Keysight PNA Network Analyzers

This manual provides documentation for the following PNA-X Pro analyzers:

NA5202A, NA5204A, NA5205A

Notices

Copyright Notice

Manual Part Number

E8356-90070

Edition

Edition 1, September 2025

Supersedes: None

Published by:

Keysight Technologies Inc.
1400 Fountaingrove Parkway
Santa Rosa, CA 95403

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.

U.S Government Rights

The Software is “commercial computer software,” as defined by Federal Acquisition Regulation (“FAR”) 2.101. Pursuant to FAR 12.212 and 27.405-3 and Department of Defense FAR Supplement (“DFARS”) 227.7202, the U.S. government acquires commercial computer software under the same terms by which the software is customarily provided to the public. Accordingly, Keysight provides the Software to U.S. government customers under its standard commercial license, which is embodied in its End User License Agreement (EULA), a copy of which can be found at http://www.keysight.com/find/sweula The license set forth in the EULA represents the exclusive authority by which the U.S. government may use, modify, distribute, or disclose the Software. The EULA and the license set forth therein, does not require or permit, among other things, that Keysight: (1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the public; or (2) Relinquish to, or otherwise provide, the government rights in excess of these rights customarily provided to the public to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation. No additional government requirements beyond those set forth in the EULA shall apply, except to the extent that those terms, rights, or licenses are explicitly required from all providers of commercial computer software pursuant to the FAR and the DFARS and are set forth specifically in writing elsewhere in the EULA. Keysight shall be under no obligation to update, revise or otherwise modify the Software. With respect to any technical data as defined by FAR 2.101, pursuant to FAR 12.211 and 27.404.2 and DFARS 227.7102, the U.S. government acquires no greater than Limited Rights as defined in FAR 27.401 or DFAR 227.7103-5 (c), as applicable in any technical data.

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.

Safety Information

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/pna

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/PreventingInstrumentDamage

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

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
PNA-X Pro	NA5202A, NA5204A, NA5205A

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

NOTE

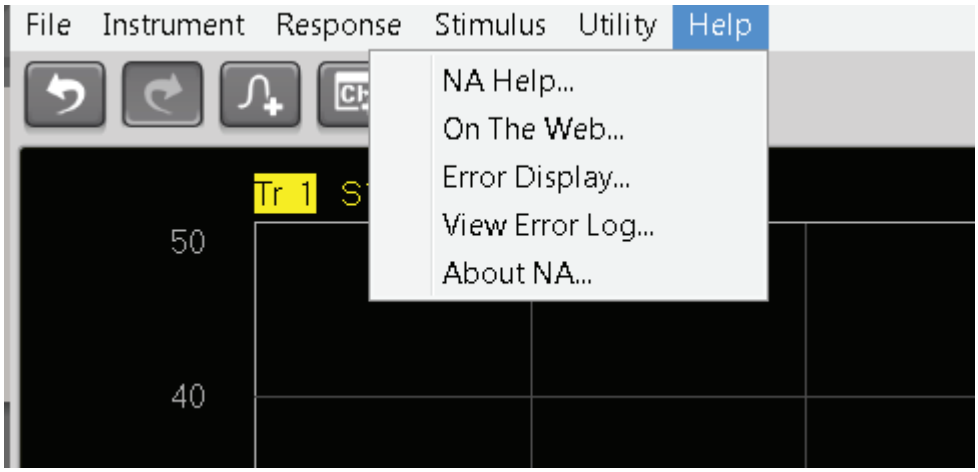
Be sure that all information stored by the user in the instrument that needs to be saved is properly backed up before attempting to clear any of the instrument memory. Keysight Technologies cannot be held responsible for any lost files or data resulting from the clearing of memory.

Be sure to read this document entirely before proceeding with any file deletion or memory clearing.

