DATA SHEET

Enhanced Security Option

(DSOXT3SECA, DSOX4SECA, and DSOX6SECA)

For Keysight InfiniiVision X-Series Oscilloscopes

KEYSIGHT TECHNOLOGIES

Introduction

Increased security of data and communication management in test instrumentation is often required in highly secure environments. This is especially true in the aerospace-defense and automotive industries. Secure Erase, which performs a secure erasure of all non-volatile memory in compliance with NISPOM chapter 8 requirements, is a standard feature in all Keysight InfiniiVision X-Series oscilloscopes. The Enhanced Security option, which is available on Keysight's InfiniiVision 3000T, 4000, and 6000 X-Series oscilloscopes, adds the following more stringent security features.

- Ability to dismount non-volatile memory causing all user-accessible files to be wiped clean on each power cycle, but otherwise retains all save/recall features while operating the oscilloscope
- Ability to disable communication ports (USB and Ethernet) to prevent data from entering or leaving the oscilloscope
- Ability to disable firmware upgrades
- Password protection of the above features

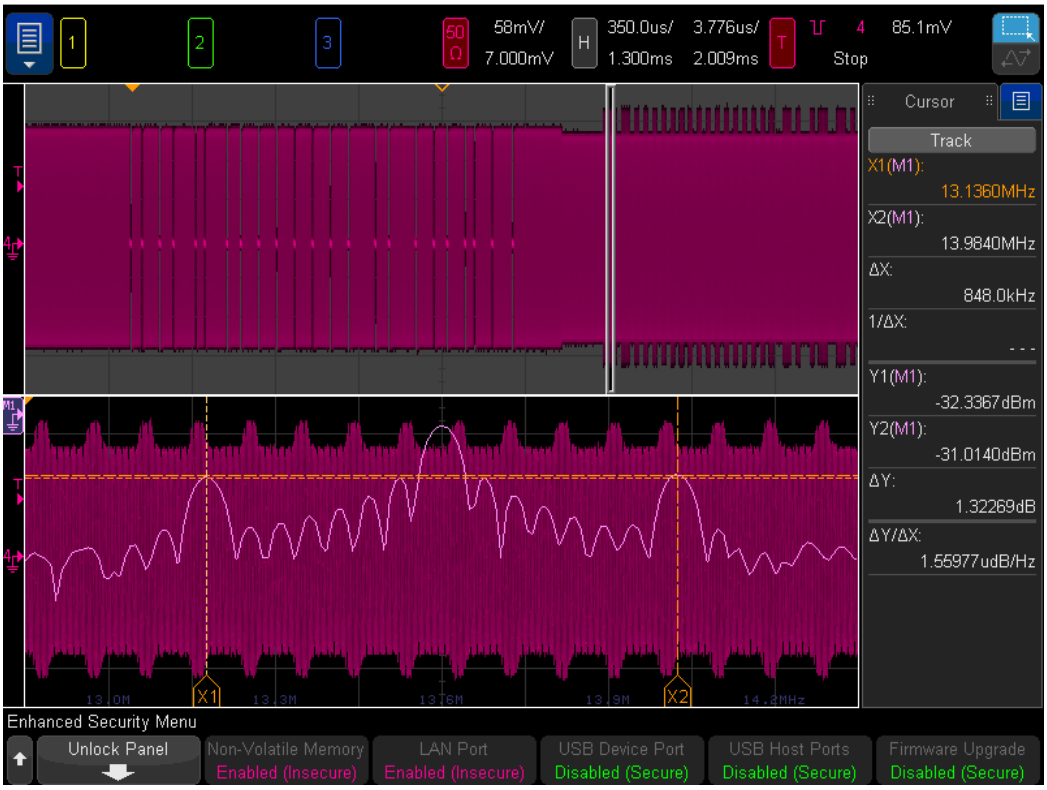

Figure 1. Locked enhanced security panel showing non-volatile memory enabled (insecure), LAN port enabled (insecure), USB device and host ports disabled (secure), and firmware upgrade disabled, (secure).

Disabling Non-volatile Memory

Disabling non-volatile memory removes the non-volatile (NAND flash) user filesystem of the oscilloscope. When you select to disable non-volatile memory, the user-visible internal filesystem moves into volatile memory (RAM) space. Although the user can browse and use these temporary/volatile memory registers normally while operating the oscilloscope, including internal save/recall registers (setup files, waveform files, mask files, symbolic decoding files, etc.), the user-accessible filesystem resets on each power cycle making user-created files and data from previous sessions non-persistent/erased (volatile). Each time the oscilloscope is powered on, the instrument is restored to a factory default setup configuration, which is stored in non-user-accessible non-volatile memory. This is also true for all licenses and calibration factors, which are also retained and used by the oscilloscope, but are not accessible by the user.

