Keysight X-Series EMI Receiver

This manual provides documentation for the following analyzers:

MXE EMI Receiver N9038A

Notice: This document contains references to Agilent. Please note that Agilent's Test and Measurement business has become Keysight Technologies. For more information, go to www.keysight.com.

Security Features and Document of Volatility

KEYSIGHT
TECHNOLOGIES

Notices

Manual Part Number

N9038-90012

Print Date

August 2014

Supersedes: March 2014

Printed 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/mxe

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/mxe_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
MXE EMI Receiver	N9038A

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.

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 7 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 (EEPROM) 2 kbit	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 (EEPROM) 8 kbit	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 (EEPROM) 8 kbit	No	Yes	Header EEPROM used to identify the assembly.	Programmed before installation.	A3 Digital IF Assy. Contains no user data.	None.
5. Config Memory (Flash) 8 Mbit	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. Disk Drive 80 GByte This drive is partitioned, as detailed in "Disk Drive Partitioning" on page 18.	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 21.
8. License Storage Memory (EEPROM) 512 kbit	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.
9. Config Memory (EEPROM) 8 kbit	No	Yes	Header EEPROM used to identify the assembly.	Programmed before installation.	A11 RF Switch / High Band Preamp. Contains no user data.	None.
10. Config Memory (EEPROM) 8 kbit	No	Yes	Header EEPROM used to identify the assembly.	Programmed before installation.	A12 YTF Assembly. Contains no user data.	None.
11. Config Memory (EEPROM) 8 kbit	No	Yes	Header EEPROM used to identify the assembly.	Programmed before installation.	A13 Front End Assembly. Contains no user data.	None.
12. Config & Cal Memory (EEPROM) 8 kbit	No	Yes	Header EEPROM used to identify the assembly.	Programmed before installation.	A14 Synthesizer Assy. Contains no user data.	None.
13. Config Memory (Flash) 8 Mbit (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.
14. Config & Cal Memory (EEPROM) 8 kbit	No	Yes	Header EEPROM used to identify the assembly.	Programmed before installation.	A15 Front End Control 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
15. Config Memory (Flash) 2 Mbit	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.
16. Config & Cal Memory (EEPROM) 8 kbit	No	Yes	Header EEPROM used to identify the assembly.	Programmed before installation.	A16 Reference Assy. Contains no user data.	None.
17. FPGA Config Memory (Flash) 2 Mbit	No	Yes	Contains measurement and control software.	Programmed before installation.	A16 Reference Assy. Contains no user data.	None.
18. Digital Potentiometer (EEPROM) 112 bits	No	Yes	Contains default data to preset digital potentiometers during power-up.	Programmed before installation.	A16 Reference Assy. Contains no user data.	None.
19. Config & Cal Memory (EEPROM) 8 kbit	No	Yes	Header EEPROM used to identify the assembly.	Programmed before installation.	A16A1 Reference Daughter Assy. Contains no user data.	None.
20. Config Memory (Flash) 1 Mbit	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.
21. Header Memory. (EEPROM) 8 kbit	No	Yes	Contains header information used to identify the assembly.	Programmed before installation.	A21 RF Preselector Input Assy. Contains no user data.	None.
22. Header Memory. (EEPROM) 8 kbit	No	Yes	Contains header information used to identify the assembly.	Programmed before installation.	A22 Radiated Filter Assy. Contains no user data.	None.
23. Config Memory (Flash) 2 Mbit	No	Yes	Contains measurement and control software, which is preloaded into FPGA during instrument power-up.	Programmed before installation.	A22 Radiated Filter 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
24. Header Memory (EEPROM) 8 kbit	No	Yes	Contains header information used to identify the assembly.	Programmed before installation.	A24 Conducted Filter 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 4 GByte or 8 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. For all instruments with Option DP2. 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 27.
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 busses (as opposed to standard computer busses 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.