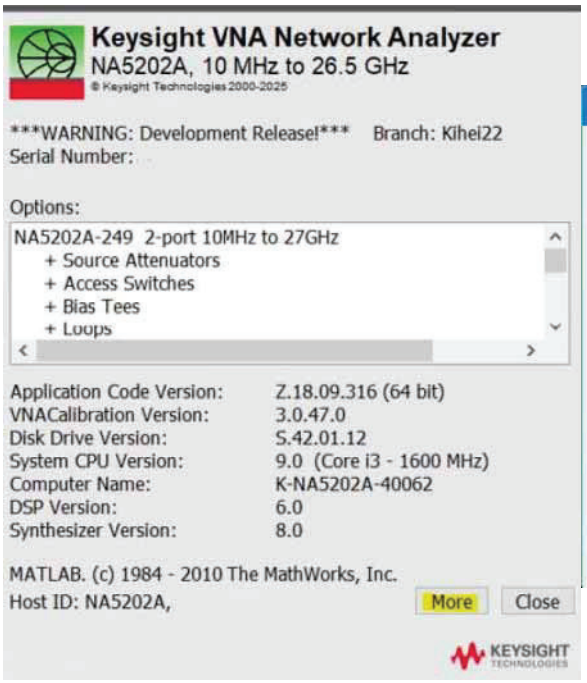
Determining Installed Options and Processor Assembly Type

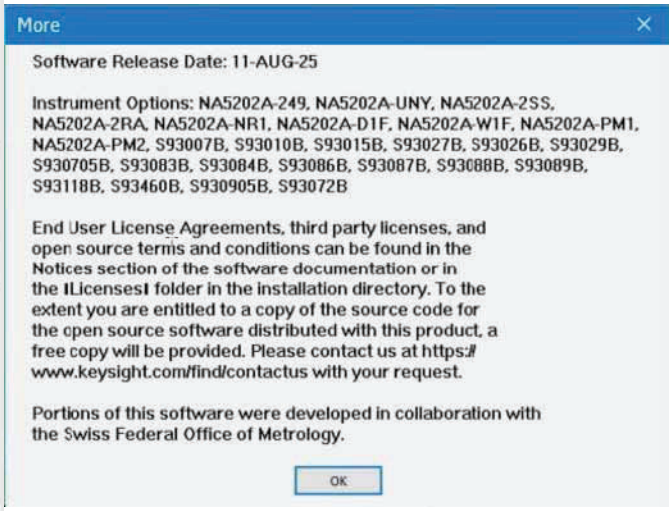
To determine your instrument's installed options and processor assembly:

1. From the main menu, select **Help** > **About NA...**.



2. Select **More** to determine the Instrument Options.





For more details, see the NA Help.

3 Security Terms and Definitions

Term	Definition
Clearing	As defined in Section 5 of NIST SP 800-88, Revision 1, Guidelines for Media Sanitization, Clearing is a sanitization method by which classified information in user-addressable storage space on the media is overwritten with non-sensitive data, using the standard read and write commands for the device. 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 (*aka* controlled area), such as is the case when the instrument is returned for calibration. Declassification procedures include memory sanitization or memory removal, or both.
Sanitization	Sanitization methods are defined and discussed in NIST SP 800-88, Revision 1, Guidelines for Media Sanitization. In that document, **Purging** is defined as a method by which classified information is completely removed from memory, or the memory is destroyed, so that even a laboratory attack using known techniques or analysis will not recover any information. In this document, the term **Sanitization** is reserved for the Purge Sanitization method described in the NIST document. 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 "Media Sanitization Matrix" in Appendix T of the Defense Security Service (DSS) Assessment and Authorization Process Manual (DAAPM).
Secure Erase	Secure Erase is a term that is used to refer to either the clearing or sanitization features of Keysight instruments.

4 Non-Volatile and Volatile Memory

This section contains information on the memory components available in your instrument.

This chapter contains the following sections:

Summary of Non-Volatile Instrument Memory

The table provides details of the size of each memory component, its type, how it is used, its location, volatility, and the sanitization procedure.

See also, "Summary of Volatile Memory" on page 17.

