Keysight X-Series Signal Analyzers

This manual provides documentation for the following analyzers:

UXA Signal Analyzer N9040B

Security Features and Document of Volatility

KEYSIGHT TECHNOLOGIES

Notices

Manual Part Number

N9040-90005

Print Date

December 2014

First Edition

Published in USA

Keysight Technologies
1400 Fountaingrove Parkway
Santa Rosa, CA 95403

Warranty

The material contained in this document is provided "as is," and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Keysight disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Keysight shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Keysight and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

Restricted Rights Legend

If software is for use in the performance of a U.S. Government prime contract or subcontract, Software is delivered and licensed as "Commercial computer software" as defined in DFAR 252.227-7014 (June 1995), or as a "commercial item" as defined in FAR 2.101(a) or as "Restricted computer software" as defined in FAR 52.227-19 (June 1987) or any equivalent agency regulation or contract clause. Use, duplication or disclosure of Software is subject to Keysight Technologies' standard commercial license terms, and non-DOD Departments and Agencies of the U.S. Government will receive no greater than Restricted Rights as defined in FAR 52.227-19(c)(1-2) (June 1987). U.S. Government users will receive no greater than Limited Rights as defined in FAR 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

Safety Notices

CAUTION

A **CAUTION** notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in damage to the product or loss of important data. Do not proceed beyond a CAUTION notice until the indicated conditions are fully understood and met.

WARNING

A **WARNING** notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in personal injury or death. Do not proceed beyond a WARNING notice until the indicated conditions are fully understood and met.

Where to Find the Latest Information

Documentation is updated periodically. For the latest information about these products, including instrument software upgrades, application information, and product information, see the following URLs:

http://www.keysight.com/find/uxa

To receive the latest updates by email, subscribe to Keysight Email Updates:

http://www.keysight.com/find/emailupdates

Information on preventing instrument damage can be found at:

http://www.keysight.com/find/PreventingInstrumentRepair

Is your product software up-to-date?

Periodically, Keysight releases software updates to fix known defects and incorporate product enhancements. To search for software updates for your product, go to the Keysight Technical Support website at:

http://www.keysight.com/find/uxa_software

Table of Contents

1 Contacting Keysight Sales and Service Offices

Assistance with test and measurement needs, and information to help you find a local Keysight office, is available via the internet at, http://www.keysight.com/find/assist. If you do not have internet access, please contact your designated Keysight representative.

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

2 Products Covered by this Document

Product Name	Model Numbers
UXA Signal Analyzer	N9040B

This document describes instrument memory types and security features. It provides a statement regarding the volatility of all memory types, and specifies the steps required to declassify an instrument through memory clearing, sanitization, or removal.

For additional information, go to:

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

IMPORTANT

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.

Products Covered by this Document

3 Security Terms and Definitions

Term	Definition
Clearing	As defined in Section 8-301a of DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)", clearing is the process of eradicating the data on media before reusing the media in an environment that provides an acceptable level of protection for the data that was on the media before clearing. Hence, clearing is typically used when the instrument is to remain in an environment with an acceptable level of protection.
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. Keysight declassification procedures are designed to meet the requirements specified in DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)", Chapter 8.
Sanitization	As defined in Section 8-301b of DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)", sanitization is the process of removing the data from media before reusing the media in an environment that does **not** provide an acceptable level of protection for the data that was in the media before sanitizing. Hence, 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. Keysight 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" in Section 5.2.5.5.5 of the ISFO Process Manual for the Certification and Accreditation of Classified Systems under the NISPOM.
Secure Erase	Secure Erase is a term that is used to refer to either the clearing or sanitization features of Keysight instruments.

4 Instrument Memory & Volatility

This chapter summarizes all memory types in the instrument.

The descriptions are divided between:

1. Non-Volatile Memory,
2. Volatile Memory.

Non-Volatile Memory

This section contains information on the memory components available in your instrument.

The table provides details of the size of each memory component, its type, how it is used, its location, volatility, and the sanitization procedure.

NOTE The instrument contains no user-accessible non-volatile memory, except for the Disk Drive described in Item 17 of Table 4-1. For this reason, as indicated in the tables below, no sanitization procedure is required for any memory component except the Disk Drive.

Table 4-1 Summary of Non-Volatile instrument memory

Memory Component, Type and Size	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Location in Instrument and Remarks	Sanitization Procedure
1. Front Panel EEPROM 64 kbit	No	Yes	Contains software for running front panel microcontroller. Operates front panel LEDs, and transmits key presses to processor.	Programmed before installation.	A1A2 Front Panel Interface Board Contains no user data.	None
2. EDID Memory 2 kbit EEPROM	No	Yes	Extended Display Identification Data. Contains basic information about a monitor and its capabilities.	Programmed before installation.	A1A2 Front Panel Interface Board. Contains no user data.	None
3. Config & Cal Memory 8 kbit EEPROM	No	Yes	Header EEPROM used to identify the assembly.	Programmed before installation.	A2 Analog IF Assy. Contains no user data.	None
4. Config & Cal Memory 8 kbit EEPROM	No	Yes	Header EEPROM used to identify the assembly.	Programmed before installation.	A3 Digital IF Assy. Contains no user data.	None
5. Config Memory 8 Mbit Flash	No	Yes	Contains measurement and control software, which is preloaded into FPGA during instrument power-up.	Programmed before installation.	A3 Digital IF Assy. Contains no user data.	None
6. CPU BIOS (CMOS NVRAM) 256 Byte (battery backed)	No	Yes	Contains default BIOS settings to use when booting the Processor Assembly.	Programmed by factory. Settings can be toggled by user.	A4 Processor Assy. Battery backed to maintain Windows calendar time. Contains no user data.	None

Table 4-1 Summary of Non-Volatile instrument memory

Memory Component, Type and Size	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Location in Instrument and Remarks	Sanitization Procedure
7. SD Memory Card 16 GByte	Yes	Yes	Calibration database file backup	Programmed by instrument software and by the user	A4 Processor Assy Contains user data.	See Table 5-3 on page 24.
8. SD card controller configuration memory 2 Kbit EEPROM	No	Yes	Configuration for the SD card controller on boot up	Programmed before installation	A4 Processor Assy Contains no user data	None
9. PCIe retimer configuration 8 Kbit EEPROM	No	Yes	Configuration for the PCIe retimer for external PCIe communication	Programmed before installation	A4 Processor Assy Contains no user data	None
10. FPGA configuration 64 Mbit SPI PROMM	No	Yes	Configuration of the FPGA	Programmed before installation	A4 Processor Assy Contains no user data	None
11. USB3 Device Side controller configuration 64 Kbit EEPROM	No	Yes	Configuration of the USB3.0 Device Side Controller	Programmed before installation	A4 Processor Assy Contains no user data	None
12. COMe EEPROM 64 Kbit EEPROM	No	Yes	Defines PCIe, SATA, USB, DisplayPort, VGA, LAN, audio link	Programmed before installation	A4 Processor Assy Contains no user data	None
13. Board Controller 512 Bytes EEPROM	No	Yes	Record board information (boot times, WDT, etc.)	Programmed before installation	A4 Processor Assy Contains no user data	None
14. CPLD 64 Mbit SPI PROMM	No	Yes	Power sequence control	Programmed before installation	A4 Processor Assy Contains no user data	None
15. I2C EEPROM 2 Kbit EEPROM	No	Yes	Stores EAPI-related settings for COMe module	Programmed by factory	A4 Processor Assy Contains no user data	None
16. COMe EEPROM 64 Mbit SPI EEPROM	No	Yes	COMe BIOS SPI ROM	Programmed before installation	A4 Processor Assy Contains no user data	None

