Venable Instruments

Instrument Security Procedures

for
Analyzer Models:
43xx, 63xx, 74xx, 88xx, 9x50 and 350c

Version 2.0

Table of Contents

Contents

Summary

The Venable Frequency Response analyzers contain 3 levels of data clearing and declassification. The memory sanitization procedures are designed for customers who need to meet the requirements specified by the US Defense Security Service (DSS). These requirements are outlined in the "Clearing and Sanitization Matrix" issued by the Cognizant Security Agency (CSA) and referenced in National Industrial Security Program Operating Manual (NISPOM) DoD 5220.22M ISL 01L-1 section 8-301.

Level 1: CLEAR DATA
Clears the Non-Volatile memory area used to store measurement data. No other memory areas are affected.

Level 2: SANITIZE
Clears all Non-Volatile memory as described in this manual, except for memory containing boot code and unit configuration data necessary to allow the end-user to reload firmware and calibration data back into the analyzer to bring it back to an operational state.

Level 3: SANITIZE
Clears all Non-Volatile memory as described in this manual, including memory containing boot code and unit configuration data. Level 3 will require the instrument to be sent to Venable Instruments to be reloaded with firmware, reinitialized and reloaded with calibration data.

Analyzer Firmware Requirements

Sanitization capability only exists in firmware released after December 2014. This consists of the following versions:

Bootloader Firmware:	1.5 or later
Communication Firmware:	2.1 or later, if running version 2.x 1.2 or later, if running version 1.x
Application Firmware:	4.0 or later 3.2 or later, if running version 3.x 2.5 or later, if running version 2.x 1.7 or later, if running version 1.x
Digital Interface Firmware (88xx only):	2.1 or later

Use the ver? button on the analyzer control menu in the Venable Stability Analysis software to determine the firmware versions loaded on your analyzer. Contact Venable Instruments to obtain a firmware update tool, with the latest firmware files, if your analyzer requires an update.

For analyzers running Application Firmware version 5.0 or later, Table 1a supercedes Table 1. Refer to Table 1a instead.

Instrument Memory

This section contains information on the types of memory available in your instrument. It explains the size of memory, how it is used, its location, volatility, and the sanitization procedure.

Table 1. Summary of Instrument Memory - Base Instrument

Memory Type and Size	Location	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose	Sanitization Procedure
Dual-Port RAM (SDRAM) 8 KBytes	MPC855T Processor	Yes	No	Firmware Operations	Cycle power
Data Cache (SDRAM) 4 KBytes	MPC855T Processor	Yes	No	Firmware Operations	Cycle power
Instruction Cache (SDRAM) 4 KBytes	MPC855T Processor	Yes	No	Firmware Operations	Cycle power
CPM ROM	MPC855T Processor	No	Yes	Operational code. Programmed only by processor manufacturer.	N/A
Operations Memory (SDRAM) 64 MBit	SDRAM64MBX16	Yes	No	Firmware Operations	Cycle power
Boot ROM (Flash) 64 MBit	M29W640	No*	Yes	Boot loader for Main Processor MPC855T	See Procedure
Instrument Memory (FLASH) 32 MBit	AT45DB321D-SU	Yes	Yes	Stores program S/W, user settings, calibration data and measurement data.	See Procedure
Program Memory (FLASH) 32 KByte	PIC 18F4550 Processor	No*	Yes	Stores program S/W for communication interface	See Procedure
Operations Memory (SRAM) 2 KByte	PIC 18F4550 Processor	Yes	No	Firmware Operations	Cycle power
Config Memory ROM (EEPROM) 256 Bytes	PIC 18F4550 Processor	No	Yes	Not used	N/A
Programmable Registers (SRAM)	NAT9914BPL	No	No	GPIB configuration control	Cycle power

* This memory can be modified using the Venable Instruments firmware update tool.