Table 4-1 Summary of Non-Volatile 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. Hard Drive 512 GB	Yes	Yes	The hard drive (actually an SSD) contains the operating system and all stored user data as well as a recovery partition to restore the PNA to its as-shipped condition.	Via typical Windows and user read/write operations.	A16 CPU board Hard drive sizes may change without notice depending upon availability.	None

Table 4-1 Summary of Non-Volatile 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
2. Flash Memory 64-128 MB	No	Yes	This device, located on the Test Set Motherboard, is used to store calibration constants used to make the PNA-X Pro function properly. The only access is via test routines that store correction data into the Flash memory. No user data can be entered; only values that are determined by the adjustment program can be stored. There is no other access to this flash memory. Reading and writing from/to this device is in a proprietary format.	Via Service Routines only.	A2 Synthesizer 2 Contains no user data.	None
					A4 Reference Contains no user data.	None
					A8 Synthesizer 1 Contains no user data.	None
					A9 Signal Processing ADC Modules board (SPAM) Contains no user data.	None
					A12 Synthesizer 0 Contains no user data.	None
					A13 System Mother board Contains no user data.	None
					A14 Mid Plane Contains no user data.	None
					A18 GPIB Contains no user data.	None
					A19 System Mother board Contains no user data.	None

Table 4-1 Summary of Non-Volatile 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
3. EEPROM 8K-bit to 64K-bit	No	Yes	These devices contain board information (name, revision, p/n, date, etc) and correction factors used to make the PNA functional. No user data is located in these EEPROMs. Each assembly below has one EEPROM. Some assemblies only exist on certain models or with certain options. These EEPROMs can only be accessed via service routines which are designed to store the appropriate data. Depending upon the device and location, changing the data may make the PNA non-functional.	Via Service Routines only.	See Table 4-2 on page 13. Contains no user data.	None
4. CPLD/FPGA The size varies	No	Yes	These devices are complex programmable logic devices that are pre-programmed before being loaded on the board. They are used to provide instructions to the various FPGA devices. In addition, several are used for simple address decoding throughout the PNA on various assemblies.	Via factory programming only	See Table 4-3 on page 14.	None

Table 4-1 Summary of Non-Volatile 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
5. BIOS and Real Time Clock (CMOS NVRAM) 256 Byte (battery backup)	No	Yes	The BIOS is a typical PC BIOS used to boot the PNA. It is pre-programmed at the factory. It contains initial boot-up instructions for the CPU. While this is normally user accessible, the type of data stored is extremely limited (such as boot-up device order and date/time settings.) A BIOS password can also be stored to limit both the BIOS setup and PNA boot-up to authorized personnel only. A lithium button battery provides backup power if the unit is unplugged.	Via Service Routines only.	A16 CPU board	None (Contains no user data)

Table 4-2 EEPROM Board Assembly Details

Board Assembly	Notes
A3 Source 2	All 4 port models
A5 Source 1	All Models
A6 Doubler	NA5204A, NA5205A only
A14 Mid Plane PCA	All Models
A19 TestSet Motherboard	All Models
A21 LO Mux PCA	All Models
A71 Port 1 Receiver	All 2 port Models
A72 Port 2 Reciever	All 2 port Models
A73 Port 3 Reciever	All 4 port Models
A74 Port 4 Reciever	All 4 port Models
A76 LO Distribution PCA	All Models

Table 4-3 FPGA and CPLD Board Assembly Details

Board Assembly	FPGA Size	CPLD	Notes
A2 Synth 2 (4 port models)	472 KB	n/a	Contains no user data
A3 Source 2 (4 port models)	84 KB	n/a	Contains no user data
A4 Frequency Ref (All models)	220 KB	n/a	Contains no user data
A5 Source 1 (All models)	84 KB	n/a	Contains no user data
A6 Frequency Doubler assembly (NA5204A and NA205A models only)	887 KB	n/a	Contains no user data
A8 Synthesizer 1 (All models)	220 KB	n/a	Contains no user data
A9 Signal Processing ADC Modules board (SPAM) (All models)	256 KB	n/a	Contains no user data
A12 Synthesizer 0 (All models)	432 KB	n/a	Contains no user data
A13 System Motherboard (All models)	486 KB	n/a	Contains no user data
A18 GPIB (All models)	220 KB	n/a	Contains no user data
A19 Test Set Motherboard (All models)	945 KB	n/a	Contains no user data
A20 IF Conditioning board (All models)	47 KB	n/a	Contains no user data
A71 Port 1 Receiver (All models)	84 KB	n/a	Contains no user data
A72 Port 2 Receiver (All models)	84 KB	n/a	Contains no user data
A73 Port 3 Receiver (4 port models)	84 KB	n/a	Contains no user data
A74 Port 4 Receiver (4 port models)	84 KB	n/a	Contains no user data

