

Configuration Quick Start Guide

Remote Spectrum Monitors

MS27100A, MS27101A, MS27102A, MS27103A
9 kHz to 6 GHz

1. Introduction

The following are the topics covered in this Quick Start Guide:

- [“Configuring for Dynamic IP through SCPI Commands”](#)
- [“UDP Discovery Tool”](#)
- [“Secure Mode”](#)
- [“Supplemental Information”](#)

To communicate with the MS2710xA Remote Spectrum Monitor (RSM) or to change its IP configuration, a PC must be correctly set up to communicate with the instrument via a direct connection using a static IP. The sections in this guide explain using:

- A Windows PC to directly communicate with the Anritsu spectrum monitor
- SCPI commands for configuring the Ethernet and DNS settings
- The Anritsu Windows network discovery tool to find the instrument IP address

The remote spectrum monitor is shipped with the following default IP configuration:

- **DHCP:** OFF (Static IP Address)
- **Static IP Address:** 10.0.0.2
- **Static Subnet:** 255.255.255.0
- **Static Gateway:** 10.0.0.1

Read the *MS2710xA Product Information, Compliance, and Safety Guide* (PN: 10100-00064) for important safety, legal, and regulatory notices. For additional information and literature covering your product, visit the product page of your instrument and select the Library tab:

- <https://www.anritsu.com/en-US/test-measurement/products/ms27100a>
- <https://www.anritsu.com/en-US/test-measurement/products/ms27101a>
- <https://www.anritsu.com/en-US/test-measurement/products/ms27102a>
- <https://www.anritsu.com/en-US/test-measurement/products/ms27103a>



2. Configuring for Dynamic IP through SCPI Commands

After the PC is properly configured, the connection can be tested. After a good connection has been confirmed, either SCPI commands or the embedded instrument user interface (UI) may be used to configure the Ethernet settings on the instrument to different values. Refer to the embedded Help for details on using the UI.

Caution

Consult with your network administrator when configuring the network interface to avoid potential loss of access or discovery of the device.

The following steps describe how to verify and set the Ethernet configuration through SCPI programming:

1. Using any SCPI client, send the *IDN? query command to 10.0.0.2 on port 9001. Verify the response includes the model and serial numbers, and other instrument information.

Note

If a response is not returned, try switching to a cross-over Ethernet cable and send the query command again. Ensure that your SCPI client has the termination character enabled: \n Line Feed (xA).

2. To configure the instrument for DHCP, send the following SCPI commands to 10.0.0.2 on port 9001:

```
SYSTem:COMMunicate:LAN:DHCP?
```

Queries the DHCP setting. The return value should be OFF if the instrument is currently configured for static IP.

```
SYSTem:COMMunicate:LAN:DHCP ON
```

Turns the DHCP setting ON. The setting is applied immediately upon sending the command.

3. Turning DHCP ON will change the IP address and the module must then be connected to a DHCP network to obtain a new IP address.
4. Obtain the new IP by one of the following:

Use the Anritsu Discovery program to retrieve the new IP address (see [“UDP Discovery Tool” on page QSG-3](#) for instructions on using the discovery program)

Insert a USB memory device into one of the USB Type-A ports to retrieve the ip.txt file containing the IP address information.

5. Send the *IDN? SCPI command to verify a connection has been established.

3. UDP Discovery Tool

The UDP Discovery Tool is a Windows application that will display a sortable list of available MS2710xA devices on the network. This tool provides the ability to find and filter devices by Hostname, Model number, Serial number, MAC address, Version number, or by IP Address. If needed, the tool also provides the ability to save the results of your search and to view a brief history of your searches for comparison.

<https://www.anritsu.com/en-US/test-measurement/support>

During the download process, a screen will appear as shown in [Figure 1](#).