Table 4-1 Summary of Non-Volatile instrument memory

Memory Component, Type and Size	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Location in Instrument and Remarks	Sanitization Procedure
17. Disk Drive 80 GByte This drive is partitioned, as detailed in "Disk Drive Partitioning" on page 20.	Yes	Yes	Contains Operating System, Instrument Software, Factory Calibration Data, Diagnostic software, Crash recovery image, user instrument states, user data files, user trace data and any user installed third party software.	Programmed before installation or by factory/service center calibration procedure software, or by upgrade installation software. Also programmed via operations and by the user.	A5 Disk Drive Assy Contains user data.	See Table 5-1 on page 23.
18. License Storage Memory 512 kbit EEPROM	No	Yes	Contains instrument serial number and license keys for measurement applications. License keys are encrypted.	Programmed before installation and by installing new license keys.	A7 Midplane Assy Contains no user data.	None
19. Config Memory 8 kbit EEPROM	No	Yes	Header EEPROM used to identify the assembly.	Programmed before installation.	A11 RF Switch / High Band Preamp. Contains no user data.	None
20. Config Memory 8 kbit EEPROM	No	Yes	Header EEPROM used to identify the assembly.	Programmed before installation.	A12 YTF Assy Contains no user data.	None
21. Config Memory 8 kbit EEPROM	No	Yes	Header EEPROM used to identify the assembly.	Programmed before installation.	A13 Front End Assy Contains no user data.	None
22. Config & Cal Memory 8 kbit EEPROM	No	Yes	Header EEPROM used to identify the assembly.	Programmed before installation.	A14 Synthesizer Assy Contains no user data.	None
23. Config Memory 8 Mbit Flash (1024 x 8)	No	Yes	Contains measurement and control software, which is preloaded into FPGA during instrument power-up.	Programmed before installation.	A14 Synthesizer Assy Contains no user data.	None
24. Config and Cal Memory 8 kbit EEPROM	No	Yes	Header EEPROM used to identify the assembly and board specific Cal data	Programmed during board pretest	A14 Synthesizer Assy Contains no user data	None
25. Spartan6 configuration memory 8 Mbit Flash	No	Yes	Contains measurement and control software, which is preloaded into Spartan6 FPGA during instrument power-up.	Programmed before installation	A14 Synthesizer Assy Contains no user data	None

Table 4-1 Summary of Non-Volatile instrument memory

Memory Component, Type and Size	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Location in Instrument and Remarks	Sanitization Procedure
26. Config and Cal Memory 8 kbit EEPROM	No	Yes	Header EEPROM used to identify the assembly	Programmed during board pretest	A14 Synthesizer Assy Contains no user data	None
27. Spartan6 configuration memory 8 Mbit Flash	No	Yes	Contains measurement and control software, which is preloaded into Spartan6 FPGA during instrument power-up.	Programmed before installation	A14 Synthesizer Assy Contains no user data	None
28. Config & Cal Memory 8 kbit EEPROM	No	Yes	Header EEPROM used to identify the assembly.	Programmed before installation.	A15 Front End Control Assy Contains no user data.	None
29. Config Memory 2 Mbit Flash	No	Yes	Contains measurement and control software, which is preloaded into FPGA during instrument power-up. Primarily YTF, attenuator, and front end switch control.	Programmed before installation.	A15 Front End Control Assy Contains no user data.	None
30. Config & Cal Memory 8 kbit EEPROM	No	Yes	Header EEPROM used to identify the assembly.	Programmed before installation.	A16 Reference Assy Contains no user data.	None
31. FPGA Config Memory 2 Mbit Flash	No	Yes	Contains measurement and control software.	Programmed before installation.	A16 Reference Assy Contains no user data.	None
32. Digital Potentiometer 112 bits EEPROM	No	Yes	Contains default data to preset digital potentiometers during power-up.	Programmed before installation.	A16 Reference Assy Contains no user data.	None
33. Config & Cal Memory 8 kbit EEPROM	No	Yes	Header EEPROM used to identify the assembly.	Programmed before installation.	A16A1 Reference Daughter Assy Contains no user data.	None
34. Config Memory 1 Mbit Flash	No	Yes	Contains measurement and control software, which is preloaded into FPGA during instrument power-up.	Programmed before installation.	A16A1 Reference Daughter Assy Contains no user data.	None

Table 4-1 Summary of Non-Volatile instrument memory

Memory Component, Type and Size	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Location in Instrument and Remarks	Sanitization Procedure
35.Local Bus CPLD 64 macrocell CPLD	No	Yes	Contains configuration for CPLD	Programmed before installation	A21 WBIF Assy Contains no user data.	None
36. Config and Cal Memory 8 kbit EEPROM	No	Yes	Header EEPROM used to identify the assembly	Programmed during board pretest	A21 WBIF Assy Contains no user data	None
37. PSoCA configuration memory 64 kByte Flash	No	Yes	Contains configuration for PSoCA processor	Programmed before installation	A21 WBIF Assy Contains no user data	None
38. PSoCMA configuration memory 64 kByte Flash	No	Yes	Contains configuration for PSoCMA processor	Programmed before installation	A21 WBIF Assy Contains no user data	None
39. PSoCD configuration memory 64 kByte Flash	No	Yes	Contains configuration for PSoCD processor	Programmed before installation	A21 WBIF Assy Contains no user data	None
40. PSoCMD configuration memory 64 kByte Flash	No	Yes	Contains configuration for PSoCMD processor	Programmed before installation	A21 WBIF Assy Contains no user data	None
41. PSoCA EEPROM memory 2 kByte EEPROM	No	Yes	Contains parameters for PSoCA processor	Programmed during board pretest	A21 WBIF Assy Contains no user data	None
42. PSoCMA EEPROM memory 2 kByte EEPROM	No	Yes	Contains parameters for PSoCMA processor	Programmed during board pretest	A21 WBIF Assy Contains no user data	None
43. PSoCD EEPROM memory 2 kByte EEPROM	No	Yes	Contains parameters for PSoCD processor	Programmed during board pretest	A21 WBIF Assy Contains no user data	None
44. PSoCMD EEPROM memory 2 kByte EEPROM	No	Yes	Contains parameters for PSoCMD processor	Programmed during board pretest	A21 WBIF Assy Contains no user data	None
45. Spartan6 configuration memory 4 Mbit Flash	No	Yes	Contains configuration for Spartan6 FPGA	Programmed before installation	A21 WBIF Assy Contains no user data	None

Table 4-1 Summary of Non-Volatile instrument memory

Memory Component, Type and Size	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Location in Instrument and Remarks	Sanitization Procedure
46. Virtex6 configuration memory 0 32 Mbit Flash	No	Yes	Contains configuration for Virtex6 FPGA	Programmed before installation	A21 WBIF Assy Contains no user data	None
47. Virtex6 configuration memory 1 32 Mbit Flash	No	Yes	Contains configuration for Virtex6 FPGA	Programmed before installation	A21 WBIF Assy Contains no user data	None

Disk Drive Partitioning

The instrument's disk drive is divided at the factory into three visible partitions, labeled C:, D: and E:, plus a fourth hidden partition.