Disk Drive Partitioning

Details of the functions of all partitions are provided in Table 4-4 and Table 4-5 below.

For the NA5xxxA models, the instrument's disk drive is divided at the factory into three visible partitions, labeled C:, D:, and E:, plus a fourth hidden partition.

Table 4-4 Disk Drive Partitions for the NA5xxxA models

Partition Label	Purpose
C:	Primary partition for applications and secondary data.
D:	Default location for user data.
E:	Calibration data.
Hidden	Factory recovery image of the C: partition.

CPU Types and Mass Storage

See also, "Summary of Volatile Memory" on page 17 and to Table 4-7 on page 18.

Table 4-5 CPU Types

CPU Type	Part Number	Drive Part Number	Models	Remarks
Intel Core i3-9100HL (Version 10) **RAM**: 16 GB DDR4 SO-DIMM	W1312-60562	NA5000-60502	NA520xA	Tray mounted, removable SSD.

Summary of 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 “Media Sanitization Matrix” in Appendix T of the "Defense Security Service (DSS) Assessment and Authorization Process Manual (DAAPM)".

See also, “Summary of Non-Volatile Instrument Memory” on page 10.

For more on volatile memory as it relates to a specific CPU, refer to Table 4-5 on page 16 and to Table 4-7 on page 18.

Table 4-6 Summary of Volatile 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. SDRAM DDR4 16G-bit	Yes	No	Contains measurement data from data acquisition system.	Programmed by firmware. Not accessible by user.	A9 Signal Processing ADC Modules board (SPAM).	Turn off instrument power[a]

a. This memory is not battery backed-up or connected to standby power.

Table 4-7 Summary of CPU Volatile 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
16 GB DDR4 SO-DIMM	Yes	No	Main dynamic RAM memory for processor. Contains working copies of the operating system, instrument measurement applications, calibration, 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.	A16 CPU assembly contains user data.	Turn off instrument power[a]

a. This memory is not battery backed-up or connected to standby power.

LAN/USB/GPIB Devices

All 3 devices (USB, GPIB, and LAN) can be disabled by using Windows **Device Manager**.

How to Disable USB, GPIB, and LAN

- To disable GPIB: disable the device "GPIB Interfaces->Keysight Technologies 82350B PCI GPIB"
- To disable host side USB: (this will disable access to keyboards, mice, etc.) can also be done through the Device Manager.
- To disable LAN, disable the device: Intel (R) Ethernet Connection (7) I219-LM

5 Memory 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, 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	512 Gigabytes
Memory clearing	Software utilities are available that comply with the clearing requirements specified for Magnetic Disks and Flash Drives in the "Media Sanitization Matrix" in Appendix T of the Defense Security Service (DSS) Assessment and Authorization Process Manual (DAAPM).
Memory sanitization	We recommend removing the Disk Drive to achieve sanitization.
Memory removal	See the Chapter "Disk Drive Removal Procedure" on page 26.
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). 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	8K-bit to 64k-bit
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.
Write protecting	Not applicable.
Memory validation	Not applicable.
Remarks	These memories are only writable by factory/service center software, or upgrade installation software. These memories are internally connected to proprietary internal control data buses (as opposed to standard computer buses 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.
Memory clearing	Software utilities are available that comply with the clearing requirements specified for Magnetic Disks and Flash Drives in the “Media Sanitization Matrix” in Appendix T of the Defense Security Service (DSS) Assessment and Authorization Process Manual (DAAPM).

