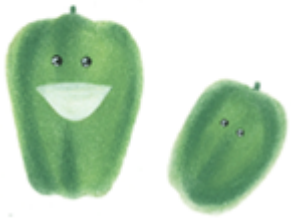
Manual menu

Disk Drive Erasing Tool

GreenPepper PRO

User's Manual



Abstract

About Erase Method

Operation of "Boot up Erase program"

Operation of "Windows Erase program"

Using "Startup environment creation tool"

Operation of "Utilities for administrator"

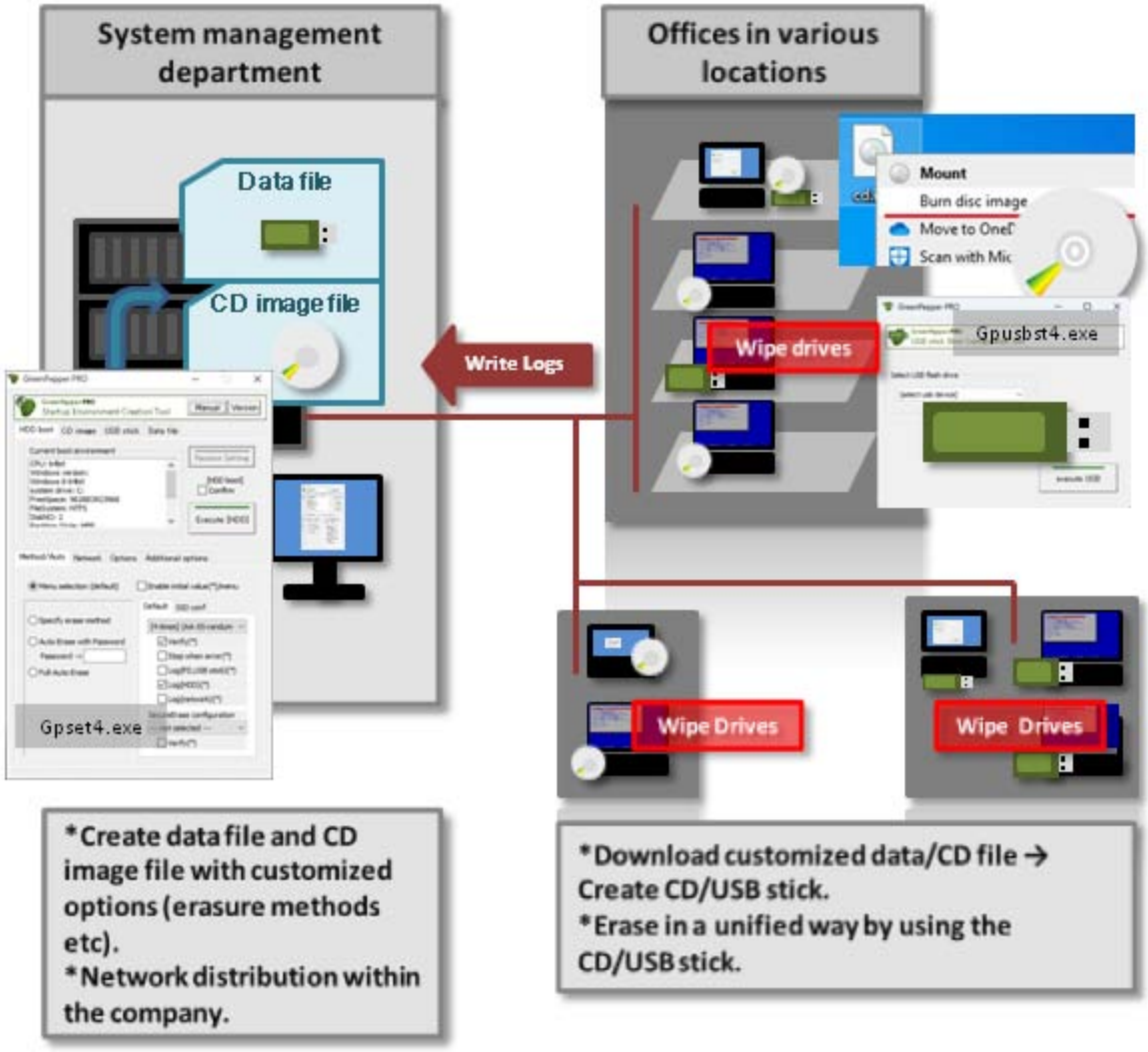
Operation of "USB stick Boot configuration tool"

Operation of Network boot Host

Other information

What is "GreenPepper PRO"?

Developed as a standard **disk drive wipe/erasing tool** for implementing security policies in the enterprise. It is a simple, compact, and erasing tool with the necessary functions.
It is intended for corporate use, where the erasing environment set by the system department is distributed to users. We have prepared various customization and distribution methods so that you can erase in a unified way within the company.



Establishment of a unified erasing method within the company,

When distributing the erasure program within the company, you can specify and fix the erasure method. The operator can perform the erasing work in the specified method with a simple operation. It is possible to realize erasing work with a unified policy within the company.
* A corresponding license is required for distribution.

Support for many types of disk drives

It supports a wide range. PATA (PararelATA), SATA (SerialATA), NVMe disks, standard for desktops and notebook PCs. eMMCs used in tablets. SCSI, SAS, FC (Fibre Channel) used in server systems, and even RAID configuration disks.
It also supports Secure Erase and Sanitize of ATA/SATA, SSD, NVMe, eMMC.

High-speed, multitasking parallel processing

Due to the Linux-based system, disk access is very fast. In addition, the multitasking function erases multiple connected disks in parallel. It reduces the time of the very time-consuming erasing process.

Supports various erasing methods, and Secure Erase / Sanitize

In addition to 1-4 erase method, it supports Secure Erase / Sanitize, which is almost indispensable for SSDs. It can be erased by a method that complies with the US Army compliant method (AR380-19), the US Department of Defense standard (DoD5220.22-M), the National Institute of Standards and Technology (NIST SP 800-88), etc. Moreover, in case of a read / write error, it retries finely for each sector and incorporates a control for more reliable erasing.

Supports various boot methods

Supports CD boot, USB flash drive boot, hard disk boot, and Network Boot is available.
You can choose the best startup method.
In addition to the legacy BIOS boot, it supports UEFI (Secure Boot on many PC) boots.

Log output that can be checked for tampering

Logs that are important as erasure records can be saved to the network (Windows share, FTP), HDD, USB flash drive, FD, etc. In addition, although the log is in an easy-to-use text format, it can be checked for tampering with a checksum.

Support for writing logs to the network

An increasing number of companies are restricting the use of writable media such as USB flash drive due to security policies. With "Green Pepper PRO", by booting from a CD and writing logs to a network drive, it is possible to write important management logs to a network drive even in a read-only media environment. You can also centrally manage logs on the network server. In addition to onboard Ethernet, it also supports USB-LAN and wireless LAN.

Erasing multiple PCs at the same time using the Network boot host feature

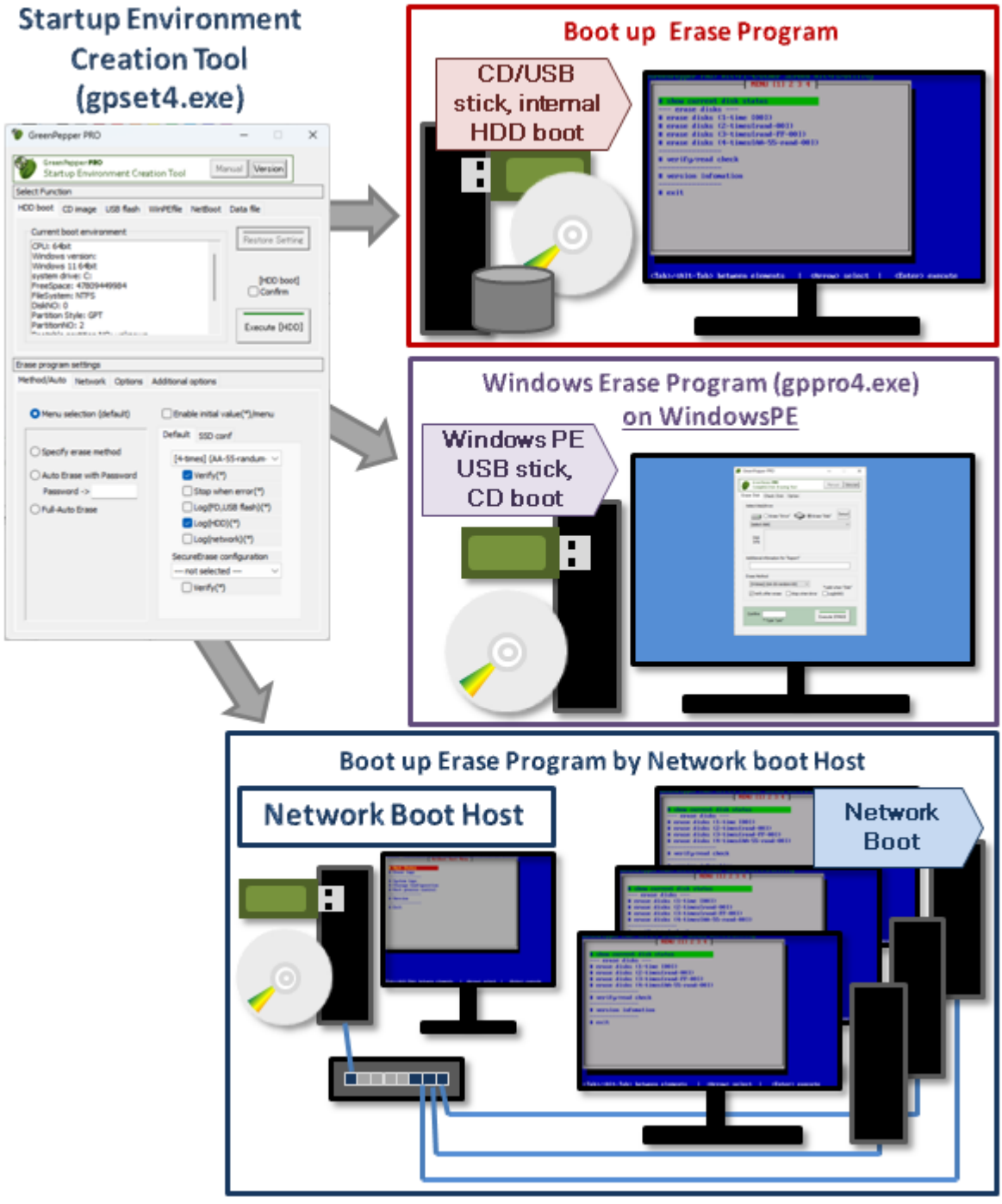
*Available with company/site license.

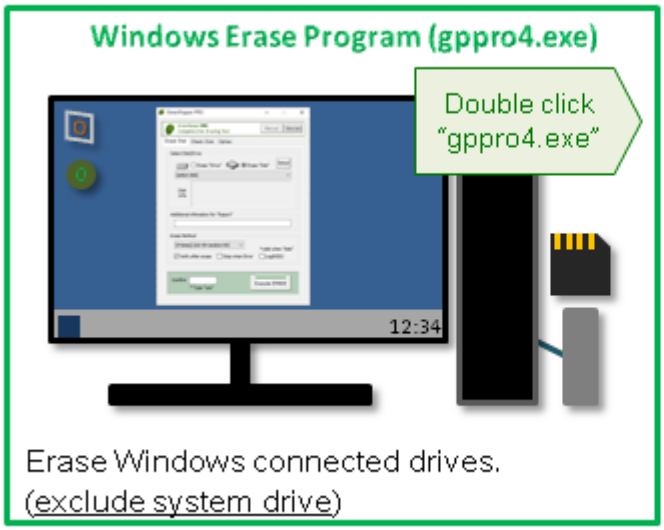
The network boot host creation function allows you to easily install a host (server) that can start the erase program via network boot.
By connecting the PC to be erased to the network that includes the network boot host, it is very easy to erase many PCs at the same time.
Additionally, by leaving the erase log on the network boot host, you can manage the logs at one place.

Composition of "GreenPepper PRO"

The erasing program of "Green Pepper PRO" consists of "Boot up Erase Program" that includes boot system (linux), and "Windows Erase Program" (gppro4.exe) that execute on Windows.
Windows erasure program (gppro4.exe) can be run on regular Windows (10, 11, etc.) or on WindowsPE. Erasing the Windows system drive (generally C:) and Secure Erase is only possible when run on WindowsPE.

In addition, as tools that run on Windows, there are "Startup Environment Creation Tool"(gpset4.exe) that creates the startup environment (bootable CD image, bootable USB flash drive) of "Boot up Erase Program", and "Utility for Administrators"(gputil4.exe) that collects various tools that assist the operation of "Green Pepper PRO".





Erase with "Boot up Erase Program"

Set and configure the boot environment for HDD, CD, and USB flash drive with Widows "Startup Environment Creation Tool"(gpset4.exe). And then boot the PC with created CD, USB flash drive, configured HDD.

* Enables erasing all drives including the Windows system drive.
* Secure Erase and Sanitize processing possible.
* Built-in disk driver.
* Able to cancel ATA Secure Erase freezen state (supported PC only).

*For the first time use for evaluation purposes, create a CD-R using "cd_eval.iso"(iso9660 cd image file) and boot your PC.
To burn CD-R from CD image file, see "How to create a CD from an image file (iso9660)".

Erase with "Windows Erase Program" on WindowsPE

If you save gppro4.exe in the WindowsPE environment, you can erase it using menu operations.
By creating a "WindowsPE configuration file" using the Windows "Startup Environment Creation Tool"(gpset4.exe) and saving it in the same folder as gppro4.exe, you can specify automatic execution, processing methods, etc.

* Enables erasing all drives including the Windows system drive.
* Secure Erase and Sanitize processing possible.
* Customers must build the WindowsPE execution environment themselves.
  If there is a missing driver, it must be incorporated.
* Fully compatible with secure boot.

MEMO
Although there are some functional differences between the "Boot up Erase Program" and the "Windows Erase Program"(on WIndowsPE) , they have equivalent erase function. However, building a WindowsPE environment is technically a little difficult, and there are some areas where the "Boot up erase program" is superior in terms of functionality, so except in the following cases, the "Boot up erase program" is basically recommended. ·For disk interface that only support Windows (WindowsPE) drivers. ·When it is necessary to fully support secure boot.

Erase with "Windows Erase Program"

Run "Windows Erase Program"(gppro4.exe) on Windows and execute Erase.

* Windows system drive (usually C:) cannot be erased.
* Can not execute Secure Erase/Sanitize.
* Use "Windows Erase Program" to erase connected external drives, memory cards, USB disks, etc.

Files included in the downloaded file

You can use the following programs, manuals, etc. by viewing with Explorer etc. in a Windows environment.

README.txt · · · Please read first. It can be displayed in Notepad.
release.txt · · · Product release note.
cd_eval.iso · · · Bootable CD image file for "Boot up erase program". For evaluation use only.

gppro4.exe · · · "Windows Erase Program"
gpset4.exe · · · "Startup Environment Creation Tool"
gputil4.exe · · · "Utility for Administrators"
* No installation process is required. You can click it directly to execute it.

gpdata.pac · · · Data file required by "Startup Environment Creation Tool" (network support,WiFi support)
gpdata.pac.net · · · Data file required by "Startup Environment Creation Tool" (network support,WiFi no-support)
gpdata.pac.nonet · · · Data file required by "Startup Environment Creation Tool" (network no-support,WiFi no-support)

gpdatahost.pac · · · Data file for Network boot host. Required by "Startup Environment Creation Tool" when you create Network boot Host.

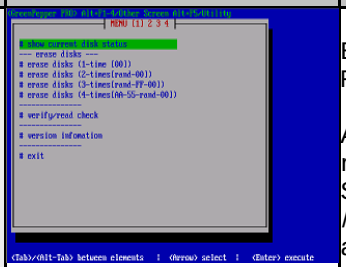
[64bit] folder
gppro4.exe · · · "Windows Erase Program" (64bit version)
gpset4.exe · · · "Startup Environment Creation Tool" (64bit version)
gputil4.exe · · · "Utility for Administrators" (64bit version)

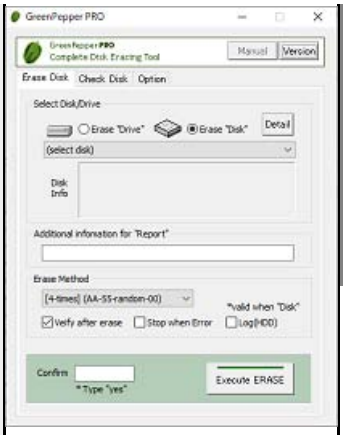
[manual] folder
FirstStep.pdf · · · First step guide (PDF)
man_gppro.pdf · · · Manual (PDF version)
index.html · · · Manual (HTML version Menu)
* Other files/folders are html manual files

[other] folder
gpusbst4.exe · · ·"USB stick Boot configuration tool"(user privileges)
Other Documents, Tools

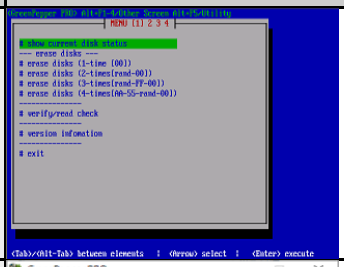
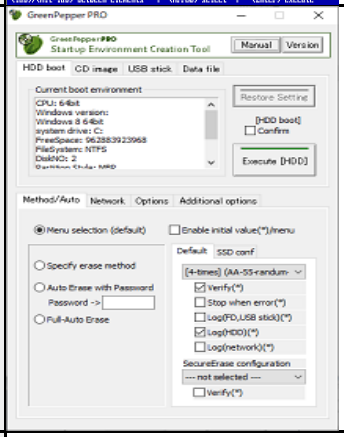
Details of each program

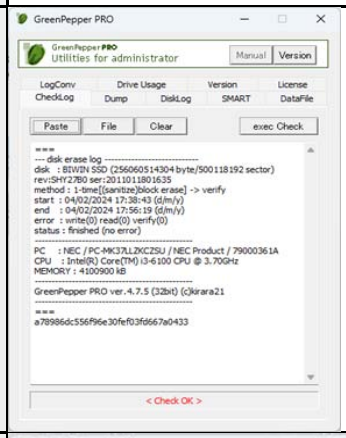
Erase Program

Description in this manual		Abstract	Target Drive of Erase	Execution environment	Where the execution log is saved
Boot up Erase Program		Boot from HDD/CD-ROM/USB flash drive Automatically recognizes SATA/NVMe/eMMC/SCSI /SAS/RAID cards, etc. and erases them. Secure erase/Sanitize erase can be executed. Can be run automatically	IDE/SATA/eMMC /NVMe/USB/SCSI /SAS/RAID Disk Drive. Includes Windows system drive.	Erase program that includes boot up system (Linux OS) * The OS installed on the hard disk is irrelevant.	1. FD/USB-FD 2. USB flash drive 3. erased HDD 4. Network share (Windows/FTP)
Windows Erase Program (gppro4.exe)		[run on WindowsPE] Erase program executed on Windows PE OS. Secure erase/Sanitize erase can be executed. Can be run automatically	Drives that WindowsPE can recognize, including the system drive. Requires installation of the required disk interface driver.	WindowsPE	1. FD/USB-FD 2. USB flash drive 3. erased HDD 4. Network share (Windows)
		[run on Windows] Erase program executed on Windows OS.	Erase drives and partitions recognized by windows.	Windows	1. Clipboard (Copy/Paste) 2. File 3. erased

					
			Windows system drives cannot be erased. SATA, USB Drive, SCSI, Memory card, iSCSI, etc.		HDD

Tool programs, data files

Description in this manual		Abstract	Execution environment
Boot up Erase Program/ Utility		Utility menu, displayed by pressing ALT + F5 while executing "Boot up Erase Program",	Erase program/Utility that includes boot up system (Linux OS)
Startup Environment Creation Tool (gpset4.exe)		Embedding the "Boot up Erase Program" into the hard disk, or set to USB flash drive, or create bootable CD-ROM image. Creating a configuration file when running (gppro4.exe) on WindowsPE.	Windows
Data for "Startup Environment Creation Tool" (gpdata.pac)		Data file required for "Startup Environment Creation Tool" "gpdata.pac" contains everything, including network and WiFi settings. Please use this basically. However, due to its large size, you can reduce the download time by using the following files instead. * When you use the network but do not need WiFi settings "gpdata.pac.net" * When not using the network "gpdata.pac.nonet" Please change the name to "gpdata.pac" and use it.	
Data file for Network boot		Data file required for "Startup Environment Creation Tool"	

host (gpdatahost.pac)		Required by "Startup Environment Creation Tool" when you create Network boot Host.	
Utilities for Administrator (gputil4.exe)		Various utilities to support the operation of "GreenPepper PRO"	Windows
USB stick Boot configuration tool (gpusbst4.exe)		Utility to configure bootable USB flash drive for "Boot up erase program". This program can be executed **with user privileges** and is useful for distributing USB flash drive boot environments within your company.	Windows

Functions of "GreenPepper PRO"

This product has the following functions.

Boot up Erase Program

	PC Boot up	HDD, CD, USB flash drive. Network Boot(PXE). * Only on supported PCs.
	Disk Erase	Erase PATA/SATA/eMMC/NVMe/SCSI/SAS/FC disks connected to PC. (includes RAID) *The following write values can be changed. **1-Time erase** · First Time: 00 (hex) * NIST SP 800-88 compliant **2-Times erase** · Frist time :Random values · Second time: 00 (hex) **3-Times erase** · Frist time :Random values · Second time: FF (hex) · Third time: 00 (hex) * US Army Information Systems Security (AR380-19) compliant 4**-Times erase** · Frist time : AA (hex) · Second time: 55 (hex) · Third time: Random values · 4th time: 00 (hex) * US Secretary of Defense DoD5220.22-M compliant **Secure Erase** Secure erasure can be executed for on board ATA (including PATA / SATA disk and SSD), NVMe, and eMMC drive. However, it is necessary that the disk itself supports it and that the Freeze command by the BIOS can be avoided. Suspend/resume feature is provided to unfreeze Secure Erase frozen state. **Sanitize** Sanitize erasure can be executed for on board ATA (including SATA disk and SSD), NVMe, and eMMC drive. However, it is necessary that the disk itself supports it.
	Disk erase verification Read check	Check the disk erasure by checking if the inside of the disk is all zero (hex number 00). In addition, by reading the entire area of the disk, it also has a read check function. * This erasure verification step is required to fully comply with NIST SP 800-88/ US Department of Defense standards (DoD5220.22-M).
	Save Log	You can save a processing log on the network share (Windows share, FTP), FD drive (internal, USB), USB flash drive, or erased HDD. A checksum string is added to the log file to ensure that the contents of the file have not changed.
		Multitasking allows simultaneous erasure of multiple

	Multi-Task	disks (up to 4).
	NTP client	NTP client to synchronize time with a NTP server.
	Utility	The following operations can be performed on the utility screen. · Save the hardware environment · Save screenshot · Processing interruption · Reload the disk environment · Disk dump · Display of HDD log · Log writing test · Set SecureErase Method/Unfreeze · Removal of HDD password · Removal of HPA (HostProtected Area) and cancellation of DCO (Device Configuration Overlay) · Network status · OPAL encryption key deletion (Revert) processing

Windows Erase Program / gppro4.exe (on Windows, WindowsPE)

	Disk Erase	Erases Windows-recognizable disks, such as USB flash drive, external USB hdd drives, iSCSI drives etc. * except Windows system drive *The following write values can be changed. **1-Time erase** · First Time: 00 (hex) **2-Times erase** · Frist time :Random values · Second time: 00 (hex) **3-Times erase** · Frist time :Random values · Second time: FF (hex) · Third time: 00 (hex) * US Army Information Systems Security (AR380-19) compliant 4**-Times erase** · Frist time : AA (hex) · Second time: 55 (hex) · Third time: Random values · 4th time: 00 (hex) * US Secretary of Defense DoD5220.22-M compliant
		WindowsPE only
		Secure Erase Secure erasure can be executed for on board ATA (including PATA / SATA disk and SSD), and NVMe drive. However, it is necessary that the disk itself supports it and that the Freeze command by the BIOS can be avoided. **Sanitize** Sanitize erasure can be executed for on board ATA (including SATA disk and SSD), and NVMe drive. However, it is necessary that the disk itself supports it.
	Disk erase verification Read check	Check the disk erasure by checking if the inside of the disk is all zero (hex number 00). In addition, by reading the entire area of the disk, it also has a read check function. * This erasure verification step is required to fully comply with US Department of Defense standards (DoD5220.22-M).
		At the end of the process, a completion report will be displayed and you can save it to a file. A checksum string is added to the report to ensure that the contents of the report have not changed. It is also possible to write the erase log to the erased disk.

	Completion Report Save Log	WindowsPE only You can save a processing log on the network share (Windows share), FD drive (internal, USB), USB flash drive, or erased HDD. A checksum string is added to the log file to ensure that the contents of the file have not changed.
	Command line instructions	It is possible to specify the initial value to be displayed and the display page by specifying the command line at the time of execution.

Startup Environment Creation Tool /gpset4.exe (on Windows)

	Embed into hard disk	If Windows is running on the PC to be erased, the "Boot up Erase Program" can be embed into the hard disk. When you restart, the "Boot up Erase Program" starts and you can erase the disk including the Windows system. Supports both Legacy(BIOS) / UEFI boot. It is possible to specify erasing method, automatic execution, etc.
	Create bootable CD-ROM image file	Create bootable CD-ROM image file that includes "Boot up Erase Program". Supports both Legacy(BIOS) / UEFI boot. It is possible to specify erasing method, automatic execution, etc.
	Configure bootable USB flash drive	Configure the "Boot up Erase Program" to a USB flash drive. Supports both Legacy(BIOS) / UEFI boot. It is possible to specify erasing method, automatic execution, etc.
	WindowsPE configuration file	Create a setting file to automatically run "Windows Erase Program (gppro4.exe)" on WindowsPE.
	Configure Data file	It is possible to set initial values or fixed values for the "Startup Environment Creation tool". Those configuration is saved in Data file.
	Command line instructions	It is possible to set initial values or fixed values for the "Startup Environment Creation tool". Those configuration can be set by command line.

Utilities for Administrator / gputil4.exe (on Windows)

	Check Log	Checks if the checksum string of the log file / completion report is correct. It is possible to check whether the log has been tampered.
	Dump disk	Display the contents of the connected disk.
	Disk Log	View and delete logs stored inside the connected disk.
	S.M.A.R.T	Show S.M.A.R.T(Self-Monitoring, Analysis and Reporting Technology) information of the connected disk.
	Data File	Check the version of Data for "Startup Environment Creation Tool". Clears the initial and fixed values set by the "Startup Environment Creation Tool".
	Log Conversion	Reads erasure log files, convert them into a text (CSV) file or "Disk Erasure Report" in XPS file format.
	Drive Usage	Displays a list of processes that are using programs/files on the specified drive.
	Version	Check the latest version of the "GreenPepper PRO".

USB stick Boot Configuration tool /gpusbst4.exe (on Windows)

	Configure bootable USB flash drive	Configure the "Boot up Erase Program" to a USB flash drive. **No administrator privileges required**, settings can be made with user privileges.

Network Boot Host (for Company/Site License)

		CD, USB flash drive.

	PC Boot up	* Only on supported PCs
	Network Boot (DHCP, TFTP server)	Boot network-connected PC's using network boot (PXE). Download the erasing program to the booted PC and run it.
	FTP server	FTP server for saving erase logs.
	NTP server	Synchronize the time with the PC running the erase program.
	Utilities	· Save Hardware Information to Erase Log Area · Save Screenshot to Erase Log Area · Rescan Disks/Reset Network · PING Test

Operationg environment of "GreenPepper PRO"

This product operates in the following environment.
* Even if the following conditions are met, it may not work. Please test before use.

Boot up Erase Program

	Personal Computer	Intel Architecture PC. (IBM PC/AT compatible, Windows PC) Server/Desktop/Laptop/Tablet.
	BIOS/UEFI	Legacy(BIOS)/UEFI bootable. * Supports "Secure Boot" (some models do not support it) * 32bit UEFI boot is supported only when 64bit CPU is installed
	CPU	Intel CPU and Other compatible CPU * exclude clover trail(Atom Z2760,Z2520,Z2560,Z2580)
	RAM reqiured	UEFI boot normal: 256MB network support: 256MB Wi-Fi supoort: 512MB BIOS boot normal: 64MB network support: 256MB Wi-Fi support: 384MB
	keyboard	PS/2, USB
	Mouse	not supported
	Display	Can show VGA(640x480) *When using secure erase "Unfreeze" (suspend/resume) feature, it is necessary to use a PC with compatible chip, "Supported display chip".
	CD-ROM Drive	Rirequired when booting from CD-ROM. IDE/USB/SATA Can boot from CD-ROM.
	Floppy disk drive	Rirequired when saving Log to FD) Internal/USB 1.44M(2HD) drive.
	USB flash drive	Rirequierd when booting from USB flash drive. 128MB or more. PC should be support USB flash drive boot. (required when saving Log to USB flash drive) The capacity required to save logs. 1KB or less per log. Should be formatted by FAT/FAT32/exFat.
	Hard disk/SSD drive (target of Erase)	PATA(IDE)/SATA/eMMC/NVMe/SCSI/SAS/FC/RAID Supported disk interface is listed in "Supported SCSI/RAID cards " 2 Tera byte or over is supported. 4096 sector size (512 byte emulation) is supported.
	Network (save Log)	(required whe saving Log to network share) Supported network interface card is listed in "Supported network interface card" 10M/100M/1G/10G ethernet.

Windows Erase Program, run on WindowsPE

	Personal Computer	PC (Intel, compatible CPU) running WindowsPE (32bit/64bit) equivalent to Windows7/8/8.1/10/11. Compatible keyboard, mouse, display.
	RAM	Enough for WindowsPE to work
	CD-ROM drive	Rirequired when booting from CD-ROM.
	USB flash drive	Rirequierd when booting from USB flash drive. 1GB or more. PC should be support USB flash drive boot. (required when saving Log to USB flash drive) The capacity required to save logs. 1KB or less per log.

		Should be formatted by FAT/FAT32/exFat.
	Hard disk/SSD drive (target of Erase)	Drives recognized by Windows. PATA/SATA/SCSI/SAS/RAID, USB ,IEEE1394,iSCSI, etc. HDD, MO, FD, Memory card, etc. There is a driver that supports Windows PE, and it can be embedded.
	Network (save Log)	(required whe saving Log to network share) A wired LAN network card that can be recognized on WindowsPE. WiFi is not possible due to WindowsPE specifications. There is a driver that supports Windows PE, and it can be embedded.

Windows Erase Program, Startup Environment Creation Tool, Utilities for Administrator

	Personal Computer	PC that runs on following Windows version. Windows7/8/8.1/10/11 2008R2server/2012server/ 2016server/2019server/2022server (32bit/64bit)
	RAM	Enough for Windows to work
	CD-ROM drive	Required when reading Product CD-ROM
	CD-R drive	Required when creating a bootable CD or when providing the product via online download. You need a CD writing software that can write ISO9660 images. Since it is supported as standard on Windows 7/8/10, no writing software is required.
	USB flash drive	Required when creating a bootable USB flash drive. (128MB or more)
	Hard disk/SSD drive (target of Erase)	Drives recognized by Windows. PATA/SATA/SCSI/SAS/RAID, USB ,IEEE1394,iSCSI, etc. HDD, MO, FD, Memory card, etc. 2 Tear byte or over is supported. 4096 sector size (512 byte emulation) is supported. * Hardware, Windows driver support for 2T over recognition, and support for 4096 sector are required.

Network Boot Host

	Personal Computer	Intel Architecture PC. (IBM PC/AT compatible, Windows PC) Server/Desktop/Laptop/Tablet.
	BIOS/UEFI	Legacy(BIOS)/UEFI bootable. * Supports "Secure Boot" (some models do not support it) * 32bit UEFI boot is supported only when 64bit CPU is installed
	CPU	Intel CPU and Other compatible CPU, 64bit only * exclude clover trail(Atom Z2760,Z2520,Z2560,Z2580)
	RAM reqiured	UEFI boot normal: 512MB BIOS boot normal: 512MB
	keyboard	PS/2, USB
	Mouse	not supported
	Display	Can show VGA(640x480)
	CD-ROM Drive	Rirequired when booting from CD-ROM. IDE/USB/SATA Can boot from CD-ROM.
	USB flash drive	Rirequierd when booting from USB flash drive. 300MB or more. PC should be support USB flash drive boot. (when using as FTP server storage) The capacity required to save logs. 1KB or less per log.
	Hard disk/SSD drive (using as FTP server storage)	PATA(IDE)/SATA/eMMC/NVMe/SCSI/SAS/FC/RAID Supported disk interface is listed in "Supported SCSI/RAID cards "

		2 Tera byte or over is supported, but only 2T is used.
	Network (required)	Supported network interface card is listed in "Supported network interface card" 10M/100M/1G/10G ethernet.

How to display manual

You can see the product manual in the following ways.

For online download

From the unzipped folder on Windows
(HTML)
Unzipped folder, in [manual] folder, double click "index.html"
(PDF)
Unzipped folder, in [manual] folder, double click "man_gppro.pdf"
* Require Acrobat Reader

From Windows Programs "Windows Erase Program", "Startup Environment Creation Tool", "Utilities for Administrator"

From "Manual" button
(HTML)
It is displayed by clicking the "Manual" button in the upper right corner of the Windows executable program.
However, this is only if the "manual" folder exists in the same folder as the executable program.
If you want to display the manual, copy the "manual" folder and below along with the executable program.

* "Index.html" is called in the "manual" folder. It is also possible to display your own manual.

About license, license activation

About License

A valid license file (license.gp4) is required to run the software.

Evaluation Use
It is possible to operate without a license file, for evaluation use before purchase, but it operates as "evaluation mode" and the disk drives cannot be erased. See "Restrictions on evaluation mode".

No license file is included in the software package, so at first you have to create the license file.
The following steps shows how to create the license file.

> If you have any issue with license activation, please contact support@kirara21.com.

License Activation / Renew / Reissue

There are three types of license processing.

Action	description	current license status	license key	license period
Activation	Activate/Create license file with newly purchased license key	Invalid (NO license or expired)	Newly purchased license key	Period of newly purchased license
Renew	Extend license period with newly purchased license key	Must Valid (before expired)	Newly purchased license key	After the expiration date of the current license, bellow periods are added. Period of newly purchased license + the renewal benefit period (one month or more)
Reissue	Reissue license file within the license validity period	Invalid (NO license file, but license is not expired)	License key previously used for activation	Expiration date at the time of last activation.

Location of the license file

The created license file ("license.gp4") should be located in the same folder as Windows executable program ("gppro4.exe", "gpset4.exe","gputil4.exe"). Name of the file must be "license.gp4" and should be readable.
The license file is read each time the program is run.

For "Boot up Erase Program", the license file is embedded by "gpset4.exe" to CD image file, USB flash drive, HDD bootable environment. Therefore, the "Boot up Erase Program" can be executed with a CD or USB flash drive alone.
"Boot up Erase Program" checks embedded license file at boot time. If license is expired, "Boot up Erase Program" changes its mode to "Evaluation Mode" and can not erase disk drives.
At that time, you have to create CD image, USB Flash drive with new valid license file by "gpset4.exe".

How to move the license file to another location

There is a method to put the license file on a network drive etc. and refer to the license file from each client PC. By using that method, you only need to manage license file updates in one place.

The license file ("license.gp4") should be in the same folder as the Windows executable ("gppro4.exe","gpset4.exe") as well. However, the content of the file should be a text file that describes the path

of the license file as shown below.

```
Sample contents of "license.gp4"
*Describe only "PATH" line below.
-----------------------------
PATH=\\server\erase\license.file
-----------------------------
```

Store the actual license file in the location indicated by the "PATH.

How to create the license file - license activation

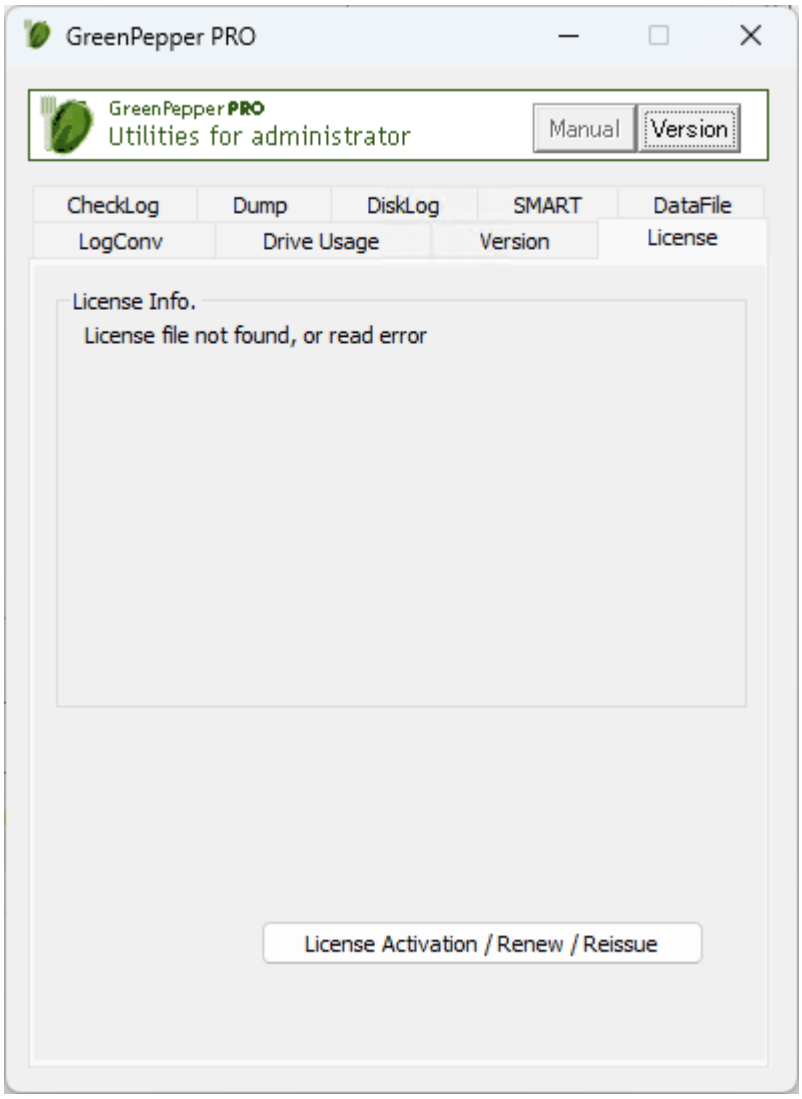
1. Provide License key

When you purchase a license, you will be provided with an License key that looks like this:

License key (sample): 12345-54321-12345-54321-12345

2. Run Utilities for Administrator (gputil4.exe) to Activate and create license file.

Execute "gputil4.exe" from extracted package files. You do not have to "install", just double click "gputil4.exe".

