

Maintaining Data Security

when Using Anritsu Remote Spectrum Monitors and Field Master™ Instruments in the Field

Introduction

Spectrum analyzers and spectrum monitors are now an essential element of security in military, aerospace & defense, and even commercial environments. Establishing and maintaining secure communications with radio technologies requires an awareness of the local RF environment and immediate notification of illegal or hostile signals. Spectrum analyzers are commonly used to set up and maintain critical communications networks and telemetry links for remote sensor monitoring. In these mission critical applications, security of data is a fundamental requirement. Data security encompasses a wide range of requirements including:

- Masking frequency information on the instrument screen
- Preventing information from being stored into memory on the instrument
- Closing digital interface communications ports
- Enabling secure encrypted data tunnels for remote access
- Requiring custom network certificates for remote access
- Removing potentially hackable interfaces such as 802.11 Wi-Fi
- Support of encrypted USB memory devices

To support the use of Anritsu Field Master spectrum analyzers and Remote Spectrum Monitors in the field, Anritsu offers three options to ensure data security at all times.

- Option 6: Remove Wi-Fi and Bluetooth
- Option 7: Secure Data
- Option 17: Secure Communications

Option 6: Remove Wi-Fi and Bluetooth

The standard configuration of the Anritsu Field Master spectrum analyzer includes an 802.11 Wi-Fi interface used for remote instrument control and file transfer to a PC. Field Masters can also connect directly to the internet for digital map downloads and normal web browsing. Many aerospace & defense organizations consider an on-board Wi-Fi module to be a security threat. Disabling by software is not always considered sufficient mitigation. Option 6 physically removes the Wi-Fi module from the instrument in the factory.

Option 7: Secure Data

The secure data option includes a number of changes to the instrument functionality.

For highly secure data handling requirements, Secure Data Option 7 prevents the storing of measurement setup or data information onto any internal file storage location. Instead, setup and measurement information is stored ONLY to the external USB memory location.

For additional security of data stored onto an external USB memory device, the USB ports are compatible with external USB memory devices that have an integrated keypad and are FIPS compliant using AES 256-bit encryption. This helps prevent easy access to data, even if the USB memory device is mislaid.



Figure 1. A Typical FIPS Compliant USB Memory Device with AES 256-bit Encryption

When moving the instrument between locations or to a non-secure site for service or calibration, a factory preset prepares the instrument for transportation. A Factory Reset deletes all user files and system files from the instrument’s internal memory.

Option 7 also allows the user to choose to blank the frequency, amplitude and bandwidth values displayed on the screen by turning on Secure Display toggle included in Advanced settings of the instrument (Figure 3).

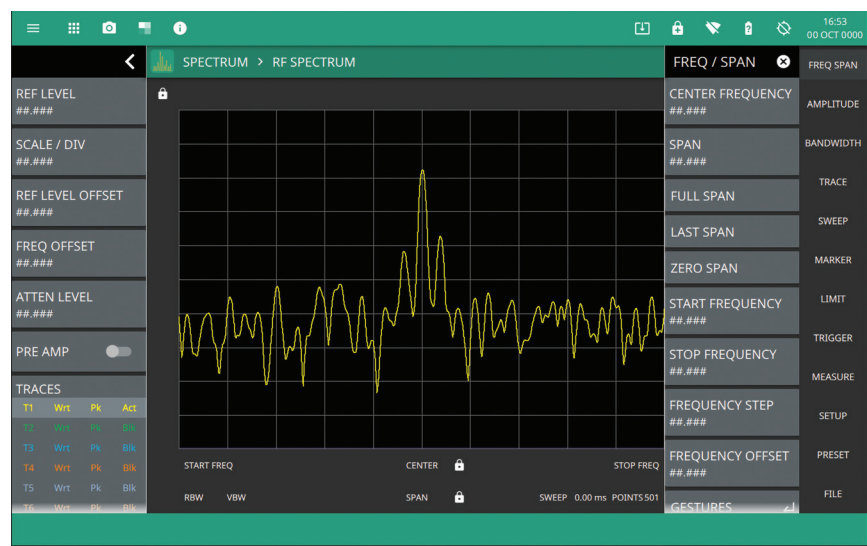


Figure 2. Instrument Screen Display Highlighting the Masking of Critical Parameters including Frequency

A further layer of security is that the SCPI command interface won't be supported when Option 7 is installed and installing Secure Communication Option 17 is required to enable the SCPI interface.

The instrument cannot be switched between secure and non-secure operation by the user once configured for secure data operation.