Details of the sizes and functions of all partitions are provided in Table 4-2 below.

Table 4-2 Disk Drive Partitions

Partition Label	Size (GBytes)	Purpose
C:	32 GB	Primary partition for applications and secondary data.
D:	17 GB	Default location for user data.
E:	2 GB	Calibration data.
Hidden	23 GB	Factory recovery image of the C: partition.

Volatile Memory

The volatile memory in the instrument does not have battery backup. It does not retain any information when AC power is removed.

Removing power from this memory meets the memory sanitization requirements specified in the “Clearing and Sanitization Matrix” in Section 5.2.5.5.5 of the ISFO Process Manual for the Certification and Accreditation of Classified Systems under the NISPOM.

Table 4-3 Summary of Volatile Instrument Memory

Memory Type and Size	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Location in Instrument and Remarks	Sanitization Procedure
1. SDRAM 256 MByte	Yes	No	Contains measurement data from data acquisition system.	Programmed by firmware. Not accessible by user.	A3 Digital IF Assy. Contains raw measurement data.	Turn off instrument power.[a]
2. Processor SDRAM 16 GByte	Yes	No	Main dynamic RAM memory for processor. Contains working copies of Operating System, instrument measurement applications, calibration data, and measurement data.	Programmed before installation, or by factory/service center calibration procedure software, or by firmware upgrade installation software. Also programmed via firmware operations and by user.	A4 Processor Assy. Contains user data.	Turn off instrument power.[a]
3. SDRAM 2 GByte	Yes	No	Contains measurement data from data acquisition system.	Programmed by firmware. Not accessible by user.	A3 Digital IF Assy. Contains raw measurement data.	Turn off instrument power.[a]
4. SDRAM 2 GByte	Yes	No	Contains measurement data from data acquisition system.	Programmed by firmware. Not accessible by user.	A22 Digital IF (Option B2X) Contains raw measurement data.	Turn off instrument power.[a]
5. SDRAM 2 GByte	Yes	No	Contains measurement data from data acquisition system.	Programmed by firmware. Not accessible by user.	A23 Digital IF (Option B5X) Contains raw measurement data.	Turn off instrument power.[a]

a. This memory is not battery backed-up or connected to standby power.

5 Memory Clearing, Sanitization and Removal Procedures

This section explains how to clear, sanitize, and remove memory from your instrument, for all types of non-volatile memory that can be written to during normal instrument operation.

Table 5-1 Disk Drive

Description and purpose	The Disk Drive is the main memory for the instrument. It has very large storage capacity, plus fast read and write times. There are no limitations on the number of read/write cycles. It contains the Operating System, Instrument Software, Factory Calibration Data, Diagnostic software, Crash recovery image, user instrument states, user data files, user trace data and any user-installed third party software. The Disk Drive is written to frequently by the Operating System and other application software.
Size	80 Gigabytes
Memory clearing	Software utilities are available that comply with the clearing requirements specified for Magnetic Disks and Flash Drives in the “Clearing and Sanitization Matrix” in Section 5.2.5.5.5 of the ISFO Process Manual for the Certification and Accreditation of Classified Systems under the NISPOM.
Memory sanitization	We recommend always removing the Disk Drive to achieve sanitization. For program classifications lower than Top Secret, this media type can be sanitized using method "d" as defined in the "Clearing and Sanitization Matrix" in Section 5.2.5.5.5 of the ISFO Process Manual for the Certification and Accreditation of Classified Systems under the NISPOM“. For Top Secret and higher program classifications, Disk Drive removal is the only acceptable sanitization procedure.
Memory removal	See the Chapter “Disk Drive Removal Procedure” on page 29.
Write protecting	The Disk Drive cannot be write protected. The operating system and software must be able to read from and write to the drive during normal operation.
Memory validation	The Disk Drive memory can be validated using third-party Windows utilities.

Table 5-2 EEPROM Memories

Description and purpose	These memories are used to identify the assemblies (header info) and store option configuration data. Some are also used to hold factory software for FPGAs. The software is loaded when the instrument powers up. This memory cannot be written to during instrument operation.
Size	2 kbit to 8 Mbit
Memory clearing	Not applicable. This memory does not contain user information and is not accessible by the user.
Memory sanitization	Not applicable. This memory does not contain user information and is not accessible by the user.
Memory removal	Not applicable.

Table 5-2 EEPROM Memories

Write protecting	Not applicable.
Memory validation	Not applicable.
Remarks	With one exception, as described below, these memories are only writable by factory/service center software, or upgrade installation software. These memories are internally connected to proprietary internal control data buses (as opposed to standard computer buses such as IDE, PCI, USB). They are not accessible by the Operating System or by third-party software, or by the user, to protect the measurement accuracy and consistency of the instrument. They are rarely modified, to ensure no degradation of instrument performance. These memories contain no user data. Many of these memories have long write times, and limited write endurance, so they are not intended to be written to dynamically by software. The sole exception applies to the EEPROM on the A7 Midplane Assembly. Inserting a USB memory device containing a valid license key file into the instrument causes the key file to be copied to both the C: drive and the EEPROM on the A7 Midplane Assembly.

Table 5-3 SD Memory Card

Description and purpose	The intended purpose of the SD Memory Card is for backing up the instrument calibration database file. The backup and restore process used by the instrument will default to this location. Users can also write to this memory, since it appears as another disk drive to the instrument.
Size	16 Gigabytes
Memory clearing	Software utilities are available that comply with the clearing requirements specified for Magnetic Disks and Flash Drives in the “Clearing and Sanitization Matrix” in Section 5.2.5.5.5 of the ISFO Process Manual for the Certification and Accreditation of Classified Systems under the NISPOM.
Memory sanitization	We recommend always removing the SD Memory Card to achieve sanitization. For program classifications lower than Top Secret, this media type can be sanitized using method "d" as defined in the "Clearing and Sanitization Matrix" in Section 5.2.5.5.5 of the ISFO Process Manual for the Certification and Accreditation of Classified Systems under the NISPOM“. For Top Secret and higher program classifications, SD Card removal is the only acceptable sanitization procedure.
Memory removal	See the Chapter “SD Memory Card Removal Procedure” on page 33.
Write protecting	The SD Memory Card can be write protected by the use of a switch located on the card itself. Write protecting the card does not interfere with the normal operation of the instrument operating system or the instrument application software.
Memory validation	The SD Memory Card can be validated using third-party Windows utilities.

Instrument Sanitization Procedures

This section includes flowcharts that describe how to sanitize an instrument by physical removal and replacement of the Disk Drive.

Application License Key Storage

Note that License keys for all Applications are stored in EEPROM on the A7 Midplane Assembly (as described in Item 18 of Table 4-1 on page 14). Therefore, when replacing the Disk Drive, you do **not** need to back up and restore the license keys.

