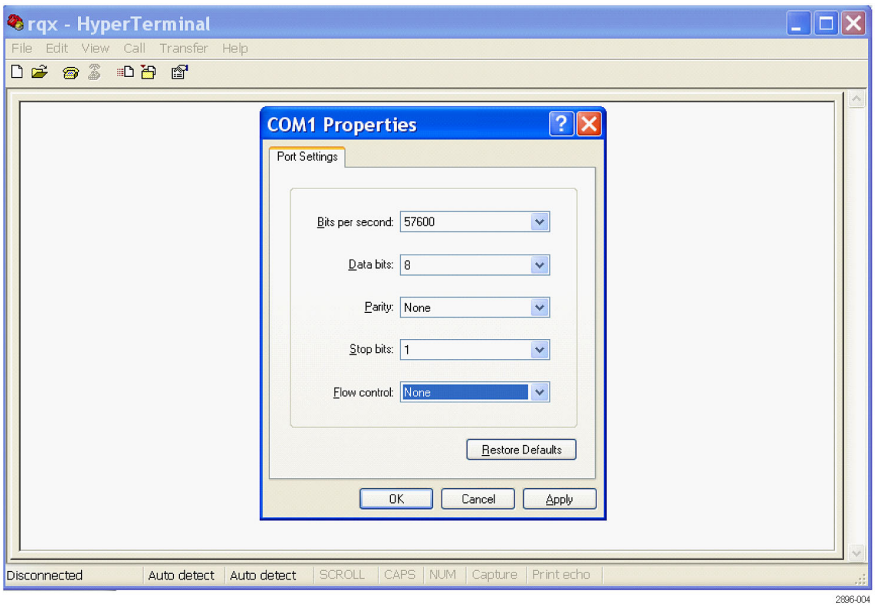


Figure 49: Entering the COM port properties for HyperTerminal

7. Check that the status bar at the bottom of the HyperTerminal window now displays **Connected**.

8. If the status bar shows Auto Detect, click the **Disconnect** icon to close the HyperTerminal connection and then perform the following steps to set a specific speed and mode for the connection.

CAUTION. *If the Status Bar displays Auto Detect, be sure to change the mode as described below. The RFM220 instrument does not support the auto detect mode.*

   a. In the HyperTerminal window, select **Properties** from the File menu.

   b. Select the **Settings** tab and then use the Emulation drop-down list to change the setting from Auto Detect to **ANSIW**.

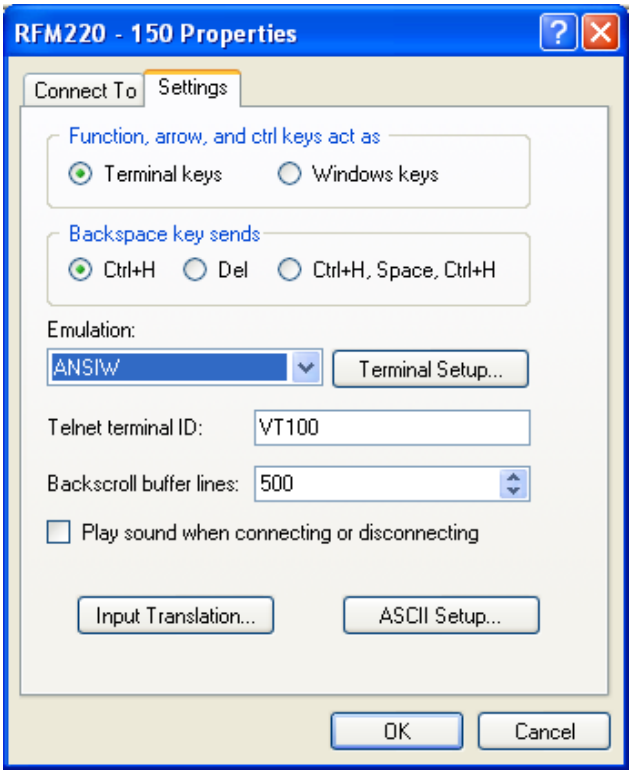


Figure 50: Setting the emulation mode for HyperTerminal

c. Click the **ASCII Setup** button to open the ASCII Setup dialog box.

d. In the ASCII dialog box, select all of the boxes as shown below. Click **OK** to confirm the settings and then click **OK** again to close the properties dialog box.