Option 17: Secure Communications

When connecting the instrument to a network, Option 17 creates a secure tunnel. Some ports are closed, and data on other ports is encrypted as shown in the Table 1 below. Security certificates can be loaded onto the instrument to establish a secure connection. Remote access to the Ethernet ports can be password protected. The USBTMC connection interface does not work on instruments installed with Secure Communication Option 17.

Ports

In order for Anritsu instruments to operate on a network, It needs the ports to be opened as described in Table 1 Under the column "PORT." There are two columns; one is the default state when an instrument does not have Secure Communication (Option 17) installed. The column "with Option 17" describes the port state when the option is installed. This table is true for the following Anritsu products:

MS2090A | MS2070A | MS2080A | MS2085A | MS2089A | MS27201A | MS27200A

The function of each port is defined by the column "service" in Table 1. The instrument will need to have all the ports described to operate correctly.

PORT	SERVICE	DEFAULT STATE	WITH OPTION 17
21 (tcp)	ftp	Open	Closed
80 (tcp)	http	Open	Closed
111 (tcp)	rpcbind	Open	Open
443 (tcp)	https	Open	Open
8001 (tcp)	vcom-tunnel	Open	Closed
8002 (tcp)	vcom-tunnel	Closed	Open (encrypted)
9001 (tcp)	tor-orport	Open	Closed
9002 (tcp)	dynamid	Open	Closed
9003 (tcp)	tor-orport	Closed	Open (encrypted)
9004 (tcp)	dynamid	Closed	Open (encrypted)
24001 (tcp)	med-fsp-rx	Open	Closed
24002 (tcp)	med-fsp-rx	Closed	Open (encrypted)
111 (udp)	rpcbind	Open	Open
123 (udp)	ntp	Open	Open
5353 (udp)	Zeroconf	Open/Filtered	Open

Table 1. Ports Anritsu Instrument Uses and Ports Used When Option 17 is Enabled

Network Security

When Option 17 is installed the network security menu appears as seen in Figure 1. This menu can be accessed from the Menu => Setting => Advanced => Network Security. From here the network certificates can be uploaded and information is displayed.

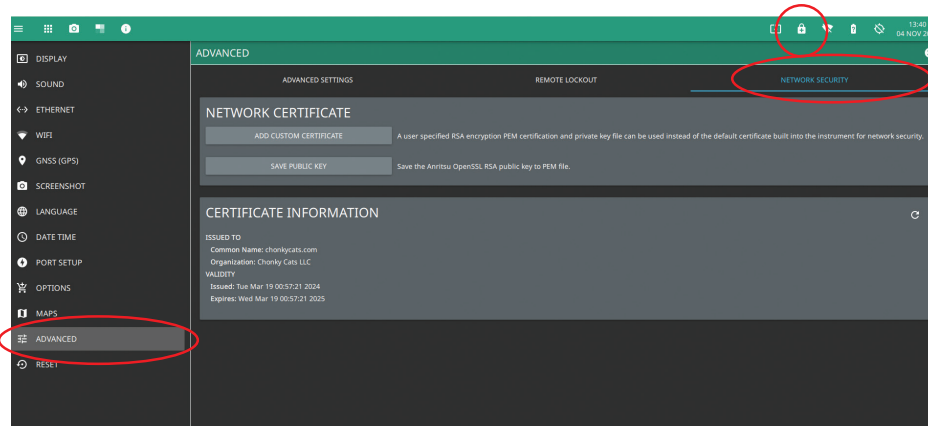


Figure 3. Advance Menu from the ARRT Software

Default Certificate

When an instrument has Option 17 installed, it comes with a default certificate that Anritsu provides. To upload a user defined certificate, the user can go into the network security and select the “Add Custom Certificate” option. The other option is when using the ARRT to select the icon on the top right corner of the window as seen in Figure 2. All certificates are located on the instrument only.

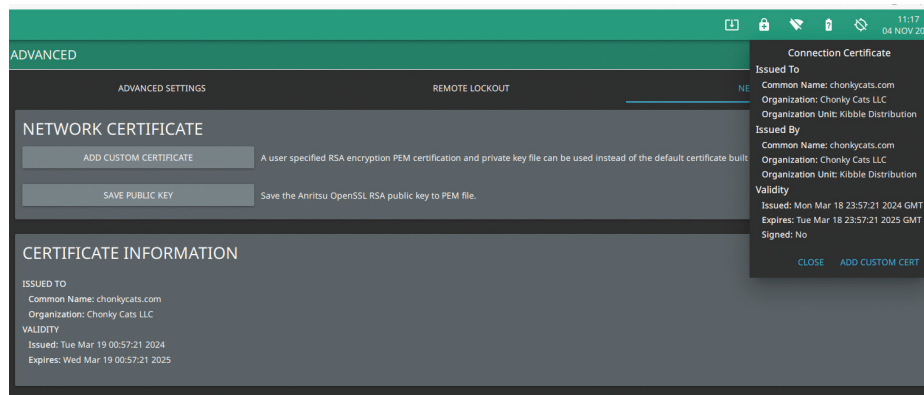


Figure 4. ARRT Showing the Methods of Uploading Certificates

The creation of custom certificates is up to the own customer’s requirements. This is typically done by the customer’s IT department to ensure that it meets all cyber security requirements. During this process the customer would also generate their own private key to match their certificates. Customers would use this to create their software to access the instruments.