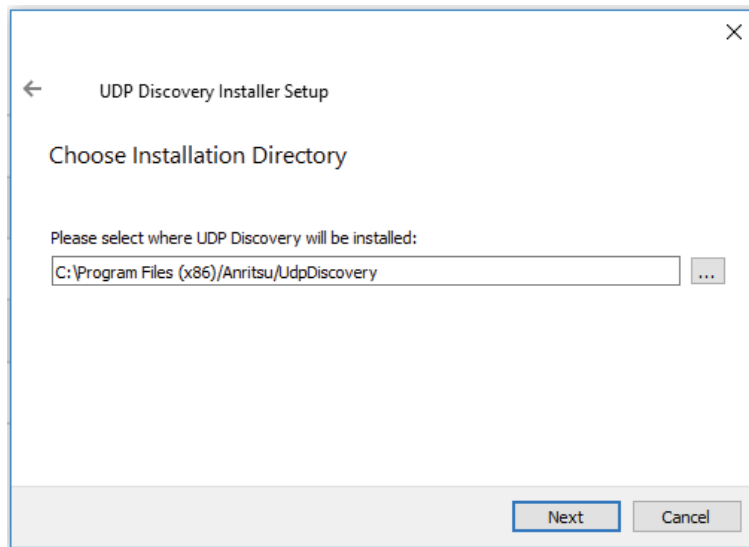
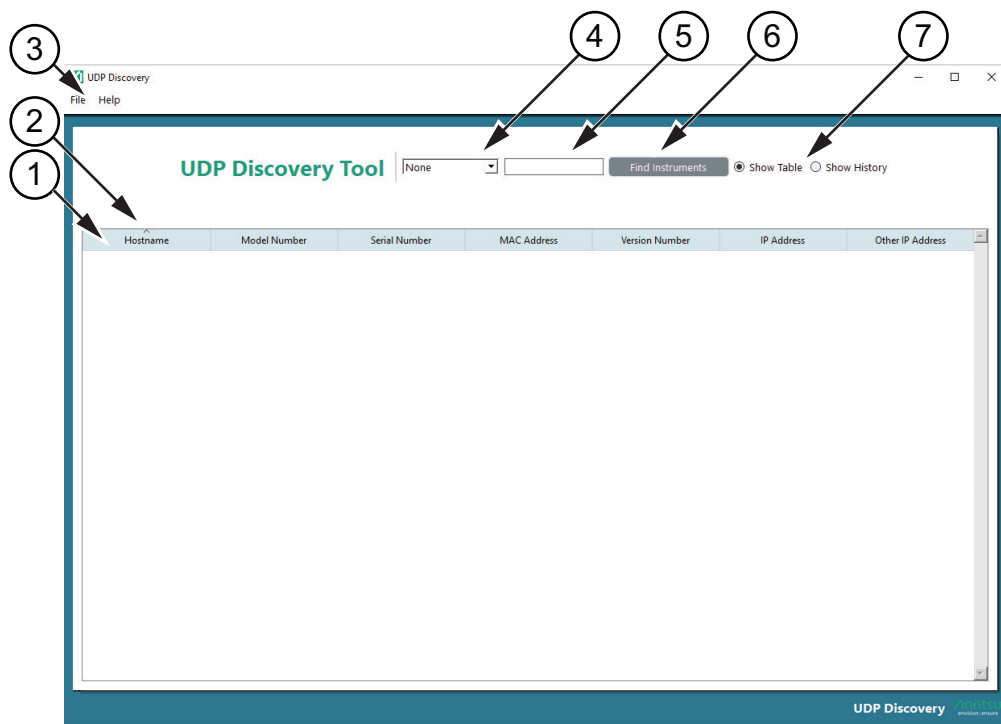


Figure 1. Installation Directory Default Location

3. UDP Discovery Tool

When the download is complete, a user interface will appear as shown in [Figure 2](#).



1. Column Header
2. Column Filter Caret
3. Toolbar
4. Selection Filter List
5. Filter Entry Field
6. Find Instruments Bar
7. Display Type

Figure 2. UDP Discovery Tool User Interface

Communicating with the RSM

There could be many instruments already connected to the network. Use the selection filter to narrow the search results.