Instrument Sanitization Procedure

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 all licensing information is stored in secure storage on one of the mostly-inaccessible assemblies.

When a PNA is shipped from the factory, it contains unique information on the hard drive as listed below. Logins, passwords, cal sets, saved files, and installed programs that have been added after delivery are not stored here. These files are located in E:\CalFiles and automatically generated if missing.

- **eebudat.dak** - Backup file of EEPROM information; it is only used for service.
- **TSMBBackup** - A backup directory of flash data.
- **TSMBOrig** - Another backup directory of Flash data.
- **SYN0/SYN1/SYN2** - Backup directories of synthesizer flash data.

Replacement of Disk Drive

Refer to the procedure below for details of how to perform this procedure.

NOTE

Ensure that the instrument software revision on the secondary non-classified disk drive matches that of the classified drive in the controlled area.

If the non–classified drive receives a software upgrade, or if the non-classified drive is replaced with a drive that contains a newer revision of software than that of the classified drive, the classified drive will require a software upgrade (inside the controlled area) to match the non-classified drive.

Items Required

To perform these tasks in a controlled area, you will need:

- 1x Instrument
- 2x Disk Drives for the instrument

  One drive (Disk Drive #1) stays permanently within the controlled area, and the other (Disk Drive #2) stays permanently outside it
- 1x One-time writable media, plus 1x compatible writing device for the non-controlled area **and** 1x reading device for the controlled area.

Procedure

Steps below that appear on a yellow background take place in the controlled area. All other steps take place in a non-controlled area.

Step	Task
1	Receive new instrument from factory.
2	Power up the instrument and verify the Instrument Software Revision. For instructions on how to verify the currently installed Instrument Software Revision, see "Is your product software up-to-date?" on page 3. Write down the software revision.
3	If the instrument's software is not the latest version, update the instrument software to the latest version available. For instructions, see "Is your product software up-to-date?" on page 3 Write down the software revision.
4	Replace the original instrument disk drive (Disk Drive #1) with the spare disk drive (Disk Drive #2) that was obtained previously. For details of how to remove the Disk Drive, see "Disk Drive Removal Procedure" on page 26.
5	Turn on the instrument with the spare Disk Drive #2 installed.
6	Verify that the instrument software on the spare Disk Drive #2 has the same revision as that on the original Disk Drive #1.
7	If the Instrument Software Revision on the spare Disk Drive #2 is not the same as that on the original Disk Drive #1, update the instrument software on this drive to match the software revision that you documented in step 3. For instructions, see "Is your product software up-to-date?" on page 3
8	Write the instrument model number, serial number, and software revision on the original Disk Drive #1, then reinstall it in the instrument.
9	Write the instrument model number, serial number, and software revision on the spare Disk Drive #2, place it back in the static safe bag that it was shipped in, then store it in a safe place until it is needed again.
10	The instrument is now ready for use in a secure environment.
11	Physically deploy instrument into controlled area.
12	Use instrument inside controlled area until cal or repair is needed.
13	Make a note of the current software version, because the instrument's software may have been updated inside the secure area. To determine this, go to the main menu and select **Help** > **About PNA...**. Write down the application code and disk drive revision and attach this note the instrument.