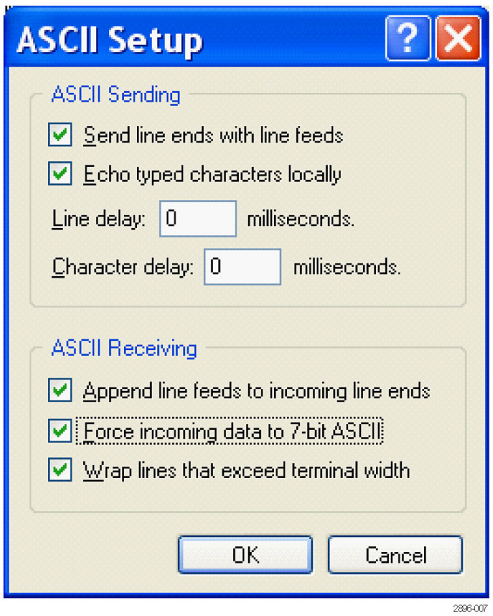


Figure 51: Configuring the ASCII setup for HyperTerminal

e. Verify that the status bar in the HyperTerminal window now shows the ANSIW emulation mode.

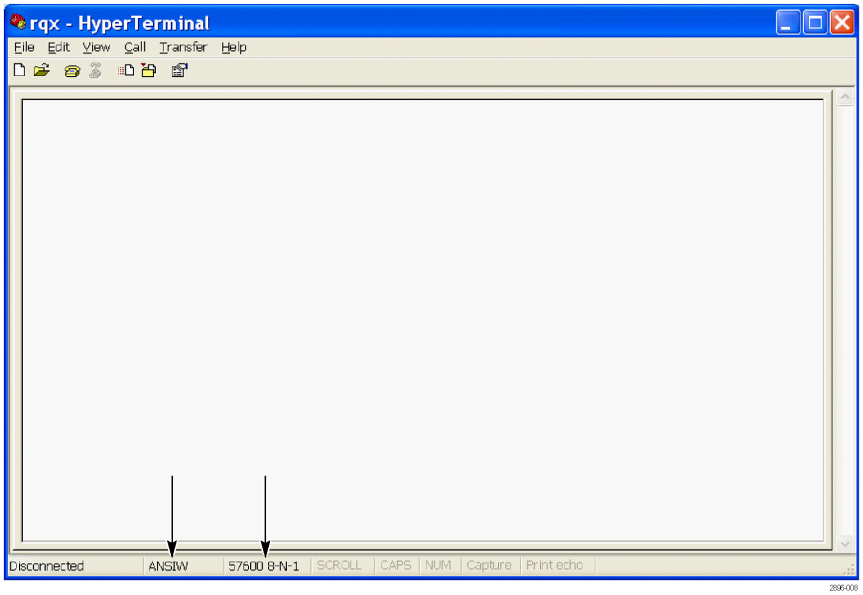


Figure 52: HyperTerminal window showing the ANSIW emulation mode

9. In the HyperTerminal window, click the **Call** icon to connect to the RFM220 instrument. The status bar will now say Connected.

10. In the HyperTerminal window, enter the following command: **TX 11 8B**. This command must be entered in upper case.

11. As shown in the example below, the HyperTerminal application returns the IP address of the RFM220 instrument in hex. The hex code is eight characters long and is between the two lines shown below.

    In this example, the IP address has been returned as C0 A8 01 D1 in hex, which translates to an IP address of 192.168.1.209 in decimal.