Replacement of Disk Drive

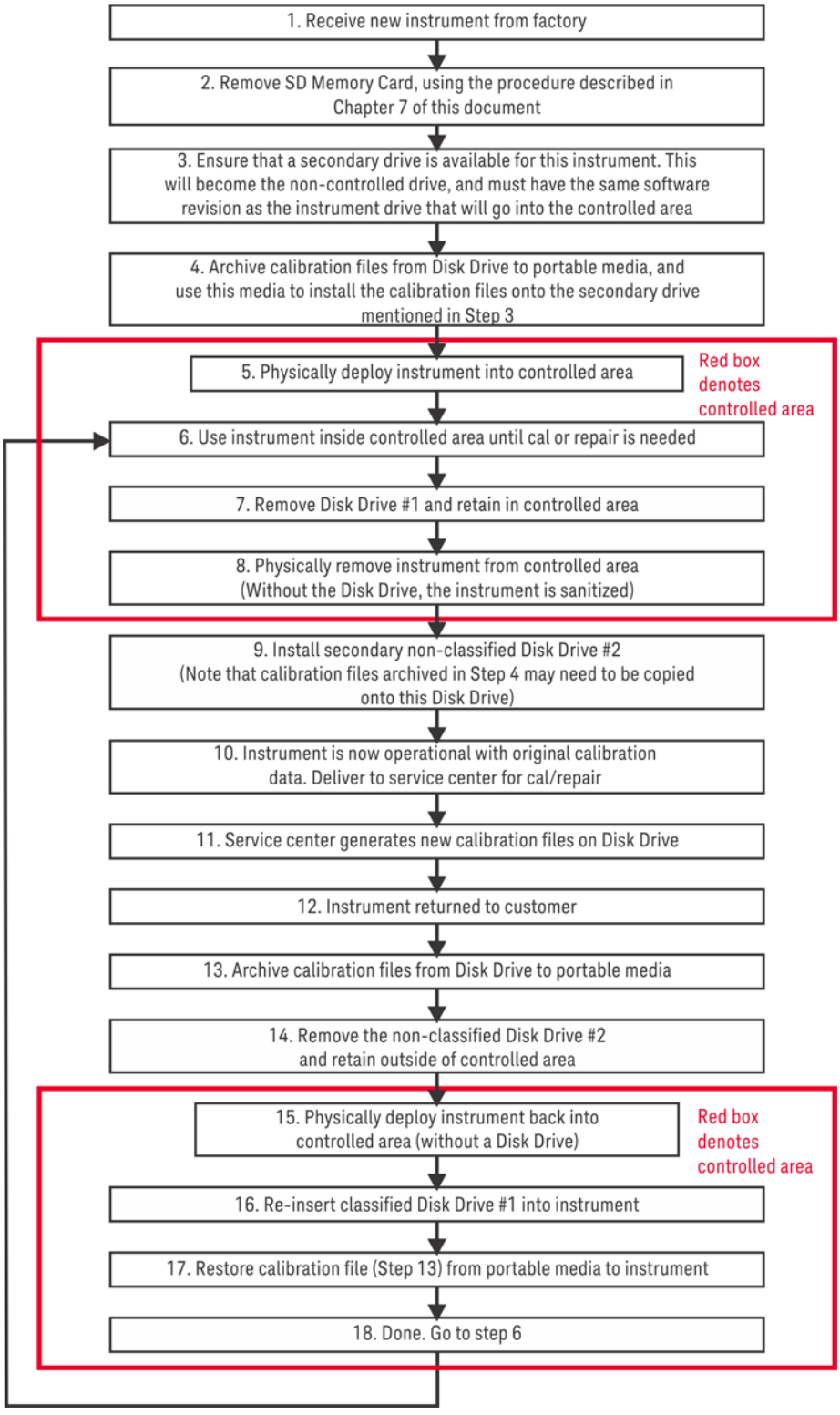
Refer to the flowchart in Figure 5-1 below for details of how to perform this procedure.

For details of how to archive or restore the instrument's calibration files (Steps 3, 12 and 16 in the flowchart), see "Archiving and Restoring Factory Calibration Data Files" on page 27.

For details of how to remove the Disk Drive (Step 6), see "Disk Drive Removal Procedure" on page 29.

IMPORTANT When installing a replacement Disk Drive, ensure that the instrument software revision on the replacement drive matches that of the original drive.

Figure 5-1 Flowchart for Instrument Sanitization Process by Disk Drive Removal



Archiving and Restoring Factory Calibration Data Files

This section describes how to archive ("back up") the instrument's factory calibration data to an external USB memory device, or restore the calibration data from an external memory device.

Tools Required

To perform backup or restore operations, you need:

- a mouse with a USB interface
- a portable memory device with a USB interface
- an alphanumeric keyboard with a USB interface

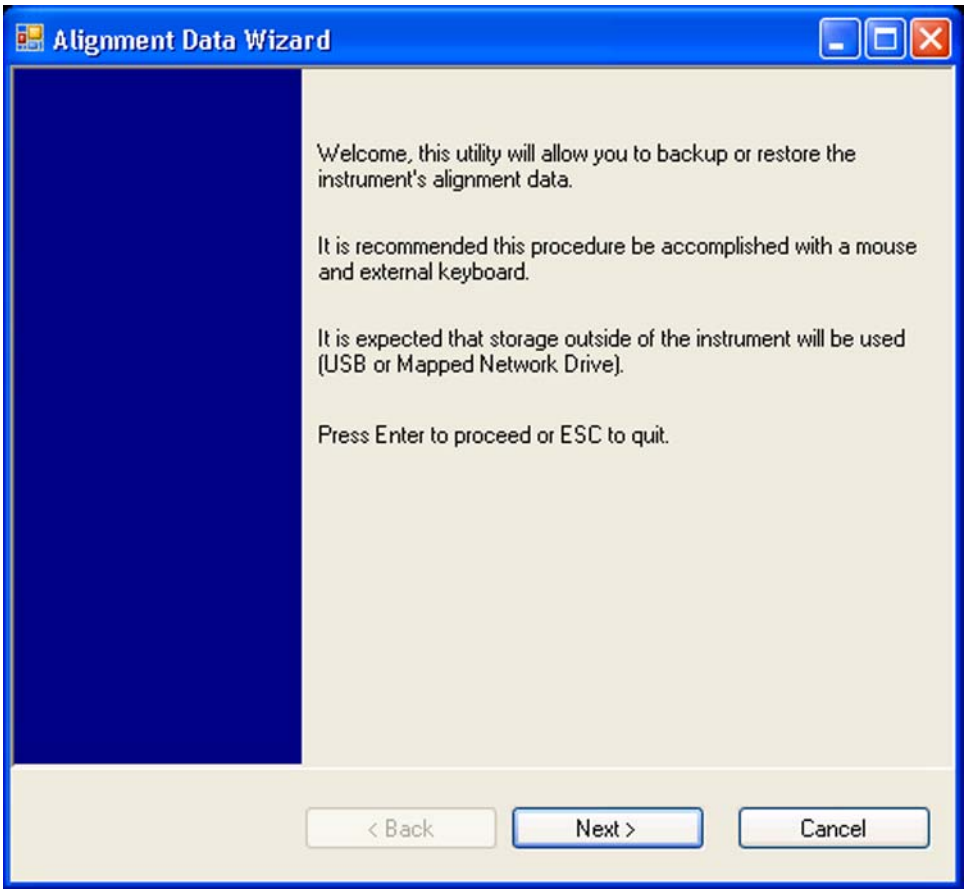
Data Backup or Restore using Alignment Data Wizard

The Alignment Data Wizard is launched directly from the instrument application software interface. You do **not** need to exit the application software before proceeding.