Table 1a. Summary of Instrument Memory - Base Instrument

Memory Type and Size	Location	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose	Sanitization Procedure
Dual-Port RAM (SDRAM) 256 KBytes	ZYNQ 7007S Processor	Yes	No	Firmware Operations	Cycle power
Data Cache (SDRAM) 32 KBytes	ZYNQ 7007S Processor	Yes	No	Firmware Operations	Cycle power
Instruction Cache (SDRAM) 32 KBytes	ZYNQ 7007S Processor	Yes	No	Firmware Operations	Cycle power
L2 Cache 512 KBytes	ZYNQ 7007S Processor			Firmware Operations	Cycle power
Boot ROM 128 KBytes	ZYNQ 7007S Processor	No	Yes	Operational code. Programmed only by processor manufacturer.	N/A
Programmable Logic	ZYNQ 7007S Processor		No	Expanded circuitry	Cycle power
Operations Memory (DDR3 RAM) 64 MBit	MT41K64M16TW -107	Yes	No	Firmware Operations	Cycle power
Boot ROM (Flash) 128 MBit	S25FL128SAGBH I200	No*	Yes	Boot loader and Application for Main Processor ZYNQ 7007S	See Procedure
Instrument Memory (FLASH) 32 MBit	AT45DB321D-SU	Yes	Yes	Stores program S/W, user settings, calibration data and measurement data.	See Procedure
Program Memory (FLASH) 32 KByte	PIC 18F4550 Processor	No*	Yes	Stores program S/W for communication interface	See Procedure
Operations Memory (SRAM) 2 KByte	PIC 18F4550 Processor	Yes	No	Firmware Operations	Cycle power
Config Memory ROM (EEPROM) 256 Bytes	PIC 18F4550 Processor	No	Yes	Not used	N/A
Programmable Registers (SRAM)	NAT9914BPL	No	No	GPIB configuration control	Cycle power

* This memory can be modified using the Venable Instruments firmware update tool.

Table 2. Summary of Additional Instrument Memory – **Model series 88xx only**

Memory Type and Size	Location	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose	Sanitization Procedure
Program Memory (FLASH) 64 KByte	TI TMS320F2808 Processor	No*	Yes	Stores program S/W	See Procedure
Boot ROM 4 KByte	TI TMS320F2808 Processor	No	Yes	Boot code installed by processor manufacturer	N/A
Operation Memory (SRAM) 18 KByte	TI TMS320F2808 Processor	Yes	No	Firmware Operations	Cycle power

* This memory can be modified using the Venable Instruments firmware update tool.

Procedures:

Level 1: CLEAR DATA

Data clear is initiated by sending the GPIB command "SANITIZE,1" to the analyzer. This command will erase the sectors of flash program memory that stores measurement data. This memory is loaded with measurement data through the use of the "STORE" GPIB command. This function is accomplished by performing a chip sector erase on the relevant sectors and followed with programming the security value, 0x55 (U), into all associated memory locations. Front panel LEDS will flash in sequence from left to right during the programming phase of the security value. When data clearing is complete, all front panel LEDS will transition to a constant "on" state. If the LEDS do not complete all transition states stated above, the data clearing should not be considered complete. Power the analyzer off for at least 30 seconds to clear volatile memory. This action can be repeated.

Level 2: SANITIZE

Level 2 sanitization is initiated by sending the GPIB command "SANITIZE,22" to the analyzer. The operational state of the analyzer can be restored by the customer without requiring the unit to be sent to the manufacturer. Contact Venable instruments to obtain the necessary software tools to restore firmware to a sanitized analyzer.

Instrument Memory (flash):
All sectors of flash program memory are erased except the sector that contains the analyzer configuration data. The configuration data consists of data that define the analyzer model and serial number, as well as interface address information. User configuration settings are also stored here. Sanitization is accomplished by performing a chip sector erase on the relevant sectors and followed with programming the security value, 0x55 (U), into all associated memory locations.
Front panel LEDs will be set to a constant state with every other LED in the "on" state during the erase phase. Front panel LEDS will flash in sequence from left to right during the programming phase of the security value.

Boot ROM (flash):

Application Firmware version 5.0 or later:

Erases all memory, except the files required for bootloading. Sanitization is accomplished by performing an erase of non-bootload sectors and followed with programming the security value, 0x55 (U), into all associated memory locations. Front panel LEDs will be set to a constant state with every other LED in the "on" state during the erase phase. Front panel LEDS will flash in sequence from right to left during the programming phase of the security value.