Note that web-based firmware upgrades are also disabled when non-volatile memory has been disabled, even if the oscilloscope's LAN port is enabled.

When the non-volatile memory selection is changed (enabled or disabled), a reboot of the oscilloscope is required for the change status to take effect.

Disabling USB and LAN Ports

The Enhanced Security options allows you to independently select to disable the USB host, USB device, and LAN communication ports for increased levels of security. Disabling the LAN port (secure) unbinds the ethernet adapter. Access to SCPI commands and the scope's web-based user-interface are no longer available when the LAN port has been disabled. Also, the oscilloscope cannot be pinged and is essentially invisible over Ethernet to any device, even if an Ethernet cable is plugged into the scope's hardware LAN port.

When the USB device port is disabled (secure), SCPI connections are not possible. When the USB host port(s) are disabled (secure), external USB storage devices are inaccessible by the user and data is prevented from entering or leaving the oscilloscope.

When USB and/or LAN port selections are changed (enabled or disabled), a reboot of the oscilloscope is required for the change status to take effect.

Disabling Firmware Upgrade

When the firmware upgrade selection is disabled (secure), firmware installers (.ksx files) are prevented from being loaded into or run in the oscilloscope. This applies for both external USB drive firmware upgrades as well as web-based firmware upgrades. Web-based firmware upgrades are also disabled when non-volatile memory has been disabled, even if the firmware upgrade selection is enabled. If firmware upgrades are disabled (secure), licenses can still be installed and recallable files (setup files, mask files, etc.) can be accessed from external media if the appropriate communication ports are enabled.

When the firmware upgrade status is changed (enabled or disabled), a reboot of the oscilloscope is not required. It takes effect immediately.

Passwords Protection

Enabling and disabling the various enhanced security settings are password protected. After the license for the Enhanced Security option has been installed, all features of security will be defaulted to an insecure status (all selections such as non-volatile memory, communication ports, and firmware upgrades will be enabled). All settings are locked behind a password-protected security panel user-interface. To unlock the security user-interface to make any security status changes you must first establish a password by entering it two times. If a password is not established, the security panel is locked by default. Once your password has been established, you can unlock the enhanced security panel to make security status changes, and then relock it at any time without entering your password. On every subsequent power cycle, or if you exit the enhanced security menu, you must enter your established password just once to unlock the panel to make any security status changes (enable or disable selections). Password protection cannot be disabled.

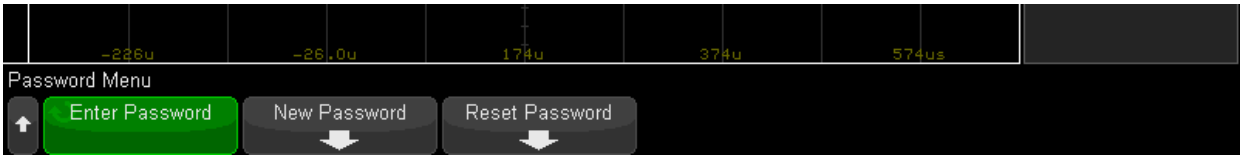

Figure 2. After you select to unlock the enhanced security panel, you can either enter your current password to unlock the panel, change your password, or reset the password.

You can also change your password, which requires that you enter your current password before creating a new one. Resetting the password back to its initial state is also possible. This also requires that you first enter your current password. But if you reset the password, the security panel will immediately lock, and no changes can be made until a new password is established. Note that resetting the password is not secure and will leave all security settings in their last established state (enabled or disabled). Anyone at this point can establish a new password to unlock the panel and make changes. If your password is lost or forgotten, the only way to recover is to return the oscilloscope to a Keysight service center for a clean factory reset.

Related Literature

Literature description	Publication number
InfiniiVision 3000T X-Series oscilloscopes – data sheet	5992-0140
InfiniiVision 4000 X-Series oscilloscopes – data sheet	5991-1103
InfiniiVision 6000 X-Series oscilloscopes – data sheet	5991-4087

Ordering Information

Product description	Model number
Enhanced Security option for InfiniiVision 3000T X-Series oscilloscopes	DSOXT3SECA
Enhanced Security option for InfiniiVision 4000 X-Series oscilloscopes	DSOX4SECA
Enhanced Security option for InfiniiVision 6000 X-Series oscilloscopes	DSOX6SECA

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES