Agilent 86100C DCA-X Wide-Bandwidth Oscilloscope Mainframe

Declassification and Security

5 May 2012

Contacting Agilent Sales and Service Offices

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

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

Product Declassification and Security

Model Number(s): 86100C
Product Name: **Infiniium DCA-X Wide-Bandwidth Oscilloscope Mainframe**
Product Family Name: Infinnium DCA
Alternate Product Numbers:

This document describes instrument security features and the steps to declassify an instrument through memory sanitization or removal. For additional information please go to
www.agilent.com/find/ad

Table of Contents

Terms and Definitions

Definitions:

Clearing – Clearing is the process of eradicating the data on media before reusing the media so that the data can no longer be retrieved using the standard interfaces on the instrument. Clearing is typically used when the instrument is to remain in an environment with an acceptable level of protection.

Sanitization – Sanitization is the process of removing or eradicating stored data so that the data cannot be recovered using any known technology. Instrument sanitization is typically required when an instrument is moved from a secure to a non-secure environment such as when it is returned to the factory for calibration. (The instrument is declassified) Agilent memory sanitization procedures are designed for customers who need to meet the requirements specified by the US Defense Security Service (DSS). These requirements are outlined in the "Clearing and Sanitization Matrix" issued by the Cognizant Security Agency (CSA) and referenced in National Industrial Security Program Operating Manual (NISPOM) DoD 5220.22M ISL 01L-1 section 8-301.

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

Instrument declassification – A term that refers to procedures that must be undertaken before an instrument can be removed from a secure environment such as is the case when the instrument is returned for calibration. Declassification procedures will include memory sanitization and or memory removal. Agilent declassification procedures are designed to meet the requirements specified by the DSS NISPOM security document (DoD 5220.22M chapter 8)

Instrument Memory

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

Summary of instrument memory - base instrument

Memory Type	Writable During Normal Operation?	Data Retained When Powered Off?	Purpose/Contents	Data Input Method	Location in Instrument and Remarks	Sanitization Procedure
Hard Drive (built in HDD) 40-80 GB	Yes	Yes	Windows XP OS, 86100C Firmware, Calibration Files, User files including instrument states, waveforms, screen shots.	OS, User	Hard Drive (NV)	Drive removal
Main Memory	Yes	No	PC Memory	OS, User	CPU board	Remove Power
EEPROM	No	Yes	FPGA code	NA	Acquisition Board	NA
SRAM	Yes	No	Data Acquisition Control, Storage and Cal Tables	Firmware operations	Acquisition Board	Remove Power

Summary of instrument memory - option ETR

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
SRAM	Yes	No	Acquisition Control	Firmware operations	Counter Board	Remove Power
EEPROM	No	Yes	FPGA Code	NA	Counter Board	NA

Memory Clearing, Sanitization and/or Removal Procedures

This section explains how to clear, sanitize, and remove memory from you instrument for all memory that can be written to during normal operation and for which the clearing and sanitization procedure is more than trivial such as rebooting your instrument.

Hard Drive

Description and purpose	Instrument OS (Windows XP), Instrument firmware, Instrument Cal data, Customer saved data including waveforms, screen shots, instrument set up etc.
Size	40-80 GB
Memory clearing	Remove and secure HDD as described below
Memory sanitization	Remove and secure HDD as described below
Memory removal	Remove HDD as described below: For Option 092 (Standard HD) the user must remove the instrument cover and locate the HDD on the main deck near the CPU board. The drive can be removed by taking four screws from the mounting bracket and disconnecting the SATA cables. For Option 090 (Removable HD) the hard drive can be removed externally by unscrewing the rear access panel and pulling the drive out. Option 090 ships with two identical drives so one can be kept in the secure area and the second hard drive can be used outside of the secure area or when returning the instrument to Agilent for calibration or repair. The online help system contains information for copying calibration data to the secure drive when the instrument is returned after a calibration or repair.
Write protecting	N/A
Memory validation	N/A
Remarks	

User and Remote Interface Security Measures

USB Mass Storage Device Security
>   To prevent USB write capability on XPSP2, create a new registry key of:
>   **HKLM\System\CurrentControlSet\Control\StorageDevicePolicies**.
>> Then create a **REG_DWORD** entry in it called **WriteProtect**. Set it to "**1"** and you'll be
>> able to read from USB drives but not write to them

Remote Access Interfaces
>   The user is responsible for providing security for the I/O ports for remote access by controlling physical
>   access to the I/O ports. The I/O ports must be controlled because they provide access to all user settings,
>   user states and the display image.
>   The I/O ports include RS-232, GPIB and LAN.
>   The LAN port provides the following services, which can be selectively disabled:
>>   a) http
>>   b) ftp
>>   c) sockets
>>   d) telnet
>   There is also a 'ping' service, which presently cannot be selectively disabled. The concern here might be
>   that it is possible to discover IP addresses of connected instruments in order to query their setups over the
>   net or break into the code.

Reset Remote Interface (GPIB) Address.
>   1. Click **Utilities, Remote Interface**.
>   2. Enter **7**.
>   3. Close the window

Procedure for Declassifying a Faulty Instrument

If the instrument is not functioning and you are unable to use the security functions, you can declassify the
instrument by removing the hard drive as described above.

To Remove the Instrument Cover to Access Non-removable HDD

CAUTION Electrostatic discharge (ESD) can damage or destroy electrostatic components.
All work on electronic assemblies should be performed at a static-safe work
station. See "Electrostatic Discharge Information" on page 8 for more information
on preventing ESD.