Remote Lockout

Option 17 allows the user to see the Remote Lockout menu in advance mode as seen in Figure 3. The remote lockout features allows the user to create a password increase the level of protection. When the remote lock out is enabled the user must enter the correct password before establishing a connection.

Important to Note: Figure 2 shows the button called “Save Public Key”. This public key is for the remote lock out feature. When users are developing their own software and if they have set up a remote password they will need this key to unlock the unit in addition to their own customer certificate.

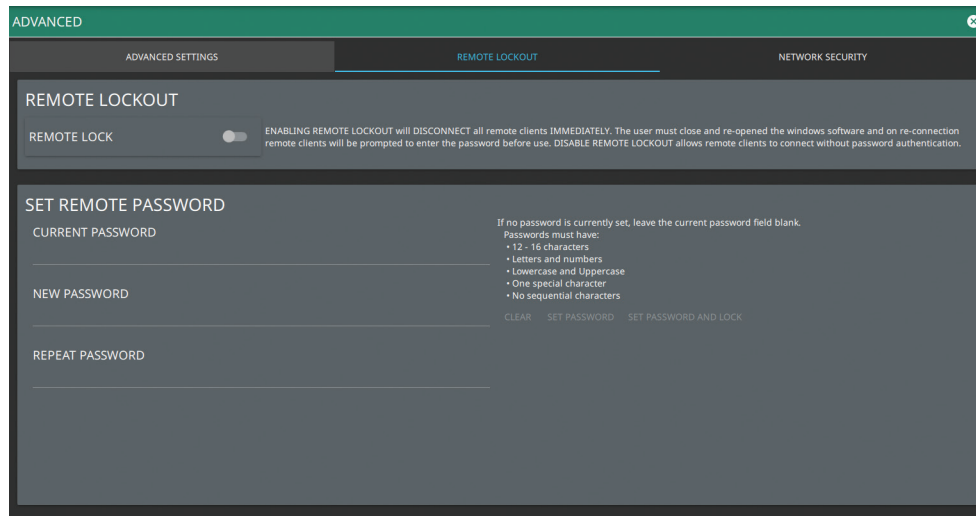


Figure 5. Remote Lockout Menu

Using Instrument with Option 17

Using ARRT

When the instrument is loaded with the correct certificate the ARRT software will be able to connect to the instrument. If there is a password set, entering the correct password will establish a connection to the unit. Please work with the user IT department to make sure ARRT and the certificates on the instrument are correct and allowed.

User Custom Interface

The user needs to have two certificates if the user is using their own interface. The custom certificate is to allow the user to connect to the instrument. The second one is the public key certificate to allow the user to enter the correct password for the remote lock out screen.

The certificate is located on the instrument, allowing the unit to be connected to the user's network without being a cyber security risk. The connection can be further protected with a password to prevent anyone from the network to connect to the instrument.

For customers creating their own interface and not using ARRT they will have to use the two keys to get full access to the unit. The first key is from the creation of their own certificate. The second is the public Anritsu key which can be downloaded from the instrument.

Summary

Data security is now an essential requirement for instrumentation deployed in mission critical applications. Threats from nefarious agents are increasing which is why Anritsu has developed these essential security options. With Options 6, 7, and 17, Anritsu offers the highest level of data security when monitoring the RF spectrum, protecting your data and your investment.



Specifications are subject to change without notice.

• **United States**

Anritsu Americas Sales Company

490 Jarvis Drive, Morgan Hill, CA 95037-2809, U.S.A.
Phone: +1-800-Anritsu (1-800-267-4878)

• **Canada**

Anritsu Electronics Ltd.

Americas Sales and Support

490 Jarvis Drive, Morgan Hill, CA 95037-2809, U.S.A.
Phone: +1-800-Anritsu (1-800-267-4878)

• **Brazil**

Anritsu Eletrônica Ltda.

Praça Amadeu Amaral, 27 - 1 Andar
01327-010 - Bela Vista - São Paulo - SP, Brazil
Phone: +55-11-3283-2511
Fax: +55-11-3288-6940

• **Mexico**

Anritsu Company, S.A. de C.V.

