PSA-Series Spectrum Analyzers

Security Features and Volatility

Table of Contents

Contacting Agilent Sales and Service Offices

Assistance with test and measurements needs, and information on finding a local Agilent office, is available on the Internet at *http://www.agilent.com/find/assist*. If you do not have access to the Internet, please contact your field engineer.

Note: In any correspondence or telephone conversation, refer to the instrument by its model number and full serial number. With this information, the Agilent representative can determine whether your unit is still within its warranty period.

Products Covered by this Document

Model Numbers: E4440A
                                  E4443A
                                  E4445A
                                  E4446A
                                  E4447A
                                  E4448A

Product Name: PSA-Series Spectrum Analyzers
Product Family Name: High-Performance Spectrum Analyzers

This document describes instrument security features and the steps to declassify an instrument through memory clearing, sanitization or removal. For additional information, go to:

http://www.agilent.com/find/security

Note: Be sure that all information stored by the user in the instrument that needs to be saved is properly backed up before attempting to clear any of the instrument memory. Agilent Technologies cannot be held responsible for any lost files or data resulting from the clearing of memory.

Be sure to read this document entirely before proceeding with any file deletion or memory clearing.

Terms and Definitions

Clearing – As defined in Section 8-301a of *DoD 5220.22-M*, Clearing is the process of eradicating the data on media before reusing the media so that the data can no longer be retrieved using the standard interfaces on the instrument. Clearing is typically used when the instrument is to remain in an environment with an acceptable level of protection.

Sanitization – As defined in Section 8-301b of *DoD 5220.22-M*, Sanitization is the process of removing or eradicating stored data so that the data cannot be recovered using any known technology. Instrument sanitization is typically required when an instrument is moved from a secure to a non-secure environment, such as when it is returned to the factory for calibration. (The instrument is declassified.) Agilent memory sanitization procedures are designed for customers who need to meet the requirements specified by the US Defense Security Service (DSS). These requirements are specified in the "Clearing and Sanitization Matrix" issued by the Cognizant Security Agency (CSA) and contained in Appendix O of the *ODAA Process Guide*.

Secure Erase – Secure Erase is a term that is used to refer to either the clearing or sanitization features of Agilent instruments.

Instrument Declassification – A term that refers to procedures that must be undertaken before an instrument can be removed from a secure environment, such as is the case when the instrument is returned for calibration. Declassification procedures include memory sanitization or memory removal, or both. Agilent declassification procedures are designed to meet the requirements specified in *DoD 5220.22-M*, chapter 8.

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 (Size is in bits)	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/ Contents	Data Input Method	Location in Instrument and Remarks	Sanitization Procedure
Main Memory (Flash) 48 M or 64 M (See Note 2 below)	Yes (See Note 1)	Yes	Used to store firmware, operating system, and other system files. If Option 117 is not installed, user-saved state files are also stored here. If Option 117 is installed, these files are stored in the Compact Flash memory (see Table 2 for details). To determine installed options, see Note 3 below.	Programmed before installed, by firmware operations, and by user input	A26A2 Flash Memory Board	See Table 4
Boot Memory (NVRAM) 96 k	Yes	Yes	Stores instrument boot information, instrument state (parameter settings) information, and the like.	Programmed before installed and by Firmware operations	A26 CPU Assembly	See Table 6
Firmware Memory (DRAM) 256 M	Yes	No	Temporarily stores the firmware "running program"	Firmware operations	A26A1 DRAM Card Volatile memory	Cycle power
Config & Cal Memory (EEPROM) 1 k	No	Yes	Used to identify the assembly and store factory calibration data and option configuration data.	Programmed before installed and by Firmware operations (cal routines)	A7 Digital IF Assembly Contains no user data	See Table 7

