Infiniium MXR/EXR-Series Real-Time Oscilloscopes

Declassification and Security Document

This document describes instrument security features and the steps to declassify an instrument through memory sanitization or removal. The following Infiniium MXR-Series oscilloscope models are covered by this document:

Table 1 Infiniium MXR-Series real-time oscilloscopes

8-Channel Model	4-Channel Model	Bandwidth	Sampling rate
MXR608A/B	MXR604A/B	6 GHz	16 GSa/s
MXR408A/B	MXR404A/B	4 GHz	16 GSa/s
MXR258A/B	MXR254A/B	2.5 GHz	16 GSa/s
MXR208A/B	MXR204A/B	2 GHz	16 GSa/s
MXR108A/B	MXR104A/B	1 GHz	16 GSa/s
MXR058A/B	MXR054A/B	500 MHz	16 GSa/s

Table 2 Infiniium EXR-Series real-time oscilloscopes

8-Channel Model	4-Channel Model	Bandwidth	Sampling rate
EXR608A	EXR604A	6 GHz	16 GSa/s
EXR408A	EXR404A	4 GHz	16 GSa/s
EXR258A	EXR254A	2.5 GHz	16 GSa/s
EXR208A	EXR204A	2 GHz	16 GSa/s
EXR108A	EXR104A	1 GHz	16 GSa/s
EXR058A	EXR054A	500 MHz	16 GSa/s

Contacting Keysight Sales and Service Offices

Help on test and measurement products and information on finding a local Keysight office is available at http://www.keysight.com/find/assist.

NOTE In all communication with Keysight, refer to the product by its model number and full serial number so the Keysight representative can determine whether your unit is still within its warranty period.

Security Terms and Definitions

Term	Definition
Clearing	The process of eradicating the data on media before reusing the media so 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.
Instrument declassification	A term that refers to procedures that must be undertaken before an instrument can be removed from a secure environment, such as when the instrument is returned for calibration. Declassification procedures include memory sanitization and/or memory removal. Keysight declassification procedures are designed to meet the requirements specified by the DSS NISPOM security document (DoD 5220.22-M chapter 8).
Sanitization	The process of removing or eradicating stored data so 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. 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” issued by the Cognizant Security Agency (CSA) and referenced in National Industrial Security Program Operating Manual (NISPOM) DoD 5220.22-M ISL 01L-1 section 8-301.
Security erases	A term used to refer to either the clearing or sanitization features of Keysight instruments.

Instrument Memory and Volatility Information

The following table provides information on the types of memory available in your oscilloscope. It includes the size of memory, how it is used, its location, volatility, and sanitization procedure.

Infiniium MXR/EXR-Series Real-Time Oscilloscopes Instrument Memory

Memory Type & Size	Is memory user-accessible as a mass storage device?	Writable during normal operation?	Is user data stored in device?	Data retained when powered off?	Purpose / Contents	Data Input Method	Location in Instrument, Remarks	Sanitization Procedure
Main memory (SDRAM) 8 GB on "A" models, 32 GB on "B" models	No	Yes	Yes	No	PC main memory	Operating system (not user)	On CPU board	Cycle power
Hard drive	Yes	Yes	Yes	Yes	Storage device for application data, operating system, option license keys, and other applications	Open PC hard drive for multiple uses	Connected via SATA cable to motherboard	Remove hard drive; replace with a sanitized hard drive
Acquisition memory (HMC) 4 GB x1 or x2*	No	Yes	Yes	No	Acquisition memory	Firmware operations	Channel acquisition board	Cycle power
Acquisition memory (SDRAM) 512 MB x1 or x2*	No	Yes	Yes	No	Acquisition memory	Firmware operations	Channel acquisition board	Cycle power
Plotting memory (SDRAM) 2 x 1 GB	No	Yes	Yes	No	Plotting memory	Firmware operations	Main board	Cycle power
FPGA Device Memory (SDRAM) 80.4 Mb	No	Yes	Yes	No	FPGA Device	Firmware operations	Main board	Cycle power
Flash memory 2 Gb	No	No	No	Yes	Store calibration data, licensing information, model & serial numbers	Calibration operation, license update, factory configuration	Main board	
Flash memory 512 Mb	No	No	No	Yes	Store FPGA image	USB from CPU board (internal cabling only)	Main board	
EEPROM (2 Kb)	No	No	No	Yes	Store board serial number information	Factory configuration	Main board	
EEPROM (2 Kb x1 or x2)*	No	No	No	Yes	Store board serial number information	Factory configuration	Channel acquisition board	
EEPROM (2 Kb)	No	No	No	Yes	Store board serial number information	Factory configuration	Front-panel board	
FPGA Device (SDRAM) 2 Mb	No	No	No	No	Keyboard micro controller program	Firmware operations	Front-panel board	

* x1 on 4-channel models, x2 on 8-channel models

Memory Clearing, Sanitization, and Removal Procedures

Follow these steps to declassify Keysight Infiniium MXR/EXR-Series oscilloscopes.

1. To clear all volatile RAM memory, cycle power on the oscilloscope.
2. To ensure a generic setup in the non-volatile hard disk drive, choose **Control > Factory Default** from the main menu.
3. Remove the hard disk drive from the instrument completely, and replace it with an Infiniium MXR/EXR-Series oscilloscope hard drive that has no security issues. (For details about the drive, refer to its data sheet.)

   The hard disk drive contains the Windows 10 operating system, oscilloscope operating system, setups, waveform memories, waveform files, screen images, and calibration data for the oscilloscope and probes.

The declassification procedure declassifies the following RAM:

- All RAM on the motherboard, which is cleared when power is cycled.
- Volatile video RAM for saving waveform display data and volatile display RAM for screen colors, which is stored to the RAM on the motherboard. This RAM is used to aid in multiplexing the graticule and alphanumeric information with the dynamic waveform information of the acquisition section of the oscilloscope.

User and Remote Interface Security Measures

This section describes options you can use to control and configure remote access to the instrument, including operating system security features and USB interfaces.

Operating System Security Features

The instrument's Windows 10 operating system includes features you can invoke or modify to enhance system security.

- The instruments provide 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.
- The instruments have the standard Windows Firewall enabled by default to provide more protection for instruments that have a network (or internet) connection.
- The instruments provide the ability to install standard third-party antivirus and spyware detection software designed for use with Windows. If your instrument uses a network (or internet) connection, using this software is advisable.

USB Interfaces

The instrument's Microsoft Windows operating system can be configured to improve the security of the USB interfaces.

Disabling or Enabling AutoRun/AutoPlay

AutoRun and AutoPlay are Windows features that help you select appropriate actions when new media and devices are detected. AutoRun 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 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 the "Disable & Enable Procedure" section assume 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`

The following section uses 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. Setting a bit flag to 1 disables AutoRun for that drive type.

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

Disable & Enable Procedure

Due to the interaction between the per-machine and per-user Registry settings, 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 default values.

1. Open the Windows Registry editor by clicking the Windows Start icon, typing **`regedit.exe`** into the Search box, and pressing **[Enter]**. The Registry Editor window appears.
2. Using the tree view control on the left side 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`. If the entry does not exist, you can create it by right-clicking and entering `NoDriveTypeAutoRun`.

   To revert AutoRun settings to the Windows default values, set the value of entry `NoDriveTypeAutoRun` to `0x91`.
4. Use the tree view control to 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.

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

Procedure for Declassifying a Faulty Instrument

If the instrument is not functioning and you are unable to use the security functions, you must physically remove the solid state drive, if present, from the instrument.

Edition 4, March 2024

54925-97028

www.keysight.com

KEYSIGHT TECHNOLOGIES