Application Firmware version 4.x or earlier:

Boot ROM is not erased. This area can only be written during a firmware update procedure, a process that loads data from a remote computer into the flash memory of the instrument.

Communications Processor (flash):
Writes the security value to Flash Blocks 0, 1, 2 and all of the Boot Block except for the bootstrap loader and sanitization routine in the first 384 bytes. Flash Block 3, which contains bootload code, is write protected and cannot be modified. Flash Block 3 can only be modified at the factory.

Digital Processor (flash): ***[Model 88xx only]***
All sectors of flash program memory are erased, except the boot sector containing the bootload code. Sanitization is accomplished by performing a chip sector erase on the relevant sectors and followed with programming the security value, 0x55 (U), into all associated memory locations.

When sanitization is complete, all front panel LEDS will transition to a constant "on" state. If the LEDS do not complete all transition states stated above, the sanitization should not be considered complete. Power the analyzer off for at least 15 seconds to clear volatile memory.

Note: It is possible that the firmware update utility could be used to upload arbitrary data into any memory devices above. It is also possible, although extremely unlikely, that a specialized remote application could write data into free areas of the Flash via the instrument's ethernet interface. The procedures for doing this are not available to users, but could possibly be "hacked" by a highly skilled and determined individual. This would allow a small amount of arbitrary data to be concealed into areas of the memory devices.

Level 3: SANITIZE

Level 3 sanitization is initiated by sending the GPIB command "SANITIZE,333" to the analyzer. Sanitization using this level requires the analyzer to be sent to the manufacturer to be reloaded with firmware.

Instrument Memory (flash):
All flash program memory is erased. Sanitization is accomplished by performing a full chip erase and followed with programming the security value, 0x55 (U), into all associated memory locations. Front panel LEDs will be set to a constant state with every other LED in the "on" state during the erase phase. Front panel LEDS will flash in sequence from left to right during the programming phase of the security value.

Boot ROM (flash):
All Boot ROM is erased. Sanitization is accomplished by performing a full chip erase and followed with programming the security value, 0x55 (U), into all associated memory locations. Front panel LEDs will be set to a constant state with every other LED in the "on" state during the erase phase. Front panel LEDS will flash in sequence from right to left during the programming phase of the security value.

Communications Processor (flash):
Writes the security value to Flash Blocks 0, 1, 2 and the Boot Block. Flash Block 3, which contains bootload code, is write protected and cannot be modified. Flash Block 3 can only be modified at the factory.
NOTE: In the event that this does not meet your security requirements, the analyzer will need to be opened up and chip U3 on the main board, P/N 102027 will need to be removed. Perform this step after completing the level 3 sanitization. It is recommended that the chip be removed by cutting the pins near the top, closest to the chip, and leaving pins soldered to main board. Damage to main board will incur additional replacement cost.

Digital Processor (flash): ***[Model 88xx only]***
All sectors of flash program memory are erased, *including the boot sector containing the bootload code*. Sanitization is accomplished by performing a chip sector erase on all sectors and followed with programming the security value, 0x55 (U), into all associated memory locations.

When sanitization is complete, all front panel LEDS will transition to a constant “on” state. If the LEDS do not complete all transition states stated above, the sanitization should not be considered complete. Power the analyzer off for at least 15 seconds to clear volatile memory.

