33600-Series Waveform Generators

This manual provides the documentation for the following instruments:
33611A, 33612A, 33621A, 33622A

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

KEYSIGHT

MEMORY INFORMATION AND PROCEDURES

Notices

Trademark Acknowledgements

N/A

Manual Part Number

5991-1950

Print Date

October 2025

Supersedes: October 2013

Published in USA

Keysight Technologies Inc.
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 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 WILL 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.

Warranty

This Keysight technologies instrument product is warranted against defects in material and workmanship for a period of one year from the date of shipment. During the warranty period, Keysight Technologies will, at its option, either repair or replace products that prove to be defective. For warranty service or repair, this product must be returned to a service facility designated by Keysight Technologies. Buyer shall prepay shipping charges to Keysight Technologies, and Keysight Technologies shall pay shipping charges to return the product to Buyer. For products returned to Keysight Technologies from another country, Buyer shall pay all shipping charges, duties, and taxes.

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/trueform

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

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

Information on preventing instrument damage can be found at:

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/techsupport

Table of Contents

Contacting Keysight Sales and Service Offices

Assistance with test and measurement needs, and information on finding a local Keysight office, is available on the Internet at:

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

If you do not have access to the Internet, please contact your field engineer.

NOTE

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

Products Covered by this Document

Product Family Name	Product Names	Model Numbers
Trueform Waveform Generator	33600-Series Waveform Generators	33611A, 33612A, 33621A, 33622A

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

For additional information, go to:

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

NOTE

Be sure that all information stored by the user in the instrument that needs to be saved is properly backed up before attempting to clear any of the instrument memory. Keysight 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.

Security Terms and Definitions

Term	Definition
Clearing	As defined in Section 8-301a **of** DoD **5220.22-M**, clearing is the process of eradicating the data on media before reusing the media so that the data can no longer be retrieved using the standard interfaces on the instrument. Clearing is typically used when the instrument is to remain in an environment with an acceptable level of protection.
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**, Chapter 8.
Sanitization	As defined in Section 8-301b of **DoD 5220.22-M**, sanitization is the process of removing or eradicating stored data so that the data cannot be recovered using any known technology. Instrument sanitization is typically required when an instrument is moved from a secure to a non-secure environment, such as when it is returned to the factory for calibration. 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**.
Secure Erase	Secure Erase is a term that is used to refer to either the clearing or sanitization features of Keysight instruments.

Instrument Memory

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

Table 1: Summary of instrument memory

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
System Flash (NAND Flash) 45 MB	Yes	Yes	Contains Operating System, instrument firmware, and the firmware recovery image	Factory Install / Firmware Upgrade	Front panel U12 1819-0748 (same chip as other parts, but managed separately)	N/A, contains no application-specific information.
User Flash (NAND Flash) 974 MB	Yes	Yes	Arbitrary waveforms, user data files, screen capture files, and user instrument states	User-saved data	Front panel U12 1819-0748 (same chip as other parts, but managed separately)	NAND Flash Sanitize – See Table 2.
Calibration Store (NAND Flash) 1 MB	Yes	Yes	Calibration constant storage, calibration count, calibration security code, and calibration message	Factory or Service and user calibration	Front panel U12 1819-0748 (same chip as other parts, but managed separately)	N/A, contains no application-specific information.
Front panel microprocessor (Flash) 8 kB	No	Yes	Front panel microprocessor execution code storage	Factory Install / Firmware Upgrade	Front panel microprocessor U10 18F22-3182 (same chip as other parts, but managed separately)	N/A, contains no application-specific information.
Front panel microprocessor (EEPROM) 512 Bytes	Yes	Yes	Stores ON/OFF state	Operating System or microprocessor execution code	Front panel microprocessor U10 1822-3182 (same chip as other parts, but managed separately)	N/A, contains no application-specific information.

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
Front panel microprocessor (RAM) 256 Bytes	Yes	No	Front panel microprocessor temporary execution data	Microprocessor execution code	Front panel microprocessor U10 1822-3182 (same chip as other parts, but managed separately)	Power cycle
Main processor (ROM) 32 kB	No	Yes	Main processor execution code	Manufacturer programmed	Front panel U1 1822-4268 (same chip as other parts, but managed separately)	N/A, contains no application-specific information.
Main processor (SRAM) 8 kB	Yes	No	Temporary execution data	Operating System	Front panel U1 1822-4268 (same chip as other parts, but managed separately)	Power cycle
Main RAM (SDRAM) 2 G-bit	Yes	No	Temporary execution data	Operating System	Front Panel U6 1819-0711	Power cycle
Back-up (EEPROM) 2 kB	Yes	Yes	Back-up storage for model number and serial number	Factory Install	Main Board U202 1819-0128	N/A, contains no application-specific information.
33611A/33621A FPGA RAM (SRAM) 6.331 Mbits	Yes	No	Data processing	Factory Install / Firmware Upgrade	Mezzanine board U301 1822-4550	Power cycle
33612A/33622A FPGA RAM (SRAM) 8.248 Mbits	Yes	No	Data processing	Factory Install / Firmware Upgrade	Mezzanine board U301 1822-3811	Power cycle
Waveform RAM (SDRAM) 256 MB	Yes	No	Synthesizer waveform memory for channel 1	Application loads memory	Mezzanine board U601/U602 1819-0653	Power cycle

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
Waveform RAM (SDRAM) 256 MB	Yes	No	Synthesizer waveform memory for channel 2	Application loads memory	33612A/33622A Mezzanine board U701/U702 1819-0653	Power cycle
FPGA 1M-bit	Yes	Yes	Control interface between main processor and GPIB	Flash Memory	GPIB interface 1822-1960	N/A, contains no application-specific information.
Flash 1 M-bit	No	Yes	Stores GPIB control FPGA program bits	Factory Install / Preprogrammed part	GPIB interface P000-80001	N/A, contains no application-specific information.

Summary of Memory Declassification Procedures

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

NOTE Read this entire document before using any sanitization procedure. Failure to do so may necessitate returning the instrument to an Authorized Keysight Service Center for firmware downloads and recalibration.

Table 2: User Flash (NAND Flash)

Description and purpose	This is the user's partition of internal storage that uses a NAND flash device. Storage may include instrument state files, screen capture images, and arbitrary waveforms.
Size	974 MB
Memory clearing	To remove files from the file system: On the front panel press: System > System Setup > Manage Files On the remote interface use: MMEMory:DELete <file> See the Trueform series programming reference for more information.
Memory sanitization	Performing an instrument sanitization requires the instrument Security option (SEC) to be installed. Please refer to the Trueform Series Operating and Service Guide for more information on available options. On front panel press: System > Test/Admin > Security > NISPOM Sanitize > Sanitize From the remote interface, use: SYSTem:SECurity:IMMediate Note: This operation requires the instrument Security option to be installed. The instrument's security setting must be unlocked to perform these actions. Executing a sanitize operation will increment the instrument's secure count. This sanitizes all user-accessible instrument memory and restarts the instrument. This includes deleting and sanitizing all arbitrary waveforms, user-defined state files, and user-defined I/O settings. The instrument's firmware, serial/model number, and calibration data are preserved. This command complies with requirements in chapter 8 of the National Instrument Security Program Operating Manual (NISPOM). This command is for users, such as military contractors, who must comply with NISPOM. Specifically, the action will fully declassify all non-volatile memory using the methods specified in the June 28, 2007 DSS Memory Clearing and Sanitization Matrix See the Trueform Series Operating and Service Guide for more information.
Memory removal	This memory cannot be removed without damaging the instrument. The user may remove the front panel assembly on which the memory chip resides. Remove the front panel board per the disassembly instructions in the Trueform Series Operating and Service Guide.
Memory validation	N/A
Remarks	N/A

Memory Sanitization Procedures

Secure Erase All

NOTE

Performing an instrument sanitization requires the Instrument Security Option (SEC) to be installed, and is recommended for customers, such as military contractors, who must comply with NISPOM. Excessive use of this command may cause premature failure of the flash memory. See the Trueform Series Programming Reference for more information on available options.

On front panel press: System > Test/Admin > Security > NISPOM Sanitize > Sanitize
From the remote interface, use: SYSTem:SECurity:IMMediate

Note: This operation requires the instrument Security option to be installed. The instrument's security setting must be unlocked to perform these actions. Executing a sanitize operation will increment the instrument's secure count.

This sanitizes all user-accessible instrument memory and restarts the instrument. This includes deleting and sanitizing all arbitrary waveforms, user-defined state files, and user-defined I/O settings. The instrument's firmware, serial/model number, and calibration data are preserved.