Config & Cal Memory (EEPROM) 1 k	No	Yes	Used to identify the assembly and store factory calibration data and option configuration data.	Programmed before installed and by Firmware operations (cal routines)	A8 Analog IF Assembly Contains no user data	See Table 7
Config & Cal Memory (EEPROM) 1 k	No	Yes	Used to identify the assembly and store factory calibration data and option configuration data.	Programmed before installed and by Firmware operations (cal routines)	A9 2nd LO Assembly Contains no user data	See Table 7
Config & Cal Memory (EEPROM) 16 k	No	Yes	Used to identify the assembly and store factory calibration data and option configuration data.	Programmed before installed and by Firmware operations (cal routines)	A10 3rd Converter Assembly Contains no user data	See Table 7
Config & Cal Memory (EEPROM) 1 k	No	Yes	Used to identify the assembly and store factory calibration data and option configuration data.	Programmed before installed and by Firmware operations (cal routines)	A11 Reference Assembly Contains no user data	See Table 7
Config & Cal Memory (EEPROM) 16 k	No	Yes	Used to identify the assembly and store factory calibration data and option configuration data.	Programmed before installed and by Firmware operations (cal routines)	A12A1 LO Synthesizer Assembly Contains no user data	See Table 7
Config & Cal Memory (EEPROM) 96 k	No	Yes	Used to identify the assembly and store factory calibration data and option configuration data.	Programmed before installed and by Firmware operations (cal routines)	A13 Front End Driver Assembly Contains no user data	See Table 7

Notes
1. This memory is *not* writable when Option 117 is installed.
2. To determine the installed memory size, press **[System]** > **More (1 of 3)** > **Show Hdwr**.
3. To determine which options are installed, press **[System]** > **More (1 of 3)** > **More (2 of 3) > Personality**. The instrument displays a list of installed options.

Table 2: Summary of instrument memory - Option 117

Memory Type and Size (Size is in bits)	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/ Contents	Data Input Method	Location in Instrument and Remarks	Sanitization Procedure
User Memory (Flash) 512 M **(Option 117)**	Yes	Yes	When Option 117 is installed, Main Memory is mounted Read Only and any user-alterable memory is relocated to the 512 M flash card (A39A1) on the A39 memory board. The 512 M flash card stores: User state, Trace, Screen dumps, Result files, Power on last state, Limit Lines, and Amplitude Corrections. See Table 3 below for a comparative summary.	User input	512M on A39A1 flash card, located on A39 Memory Board.	See Table 5

The table below summarizes the memory locations for all file types, with and without Options 115 or 117 installed.

Option 115 uses the same Compact Flash memory card as Option 117, but uses the additional memory to store Downloadable Personalities, User State, Trace, and Power On Last State files. Option 115 and Option 117 are mutually exclusive: an instrument may have at most one of these options installed.

Table 3: Summary of File Locations by Type

File Type	Location without Options 115 or 117	Location with Option 115	Location with Option 117
Amplitude Corrections	Main Flash	Main Flash	Compact Flash
Core User Preset Files	Main Flash	Main Flash	Compact Flash
License Keys	Main Flash	Main Flash	Main Flash
Limit Line	Main Flash	Main Flash	Compact Flash
Mode Cache Files	Main Flash	Compact Flash	Compact Flash
Network Settings	Main Flash	Main Flash	Main Flash
Personalities	Main Flash	Compact Flash	Main Flash
Personality Data Files	Main Flash	Compact Flash	Main Flash
Personality Package Files	Main Flash	Compact Flash	Main Flash
Personality Power On Last State	Main Flash	Compact Flash	Compact Flash
Personality User Preset Files	Main Flash	Compact Flash	Compact Flash
User State, Trace, Screen dumps and result files	Main Flash	Compact Flash	Compact Flash

Summary of Memory Declassification Procedures

This section explains how to clear, sanitize, and remove memory from your instrument, for all classes of memory that are writeable during normal operation.

Important: Before beginning clearing or sanitization, be sure to write down and save the instrument's Option and License Key information. The "Secure Erase All" procedure erases the option and license key information and this information is essential for successful restoration of the instrument's operating system.

Note: Read this entire document before using any sanitization procedure. Failure to do so may result in having to send the instrument back to an Authorized Agilent Service Center for firmware downloads and recalibration.