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 8 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

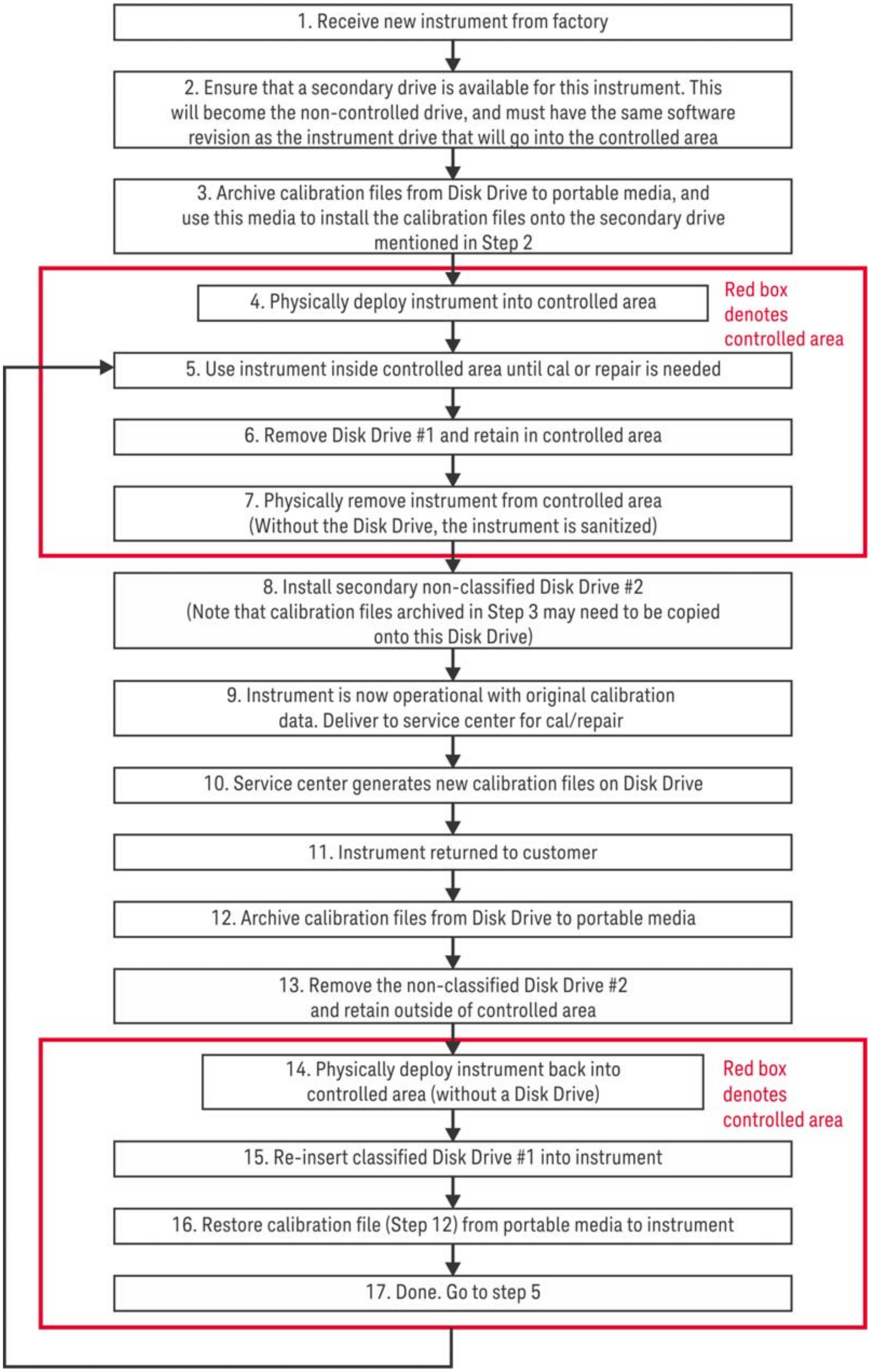
Refer to the flowchart in Figure 5-1 below for details of how to perform this procedure.

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 25.

For details of how to remove the Disk Drive (Step 6), see “Disk Drive Removal Procedure” on page 27.