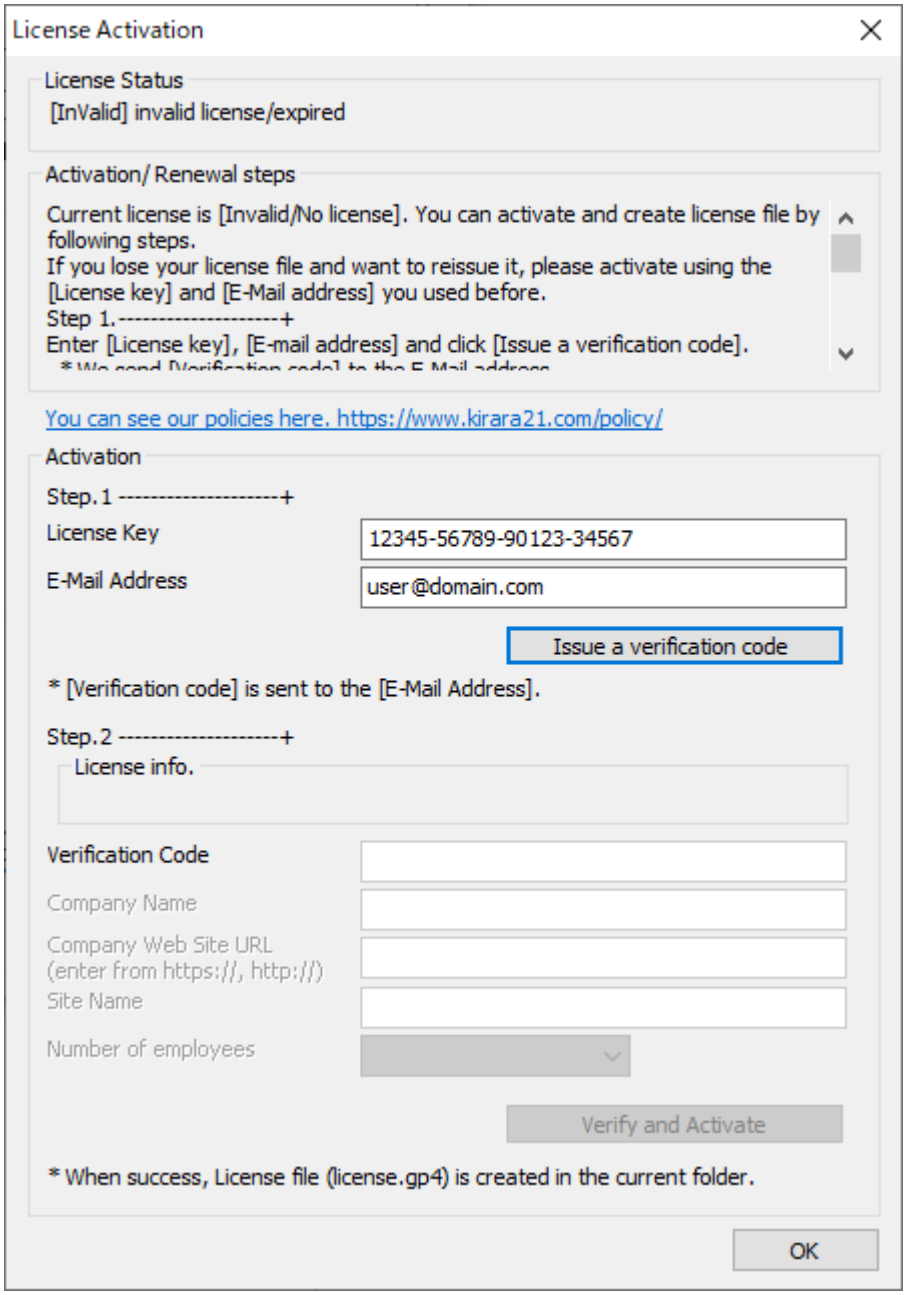


From "license" tab, click "License Activation / Renew / Reissue"

Privacy Policy and Other Policies

Click "You can see our policies here" to check our Privacy Policy and other policies.

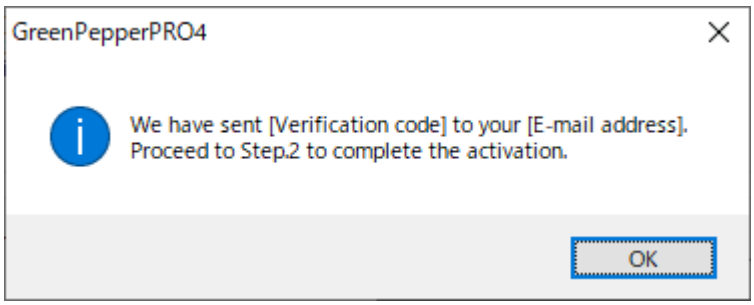
Step.1 ----------+



Enter "License Key", your "E-Mail Address" and click "Issue a verification code".
"Verification Code" is sent to the E-mail address.

* Internet connection is needed for this step.
* This process may take from a few seconds to a minute. Please wait until the end message is displayed.

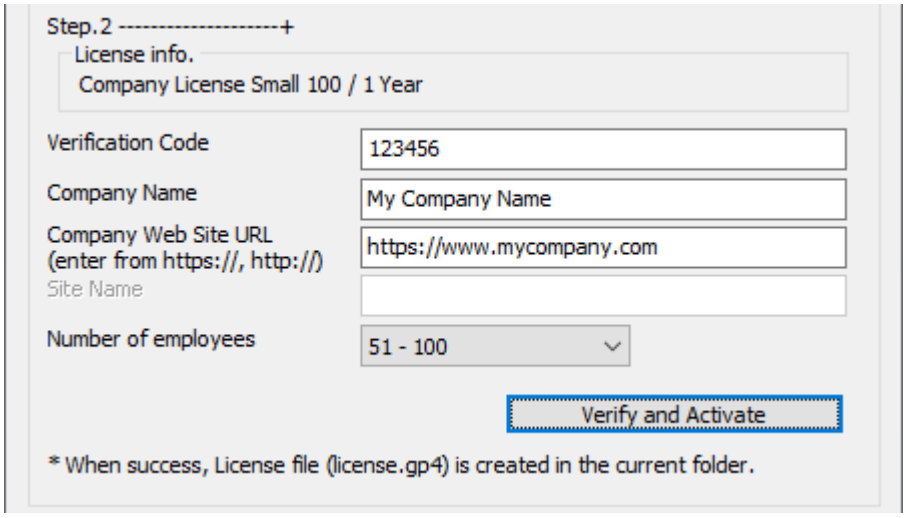
Choose your e-mail address carefully.
·The "Verification Code" required for the next step of activation will be sent to that E-mail address. Use an address that you can reliably receive.
· The email address used this time will be required when reissuing or renewing the license file in the future. Please use the address that you will continue to use in the future.
· If you want to change the registered e-mail address, please contact support@kirara21.com.



If you have this message, "License key" is valid, then "Verification Code" is sent to the E-mail address.

* If you enter the wrong e-mail address, the above completion message will be displayed, but the email will not be sent correctly. Please close the screen once, open this "License Activation" screen again, and retry

Step.2 ----------+



License information is displayed at "License Info.". Make sure it matches the license you purchased.

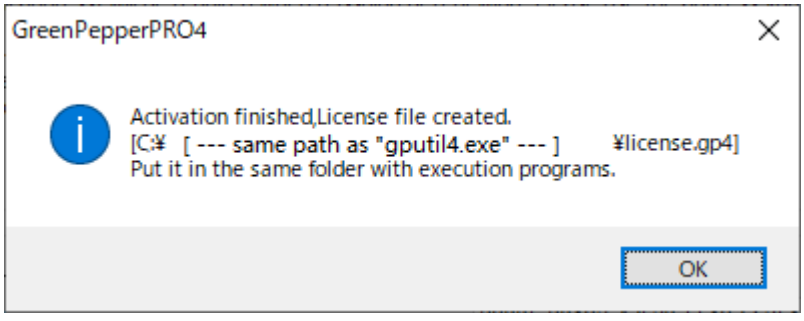
Enter "Verification Code" written in E-Mail message.
Other information required depends on the type of license.

Required informations.

Item	description	Single-User License	Company License	Site License
Company Name	The name of the company that uses the license.	-	required	required
Company Web Site URL	Web site URL of the company. It should start with "http://" or "https://"	-	required	required
Site Name	The name of the Site that uses the license.	-	-	required
Number of Employees	Number of employees of the company or the site.	-	required * Enter number of employees of the Company.	required * Enter number of employees of the Site.

Click "Verify and Activate".

* Internet connection is needed for this step.
* "Verification code" is valid only for one hour, if expired, start over from the first step.
* License file "license.gp4" is created in the same folder as "gputil4.exe". The folder must be writeable.



When license file is created successfully, above message is displayed.

Reissue the license file

If you lose your license file, you can reissue it.
To reissue, you will need the License key and E-Mail address used at the time of initial issuance.

The procedure for reissuing is the same as "How to create the license file - license activation - ". (described above)
* **You have to use the same E-Mail address** used at the time of initial issuance.
  If the E-Mail address is different, the reissuing procedure fails.

Renew the license

It is possible to extend the valid period by the renewal process.
The renewal process must be done while the current license is valid. The renewal process will add the period of the newly purchased license + the renewal benefit period (one month or more) to the expiration date of the current license.

*It is possible to activate with a newly purchased license even after the expiration date of the current license. However, in that case, the validity period is from the date of activation to the period of the purchase license.

The procedure for renewing is the same as "How to create the license file - license activation - ". (described above)
* Make sure that the current **license has not expired**, and that **the license is recognized valid** by the renewal program (gputil4.exe).
  If the processing is performed when the current license is not valid,
  the validity period of the newly activated license will be from the activation date to the purchased license period.
* **You have to use the same E-Mail address** used at the time of initial issuance.
  If the E-Mail address is different, the renewal procedure fails.

About 'Renewal benefit'
As a renewal benefit, even if you purchase a license for a one-year period, the expiration date will be extended to 1-year + one month for the first renewal and 1-year + two months for the second renewal and so on.
The renewal benefits are subject to change in the future, but the latest information will be posted on the website.

First step - License activation

For evaluation use without license

This step is not necessary when used in "evaluation mode". No license purchase is required.
See "Restrictions on evaluation mode" for restrictions in this mode.

License Activation

By purchasing a license and activating it, you will be able to use all the features of the product.
See "About license, license activation" to activate license.

Using "Boot up Erase Program"

For evaluation use only, Use the prepared evaluation CD image. (cd_eval.iso)

*** It is provided for easy evaluation.**

	Step	Contents	Corresponding manual page
1	Create CD-R	Burn the unzipped file "cd_eval.iso" to a CD-R to create a bootable CD-ROM.	How to create a CD from an image file
2	Configure CD boot environment	* Many PCs can boot from CD in the initial state. Make settings so that you can boot from CD on the computer to be erased.	Setting the boot environment on BIOS/UEFI
3	Boot from the CD	Insert the created bootable "CD-R" into the computer to be erased and start it.	Boot from CD/USB stick memory
4	Erasing operation	You can erase the disk by operating the menu. * It runs as "Evaluation Mode", disk drives are not erased.	Erase Disks

Executing the "Boot up Erase Program" from hard disk drive (options can be set).

NO	Step	Contents	Corresponding manual page
1	Place the license file	* For evaluation use, this step is not needed. Place the license file("license.gp4") in the same folder as the executable program (gpset4.exe).	About license, license activation
2	Execute "Startup Environment Creation Tool"	Operate **on the PC to be erased**. The target PC must be able to run Windows. Execute the "Startup Environment Creation Tool" (gpset4.exe) on the Windows of the PC to be erased. *Data file "gpdata.pac" is needed in the same folder.	Executing "Startup Environment Creation tool"
3	Embed boot/erase program to HDD	Install and Embed in the HDD using the "Startup Environment Creation Tool". Specify the required options . * When using the network log, specify "Network".	Operation of "HDD boot" Common option
4	Reboot PC, erasing operation	When the PC is restarted after the installation is completed, the "Boot up Erase Program" will start and erase. * Before erasing, you can also boot existing Windows by selecting in the startup menu. You can uninstall the erase program in the Windows environment.	Boot from Hard disk drive Erase Disks Secure Erase/Sanitize

Creating bootable USB flash drive with "Boot up Erase Program" (options can be set)

3	Step	Contents	Corresponding manual page
1	Place the license file	* For evaluation use, this step is not needed. Place the license file("license.gp4") in the same folder as the executable program (gpset4.exe).	About license, license activation
2	Execute "Startup Environment Creation Tool"	Execute the "Startup Environment Creation Tool" (gpset4.exe) on Windows. You can use a different PC than the one you want to erase. *Data file "gpdata.pac" is needed in the same folder.	Executing "Startup Environment Creation Tool"
3	Setting bootable USB flash drive	Insert the USB flash drive to be set, specify the option in the "Startup Environment Creation tool", and configure the USB memory. * When using the network log, specify "Network".	Setting bootable "USB stick" Common option
4	Configure USB boot environment	Make settings so that you can boot from USB device on the computer to be erased.	Setting the boot environment on BIOS/UEFI _
5	Boot from USB flash drive/Erase operation	Insert the set USB flash drive into the PC to be erased and boot it. Erase with the "Boot up Erase Program".	Boot from CD/USB stick memory Erase Disks Secure Erase/Sanitize

Creating bootable CD with "Boot up Erase Program" (options can be set)

NO	Step	Contents	Corresponding manual page
1	Place the license file	* For evaluation use, this step is not needed. Place the license file("license.gp4") in the same folder as the executable program (gpset4.exe).	About license, license activation
2	Execute "Startup Environment Creation Tool"	Execute the "Startup Environment Creation Tool" (gpset4.exe) on Windows. You can use a different PC than the one you want to erase.	Executing "Startup Environment Creation Tool"
3	Creating bootable CD image	Execute "Startup Environment Creation tool", and create CD image file with various options. * When using the network log, specify "Network".	Creating bootable "CD image" file Common option
4	Create CD-R	Burn CD-R with created CD image file.	How to create a CD from an image file
5	Boot from the CD/Erasing operation	Insert the CD into the PC to be erased and boot it. Erase with the "Boot up Erase Program".	Boot from CD/USB stick memory Erase Disks Secure Erase/Sanitize

Creating bootable CD/USB flash drive with Network boot Host

NO	Step	Contents	Corresponding manual page
1	Place the license file	* For evaluation use, this step is not needed. Place the license file("license.gp4") in the same folder as the executable program (gpset4.exe). * Company/Site license is requierd for Network boot host.	About license, license activation
2	Execute "Startup Environment Creation Tool"	Execute the "Startup Environment Creation Tool" (gpset4.exe) on Windows. Datafile (both gpdata.pac and gpdatahost.pac) must be in the same folder as "gpset4.exe".	Executing "Startup Environment Creation Tool"
	Creating bootable CD	On "netboot" tab, specify CD image file/USB flash drive,	Creating Network boot host image/ USB flash

3	image/USB flash drive	address, functions. Specify options for the erase program downloaded from network boot host.	drive Common option
4	Create CD-R (when using CD image file)	Burn CD-R with created CD image file.	How to create a CD from an image file
5	Boot from the CD/US flash drive	Insert the CD/USB flash drive into the PC to be used for Network boot host. Erase with the "Boot up Erase Program".	Boot from CD/USB flash drive

Using "Windows Erase program"

Using "Windows Erase Program" on Windows.

NO	Step	Contents	Corresponding manual page
1	Place the license file	* For evaluation use, this step is not needed. Place the license file("license.gp4") in the same folder as the executable program (gppro4.exe).	About license, license activation
2	Execute Program	Execute the "Windows Erase Program" (gppro4.exe) directly from the "Product CD-ROM". For online download, execute from the unzipped folder.	Executing "Windows Erase program"
3	Erasing operation	You can erase the disk by operating the program.	Erase Disks

Using "Windows Erase Program" on WindowsPE

*Erasing the system drive(c:) and SecureErase are possible by running "gppro4.exe" on WindowsPE.

NO	Step	Contents	Corresponding manual page
1	Create WindowsPE environment	Using Windows "System Repair disc" or, Download WindowsPE related files from Microsoft site, building the environment. Place "Windows Erase program" (gppro4.exe) in the WinPE tree.	Building WindowsPE boot environment
2	Place the license file	* For evaluation use, this step is not needed. Place the license file("license.gp4") in the same folder as the "Windows Erase program" (gppro4.exe).	About license, license activation
2	Execute "Startup Environment Creation Tool" to create "WindowsPE configuration file"	(Only when you want to automatically erase disk drives or specify the processing method.) Execute "Startup Environment Creation tool", and create "WindowsPE configuration file"(config.gp4) with various options. * When using the network log, specify "Network". *Data file "gpdata.pac" is needed in the same folder. Place the file("config.gp4") in the same folder as the "Windows Erase program" (gppro4.exe).	Executing "Startup Environment Creation Tool"
3	Creating bootable CD image,bootable USB flash drive	In the WindowsPE creation environment, use the command to create a CD image or set the USB memory. If you want to boot from CD, burn CD-R with created CD image file.	Runing on WindowsPE How to create a CD from an image file
4	Boot from the CD/USB flash drive/Erasing operation	Boot PC with the CD/USB flash drive. Erase with the "Windows Erase Program".	Erase Disks

How to create a CD from an image file (iso9660)

If we provide the product CD as an image file, or if you use a bootable CD, you need to create a bootable CD-R from the CD image file (iso9660 format).
Writing in the same way as normal data file does not result in a bootable CD-R. After writing, if the same file name with CD image file is found in CD-R , the writing method is incorrect.

* You may use CD-RW, DVD-R, DVD-RW instead of CD-R.

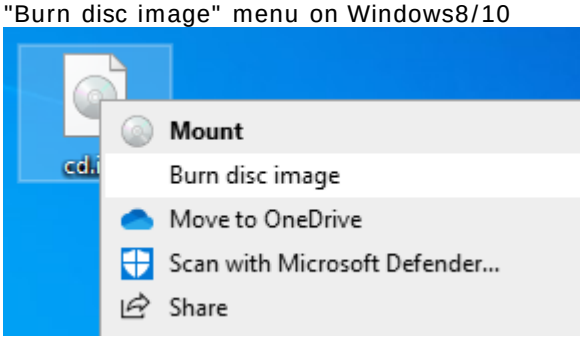
Incorrect example: After writing "cd.iso", only the "cd.iso" file exists on the CD-R.

Burn a CD-R using the following method on a Windows PC to which a CD writable device is connected.

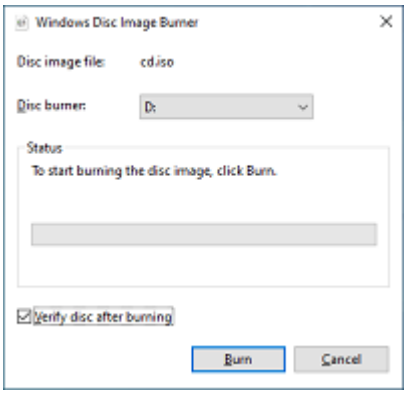
Windows 7/8/10/11

In Windows 7 or later, it supports writing CD image files.
In Windows 8/10, click the right mouse button on the file to burn and select "Burn Disc Image".
In Windows 7, just double-click the file you want to burn and you're ready to burn.

"Burn disc image" menu on Windows8/10



If you select "Burn Disc Image", you will see a screen like this. Insert a blank CD-R media into the drive and click the "Burn" button to burn.
* Please check "Verify disc after burning" for reliable writing.



Other than Windows 7/8/10/11

A CD-R writing software that supports writing of CD image files (ISO9660 format) is required.
The writing method differs depending on the CD-R writing software. For details, see the manual of the software you are using.

Setting the boot environment on BIOS

It may be necessary to change the BIOS/UEFI settings of the computer in order to boot the CD-ROM or USB flash drive, which is a feature of this product. Follow the steps below to change the BIOS/UEFI settings.
In many cases, you do not need to change the default settings.

* The following is an explanation using Phoenix's Award BIOS as an example.
The contents vary depending on the model and manufacturer. For details, refer to the computer manual or contact the manufacturer.

Phoenix's Award BIOS example

Display the BIOS setting screen

Turn on your computer and press the Delete key once (or several times in a row) while the message "Press DEL to enter SETUP" is displayed.
(Depending on the manufacturer, it may be F1, F2, or other multiple key combinations.)

Setting boot device priority

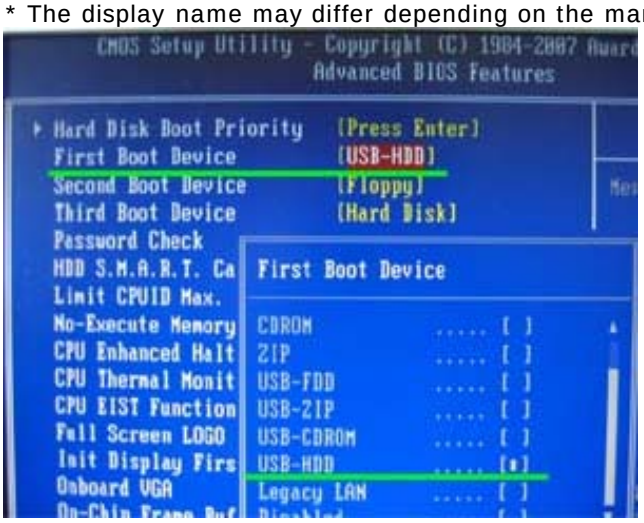
The PC has a boot priority, and if it is possible to boot from multiple hard disks, CDs, USB flash drive, etc., it will try to boot in the specified priority.
To boot from a CD-ROM or USB flash drive, it is necessary to prioritize them over the hard disk.

Select "Advanced BIOS Features" and press the [Enter] key.

When booting from the CD-ROM, select the CDROM in "First Boot Device"

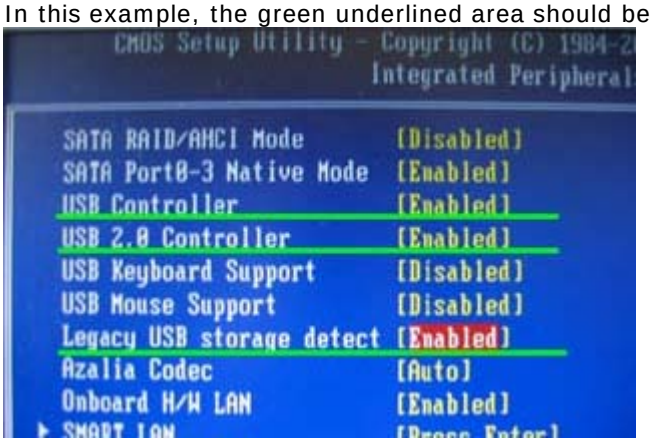
When booting from the USB flash drive, select the USB-HDD in "First Boot Device"

* The display name may differ depending on the manufacturer.



Setting to enable USB flash drive (only when USB flash drive boot)

If the USB flash drive is not recognized at all, the following USB-related settings may not have been made. In this example, the green underlined area should be Enabled.



Select "Save & Exit Setup" to save the settings

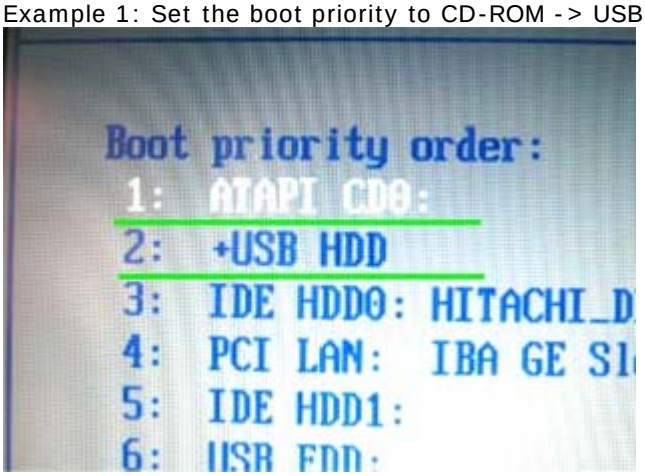
Press [Y] (Yes) on the confirmation screen below.

With this BIOS, you can now boot from the CD-ROM / USB flash drive.

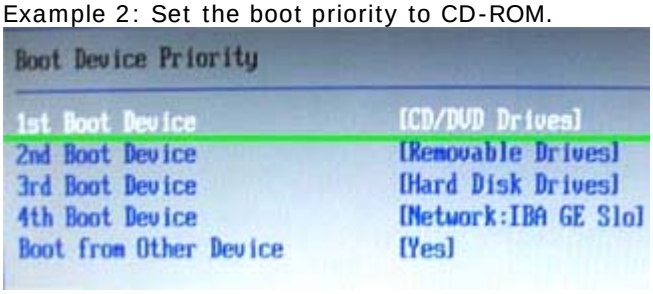
* CD-ROM is basically compatible with many IDE / USB / SATA, but some are not.
* USB memory booting has various settings depending on the BIOS, and it is not possible to boot with all PCs and USB flash drive combinations.
* You cannot use an encryption-compatible USB flash drive that requires a password to be entered when accessing.

Example of other BIOS

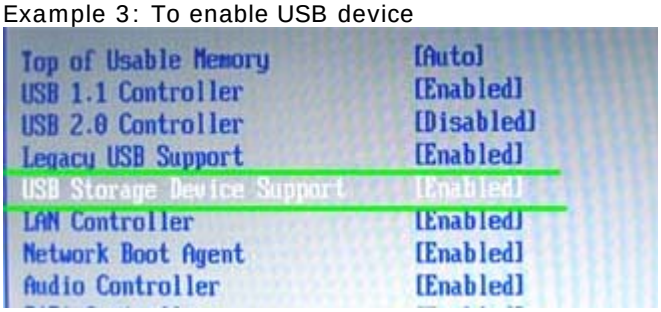
Example 1: Set the boot priority to CD-ROM -> USB memory.



Example 2: Set the boot priority to CD-ROM.



Example 3: To enable USB device

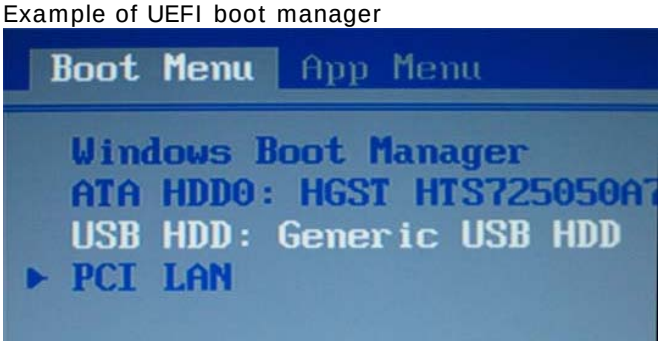


Setting the boot environment on UEFI

With "GreenPepper PRO", UEFI boot is possible when booting from a CD / USB flash drive or hard disk.
Select the boot device with the UEFI boot manager, or set the boot priority of USB memory, CD, etc. to the top in the UEFI settings. Also, depending on the PC model, it may not be possible to boot unless SecureBoot is disabled.

The UEFI boot manager is usually displayed by pressing the F12, F11 or F10 key at PC startup.

Example of UEFI boot manager



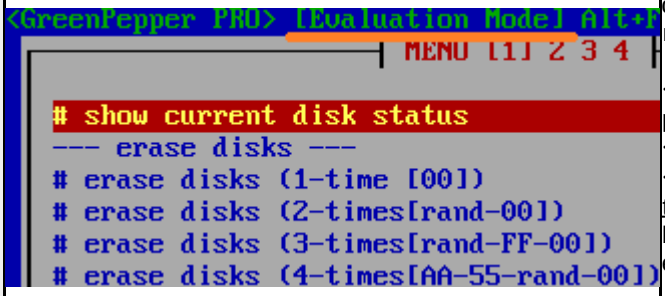
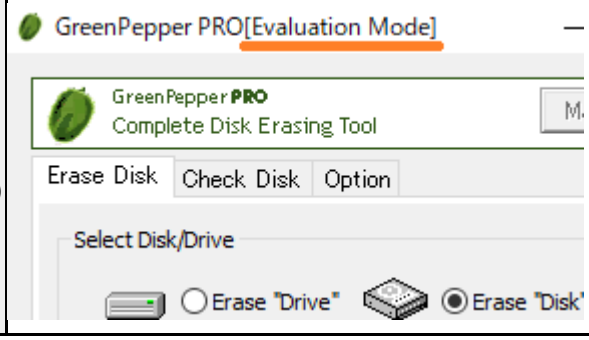
About "Evaluation mode"

The product has an "evaluation mode" that you can use and evaluate before purchasing a license.
"Evaluation mode" is automatically set when the license file does not exist or the license has expired and is invalid.

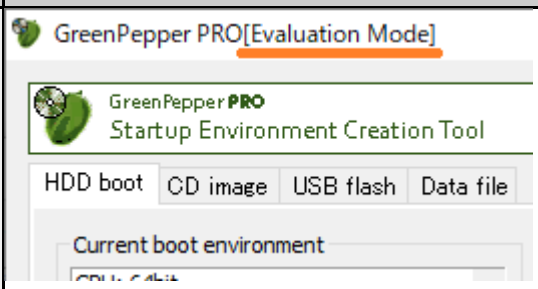
You can check whether the program is currently running in "evaluation mode" by checking the message at the time of starting the program, the screen display after starting, and so on. "Evaluation mode" has some restrictions as described below.

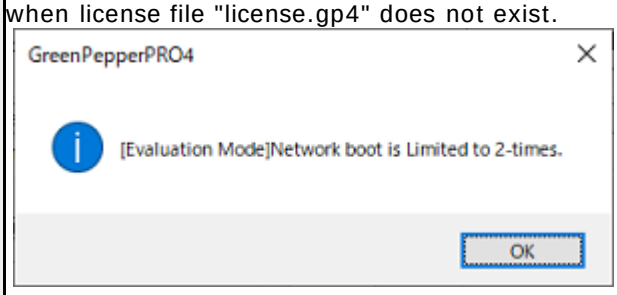
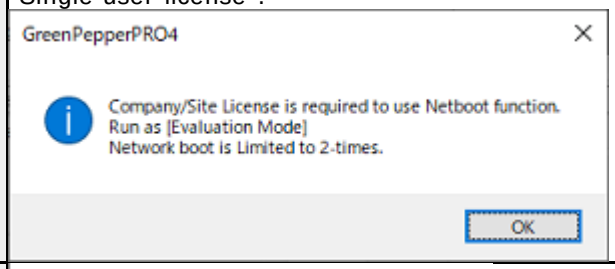
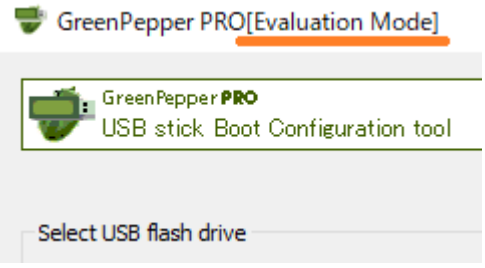
Restrictions on Evaluation mode

Erase Program

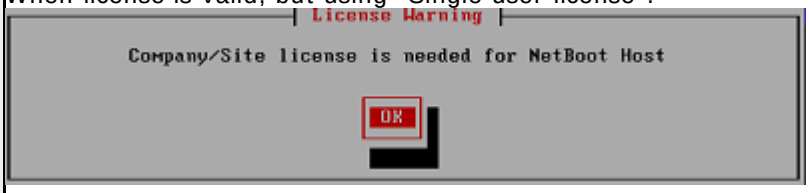
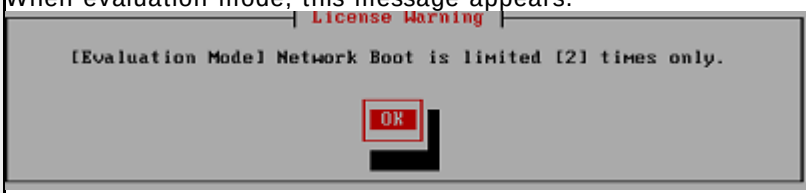
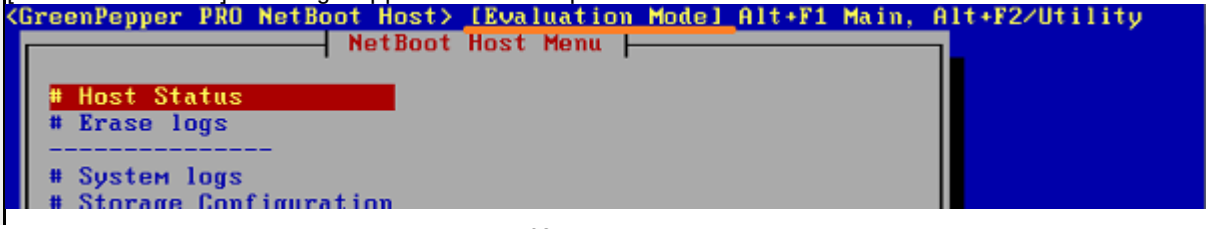
Program	Identification of Evaluation mode	Restrintions of Evaluation mode
Boot up Erase Program		· Disk drives will **not be erased.** The write process is replaced by the read process. Therefore, the processing speed may be slightly faster than writing. * Especially in the case of RAID configuration, the processing time may change significantly. · Secure erase/Sanitize cannot be performed. · HDD log is not written. · The read verification process after the erase process will result in error because it has not actually been erased. · The following cannot be executed in the "utility" menu displayed by ALT + F5. "Secure erase processing test" "Erase HDD password" "HPA removal"
Windows Erase Program(gppro4.exe)		· Disk drives will **not be erased.** The write process is replaced by the read process. Therefore, the processing speed may be slightly faster than writing. · HDD log is not written. · The read verification process after the erase process will result in error because it has not actually been erased.

Tools/Utilities, Data

Program	Identification of Evaluation Mode	Restrintions of Evaluation mode
		"Boot up Erase Program" executed from HDD, USB flash drive, CD image, created/set by this program will run as "Evaluation Mode". So **disk drives will not be erased**.
	for "Network Boot" configuration	

Startup Environment Creation Tool (gpset4.exe)	When press "Execute [Host]", following message appears. when license file "license.gp4" does not exist.  when valid license file "license.gp4" exists, but it is "Single user license".  	If you use a network boot host to perform network boot and download the erase program, the number of times is limited to two. If this is done twice, the network boot server function will stop and subsequent network boots will no longer be possible.
USB stick Boot configuration tool (gpusbst4.exe)	 	"Boot up Erase Program" executed from USB flash drive, set by this program will run as "Evaluation Mode". So **disk drives will not be erased**.
Utilities for Administrator (gputil4.exe)	---	No evaluation mode.
Data for "Startup Environment Creation Tool" (gpdata.pac)	---	No evaluation mode.
Network boot Data file for "Startup Environment Creation Tool" (gpdatahost.pac)	---	No evaluation mode.

Network Boot Host

Program	Identification of Evaluation mode / Restrintions of Evaluation mode
Network Boot Host	When license is valid, but using "Single user license".  When evaluation mode, this message appears.  [Evaluation mode] message appears on the top of the menu. 

If you use a network boot host to perform network boot and download the erase program, **the number of times to perform network boot is limited to two**.
If this is done twice, the network boot server function will stop and subsequent network boots will no longer be possible.
The following message is shown on the top of the menu, when one of menu item is executed.

What is "Secure Erase", "Sanitize"?

"GreenPepper PRO"-"Boot up Erase Program", and "Windows Erase Program"(only when runnin on WindowsPE) have "Secure Erase" and "Sanitize" functions.

"Secure erase" is superior to normal erasure in terms of security and processing speed, but its execution environment is limited and there are uncertainties due to processing outside the control of the software. Please use it after fully understanding the features.

"Sanitize" is a newer standard than "Secure erase", and if it is a compatible hard disk or SSD, there are less restrictions on the execution environment (Some PCs have some restrictions) and it can be executed more easily. In addition, since it is possible to grasp the progress status during execution, it is possible to erase more reliably. However, currently fewer disks support "Sanitize" than "Secure erase".

Supported disks by "GreenPepper PRO"(Boot up Erase Program) ver. 4.6.4 or later
· ATA(IDE,SATA) disk (include SSD) · · · SecureErase/Sanitize
· NVMe drive · · · SecureErase/Sanitize
· eMMC drive · · · SecureErase/Sanitize
· Other(SAS, RAID etc.) · · · only normal erase

Supported disks by "GreenPepper PRO"(Windows Erase Program on WindowsPE) ver. 4.7.1 or later
· ATA(IDE,SATA) disk (include SSD) · · · SecureErase/Sanitize
· NVMe drive · · · SecureErase/Sanitize
· eMMC drive · · · only normal erase
· Other(SAS, RAID etc.) · · · only normal erase

Normal erasing process

The normal erasing process that "GreenPepper PRO" also has is realized by performing the process of writing data by specifying the location and value for the entire disk area.

Secure Erase/Sanitize process

Secure erase and sanitize processing are functions provided by ATA (PATA , SATA), NVMe, and eMMC disk itself. By sending a command to perform Secure erase / Sanitize to the corresponding disk, the erase process is executed inside the disk.