Select a filter method

1. Click the connection arrow to display the filter list box are shown in [Figure 3](#).
-

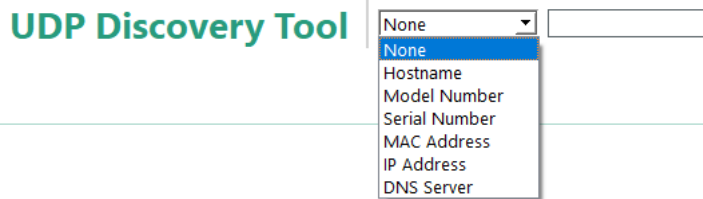


Figure 3. Filter List Box

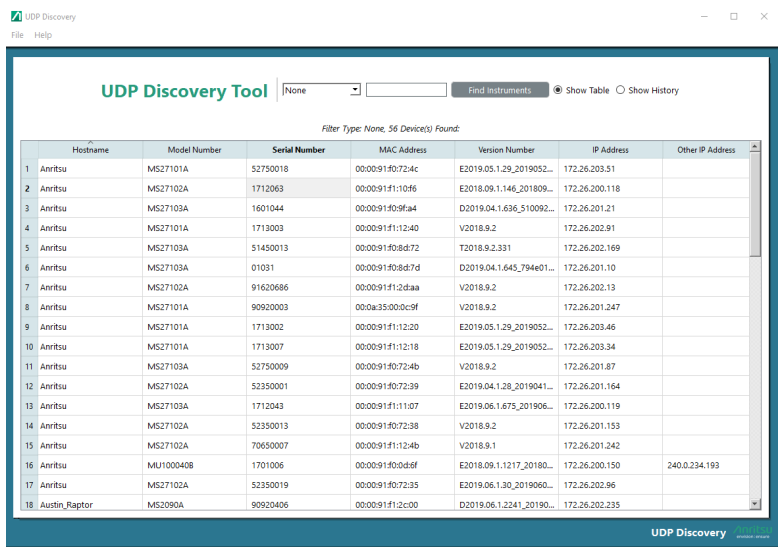
2. Click a filter method from the list. The selections available are None, Hostname, Model Number, Serial Number, Mac Address, IP Address, IP Address, and DNS Server.

If a Hostname, Model Number, Serial Number, Mac Address, IP Address, IP Address, or DNS Server is not known, select None.

- None: All instruments attached to the local area network will be listed.
- Hostname: Host name of the probe
- Model Number: Model Number of the probe
- Serial Number: Serial Number of the probe
- MAC Address: Medium Access Control (MAC) address
- IP Address: Internet Protocol (IP) address
- DNS Server: Domain Name System (DNS) server

3. UDP Discovery Tool

3. Click None to display an alphabetical listing of the inventoried instruments available to connect as shown in Figure 4.



The screenshot shows the 'UDP Discovery Tool' window. At the top, there's a title bar and a menu bar with 'File' and 'Help'. Below the menu bar, there's a toolbar with a dropdown menu set to 'None', a text input field, and buttons for 'Find Instruments', 'Show Table', and 'Show History'. A status bar at the top of the table area reads 'Filter Type: None, 56 Device(s) Found:'. The table itself has columns for Hostname, Model Number, Serial Number, MAC Address, Version Number, IP Address, and Other IP Address. It lists 18 devices, mostly 'Anritsu' models MS27101A and MS27102A, with one 'Austin_Raptor' model MS2090A at the bottom.

	Hostname	Model Number	Serial Number	MAC Address	Version Number	IP Address	Other IP Address
1	Anritsu	MS27101A	52750018	00:00:91:f0:72:4c	E2019.05.1.29_2019052...	172.26.203.51	
2	Anritsu	MS27102A	1712063	00:00:91:f1:10:f6	E2018.09.1.146_201809...	172.26.200.118	
3	Anritsu	MS27103A	1601044	00:00:91:f0:9f:a4	D2019.04.1.636_510092...	172.26.201.21	
4	Anritsu	MS27101A	1713003	00:00:91:f1:12:40	V2018.9.2	172.26.202.91	
5	Anritsu	MS27103A	51450013	00:00:91:f0:8d:72	T2018.9.2.331	172.26.202.169	
6	Anritsu	MS27103A	01031	00:00:91:f0:8d:7d	D2019.04.1.645_794e01...	172.26.201.10	
7	Anritsu	MS27102A	91620686	00:00:91:f1:3d:aa	V2018.9.2	172.26.202.13	
8	Anritsu	MS27101A	90920003	00:0a:35:00:0c:9f	V2018.9.2	172.26.201.247	
9	Anritsu	MS27101A	1713002	00:00:91:f1:12:20	E2019.05.1.29_2019052...	172.26.203.46	
10	Anritsu	MS27101A	1713007	00:00:91:f1:12:18	E2019.05.1.29_2019052...	172.26.203.34	
11	Anritsu	MS27103A	52750009	00:00:91:f0:72:4b	V2018.9.2	172.26.201.87	
12	Anritsu	MS27102A	52350001	00:00:91:f0:72:39	E2019.04.1.28_2019041...	172.26.201.164	
13	Anritsu	MS27103A	1712043	00:00:91:f1:11:07	E2019.06.1.675_201906...	172.26.200.119	
14	Anritsu	MS27102A	52350013	00:00:91:f0:72:38	V2018.9.2	172.26.201.153	
15	Anritsu	MS27102A	70650007	00:00:91:f1:12:4b	V2018.9.1	172.26.201.242	
16	Anritsu	MU1000408	1701006	00:00:91:f0:0d:6f	E2018.09.1.1217_20180...	172.26.200.150	240.0.234.193
17	Anritsu	MS27102A	52350019	00:00:91:f0:72:35	E2019.06.1.30_2019060...	172.26.202.96	
18	Austin_Raptor	MS2090A	90920406	00:00:91:f1:2c:00	D2019.06.1.2241_20190...	172.26.202.235	