Table 4: Main Flash

Description and purpose	This memory is used to store firmware, operating system, and other system files. If Option 117 is not installed, this memory also stores all user-saved files, including: User State, Trace, Screen Dumps, Results, Power On Last State, Limit Lines and Amplitude Corrections. If Option 117 is installed, all user-saved files are instead stored in the additional Compact Flash memory, as described in Table 5.
Size	Either 48 Mbits or 64 Mbits. To determine how much Flash is installed, press **[System]** > **More (1 of 3)** > **Show Hdwr**.
Memory clearing	This memory can be cleared by carefully following the instructions in "Secure Erase All" presented later in this document. This procedure complies with the clearing requirements specified for Flash EPROM in the "Clearing and Sanitization Matrix" in Appendix O of the *ODAA Process Guide*.
Memory sanitization	This memory can be sanitized by carefully following the instructions in "Secure Erase All" presented later in this document. This procedure complies with the sanitization requirements specified for Flash EPROM in the "Clearing and Sanitization Matrix" in Appendix O of the *ODAA Process Guide*..
Memory removal	N/A
Memory validation	When this memory is cleared, the instrument will not load the operating system or the firmware and is effectively rendered inoperative.
Remarks	Be sure to write down and save the instrument's option and license key information before performing a "Secure Erase All" procedure. This procedure erases the option and license key information, which is essential for successful restoration of the instrument's hardware and software options.

Table 5: Compact Flash (Option 117)

Description and purpose	If Option 117 is installed, this memory is used to store: User State, Trace, Screen Dumps, Results, Power On Last State, Limit Lines, and Amplitude Corrections.
Size	512 Mbits

Memory clearing	This memory can be cleared by carefully following the instructions in "Secure Erase User" presented later in this document. This procedure complies with the clearing requirements specified for Flash EPROM in the "Clearing and Sanitization Matrix" in Appendix O of the *ODAA Process Guide*.
Memory sanitization	This memory can be sanitized by carefully following the instructions in "Secure Erase User" presented later in this document. This procedure complies with the sanitization requirements specified for Flash EPROM in the "Clearing and Sanitization Matrix" in Appendix O of the *ODAA Process Guide*.
Memory removal	You can physically remove the A39 Memory Board, which contains this memory, from the instrument.
Write protecting	This memory cannot be write-protected.
Memory validation	N/A

Table 6: NVRAM

Description and purpose	Memory used to store instrument boot information, instrument state (parameter settings) information, and the like.
Size	96 kbits (about 32 kbits are dedicated to storing boot information)
Memory clearing	Press [System] > Power On/Preset. If "Factory" is not shown under Preset Type, press Preset Type and select Factory. Pressing Power On toggles between "Last" and "Preset." Make sure Preset is selected, then press the green Preset key. This will clear the NVRAM of any measurement data and restore factory default settings. This procedure complies with the clearing requirements specified for NVRAM in the "Clearing and Sanitization Matrix" in Appendix O of the *ODAA Process Guide*.
Memory sanitization	This memory can be sanitized by carefully following the instructions in "Secure Erase All" presented later in this document. This procedure complies with the sanitization requirements specified for Flash in the "Clearing and Sanitization Matrix" in Appendix O of the *ODAA Process Guide*.
Memory removal	N/A
Memory validation	N/A

Table 7: EEPROM

Description and purpose	This memory is used to identify the assembly and store factory calibration data and option configuration data.
Size	1 kbit, 16 kbits, or 96 kbits (refer to Table 1)
Memory clearing	Since this memory contains no user information, it need not be cleared.
Memory sanitization	This memory cannot be sanitized in compliance with the sanitization requirements specified for EEPROM in the "Clearing and Sanitization Matrix" in Appendix O of the *ODAA Process Guide*. To meet declassification requirements, see "Memory removal."
Memory removal	EEPROM is not accessible to the instrument user and therefore need not be cleared or sanitized.
Memory validation	N/A

Memory Sanitization Procedures

Recording Critical Information

1. Record the Ethernet Number of the instrument. Press **[System]** > **More** > **Show System**. The Ethernet Number is a 12-digit alphanumeric string with a hyphen between the first set of six characters and the last set of six characters; for example, 001083-b80c55. Having this number recorded will save time when you re-install the firmware.