When Secure erase / Sanitize is recommended

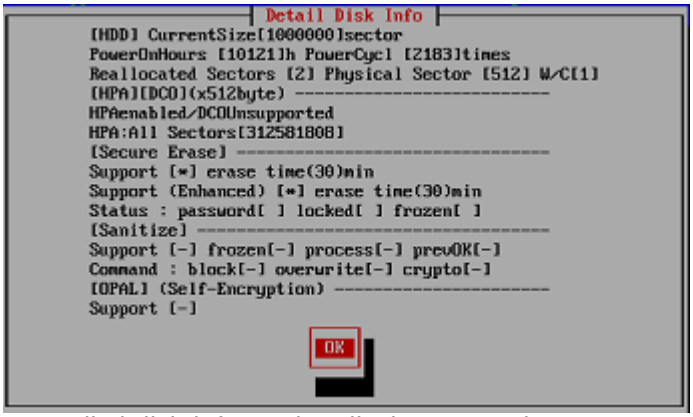
1.When there are many "Reallocated sectors"

Hard disks are processed in units called sectors (usually 512 or 4096bytes). If an error occurs frequently in a certain place due to a defect on the disk surface, the disk isolates the bad sector by allocating the area that it has as a spare as a substitute for the bad sector.

There may be some data left in the reallocated bad sectors, but the detached bad sectors cannot be erased by normal erasing because they are completely inaccessible to the software.
There are two types of secure erase. Normal "Secure Erase" does not erase reallocated bad sectors, but "Enhanced Secure Erase" erases reallocated bad sectors as well. The "Sanitize" process also erases reallocated bad sectors.

The following points should be considered regarding the necessity of erasing reallocated sectors.
· Cannot be read by normal software processing
· Because it is "bad", the possibility of reading is low.
· Even if secure erasure is performed, it is uncertain whether it can be completely erased because it is defective.

You can check the number of "reallocated sectors" on the "GreenPepper PRO" screen.



* Detailed disk information display screen in "Boot up Erase Program"

2. flash drive media such as SSD (ATA), NVMe, eMMC
Since flash drive has a finite limit on the number of rewrites, SSDs and the like often have a built-in mechanism that averages the writing locations (Wear Leveling) so that writing does not concentrate on the same location. With these mechanisms, the correspondence between the write position (sector) specified by the software and the memory cell where the write is actually performed is dynamically changed. In addition, the memory for allocation is often more than the total capacity available to the user. Therefore, even if the entire disk is written (erased), the entire installed memory may not always be erased.

In addition, in order to avoid time-consuming erasing processing during normal writing, the target memory area may not be erased and area replacement may be performed (dynamic memory mapping).
For SSD (ATA), eMMC, etc. that support secure erase / sanitize, it is possible to avoid "Wear Leveling" and dynamic memory mapping by performing secure erase / sanitize processing , and erase all installed memory cells.

3. When processing speed is required
Since the secure erase / sanitize process is performed inside the disk, it is executed at the highest processing speed of the disk hardware. Therefore, it can be processed faster than normal erasing.
Especially for flash drive (SSD, NVMe, eMMC), secure erase / sanitize processing is considerably faster.
However, if it is a hard disk, the normal erasing process in "Green Pepper PRO" is performed at a very high speed, so it is possible to perform the processing in a time close to secure erasing.

See "Time required to erase disk"

Problems with Secure Erase / Sanitize

Secure Erase / Sanitize has many advantages as mentioned above, but it also has the following problems.
· The processing environment is limited. (See "Details of Secure Erase / Sanitize" below)
· Especially for Sanitize, there are not many HDDs and SSDs that support it.
· Since it is a process outside the control of the software, the status cannot be grasped, the content of the process depends on the manufacturer's implementation and cannot be known, and even if a write error occurs, it may not be known.
Therefore, in "Green Pepper PRO", after Secure Erase and Sanitize, we provide normal writing/reading process to check the contents of the disk.

Details of Secure Erase / Sanitize

ATA (SATA) Secure Erase processing details

There are two types of secure erase: normal "Secure Erase" and "Enhanced Secure Erase". "Enhanced" is a newer and more reliable erasing method. If the disk supports "enhanced", "Green Pepper PRO" will automatically select "enhanced".

· Secure Erase
Erase the entire disk with zero. "Reallocated sectors" that have been detached are not erased.

· Enhanced Secure Erase
Erase the entire disk with zero or a value specified by the manufacturer. "Reallocated sectors" that have been detached are also erased. * The same value may not be written to the entire disk, such as when a random value is written. Therefore, a verification error may occur in the read verification process performed just after secure erase.

The time required for Secure Erase is written in advance on the disk by the manufacturer. "Green Pepper PRO" reads the value and display it on the screen.

ATA(SATA) Sanitize processing details

The sanitize process erases all user areas, including reallocated bad sectors and unallocated areas.
There are three types of ATA standard sanitize process as follows.

· CRYPTO SCRAMBLE: Delete the encryption key on the encryption-compatible HDD / SSD.
· BLOCK ERASE: Performs memory block erasure processing, especially on SSDs.
· OVER WRITE: Erase by overwriting.

In "Pepper PRO", the following processing is performed.
O: supported X: unsupported -: any

CRYPT	BLOCK ERASE	OVER WRITE	Content of processing
O	O	-	CRYPT SCRAMBLE + BLOCK ERASE
O	X	O	CRYPT SCRAMBLE + OVER WRITE
O	X	X	CRYPT SCRAMBLE
X	O	-	BLOCK ERASE
X	X	O	OVER WRITE

NVMe Secure Erase/Sanitize processing details

NVMe drives have more memory than the user's available capacity and are configured with constantly changing memory allocations (dynamic memory mapping). NVMe Secure Erase erases the entire device, including unallocated space. Note that if the device is divided into multiple drives (NameSpace), the entire device will be erased, including unselected drives, depending on the model.
The processing content is almost the same as the ATA drive.

eMMC Secure Erase/Sanitize details

eMMC drives have more memory than the user's available capacity and are configured with constantly changing memory allocations (dynamic memory mapping). In the Sanitize process of eMMC flash drive, the entire user's available capacity is erased (Erase) and then the non-allocated area is erased (sanitized). Secure Erase performs memory erase processing only on the user's available capacity.
In "Green Pepper PRO", Sanitize processing is performed when sanitize is supported, and Secure Erase is performed when sanitize is not supported (secure erase is supported).

Settings for secure erase / sanitize processing method on ATA / MVMe / eMMC drives

The processing method in "Secure Erase / Sanitize" can be changed arbitrarily.
See "Utilities"-> "Set Secure Erase Method / Unfreeze".

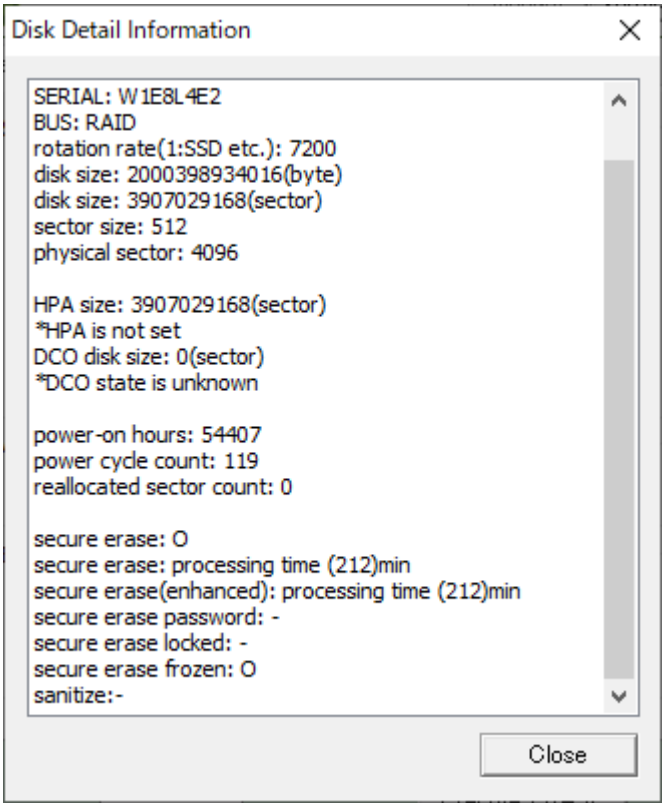
Disk / Interface support

To perform Secure Erase, the disk itself must comply with the Secure Erase standard. If it is an ATA (PATA, especially SATA) disk that has been on the market in recent years, it seems that the disk is compatible in many cases.
However, it is often the case that disks less than 100G several years ago do not support enhanced processing. There are many disks that do not support Sanitize.

In addition to being supported by the disk, the disk interface you are using (both hardware and software) must pass the ATA command processing for Secure erase. For example, SATA and PATA connected to Intel chipset (ICH7,8,9,10, etc.) can be processed in many cases. But disks connected by USB interfaces may not be processed even if it is the same disk drive.

Whether processing is possible or not

Even if the disk and interface are compatible, processing may not be possible depending on the disk status.



* Detailed disk information display screen in "Windows Erase Program"

Secure Erase "Frozen" state / ATA drive
If a freeze command is sent to the disk and the disk is in a frozen state, secure erase-related operations cannot be performed.
The freeze command is automatically sent from your computer to the disk when you turn on the power.
Normal disk read / write works fine even if the disk is frozen state.

On many PCs, the BIOS sends a freeze command to all disks at boot time.
It is to prevent malicious software such as viruses from setting passwords or erasing the disk. In such a PC, the disk is originally unfrozen when the power is turned on, but immediately after that, BIOS sends a freeze command unconditionally, so if you look at the state of the disk after the PC starts up, It will be frozen.
*Freezing processing for Sanitize(ATA) is not performed on many PCs, but it is frozen on some PCs.

In order to release the frozen state, it is necessary to either prevent the Freeze command from being sent by changing the BIOS settings, or to connect the disk to a PC that does not send such a command. It cannot be canceled by software processing.
It is possible to turn the power of the disk off and on while the PC is running, but there is a risk of damaging the disk and other parts, so please be aware of the danger and do so at your own risk.
* In general, it seems that the SATA power supply is relatively safe even if it is inserted or removed when PC is running. IDE power cable should not remove or insert.

Unfreeze process (ver 4.7.1 or later)
In order to unfreeze the ATA drive, we have implemented a process that suspends the PC and then resumes it. (Only when booting from a CD/USB memory with the "Boot up erase program").
There are two ways to do this: specify the option at startup, or select "Utility"/"Set Secure Erase Method/Unfreeze".
However, in order to perform this process, the video chip of the PC must be compatible. If it is not compatible, it will not be executed even if the process is selected, or the screen will remain black after processing and nothing will be displayed.
* NVMe drives do not have a frozen state due to their specifications, but with some drives, secure erasing will result in an error under normal conditions, and processing may be possible by "unfreezing" processing.

See "Boot from CD/USB flash drive".
See "Utilities"-> "Set Secure Erase Method / Unfreeze".
See "Supported display chips"

Secure Eras "Password Locked" state / ATA drive
One of the standards for secure erasure is the setting of a hard disk password. When the power of the password-set disk is turned on, the disk becomes "locked state" and you cannot access the disk including reading and writing.
To unlock the "locked state", you need to unlock with the set password or delete the password.
Of course, if you don't know your password, you can't unlock / delete it.

· "Frozen" state

Read / write is possible. Password setting/deleting and unlocking are not possible. Secure erase is NOT possible. Cannot be canceled by command.

· "Password Locked"state
Read / write is NOT possible. Secure erase is NOT possible.
The status can be released by the unlock / password delete command. Password required.

Secure Erase / Sanitize processing procedure

"Green Pepper PRO" automatically performs a series of processes internally, so you do not need to be aware of it. However, if you know the process it will be easier for recovery when Secure erase / Sanitize is interrupted.

To perform secure erase on an ATA disk, you must set a hard disk password in advance and specify it during the secure erase process. In "GreenPepper PRO", the word "pass" is set as the disk password (master) and processing is performed.

Problems when Secure Erase is interrupted

If the Secure erase process is interrupted in the middle, the disk erase is not completed.
Please execute the erasing process again.

Problems when ATA disk Sanitize is interrupted

Depending on the supported specifications, the Sanitize process will continue the next time the power is turned on.
In that case, normal reading and writing will NOT be possible.
It must be left power-on until the Sanitize process is complete.

Standards to be complied with in erasing disks

Various standards have been established for disk erasing since the 1990s, centered on the national institutions of the United States. However, due to the recent increase in disk capacity and the spread of memory media such as SSDs, the methods required for erasing have changed significantly.

"Green Pepper PRO" complies with "US Army Information Systems Security AR380-19"(Feb. 1998) for 3 writings and "US Secretary of Defense DoD5220.22-M Supplement 1"(Feb. 1995) for 4 writings + verification.
However, these standards are obsolete and are moving in recent years to the National Institute of Standards and Technology (NIST SP 800-88 Rev1) (December 2014), which was revised in December 2014. NIST 800-88 does not simply define the writing pattern for erasing, but also mentions how to determine how to dispose of it, and how to handle each individual medium such as HDD and SSD.
It is recommended that the person in charge of erasing read it.

US Army AR380-19 standards

US Army Information Systems Security (AR380-19) 27-Feb-98

Overwrite 3 times

Appendix F Clearing, Sanitizing, and Releasing Computer Components
Overwrite all locations three times (first with random character, second time with a specified character, third time with the compliment of the specified character.

US Secretary of Defense DoD5220.22-M standards

Secretary of Defense DoD5220.22-M Supplement 1 Feb-95

Overwrite 3 times and verify

Overwrite all locations with a character, its complement, then with a random character.
Verify that all sectors have been overwritten and that no new bad sectors have occurred.

In the subsequent revised editions, the erasure method is left to the CSA, and there is no mention of the specific method.

CSA: Cognizant Security Agency. These agencies include the Department of Defense (DoD), Department of Energy (DOE), Central Intelligence Agency (CIA), and Nuclear Regulatory Commission (NRC).

DoD5220.22-M Feb-2006
Clearing and Sanitization. Instructions on clearing, sanitization and release of IS(Information system) media shall be issued by the accrediting CSA.

DoD5220.22-M Incorporating Change 1 ,Mar-2013
Clearing and Sanitization. Instructions on clearing, sanitization and release of IS media shall be issued by the accrediting CSA.

DoD5220.22-M Incorporating Change 2 ,May-2016
Sanitize or destroy ISs media before disposal or release for reuse in accordance with procedures established by the CSA.

Only in the following unofficial revisions, you can see the description of the deletion method as an informal comment.

DoD 5220.22-M Incorporating Change 1 with inline ISLs Compiled May 2, 2014
Non-Removable Rigid Disk: Overwrite all addressable locations with a single character.

NIST SP 800-88 standards

NIST: National Institute of Standards and Technology

NIST Special Publication 800-88 Guidelines for Media Sanitization (NIST SP 800-88) **September, 2006**

Drives after 2001, Overwriting once is adequate

That is, for ATA disk drives manufactured after 2001 (over 15 GB) clearing by overwriting the media once is adequate to protect the media from both keyboard and laboratory attack.

4 types of sanitization

Disposal, Clearing, Purging, Destroying
Decide on the appropriate type of sanitization.
The selected type should be assessed as to cost, environmental impact, etc.,

Determining what type of sanitization

Make decisions by considering factors such as the importance of security, reuse, or leaving your organization's control. In addition, it is necessary to confirm the process and document it.

Media Sanitization Decision Matrix

Media Type	Clear	Purge	Physical Destruction
Floppies	Overwriting	Degauss	incinerate, shred
ATA Hard Drives	Overwriting	Secure Erase Degauss	disintegrate, shred, pulverize, incinerate
Other (SCSI,SAS) Hard Drives	Overwriting	Degauss	disintegrate, shred, pulverize, incinerate
Compact Flash Drives, SD	Overwriting	Physical Destruction	disintegrate, shred, pulverize, incinerate
USB Removable Media	Overwriting	Clear	disintegrate, shred, pulverize, incinerate

---

NIST Special Publication 800-88 Guidelines for Media Sanitization (NIST SP 800-88) Revision 1
December, 2014

For magnetic media, a single overwrite hinders recovery of data

For storage devices containing magnetic media, a single overwrite pass with a fixed pattern such as binary zeros typically hinders recovery of data even if state of the art laboratory techniques are applied to attempt to retrieve the data.
One major drawback of relying solely upon the native Read and Write interface for performing the overwrite procedure is that areas not currently mapped to active Logical Block Addressing (LBA) addresses (e.g., defect areas and currently unallocated space) are not addressed.

3 actions that can be taken to sanitize media

Clear: applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques
Purge: applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.
Destroy: renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.

Making decisions of disposition

Make decisions by considering factors such as the importance of security, reuse, or leaving your organization's control. In addition, it is necessary to confirm the process and document it.

Processing method in each media

media	Clear	Purge	Physical Destruction
Floppies	Overwrite all accessible area at least a single write pass with a fixed data value.	Degauss	incinerate, shred
ATA(PATA,SATA)	Overwrite all accessible area at least a single write pass with a fixed data value.	Execute SANITIZE. (OVERWRITE,CRYPTO_SCRAMBLE) Execute SECURE_ERASE. (SANITIZE commands are preferred)	disintegrate, shred,

Fixed Magnetic Disks	Verification must performed, should cover at least 10% of the media.	Verification must performed, should cover at least 10% of the media. or Degauss	pulverize, incinerate
ATA(PATA,SATA) SSD	Overwrite all accessible area at least a single write pass with a fixed data value. Execute SECURE_ERASE. Verification must performed, should cover at least 10% of the media.	Execute SANITIZE. (OVERWRITE,CRYPTO_SCRAMBLE) Verification must performed, should cover at least 10% of the media.	disintegrate, shred, pulverize, incinerate
SCSI (SCSI,SAS) Fixed Magnetic Disks	Overwrite all accessible area at least a single write pass with a fixed data value. Verification must performed, should cover at least 10% of the media.	Execute SCSI SANITIZE. (OVER WRITE, CRYPTOGRAPHIC ERASE) Verification must performed, should cover at least 10% of the media. or Degauss	disintegrate, shred, pulverize, incinerate
NVMe (SSD)	Overwrite all accessible area at least a single write pass with a fixed data value. Verification must performed, should cover at least 10% of the media.	Execute NVMe FORMAT (User Data Erase, Cryptographic erase) Verification must performed, should cover at least 10% of the media.	disintegrate, shred, pulverize, incinerate
Memory Cards (SD, MMC, etc.)	Overwrite all accessible area at least a single write pass with a fixed data value.	N/A	disintegrate, shred, pulverize, incinerate
USB Removable Media	Overwrite all accessible area at least a single write pass with a fixed data value.	Execute SANITIZE (if supported)	disintegrate, shred, pulverize, incinerate

While the evolution of memory media such as SSD is remarkable, the standards of AR380-19, DoD5220.22-M, etc. are becoming older.
In addition, since there are many parts that are not sufficiently described in the standard, it is necessary for each company to establish an erasure policy and perform erasure.

Points to consider about erasing method

Consideration of "Reallocated sector"

In a hard disk, when an error occurs frequently at a certain place (sector) due to a defect on the disk surface, the bad sector is detached by allocating an area that the disk has as a spare as a substitute for the bad sector (reallocation). Detached bad sectors will not be accessible in software processing from outside the disk.
Therefore, it is unlikely that it will be a serious problem for normal level erasure, but in cases where strict security is required, "Reallocated sectors" should be considered.
Erasing reallocated sectors requires Enhanced Secure erase/Sanitize processing.

Consideration of "Wear Leveling" in flash drive media such as SSD

Since flash drive has a finite limit on the number of rewrites, SSDs and the like often have a built-in mechanism that averages the writing locations (Wear Leveling), so that writing does not concentrate on the same location. (See "About Secure Erase/Sanitize")
Therefore, in normal overwrite processing, the allocation of the memory cell to be erased may be changed and may not be erased.
To avoid Wear Leveling and erase the entire area, Enhanced Secure Erase / Sanitize processing is required.
However, for USB memory that does not process ATA commands, and SSDs that do not support secure erase / sanitize, it is possible to reduce the risk of data remaining by erasing three or more times.

Consideration of unallocated space in flash drive media such as SSD

In addition to the above "Wear Leveling", many flash memories frequently change the memory area allocation in order to shorten the erase processing time. As a result, memory in unallocated space cannot be accessed in the usual way, and data may remain.
Erasing unallocated space requires Enhanced Secure erase/Sanitize processing.

Consideration of RAID drive

Many disks are RAID-configured in the server system. From "Green Pepper PRO", RAID-configured disks are accessed in units of logical disks, and erasing processing is also performed in units of logical disks.
If it is RAID1 (mirror), write the same value to two disks. Strictly speaking, RAID5 / 6 etc. are not cleared by the specified value for all physical disks. There is a physical disk to which the parity value is written. It is practically impossible to restore the original data from that value, but if you request strict value writing, change the setting to 1 logical disk = 1 physical disk and perform erasing processing.
Spare drives should also be considered. Spare drives are not assigned to logical disks and are not erased.

Consideration of HPA, DCO, Recovery area

A recovery area may be provided for desktops / laptops. The mechanism of the recovery area varies depending on the manufacturer, but when erasing the disk, it is necessary to consider how much the user has accessed and written to the area, whether the recovery area can be erased, etc. ..

As one method of configuring the recovery area, HPA (Host Protected Area) in the ATA (PATA, SATA) disk standard may be set. When HPA is set, the part after the set capacity of the disk becomes inaccessible from the software, and the software recognizes it as a disk with a smaller capacity than the actual capacity. Recovery information is stored in an inaccessible area (Protected Area), and recovery is performed with the HPA setting disabled.

Therefore, user data will not be written to that area unless the user changes the settings related to HPA. The normal erase process is limited to areas other than the protected area unless HPA is disabled.
* However, with secure erase/Sanitize, the HPA setting is ignored and the entire disk area is erased.

"Green Pepper PRO" has an option to disable HPA. Specify this option if you want to erase the entire disk area, including the protected area.

There is another setting on the hard disk that makes the disk capacity smaller than it actually is. A method called Device Configuration Overlay (DCO) is used to set the disk size, data transfer speed, and other settings below the original disk performance. DCOs are mainly used by PC manufacturers for limited purposes when the discs are shipped, such as by unifying the specifications of discs with different model numbers. Therefore, even if the disk capacity is set smaller than it should be by the DCO, it is unlikely that any data will be written to and left in an inaccessible area.
* Enhanced Secure Erase/Sanitize erases the entire area including the DCO. Normal secure erase does not erase the DCO settings area.

"Green Pepper PRO" provides a function to display information on whether the disk size is set small by DCO and to cancel the DCO setting. Removing the DCO also disables the HPA.

DCO is a higher level limit than HPA, and HPA is a DCO-limited internal capacity limit mechanism.
Example:
All capacity 100,0000 DCO-limited capacity 900,000

In this state, HPA is set to the internal 900,000 or less limited by DCO.
All capacity 100,0000 DCO-limited capacity 900,000 HPA-limited capacity 800,000

reference:
"Boot from CD/USB flash drive" "gph" boot
"Common options" Disable HPA, erase entire disk

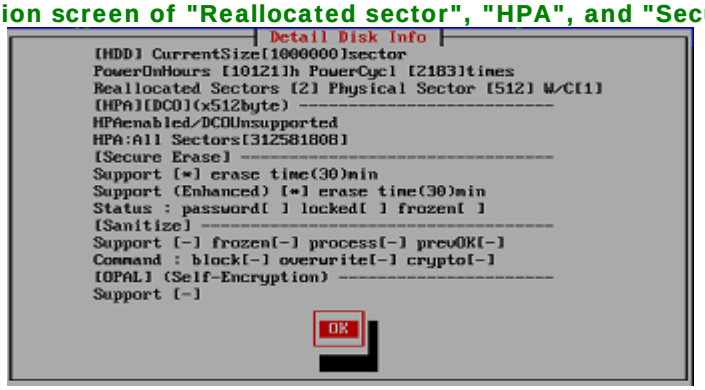
If the recovery area exists in an area that can be accessed normally (such as another partition), the entire disk including that area will be erased even with normal erasing.

Consideration of READ/WRITE error

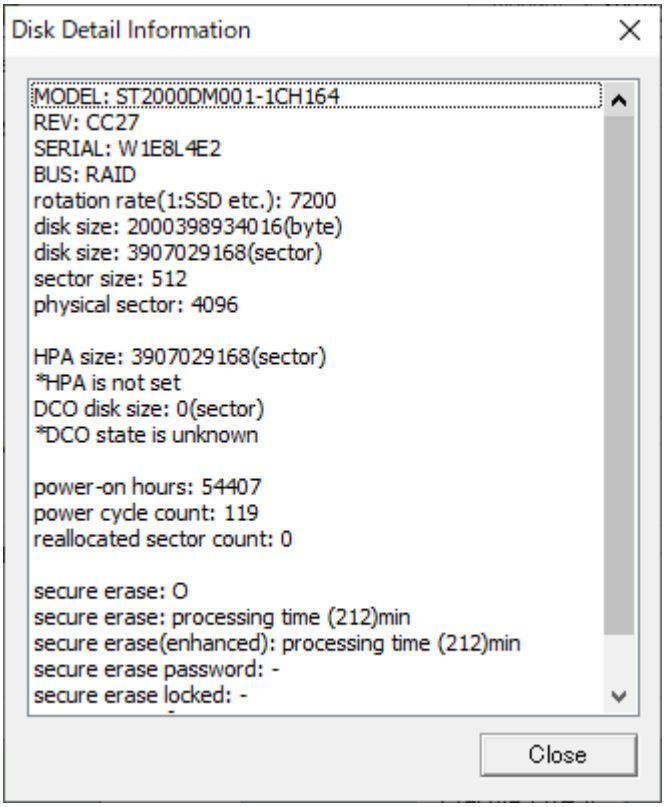
If there is a disk failure, READ and WRITE errors will occur during erasure and verification.
A WRITE error occurs when the overwrite process results in an error during erasure. The error part (sector) may not be overwritten, and data may remain in that part.
A READ error occurs when reading data during read validation and the data cannot be read. The value of that part cannot be verified, and it cannot be confirmed whether it has been erased.
If the WRITE cache is enabled, writing to a failed sector can be completed without error, but an error can occur when reading. The read verification process is also an important step for its detection.
Also, in the error part, retry processing is performed many times, so the progress of processing becomes very slow.

Depending on the number of errors and the importance of the contents of the disk, it is necessary to consider how to handle the disk with many errors. Since errors are unstable, the number of errors often changes with each process. Therefore, one method is to repeat the process many times for the disk with the error to reduce the possibility of data remaining.
Physical destruction is also an option if possible.

Confirmation screen of "Reallocated sector", "HPA", and "Secure erase" in the "Startup Erase Program"



Confirmation screen of "Reallocated sector", "HPA", and "Secure erase" in the "Windows Erase



Program"

Consideration of the number of erasures

According to the "NIST SP 800-88" standard, write once is "adequate". But, of course, it's still better to write more times. In addition, when a write error occurs, it is more desirable to write several times because the possibility of completing the write increases.
For error-free disks, a single erase is sufficient. However, if you have time to spare, we recommend that you write at least twice. Especially for the disk where the error occurs, it is necessary to write more times such as 4 times.
* "Green Pepper PRO" has a mechanism to perform detailed retries on a sector-by-sector basis in the event of an error.

Read verification is an important step in each case. The "write process" to the disk is a process that "write command is completed without returning an error" in terms of software, and it does not mean that the physical write is completed. Therefore, even if there is no error when writing, it cannot be said that it is 100% certain that it was written reliably. Read verification allows you to see the actual disk status.

In Secure erase, "Green Pepper PRO" has a menu of 2-times erases (secure erase + 00 normal write) and 3-times erases (secure erase + random + 00 normal write). The write error cannot be grasped by the Secure erase, so added normal write step. In the Enhanced Secure erase, the value to be written is not always zero, so added zero write step to make it easier to verify.
In addition, secure erase / sanitize is implemented by the manufacturer's own method, its substance is unknown, and it is a function that is not usually used often, so there is a possibility that it may be defective.
Read verification is also an important step in Secure erase.

Enhanced Secure Erase also writes to reallocated sectors that have been detached, but the second and subsequent writes do not write to detached sectors. However, detached bad sectors are "bad", it is not possible to know exactly how much they have been "erased" by the Secure erase process. In addition, when HPA (Host Protected Area) is set, HPA is ignored in Secure erase, and the entire disk is processed. But the second and subsequent writes, and verification are performed only in the restricted area, excluding HPA.

* Note) HPA (HostProtected Area)
HPA is a setting that limits the range that can be accessed by software for an disk from the beginning to a certain area.
An HPA-configured disk is perceived by the software as a small disk, only part of the capacity from the beginning, rather than the entire disk.
HPA may be set by the manufacturer as a recovery area. In that case, please note that the recovery area will also be erased by the process of disabling HPA/secure erase.

Recommended processing policy for each media

In addition to the method listed in "NIST SP 800-88" standard, we will summarize the recommended method (recommended by us).
* If many Read / Write errors occur, physical destruction may be required depending on the number of errors.

Recommended processing method for each media

Media Type	Method in "Green Pepper PRO"	Comment
Hard Disk Drive ATA(SATA)/SCSI(SAS)	*When executable [Secure Erase/Sanitize(1-time)]+Verify or [Secure Erase/Sanitize(2-times)]+Verify *Other [Erase disks(1-time)] +Verify	If there is no Reallocated Sectors count, There is no problem with "[Erase disks(1-time)]" + verify. "[Secure erase / sanitize (2-times)]" is also an option for detecting write errors. Verification processing should always be performed to verify error sectors.
SSD ATA(SATA),NVMe,eMMC	*When executable [Secure Erase/Sanitize(1-time)]+Verify or [Secure Erase/Sanitize(2-times)]+Verify *Other [Erase disks(4-times)] +Verify	In SSD, there are many unallocated areas, and "Secure Erase / Sanitize" is recommended. "[Secure erase / sanitize (2-times)]" is also an option for detecting write errors. If it is not feasible, erase as many unallocated areas as possible by increasing the number of erases. Verification processing should always be performed to verify error sectors.
USB Flash drive, ,etc., Flash memory media	[Erase disks(3-times)] +Verify or [Erase disks(4-times)] +Verify	erase as many unallocated areas as possible by increasing the number of erases. Since the capacity is relatively small compared to SSD, it is described to be "[erase disk (3-times)]", but if the capacity is large, use "[erase disk (4-times)]". Verification processing should always be performed to verify error sectors.

Boot from CD / USB flash drive

Boot

Insert the "Green Pepper Pro" product CD-ROM or the created bootable CD / USB flash drive into your computer, and turn on the power.
The system will start and the screen will look like the one below.

* To create bootable CD, see "Creating bootable "CD image" file"
* To create bootable USB flash drive, see "Setting bootable "USB flash drive""

The boot screen differs depending on the Legacy(BIOS) / UEFI boot. The processing after startup is exactly the same.

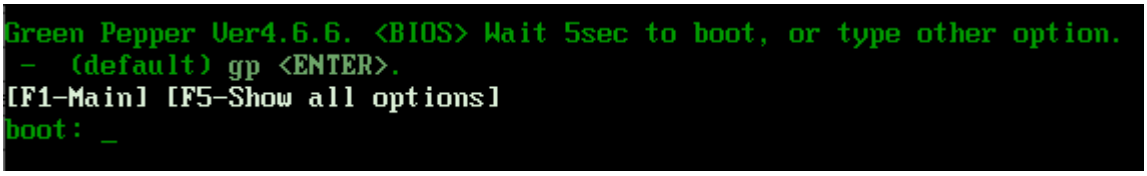
* Screen when booting in Legacy(BIOS)

* Screen when booting for UEFI (In the case of secure boot, the background image may not be displayed)

If the PC does not boot or the OS installed on the hard disk boots

· Check the Legacy(BIOS) / UEFI settings. The boot priority of the CD / USB flash drive may be low.
see "Setting the boot environment on BIOS/UEFI"
· The created CD-R may not have been created correctly for booting.
see "How to create a CD from an image file"
· The type of USB flash drive you have set may not match your PC.
see "Setting the boot environment on BIOS/UEFI""Setting bootable "USB flash drive""
· Your PC may not support booting from the CD / USB flash drive.
see "Setting the boot environment on BIOS/UEFI"
· A message will be displayed at startup, and some models will not start from a CD unless the specified key is pressed at that timing.
example: "Press any key to boot from CD..." message appear at boot time.

Operation on the boot screen - Legacy(BIOS) boot



Normally, even if you do nothing, it will automatically start the startup process after 5 seconds.
Press the [enter] key to start immediately.

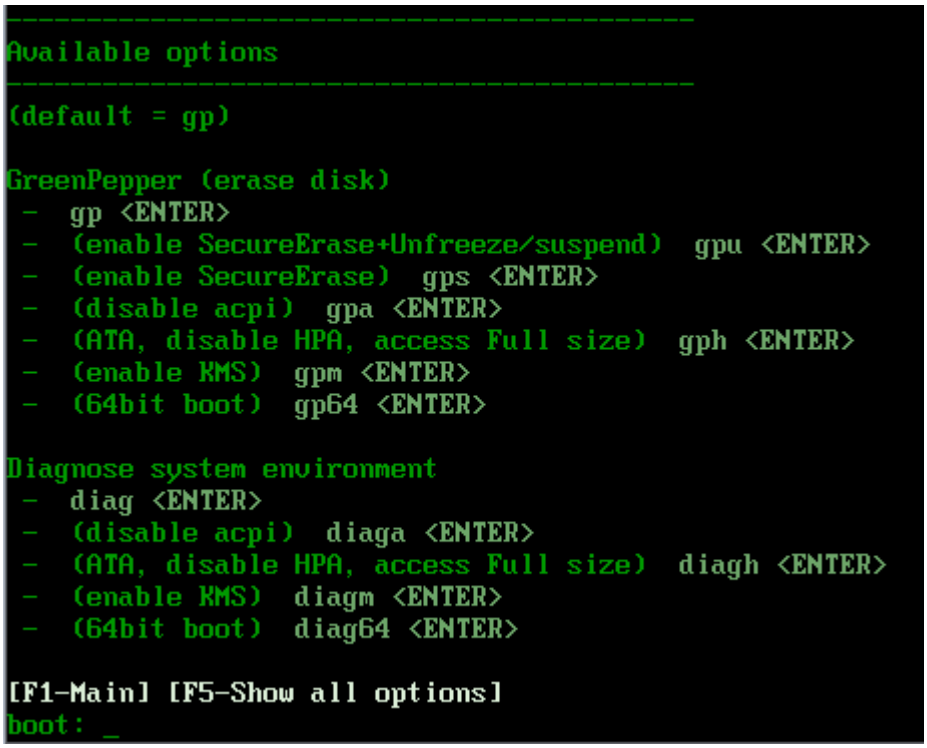
If there is a network function setting, it will be displayed as follows.
Green Pepper [NET], Wait 5sec ...
If there is a Wi-Fi network function setting, it will be displayed as follows.
Green Pepper [NETW], Wait 5sec ...

* The screen may not switch immediately after [enter], such as when media access is slow, but please wait for a while.
* If you enter one character within 5 seconds, the automatic startup will stop.

Select other option

The available options are displayed by pressing the "F5" key within 5 seconds.
* Once the screen is switched, the automatic startup will be stopped.

The following is the one when boot from the "product CD-ROM" or created bootable CD with default option.
The options that can be selected depend on the option specifications when creating a bootable CD / USB flash drive.
see "Common options"



input	contents
gp	Display normal erase screen
gpu	Display erase screen with Secure Erase menu Before the menu is displayed, suspend/resume processing is performed to unfreeze the ATA drive. *If there is no frozen ATA drive, suspend processing will not be performed. * Suspend processing may not be performed when the video driver is not supported. * If the video driver is not compatible enough, the screen may remain black and nothing will be displayed. If so, don't select tion option.
gps	Display erase screen with Secure Erase menu
gph	Disable HPA(HostProtectedArea) and erase entire disk. * Depending on the disk interface, such as when connecting to a USB interface, HPA cancellation may not be effective. see "Points to consider about erasing method"
gpa	Start with ACPI disabled

	* On a general PC, the disk may not be recognized and the power may not be turned off automatically.
gpm	Enable Kernel Mode Setting (KMS). If there is a problem with the display, please try it.
gp64	Start using 64bit kernel
diag	Diagnose: Problem investigation screen to check the status when startup is not completed or disk is not recognized.
diagh	Diagnose: Disable HPA(HostProtectedArea) and show problem investigation screen. * Depending on the disk interface, such as when connecting to a USB interface, HPA cancellation may not be effective.
diaga	Diagnose: Start problem investigation screen with ACPI disabled * On a general PC, the disk may not be recognized and the power may not be turned off automatically.
diagm	Diagnose: Enable Kernel Mode Setting (KMS). If there is a problem with the display, please try it.
diag64	Diagnose: Start problem investigation screen using 64bit kernel

If the startup is not completed

If the startup is not completed and the erase screen is not displayed, the following causes are possible.

· The hardware is not compatible with this product.
  * Not compatible CPU, motherboard, and peripheral devices.
  * Please remove peripheral devices and try again.
  * If there is a device that can be separated by the BIOS, try disconnecting it.
· Media failure (CD-ROM, USB flash drive)
· Other hardware failures

Please try starting with "gpa" (disable ACPI) etc. from the above selection menu at startup.

Also, start with "diag" and let us know the contents of the screen at the time of stop.

If the startup stops halfway and the menu is not displayed, there is no function to get the screen.
Please take a picture of the screen with a digital camera and send it to us.

For the operation of the screen displayed by the "diag" option, see "Using diagnose screen".

Operation on the boot screen - UEFI boot

"Green Pepper PRO" supports Secure Boot of many PCs, but if the Secure Boot specification of your PC is not supported , the following boot screen will not be displayed and a message such as a Security error will be displayed.
In that case, try disabling Secure Boot in the BIOS (UEFI) settings.