Step	Task
14	Remove Disk Drive #1 and retain in controlled area. For details of how to remove the Disk Drive, see "Disk Drive Removal Procedure" on page 26.
15	Physically remove instrument from controlled area. Without the Disk Drive, instrument is sanitized.
16	Install secondary non-classified Disk Drive #2, which was previously prepared in Step 9. Power on instrument.
17	When the instrument has booted up, press **Help** > **About NA...**, and confirm that the Instrument Software Revision is the same as noted in Step 13. If not, upgrade the instrument software to the same version as recorded in Step 13.
18	Instrument is now operational with original calibration data. Deliver to service center for cal/repair.
19	Service center may or may not generate new calibration files on Disk Drive, depending on whether an adjustment is performed. This procedure assumes that new cal data was generated.
20	Instrument returned to customer's non-controlled area.
21	Verify Instrument Software Revision, to determine whether the service center upgraded the software. See Step 2 and Step 9.
22	Remove the non-classified Disk Drive #2 and retain outside of controlled area. If necessary, update the documented software revision on the drive label. For details of how to remove the Disk Drive, see "Disk Drive Removal Procedure" on page 26.
23	Physically deploy instrument back into controlled area, without a Disk Drive.
24	Re-insert classified Disk Drive #1 into instrument, and verify Instrument Software Revision, as in Step 2.
25	If the Instrument Software Revision does **not** match the revision documented in step 21 (because the software was updated at service center), then a software update must be performed, to force the controlled-area drive to match the non-controlled-area drive that was used to calibrate the instrument.
26	Done. Go to Step 12.

6 Disk Drive Removal Procedure

This chapter describes the procedures for physical removal of the instrument's disk drive.

NOTE

Application License keys are stored in Flash on the GPIB Assembly. 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.

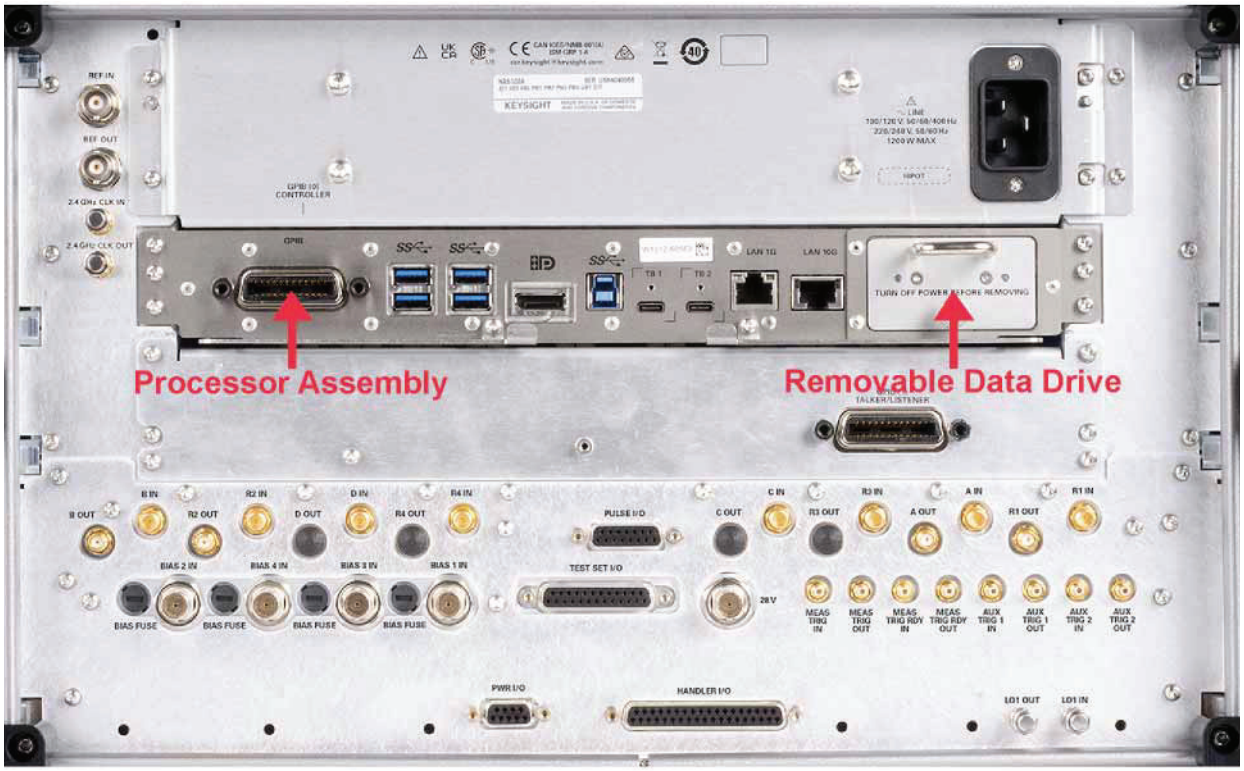
To remove the disk drive, follow the steps below. The numbered items in the figures correspond to the step numbers in the procedure.