2. Record the IP address of the instrument. Press **[System]** > **Config I/O**.

3. Save the Application License Keys by either saving a screen capture of the license keys or writing down the options and license key information:

4. Obtain a list of the License Keys by saving a screen capture of the instrument's Licensing Screen. To do this, press **[System]** > **More (1 of 3)** > **More (2 of 3)** > **Licensing** > **Show License**. Next, use the PSA file manager to save an image of the PSA screen to a formatted floppy disk. Insert a formatted disk in the front panel disk drive, then press **[File]** > **Save**, press **Type** and select **Screen**, press **Format** and select **Bitmap**, press **Dir Select** and select "A." Press **Save Now**. The file can be displayed or printed from any application capable of reading bitmap (.bmp) files.

5. Verify the screen capture of the license keys has been properly saved to the floppy disk, prior to proceeding, by opening the file using a computer. If you are *unable* to save the license key information using this procedure, write down the "Option" and "License Key" numbers.

6. Properly store this Application License Key data in a safe place (or attach this information to the top cover of the instrument).

Backing up the Option and License Key Information to a PC

1. Load the PSA Series Firmware Update Program from the following Agilent Web site: http://www.agilent.com/find/psa_firmware. Click the download link for the firmware update EXE file: PSA Axx.xx.exe.

2. Begin the PSA firmware upgrade procedure. Accept the licensing agreement. When prompted for an instrument IP address, enter the instrument's IP address.

3. Allow the configuration files to be saved to the default location on the PC.

4. The analyzer's user data, options, and license keys are saved in a file named 'Config' under a directory that begins with the model number, followed by the serial number, then a date and time stamp on the C: drive of the PC; for example, "C:\E4448A\US42070187\15-Oct-02-11-29-AM\Config." Make note of the path name. This file will be used to restore the analyzer's configuration and License Keys after Secure Erase All has been used to erase its memory.

5. When the screen regarding loading the operating system and options appears, exit the firmware upgrade process. At this point, you have saved the configuration files (including the License Keys). You do not need to continue with the instrument firmware download.

Secure Erase All

Note: Before starting this procedure, make a record of the instrument's license key and other critical information by following either of the procedures Recording Critical Information or Backing up the Option and License Key Information, as described above.
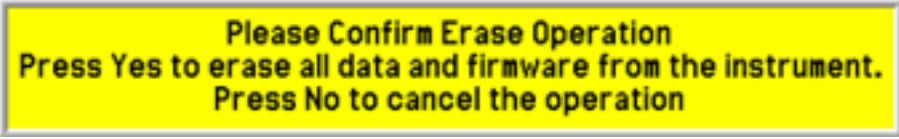
The following procedure erases all persistent storage in the instrument; that is, the operating system, firmware, and all user files. This procedure should be performed *only* when the instrument is going to be removed from a secure area.

1. Press **[System]** > **More (1 of 3)** > **More (2 of 3)** > **Security** > **Secure Erase All**.

2. The instrument displays a message warning you that, if you proceed with the erasure operation, the instrument will be rendered unusable until you reinstall the instrument firmware . If you definitely want to proceed, press **Secure Erase All** again.

> This key will delete all data and firmware in the instrument.
> You will need to reinstall firmware after executing this operation.
> Press the key again if you wish to proceed

3. The instrument displays a further message, asking you to confirm that you wish to proceed. Press **Yes** to continue, or press **No** to exit without altering any part of the memory.