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


1. Receive new instrument from factory
2. Ensure that a secondary drive is available for this instrument. This will become the non-controlled drive, and must have the same software revision as the instrument drive that will go into the controlled area
3. Archive calibration files from Disk Drive to portable media, and use this media to install the calibration files onto the secondary drive mentioned in Step 2
4. Physically deploy instrument into controlled area
Red box denotes controlled area
5. Use instrument inside controlled area until cal or repair is needed
6. Remove Disk Drive #1 and retain in controlled area
7. Physically remove instrument from controlled area (Without the Disk Drive, the instrument is sanitized)
8. Install secondary non-classified Disk Drive #2 (Note that calibration files archived in Step 3 may need to be copied onto this Disk Drive)
9. Instrument is now operational with original calibration data. Deliver to service center for cal/repair
10. Service center generates new calibration files on Disk Drive
11. Instrument returned to customer
12. Archive calibration files from Disk Drive to portable media
13. Remove the non-classified Disk Drive #2 and retain outside of controlled area
14. Physically deploy instrument back into controlled area (without a Disk Drive)
Red box denotes controlled area
15. Re-insert classified Disk Drive #1 into instrument
16. Restore calibration file (Step 12) from portable media to instrument
17. Done. Go to step 5

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

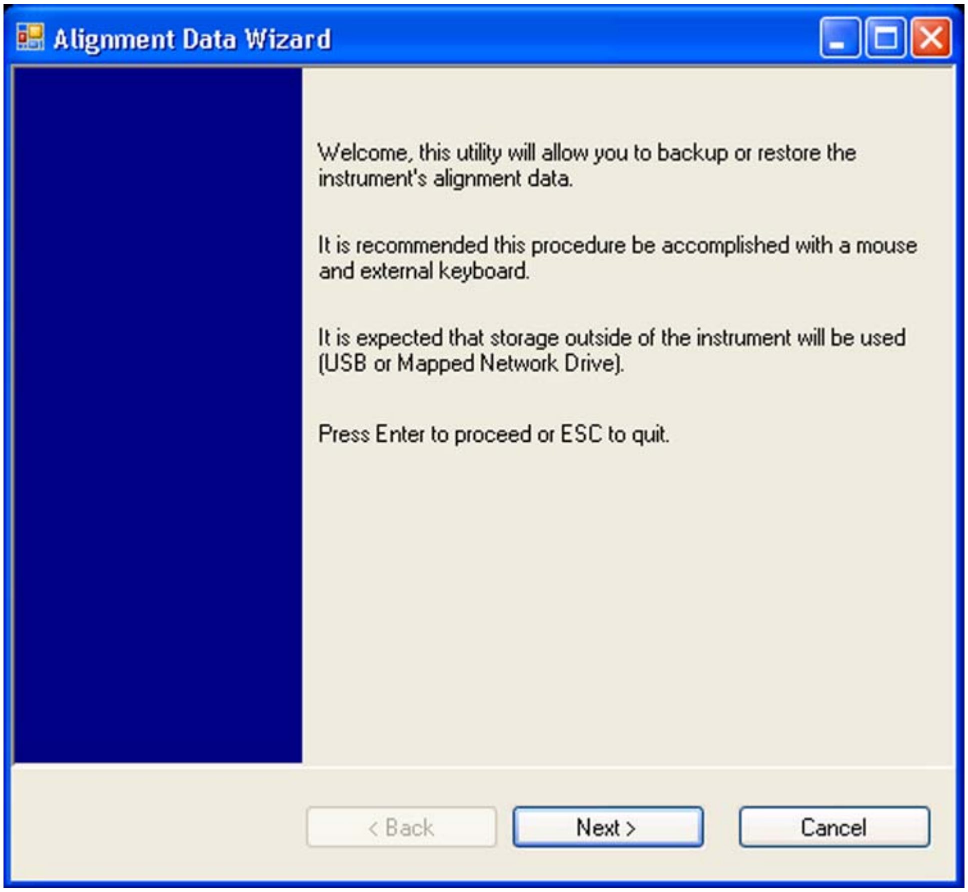
Data Backup or Restore using Alignment Data Wizard

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. The Alignment Data Wizard dialog appears, as shown in Figure 5-2 below:

Figure 5-2 Alignment Data Wizard Dialog



Alignment Data Wizard

Welcome, this utility will allow you to backup or restore the instrument's alignment data.