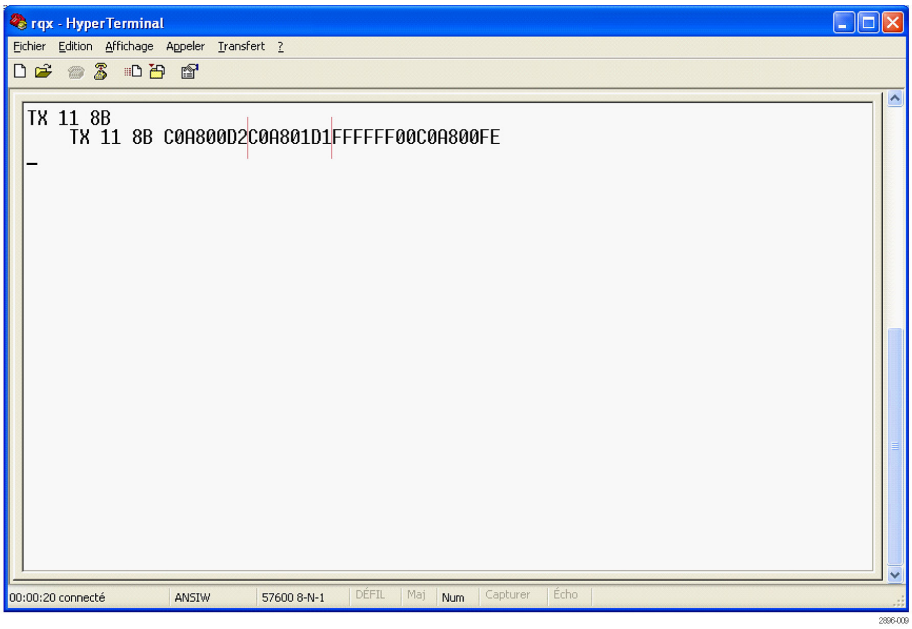


Figure 53: HyperTerminal window showing the IP address in hex

12. Use the returned IP address to connect to the RFM220 instrument.

Preventative Maintenance

Protect the instrument from adverse weather conditions. The instrument is not waterproof.

CAUTION. *To avoid damage to the instrument, do not expose it to sprays, liquids or solvents.*

Do not use chemical cleaning agents; they may damage the instrument. Avoid chemicals that contain benzene, toluene, xylene, acetone or similar solvents.

Preventive maintenance mainly consists of periodic cleaning. The instrument should be cleaned as needed based on the operating environment.

Cleaning the Exterior

WARNING. *To avoid personal injury or damage to the instrument, do not allow moisture inside it. Use only enough cleaning solution to dampen your cloth or swab.*

Clean the exterior surfaces of the instrument with a dry, lint-free cloth or a soft-bristle brush. If dirt remains, use a cloth or swab dampened with a 75% isopropyl alcohol solution. To rinse, repeat the same process using a cloth dampened with deionized water. A swab is useful for cleaning in narrow spaces around the connectors. Do not use abrasive compounds on any part of the unit.

Make sure that the air intake area on the left side of the instrument is clear of any obstructions.

Repacking for Shipment

If an instrument is to be shipped to a Tektronix field office for repair, attach a tag to the instrument showing the following:

- Owner's name and address
- Serial number
- Description of the problem(s) encountered and/or service required.

The RFM220 demodulator is shipped in cartons designed to provide it with the maximum protection. If you ship the instrument subsequently, you will need to use these cartons, the spacer pads, the protective bag, and the instrument support inserts to provide adequate protection.

CAUTION. *Tektronix cannot honor the instrument's warranties if the RFM220 demodulator arrives at the service center in a damaged condition. The instrument must be packed in its original carton (and its supporting packaging material) or in such a way as to provide similar protection.*

To prevent the loss of your instrument's warranties, Tektronix strongly recommends that you use an RFM220 shipping carton (that is in good condition) when you ship your instrument to another location or when you return the instrument to a Tektronix service center for repair.

New packaging material is available from Tektronix. To obtain these items, contact your nearest Tektronix office or representative.

Troubleshooting

This section provides some solutions to common RFM220 system problems.

NOTE. *If you need to contact Tektronix about a RFM220 system problem, please provide the version numbers for each component of your RFM220 system. Use the About menu in the RFM220 Client to display the version numbers associated with your system.*

Log Files

To help solve a problem with your RFM220 system, Tektronix may request a copy of your log files. If your logging has been set to a low level such as Info in the Configuration.xml file (See page 22, *Configuring the RFM220 Aggregator*.), Tektronix may request that you change the logging to a higher level such as Debug or Verbose in order to get a better diagnosis of the problem. Except in such support request cases, users are advised to set the logging level to Info.

General Issues

Alarms are not appearing in the event logs. If SNMP alarms are not appearing in the event logs, verify that the SNMP ports that are configured to be used by the Aggregator in the Configuration.xml file are entered as exceptions in the Windows firewall. (See page 31, *Configuring the Windows Firewall*.)

Alarms are not cleared when the Clear Threshold is crossed. Perform the following steps In the event that active alarms are not being cleared when the Clear Threshold set in the Alarm Configuration dialog is being crossed:

1. Resynchronize the alarms by using the RFM220 Client to open the Alarm Configuration dialog, and then click **OK** or **Apply**. If this does not solve the problem, then proceed to the next step.
2. Remove the RFM220 instrument for maintenance. (See page 48, *Performing RFM220 System Maintenance*.)
3. Use the RFM220 Device Setup utility to first reset the instrument to the default settings, and then to reset the instrument.
4. Return the instrument to the RFM220 system. (See page 48, *Performing RFM220 System Maintenance*.)
5. Use the RFM220 Client to retune the input frequency in the channel plan and to change the alarm configuration settings back to the settings required for your input signal. (See page 58, *Edit Settings*.) (See page 63, *Alarm Thresholds*.)