Normally, even if you do nothing, it will automatically start the startup process after 5 seconds.

[ESC]key for menu .....
4

If you want to start with other options, press the [ESC] key before the 5-second countdown ends.
The following option menu screen is displayed.

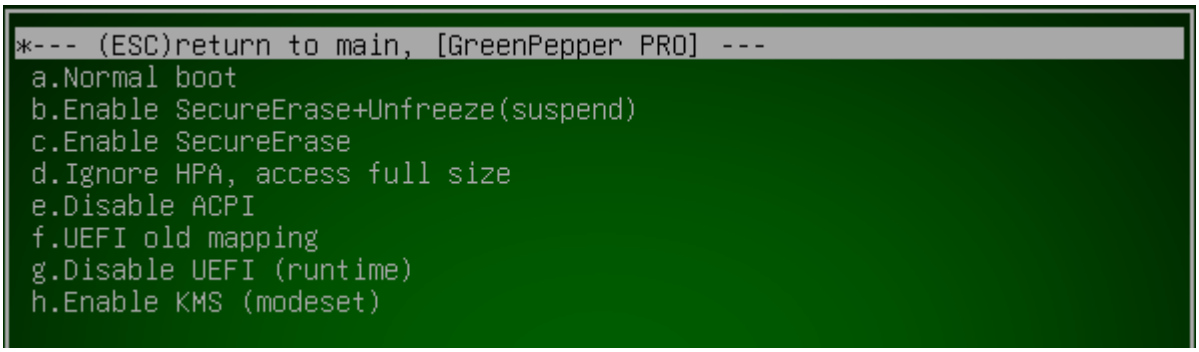
If the "[ESC]key for menu" screen is not displayed and "loading system..." is displayed

·If you do not need to select any other options at startup, the program will run until the menu is displayed, so please use it as is.
· If you need to select an option at startup, press and hold the [Esc] key immediately after the PC starts booting.
A boot option selection menu will be displayed.

Operation on the option menu screen

Use the "Down" and "Up" keys to select a function, and the [enter] key to execute the option menu.
Under "---- Other boot options", a submenu will be displayed that allows you to select more detailed options.

1. Under the "[GreenPepper PRO] English ver4.xx" menu, when "--- Other boot options" is selected.



From this screen, press the [ESC] key to return to the first option menu screen.

Menu Structure

In the standard state, the menu structure is as follows.

The following is the one when boot from the product CD-ROM.
The options that can be selected depend on the option specifications when creating a bootable CD / USB flash drive.
See "Common options"

Option menu structure

selection menu	contents
[GreenPepper PRO] Ver 4.x.x	Display normal erase screen
--- Other boot options	Boot option submenu
Diagnose	Diagnose: Problem investigation screen to check the status when startup is not completed or disk is not recognized.

Boot option submenu

selection menu	contents
*--- (ESC)return to main, [GreenPepper PRO]	* press the [ESC] key to return to the first option menu screen.
a.Normal boot	Display normal erase screen
b.Enable SecureErase+Unfreeze(suspend)	Display erase screen with Secure Erase menu Before the menu is displayed, suspend/resume processing is performed to unfreeze the ATA drive. *If there is no frozen ATA drive, suspend processing will not be performed.

	* Suspend processing may not be performed when the video driver is not supported. * If the video driver is not compatible enough, the screen may remain black and nothing will be displayed. If so, don't select tion option.
c.Enable SecureErase	Display erase screen with Secure Erase menu
d.Ignore HPA, access full size	Disable HPA(HostProtectedArea) and erase entire disk. * Depending on the disk interface, for example, when connecting to a USB interface, HPA cancellation may not be effective. see "Points to consider about erasing method"
e.disable ACPI	Start with ACPI disabled * On a general PC, the disk may not be recognized and the power may not be turned off automatically.
f.UEFI old mapping	Set UEFI old memory mapping mode * Use it when UEFI startup stops in the middle.
g.Disable UEFI (runtime)	Disable runtime UEFI function * Use it when UEFI startup stops in the middle.
h:Enable KMS (nodeset)	Enable Kernel Mode Setting (KMS). If there is a problem with the display, please try it.

Boot option submenu (diagnose)

selection menu	contents
*--- (ESC)return to main, diagnose ---	* press the [ESC] key to return to the first option menu screen.
a.Normal boot	Diagnose: Problem investigation screen to check the status when startup is not completed or disk is not recognized.
b.Ignore HPA, access full size	Diagnose: Disable HPA(HostProtectedArea) and show problem investigation screen. * Depending on the disk interface, such as when connecting to a USB interface, HPA cancellation may not be effective.
c.disable ACPI	Diagnose: Start problem investigation screen with ACPI disabled * On a general PC, the disk may not be recognized and the power may not be turned off automatically.
d.UEFI old mapping	Diagnose: Start problem investigation screen with UEFI old memory mapping mode * Use it when UEFI startup stops in the middle.
e.Disable UEFI (runtime)	Diagnose: Start problem investigation screen with disabling runtime UEFI function * Use it when UEFI startup stops in the middle.
g:Enable KMS (nodeset)	Diagnose: Enable Kernel Mode Setting (KMS). If there is a problem with the display, please try it.

If the startup is not completed

If the startup is not completed and the erase screen is not displayed, the following causes are possible.

· The hardware is not compatible with this product.
  * Not compatible CPU, motherboard, and peripheral devices.
  * Please remove peripheral devices and try again.
  * If there is a device that can be separated by the BIOS, try disconnecting it.
· Media failure (CD-ROM, USB flash drive)
· Other hardware failures

· Unsupported Secure Boot specification
  * Try disabling Secure Boot in the BIOS (UEFI) settings.
  * If you see the "disable SecureBoot if stops here" message on the screen and it stops, try disabling Secure Boot.

Please try starting with "disable ACPI","UEFI old mappong", etc. from the above selection menu at startup.

Also, start with "diagnose" menu and let us know the contents of the screen at the time of stop.

If the startup stops halfway and the menu is not displayed, there is no function to get the screen.
Please take a picture of the screen with a digital camera and send it to us.

For the operation of the screen displayed by the "diag" option, see "Using diagnose screen".

Boot from Hard disk drive

Boot

In order to start the "Boot up Erase program" from the hard disk drive, it is necessary to execute the "Startup environment creation tool" on the PC to be erased and install the boot environment to the hard disk drive.
For details, see "Abstract of Startup environment creation tool".

When booting is not completed / When booting is completed but the hard disk is not recognized.
Erase by booting from the CD or USB flash drive.

When the system starts, the following screen will be displayed, and the erase program will start automatically after 5 seconds without any operation. (Common to BIOS / UEFI)

If it does not boot, or if the OS installed on the hard disk boots

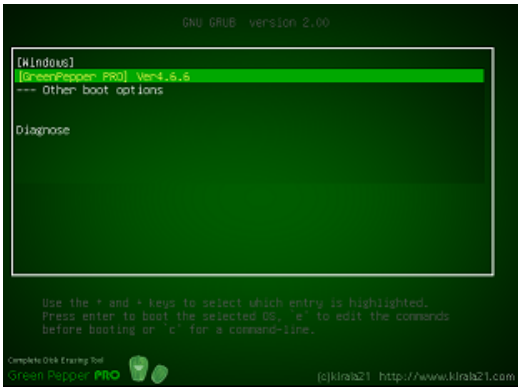
· Please remove the CD, USB memory, etc. and try again.
· The hard disk boot environment may not be set correctly or may not be supported.
In that case, boot from the CD / USB flash drive and erase it.

When Windows starts in a UEFI environment
For security reasons, some PCs disable programs to change the boot order and force Windows to always start up first. In that case, display the PC's boot device selection menu (displayed by pressing F9, F12, etc. at startup, depending on the model) and select "GreenPepper PRO, Disk ERASE" from there. If you cannot select it, e+rase by booting from the CD or USB flash drive.

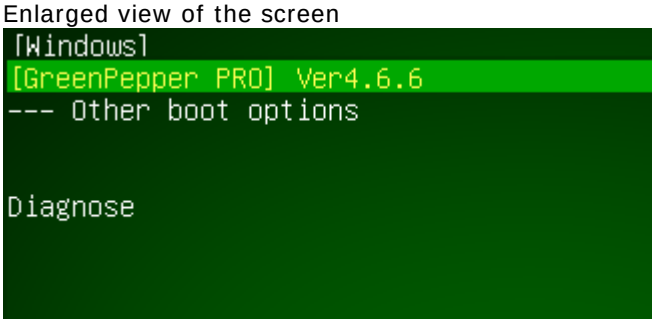
Operation on the boot screen

[ESC]key for menu .....
4

If you want to start with other options, press the [ESC] key before the 5-second countdown ends.
The following option menu screen is displayed.



Enlarged view of the screen



To boot Windows on your hard disk

If you want to restore the boot environment without erasing, use the up and down arrow keys to select [Windows] and press [enter]. After starting Windows, you can restore the boot environment by executing the "Startup Environment Creation Tool".
See "Operation of HDD boot"

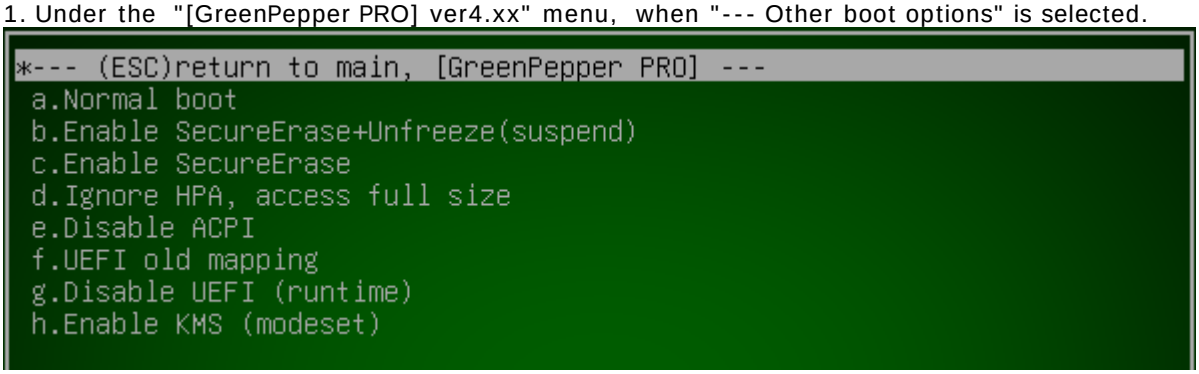
When starting erasing process after displaying the menu

Select "[GreenPepper PRO] English Ver4.x.x", press [enter].

Operation on the option menu screen

Use the "Down" and "Up" keys to select a function, and the [enter] key to execute the option menu.
Under "---- Other boot options", a submenu will be displayed that allows you to select more detailed options.

1. Under the "[GreenPepper PRO] ver4.xx" menu, when "--- Other boot options" is selected.



From this screen, press the [ESC] key to return to the first option menu screen.

Menu Structure

In the standard state, the menu structure is as follows.

The options that can be selected depend on the option specifications when configuring HDD boot environment.
See "Common options"

Option menu structure

selection menu	contents
[Windows]	Boot Windows installed on Hard disk drive. To restore the boot environment without erasing, select [Windows] and execute the "Startup Environment Creation Tool".
[GreenPepper PRO] English Ver 4.x.x	Display normal erase screen
--- Other boot options	Boot option submenu
	Diagnose: Problem investigation screen to check

Diagnose	the status when startup is not completed or disk is not recognized.

Boot option submenu

selection menu	contents
*--- (ESC)return to main, [GreenPepper PRO] English	* press the [ESC] key to return to the first option menu screen.
a.Normal boot	Display normal erase screen
b.Enable SecureErase	Display erase screen with Secure Erase menu
c.Ignore HPA, access full size	Disable HPA(HostProtectedArea) and erase entire disk. * Depending on the disk interface, for example, when connecting to a USB interface, HPA cancellation may not be effective. see "Points to consider about erasing method"
d.disable ACPI	Start with ACPI disabled * On a general PC, the disk may not be recognized and the power may not be turned off automatically.
<UEFI boot only> e.UEFI old mapping	Set UEFI old memory mapping mode * Use it when UEFI startup stops in the middle.
<UEFI boot only> f.Disable UEFI (runtime)	Disable runtime UEFI function * Use it when UEFI startup stops in the middle.
g.Enable KMS (nodeset)	Enable Kernel Mode Setting (KMS). If there is a problem with the display, please try it.

*When boot from HDD, "Enable SecureErase+Unfreeze" is not supported, use CD/USB flash drive boot.

Boot option submenu (diagnose)

selection menu	contents
*--- (ESC)return to main, diagnose ---	* press the [ESC] key to return to the first option menu screen.
a.Normal boot	Diagnose: Problem investigation screen to check the status when startup is not completed or disk is not recognized.
b.Ignore HPA, access full size	Diagnose: Disable HPA(HostProtectedArea) and show problem investigation screen. * Depending on the disk interface, for example, when connecting to a USB interface, HPA cancellation may not be effective.
c.disable ACPI	Diagnose: Start problem investigation screen with ACPI disabled * On a general PC, the disk may not be recognized and the power may not be turned off automatically.
<UEFI boot only> e.UEFI old mapping	Diagnose: Start problem investigation screen with UEFI old memory mapping mode * Use it when UEFI startup stops in the middle.
<UEFI boot only> f.Disable UEFI (runtime)	Diagnose: Start problem investigation screen with disabling runtime UEFI function * Use it when UEFI startup stops in the middle.
g:Enable KMS (nodeset)	Diagnose: Enable Kernel Mode Setting (KMS). If there is a problem with the display, please try it.

If the startup is not completed

If the startup is not completed and the erase screen is not displayed, the following causes are possible.

· The hardware is not compatible with this product.
  * Not compatible CPU, motherboard, and peripheral devices.
  * Please remove peripheral devices and try again.
  * If there is a device that can be separated by the BIOS, try disconnecting it.
· HDD drive failures
· Other hardware failures

· Unsupported Secure Boot specification
  * Try disabling Secure Boot in the BIOS (UEFI) settings.
  * If you see the "disable SecureBoot if stops here" message on the screen and it stops, try disabling Secure Boot.

Please try starting with "disable ACPI","UEFI old mappong", etc. from the above selection menu at startup.

Also, start with "diagnose" menu and let us know the contents of the screen at the time of stop.

If the startup stops halfway and the menu is not displayed, there is no function to get the screen.
Please take a picture of the screen with a digital camera and send it to us.

For the operation of the screen displayed by the "diag" option, see "Using diagnose screen"

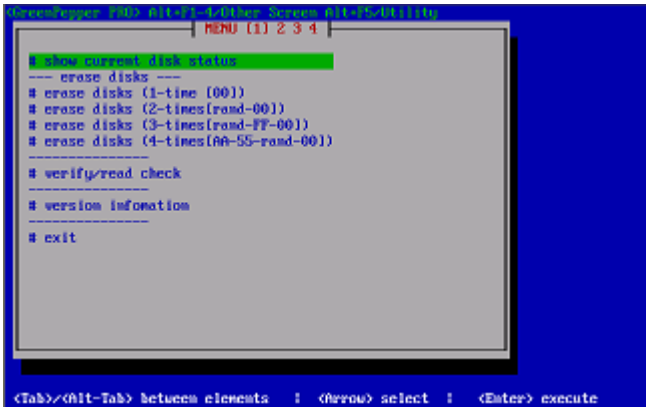
Basic operation of "Bootup Erase program"

Menu screen

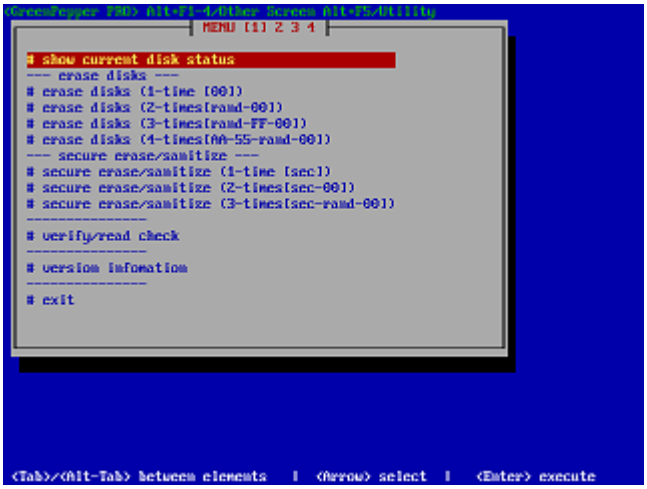
If you start the "Bootup Erase program" from the bootable CD, USB flash drive, or hard disk, the following menu will be displayed.

* Depending on the settings, the password input screen will be displayed before the menu is displayed.
* You can change the menu contents, such as limiting them to specific ones, by setting.
See "Common options"

Normal menu screen



When a disk capable of Secure erase / Sanitize processing is connected,
the selection menu of "---- Secure erase / Sanitize ---" is automatically displayed as shown below.



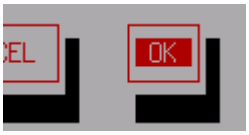
Key operation

Move choices: Arrow keys
Move between input items: [tab] / [alt] + [tab] keys
Select / execute choice: [enter] key
Check / uncheck check items: [space] key

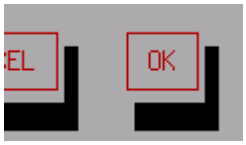
Cursor position

Check the current position of the cursor as follows.

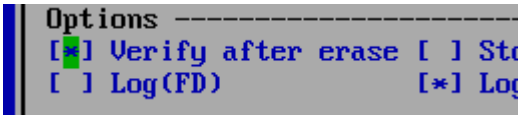
cursor is on "OK" button



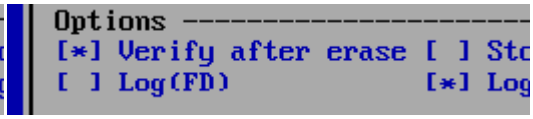
no cursor on "OK" button



cursor is on "Verify after erase"



no cursor on "Verify after erase"



Switch to another screen

There are a total of 5 separate screens, including the screen you are currently viewing, and you can perform different processes in parallel. By erasing multiple disks in parallel, the overall processing time can be shortened.

Use the ALT + F1, ALT + F2, ALT + F3, ALT + F4, and ALT + F5 keys to switch screens.

* Multiple erases and check processes (such as checking on a separate screen while erasing) cannot be performed on the same disk.

Outline of menu contents

* Menu contents can be customized in various ways, and the contents vary depending on the setting status.
* For customizing the menu screen, refer to "Common options"

show current disk status
A list of disks currently connected (recognized) to the system is displayed.
You can also get detailed information about the disk, PC, and disk interface.

erase disks (1-time [00])
erase disks (2-times[rand-00])
erase disks (3-times[rand-FF-00])
erase disks (4-times[AA-55-rand-00])
This process erases the contents of the specified disk.
Select the required number of erases and perform the erase.

secure erase/sanitize (1-time [sec])
secure erase/sanitize (2-times[sec-00])
secure erase/sanitize (3-times[sec-rand-00])
This is the process of performing Secure Erase / Sanitize on the specified disk.
Except for the [sec] step, the procedure is the same as for normal erasing.
When a compatible disk is not connected, "*** NO supported disk ***" is displayed and the menu cannot be selected.

* When booting from the product CD-ROM, the "Secure Erase / Sanitize" menu is displayed only when a disk that can be execute secure erase / sanitize is connected.

Conditions for displaying the "Secure Erase / Sanitize" menu
·There is a disk that supports Secure Erase and is not "Frozen" state.
·There is a disk that supports Sanitize.

If you want to force the display "Secure erase/Sanitize" menu, please boot with secure boot option.
* "gps" for BIOS boot, "Enable Secure Erase" for UEFI boot. See "Boot from CD / USB flash drive".

It is possible to switch between display / non-display and automatic display by setting in "Common options".

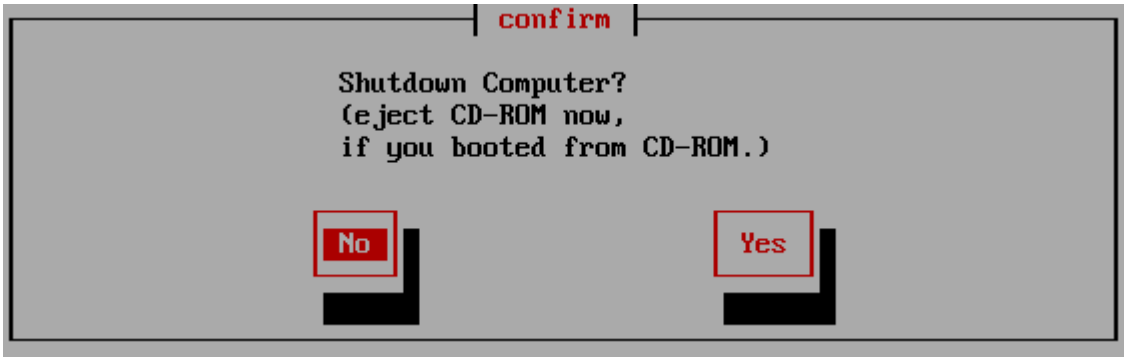
verify/read check
Checks if the disk has been erased and checks for read errors in the entire disk.

version information
Display version information.

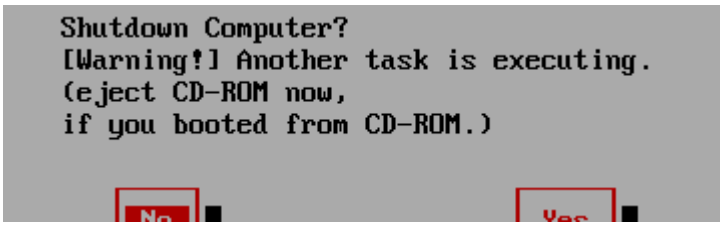
exit
Shut down the system and turn off the power.

System shutdown.

Select "Exit" from the menu and press [enter].
On the screen below, select [Yes] and press [enter].



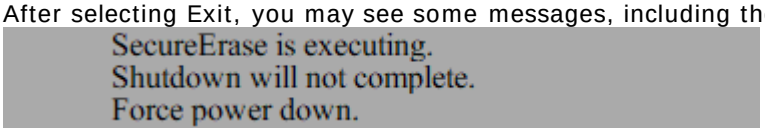
Many PCs will turn off automatically after this.
Therefore, if you are booting from the CD-ROM, it is convenient to remove the CD at this timing.

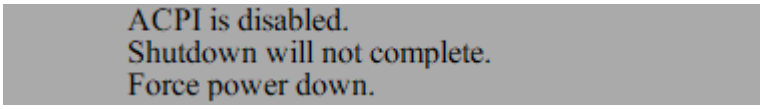


If this message is displayed, some processing is being performed on another screen (switched with ALT + F1, ALT + F2, ALT + F3, ALT + F4).
Please switch screens to check. It is also possible to forcibly terminate as it is.

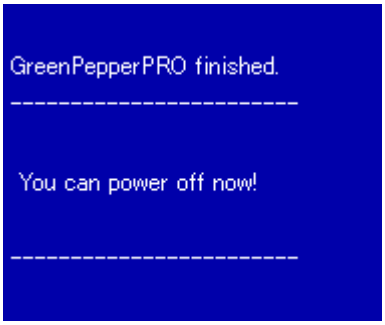
If the power does not turn off automatically

After selecting Exit, you may see some messages, including the following:



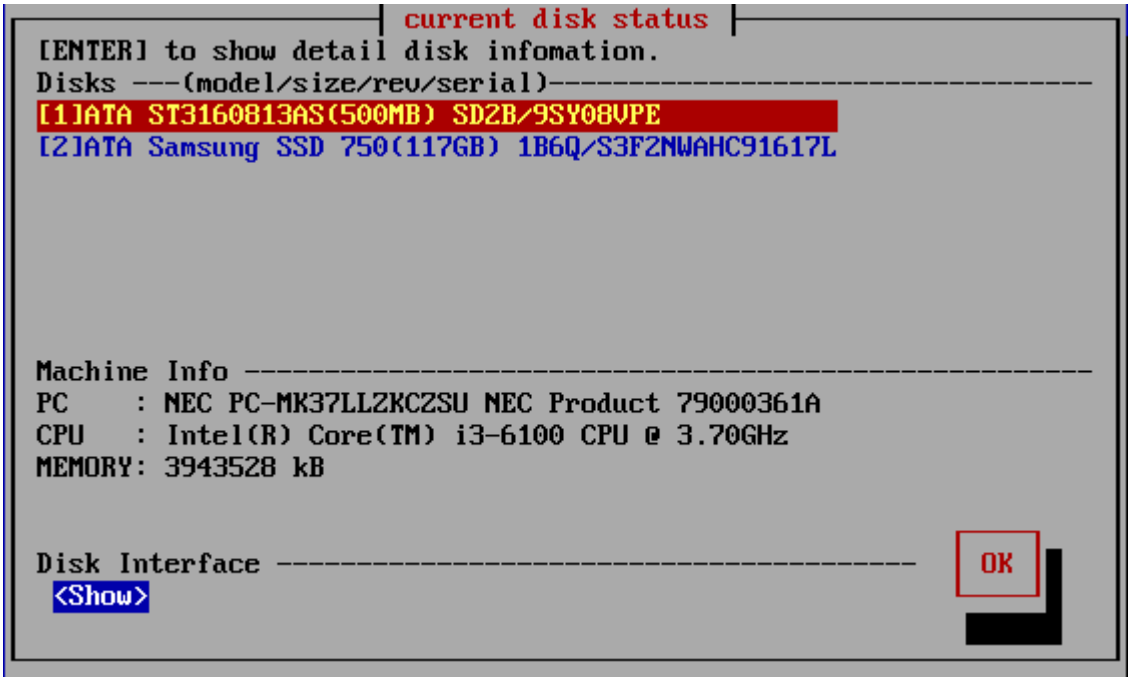


In such a case, or if the power does not turn off automatically, etc.,
after the following screen is displayed, press the power button (may be a long press) to turn off the power.



Show current disk status

If you select "Show current disk status", the following screen will be displayed.



List of connected disks

The model number, capacity, firmware revision, and disk serial number of the disk recognized by the "Green Pepper PRO" system are listed.
* For a single disk, it is a physical disk unit, and for a RAID configuration, it is a logical disk unit.
* For RAID disk or others, revision, and serial number may not be displayed.

As shown below, if the message "NO supported disk" is displayed even though the disk is connected, the disk is not recognized.
* There may be a disk failure.

MEMO *** If the disk does not appear in the list

Check the disk hardware

· First, check that the disk is recognized on the BIOS screen of the PC.
To display the BIOS screen, see "Setting the boot environment on BIOS/UEFI".
Information about the disk is displayed in this screen.
· If Windows works, make sure that Windows recognizes the disk.

Check if it is supported by "Green Pepper PRO"

· If the interface is not supported by "Green Pepper PRO", the disk will not be displayed.
· Please let us know the contents of "Disk Interface" displayed in "Show current disk status"

* You can save the screen image to the FD / USB flash drive /Net share with "Utility" / "Save screenshot (FD / USBmem/Net)" displayed by ALT + F5.
Or
* Use "Write hardware information to FD / USBmem / Net" in "Utility" displayed by ALT + F5, save the PC information to USB flash drive / FD, and send the file (HWINFO.TXT) to us.

MEMO

The beginning of the line is
[1] (parentheses) are ATA (IDE, SATA) disks.
<3> (parentheses) are SAS / SCSI / RAID connections.

! 1 xxxxxxxx
Those with "!" Displayed are IDE disk interfaces that do not support high-speed mode (DMA) in the hardware / driver.
The access is low-speed mode (PIO mode), and the processing speed is very slow.

MEMO - about eMMC drive

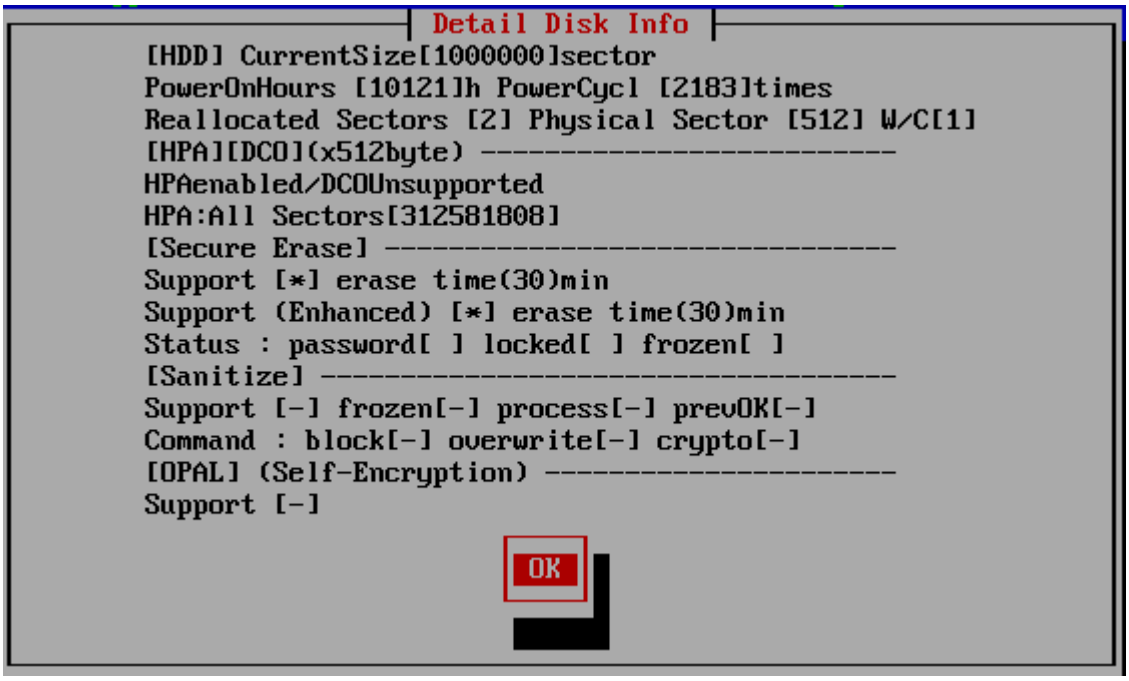
On eMMC drives, you will often see multiple drives as shown below.

This is because one eMMC drive is divided into multiple drives.
Among them, (boot0) (boot1) is the boot partition. (rpmb) is a security partition called "Replay Protected Memory Block". Both are normally not writable and cannot be erased.

Detailed information of the disk

Select the disk using the [up] and [down] keys in the list, and press [enter].
Detailed information about the disk is displayed as shown below.

Display for ATA (IDE, SATA), SCSI, SAS, etc.



* The following information is available only if it can be obtained. The correct value will not be displayed on disks and interfaces that do not support data acquisition.

HDD/SSD,Flash

For hard disks, "[HDD]" is displayed, and for Flash drive/ SSDs, etc., "[SSD, Flash]" is displayed.
If it is not sure, "[HDD/SSD]" will be displayed.

Current Size

The currently accessible disk size is displayed in terms of the number of sectors.
This number of sectors x 512 bytes (logical sector size) is the disk capacity (bytes).

PowerOnHours, PowerCycl

Shows how long the disk has been used and how many times it has been turned on.

Reallocated Sectors

Displays the number of sectors that have been detached and reallocated.
1 sector = 512 bytes. The area of detached sector x 512 bytes is inaccessible.

This number is used to indicate how damaged the disk is and to determine the need for "Secure erase/Sanitize".
See "About Secure Erase/Sanitize","Points to consider about erasing method".

Physical Sector
Shows the physical sector size of the disk. Usually 512 or 4096.

W/C
Shows the status of Write Cache. [1]:ON, [0]:OFF. [-]not supported or undefined.
* Supports ATA(SATA,IDE) drives or SCSI (SAS) drives connected by compatible interfaces which does not have RAID function.

HPA/DCO/AMA(x512byte)
HPA, DCO and AMA is a standard for ATA disks that allows access only to the limited area.
Displays the disk size limitation status by HPA (Host Protected Area), DCO (Device Configuration Overlay) and AMA(Accesible Max Address).
See "Points to consider about erasing method".

HPA disabled	HPA is not set.
HPA enabled HPA:All Sectors[xxxx]	HPA is set. The total disk capacity is [xxxx] x512 bytes. * Currently accessible area is the above "Current size".
HPA Unknown: error to get size	Cannot get the correct HPA information.
HPA Unsupported	A disk that does not support HPA.

* The DCO setting is a higher level limit than HPA, and the HPA is set internally when the DCO is set.

DCO disabled	DCO is not set.
DCO enabled DCO:All Sectors[xxxx]	DCO is set. The total disk capacity is [xxxx] x512 bytes. * Currently accessible area is the above "Current size".
DCO Unknown: error to get size	Cannot get the correct DCO information.
DCO Unsupported	A disk that does not support DCO.

AMA disabled	AMA is not set.
AMA enabled AMA :All Sectors[xxxx]	AMA is set. The total disk capacity is [xxxx] x512 bytes. * Currently accessible area is the above "Current size".
AMA Unknown: error to get size	Cannot get the correct AMA information.
AMA Unsupported	A disk that does not support AMA.

* The total capacity displayed in the DCO/AMA/HPA settings is the total physical capacity of the disk.

Unallocated/Other memory area
For NVMe drives, displays information about unallocated NameSpace and other internal memory (rpmb, cmb, pmr, etc.).

Secure Erase
Support status of Secure Erase.
See "About Secure Erase/Sanitize"

Support	When (*) is displayed, the disk supports Secure erase.
erase time	The time required for the erasing process(Secure erase).
Support (Enhanced)	When (*) is displayed, the disk supports Enhanced-Secure erase.
erase time	The time required for the erasing process (enhanced-Secure erase).
Status: password	A secure erase password (HDD password) is set on the disk.
Status: locked	A secure erase password (HDD password) is set on the disk, and locked.
Status: frozen	Disk is Frozen for Secure erase.

Sanitize
Support status of Sanitize.
See "About Secure Erase/Sanitize"

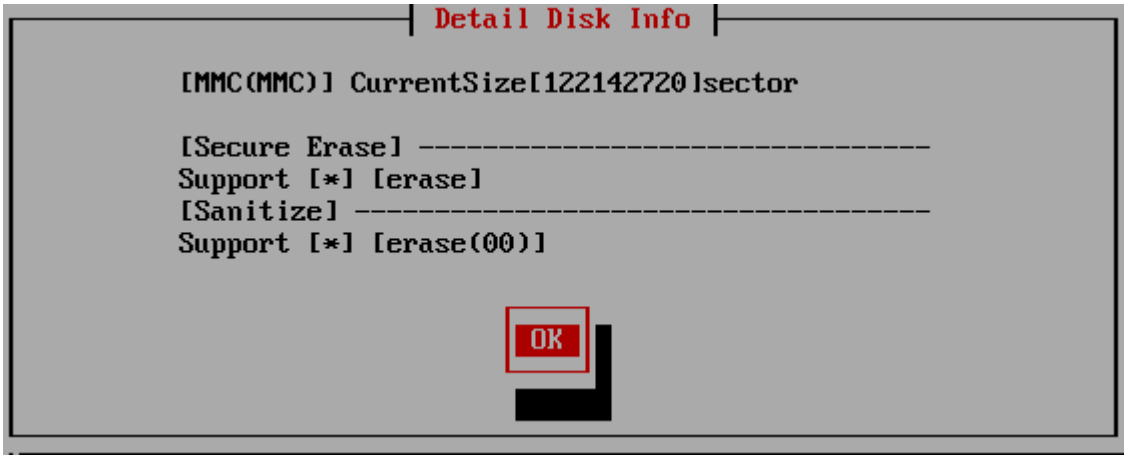
Support	When (*) is displayed, the disk supports Sanitize.
frozen	When (*) is displayed, The Sanitize process has been frozen and cannot be processed.
process	If you see a number, it indicates that Sanitize is currently in progress. After the Sanitize process starts, even if the power is turned off, the process will continue the next time the power is turned on. You cannot read or write to the disk during processing. Please wait with the power on until the end.
prevOK	If the previous Sanitize process is completed without any error, [OK] is displayed. If the disk does not support that feature, nothing will be displayed.
Command: block	Of the Sanitize processing, if the [block erase] command is supported, it will be (*).
Command: over write	Of the Sanitize processing, if the [over write] command is supported, it will be (*).
Command:	Of the Sanitize processing, if the [crypto scramble] command is supported, it will be (*).

crypto	

OPAL (self-encryption)
Support status of OPAL (disk self-encryption function).

Support	When (*) is displayed. the disk supports OPAL. The following is displayed only if it is supported.
Ver	Shows the OPAL version.
mode	Displays the current mode (ATA · NVMe / OPAL).
lock	If locked (OPAL mode) (*) is displayed.

Display for MMC(eMMC,SD)



[MMC(MMC)]
[MMC (MMC)] is displayed for MMC drive, [MMC (SD)] is displayed for SD card drive, etc.

CurrentSize
The currently accessible disk size is displayed in terms of the number of sectors.
This number of sectors x 512 bytes (logical sector size) is the disk capacity (bytes).

SecureErase
When (*) is displayed, the disk supports Secure erase.
The following is the erasing method performed by the drive.