It is recommended this procedure be accomplished with a mouse and external keyboard.

It is expected that storage outside of the instrument will be used (USB or Mapped Network Drive).

Press Enter to proceed or ESC to quit.

6. 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.

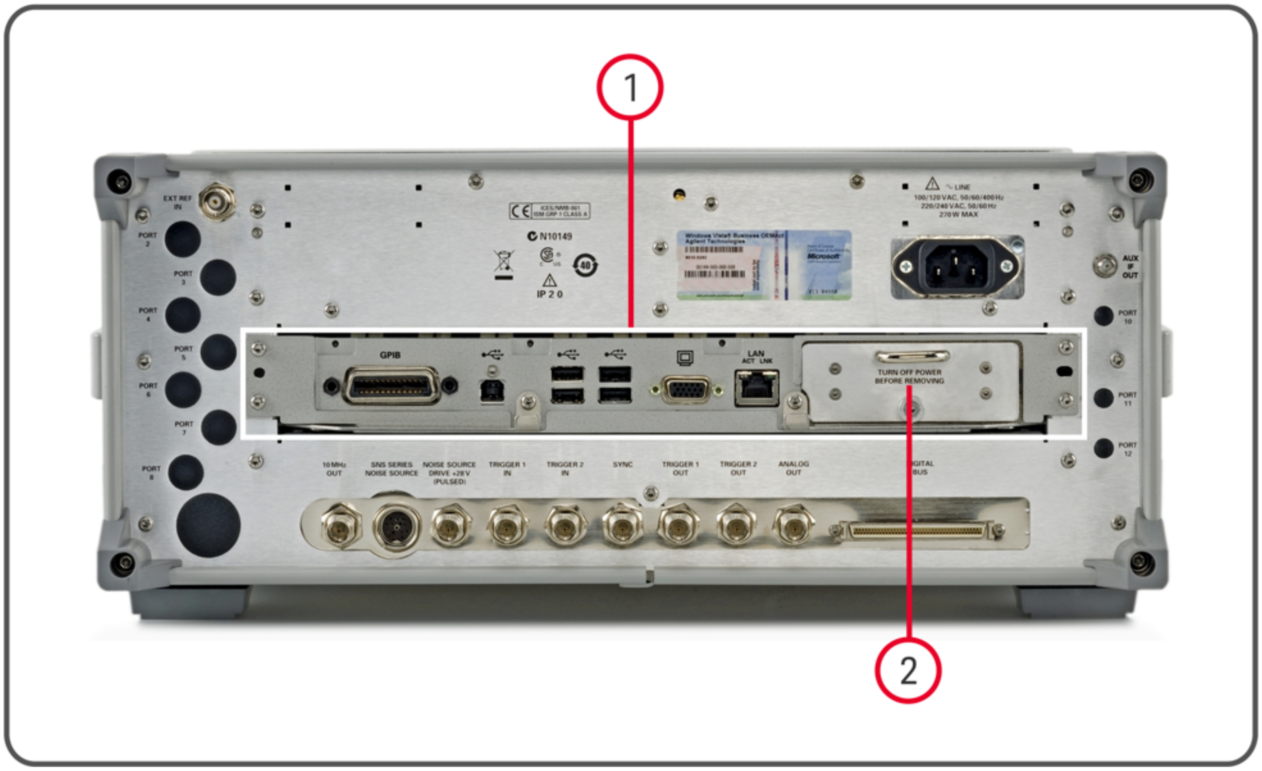
TIP	Application License keys are stored in EEPROM on the A7 Midplane Assembly (as described in Item 8 of Table 4-1 on page 14). Therefore, when replacing the Disk Drive, you do **not** need to back up and restore the license keys. When installing a replacement Disk Drive, ensure that the instrument software 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.