CAUTION

Before removing the disk drive, ensure that the instrument's power is turned off.

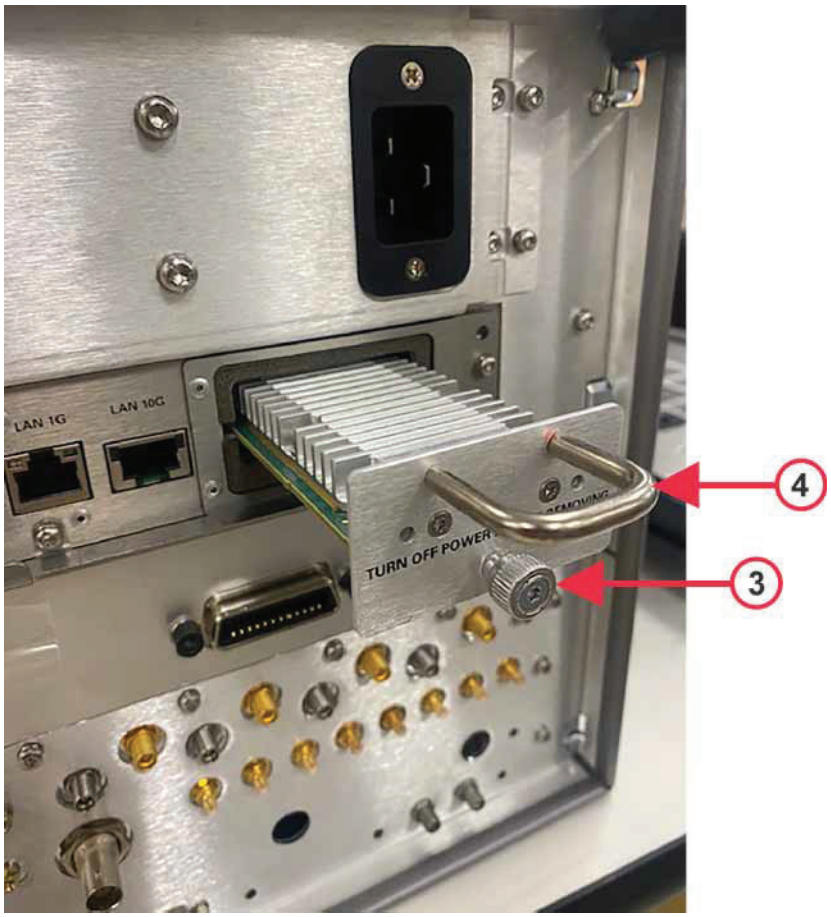
1. Locate the Processor and Disk Drive Assembly on the instrument's rear panel, as shown in Figure 6-1.
2. Locate the removable drive, and its retaining thumbscrew, as shown in Figure 6-1.

Figure 6-1 Instrument Rear Panel & Processor Assembly



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 fully 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 user and 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.
- Recommended Thunderbolt BIOS-Level Security Settings

NOTE **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 30 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.**

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 30
- "Configuring USB for Read-only" on page 30

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.)