Figure 4. Displayed Instrument Inventory

Sorting the Listing

Selecting a column header displays a filter caret above column header as shown in Figure 2. When the caret is clicked, the listing is sorted by the column in the direction the caret is pointing. Clicking the caret again reverses the caret direction and sorts the listing in reverse order.

Copy and Paste Example

In this example, refer to the listing in Figure 4.

- 1. Click serial number 1713003.
- 2. Copy the serial number.
- 3. Paste the serial number in the box to the right of the filter list.
- 4. Click the Find Instruments bar. If the instrument is located, the instrument details will be displayed as shown in Figure 5.

A status readout is displayed above the column headings. In this example, the readout is:
Filter Type: Serial Number, Filter Value: 1713003, 1 Device(s) Found:
If the device could not be found, the last section would read: *No Device Found*

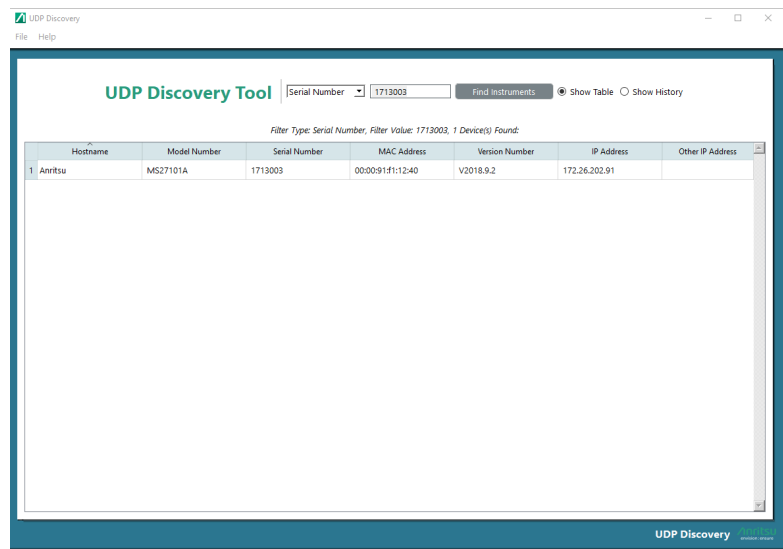


Figure 5. Locate Instrument

Connecting another device will erase the Show Table log and display the new device details. The previous erased device details will be available in the Show History log until the history details are erased. See [“Clearing the History”](#) on page QSG-9.

3. UDP Discovery Tool

User Interface Display Types

The selectable radio buttons provide the **Show Table** and **Show History** user interface connection display.

Show Table : Click this radio button to display the device connection details as shown in [Figure 5](#).

Show History : Click this radio button to display current and previous connection-activity details as shown in [Figure 6](#).