This command complies with requirements in chapter 8 of the National Instrument Security Program Operating Manual (NISPOM). This command is for users, such as military contractors, who must comply with NISPOM. Specifically, the action will fully declassify all non-volatile memory using the methods specified in the June 28, 2007 DSS Memory Clearing and Sanitization Matrix.

See the Trueform Series Operating and Service Guide for more information.

User and Remote Interface Security Measures

Screen and Annotation Blanking

To provide basic security, you may disable the front panel display.

To disable the display on the front panel, press: System > System Setup > User Settings > Display Options > Display OFF
Note: pressing any key will enable the display again.

To disable the display on the remote interface, use: DISP OFF
Note: pressing Local will enable the display again.

The display is enabled when power is cycled. See the Trueform Series Operating and Service Guide for more information.

USB Mass Storage Device Security

Not supported

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 most user settings, user states, and the display memory.

The I/O ports include USB, GPIB, and LAN.

With the instrument Security option, modifying these settings requires the instrument password. The secure count will increment when a remote interface is disabled or enabled. See the Trueform Series Operating and Service Guide for more information.

The LAN port provides the following services, which can be selectively disabled:

a) VXI-11
b) Sockets
c) Telnet
d) Web
e) mDNS

To disable LAN services:

On the front panel press: System > I/O Config > LAN Off/On
On the remote interface use: SYSTem:COMMunicate:ENABle <state>, <interface>
For mDNS on the remote interface, use: LXI:MDNS:ENABle <state>

See the Trueform Series Programming Reference for more information.

To disable USB:

On the front panel, press: System > I/O Config > USB Settings > USB SCPI Off/On
On the remote interface use: SYSTem:COMMunicate:ENABle <state>, <interface>

To disable GPIB:

On the front panel press: System > I/O Config > GPIB Settings > GPIB Off/On
On the remote interface, use: SYSTem:COMMunicate:ENABle <state>, <interface>

To disable the USB device MTP (driverless) connection service:

On the front panel press: System > I/O Config > USB Settings > File Access Off/On
On the remote interface use: SYSTem:COMMunicate:ENABle <state>, <interface>

Note: If the instrument Security option is installed, this requires that the instrument is unlocked. The secure count will increment when this port is disabled or enabled. See the Trueform Series Operating and Service Guide for more information.

How to disable the Front Panel USB Host port

On the front panel press: System > I/O Config > USB Settings > USB Front Off/On
On the remote interface use: SYSTem:USB:HOST:ENABle <state>

Note: This requires the instrument Security option, and that the instrument is unlocked. The secure count will increment when this port is disabled or enabled. See the Trueform Series Operating and Service Guide for more information.

How to disable the Front Panel during remote operation

To programmatically lock out all front panel operation and remote access over the current interface, use the SYSTem:LOCK command. See the Trueform Series Operating and Service Guide for more information.

Calibration Regulation

The instrument requires a password to unsecure the instrument before calibration. The instrument’s calibration count will increment with each successful calibration step.

Firmware Update Regulation

The instrument requires a password to unsecure the instrument before updating firmware. The instrument’s calibration count will increment with each successful update.

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 processor board from the instrument. Once this assembly is removed, you can proceed with one the following options:

- If you have another working instrument, install the processor board into an instrument and erase the memory. Then reinstall the processor board back into the non-working instrument and send it out for repair and calibration. If you discover that the processor board does not function in the working instrument, indicating that it caused the instrument failure, discard the processor board and send the original failed instrument to a repair facility. Be sure to inform the repair facility that the processor board did not function in the working instrument. If the instrument is still under warranty, the repair facility will install a new processor board without charge.
- If you do not have another working instrument, discard the processor board and send the instrument to a repair facility. If the repair facility determines that a new processor board fixes the problem and the instrument is still under warranty, you will not be charged for the new board. If they determine that the failure was caused by something other than the processor board, you will be charged for the new board even though the instrument is still under warranty. The customer is responsible for removing and replacing the storage media assemblies at their secure location. Refer to the service guide for assembly replacement procedures.

References

1. **DoD 5220.22-M, “National Industrial Security Program Operating Manual (NISPOM)”**

   United States Department of Defense. Revised February 28, 2006.

   May be downloaded in Acrobat (PDF) format from:

   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