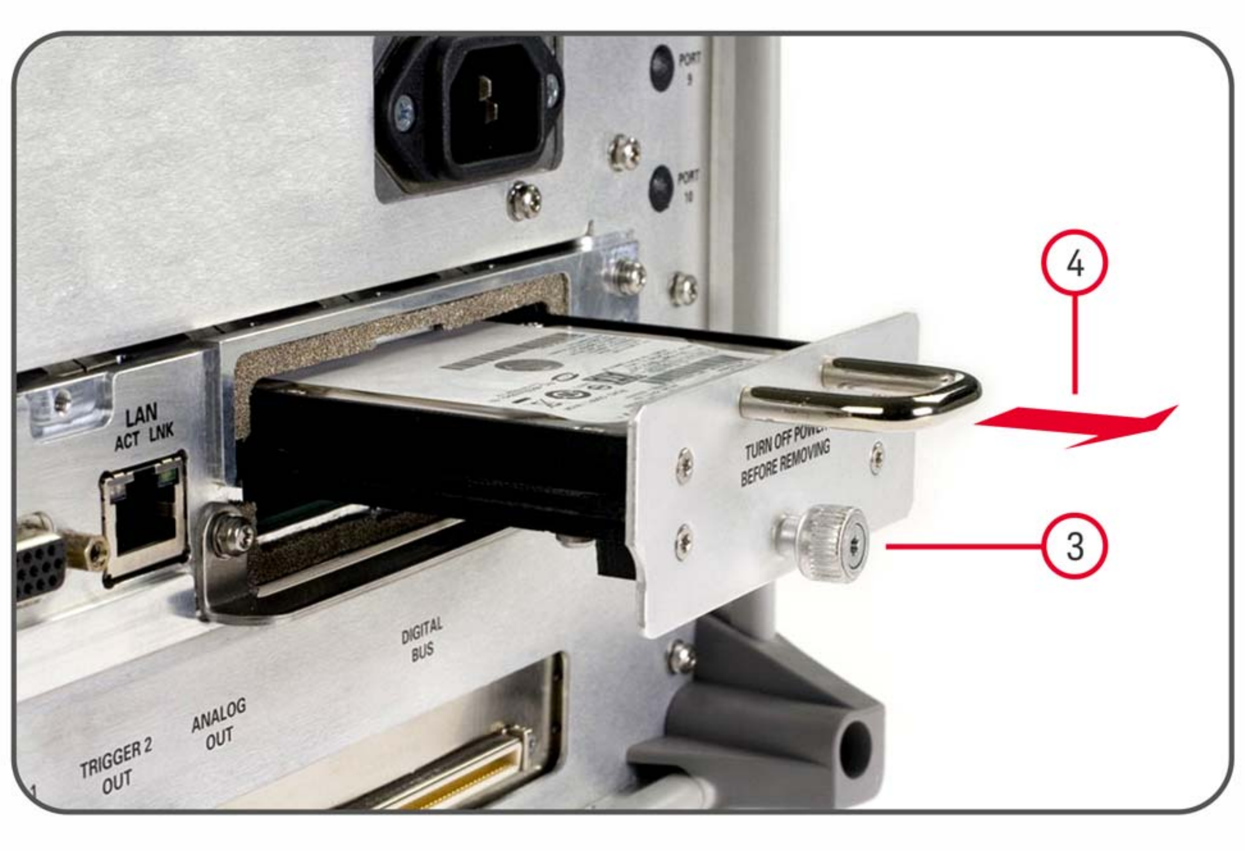
1. Locate the Processor and Disk Drive Assembly on the instrument's rear panel, as shown in Figure 6-1.

Figure 6-1 Instrument Rear Panel & Processor Assembly



2. Locate the removable drive, and its retaining thumbscrew, as shown in Figure 6-1.
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 partially 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 User and Remote Interface Security Measures

This chapter discusses options that are available to you to control and configure 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.

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 35 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.