How to send GPIB commands to the Analyzer

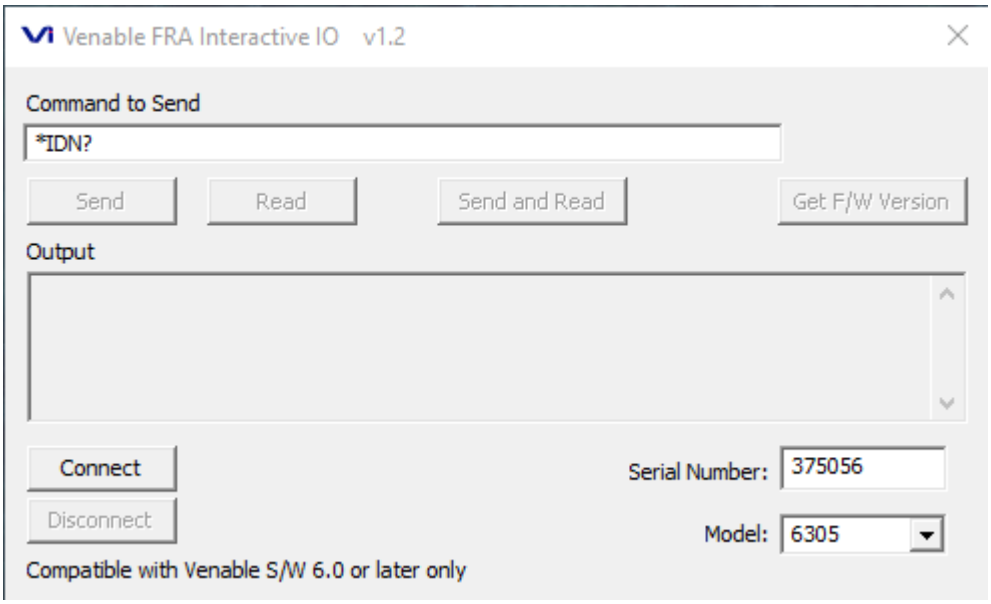
Turn on analyzer power.
Wait for analyzer to finish boot up.

Connect USB cable to back of analyzer. Or, Connect GPIB cable for firmware version 1.x and skip to “Using National Instruments Tools”.

If you are using Venable Software version 6.0 or later, refer to the section on “Using the Venable FRA Interactive IO Tool”. Otherwise, refer to the sections for Keysight/Agilent or National Instruments Tools, depending on which driver set you are using.

Using the Venable FRA Interactive IO Tool
(Venable S/W ver. 6 or later)

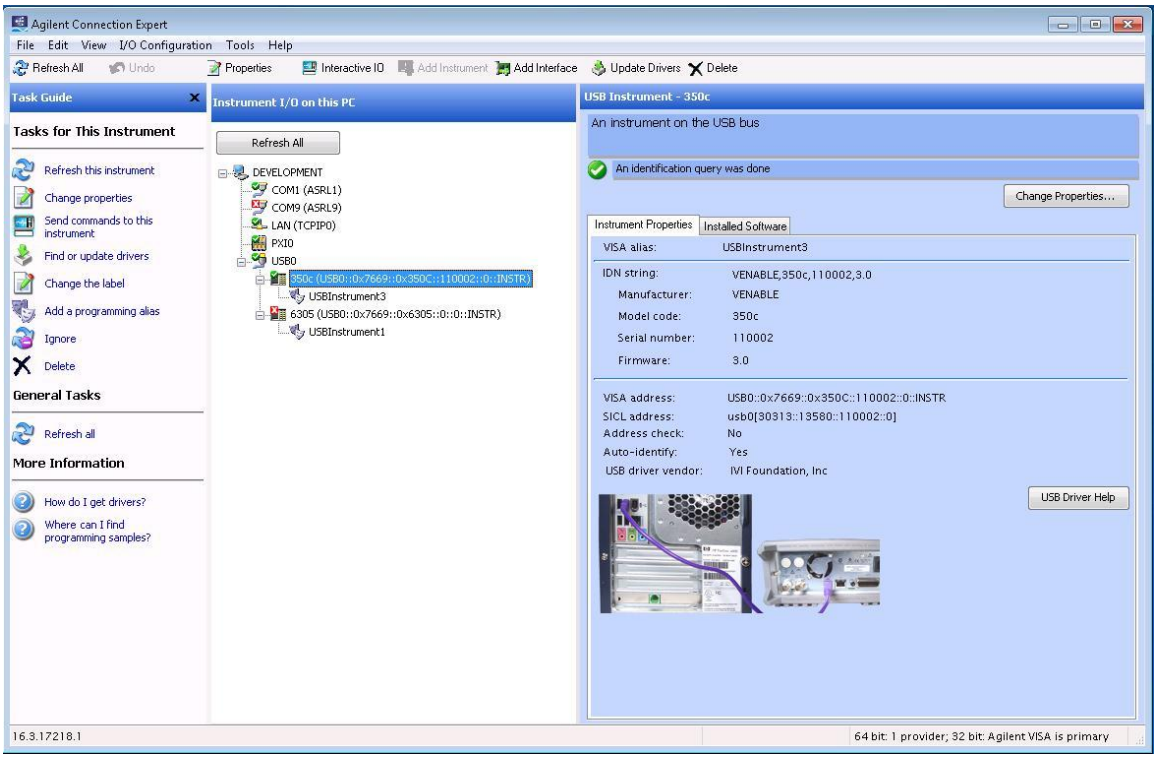
Open the Venable FRA Interactive IO tool from the Windows Start Menu.
Enter the instrument Serial Number and select the Model number of the FRA. Click on the “Connect” button.