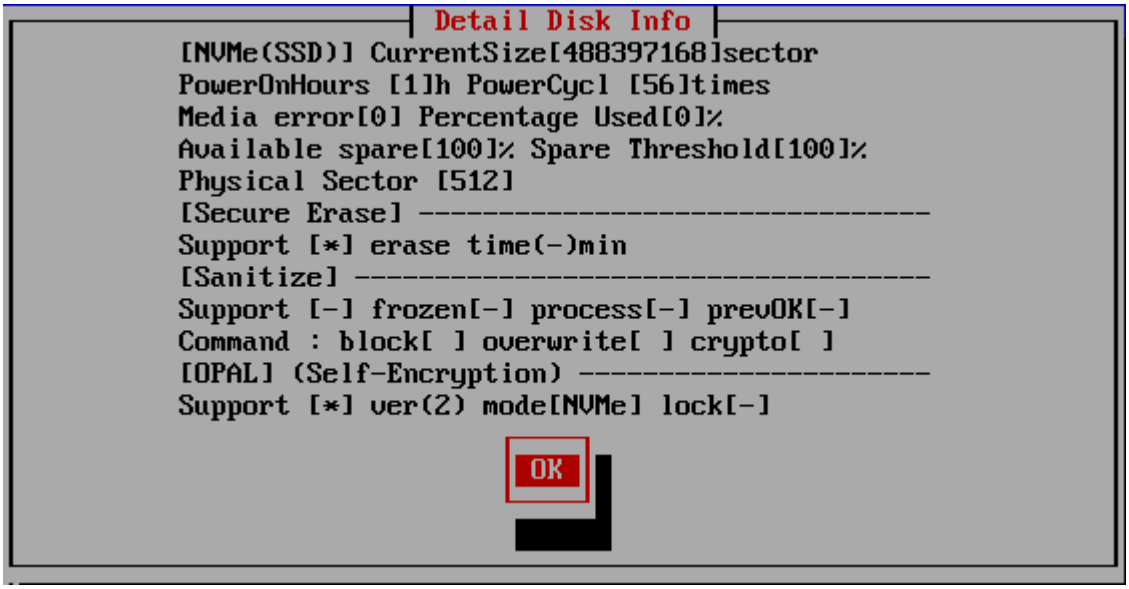
[erase]:The process of erasing the whole
[easer-ch]:After writing a specific value to the whole, perform the erase process.
[ch-comp-rand]: After writing a specific value to the whole, its complement and finally a random number are written
[vend]:Drive maker specific method.

Sanitize
When (*) is displayed, the disk supports Sanitize.
In the Sanitize process, the entire allocated memory is first erased, and then the unallocated area is erased.

The following is the erasing method performed by the drive.

[erase(00)] The whole is cleared with 0
[erase(01)] The whole is cleared with 1

Display for NVMe



[NVMe(SSD)]
[NVMe (SSD)] is displayed for NVMe drive

Current Size
The currently accessible disk size is displayed in terms of the number of sectors.
This number of sectors x 512 bytes (logical sector size) is the disk capacity (bytes).

PowerOnHours, PowerCycl
Shows how long the disk has been used and how many times it has been turned on.

Media Error (Media and Data Integrity Errors)
The number of occurrences where the controller detected an unrecovered data integrity error.

Percentage Used
Contains a vendor specific estimate of the percentage of NVMe subsystem life used based on the actual usage and the manufacturer's prediction of NVMe life.

Available Spare
Contains a normalized percentage (0 to 100%) of the remaining spare capacity available.

Available Spare Threshold
When the Available Spare falls below the threshold indicated in this field, an asynchronous event completion may occur.

Physical Sector
Shows the physical sector size of the disk. Usually 512 or 4096.

Secure Erase
Support status of Secure Erase.
See "Display for ATA" above.
See "About Secure Erase/Sanitize"

Sanitize
Support status of Sanitize.
See "Display for ATA" above.
See "About Secure Erase/Sanitize"

OPAL (self-encryption)
Support status of OPAL (disk self-encryption function).
See "Display for ATA" above.

Machine Info

Information about the PC, CPU, and memory of your machine is displayed.

Disk Interface

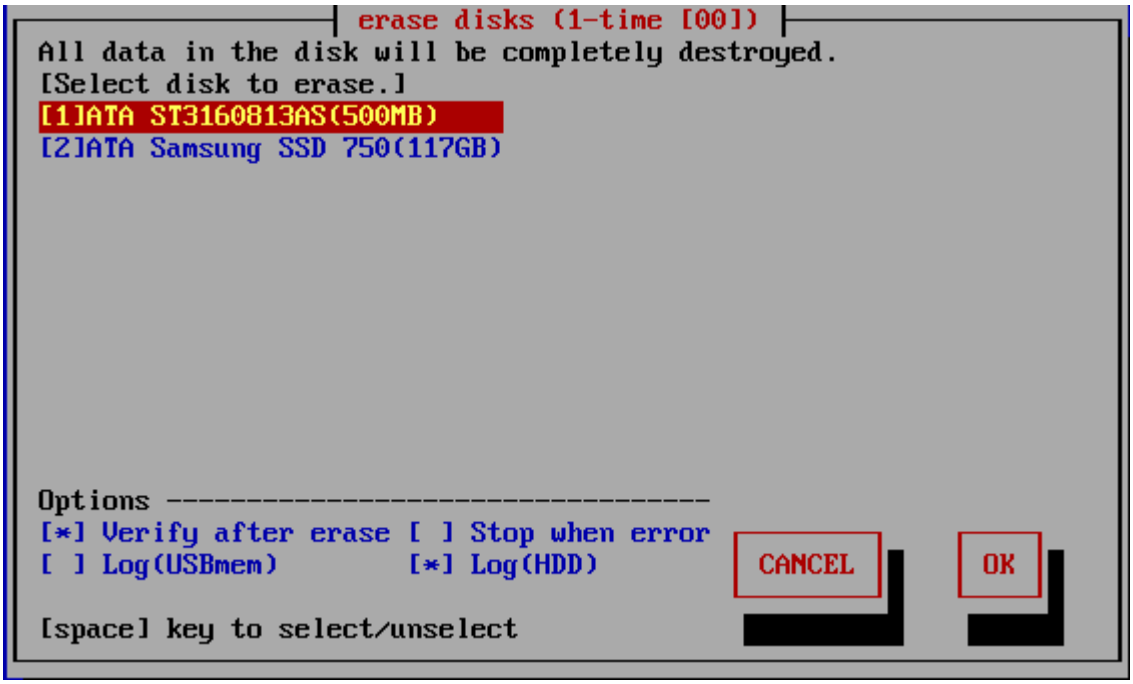
Move the cursor to "" and press [enter] to display a list of disk interfaces installed in the PC. If you don't see the disk that should be connected, this is one piece of information you should provide to resolve the issue. If there is an interface that is not supported, "unsupported" will be displayed instead of "OK" as shown below.

Exit

After checking the contents, press the [tab] key to move the cursor to [OK], and press the [enter] key to exit.

Erase disk drives (1time - 4times)

If you select "Erase disks"(1time-4times), the following screen will be displayed.



List of connected disks

The model number, capacity, firmware revision, and disk serial number of the disk recognized by the "Green Pepper PRO" system are listed.
* For a single disk, it is a physical disk unit, and for a RAID configuration, it is a logical disk unit.
* For RAID disk or others, revision, and serial number may not be displayed.

As shown below, if the message "NO supported disk" is displayed even though the disk is connected, the disk is not recognized.
* There may be a disk failure.

MEMO *** If the disk does not appear in the list

Check the disk hardware

· First, check that the disk is recognized on the BIOS screen of the PC.
To display the BIOS screen, see "Setting the boot environment on BIOS/UEFI".
Information about the disk is displayed in this screen.
· If Windows works, make sure that Windows recognizes the disk.

Check if it is supported by "Green Pepper PRO"

· If the interface is not supported by "Green Pepper PRO", the disk will not be displayed.
· Please let us know the contents of "Disk Interface" displayed in "Show current disk status"

* You can save the screen image to the FD / USB flash drive /Net share with "Utility" / "Save screenshot (FD / USBmem/Net)" displayed by ALT + F5.
Or
* Use "Write hardware information to FD / USBmem / Net" in "Utility"

displayed by ALT + F5, save the PC information to USB flash drive / FD, and send the file (HWINFO.TXT) to us.

MEMO

The beginning of the line is
[1] (parentheses) are ATA (IDE, SATA) disks.
<3> (parentheses) are SAS / SCSI / RAID connections.

! 1 xxxxxxxx
Those with "!" Displayed are IDE disk interfaces that do not support high-speed mode (DMA) in the hardware / driver.
The access is low-speed mode (PIO mode), and the processing speed is very slow.

MEMO - about eMMC drive

On eMMC drives, you will often see multiple drives as shown below.

This is because one eMMC drive is divided into multiple drives.
Among them, (boot0) (boot1) is the boot partition. (rpmb) is a security partition called "Replay Protected Memory Block". Both are normally not writable and cannot be erased.

Select the disk using the [up] and [down] keys in the list, and press [enter].

* Multiple processes cannot be performed on the same disk on different screens.

Setting "Options"

When "Specify erase method", "Auto erase with password", "Full-auto erase" is selected, the specified value is displayed and cannot be changed.
See "Common Options".

* You can change the selection / deselection by pressing the [space] key while the cursor is on it. [ ]

[ ] Verify after erase

After the erasing process is completed, read the whole disk and verify that all sectors have been erased. The processing time required for verification is about the same as the erasing process.
The state of [*] is the selection to "verify".

[ ] Stop when error

If a write error to the disk occurs in the middle, you can choose to interrupt the process or ignore it and continue.
If you ignore it and continue, the number of errors is counted.
The [*] state is the selection to suspend.

[ ] Log(USBmem,FD)

After the erasing process is completed, write the processing log to the floppy disk / USB flash drive.
The status of the currently recognized FD and USB flash drive is displayed in parentheses.
The state of [*] is the selection of write log.

USBmem · · · USB flash drive
FD · · · Floppy disk
- · · · Writable media is not recognized. Even if you select it in this state, the log will not be written.

For FDs, there must be a 1.44M (2HD) internal / USB floppy disk drive with an MS-DOS formatted floppy disk in it.
The USB flash drive must be formatted with FAT / FAT32 / exFat.
Both must be connected and inserted when the PC starts up.
Writing is done at the end of all processing.

* If you connect a USB memory or USB-FD after booting, perform "Utility"/ "Rescan Disks/Reset Network".

About the log write destination

Search for the write destination in the following priority order.
(When booting with a USB flash drive)USB flash drive used for booting -> USB-FD-> USB flash drive ->FD
* Up to 64GB is recognized as the USB flash drive to write the log to.
* If the boot option is set to "Erase USB drives of 64G or less", the USB flash drive cannot be used as the log writing destination. Refer to "Common options" when creating a boot environment and "Erasing USB drives of 64G or less"

* If a log write error occurs because the floppy disk / USB flash drive does not exist or is not formatted and so on, an error message will be displayed at the end. Even in that case, the disk erasing process itself is completed as usual.
*After specifying the USB flash drive as the log write destination and starting the erasure process, you can remove the USB flash drive. In that case, you can either insert it again before the erasure is complete, or insert it after the message "Can't write log to USB Memory/FD" is displayed, and select "Rerty".

[ ] Log(HDD)
After the erasing process is completed, write the processing log to the erased hard disk drive.
The state of [*] is the selection of write log.

The written log file can be referenced by the following method.
* When you start the PC from the disk on which the log file is written, the log file is displayed on the screen (only when legacy/BIOS boot).
* Displayed by "Utility"/" Read HDD log" of "Boot up erase program".
* Use Windows "Utility for administrators" / "Disk log".

* Log files and small programs for starting and displaying logs are written in the first few sectors of the disk.
* If you perform a "Verify/read check" on the disk to which the log is written, only a few sectors will be counted as non-zero.
* Only the log part can be deleted by the above log file display utility.

[ ] LogNET(WIN/FTP)
After the erasing process is completed, write the processing log to the network share.
The state of [*] is the selection of write log.

This network log selection is displayed only when the network function is built in.
For details on incorporating network functions, see "Common options "/"Network" when creating a boot environment.

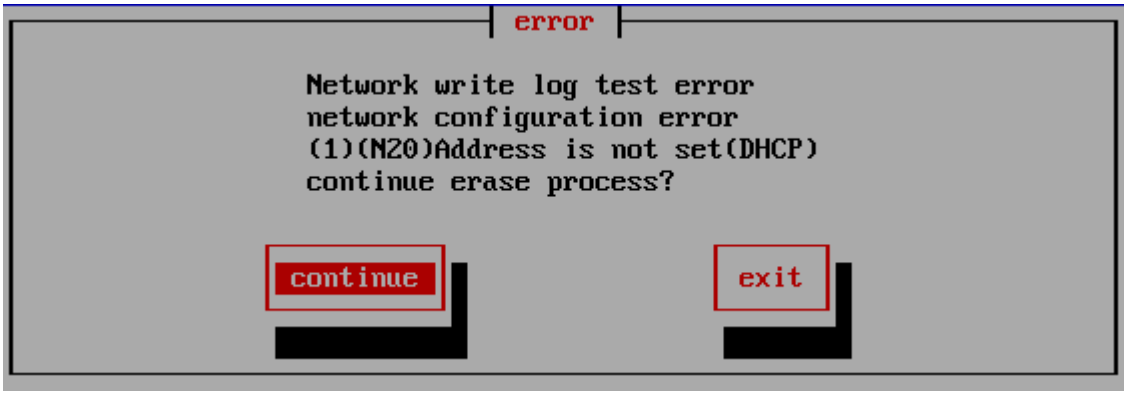
WIN· · · write log to Windows share.
FTP· · · write log to FTP server

Execute Erase

Move the cursor with the [tab] key and press [enter] with "OK" to start erasing.
Select "Cancel" to close the screen.

Confirmation in Locked/OPAL mode
If the HDD is password-locked, in OPAL mode for OPAL (self-encrypting) compatible disk, a warning will be displayed.

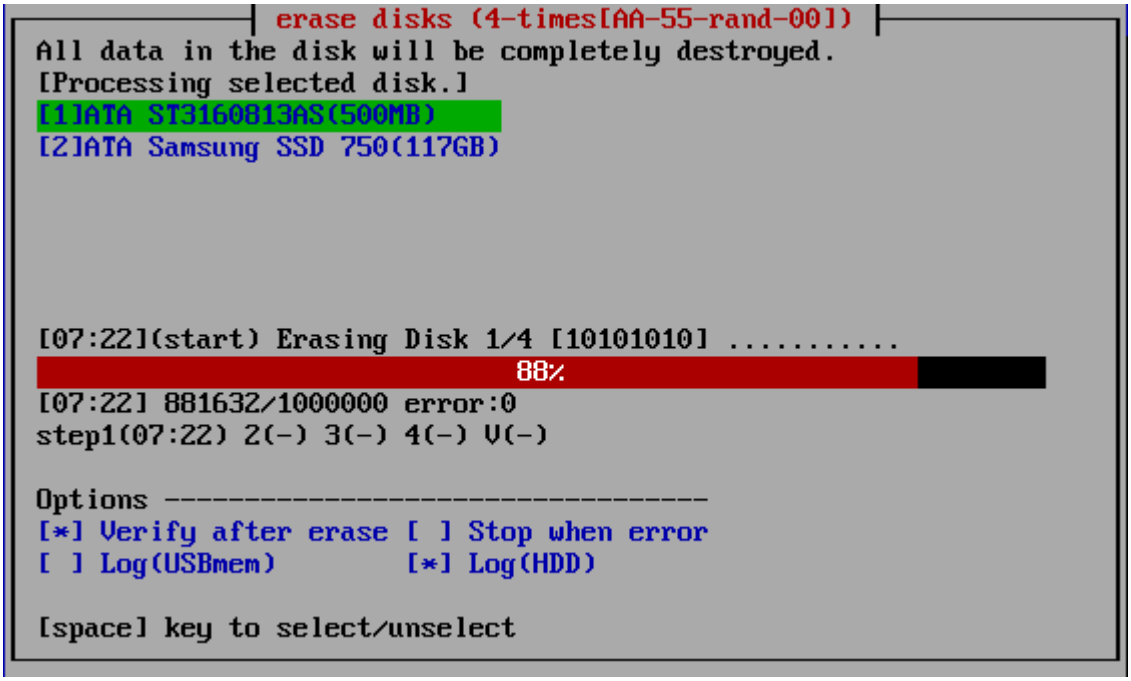
Log write test
A log write test is automatically performed just before the erase process begins.



If there is an error when writing the log, an error message will be displayed like this.
Select "Continue" to continue processing with an error, or select "End" to cancel processing.
If you continue, an error will occur when writing the log after the erase process is completed.

See "Using "Network log"/ Trouble shootings" for details and how to deal with it.

Screen during erasing process



The current processing status and the start time for each step are displayed.

[hh:nn](start) ・・・Start time of current step, content of the process
----------10%---------- ・・・Percentage of progress of the current step
[hh:mm] :xxxx/xxxxx error:xxx ・・・Current time, number of processed sectors / total number of sectors, number of error sectors. (1 sector = 512 bytes)
step1(hh:nn) 2(-) 3(-) 4(-) V(-) ・・・Start time for each step (V is the verification step)

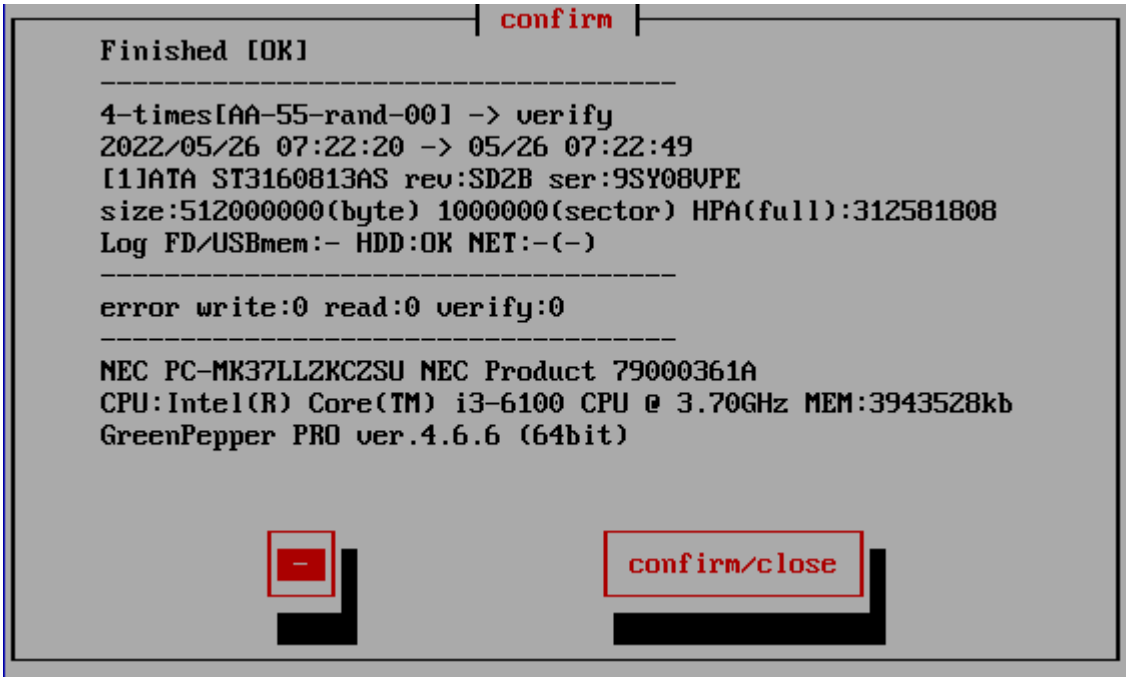
MEMO
The display of "Number of processed sectors" is updated in small units up to the first 1% to confirm the start of operation, and then updated about 1% every progress. The processing speed does not decrease on the way. If there is a write / read error, retry and do a more detailed write / read check. Therefore, it may take much longer than usual.

When interrupting processing in the middle

If you want to interrupt the process in the middle, move to another screen (ALT + F1-5) and exit the system from the menu, or execute "Interrupt the processing process" on the "Utility" screen displayed by ALT + F5.

Confirmation screen at the end of processing

When the process is completed, the following screen will be displayed.
Use the [tab] key to move the cursor to "Close" and press [enter] to close the screen.
The "-" button is to prevent accidental closing. No processing is done.



Checking the log writing result
Log FD/USBmem;- HDD:OK NET:OK(0926181439.log)
This line is the result of writing the log. "-" Indicates that writing is not specified, "OK" indicates that writing is complete, and "X" indicates that a writing error has occurred.
In the case of "NET", the written file name is displayed.

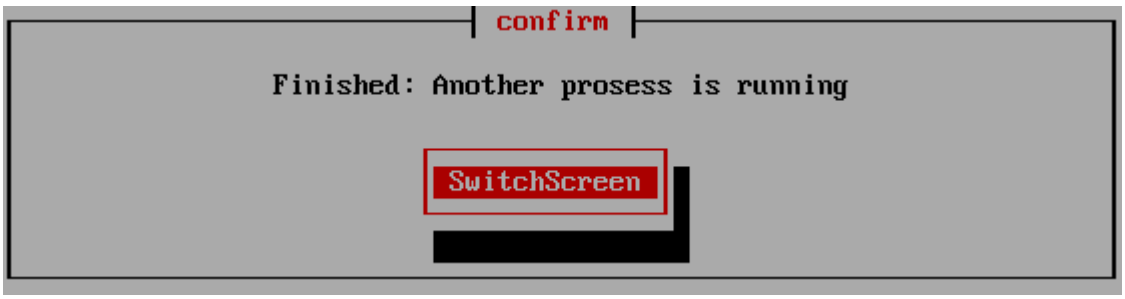
* If there is a write error
error write:1234(1:100 2:200 3:34 4:900)
The number of errors for each step is displayed along with the total number of errors.

* If there is retry processing
retry: write(1234)1:100 2:200 3:34 4:900 read(1000)
A display like this is added.

When "Auto Erase with password", "Full-auto Erase" is specified

If you select "Close" on the confirmation screen, the following screen will appear, and you can shut down immediately after selecting "Yes".

However, if processing is still being performed on another screen (displayed by ALT + F1-5), the following screen will be displayed, and "SwitchScreen" will automatically switch to the screen being processed.
This is to prevent a PC with multiple disks connected from shutting down before the other disks have been erased.



About Log file

Log file name

The log file name written to the FD / USB flash drive is determined as follows. The file name is determined including seconds, so writing to the same media in succession will not easily overwrite it.

[Date (day)] [hour] [minute] [second] .log
Example: Log created at 13:08:12 on June 5th-> 05130812.log

The name of the log file written to the network is as follows.

[Date (month/day)] [hour] [minute] [second] .log
Example: Log created at 13:08:12 on June 5th-> 0605130812.log

However, if "Log file name prefix" is specified in "Common options"/"Network" when creating boot environment, another character string is added at the beginning.

When writing to network share, the existence of the file name is checked, and if the same file name already exists,
ex. 0605130812_1.log
A branch number is added after the file name to prevent the file from being overwritten.

Log file sample

* The contents of the log file may differ depending on the version.

```
===
--- disk erase log ---------------------------
disk : ATA ST3160813AS (160041885696 byte/312581808 sector)
rev:SD2B ser:9SY082C5
method : 4-times[AA-55-rand-00] -> verify
start : 2014/02/16 14:02:39
end : 2014/02/16 16:28:34
error : write(0) read(0) verify(0)
status : finished (no error)
-------------------------------------------
PC : Dell Inc. PowerEdge SC440 - XXXXXXX
CPU : Intel(R) Pentium(R) D CPU 2.80GHz
MEMORY : 2071552 kB
-------------------------------------------
GreenPepper PRO ver.4.2.0 (c)kirala21
-------------------------------------------
===
92ae1655be5a5b95977863ac87c637a5
```

* If there is write error,
error: write(1234)1:100 2:200 3:34 4:900
The total number of errors, as well as the number of errors for each step, is displayed.

* When there is retry processing
retry: write(1234)1:100 2:200 3:34 4:900 read(1000)
A display like this is added.

About log file Checksum

As shown above, the "checksum" character string "92ae1655be5a5b95977863ac87c637a5" (example) is added at the end.
This is to check that the content of the report is output by "Green Pepper PRO" and that no single character has been changed since then.
To check the checksum, use Windows "Utilities for Administrator"/"check log".

* Please handle the log file in units of the contents between "===" (including itself) and the checksum character string on the next line.
* The checksum of the above sample is incorrect (security reason).

About the number of erasures

*The following write values can be changed. See "Common options"/"Erasure Pattern".
*For SSD drives, TRIM process is performed before the first erasure step when 2-4 times erasure is selected.

1-Time

The process of filling the entire disk with "zero" (00: hexadecimal number) is performed.

1st time: Write 00 (hexary) / 00000000 (binary)

2-Times

Perform the erasing process twice as shown below. Processing time is doubled. It is a method that makes reading by residual magnetism more difficult by using random values and zero clear without spending much processing time.

1st time: Write a random value
2nd time: Write 00 (hexary) / 00000000 (binary)

3-Times

Perform the erasing process three times as follows. Processing time is tripled. It is a method that conforms to the US Army compliant method (AR380-19). It is a method that shortens the processing time and makes reading by residual magnetism even more difficult by random value, FF value, and zero clear (inversion of each bit).

1st time: Write a random value
2nd time: Write FF (hexary number) / 11111111 (binary number)
3rd time: Write 00 (hexary) / 00000000 (binary)

4-Times

Erase the disk using a US Department of Defense standard compliant method (DoD5220.22-M). Use this if you need a higher level of security where residual magnetism is an issue. The processing time is 4 times longer.

1st time: Write AA (hexary) / 10101010 (binary)
2nd time: Write 55 (hex complement, AA complement) / 01010101 (binary)
3rd time: Write a random value
4th time: Write 00 (hexary) / 00000000 (binary)

* In order to comply with (DoD5220.22-M), perform the verification process by "Verify after erase".

About the number of errors

The number of errors is counted for each of write, read, and verify. The unit is 1 sector = 512 bytes.
* Even if the physical sector is 4096 bytes, the count is in 512-byte units.

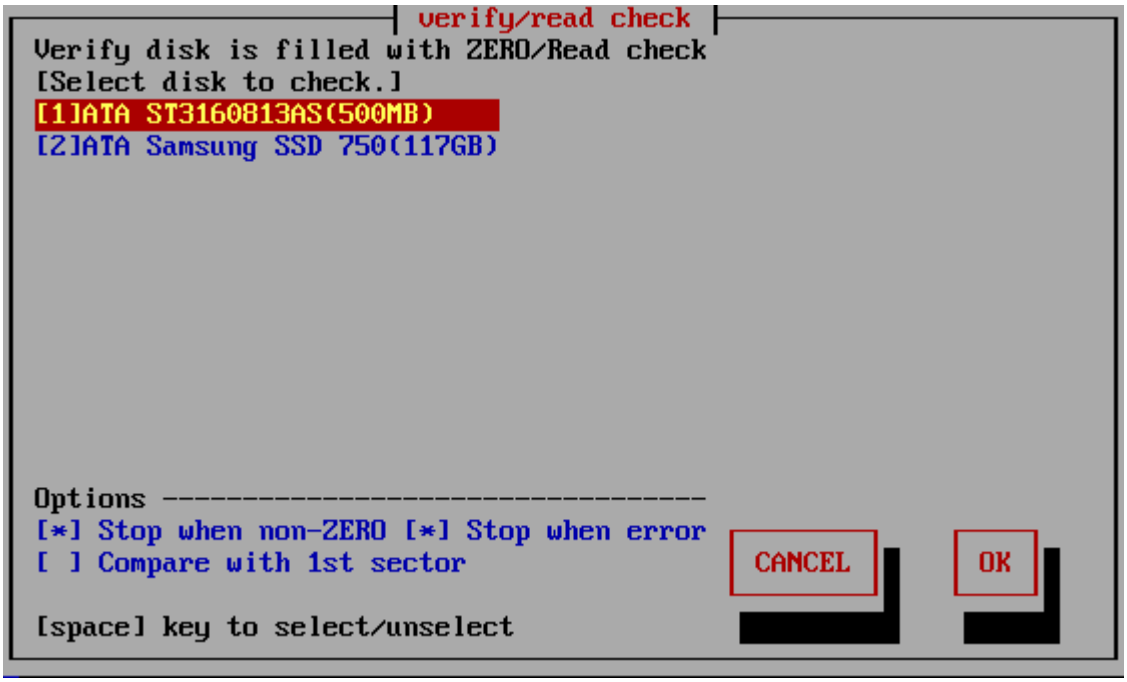
WRITE error	This is an error that occurred when writing. It is possible that this number x 512 bytes was not written (not erased) correctly.
READ error	Only when read verification is performed. This is the number of cases that could not be read. The contents of the disk are unknown for this number x 512 bytes. Even if a WRITE error has not occurred, READ may not be possible and a READ error may occur. This is a phenomenon that tends to occur on a failed disk.
VERIFY error	Only when read verification is performed. The number of sectors where the read data had a non-zero value (there was a difference when comparing with 0 sector). The part of the READ error is not included in the VERIFY error. Even if a WRITE error has not occurred, a VERIFY error may occur if the writing to the disk surface is not actually performed correctly. This is a phenomenon that tends to occur on a failed disk.

About retry processing

If an error occurs in the write process or read process, retry is performed.
The count of the number of times of retry is displayed in the log file "retry" part.
Even if "retry" has a count, it will not be counted as an error if it is processed normally at the time of retry.

Verify/read check

If you select "Verify/read check", the following screen will be displayed.



List of connected disks

The model number, capacity, firmware revision, and disk serial number of the disk recognized by the "Green Pepper PRO" system are listed.
* For a single disk, it is a physical disk unit, and for a RAID configuration, it is a logical disk unit.
* For RAID disk or others, revision, and serial number may not be displayed.

As shown below, if the message "NO supported disk" is displayed even though the disk is connected, the disk is not recognized.

* There may be a disk failure.

MEMO *** If the disk does not appear in the list

Check the disk hardware

· First, check that the disk is recognized on the BIOS screen of the PC.
To display the BIOS screen, see "Setting the boot environment on BIOS/UEFI".
Information about the disk is displayed in this screen.
· If Windows works, make sure that Windows recognizes the disk.

Check if it is supported by "Green Pepper PRO"

· If the interface is not supported by "Green Pepper PRO", the disk will not be displayed.
· Please let us know the contents of "Disk Interface" displayed in "Show current disk status"

* You can save the screen image to the FD / USB flash drive /Net share with "Utility" / "Save screenshot (FD / USBmem/Net)" displayed by ALT + F5.
Or
* Use "Write hardware information to FD / USBmem / Net" in "Utility" displayed by ALT + F5, save the PC information to USB flash drive / FD, and send the file (HWINFO.TXT) to us.

MEMO

The beginning of the line is
[1] (parentheses) are ATA (IDE, SATA) disks.
<3> (parentheses) are SAS / SCSI / RAID connections.

! 1 xxxxxxxx
Those with "!" Displayed are IDE disk interfaces that do not support high-speed mode (DMA) in the hardware / driver.
The access is low-speed mode (PIO mode), and the processing speed is very slow.

Select the disk using the [up] and [down] keys in the list, and press [enter].

* Multiple processes cannot be performed on the same disk on different screens.

Setting "Options"

* You can change the selection / deselection by pressing the [space] key while the cursor is on it. 

[ ] Stop when non-ZERO
The disk is read sequentially, and if there is a non-zero location, the process is interrupted. If not interrupted, it will be counted up and displayed as "non-zero".
The [*] state is the selection to interrupt.

However, when "Compare with 1st sector" is selected in the following options, it is compared with the contents of the first sector instead of zero, and if there is a difference, the interruption / non-zero count up is performed.

[ ] Stop when error
If a read error to the disk occurs in the middle, you can choose to interrupt the process or ignore it and continue.
If you ignore it and continue, the number of errors is counted.
The [*] state is the selection to suspend.

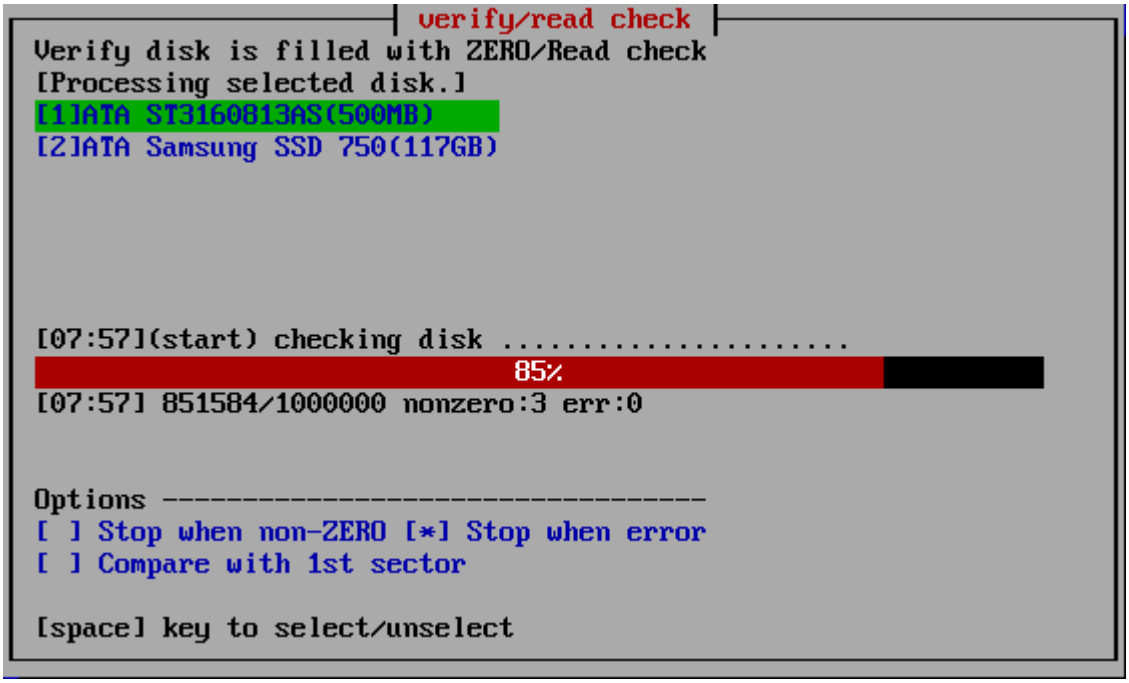
[ ] Compare with 1st sector
Checks if the contents of the disc are the same as the contents of the first sector.
This is used for read validation when a particular pattern is written. "Enhanced Secure Erase" may write non-zero values.
First, the first sector (512 bytes) is read, and the subsequent sectors are compared in units of 512 bytes.
The count displayed as "non-zero" is the number of sectors different from the first sector.
The [*] state is the selection to compare with 1st sector.

Execute check

Move the cursor with the [tab] key and press [enter] with "OK" to start checking.
Select "Cancel" to close the screen.

Confirmation in Locked / OPAL mode
If the HDD is password-locked, in OPAL mode for OPAL (self-encrypting) compatible disk, a warning will be displayed.

Display during checking process



The current processing status and the start time are displayed.

[hh:nn](start) ・・・Start time of current step, content of the proces
----------10%---------- ・・・Percentage of progress of the current step
[hh:mm] xxxxx/xxxx nonzero:xxxx err:xxx ・・・Current time, number of processed sectors / total number of sectors,
number of non-zero sectors, error sectors. (1 sector = 512 bytes)

MEMO
The display of "Number of processed sectors" is updated in small units up to the first 1% to confirm the start of operation, and then updated about 1% every progress. The processing speed does not decrease on the way. If there is a write / read error, retry and do a more detailed write / read check. Therefore, it may take much longer than usual.

When interrupting processing in the middle

If you want to interrupt the process in the middle, move to another screen (ALT + F1-5) and exit the system from the menu, or execute "Interrupt the processing process" on the "Utility" screen displayed by ALT + F5.

Confirmation screen at the end of processing

When the process is completed, the following screen will be displayed.
Use the [tab] key to move the cursor to "Close" and press [enter] to close the screen.
The "-" button is to prevent accidental closing. No processing is done.

About the number of errors

The number of errors is counted for each of write, read, and verify. The unit is 1 sector = 512 bytes.
* Even if the physical sector is 4096 bytes, the count is in 512-byte units.

READ error	This is the number of cases that could not be read. The contents of the disk are unknown for this number x 512 bytes.
VERIFY error	The number of sectors where the read data had a non-zero value (there was a difference when comparing with 0 sector). The part of the READ error is not included in the VERIFY error.

For more information on Secure Erase/Sanitize, see "About Secure Erase/Sanitize".

Secure erase/Sanitize

Secure erase / sanitize menu display

In the following cases, the Secure Erase / Sanitize Erase process menu is displayed.

· When booting with a normal CD / USB flash drive and a disk that supports Secure erase and is not frozen or a disk that supports Sanitize is connected.
· When Secure erase/Sanitize is enabled in the boot option.

When booting with Legacy/BIOS, enter the "gps" options to boot.

When booting with UEFI, press the [ESC] key and select
"---other boot options"-> "b. Enable Secure Erase"
from the option menu screen that appears. (See "Boot from CD/USB flash drive")

· When the "Secure erase / Sanitize menu" is set to "Always show" on a customized CD or USB flash drive (see "Common options")

When the menu option including Secure erase is selected and there is an disk that supports Secure erase, the menu is displayed as shown below, and Secure erase can be selected.

When the Secure erase / Sanitize menu is displayed

```
# erase disks (4-times[AA-55-rand-00])
--- secure erase/sanitize ---
# secure erase/sanitize (1-time [sec])
# secure erase/sanitize (2-times[sec-00])
# secure erase/sanitize (3-times[sec-rand-00])
---------------
# verify/read check
```

If the Secure erase/Sanitize menu display is specified (in the boot options/"Always show" customization) and there is no compatible disk, the following is displayed and Secure erase/Sanitize cannot be selected.

```
# erase disks (4-times[AA-55-rand-00])
--- X secure erase/saniize no disk X ---
---------------
# verify/read check
```

MEMO
During "Secure Erase" (ATA disk) processing on one screen, erasing ATA discs (both normal erase and secure erase) on other screens, checking ATA disks, etc. does not work until "Secure Erase" is completed. (the screen stops and starts moving after the secure erase is completed). If it is "sanitize" (ATA disk) processing, it can be operated on other screens. In particular, you need to be careful in the case of automatic erasing processing on a PC to which multiple HDDs / SSDs are connected.