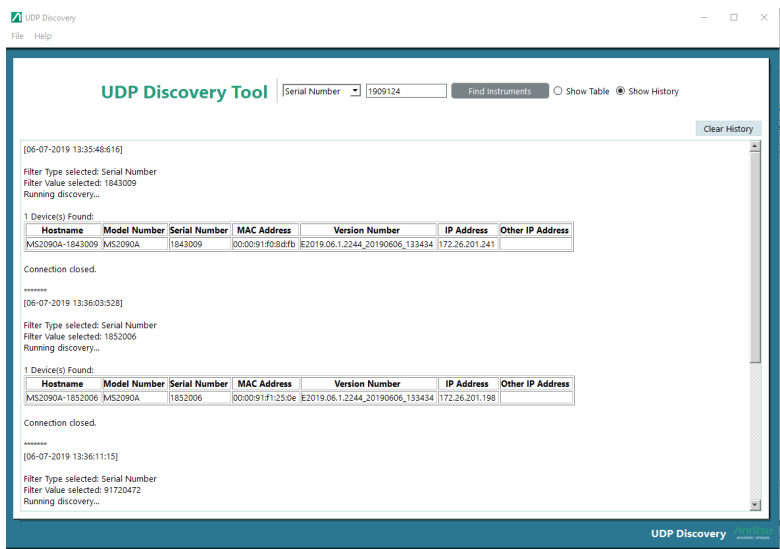


Figure 6. Show History

4. Secure Mode

Overview

Secure Mode prevents unauthorized access to both the setup parameters and measurement data stored on the monitor. The following sections detail the method and commands for securing a Remote Spectrum Monitor (RSM). Steps are listed to turn On or Off the Secure Mode for the desired remote spectrum monitor. Placing the RSM in secure mode requires a password. Users should determine that password before going through the setup. The default password is described in Setup Step 5. Communication to the RSM is done through port 8001. Port 8001 is always available whether Secure Mode is on or off.

A command is also provided to reset passwords to default. If this command is used, all setup parameters and measurement data stored on the RSM unit will be cleared. This ensures that unauthorized users will not have access to this information if they are able to gain physical access to the monitor. The secure mode will be off.

To communicate to the RSM unit, you must download Anritsu RSM Secure Mode.zip from the Anritsu website. This allows you to run the utility script, **Anritsu RSM Secure Mode.exe**, that communicates with the remote spectrum monitor.

Setup

Utility Program

1. Download from the Anritsu website Anritsu RSM Secure Mode.zip. Unzip the file on to your computer.
2. Insure you are connected to the remote spectrum monitor either via Ethernet or wireless. You will need to know either the monitor's IP address or DNS name.
3. Double-click **Anritsu RSM Secure Mode.exe** to run the utility script. Insure that all the unzipped files are in the same directory. The following command window opens.