1. Disconnect the power cord from the instrument.

**WARNING Opening covers or removing parts is likely to expose dangerous voltages.
Disconnect the instrument from all voltages before it is opened.**

2. Remove the four cabinet screws and four feet screws, as shown in Figure 1.
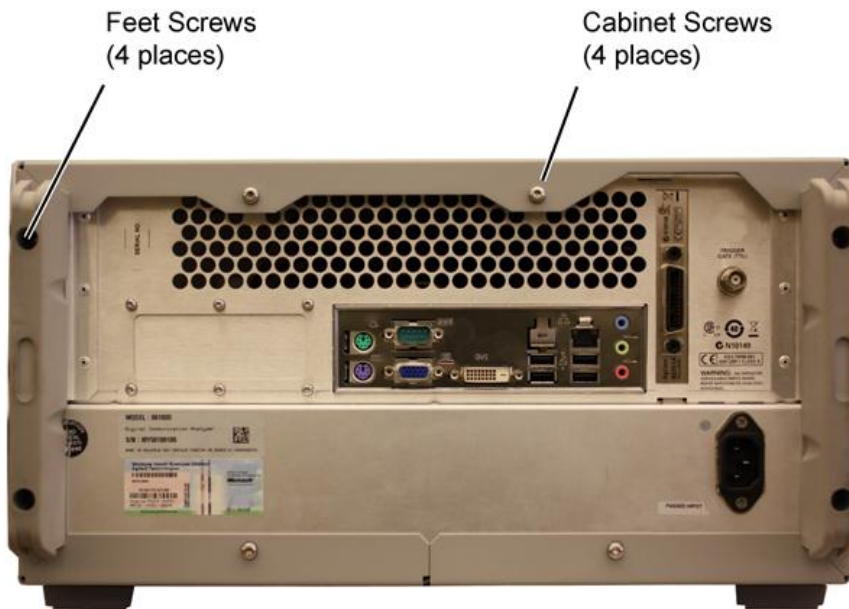

Figure 1. Removing the Rear Cabinet Screws

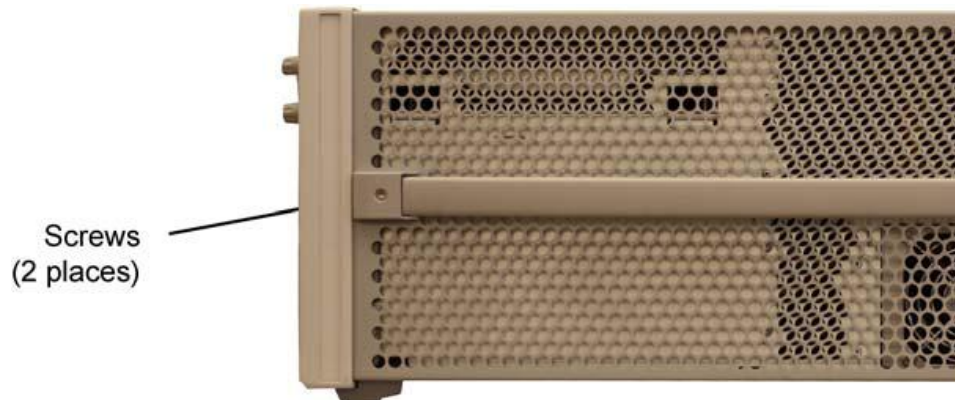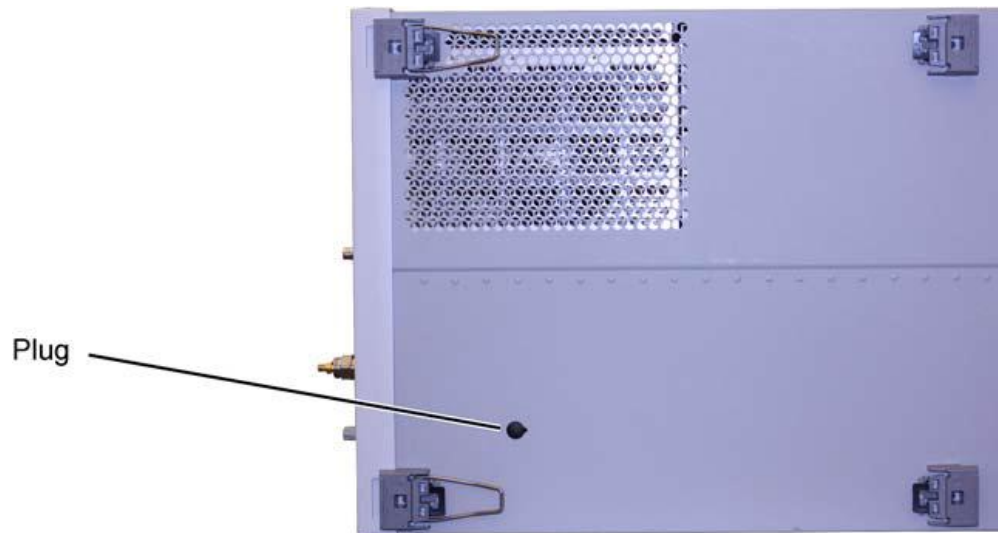**3.** Remove the two screws that secure each handle to the side of the mainframe, as shown in Figure 2.

Figure 2. Removing the Side Handles

4. Use a small flat- bladed screw driver to remove the hole plug on the bottom of the instrument to avoid damaging the plug.

Plug

Figure 3. Removing the Timebase Adjustment Access Plug

5. To slide the cover off the instrument, first turn the mainframe upside down on the bench. Place your hands on each side of the cover, and using your thumbs, push the instrument out the front of the cover.

6. Once the instrument has begun to slide forward, you can then set the instrument on its side and slide the cover off completely.