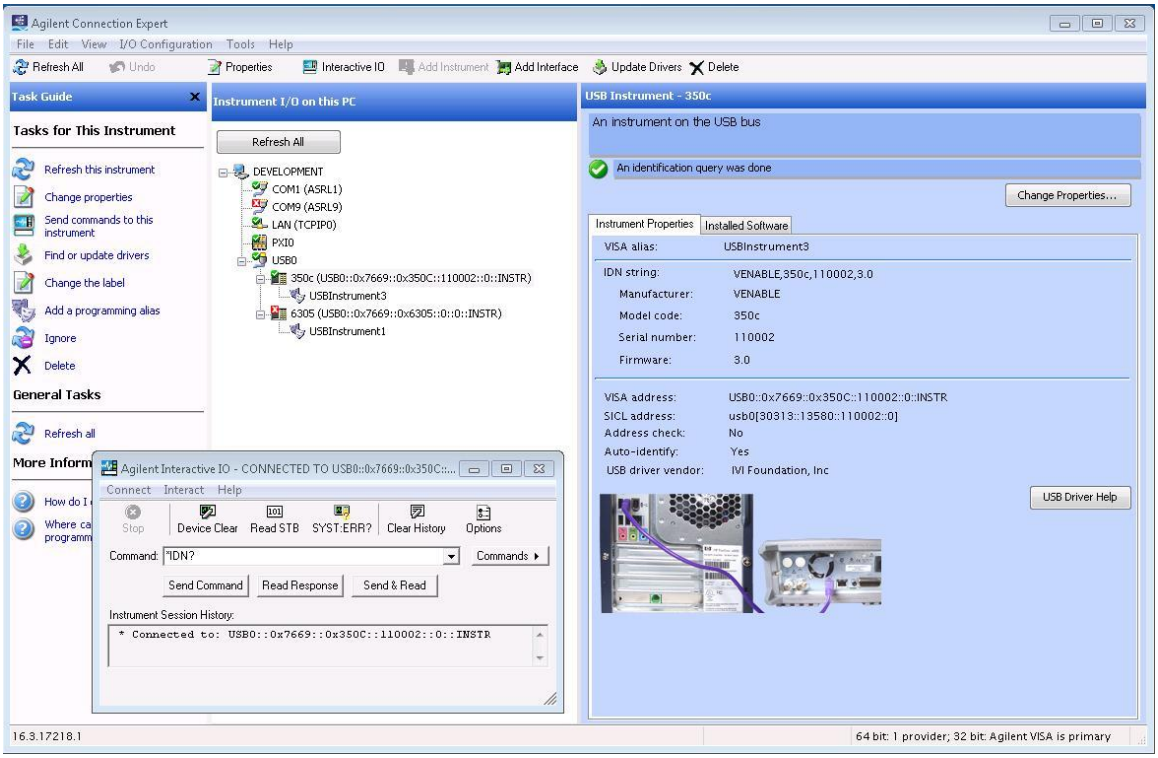
Wait for Output to say “Connected”. Enter the Command to Send and then click on the “Send” button.