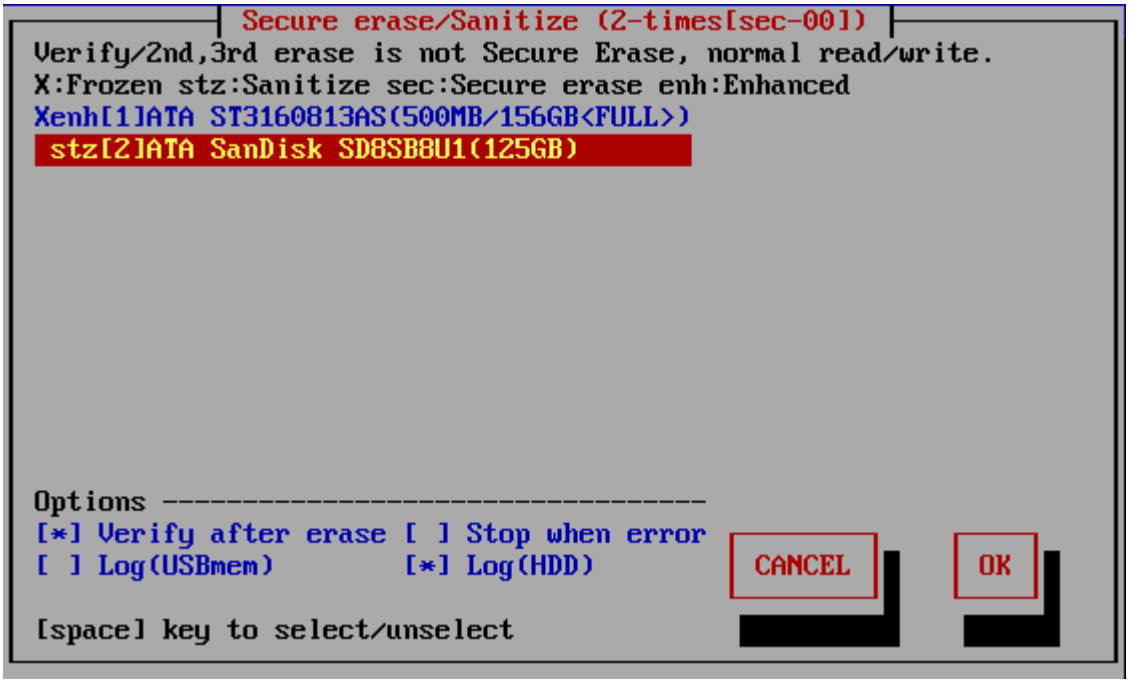
Unfreeze Process

For ATA disk drives (HDD, SSD), Secure Erase is frozen in most PCs.
The frozen state may be removed by the "unfreeze" process.
There are two ways to do this: specify the option at startup, or select "Utility"/"Set Secure Erase Method/Unfreeze".

See "Boot from CD/USB flash drive".
See "Utilities"-> "Set Secure Erase Method / Unfreeze".

Secure erase/Sanitize (1time - 3times)

If you select "SecureErase/Sanitize" (1time-3times), the following screen will be displayed.



List of connected disks

The model number, capacity, firmware revision, and disk serial number of the disk recognized by the "Green Pepper PRO" system are listed.
However, unlike the "Erase Disk" screen, this screen only displays disks that support Secure Erase / Sanitize.

"NO supported disk"

If the message "No supported disk" is displayed as shown below, it means that the disk that supports Secure erase / Sanitize cannot be recognized.
If it is displayed in "Show current disk status" but not displayed on this screen, it means that the disk or interface does not support Secure erase / Sanitize processing.

For example, when connecting a disk via USB, even if the disk itself supports Secure erase / Sanitize, it cannot be process Secure erase, because many USB interfaces do not pass through Secure erase command.
In many cases, it can be processed by connecting IDE / SATA directly to the motherboard interface of the PC.

Display of Secure erase/Sanitize, Frozen

If the disk supports Sanitize, it will be displayed as "stz". (Sanitize is displayed with priority)
If Sanitize is not supported and Secure erase is supported, "sec" or "enh" is displayed.
"sec" is a Secure erase display that does not support enhanced processing, and "enh" is a display that supports Enhanced Secure erase.
Those with an "X" at the beginning of the line are "Frozen" disks. In this state, Secure erase processing cannot be performed.
For the state of the disk for Secure erase / Sanitize, see "About Secure erase / Sanitize".

Display when HPA / DCO is set

If HPA / DCO is set (recognized), it will be displayed as follows.

MEMO
Secure Erase / Sanitize ignores the HPA setting and erases the entire disk, even if HPA is set. If the DCO setting is set, Enhanced Secure Erase erases all disks, but Normal Secure Erase keeps the DCO setting valid and does not erase the area outside the area restricted by the DCO setting.

In the example below, the total capacity of the disk is (156.3GB), but because HPA / DCO is set, normal access is limited to (100.0GB).
* HPA / DCO information may not be obtained by the system. Check the capacity of the disk before processing.

In this case, "Secure erase" erases the entire (156.3GB), while the second and subsequent erasures and read verifications are performed for the range (100.0GB).

ATA ST160813AS(100.0GB/156.3GB<!DCOleft>)
It may be displayed like this. This is the display when the DCO is set and it does not support Enhanced Secure Erase.
This message indicates that the part outside the area restricted by the DCO setting will not be erased.

Select the disk using the [up] and [down] keys in the list, and press the [tab] key to proceed to setting options.

* Multiple processes cannot be performed on the same disk on different screens.

Setting "options"

At the time of "Specify Erase method", "Auto Erase with Password", and "Full-Auto Erase", the following preset items are displayed and cannot be changed.
See "Common options" / "Specify erase method".

* You can change the selection / deselection by pressing the [space] key while the cursor is on it. [ ]

[ ] Verify after erase
After the erasing process is completed, read the whole disk and verify that all sectors have been erased.
The verification process is a normal read verification process, unlike Secure erase / Sanitize.

In the case of "secure erase/sanitize (1-time)" processing, the verification is not a confirmation of zero, but a verification that all sectors are the same as the contents of the first sector. This is because that Secure erase writes are not always zero and may be a specific value specified by the manufacturer.
However, depending on the HDD / SSD, a random value may be written, in which case the erasure cannot be confirmed by the verification step. (Counted up as a verification error)
In that case, it is necessary to select "secure erase/sanitize (2-times)" to write "00" after Secure erase, and then execute erasure verification in succession.

The state of [*] is the selection to "verify".

[ ] Stop when error
If a write error to the disk occurs in the middle, you can choose to interrupt the process or ignore it and continue.

If you ignore it and continue, the number of errors is counted.
No errors are counted in the secure erase process. It may occur only in the second and subsequent write / verification processes.
The [*] state is the selection to suspend.

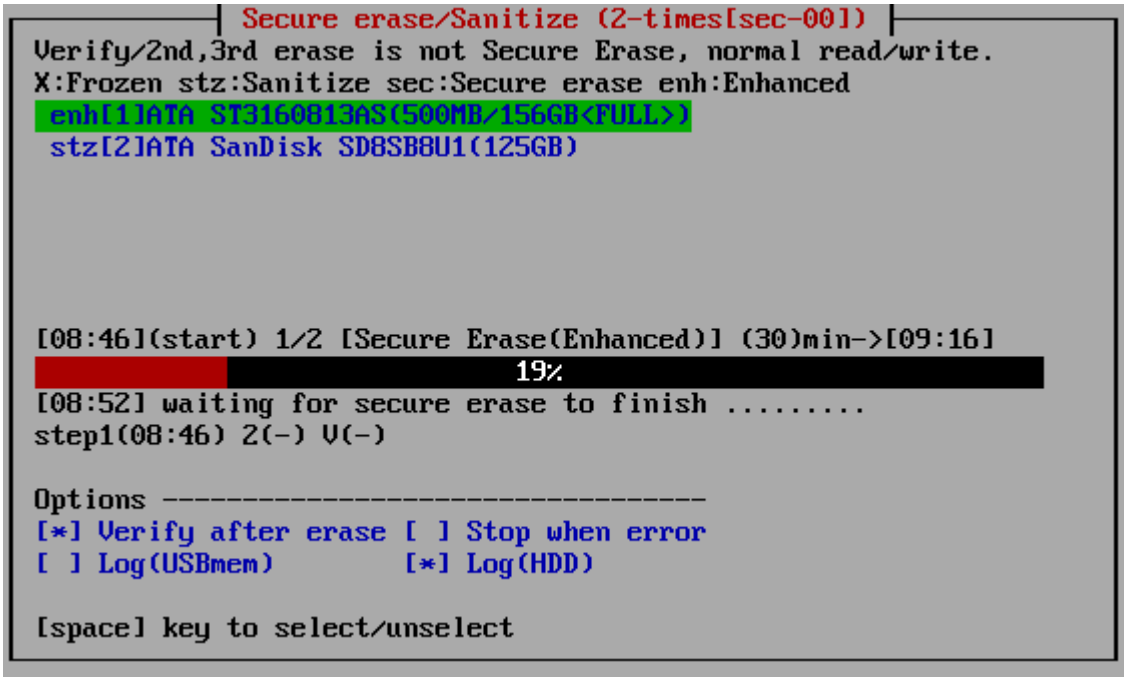
[ ] Log(USBmem,FD)
[ ] Log(HDD)

See "Erase Disks" about Log writing.

Execute Erase

If processing is possible, move the cursor with the [tab] key and press [enter] with "OK" to start erasing.
Select "Cancel" to close the screen.
* The screen display may differ depending on the process.

Screen during Secure erase of ATA(SATA) disk

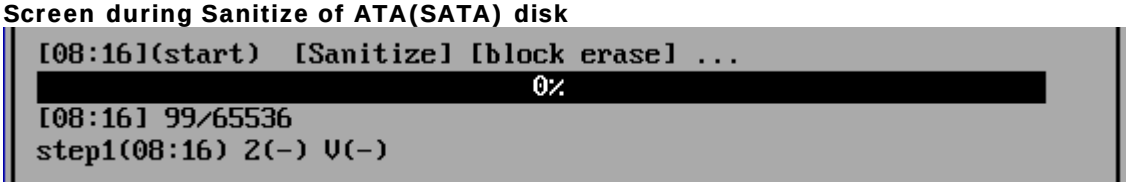


The current processing status and the start time for each step are displayed.

[hh:nn](start) ・・・Start time of current step, content of the process. Scheduled end time.
----------18%---------- ・・・Percentage of progress of the current step
[hh:mm] ・・・Current time.
step1(hh:nn) 2(-) V(-) ・・・Start time for each step (V is the verification step)

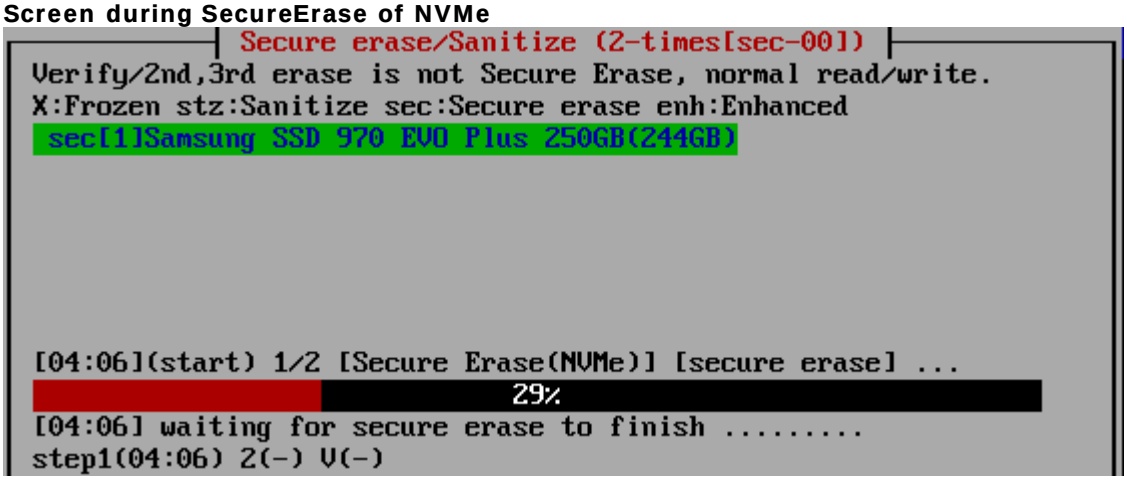
* The progress rate for Secure erase of ATA (SATA) disks indicates the elapsed time with respect to the "processing time" (predetermined). It is not the actual progress rate of disk processing

Screen during Sanitize of ATA(SATA) disk

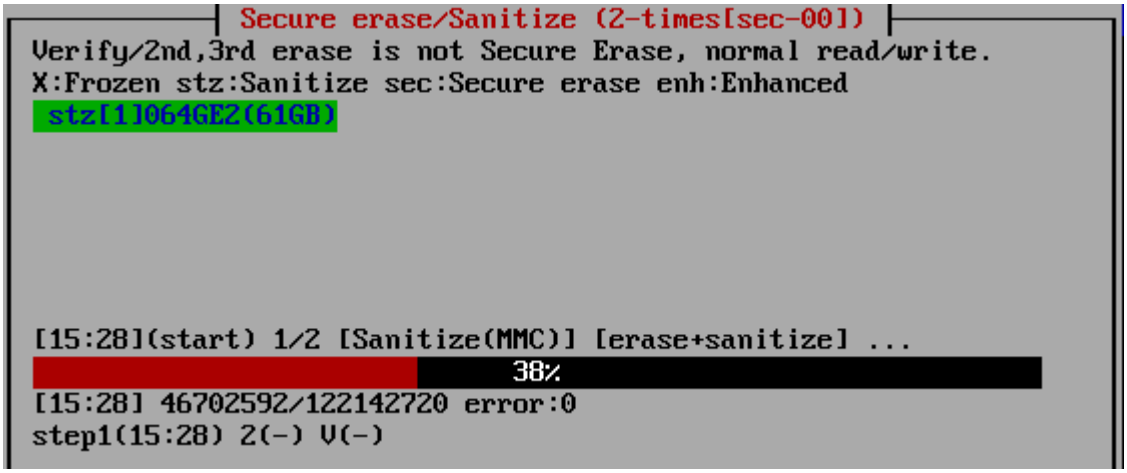


* The progress rate of ATA (SATA) disk sanitization ends up to 1/65536-> 65536/65536 according to the ATA standard. However, depending on the disk manufacturer / model, it may end up to 1/65536-> 100/65536. In that case, the percentage remains 0%. (Normal processing)

Screen during SecureErase of NVMe



Screen during Sanitize of eMMC



About processing time

Secure erase -ATA(SATA)
The processing time for Secure erase is specified by the manufacturer, and can be known in advance . This value is almost constant no matter what PC you connect to and process. That is why the "scheduled end time" can be displayed on the screen.
The processing time can also be found in "Show current disk status".
However, depending on the disk, that value may not be obtained and may be (0) in the "Show current disk status". In that case, it is processed as 120 minutes. Therefore, it may differ significantly from the displayed time.

In addition, this value is just a guideline, and the actual erasing time may vary. (It seems that it often finishes a little faster)

Sanitize -ATA(SATA)
The processing time of the Sanitize process cannot be known in advance. Please grasp according to the progress of the screen.

Secure erase/Sanitize -NVMe
The processing time of the Secure Erase/Sanitize process cannot be known in advance. Please grasp according to the progress of the screen.

Secure erase/Sanitize -eMMC
Since eMMC processes in memory block units, the progress is displayed in the same way as normal erasing. Please grasp according to the progress

When interrupting processing in the middle

Secure erase -ATA(SATA)
It is possible during the normal erase process, but the Secure erase process cannot be interrupted.
If you want to stop in the middle of the secure erase process, move to another screen (ALT + F1-5) and shut down the system.
At that time, the power will not be turned off automatically. After the end screen is displayed, press and hold the power button to forcibly turn it off.

* If the power is not turned off, the secure erase process will continue.
* (Ver4.5.0 or earlier) If the power is turned off during secure erasure, the HDD password will remain set on the disk and will be locked the next time the power is turned on. It is possible to perform secure erase again as it is, but normal disk reading and writing is not possible at all.
Use "Utility" and "Remove HDD Password" to erase the password.

For the state of the disk for Secure erase, see "About Secure erase/Sanitize".

After the secure erase step is completed, the second and subsequent writes and verification processes can be interrupted. Execute "Abort execution process" on the "Utility" screen displayed by ALT + F5.

Sanitize -ATA(SATA)
For Sanitize process, the processing program can be stopped by executing "Abort execution process" on the "Utility" screen displayed by ALT + F5.
However, the Sanitize process itself continues to run inside the disk.
Even if the power is turned off, the process will continue the next time the power is turned on.

Therefore, once the Sanitize process is started, keep the power of the disk ON until it is completed.
While processing is ongoing, the disk cannot be used because it cannot be read or written.
To check whether processing is in progress, check "process"/Sanitize in "show detail disk information" /"show

current disk status".
This content will be updated by returning to the initial menu.

Secure erase -NVMe
The processing program can be stopped by executing "Abort execution process" on the "Utility" screen displayed by ALT + F5.
However, the Secure erase process itself continues to run inside the disk.
It cant be interrupted when the power is turned off.

Sanitize -NVMe
For Sanitize process, the processing program can be stopped by executing "Abort execution process" on the "Utility" screen displayed by ALT + F5.
However, the Sanitize process itself continues to run inside the disk.
Even if the power is turned off, the process will continue the next time the power is turned on.

Secure erase/Sanitize -eMMC
For eMMC process, the processing program can be stopped by executing "Abort execution process" on the "Utility" screen displayed by ALT + F5.
It will also be interrupted when the power is turned off.

Errors that may occur during processing

Secure erase -ATA(SATA)

error code	contents
-3	Create process error
-2	Process error
-1	Secure erase not supported or frozen
1	Device open error
2	Read identify error
3	Could not unlock (by user password) The currently set password is different from the standard "pass" of "Green Pepper PRO", or the password cannot be canceled.
4	Read identify error
5	Could not unlock (by user password) (after some try)
6	Could not set HDD password.
7	Read identify error
8	Could not set HDD password (after some try)
9	Secure erase Prepare command test error
10	Secure erase Prepare command error
11	Secure erase Execution command error
15	Remove HDD password error
16	Read identify error
30	Secure erase test error
31	Secure erase process finishes in much shorter time than expected
32	Confirmation error after secure erase process
40	read identify error *Secure erase is finished
50	Verify check error

Sanitize -ATA(SATA)

error code	contents
-8	BLOCK ERASE is not supported
-7	OVERWRITE is not supported
-6	CRYPT ERASE is not supported
-5	Unsupported erase type
-4	Sanitize is not supported
-3	Read identify error
-2	Device open error
-1	Unsupported execution parameter
1	Could not get Sanitize status
2	Sanitize frozen
3	Sanitize is executing
10	Sanitize execution error (CRYPTO_SCRAMBLE)
11	Sanitize execution error (OVERWRITE)

12	Sanitize execution error (BLOCK_ERASE)
50	Verify check error
99	Process aborted

Secure erase -NVMe

error code	contents
-20	Secure erase (format) execution error
-17	Secure erase (format) is not supported
-16	Read identify error (identify ns)
-15	Read identify error (get ns id)
-14	Read identify error
-13	not Block device
-12	Device get information error (fstat)
-11	Device open error
-5	Verify check error
-3	Create process error
-2	Process error
>0	Secure erase execution error

Sanitize -NVMe

error code	contents
-99	Sanitize process error
-80	Verify check error
-10	Getting execution log error
-3	Device open error (get log)
-2	Sanitize process type error
-1	Device open error
>0	Sanitize execution error

Secure erase/Sanitize -eMMC

error code	contents
1	Device open error
2	Device lock error
11	Setting start area error
12	setting end area error
13	erase area error
21	Device open error(sanitize)
22	Sanitize execution error

Confirmation screen at the end of processing

See "Erase disks" about Confirmation screen.

About Log file

See "Erase disks" about Log file.

About the number of erasures

Since it is possible to grasp the status of a write error by performing normal writing after Secure erase / Sanitize, we have prepared a pattern that performs writing processing in addition to Secure erase / Sanitize.
However, since the second and subsequent times are normal write processing, it is not possible to write to bad sectors that have been replaced, as in Secure erase / Sanitize. Also, if HPA is set (ATA disk), Secure Erase erases the entire disk, but does not write to the HPA-protected area from the second time onward.

1-Time ([sec])
This is a process that performs only one secure erase / sanitize.

1st time: Secure erase/Sanitize

2-times ([sec-00])
The process of writing zeros (00) to the entire disk after Secure erase / Sanitize.

1st time: Secure erase/Sanitize
2nd time: Write 00 (hexary) / 00000000 (binary)

3-Times ([sec-randum-00])
The process to write a random value, zero (00), after Secure erase / Sanitize.

1st time: Secure erase/Sanitize
2nd time: Write a random value
3rd time: Write 00 (hexary) / 00000000 (binary)

About the number of errors

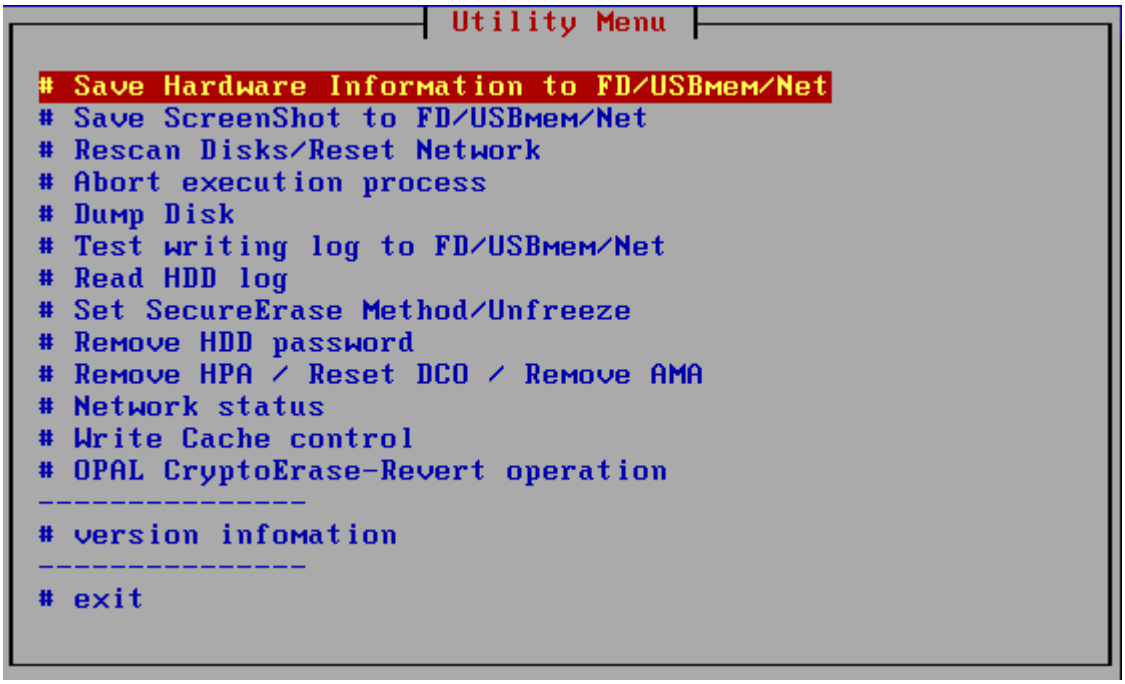
The number of errors is not counted in the Secure erase / Sanitize step.
If you perform 2-times erase or more, or if you perform read verification, it will only be counted in those normal write / read steps.

See "Erase Disks" for more information.

Operation of "Utility"

Utility screen

When the "Bootup Erase Program" menu or the operation screen is displayed, press "ALT + F5" to display the following utility menu.



Common operation when writing to FD / USB flash drive

Floppy disk and USB flash drive must be prepared and inserted at startup. Format the floppy disk in MS-DOS format and the USB flash drive in FAT / FAT32 / exFat.
* USB flash drive over 64G cannot be used for log storage.
* Built-in FD drive and USB-connected FD (1.44MB) can be used.

If you insert a USB FD/flash drive after displaying the menu, execute this utility screen "Rescan Disks/Reset Network".

Save Hardware Information to FD/USBmem/Net

If there is any problem such as the disk is not recognized or the network does not work, this process is used to acquire the information of your PC.
The acquired information is saved as "HWINFO.TXT" on the connected floppy disk or USB flash drive. If the network settings are valid and writing to a floppy disk/USB flash drive cannot be performed, the data will be written to the network share.
When written to the network share, the file name will be "hwinfo_mmddhhMMss.txt" (month, day, hour, minute, second).

Please send the saved information file to us.

The file is a text file. You can check the contents in advance with a notepad etc,.

If you see the message "could not write file (Net)", then there is an error saving to the network share.
For details and how to deal with it, see "Using "Network log"/ Trouble shootings".

Save ScreenShot to FD/USBmem/Net

It is used when there is some problem in processing, or when you want to save screen information and use it as a processing record, or when you want to maintain a manual. The screen shot (hard copy) is saved as a binary screen file (* .stx) on the FD / USB flash drive.
If the network settings are valid and writing to a floppy disk/USB flash drive cannot be performed, the data will be written to the network. When written to the network, the file name will be "mmddhhMMss.stx" (month, day, hour, minute, second).

The (* .stx) file is a hard copy file for Linux.
Use the "stx2bmp.exe" program that comes with the product to convert it to an image file (* .bmp).

If you see the message "could not write file (Net)", there is an error saving to the network share.
For details and how to deal with it, see "Using "Network log"/ Trouble shootings".

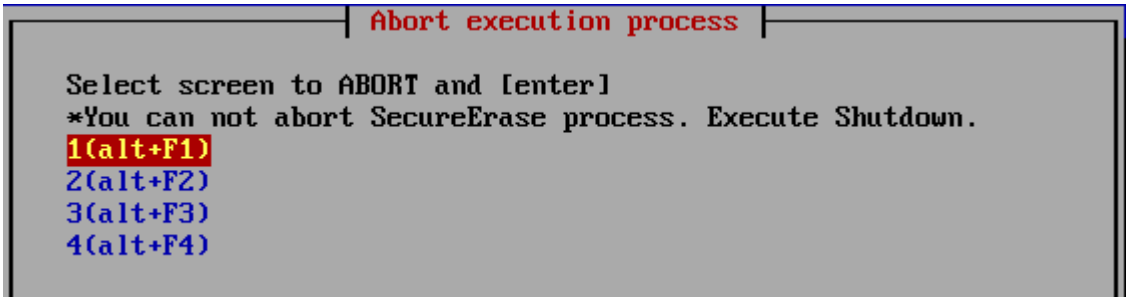
Rescan Disks/Reset Network

When the USB flash drive is inserted or the disk is hot-swapped after the boot is completed, this process updates the disk environment to the latest state. In addition, the network environment will be reset.
The screen shows the status of drivers installed and the network status, so you can use it to check the status.
When the process is completed, "press [enter]" will be displayed at the end, so press the [enter] key.

All screens (ALT + F1-F4) must be returned to the menu to perform this process.

Abort execution process

It is used to interrupt the process ,when the processing of "erase disk", "verify/read check".
However, it cannot be interrupted during the Secure Erase step in "secure erase".

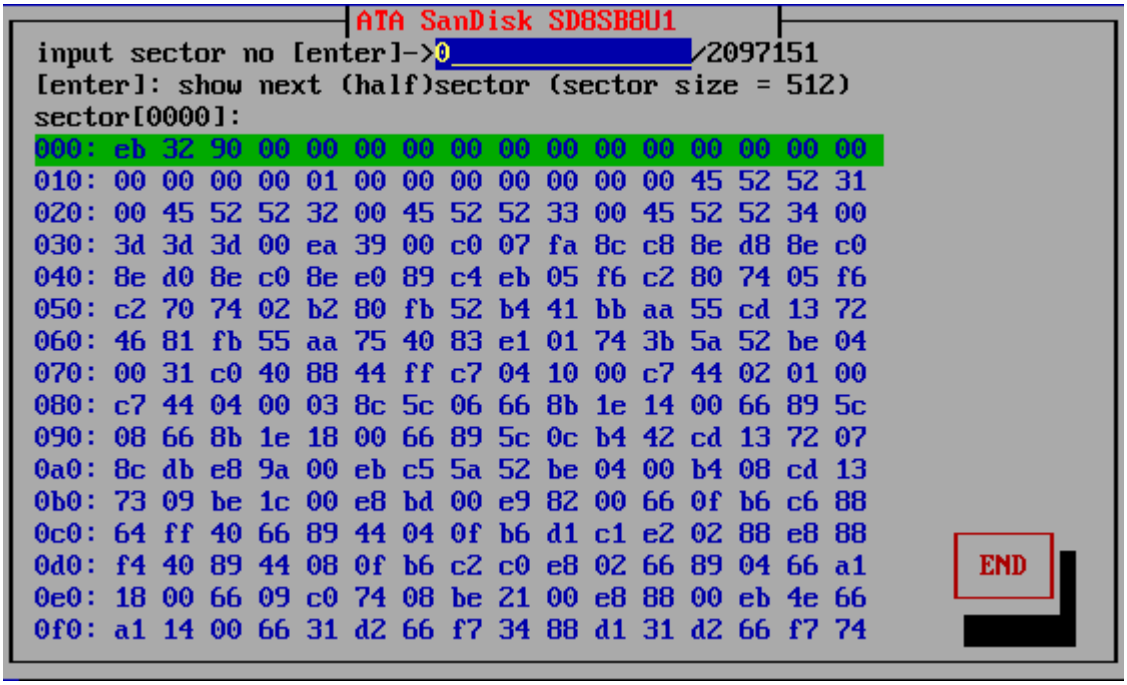


Select the screen (1-4) where the process you want to interrupt is being performed, and press the [enter] key.

Dump Disk

This is a function that displays the contents written on the disk as they are.
You can actually see what the contents of the disk are now.

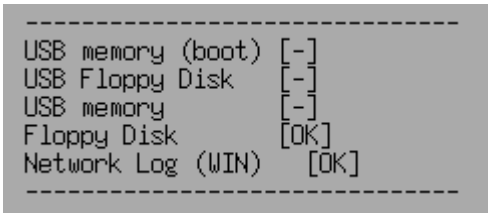
In the list display, select the disk to dump and press [enter].



The contents of the current sector (1/2 sector = 256 bytes) are displayed in hexadecimal.
If you press [enter] in this state, the next 1/2 sector will be displayed.
You can also display the contents of the specified sector by directly entering the sector number and pressing [enter].

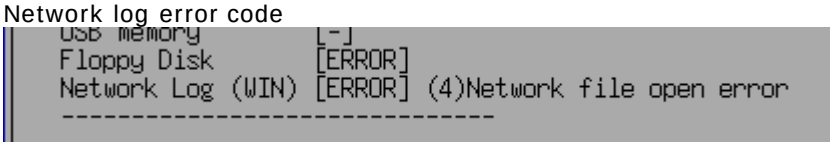
Test writing log to FD/USBmem/Net

Tests whether the disk erase log can be written.
You can make sure that the logs are really written by testing them before you start the erasure process.



If the write is OK, [OK] is displayed, if the write fails, [ERROR], and if the device cannot be found, [-] is displayed.

Network log error code



For details and how to deal with it, see "Using "Network log"/ Trouble shootings".

Read HDD log

The HDD log, written when "Log (HDD)" is selected in the erase process is read from the disk and displayed.

After selecting the disk you want to display in the list,
[Show log] Shows log on the screen.
[Copy log] Copy and save the contents of the log to the FD / USB flash drive.
If the network settings are valid and writing to a FD/USB flash drive cannot be performed, the data will be written to the network share.
[Del log] Delete the log from the disk. Writes zero only to the written part of the disk log.

Set Secure Erase Method/Unfreeze

Used to perform secure erase method selection ,secure erase processing test (ATA drive) and Unfreeze process.
In the list display, select the disk to process and [Set Method] or [Test Secure Erase].

In the list view, the supported secure erase processes are displayed.
sec: Secure Erase
enh: Enhanced Secure Erase
* If "X" is displayed before "sec" and "enh", it is in a "frozen" state.
stz: Sanitize

* If there is no disk that supports secure erase / sanitize, "*** NO supported disk ***" is displayed.

Secure Erase Setting (**Set Method**) (for ATA,NVMe,eMMC drives)
The normal "Secure Erase / Sanitize" process automatically selects and processes the most effective method supported by the disk.
If you want to perform a specific method, or if an error occurs in the automatically selected method, you can specify the method here.
The specified method is performed by "Secure Erase / Sanitize".

The corresponding methods are displayed as shown below. Select the method with the space key and press "OK".The method to be executed is registered.
When the "Secure Erase / Sanitize" process is executed next time, the selected method is performed.

(*)Auto(default)

( )Secure Erase
( )Enhanced Secure Erase
( )Sanitize/Block Erase
( )Sanitize/Over Write
( )Sanitize/Crypt Scramble

* If the process is not supported, you will not be able to select it as shown below.
--- Sanitize / Over Write

Test Secure Erase (only for ATA drives)
* This test is for ATA (IDE, SATA) drives. Not used for NVMe and eMMC drives.

It does not actually erase, it only tests whether the command processing step of secure erase processing is processed without error. The process may take up to 1 minute.

No actual secure erasure can be done unless this test is OK.
However, even if it is OK, there is a possibility that an error will occur in the actual erasure.

For details on processing interruptions and errors that may occur, see "Secure Erase/Sanitize".

In the list, select the disk you want to test and press [enter].
If the test is OK,
Secure Erase execution test [OK]
In case of error
Secure Erase execution test error[error code]
Message is displayed.

Unfreeze
Perform Suspend-wait 3 second-Resume.
By this process, ATA frozen state may released.
If there is no disk that supports secure erase / sanitize, this process is not executed.

* When performing this process, the CD/USB flash drive used for booting must be left in without removing it.

Do not enter any key until the confirmation screen after the process is displayed.
When the confirmation screen is displayed, press "Confirm" within 30 seconds.If "Confirm" is not pressed, the PC will shutdown.
*This is a function for automatic shutdown when the screen is not displayed.

In order to perform this process, the video chip of the PC must be compatible. If it is not compatible, it will not be

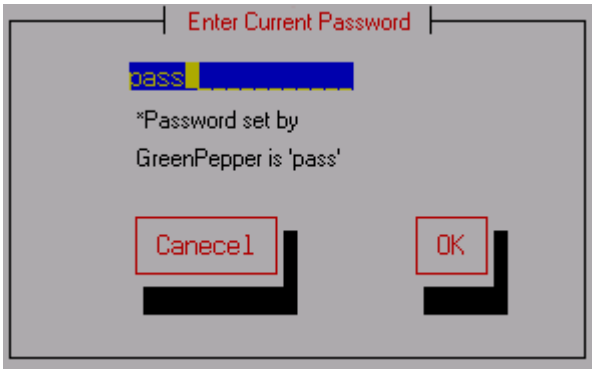
executed even if the process is selected, or the screen will remain black after processing and nothing will be displayed. When it becomes blank screen, trun off the power switch.
This process changes the screen resolution by installing the video driver.

* NVMe drives do not have a frozen state due to their specifications, but with some drives, secure erasing will result in an error under normal conditions, and processing may be possible by "unfreezing" processing.

See "Supported display chips"

Remove HDD password

Use this when you want to erase the preset HDD password when the secure erase (ATA disk) is interrupted and the HDD password is still set.
* In Ver4.6.x or later, this process is not required even after the secure erasure on the ATA disk is interrupted.



In the list, select the disk for which you want to erase the password and press [enter].
On the password entry screen, enter the currently set password and select "OK" to complete the process.

n the "Green pepper" system, a password "pass" is temporarily set and used for secure erasure. If you want to erase the password set in the "Green Pepper" system, use "pass" on the screen to erase the password.

Remove HPA / Reset DCO / Remove AMA

Please note that removing the HPA/DCO/AMA will prevent you from accessing the internal data. Or may cause problems when reusing the disk.

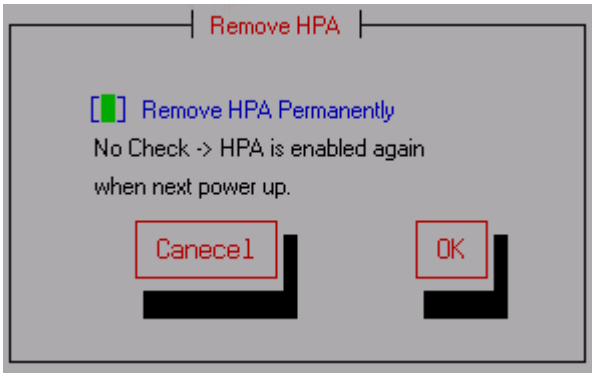
Performs the process of canceling the HPA/AMA setting for the disk HPA (Host Protected Area)/AMA(AccesibleMaxAddress) is set.

In the DCO reset process, first, only the disk size is returned to the physical disk size.
If that process results in an error, it resets all DCO data.
Therefore, if the personal computer assumes that setting, it may cause an obstacle during re-installation.
However, since it only returns to the original specifications and performance of the disk, there is no problem in using it on other computers.

* For HPA / DCO /AMA, see "Points to consider about erasing method" (Consideration of HPA, DCO, Recovery area).

In the list, select the disk for which you want to remove HPA / reset DCO / remove AMA and press [enter].
*If multiple settings are made, processing will be performed in the following order of priority: AMA, HPA, DCO.

Remove HPA



Remove HPA permanently
If checked (selected with the spacebar), the HPA will be permanently removed and will remain removed when the

disk is powered off.
If you do not check it, HPA removal will be temporary and effective until the power is turned off. The previous HPA settings will be maintained the next time the power is turned on.

Reset DCO
Check "Confirm execution" (select with the space key), and then select [OK].
The DCO is reset.

Remove AMA
Check "Confirm execution" (select with the space key), and then select [OK].
The AMA is reset.

When the removal / reset is completed, "Rescan Disks/Reset Network " is automatically performed.