Communication port conflicts. The Aggregator will display the message "An attempt was made to access a socket in a way forbidden by its access permissions" if it detects conflicts with another device on a communication port. To correct this problem, perform the following steps:In this case, you will need to edit the Configuration.xml file to change the communication ports to an unused port number.

1. On the PC or server that is hosting the RFM220 Aggregator, open a command prompt window and enter the following command to view a list of the ports on the PC that are currently in use.

   netstat –anobv

2. Check that none of the listed ports are used in the Configuration.xml file.
3. If a port listed by the netstat command is used in the Configuration.xml file, edit the file to change the port number to an unused port.

SNR alarm will not clear. When a RFM220 instrument is reset, the alarm state for the SNR test is set to true. This is because during the instrument reset, the SNR value is set to 0. If the Aggregator is started after the instrument is reset, it will be observed that the SNR value will go below the threshold with no alarm being reported (because the alarm state is already set to true). The work-around for this situation is to first clear the SNR alarm by setting a lower value for the Clear Threshold, and then later setting new Active and Clear thresholds. Resetting the instrument to the factory default settings will not solve this issue.

Compensation for an external attenuator. If your input signal has an external attenuator, you need to adjust the alarm thresholds to compensate for the attenuator. The Channel Input Level upper threshold will not adjust past the –30 dB maximum.

Windows 7 Issues

Cannot edit the Configuration.xml file because it is read-only. If you attempt to edit the Configuration.xml file for the RFM220 Aggregator and you cannot because the file is read only, there is likely one of the following permission problems:

- The file permissions were not set properly when the RFM220 software was installed. In this case, reinstall the software as described for Windows 7 systems. (See page 15, *Installing the RFM220 Software*.)
- The user who logged in does not have Full Access permissions. In this case, right-click the RFM220 Aggregator and RFM220 Client icons and select **Properties**. Set the access privileges. (See page 34, *Windows 7 Privileges*.)
- The RFM220 application was not started using the "Run as Administrator" command. In this case, stop the application, and then right-click the application icon and select **Run as Administrator**.

Cannot access the RFM220 applications. To operate the RFM220 software on Windows 7 systems, observe the following:

- Install the RFM220 software when you are logged on to the computer with administrative privileges.
- Ensure that the user who is logged onto the computer has Full Access privileges for the RFM220 applications.
- Start the RFM220 applications using the "Run as administrator" command.

Trend graphs are not displayed. If trend graphs are not being displayed by the RFM220 Client on a Windows 7 system, the WCF HTTP and Non-HTTP Activation features in the Microsoft .NET Framework 3.5 software may not be enabled. In this case, open the Windows Features dialog and verify that the features are checked as shown below.

If the features are not checked, enable the features and then reinstall the RFM220 software.

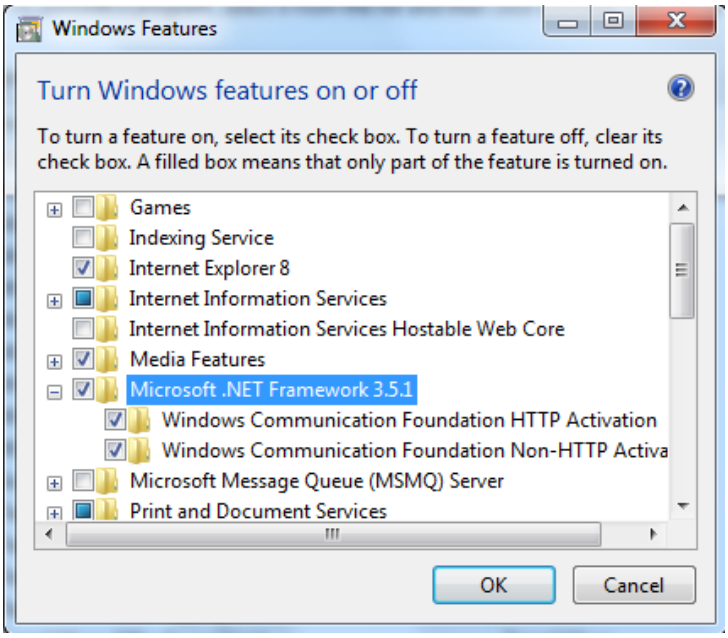


Figure 54: Enabling the WCF HTTP and Non-HTTP activation features

Index

S

T

U

V

W