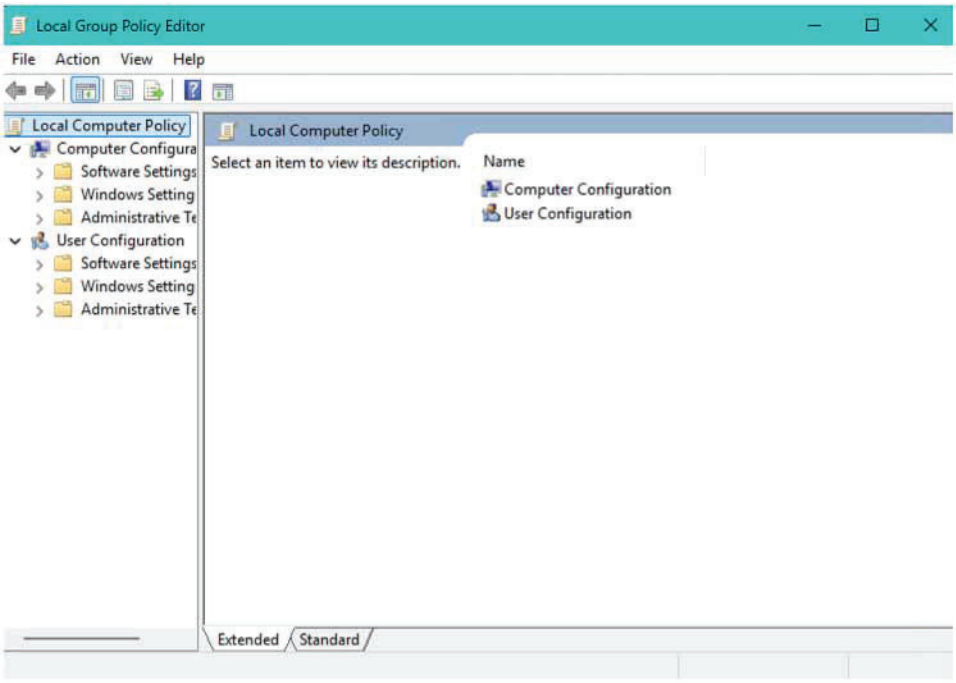
You can disable or enable AutoPlay via the Control Panel. Open the Control Panel and select **Hardware and Sound > AutoPlay**, then clear or check the `Use AutoPlay for all media and devices` check box.

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. To change the setting, do the following:

Group Policy Method



On the PNA-X Pro desktop, navigate to:

1. Computer Configuration > Administrative Templates > System > Removable Storage Access
2. Enable the policy: "Removable Disks: Deny write access".

Recommended Thunderbolt BIOS-Level Security Settings

1. Enable IOMMU / VT-d (Intel) or AMD-Vi (AMD)

   This is essential for DMA remapping, which restricts Thunderbolt devices to designated memory regions. It forms the basis for Kernel DMA Protection.

2. Set Thunderbolt Security Level to “User Authorization” or “Secure Connect”:

   a. User Authorization (SL1): Prompts users to approve new Thunderbolt devices.

   b. Secure Connect (SL2): Adds cryptographic verification for trusted devices, preventing spoofing.

3. Disable “No Security” Mode (SL0)

   This mode allows any Thunderbolt device to connect without restriction and is highly vulnerable to DMA attacks.

4. Enable Kernel DMA Protection

   This feature uses IOMMU to block unauthorized DMA access until a user signs in. It’s supported on Windows 10/11 Pro and Enterprise editions.

5. Disable Thunderbolt Boot Support (if not needed)

   This prevents DMA access during pre-boot, which is otherwise unprotected by the OS.

6. Physically Disable Thunderbolt Ports (if unused)

   If Thunderbolt is not required, disabling it entirely in BIOS is the most secure option.

Additional Tips

- Ensure BIOS is password-protected to prevent unauthorized changes.
- Keep firmware and Thunderbolt drivers up to date.
- Use only trusted Thunderbolt peripherals.

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 26.

A: References

1. **Defense Security Service (DSS) Assessment and Authorization Process Manual (DAAPM)**

   Defense Security Service. Version 2.0, May 6, 2019

   May be downloaded in PDF format from:

   https://www.dcsa.mil/Portals/91/Documents/CTP/tools/DCSA%20Assessment%20and%20Authorization%20Process%20Manual%20Version%202.2.pdf

2. **NIST SP 800-88, Revision 1, Guidelines for Media Sanitization**

   National Institute of Standards and Technology. December 17, 2014

   May be downloaded in PDF format from:

   http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

Edition 1, September 2025

E8356-90070

www.keysight.com