Using Keysight (Agilent) Tools

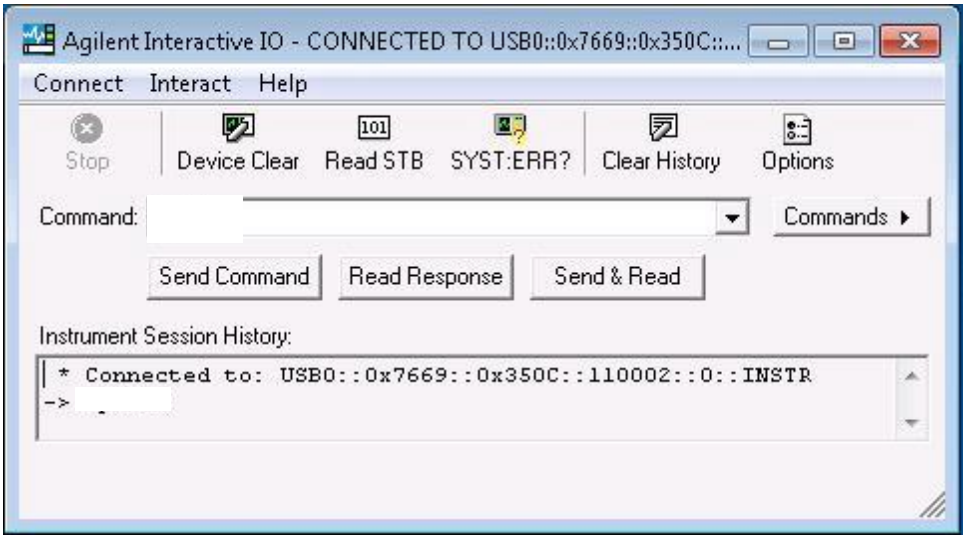
Open the Keysight/Agilent “Connection Expert” application.
Select your instrument in the list.



Click on “Interactive IO” tab, to open a communication window.

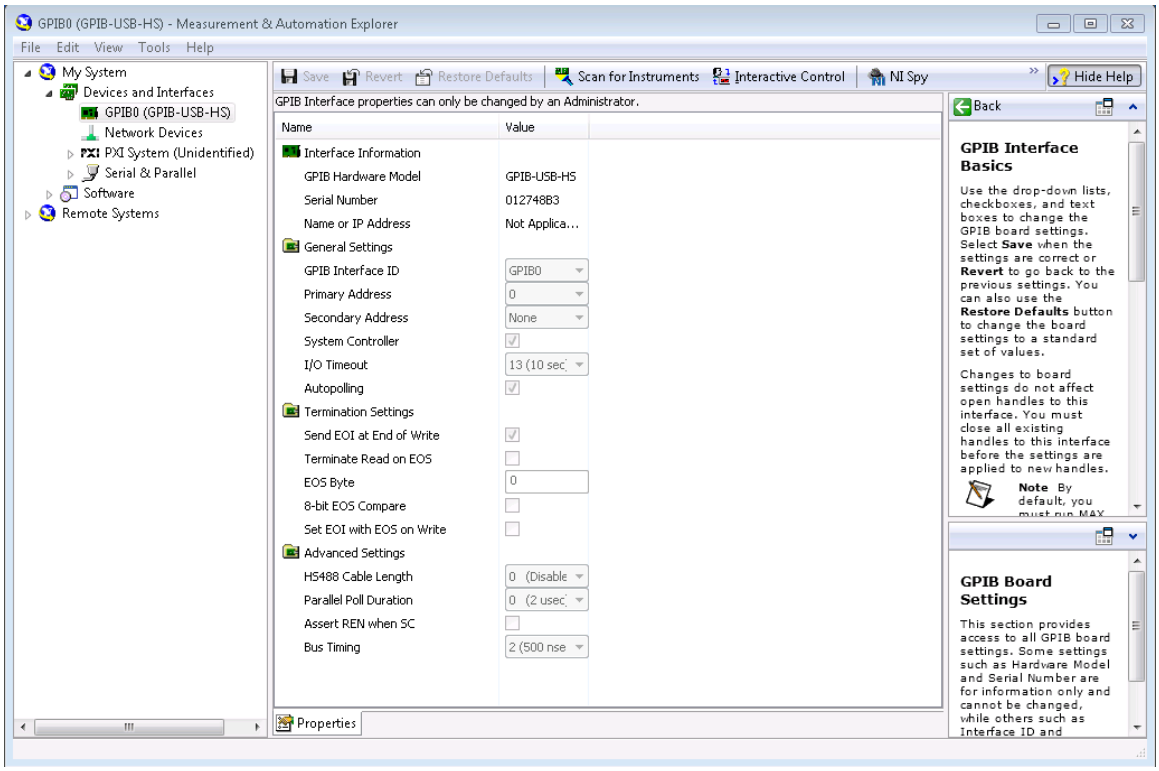


Enter the command into the Command box.
Click on “Send Command” button.