Follow the steps below to start the wizard:

1. Plug the mouse's USB cable into one of the instrument's USB ports.
2. Plug the USB memory device into another of the instrument's USB ports.
3. Plug the USB keyboard into another of the instrument's USB ports.
4. Press **System** > **Alignments** > **Backup or Restore Align Data...**
5. When prompted, press **OK** to close the instrument application.
6. The Alignment Data Wizard dialog appears, as shown in Figure 5-2 below:

Figure 5-2 Alignment Data Wizard Dialog



7. Follow the wizard's on-screen instructions to back up the calibration data to the external USB memory device, **or** restore the data from the device.

6 Disk Drive Removal Procedure

This chapter describes the procedures for physical removal of the instrument's disk drive.

TIP Application License keys are stored in EEPROM on the A7 Midplane Assembly (as described in Item 18 of Table 4-1 on page 14). Therefore, when replacing the Disk Drive, you do **not** need to back up and restore the license keys.

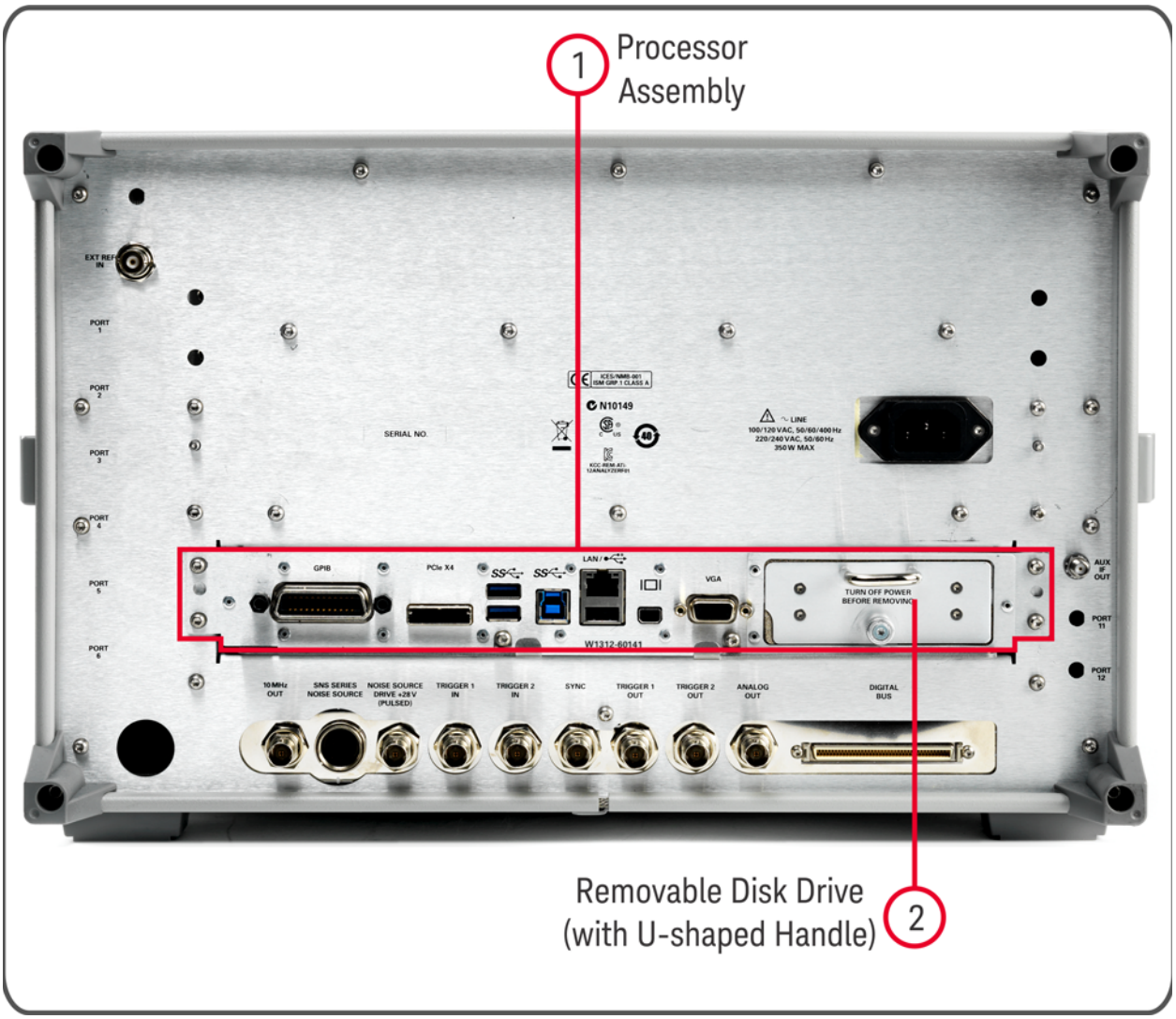
When installing a replacement Disk Drive, ensure that the instrument software revision on the replacement drive matches that of the original drive.

To remove the disk drive, follow the steps below. The numbered items in the figures correspond to the step numbers in the procedure.

CAUTION Before removing the disk drive, ensure that the instrument's power is turned off.

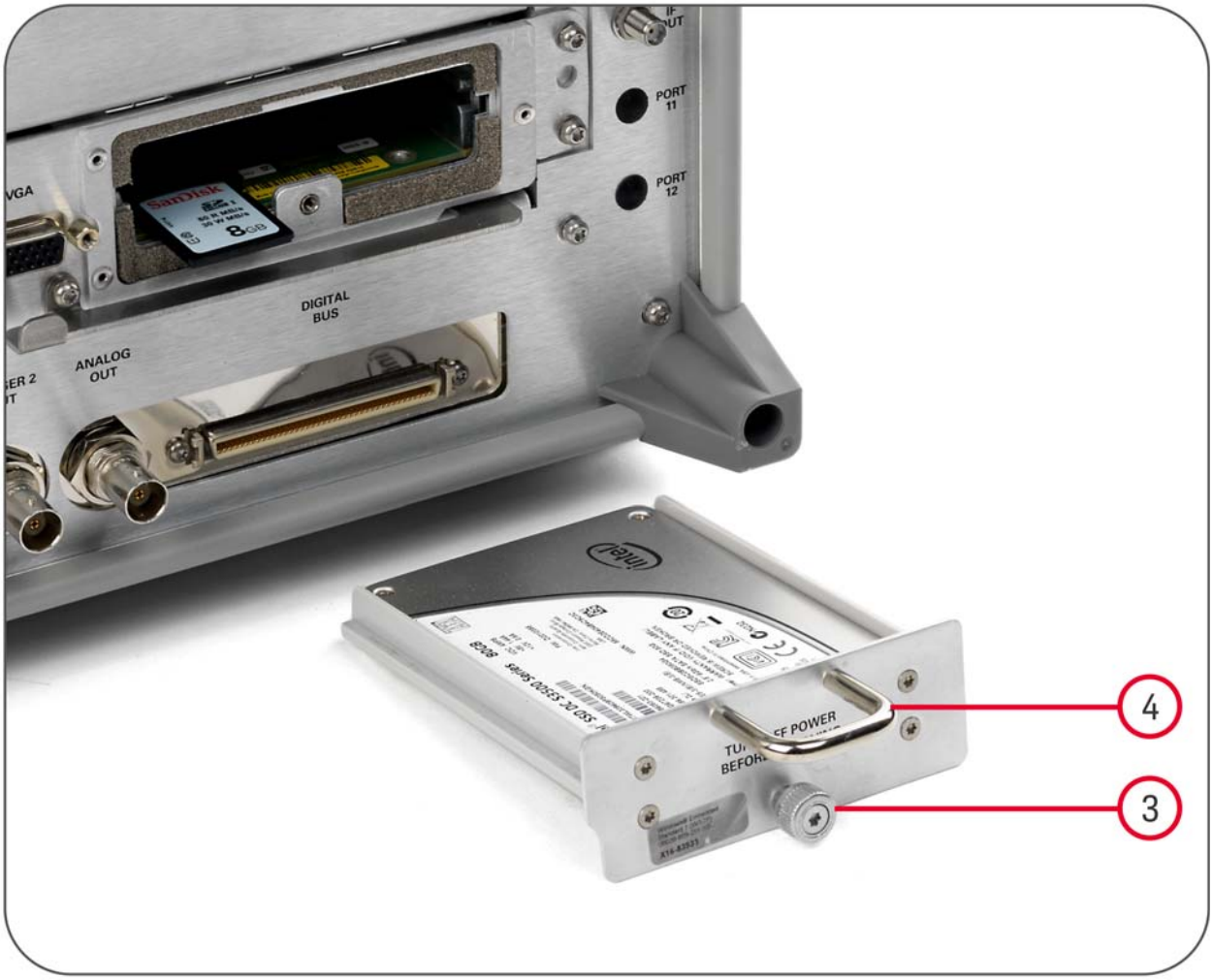
1. Locate the Processor and Disk Drive Assembly on the instrument's rear panel, as shown in Figure 6-1.
2. Locate the removable drive, and its retaining thumbscrew, as shown in Figure 6-1.

Figure 6-1 Instrument Rear Panel & Processor Assembly



3. Turn the thumbscrew to release the drive from the panel, as shown in Figure 6-2 below. If the thumbscrew is too tight to turn by hand, use a TORX T10 screwdriver to loosen it.

Figure 6-2 Removable Disk Drive Unit fully extracted



4. Pull the U-shaped handle attached to the drive unit, to remove the drive from the Processor Assembly, as shown in Figure 6-2.

7 SD Memory Card Removal Procedure

The SD Memory Card is located on the A4 Processor assembly. However, it can only be accessed after the instrument's disk drive is removed.

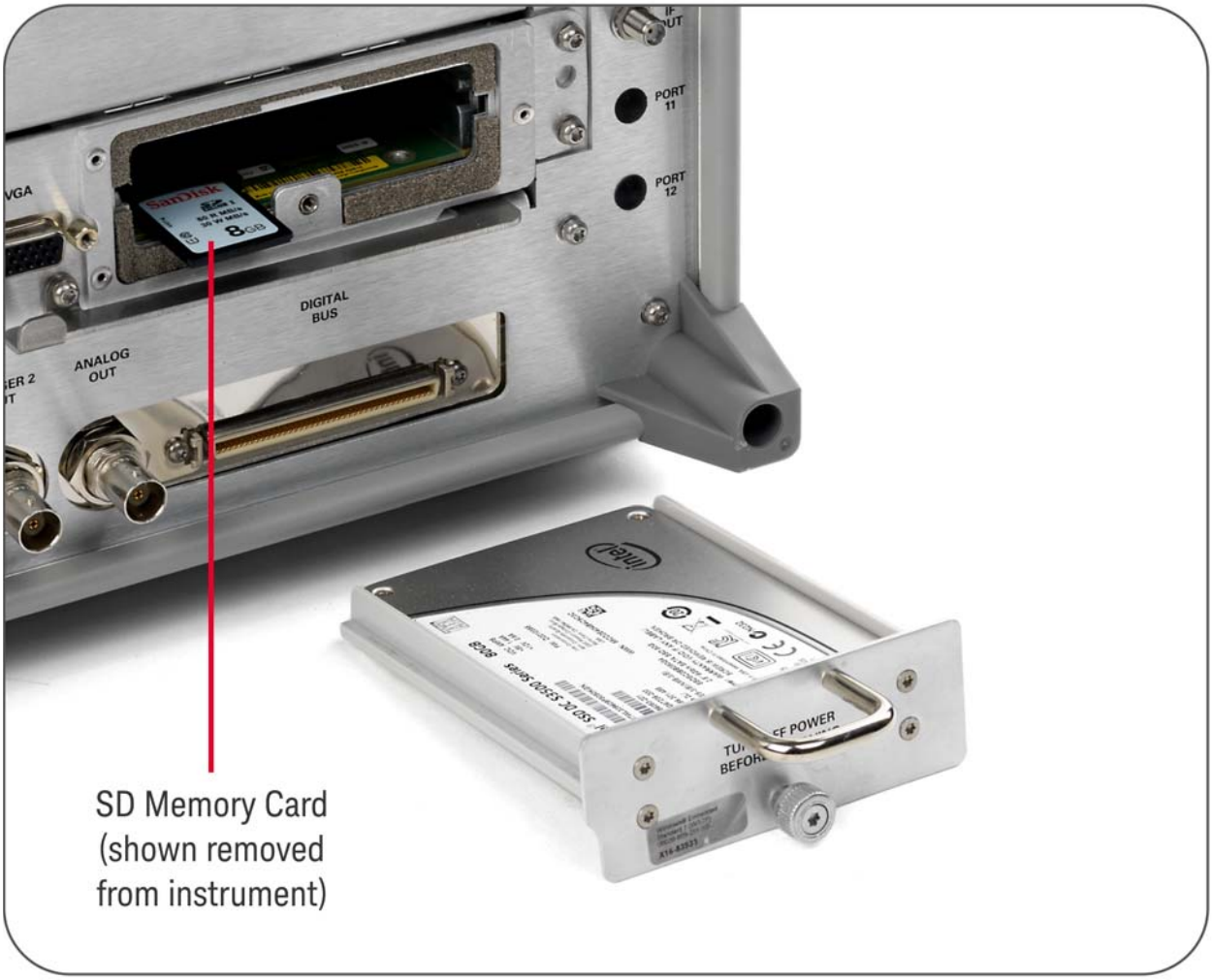
To remove the SD Memory Card:

1. Remove the disk drive by following the "Disk Drive Removal Procedure" on page 29.

   Once the disk drive has been removed, the SD Memory Card is accessible.

2. Push in on the SD Memory Card and release. The Card springs back out, and can then be removed. Figure 7-1 on page 34 below shows the instrument rear panel, with the Disk Drive Assembly and SD Memory Card extracted from the instrument.

Figure 7-1 Instrument Rear Panel, showing Removable Disk Drive Assembly and SD Memory Card



3. Reinstall the disk drive assembly.

Removing the SD Memory Card does not interfere with normal operation of the instrument operating system or the instrument application software.

8 User and Remote Interface Security Measures

This chapter discusses options that are available to you to control and configure user and remote access to the instrument, including:

- SCPI/GPIB Control of Interfaces
- Operating System Security Features
- USB Interfaces. This topic includes information about how to set the instrument's USB ports to read-only.
- SD Memory Card

IMPORTANT Users are 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.

SCPI/GPIB Control of Interfaces

The GPIB command **LLO** (local lockout) can be sent by the controller to disable operation of the instrument's front-panel keys and softkey menus.

However, sending the **LLO** command does **not** disable access to the instrument via its USB ports. For details of how to restrict the operation of the USB ports, see "Configuring USB for Read-only" on page 36 below.

Operating System Security Features

The instrument's Windows operating system includes a variety of features that you can invoke or modify to enhance system security. These include the following:

- The ability to create custom user accounts, and assign different security levels to each account by adding it to an existing group. The group types predefined by Windows are: Administrator, Power User, User, Backup Operator, and Guest, but you can also define new group types.
- To provide additional protection for instruments that have a network (or internet) connection, the standard Windows Firewall is enabled by default.
- You can install standard third-party antivirus and spyware detection software designed for use with Windows. If your instrument has a network (or internet) connection, this may be advisable.

CAUTION Running any third-party program while making measurements may adversely affect the instrument's performance.

USB Interfaces

The instrument's Microsoft Windows operating system can be configured to improve the security of the USB interfaces. This section includes the following topics:

– "Disabling or Enabling AutoRun/AutoPlay" on page 36
– "Configuring USB for Read-only" on page 36

Disabling or Enabling AutoRun/AutoPlay

AutoRun, and the associated **AutoPlay**, are Windows features that assist users in selecting appropriate actions when new media and devices are detected. The AutoRun feature is disabled in the instrument by default, for improved security, unless the Administrator account is running. (In Administrator mode, AutoRun is enabled, to aid with program installation.)

You can disable or enable AutoPlay via the Control Panel. Open the Control Panel and select **Hard ware and Sound > AutoPlay**, then uncheck or check the "Use AutoPlay for all media and devices" checkbox.

Configuring USB for Read-only

A convenient mechanism is provided to set the instrument's USB interfaces to read-only, thus preventing transfer of files from the instrument onto USB devices.

You can change this setting only when you are logged on as the Administrator. To change the setting, do the following:

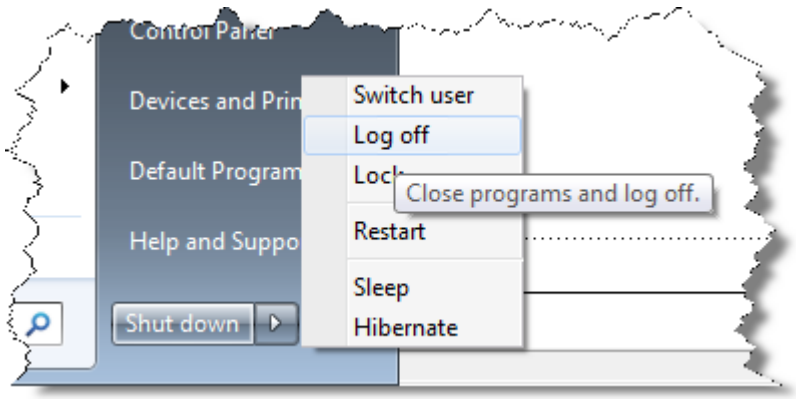
1. If you are **not** currently logged on to the instrument as the Administrator, you must log off.

   If you are currently logged on to the instrument as the Administrator, and the Keysight XSA application is already running, go to Step 4.

   The log-off procedure executes more quickly if you first exit the Keysight XSA application, but you can also log off without exiting the application.

2. To log off, click the Windows **Start** button, then select **Shut down > Log off** from the Windows Start menu, as shown in Figure 8-1 below.

Figure 8-1 Windows Log off Control



3. After you have logged on to the instrument as the Administrator, restart the Keysight XSA application.
4. When the XSA application has fully initialized (that is, when the main results view and softkey menu are visible), press the **System** front-panel key.
5. From the System softkey menu, select: **More** > **Security** > **USB**.
6. Select the option **Read Only**.
7. To activate the configuration change, either log out and then back in under your usual user name (which by default is "instrument"), or cycle the instrument power.

SD Memory Card

The SD Memory Card can either be write protected, or removed from the instrument.

- To remove the SD Memory Card, follow the instructions in "SD Memory Card Removal Procedure" on page 33.
- To write protect the SD Memory Card, first remove it from the instrument, as above. The SD Memory Card features a Lock switch that, when set, prevents the writing of data to the card.

Write protecting or removing the SD Memory Card does not interfere with normal operation of the instrument operating system or the instrument application software.

9 Procedure for Declassifying a Faulty Instrument

Even if the instrument is not able to power on, it may be declassified by removing the disk drive from the instrument, using the appropriate procedure as described in “Disk Drive Removal Procedure” on page 29.

10 Special Options

You can install certain special options that provide security-related functionality. The following available options are described in this chapter.

Option SF1

Option SF1 is a license key-enabled special option that addresses the requirements of security-conscious users. Installing Option SF1 in the instrument causes changes to available functionality in certain menus, and suppression of certain SCPI commands, to prevent the launching of Windows programs from the instrument application. This reduces the instrument's vulnerability to the effects of unauthorized or undesirable third-party programs or scripts.

This section summarizes the functional modifications to the instrument capabilities when Option SF1 is installed.

Menu & Command Changes

Installing Option SF1 causes the following menu and command changes in the instrument.

File Menu

- In the **File** menu, the **File Explorer** key is not available.

System Menu

- In the **System** menu, the keys **Control Panel...**, and **Web Browser** are not available.
- In the **System** > **Service** menu, the keys **Front Panel Test...**, **Front Panel Pixel Test...**, and **Front Panel Touch Test**... are not available.
- In the **System** > **Licensing** menu, the key **License Manager...** is not available.

SCPI Commands

- The SCPI command `:SERVice[:PRODuction]:RUN` is not available.

Option SF2

Option SF2 is a license key-enabled special option that addresses the requirements of security-conscious users who need to be able to prevent the saving of measurement results or user configurations to the instrument's disk drive. The option also prevents the recall of results and configurations from the disk.

Installing Option SF2 makes the following changes to the instrument's operating environment:

- Modifies aspects of the Windows operating system, specifically to disable memory page file usage. For details, see "Operating System Changes" on page 43.
- Disables certain menu keys and SCPI commands, eliminating the ability to save or recall user data. For details, see "Menu & Command Changes" on page 43.

Operating System Changes

Installing Option SF2 disables Windows memory page files. The reason for this change is to ensure that memory page swapping does not inadvertently cause the instrument to create on-disk copies of RAM data.

Note that one effect of disabling memory page files is to reduce the available memory space for preloading applications at power-on.

TIP

If a disk recovery and software update is performed, memory paging files will automatically be re-enabled. If the X-Series application is then started (with Option SF2 installed), an advisory dialog appears, describing how to disable the page files.