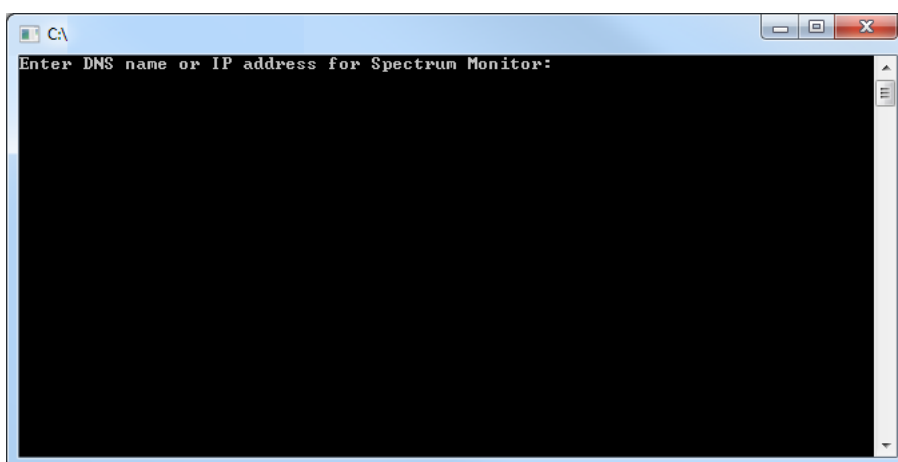


Figure 9. Command Window for Secure Mode

4. At the prompt, enter the DNS name or the IP address of the remote spectrum monitor.

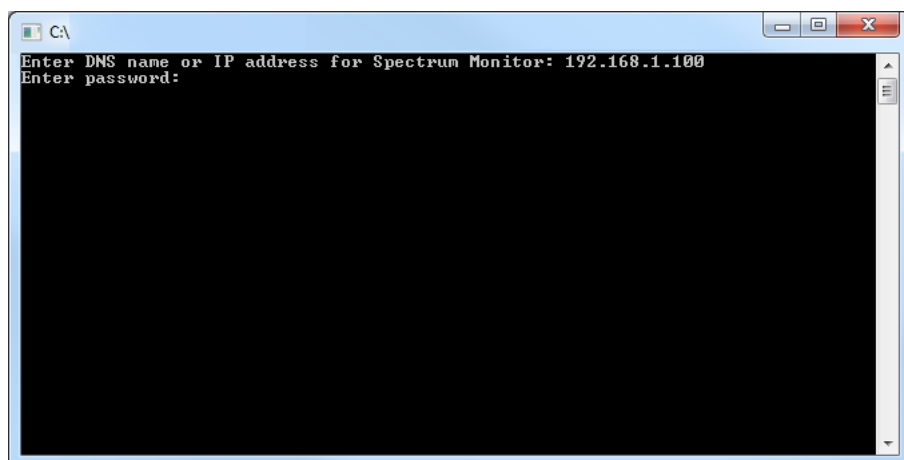


Figure 10. Command Window Waiting for Password

5. Enter the default password if setting up Secure Mode for the first time. The default password is a combination of the RSM MAC address and the word “system”. For example, if the MAC address is 00:00:82:e1:63:40, the password is **00s00y82se1t63e40m**. Successfully entering the password will return the following response and Secure Mode commands shown in [Figure 11](#). The MAC address can be found on a label on the RSM unit.

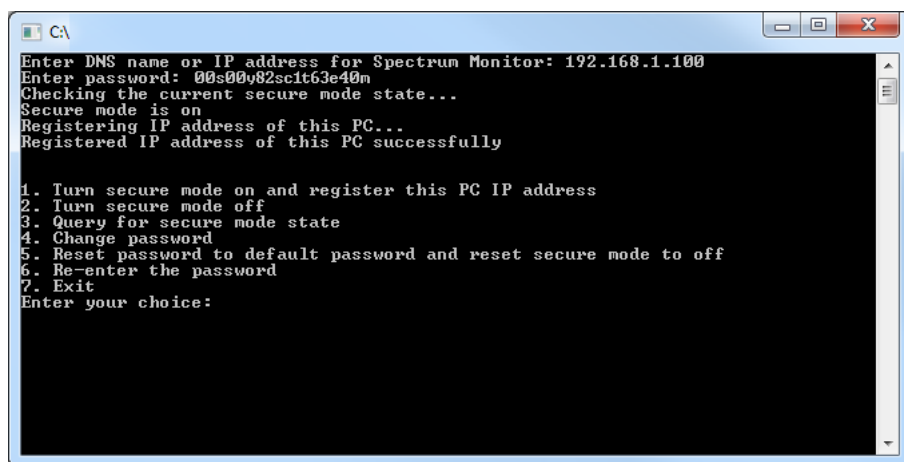


Figure 11. Command Window with the Default Password Entered

6. Enter the number of the desired command to execute the corresponding action. The [“Commands” on page QSG-12](#) illustrate what happens when a specific number in the command window is entered.
7. To end the Secure Mode, enter **7** to exit the **Anritsu RSM Secure Mode** utility script.

4. Secure Mode

Commands

set_secure_mode,<system override password>,<on/off>

Description: Sets Secure Mode on or off. Responds with “ok” if secure mode has been successfully turned ON or OFF. If secure mode is OFF, sending “on” turns secure mode ON (blocking all users not on the whitelist from accessing any port except 8001) and adds the user to a whitelist. If secure mode is ON already and the user sends “on”, the user is simply added to the whitelist. Sending “off” triggers a master reset and unblocks ports for all users. Responds with “password_match_fail” if provided System Override password is incorrect. Responds with “command_match_fail” if “on” or “off” is not sent. The maximum number of registered clients is 100. Responds with “exceeded_max_secure_mode_users_fail” if max number of secure mode users have already been reached prior to the command being sent.

Parameters: <system override password>,<on or off>

Syntax Example: set_secure_mode,<demopassword>,<on>

force_reboot,<system override password>

Description: Reboots the remote spectrum analyzer. Responds with “ok” if command is accepted. A response of “password_match_fail” is returned if the provided System Override password is incorrect.

Parameters: <system override password>

Syntax Example: force_reboot,<demopassword>

change_password,<System Override Password>,<New Password>

Description: Changes the System Override Password. A response of “ok” if password has successfully been changed.

- “password_match_fail” is returned if the provided System Override password is incorrect.
- “command_match_fail” is returned if the new password is empty.
- “password_over_50_characters_fail” is returned if the password length is greater than 50 characters.

Parameters: <system override password>,<new password>

Syntax Example: change_password,<demopassword>,<newdemopassword>

reset_password

Description: Resets the System Override password back to the default value. A response of “ok” is returned when the password has successfully been reset.

Parameters: None

Syntax Example: `reset_password`

query_secure_mode_state

Description: Retrieves secure mode state, ON or OFF. A response of “on” is returned if secure mode is ON or “off” if secure mode is OFF.

Parameters: None

Syntax Example: `query_secure_mode_state`

5. Supplemental Information

Configuring for Static IP through SCPI Commands

To change from DHCP to Static IP, send these commands to port 9001 of the instrument's dynamic IP address:

1. Set the static values of the Ethernet configuration that are used when DHCP is OFF:

```
SYSTem:COMMunicate:LAN:CONFig <Static IP>,<Static Gateway>,  
<Static Subnet>
```

The <Static IP>, <Static Gateway>, and <Static Subnet> must be enclosed in quotes like the following example:

```
SYST:COMM:LAN:CONF "124.168.1.1","124.168.1.0","255.255.255.0"
```

2. Confirm the static IP settings by querying the static Ethernet configuration:

```
SYSTem:COMMunicate:LAN:CONFig?
```

3. Turn off DHCP and set the instrument to static IP mode:

```
SYSTem:COMMunicate:LAN:DHCP OFF
```

4. Reboot the instrument.

FTP Access

A FTP server has been included in the instrument to allow user access to files stored on the instrument or in a USB drive connected to the instrument. To access the FTP server, use a FTP client of choice and enter the IP address of the instrument as the host. The user name is "ftp" and the password is the serial number of the instrument. The serial number can be obtained through SCPI using the "*IDN?" command.

System Override

In the event that the instrument does not respond to SCPI commands (due to circumstances like a long sweep used in conjunction with *OPC?) and needs to be reset remotely, the system override feature can be used. System override can be accessed through TCP port 8001 of the instrument. All commands except a password reset will require the instrument's password to be sent. The default password for an instrument is the MAC address interleaved with the word "system" between MAC address pairs. As an example, an instrument with the MAC address "1a:2b:3c:4d:5e:6f" will have a default password of "1as2by3cs4dt5ee6fm". Currently, system override only supports three commands as described below:

1. Reboot the instrument:

To reboot the instrument, send the following string to the instrument through port 8001:

```
"force_reboot,<instrument_password>"
```

Replace <instrument_password> with the password of the instrument. After the command has been sent, the instrument will respond with "ok" if the command has been successfully processed. If the password is incorrect, "password_match_fail" will be returned.

2. Set a new password:

To set a new password for the instrument, the following string should be sent through port 8001:

```
"change_password,<old_instrument_password>,<new_instrument_password>"
```

Note that the max length of a password is 50 characters. If the new password has been successfully set, "ok" will be returned. If the password is too long, a "password_over_50_characters_fail" will be returned. If the old password does not match, a "password_set_fail" message will be returned.

3. Reset the password:

In the case where the system override password needs to be reset to default, the following command can be sent through port 8001:

```
"reset_password"
```

Note that this command DOES NOT require the instrument password. If the password has been successfully reset, "ok" will be returned.

If an improperly formatted command is sent to the instrument, a "command_match_fail" will be sent back.



10580-00414



E



Anritsu utilizes recycled paper and environmentally conscious inks and toner.

Anritsu Company
490 Jarvis Drive
Morgan Hill, CA 95037-2809
USA
<http://www.anritsu.com>