Details of all these features are provided in the "Windows Security" section of the Keysight MXE EMI Receiver: Getting Started Guide.

Determining the Instrument’s Operating System

You can easily determine your instrument’s operating system version as follows:

1. Using the instrument front-panel, press **System** > **Show** > **System**
2. The System Information Screen appears. If the list of options includes `N9038A-W7X`, then the operating system is Windows 7. If the list of options includes `N9038A-WXP`, then the operating system is Windows XP.

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 32

“Configuring USB for Read-only” on page 35

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.)

The procedure for disabling and enabling AutoPlay depends on your instrument’s operating system (either Windows 7 or Windows XP). To determine the operating system version of your instrument, see “Determining the Instrument’s Operating System” on page 32.

Windows 7

If your instrument has the Windows 7 operating system, 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.

If you want to understand details of how this AutoPlay setting affects the Windows Registry, see the Windows XP discussion below.

Windows XP

You can change the AutoRun configuration by editing the value of one of two Windows Registry keys. The Windows Registry is a database that stores critical configuration information for the instrument’s operating system.

CAUTION Exercise extreme caution whenever you edit the Windows Registry. Entering an incorrect Registry value, or accidentally deleting Registry keys, may have serious consequences that can prevent the system from starting, or require that you reinstall Windows. The instructions in “Disable & Enable Procedure” on page 34 below assume that you are familiar with the use of the

Windows Registry Editor to modify Registry settings.

Registry Key Definitions

AutoRun can be configured per-machine or per-user.

NOTE If the per-machine Registry key is present, its settings override those of the per-user Registry key.

The Registry key that controls the **per-machine** AutoRun settings is:

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun`

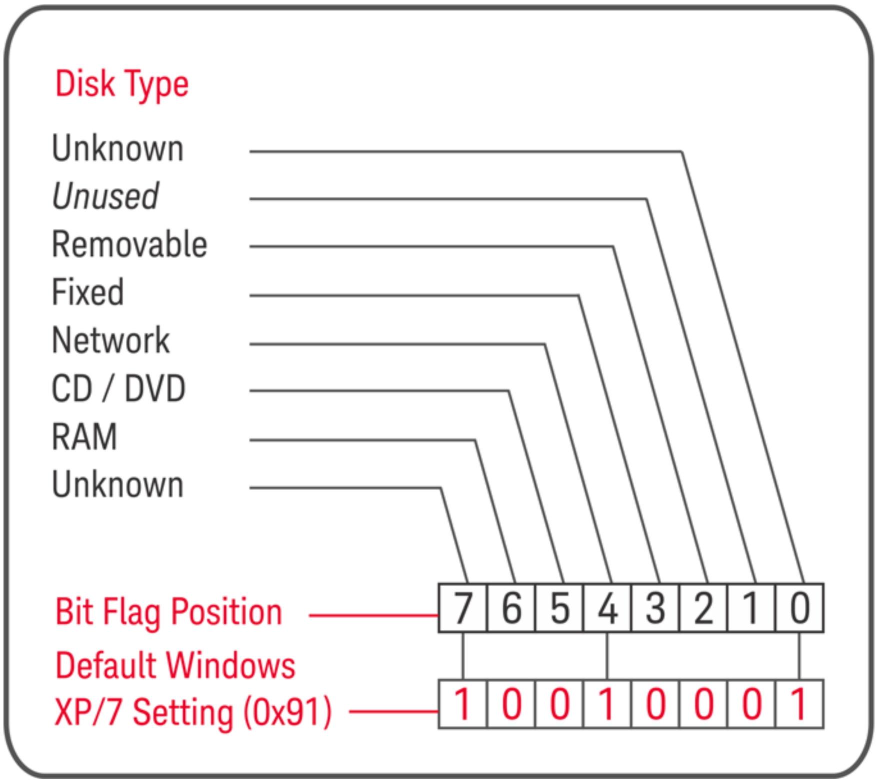
The Registry key that controls the **per-user** AutoRun settings is:

`HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\NoDriveTypeAutoRun`

In the following discussions, we use the industry-standard abbreviation `HKLM` for the root key `HKEY_LOCAL_MACHINE`, and the industry-standard abbreviation `HKCU` for the root key `HKEY_CURRENT_USER`.

The DWORD value of either of these entries represents a set of single-bit flags. Each flag specifies the AutoRun setting for a specific drive type, as shown in Figure 7-1. Setting a bit flag to 1 disables AutoRun for that drive type.

Figure 7-1 AutoRun Flag Definitions for NoDriveTypeAutoRun Registry entry



As shown in Figure 7-1 above, the default Windows XP (post-SP2) and Windows 7 value for this entry is `0x91` (under the entry `HKCU\...\NoDriveTypeAutoRun`). This setting disables AutoRun for `Unknown` and `Network` drives, but enables AutoRun for `Removable`, `Fixed`, `CD/DVD` or `RAM` drives.

You can disable AutoRun for all drive types by changing the value to `0xFF`, as described in the following section.

Disable & Enable Procedure

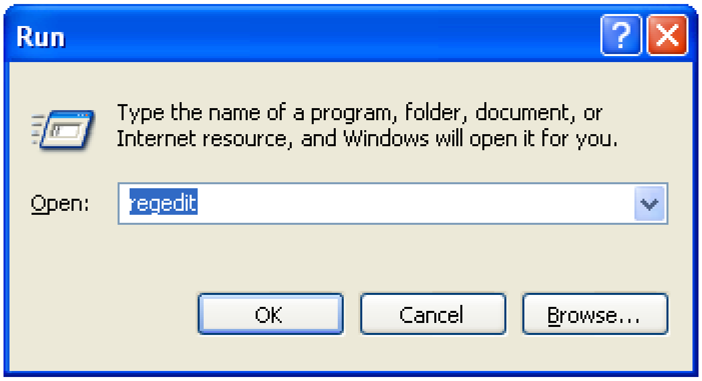
In view of the interaction between the per-machine and per-user Registry settings, as described above, it is recommended that, if both keys exist in your instrument's Registry, you should alter the settings of **both** Registry keys to the same value at the same time.

Use the following procedure to disable AutoRun for all drive types, or to revert all AutoRun settings to their Windows XP or Windows 7 default values. (Note that if your instrument has a Windows 7 operating system, there is a simpler way to do this via the Control Panel; see "Windows 7" on page 32 above.)

1. Open the Windows Registry editor, using one of the following methods depending on your instrument's operating system:

   a. For Windows XP, select **Run...** from the Windows Start menu. Then, type `regedit` into the Windows Run dialog box, as shown in Figure 7-2 below, and click **OK**.

   Figure 7-2 Windows XP Run Dialog

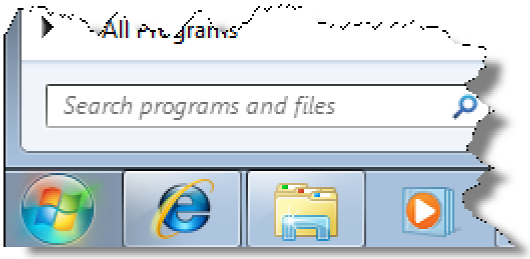


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit

   b. For Windows 7, click the Windows **Start** button at the bottom left of the screen, type `regedit` into the **Search programs and files** box, as shown in Figure 7-3 below, then press **Enter**.

   Figure 7-3 Windows 7 Search edit box



2. The Registry Editor window appears. Using the tree view control on the left of the window, navigate to the per-machine (`HKLM`) key: `HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer`.

3. To **disable** AutoRun for all drive types, set the value of entry `NoDriveTypeAutoRun` to `0xff`.

   To **revert** AutoRun settings to the Windows default values, set `the value of entry NoDriveTypeAutoRun` to `0x91`.

4. Again using the tree view control on the left of the Registry Editor window, navigate to the per-user (`HKCU`) key: `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer`.
5. To **disable** AutoRun for all drive types, set the value of entry `NoDriveTypeAutoRun` to `0xff`.