Blvd Miguel de Cervantes Saavedra #169 Piso 1, Col. Granada
Mexico, Ciudad de Mexico, 11520, MEXICO
Phone: +52-55-4169-7104

• **United Kingdom**

Anritsu EMEA Limited

200 Capability Green, Luton, Bedfordshire, LU1 3LU, U.K.
Phone: +44-1582-433200
Fax: +44-1582-731303

• **France**

Anritsu SA

12 avenue du Québec, Immeuble Goyave,
91140 VILLEBON SUR YVETTE, France
Phone: +33-1-60-92-15-50

• **Germany**

Anritsu GmbH

Nemetschek Haus, Konrad-Zuse-Platz 1,
81829 München, Germany
Phone: +49-89-442308-0
Fax: +49-89-442308-55

• **Italy**

Anritsu S.R.L.

Spaces Eur Arte, Viale dell'Arte 25, 00144 Roma, Italy
Phone: +39-6-509-9711

• **Sweden**

Anritsu AB

Kistagången 20 B, 2 tr, 164 40 Kista, Sweden
Phone: +46-8-534-707-00

• **Finland**

Anritsu AB

Technopolis Aviapolis, Teknobulevardi 3-5 (D208.5.),
FI-01530 Vantaa, Finland
Phone: +358-20-741-8100

• **Denmark**

Anritsu A/S

c/o Regus Winghouse, Ørestads Boulevard 73, 4th floor,
2300 Copenhagen S, Denmark
Phone: +45-7211-2200

• **Spain**

Anritsu EMEA GmbH

Representation Office in Spain

Calle Manzanares 4, Primera planta, 28005 Madrid, Spain
Phone: +34-91-572-6761

• **Austria**

Anritsu EMEA GmbH

Am Belvedere 10, A-1100 Vienna, Austria
Phone: +43-(0)1-717-28-710

• **United Arab Emirates**

Anritsu A/S

Office No. 164, Building 17, Dubai Internet City
P. O. Box – 501901, Dubai, United Arab Emirates
Phone: +971-4-3758479

• **India**

ANRITSU INDIA PRIVATE LIMITED

6th Floor, Indique ETA, No.38/4, Adjacent to EMC2,
Doddanekundi, Outer Ring Road, Bengaluru – 560048, India
Phone: +91-80-6728-1300
Fax: +91-80-6728-1301

• **Singapore**

ANRITSU PTE LTD

1 Jalan Kilang Timor, #07-04/06 Pacific Tech Centre
Singapore 159303
Phone: +65-6282-2400
Fax: +65-6282-2533

• **Vietnam**

ANRITSU COMPANY LIMITED

16th Floor, Peakview Tower, 36 Hoang Cau Street, O Cho Dua Ward,
Dong Da District, Hanoi, Vietnam
Phone: +84-24-3201-2730

• **P.R. China (Shanghai)**

Anritsu (China) Co., Ltd.

Room 2301-2303, Tower A, New Caohejing International Business
Center No. 391 Gui Ping Road, Shanghai, 200233, P.R. China
Phone: +86-21-6237-0898
Fax: +86-21-6237-0899

• **P.R. China (Hong Kong)**

ANRITSU COMPANY LIMITED

Unit 1302, 13th Floor, New East Ocean Center,
No.9 Science Museum Road, TsimShaTsui East,
Kowloon, Hong Kong
Phone: +852-2301-4980
Fax: +852-2301-3545

• **Japan**

Anritsu Corporation

8-5, Tamura-cho, Atsugi-shi, Kanagawa, 243-0016 Japan
Phone: +81-46-296-6509
Fax: +81-46-225-8352

• **Korea**

Anritsu Corporation Limited

8F, A TOWER, 20, Gwacheondaero 7-gil, Gwacheon-si,
Gyeonggi-do, 13840, Republic of Korea
Phone: +82-2-6259-7300
Fax: +82-2-6259-7301

• **Australia**

Anritsu Pty Ltd

Unit 20, 21-35 Ricketts Road, Mount Waverley, Victoria 3149, Australia
Phone: +61-3-9558-8177
Fax: +61-3-9558-8255

• **Taiwan**

ANRITSU COMPANY, INC.

7F, No. 316, Sec. 1, NeiHu Rd., Taipei 114, Taiwan
Phone: +886-2-8751-1816
Fax: +886-2-8751-1817

List Revision Date: 20241028



Anritsu utilizes recycled paper and environmentally conscious inks and toner.



© Anritsu All trademarks are registered trademarks of their
respective owners. Data subject to change without notice.
For the most recent specifications visit: www.anritsu.com

11410-02960, Rev. A Printed in United States 2025-05
©2025 Anritsu Company. All Rights Reserved.