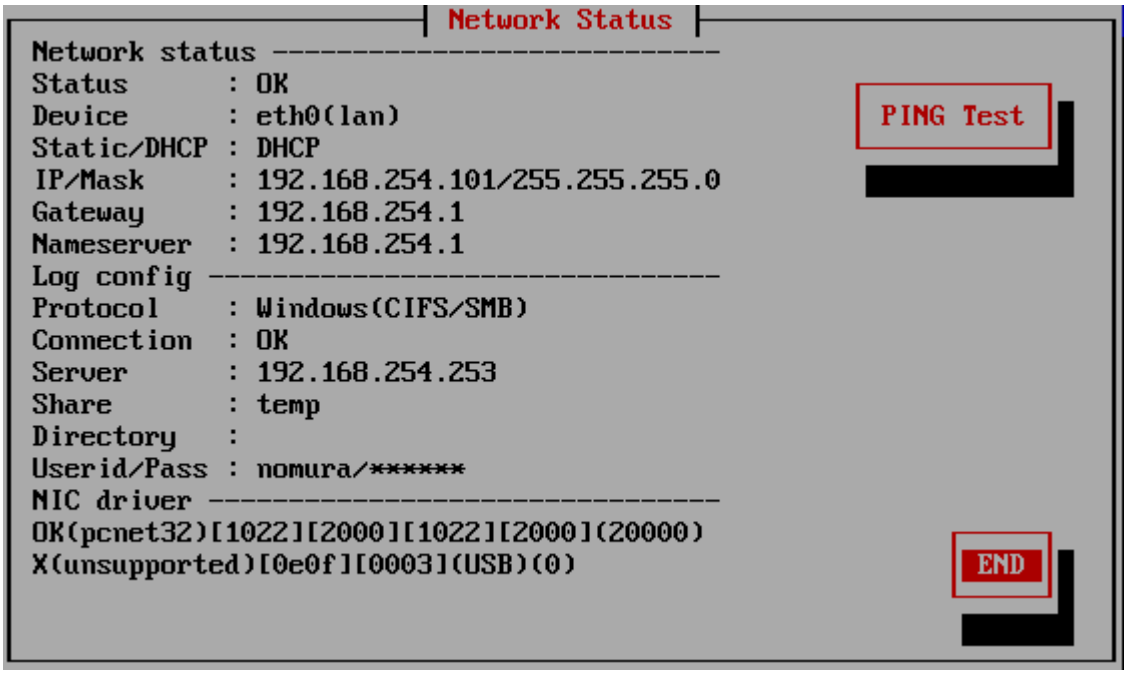
Network status

You can check the current network status.
If the network is not set, "Network configuration is not enabled" is displayed.

For the errors displayed on your screen and how to deal with them, see "Using "Network log"/ Trouble shootings".

For details on incorporating network functions, see "Common options "/"Network" when creating a boot environment.

Please incorporate the network settings when creating the boot environment.
It cannot be changed with "Utility" etc. after starting "Boot up Erase Program".



Network status
If the driver of the network interface card installed in the PC is read correctly and the IP address (ipv4), subnet mask, etc. are enabled, "Status: OK" will be displayed and the address etc. will be displayed.

If Status: is "NG", it means that the network address etc. have not been set.
For details and how to deal with it, see "Using "Network log"/ Trouble shootings".

Log config
* Protocol:
Windows(CIFS/SMB) · · · When writing to a Windows share.
FTP· · · When writing to a FTP server.
* Connection:
Only displayed for Windows shares.
"OK" is displayed when the connection to the Windows share can be established,
"NG" is displayed in the case of an error.

For the errors displayed on your screen and how to deal with them, see "Using "Network log"/ Trouble shootings".

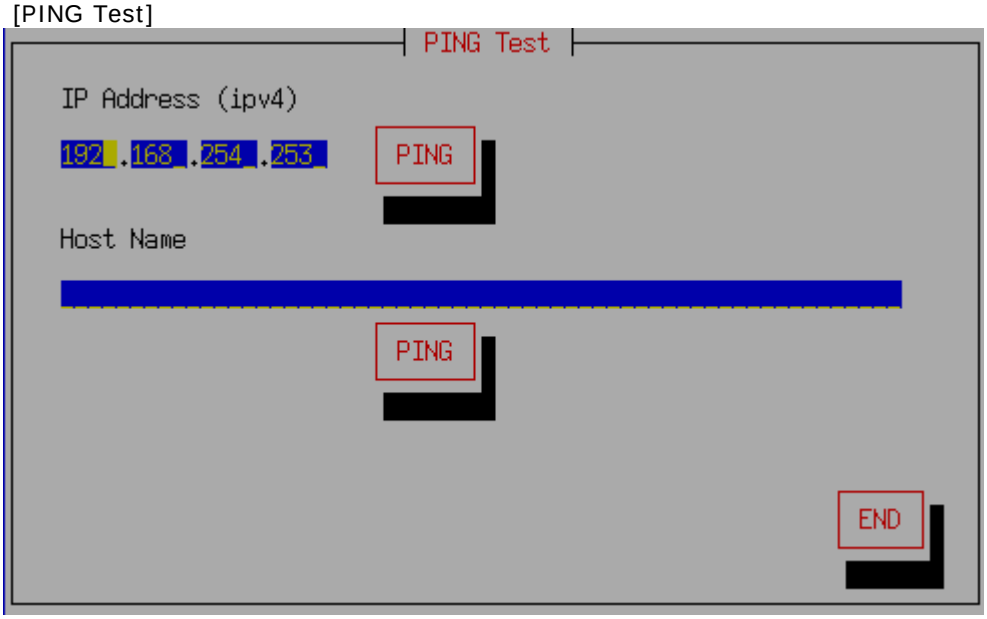
* Server:
The IP address (ipv4) of the Windows / FTP server, or the server name.
* Share:
Only for Windows shares. The name of the shared folder.

* Directory:
In Windows sharing, it is the folder to write under the shared folder.
For FTP connection, this is the write directory after connection.

* UserID/Pass:
User ID / password for connection. (Password is not displayed)

* NIC driver
Displays the information of the network interface card used in your PC and the status of the installed driver.

[PING Test]



A tool for checking connections for specific IP addresses and host names.
Enter the IP address or Host Name for which you want to test the connection, and select [PING].
If "ping test OK" is displayed, the basic connection with the PC has been established.

* When connecting with a host name, it is necessary that the name server (NamerServer) is set correctly and that the name server can resolve the name.
* Caution: Depending on the firewall of the PC, the PING response may be blocked.
In that case, you may be able to connect even if it becomes NG here.

'Write Cache' control

This is the process to change the state (on / off) of the write cache of the disks.
The disks that can be processed are ATA (SATA, IDE) and SCSI / SAS drives (when connecting with a compatible interface without RAID function).

In the list display, select the disk for which you want to change the write cache and press [enter].
It can be turned on if the current state is off and off if it is on.

Write Cache is a mechanism that the disk drive itself has.
When writing to a disk, it is written to the memory inside the disk drive first, and then writing to internal magnetic disk media is performed in the subsequent processing.

By using the write cache, the writing process of the PC software becomes faster, but there is a risk that the data before writing to the disk media will be lost due to a power failure.
Therefore, in the initial state, the SATA drive used for desktops and laptops is often in the write cache ON state, and the SAS drive used for servers etc. is often OFF.

In the erase process, it is faster to process with the write cache turned ON.
In "Green Pepper PRO", if the write cache of the disk drive is OFF on the compatible disk / disk interface, it is automatically turned ON at the start of erasing, and then returned to OFF after the erasing process is completed.
Therefore, if the erase process is interrupted in the middle, the cache status may remain ON. There are many disks whose write cache returns to the initial state when the power is turned off. But if you want to change the cache state for a disk whose set value is retained even when the power is turned off, change it in this process.

In addition, in the case of a disk with many failures such as error sectors, the failure status can be grasped more accurately by turning off the write cache for processing.

* If the write cache is set to off on this screen, it will not be automatically turned on even in the erase process.

OPAL CryptoErase-Revert operation

Only valid for OPAL (self-encrypting) disks.

Displays the mode and lock status of OPAL compatible discs.
Also, using the set password, the OPAL mode (encryption mode) is canceled and the normal ATA mode is restored.
Please note that the encryption key will be deleted and **any data inside the disk will be unreadable**.

For the unlock password, the entered value is sent to the disk as it is.
The password may be stored on the disk in the form converted by the software, such as when operating in OPAL mode by OPAL processing software.
In that case, even if the entered password itself is correct, the password will not match and processing will not be possible.

Using "Network Log"

Network log overview

The network log can also be used when the PC to be erased does not have writing media such as USB flash drive or FD, or when it is disabled as an internal security policy.
In addition, by managing logs collectively on a network server and creating a process for writing from log files to a database, it is possible to develop erasure history management in an in-house PC management database.

Windows share and FTP servers can be used as network drives.
* Windows sharing supports SMB3.0, 2.1, 2.0, 1.0

Onboard Ethernet, USB Ethernet, and WiFi (onboard, USB) can be used as network devices.
* However, some are not supported.

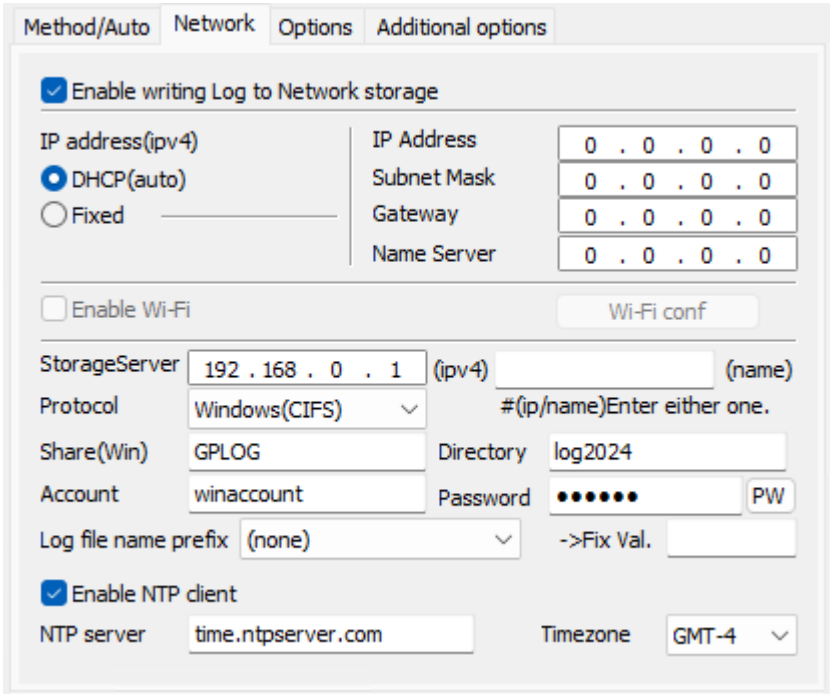
Network connections are more error-prone than writing to the local environment.
In order to prevent the loss of log files after a long erasing process, use "HDD log" (log to hard disk) as much as possible so that even if an error occurs in the network, the log file can be retrieved later. We recommend that operation.

Preparing to use network logs

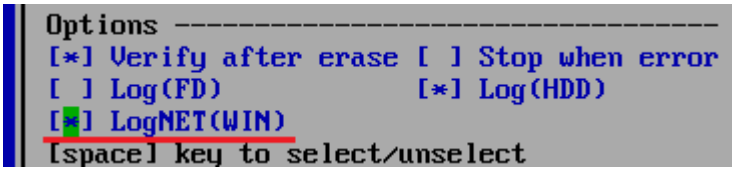
To write the log to the network share, It is necessary to create a bootable CD or USB flash drive that incorporates the network environment using the "Startup environment creation tool".
Alternatively, it is necessary to incorporate the network environment when setting the hard disk boot using the "Startup environment creation tool".

Network logs cannot be used when booting from the product CD-ROM in the initial state.

See "Abstract of "Startup environment creation tool", "Common options"/Network.



Specify log write destination



After starting the "Boot up Erase Program", on the disk erase process screen, check "Log NET" to write log to the network share.

The meanings of the indications in parentheses"()" are as follows.

WIN · · · When writing to a Windows share.
FTP· · · When writing to a FTP server.

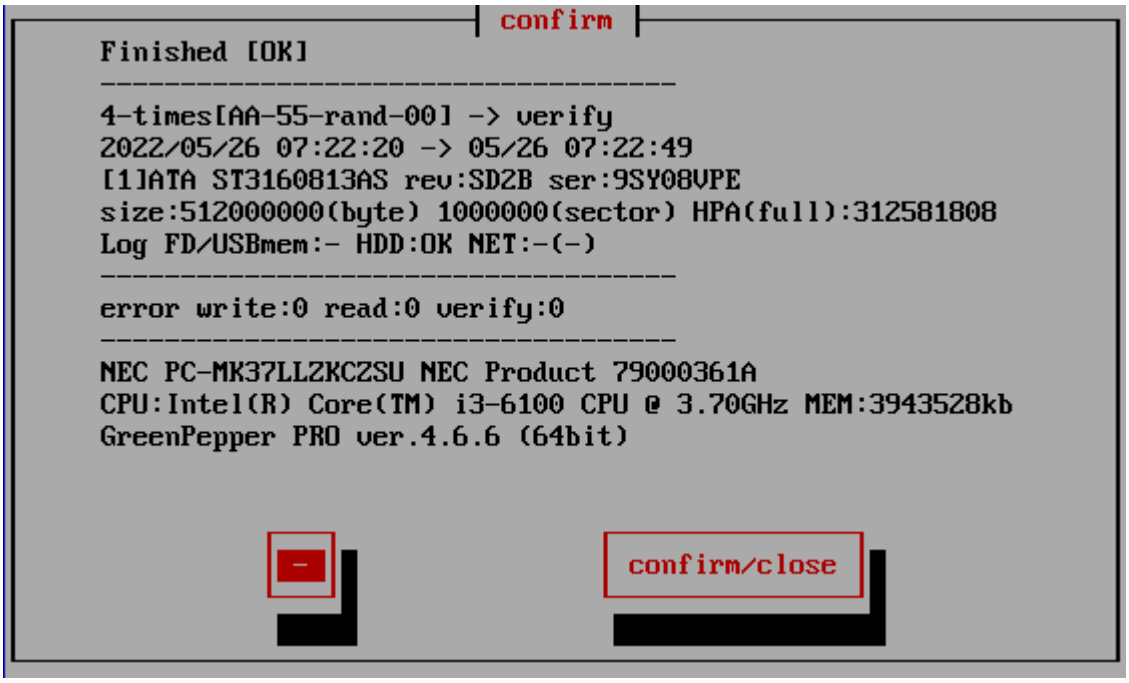
The "Log NET" is displayed only when the network function is incorporated.

Log write check immediately after the start of erasing process

When the start of the erasure process is selected, the log write check is automatically performed first.
* Write check before starting processing is also performed for USB flash drive/FD.
It is a function to check whether the log is written without any problem before the erasing process that requires a long time is started.
If you receive an error message, see "Network error codes and their troubleshooting" below.

Confirmation of log writing after erasing process

After the erasing process is completed, the network log will be written.
If there is an error when writing the log, an error message will be displayed before the confirmation screen below.



On the confirmation screen after the end, the log writing result is displayed.

Log FD/USBmem;- HDD:OK NET:-

"-" Indicates that writing is not specified, "OK" indicates that writing is complete, and "X" indicates that a writing error has occurred.
In the case of "NET", the written file name is displayed.
ex. NET:OK(0926181439.log)

Check the network environment, trouble shooting

Network connections have more error-prone elements than writing to the local environment and can be a bit more difficult to troubleshoot.
Please refer to the following to check the network status and solve the problem.

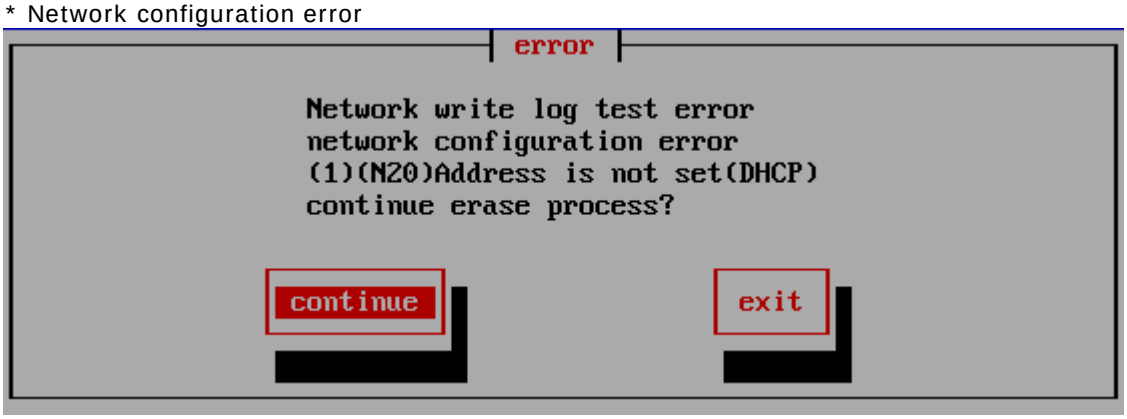
If the following troubleshooting do not resolve the issue, use "Utilities"/"Save Hardware Information to USBmem/FD/Net" to save the detailed information of your PC to a file(HWINFO.TXT) and send it to us.

Error when writing log

If an error occurs during the write check, the following error message will be displayed. Select "Continue" to ignore the error and continue.
However, log writing after the erase process will also result in an error.

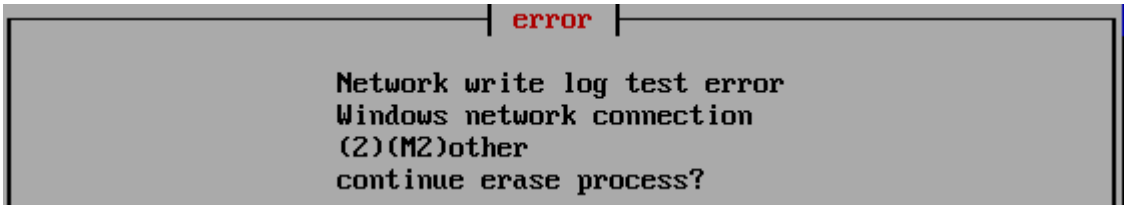
For details and how to deal with it, see "Network error codes and their troubleshooting" below.

* Network configuration error



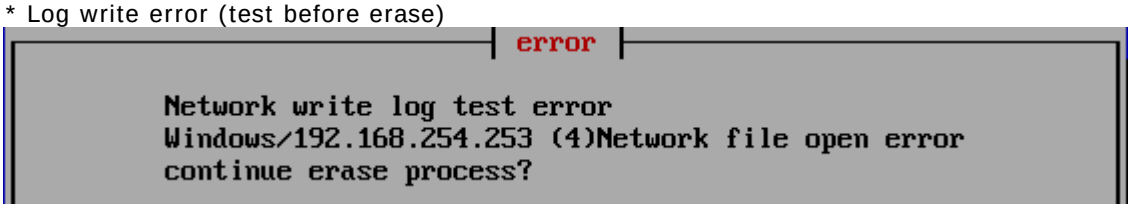
In the case of this error, basic network settings such as IP address have not been completed.

* Windows network connection



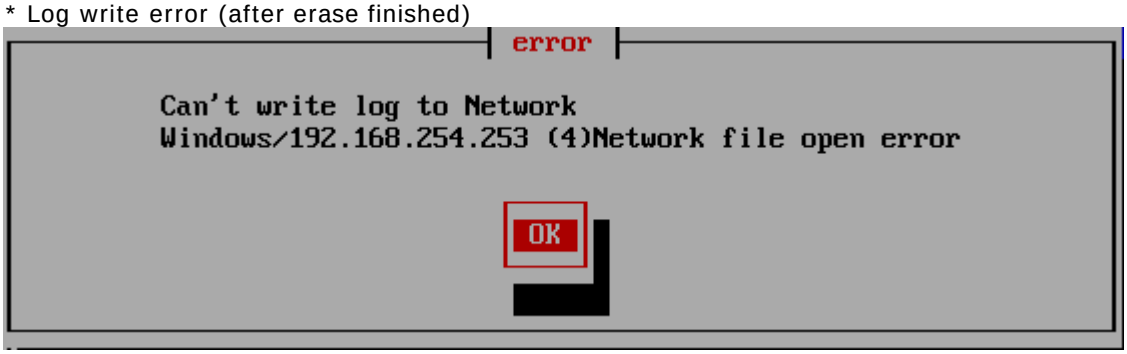
In the case of this error, the basic settings such as the IP address have been completed, but an error has occurred at the connection stage to the specified Windows shared folder.

* Log write error (test before erase)



In the case of this error, there is an error when writing the log.

* Log write error (after erase finished)



In the case of this error, there is an error writing the log, including network configuration issues, server connectivity issues.

Error when writing other files

In "Utility"/ "Save hardware information to FD / USBmem / Net", "Save screenshot to FD / USBmem / Net", etc., an error may occur when writing a file to the network share.

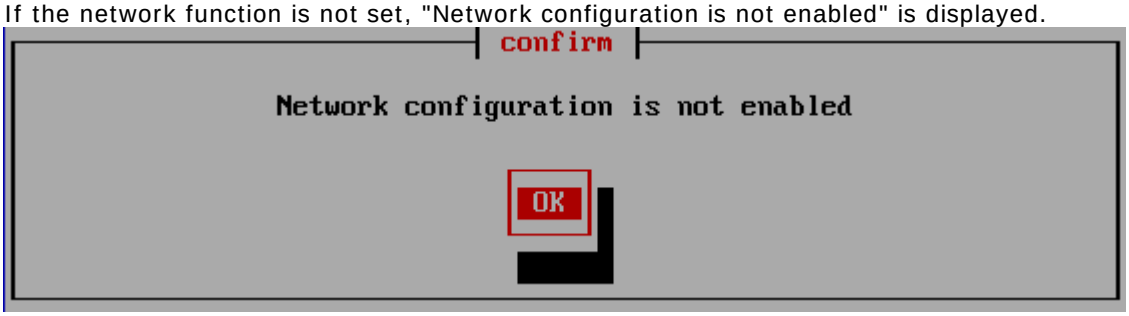
If an error occurs during writing, the following error message will be displayed.
If "(Net)" is displayed, it is a write error to the network share.
For details and how to deal with it, see "Network error codes and their troubleshooting" below.

Check "Network status"

You can check the network settings and the status from "Utilities" /"Network status".
If you have any problems, please check this screen.

If you change the problem on the server side and try to connect again,
restart "Green Pepper PRO" system or perform "Utilities" and "Rescan Disks/Reset Network".

If the network function is not set, "Network configuration is not enabled" is displayed.

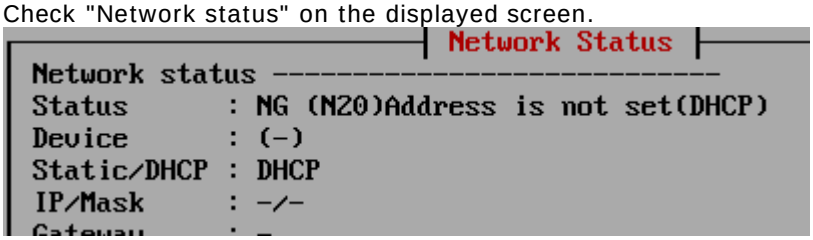


Troubleshooting

Create a CD / USB flash drive that incorporates the "Boot up erase program" with the network function enabled, and boot it.
See "Abstract of "Startup environment creation tool"", "Common options".

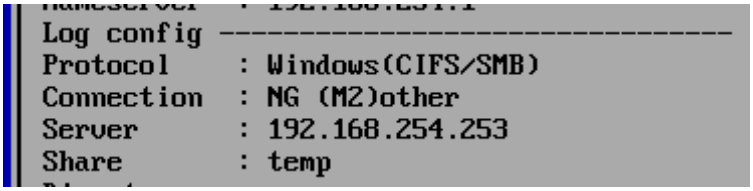
* Network status

Check "Network status" on the displayed screen.



If Status: is "NG", it means that the network address etc. have not been set.
For details and how to deal with it, see "Network error codes and their troubleshooting" below.

* Log config



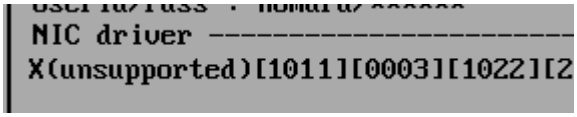
For Windows shares, Connection: may be "NG".
If the basic network settings such as the IP address are completed, but the connection to the shared folder of the

specified Windows server cannot be established, Connection: NG will occur.
For details and how to deal with it, see "Network error codes and their troubleshooting" below.

With FTP connection, the section is not displayed because the connection is attempted each time you write.

* NIC driver

If the network interface card installed in your PC is not supported by the version of "Green Pepper PRO" you are using, the following will be displayed.

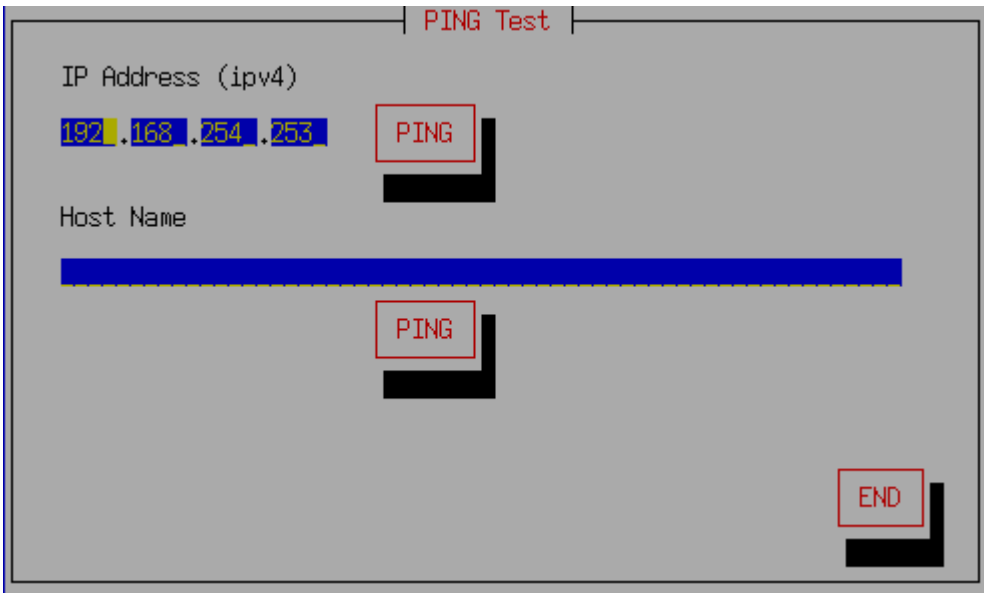


Troubleshooting
The numerical value is an ID number unique to the interface card model number, and if you inform us of this numerical value, we can inform you of the detailed correspondence status.
Also, if this field is blank, it means that the network interface card (a card that can be recognized) cannot be found.

More detailed information can be obtained by using "Utility" "Save hardware information to USBmem / FD / Net".
Please send the obtained file (HWINFO.TXT) to us.

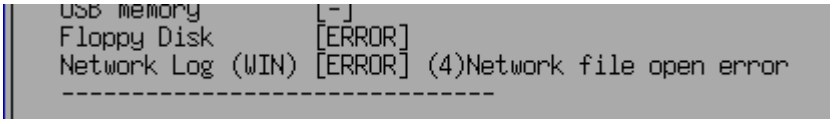
* PING Test

Use "PING TEST" to check the basic connection with other network devices such as servers and routers.
For usage, see "Utilities"/"Network status (PING test)".



Execution of "Test writing log to FD/USBmem/Net"

With "Utility"/"Test writing log", you can execute the log write test to the network share.



If there is an error, it will be displayed as [ERROR] like this.
For details and how to deal with it, see "Network error codes and their troubleshooting" below.

Network error codes and their troubleshooting

Network error codes and their troubleshooting

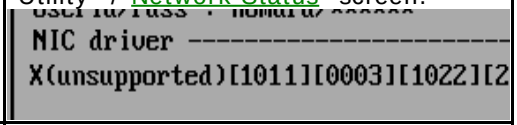
This is an error code that occurs when writing a log file, writing hardware information, or taking a screenshot.

Error code	Contents	Troubleshooting

(1) Network is not Enabled	The network function is not enabled, the IP address cannot be obtained, and so on. Check the network function, IP address(DHCP).	Check the network settings in "Utilities"/"Network status". You can get more detailed error information.
When writing to a Windows share		
(2) Windows share is not mounted	Could not connect to Windows share. Check the connection information.	Check the network settings in "Utilities"/"Network status". You can get more detailed error information.
(3) Internal file open error (5) Internal file read error	Internal processing file error.	
(4) Network file open error (6) Network file write error	The connection to the Windows share is complete. Error opening or writing log file.	If you have specified a directory, that directory may not exist. Create a directory in advance. You may not have write permission to the shared folder. Check the write permission of the shared folder. The content specified in "Log file name prefix" may contain inappropriate characters. Try setting the prefix to "None".
(50) Written file not found (51) Written file size error	In the process, writing of the file is completed, but the file is not found by the subsequent existence check of the file, or the file size is different from the writing size.	Check the same contents as (4) and (6) above. Also, if you have specified special security permissions for the folder, cancel it and try again. Some error has occurred in the write process. Check the free disk space, file system error, etc.
When writing to a FTP server		
(3) Internal file open error (5) Internal file write error	Internal processing file error.	
(10) Server connection error	This is an error that occurs when connecting to the FTP server.	The address specified for the server is incorrect. A valid FTP server is not running on the server. Packets (data) cannot reach the server. Check that the server address is correct, that there is no problem on the server side, and that there is no problem with the route (cable, router, etc.). Check if the packet can be reached in "Utility"/ "Network status (PING test)".
(11) Internal conversion(stream)	Internal processing error	
(20) Login error	Server login error	Please check your user ID / password.
(21) Get data port error	FTP protocol processing error (Data port acquisition)	
(32) Internal file open error (35) Internal file read	Internal processing file error.	

error		
(33) Remote file creation error	Remote file creation error	If you have specified a directory, that directory may not exist. Create a directory in advance. You may not have write permission to the write directory. Check the write permission. You may not have enough permissions to overwrite with the same file name that already exists. The content specified in "Log file name prefix" may contain inappropriate characters. Try setting the prefix to "None".
(36) Write to Remote file error	An error occurred while writing the remote file.	Make sure you have write permission for the file. For an FTP server, the file creation permission and the file write permission may differ.
(38) File close error	FTP protocol processing error (End of writing)	
(50) Written file not found (51) Written file size error	In the FTP process, writing of the file is completed, but the file is not found by the subsequent file existence check (SIZE), or the file size is different from the writing size.	You may not have permission to get the file information of the FTP server. Some error has occurred in the write process. Check the free disk space, file system error, etc.

Error related to network settings.
Code is displayed in the form of "**(N number)**".

Error code	Contents	Troubleshooting
Error that may occurs		
(N3) No network device found	The network device is not enabled because there is no corresponding network driver.	The network interface card installed in your PC may not be supported by your "Green Pepper PRO" version. Or, no valid network interface was found. Please let us know what is displayed in "Network Interface Driver" in the "Utility" /"Network Status" screen. 
(N20) Address is not set(DHCP) Address is not set(static)	The IP address could not be set. In the case of DHCP, the address cannot be obtained because the network cable is not connected or the DHCP server cannot be found.	When specifying an IP address by DHCP, it often occurs when the IP address cannot be obtained because the DHCP server cannot be found or the DHCP server does not respond. Please check the network route to the DHCP server and check the operation of the DHCP server. If you change the network route (cable, hub, etc.) or DHCP server side and try to connect again, restart "Green Pepper PRO" system or perform "Utilities"/"Rescan disks /Reset network". In the case of IP address setting with a fixed value, the specified address is incorrect, etc. Check the IP address / subnet mask settings.

The following rarely occurs		
(N1) Confing file not found	The network configuration file cannot be found.	
(N2) Confing file read error	An error occurred while reading the network configuration file.	
(N10) No ip/netmask in config	The fixed IP address (ipv4) and subnet mask values are not set.	
(N11) Bad ip(ipv4) address	Specified fixed IP address (ipv4) is incorrect.	
(N12) Bad subnet mask(ipv4)	Specified subnet mask (ipv4) is incorrect.	
(N13) Bad gateway address(ipv4)	Specified gateway address (ipv4) is incorrect.	

Error related to Windows shared connection.
Code is displayed in the form of "**(M number)**".

Error code	Contents	Troubleshooting
(M6) No such SHARE	The specified shared folder (displayed in [Share]) cannot be found on the server.	Review the shared folder settings. Alternatively, the server may be specified incorrectly.
(M13) Permission denied(ID/Password)	The connection was refused because the ID / Password is different or other reason.	Review the ID / password settings. It may not match the ID / password registered on the server, or you may not have access rights to the specified shared folder.
(M110) Connection timed out	Tried to connect to the server, but there was no response in time.	The server settings may be incorrect, the server may be down, or there may be firewall restrictions.
(M113) No route to SERVER	The packet cannot reach the server.	Review the IP address / subnet mask / gateway settings.
(M[error code]) Other error	Other errors.	Please let us know the error code etc.

Diagnose - Using diagnose screen

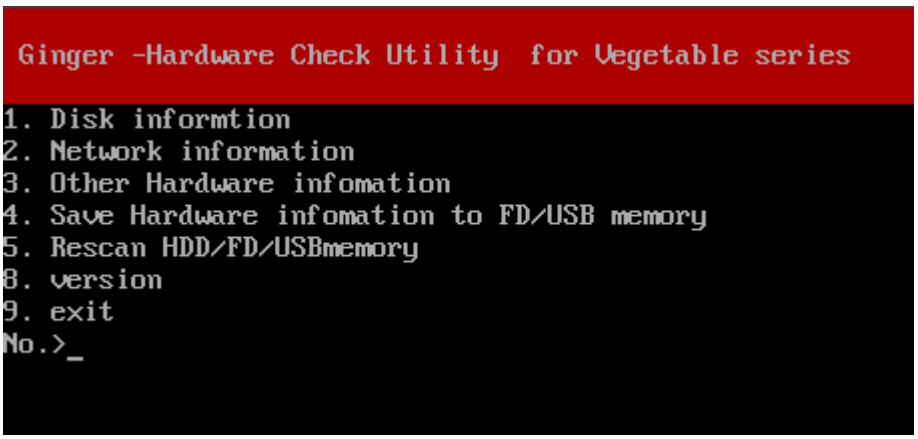
Diagnose screen

Legacy(BIOS) boot
* When booting from the CD / USB flash drive, enter "diag".
* When booting from the HDD, select "(--- green pepper, diagnose ---)".

UEFI boot
* select "(--- green pepper, diagnose ---)".

The following screen will be displayed.

If you stop before this screen, there is no function to get the screenshot.
Please take a picture of the screen with a digital camera and send it to us.



Of these, "4. Save'All Hardware information' to FD / USB memory" is equivalent to "Utility"/"Save hardware information to FD / USB mem".
If you insert a USB flash drive after booting, rescan with "5. Rescan HDD / FD / USB memory" and then write.

9 Exit with [enter].

"Windows Erase Program" (gppro4.exe) can be executed in normal Windows (8, 10, 11, server, etc.) or Windows PE environment.
You need to download WindowsPE from the Microsoft site and build an execution environment.

***License file "license.gp4" is requierd in the same folder as "gppro4.exe".**

Below, each unique part is separated and described as follows.

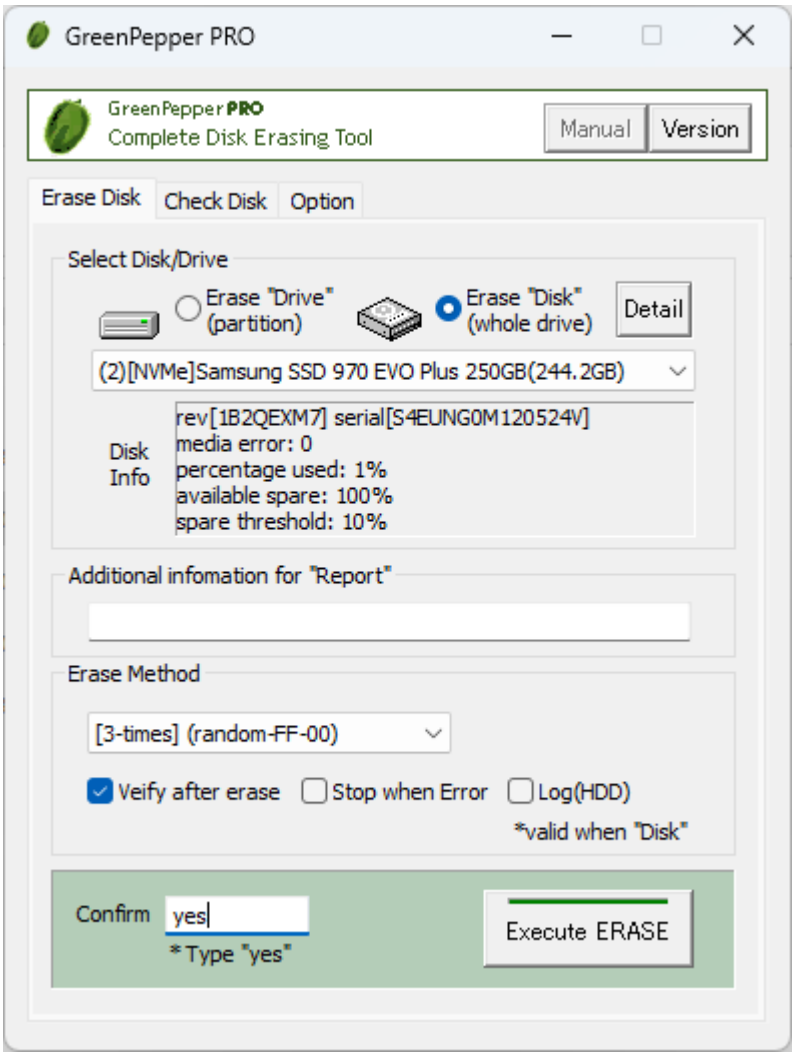
Windows10/11 etc.
This range applies only when executed on Windows (8, 10, 11, Server, etc.) .
Windows10/11 etc.