   To **revert** AutoRun settings to the Windows default values, set the value of entry `NoDriveTypeAutoRun` to `0x91`.
6. From the Registry Editor menu, select **File** > **Exit** to save the settings and exit the editor.
7. Shut down and restart the instrument, to enable the new settings to take effect.

Microsoft AutoRun Patch

NOTE The information in this section applies only to Windows XP. If your instrument has a Windows 7 operating system, you do not require this patch.

There is a defect in Windows XP that compromises the ability to disable AutoRun. This defect has been fixed by a patch from Microsoft, as described in the Microsoft Knowledge Base Article ID: 967715.

This patch has been included in new instrument shipments from the factory since revision A.03.00.

After the patch has been applied, there will be a Registry entry at:

`HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\HonorAutorunSetting` with a default value of 1.

More Information

The following Wikipedia articles provide more information about AutoRun and AutoPlay:

http://en.wikipedia.org/wiki/AutoRun

http://en.wikipedia.org/wiki/AutoPlay

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. For details of how to log on to the instrument as the Administrator, see the Keysight MXE EMI Receiver: Getting Started Guide. To change the setting, do the following:

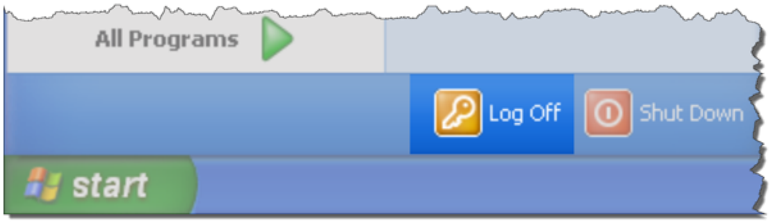
1. If you are **not** currently logged on to the instrument as the Administrator, you must log off.

   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, use one of the following procedures, depending on your instrument’s operating system:

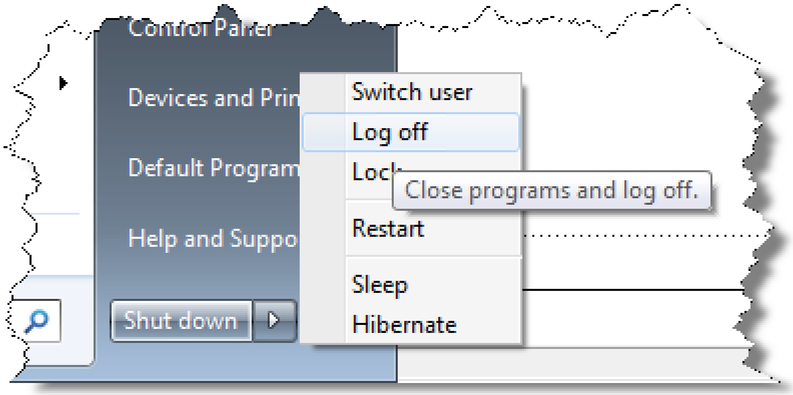
   a. For Windows XP, select **Log Off** from the Windows XP Start menu (as highlighted in Figure 7-4 below), then click **Log Off** in the Log Off Windows dialog that appears.

Figure 7-4 Log Off Button in Windows XP Start Menu



b. For Windows 7, click the Windows **Start** button, then select **Shut down > Log off** from the Windows Start menu, as shown in Figure 7-5 below.

Figure 7-5 Windows 7 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.

8 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 27.

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

3. **Keysight MXE EMI Receiver: Getting Started Guide**

   Keysight Technologies 2011-2014. Part Number: subject to change as document is revised.

   A printed copy of this document is supplied with each instrument.

   It is also available in Acrobat (PDF) form:

   - on the Documentation DVD supplied with each instrument,
   - on the instrument’s disk drive at the following location:
     C:\Program Files\Agilent\SignalAnalysis\Infrastructure\Help\bookfiles\getstart.pdf
   - via download from:
     http://www.keysight.com/find/mxe_emi_receiver_getting_started_guide

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.