> Please Confirm Erase Operation
> Press Yes to erase all data and firmware from the instrument.
> Press No to cancel the operation

4. If you press **Yes**, the erase operation starts, and cannot be aborted. The instrument displays a progress bar during the operation.
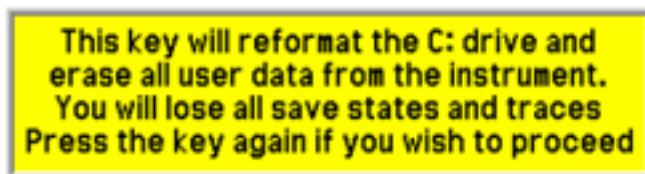
```
Erasing System Flash
  Percent Complete
        4%
```
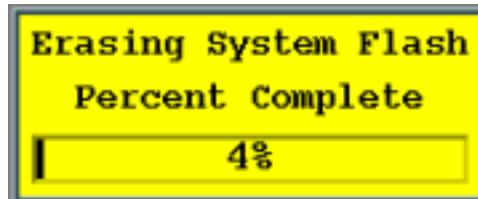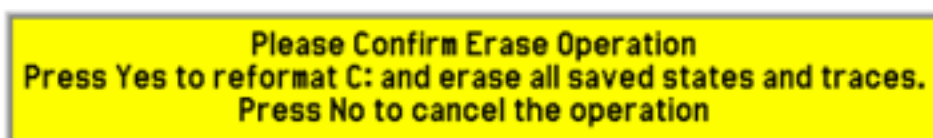
Secure Erase User

Note: This function is available *only* if Option 117 is installed.

Use this function to erase all user-saved files from the instrument, while retaining the instrument's operating system, firmware, license keys and network settings.

1. Press **[System]** > **More (1 of 3)** > **More (2 of 3)** > **Security** > **Secure Erase User**.

2. The instrument displays a message warning you that, if you proceed, you will erase all user data. If you definitely want to proceed, press **Secure Erase User** again.

```
This key will reformat the C: drive and
erase all user data from the instrument.
You will lose all save states and traces
Press the key again if you wish to proceed
```

3. The instrument displays a further message, asking you to confirm that you wish to proceed. Press **Yes** to continue, or press **No** to exit without altering any part of the memory.

```
           Please Confirm Erase Operation
Press Yes to reformat C: and erase all saved states and traces.
           Press No to cancel the operation
```

4. If you press **Yes**, the erase operation starts, and cannot be aborted. The instrument displays a progress bar during the operation.

```
Erasing User Flash
 Percent Complete
███         15%
```
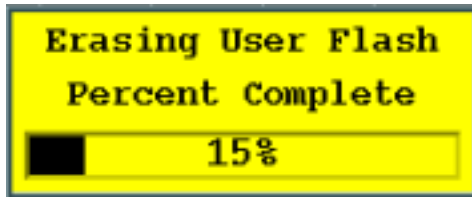
User and Remote Interface Security Measures

Remote Access Interfaces

The GPIB command LLO (local lockout) can be sent by the controller to prevent front-panel keyboard access.

The user is responsible for providing security for the I/O ports for remote access by controlling physical access to the I/O ports. The I/O ports must be controlled because they provide access to most user settings, user states, and the display memory.

USB 2.0 Interface (Option 111)

The USB connection on the PSA is a USB 2.0 compliant Type B interface. The PSA USB is a device-side (slave) connection and is only for instrument control through the Agilent IO Suite drivers. Data cannot be uploaded into the instrument using this connection other than through SCPI command in the same manner that data can be uploaded into the instrument using the GPIB bus.

All commercial and military approved USB devices use a USB Type A connection that eliminates the possibility of information being downloaded to an unapproved memory device.

Procedure for Declassifying a Faulty Instrument

If the instrument is not able to power on, the user information cannot be cleared using the front panel or the remote interface. The only choice in this situation is to take manual steps to remove any user information that may be present. This includes removing the A26 CPU assembly. Refer to the Service Guide for your instrument for removal procedures.

References

1.   *DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)"*;
   United States Department of Defense. Revised February 28, 2006.

        May be downloaded in Acrobat (PDF) format from:
   https://www.dss.mil/GW/ShowBinary/DSS/isp/fac_clear/download_nispom.html

2.   *ODAA Process Guide for C&A of Classified Systems under NISPOM,* Rev. 2008.1;
   Defense Security Service.

        May be downloaded in Acrobat (PDF) format from:
   https://www.dss.mil/GW/ShowBinary/DSS/isp/odaa/odaa.html

Agilent Technologies