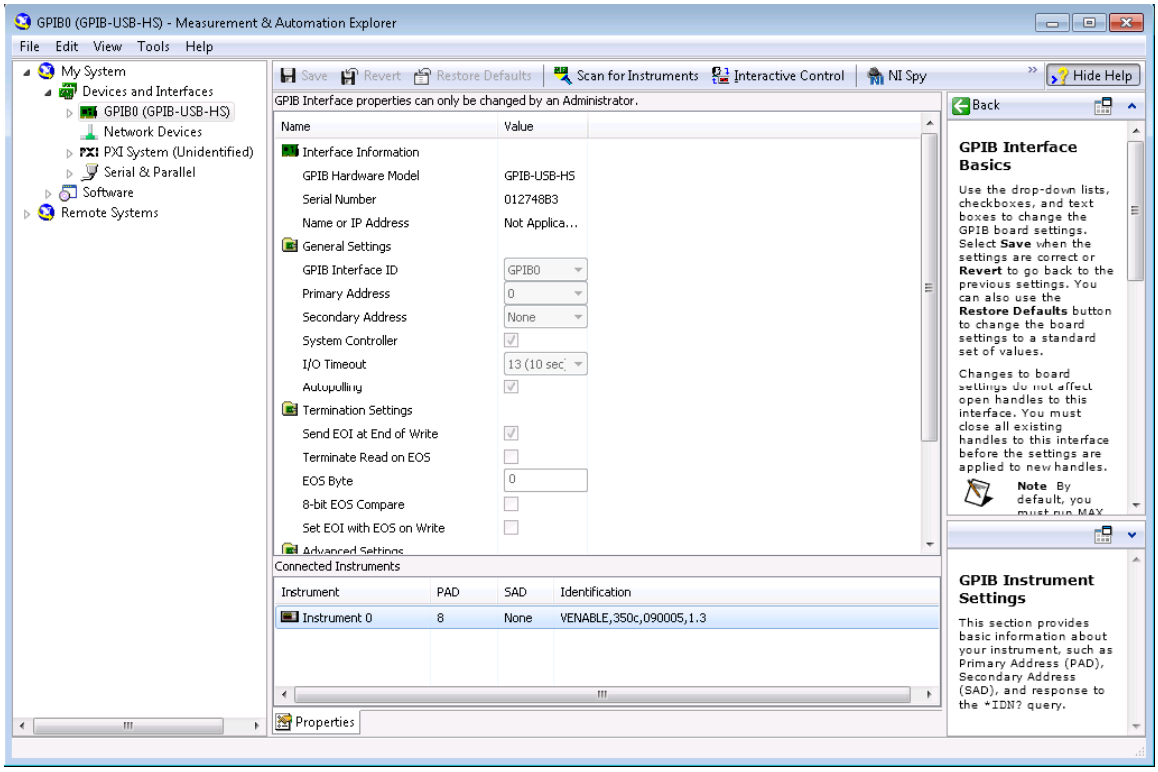


Using National Instruments Tools

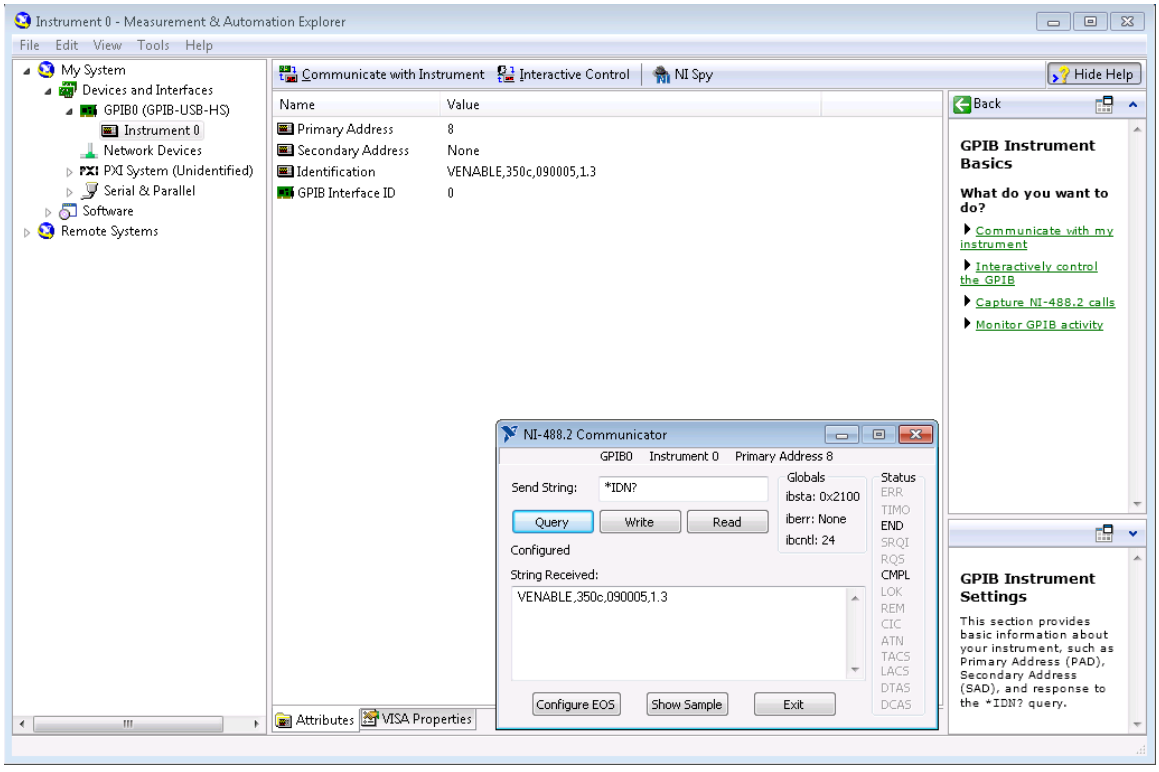
Open the National Instruments “Measurement & Automation Explorer” application.
Open Devices and Interfaces on left panel and select GPIB.



Click on the “Scan for Instruments” tab.

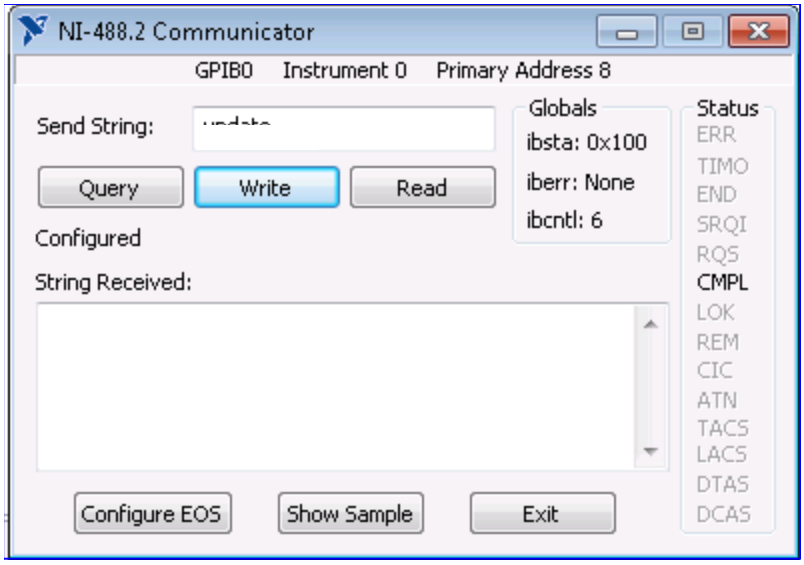


Double click the VENABLE instrument listed in “Connected Instruments” window.



Click on the “Communicate with Instrument” tab to open an NI-488.2 Communicator window.

Enter the command into the Send String box. Click on Write button.



Contact Information

Venable Industries
8656 SH 71 West, Cuesta Centre — Bldg. E
Austin, TX 78735

Phone: (512) 949-3100

Website: *http://www.venableinstruments.com*

Call our main phone number between 9am and 5pm (U.S. Central Time) and speak directly with a systems engineer for prompt problem resolution.