The X-Series application will not start until memory page files are disabled. For details of how to run `SF2RegSetup.reg`, refer to Installation Note: Keysight X-Series Signal Analyzers Option SF2.

Menu & Command Changes

Installing Option SF2 causes several menu and command changes in the instrument, as follows.

Front-panel Keys

The functions of the following front-panel keys are disabled. Pressing one of these keys displays the informational message "Settings conflict; Feature not available for Option SF2".

- **Quick Save**
- **Recall**
- **Save**

File Menu

- The **Page Setup**, **Print**, **Quick Save**, **Recall** and **Save** icons are not available.

Preset Menu

- The **User Preset**, **Save User Preset**, and **User Preset All Modes** icons are not available.

System Menu

- In the **System** > **Power On** menu, the Power On Type selection keys (**Mode Preset, User Preset** and **Last State**) are not available.

SCPI Commands

The following SCPI commands are **not** available. Attempting to use these commands generates the Error message: `-113,"Undefined header"`.

Note that some of the commands listed are specific to individual applications, thus the set of available commands depends on which applications are licensed for a given instrument.

- `*RCL`
- `*SAV`
- `:MMEMory:CLEar:ALL`
- `:MMEMory:CLEar:STATe`
- `:MMEMory:COMMent`
- `:MMEMory:COPY:DEVice`
- `:MMEMory:INITialize`
- `:MMEMory:LOAD:ALIMit`
- `:MMEMory:LOAD:ALISt`
- `:MMEMory:LOAD:ATRace`
- `:MMEMory:LOAD:AUTO`
- `:MMEMory:LOAD:CAPTured`
- `:MMEMory:LOAD:CHTable`
- `:MMEMory:LOAD:CORRection`
- `:MMEMory:LOAD:ENR`
- `:MMEMory:LOAD:EVMSetup`
- `:MMEMory:LOAD:FREQuency`
- `:MMEMory:LOAD:LIMit`
- `:MMEMory:LOAD:LOSS`
- `:MMEMory:LOAD:MASK`
- `:MMEMory:LOAD:MPADapter:CORRection`
- `:MMEMory:LOAD:PSET`
- `:MMEMory:LOAD:REGister`
- `:MMEMory:LOAD:SCAN`
- `:MMEMory:LOAD:SETup`
- `:MMEMory:LOAD:SLISt`
- `:MMEMory:LOAD:SSSetup`
- `:MMEMory:LOAD:STATe`
- `:MMEMory:LOAD:STATe:VSA`
- `:MMEMory:LOAD:T2Config`
- `:MMEMory:LOAD:TMMConfig`
- `:MMEMory:LOAD:TRACe`
- `:MMEMory:LOAD:TRACe:DATA`
- `:MMEMory:LOAD:TRACe:REGister`
- `:MMEMory:LOAD:VSASetup`

- :MMEMory:LOAD:ZMAP
- :MMEMory:MSIS
- :MMEMory:NAME
- :MMEMory:NFIGure:LOAD:ENR
- :MMEMory:NFIGure:LOAD:FREQuency
- :MMEMory:NFIGure:LOAD:LOSS
- :MMEMory:NFIGure:STORe:ENR
- :MMEMory:NFIGure:STORe:FREQuency
- :MMEMory:NFIGure:STORe:LOSS
- :MMEMory:REGister:STATe:LABel
- :MMEMory:RESults:CORRection:MODE
- :MMEMory:RESults:LIMits:MODE
- :MMEMory:RESults:OUTPut
- :MMEMory:RESults:SCAN
- :MMEMory:RESults:SCReen:THEMe
- :MMEMory:RESults:SLISt
- :MMEMory:RESults:TRACe:DATA
- :MMEMory:RESults:TRACe:HEADer
- :MMEMory:RESults:TRACe:SETTing
- :MMEMory:SELect[:ITEM]:ALL
- :MMEMory:SELect[:ITEM]:DEFault
- :MMEMory:SELect[:ITEM]:HWSettings
- :MMEMory:SELect[:ITEM]:LINes:ALL
- :MMEMory:SELect[:ITEM]:NONE
- :MMEMory:SELect[:ITEM]:SCData
- :MMEMory:SELect[:ITEM]:TRACe[:ACTive]
- :MMEMory:SELect[:ITEM]:TRANsducer:ALL
- :MMEMory:STORe:ALIMit
- :MMEMory:STORe:ALISt
- :MMEMory:STORe:ATRace
- :MMEMory:STORe:CAPTured
- :MMEMory:STORe:CHTable
- :MMEMory:STORe:CORRection
- :MMEMory:STORe:ENR
- :MMEMory:STORe:FREQuency
- :MMEMory:STORe:LIMit
- :MMEMory:STORe:LOSS
- :MMEMory:STORe:MPADapter:CORRection
- :MMEMory:STORe:PSET
- :MMEMory:STORe:RESults

- :MMEMory:STORe:RESults:MTABle
- :MMEMory:STORe:RESults:PTABle
- :MMEMory:STORe:RESults:SNGLS
- :MMEMory:STORe:RESults:SPECtrogram
- :MMEMory:STORe:SCAN
- :MMEMory:STORe:SCReen
- :MMEMory:STORe:SCReen:THEMe
- :MMEMory:STORe:SLISt
- :MMEMory:STORe:STATe
- :MMEMory:STORe:T2Config
- :MMEMory:STORe:TMMConfig
- :MMEMory:STORe:TRACe
- :MMEMory:STORe:TRACe:DATA
- :MMEMory:STORe:TRACe:REGister
- :MMEMory:STORe:ZMAP
- :MMEMory:TRACe:CLIent
- :MMEMory:TRACe:CLIent:STATe
- :MMEMory:TRACe:OPERator
- :MMEMory:TRACe:OPERator:STATe
- :MMEMory:TRACe:PDEScription
- :MMEMory:TRACe:PDEScription:STATe
- :MMEMory:TRACe:TITLe
- :MMEMory:TRACe:TITLe:STATe
- :SYSTem:PON:TYPE
- :SYSTem:PRESet:SAVE
- :SYSTem:PRESet:TYPE
- :SYSTem:PRESet:USER
- :SYSTem:PRESet:USER:ALL
- :SYSTem:PRESet:USER:SAVE
- :SYSTem:PRINt:THEMe

A: 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:
http://www.dss.mil/isp/fac_clear/download_nispom.html

2. **ISFO Process Manual for the Certification and Accreditation of Classified Systems under the NISPOM**
Defense Security Service.
DSS-cleared industries may request a copy of this document via email, by following the instructions at:
http://www.dss.mil/isp/odaa/request.html

4. **Microsoft Knowledge Base Article ID: 967715**
"How to disable the AutoRun functionality in Windows": may be viewed at:
http://support.microsoft.com/kb/967715
Note that a second article, at: http://support.microsoft.com/kb/953252, "How to correct 'disable AutoRun registry key' enforcement in Windows", redirects to article ID 967715.

5. **Installation Note: Keysight X-Series Signal Analyzers Option SF2**
Keysight Technologies 2014. Part Number: N9020-90234.
May be downloaded from:
http://literature.cdn.keysight.com/litweb/pdf/N9020-90234.pdf

References