Windows PE
This range applies only when executed on WindowsPE.
Windows PE

Executing "Windows Erase program"

Windows10/11 etc.

"Windows Erase Program" can be easily executed without any prior installation work.
Follow the procedure below to start it.



Double-click [gppro4.exe] to start it.

· For online download, it is in the unzipped folder.
· If provided on a CD-ROM, it is located on the product CD-ROM (root).

You can boot directly from the product CD-ROM, or copy it to a hard disk, network drive, etc. for use.

Administrator privileges required to run

Windows7/2008 or later (include Windows10/11)
The following message will be displayed.

Do you want to allow this app to make changes to your device?
---
* The message varies depending on the Windows version.

* If you are logged on as a non-administrator,
  You will be required to enter the administrator user password.

Click (continue) "Yes" to boot.

Windows10/11 etc.

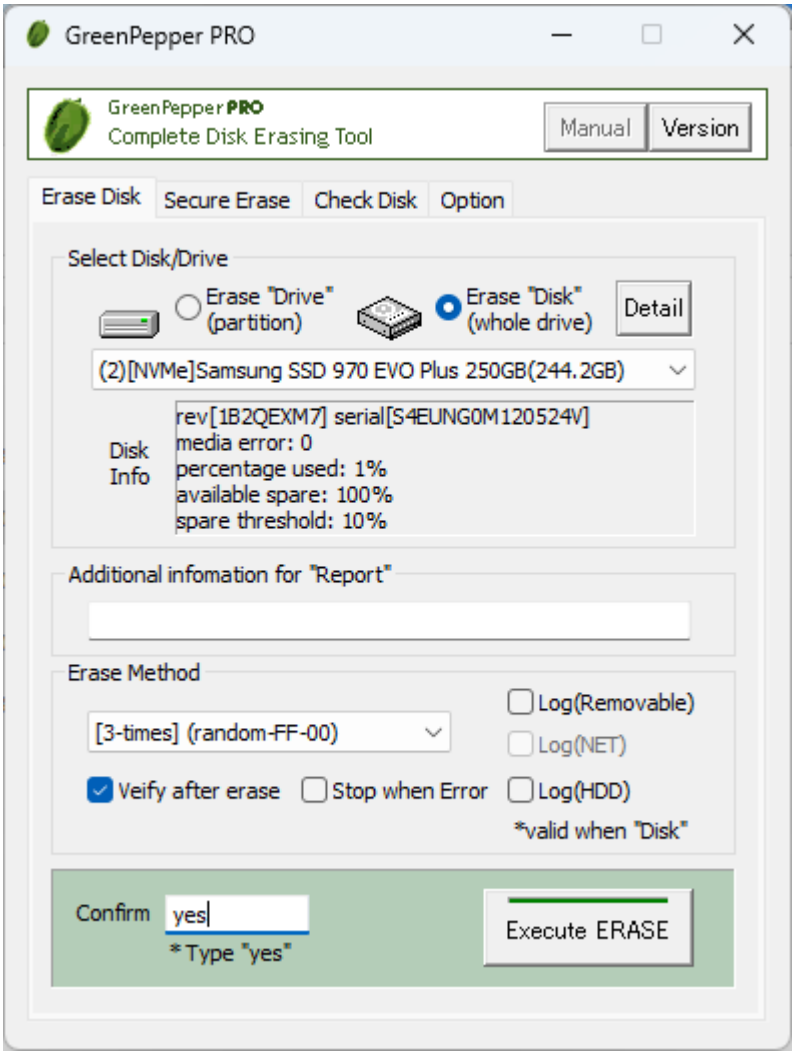
Executing "Windows Erase program" on WindowsPE

Windows PE

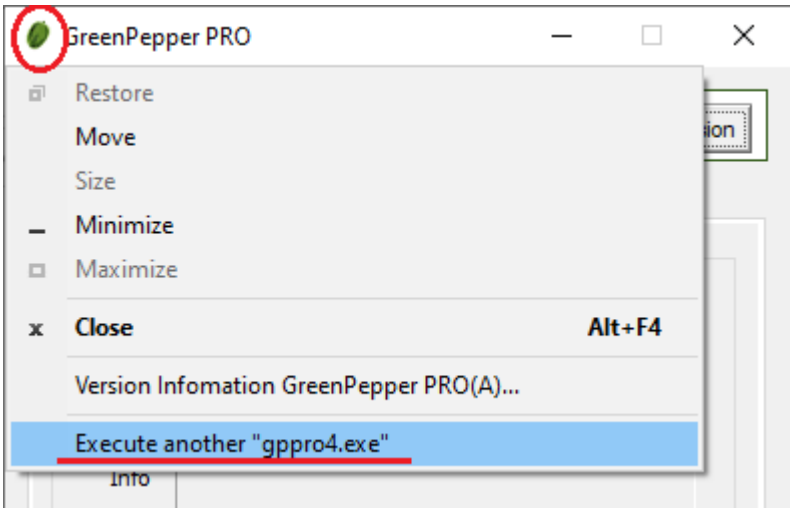
First, you need to build a WindowsPE boot environment and install "gppro4.exe" into it.
When running WindowsPE, if automatic execution is set, "gppro4.exe" will start automatically.
If you want to run it manually, run "gppro4.exe" in the saved folder.

For details on how to install it, see "Building WindowsPE Boot Environment".

In a WindowsPE environment, the [Secure Erase] tab and "Log Write (Removeable)/(NET)" are added.



After executing one "gppro4.exe", click the upper left icon to display system menu.
By selecting "Execute another GPPRO4.exe", multiple programs can be launched and each can be used to erase different disk drive.



Windows PE

About the [manual] folder

The "Manual" button on the upper right of the screen is enabled when the [manual] folder exists in the same folder as [gppro4.exe], and the manual will be displayed when the button is pressed.
If you want to display the manual with this button, you need to copy the [manual] folder along with [gppro4.exe].

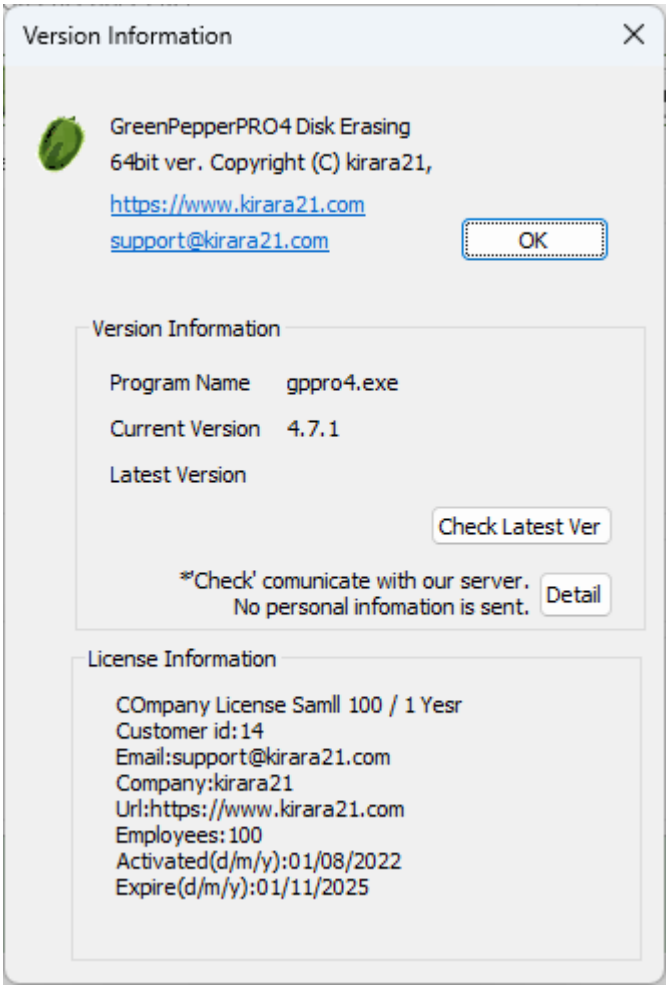
*"index.html" in the [manual] folder is called. It is also possible to display any document.

when "disabled" when "enabled"

[Version] button

You can check the version currently in use and the latest version by clicking the [Version] button on the upper right of the screen.

"64bit ver." indicates a 64bit program, and "32bit ver." indicates a 32bit program.



Check Latest Ver

When you press this button, it communicates with our (kirala21) server and displays the latest version information on the screen.

* Customer-specific information (PC information, Windows information, etc.) will NOT be sent in this communication.
* Communicate via http. Please use it in an environment where you can access the Internet via http.

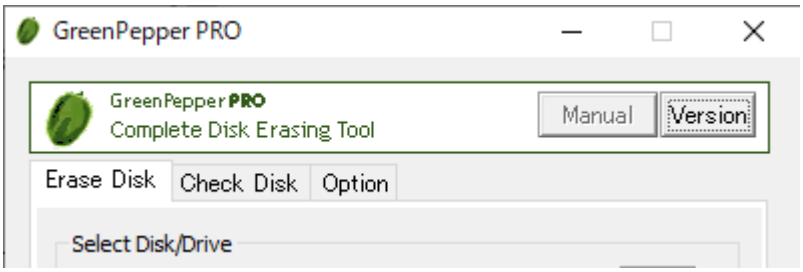
Detail

Click the [Detail] button to see the details of what is sent to the server.
No further information will be sent.

Erase disk drives

"Erase Disk" erases the hard disk, floppy disk, memory card, etc. connected to the Windows PC.
When erasing with "erase Disk"(not "erase Drive"), all the contents of the disk including the format data will be erased.

*"Disk" refers to a whole physical disk unit.
*"Drive" refers to a partition within a disk drive. Usually a drive letter "A"-"Z" is assigned.



* If you format the disk again, you can use the disk again.
* Drives / disks accessed by some programs, including background services, cannot be erased.

Windows10/11 etc.

* **Drives used in Windows systems, such as C drive and disks containing C drive partition, cannot be erased**.
* Use the "Boot up Erase Program" or run on WIndowsPE environment for Windows system drive, other drives used by Windows background process.

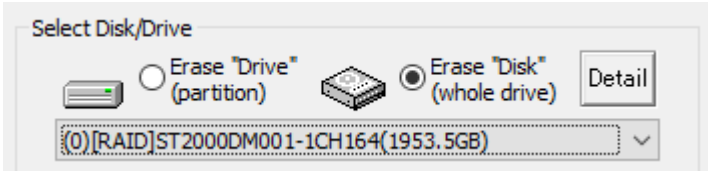
Windows10/11 etc.

Windows PE

*It is possible to erase all drives, including the Windows system drive.

Windows PE

Select Disk/Drive



Select whether to erase etc. on a drive (C,D,..., a partition) or on a whole physical disk.

Windows10/11 etc.

erase Drive
In Windows, drive letters such as A, C, D, etc. are basically assigned to each disk (whole physical disk) for removable disks (such as floppy disks ,USB flash drives), and to each partition for hard disk drives.
If you want to erase this drive unit, select "erase Drive".

* on WindowsPE, you cannot select "erase Drive"

Windows10/11 etc.

erase Disk
For hard disks, etc. (include removable drive), you can erase entire disk regardless of the partition state. In that case, all data on the disk, including partition information, will be erased.

* For a single disk, it is a physical disk unit, and for a RAID configuration, it is a logical disk unit.

Disks with no drive letter assigned or unformatted disks can also be selected.

MEMO
When erasing in disk units, it is necessary that all the drives (E, F, G, etc.) contained in the disk are not accessed by any process at all. Even if the folder on that drive is displayed in Explorer, it cannot be processed.

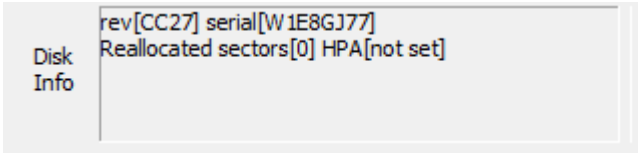
At the start of the erase process, all the allocated drives will be separated from Windows, so those drives will not be visible from Explorer.

Select Drive / Disk to erase

After specifying "erase Drive" or "erase Disk", select the drive/disk to erase.

Disk information

Choose "erase Disk" and a select disk to display information about the disk.
* Not displayed when "erase Drive".

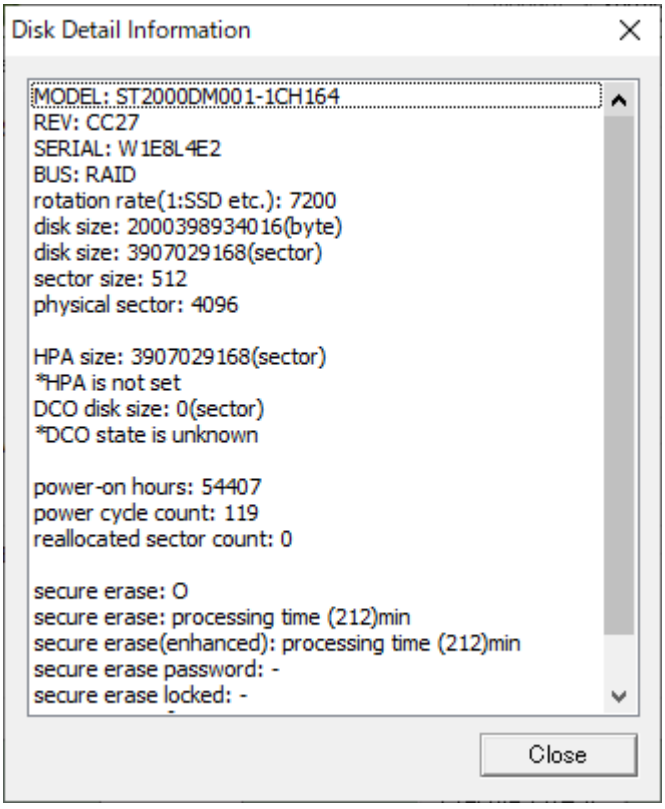


If the information can be obtained, the following information will be displayed.
rev: Disk firmware revision
serial: Disk serial number reallocated sector: Number of sectors that have been reallocated
HPA: Host protected area, Setting information
and other information.

* For "Reallocated sector" and "HPA", see "Points to consider about erasing method".

Disk Detail information

Choose "erase Disk", select a disk, and then click the "Detail" button to display detailed disk information.
* Not displayed when "erase Drive".



What is displayed

* Some items may not be displayed depending on the disk, disk interface.
* For "Reallocated sector", "HPA", "DCO", "Secure Erase",, see "Points to consider about erasing method".

MODEL	Model name
REV	Firmware revision
SERIAL	Serial No
BUS	The name of the BUS to which the disk is connected. SCSI, ATA, USB, RAID, iSCSI, SAS, etc.
rotation rate	The rotation rate of the disk. Displayed as "1" for SSDs, etc.
disk size	Disk size in bytes
disk size	Disk size in sectors (512 bytes)

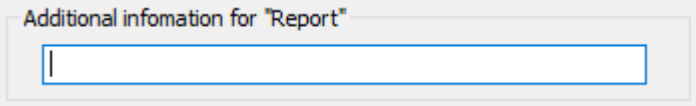
sector size	Logical sector size
physical sector	Physical sector size
HPA size (ATA drive)	Disk size including areas other than those protected as HostProtected Area. If it is the same as "disk size", it means that HPA is not set. "*HPA is set" HPA is set. The "disk size" is smaller than the physical disk size, and **there are areas that are normally inaccessible**. "*HPA is not set" HPA is not set and "disk size" is the same as the physical disk size. However, if DCO/AMA is set, the "disk size" will be smaller than the physical disk size. "*HPA state is unknown The HPA status cannot be obtained and the setting status is unknown. "*HPA is not supported" HPA is not supported.
DCO disk size (ATA drive)	If the disk size is set (reduced) in DeviceConfigurationOverlay, the DCO disk size is the actual physical disk size. "*DCO is set" DCO is set. The "disk size" is smaller than the physical disk size, and **there are areas that are normally inaccessible**. "*DCO is not set" DCO is not set and "disk size" is the same as the physical disk size. However, if HPA/AMA is set, the "disk size" will be smaller than the physical disk size. "*DCO state is unknown" The DCO status cannot be obtained and the setting status is unknown. "*DCO is not supported" DCO is not supported.
AMA disk size (ATA drive)	If the disk size is set (reduced) in Accessible Max Address (AMA), the disk size is smaller then the actual physical disk size. "*AMA is set" AMA is set. The "disk size" is smaller than the physical disk size, and **there are areas that are normally inaccessible**. "*AMA is not set" AMA is not set and "disk size" is the same as the physical disk size. However, if HPA/DCO is set, the "disk size" will be smaller than the physical disk size. "*AMA state is unknown" The AMA status cannot be obtained and the setting status is unknown. "*AMA is not supported" AMA is not supported.
power-on hours	Disk usage time (in hours) recorded on the disk.
power cycle count	The number of times the disk is turned on, recorded on the disk
reallocated sector count (ATA)	Number of reallocated bad sectors.
media error (NVMe)	Media errors count of the drive.
percentage used (NVMe)	Used (consumed) percentage of the drive.
available spare (NVMe)	Available spare (for replacement of error media) percentage.
spare threshold (NVMe)	Healthy threshold for available spares.
secure erase	Support for Secure erase and processing time.
secure erase(enhanced)	Support for enhanced secure erasure and processing time.
secure erase password	Whether the HDD password is set. "O": Set "-": Not set, unknown
secure erase locked	Whether the HDD is locked. "O": Locked state "-": Not set, unknown
secure erase frozen	Whether the HDD is frozen. "O": Frozen state "-": Not set, unknown
sanitize	Support for Sanitize
sanitize OverWrite	Supports erasure by "OverWrite" processing in Sanitize.
sanitize BlockErase	Supports erasure by "BlockErase" processing in Sanitize.
sanitize CryptoErase	Supports erasure by "CryptoErase" processing in Sanitize.
OPAL supported	"O": if the disk supports OPAL (self-encryption). If it is not supported, it will not be displayed. Ver: OPAL version mode: Display of OPAL mode or ATA,NVMe mode lock: "O" if locked in OPAL mode, "-" if not locked

Additional information for "Report"

Enter the information to be added in the end "Report" displayed after the processing is completed.
It is convenient to use it to record the name of the device, ID number, name of the person in charge, etc.
The characters entered here will be included in the checksum of the report and will be checked for tampering with the report.

* It is not added to the log file.

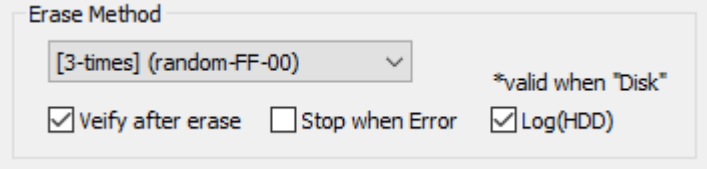
Example: "Manufacturing Depart. Nomura"



Erase method, options

Select the erasing method and processing option.

* Secure erase is not possible with "Windows Erase Program". Please use the "Boot up Erase Program".
* The following write values can be changed. See "Common options"/"Erasure Pattern".



1-Time

The process of filling the entire disk with "zero" (00: hexadecimal number) is performed.

1st time: Write 00 (hexary) / 00000000 (binary)

2-Times

Perform the erasing process twice as shown below. Processing time is doubled. It is a method that makes reading by residual magnetism more difficult by using random values and zero clear without spending much processing time.

1st time: Write a random value
2nd time: Write 00 (hexary) / 00000000 (binary)

3-Times

Perform the erasing process three times as follows. Processing time is tripled. It is a method that conforms to the US Army compliant method (AR380-19). It is a method that shortens the processing time and makes reading by residual magnetism even more difficult by random value, FF value, and zero clear (inversion of each bit).

1st time: Write a random value
2nd time: Write FF (hexary number) / 11111111 (binary number)
3rd time: Write 00 (hexary) / 00000000 (binary)

4-Times

Erase the disk using a US Department of Defense standard compliant method (DoD5220.22-M). Use this if you need a higher level of security where residual magnetism is an issue. The processing time is 4 times longer.

1st time: Write AA (hexary) / 10101010 (binary)
2nd time: Write 55 (hex complement, AA complement) / 01010101 (binary)
3rd time: Write a random value
4th time: Write 00 (hexary) / 00000000 (binary)

* In order to comply with (DoD5220.22-M), perform the verification process by "Verify after erase".

Windows PE

For SSD drives, TRIM process is performed before the first erasure step when 2-4 times erasure is selected.

Windows PE

Verify after erase

After the erasing process is completed, read the whole disk and verify that all sectors have been erased. The processing time required for verification is about the same as the erasing process.

Stop when error
If a write error to the disk occurs in the middle, you can choose to interrupt the process or ignore it and continue.
If you ignore it and continue, the number of errors is counted.

Log(HDD)
After the erasing process is completed, write the processing log to the erased disk drive.
* This process is valid only when erasing in "erase Disk".

The written log file can be referenced by the following method.
* When you start the PC from the disk on which the log file is written, the log file is displayed on the screen (only when legacy/BIOS boot).
* Displayed by "Utility"/" Read HDD log" of "Boot up erase program".
* Use Windows "Utility for administrators" / "Disk log".

* Log files and small programs for starting and displaying logs are written in the first few sectors of the disk.
* If you perform a "Verify/read check" on the disk to which the log is written, only a few sectors will be counted as non-zero.
* Only the log part can be deleted by the above log file display utility.

Log(Removable)
After the erasure process is complete, write the process log to a removable drive such as FD or USB flash drive.
The removable drive targeted for log writing is a floppy disk drive or a removable drive (USB flash drive, etc.) of 128 Gbyte or less.

The file name will be [month][day][hour][minute][second].log based on the current time.

Log(NET)
After the erasure process is complete, the process log is written to a Windows shared folder on the network.
To enable it, use the "Startup Environment Creation Tool" and "Create WindowsPE Configuration File" to create "config.gp4" with network settings enabled, and save it in the same folder as "gppro4.exe".

By default, the file name is [month][day][hour][minute][second].log based on the current time.
It is also possible to add fixed values or user input values to the beginning of the file name.
For more information, see "Common options" of "Startup environment creatin tool".

Confirm

It is provided for confirmation so that it will not work even if you accidentally press the "execute ERASE" button.
Please enter "YES" ("yes" is also possible).

execute ERASE

Press this button to start the process.

Errors that can occur at the start

Disk is locked (Secure Locked)
Since the HDD password is set on the disk, read / write processing cannot be performed.
To cancel, use "Remove HDD Password" in "Boot up Erase Program"/"Utility".

Cannot lock drive/Cannot unmount drive
Cannot open drive
The specified drive / disk cannot be opened. Lock processing for exclusive use is not possible.
It is displayed when the program or file on the drive / disk is used by any process, including the case where the folder is displayed in Explorer.

For removable media such as USB flash drive, try removing it once. Check if the files are not used on the hard disk, including the service program in the background.

MEMO
If you get an error such as "Cannot lock", it is likely that one of the processes is accessing the file on that drive. It may be an antivirus or an explorer or other background process. To find out which process is accessing it, it is convenient to use "openfiles.exe" which comes standard with Windows.

1. Open "Command Prompt" with administrator privileges
2. execute
---
openfiles /local on

To enable openfiles.exe to monitor the file list

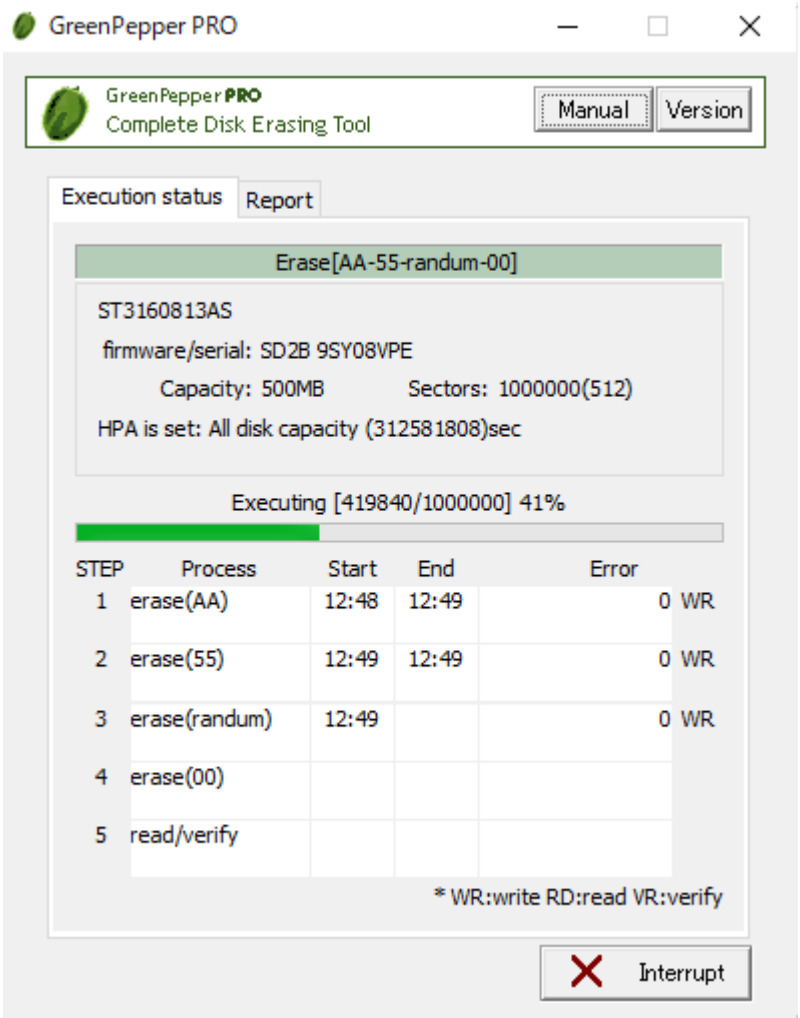
--- You need to restart your PC here to enable it.

3. After rebooting, open "Command Prompt" again with administrator privileges.
4. execute
---
openfiles /query | findstr -i "E:"
---
* Replace "E" with the drive name you want to check.
A list of processes using files on the specified drive will be displayed.
5. If you do not use openfiles any more
---
openfiles /local off

To disable monitoring.

Display during erasure

The following is displayed while the erase process is being executed.



You can check the start / end time of each erase and verification step, and the number of errors for each step.

WR: count of WRITE errors
RD: count of READ errors
VR: count of VERIFY errors

About the count of errors

The number of errors is counted for each of write, read, and verify.
The unit is the number of sectors per sector = 512 bytes.

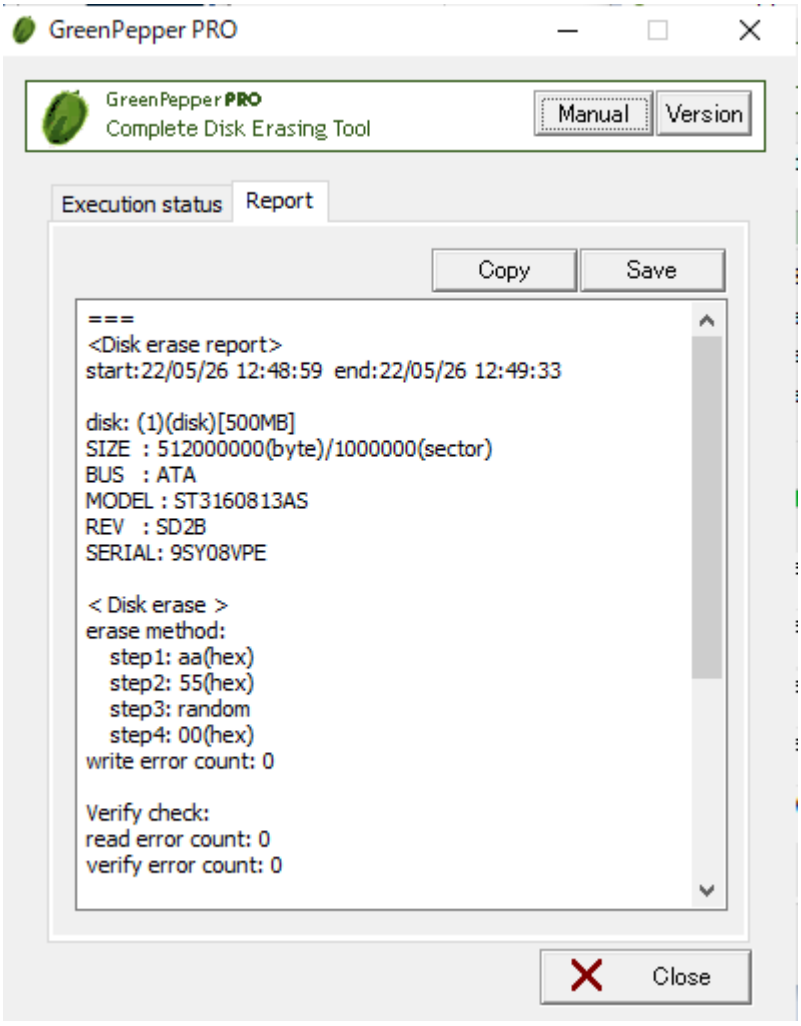
WRITE error	This is an error that occurred when writing. It is possible that this number x 512 bytes was not written (not erased) correctly.
READ error	Only when read verification is performed. This is the number of cases that could not be read. The contents of the disk are unknown for this number x 512 bytes. Even if a WRITE error has not occurred, READ may not be possible and a READ error may occur. This is a phenomenon that tends to occur on a failed disk.
VERIFY error	Only when read verification is performed. The number of sectors where the read data had a non-zero value. The part of the READ error is not included in the VERIFY error. Even if a WRITE error has not occurred, a VERIFY error may occur if the writing to the disk surface is not actually performed correctly. This is a phenomenon that tends to occur on a failed disk.

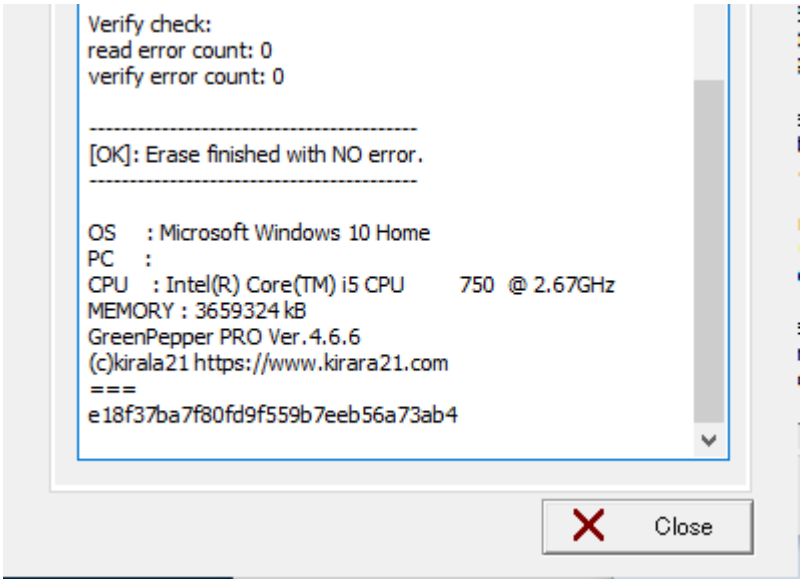
Interrupt

You can interrupt the process with the "Interrupt" button at the bottom right.

End Report

When the process is completed, the following "End Report" will be displayed.





Copy allows you to copy the content and paste it into another application (word processor, notepad, etc.).
"Save" allows you to save the contents to a file.
* You can switch between "Execution status" and end "Report" until you finish with the "Close" button.

About the checksum of the Report

===
<Disk erase report>
. . .
. . .
(c)kirala21 http://www.kirala21.com
===
5690773027bfdc37a502d404eba0eacc

As shown above, the "checksum" character string "5690773027bfdc37a502d404eba0eacc" (example) is added at the end.
This is to check that the content of the report is output by "Green Pepper PRO" and that no single character has been changed since then.
To check the checksum, use Windows "Utilities for Administrator"/"check log".

* Please handle the Report text in units of the contents between "===" (including itself) and the checksum character string on the next line.
* The checksum of the above sample is incorrect (security reason).

Close

Click the "Close" button to close the Report screen.

Windows PE

The "Secure Erase" page (tab) is only displayed when running on WindowsPE.
It is not displayed when executed on Windows (8, 10, 11, Server, etc.).

Secure Erase / Sanitize

Performs Secure Erase/Sanitize processing on supported disks. Please see "Secure erase/ Sanitize" for the details of the process.

Warning! About "Secure Erase" of ATA drives

Never interrupt Secure Erase process of ATA drives!

When performing Secure Erase on ATA drives (including SATA), according to Microsoft specifications,
"AutoATAWindowsString12345678901"
is registered as the HDD password (user password) before the process is executed.

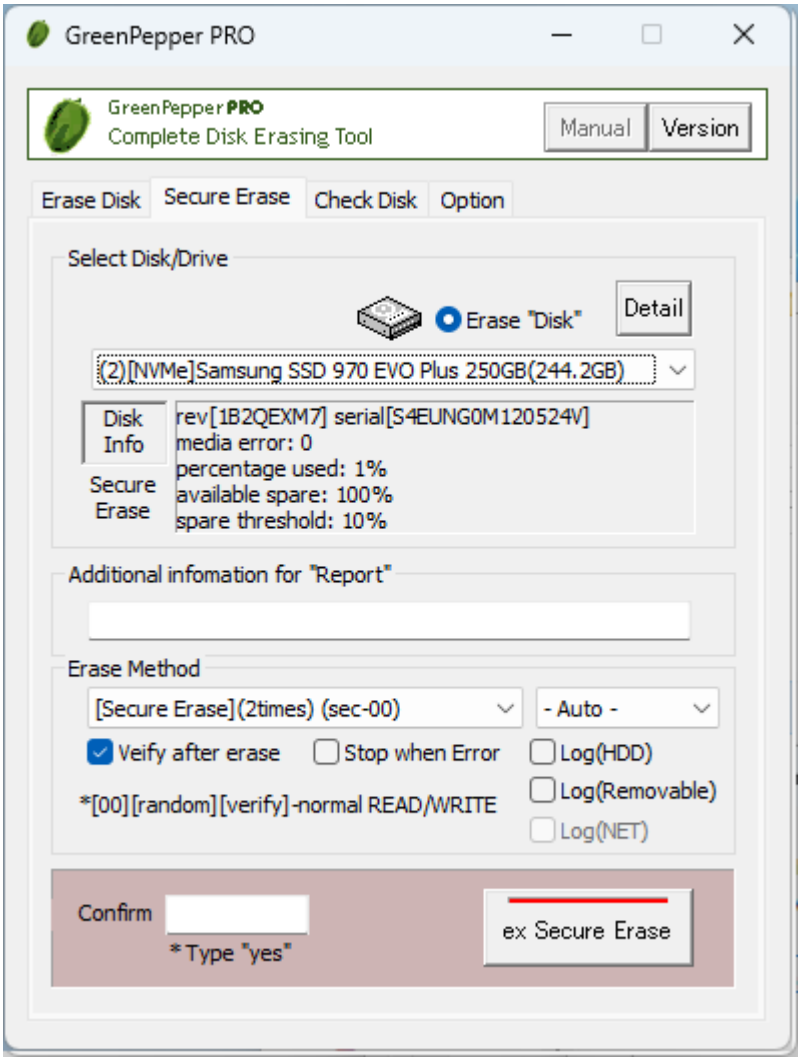
If the secure erase is successfully completed, the password will also be erased and you can use the disk drive as usual.
However, if it is interrupted midway (power off, etc.), the HDD password will remain on the drive and the drive will be password-locked. You will not be able to use it again, It becomes inaccessible.

If the HDD password is enabled, you will be asked to enter the password when you turn on the PC, and if the password does not match, you may not be able to boot or access the HDD. In that case, you may be able to remove the password by using the above password in the HDD password section of the PC's BIOS settings. But if the PC performs its own conversion of input values, in that case, you may not be able to cancel the password

How to remove HDD password
·Cancel it in the PC's BIOS settings.
·If the PC can start, perform the Secure Erase using this program (gppro4.exe) again.
·If the above is not possible, remove the drive from the PC, connect it to a PC that can boot even if there is an HDD password, and remove the password.
·**If the drive cannot be removed from a laptop PC, etc., it may become unusable.**

Due to these problems, please be very careful when performing Secure Erase of ATA.

Below, only the parts that differ from "Erase Disk drive" are described in detail.



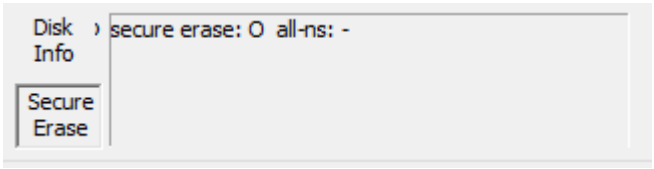
* If you format the disk again, you can use the disk again.

Select Disk to erase

Only processable(SecureErase/Sanitize) disk drives are listed. Select the disk drive (physical drive) to erase.

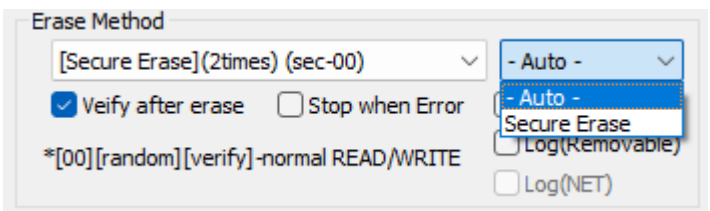
Disk information

Choose "erase Disk" and a select disk to display information about the disk.
Also, click on the "Secure Erase" section to display information about secure erase.
Click "Disk Information" to return to normal disk information display.



Erase method, options

Select the erasing method and processing option.



[Secure Erase](1time)(sec)
Only "Secure Erase"/"Sanitize" process is performed.

1st time: Secure Erase/Sanitize

[Secure Erase](2times)(sec-00)
Perform "Secure Erase"/"Sanitize" process and then write [00] to the whole disk drive.
2nd process is normal write process.

1st time: Secure Erase/Sanitize
2nd time: Write 00 (hexary) / 00000000 (binary)

[Secure Erase](3times)(sec-random-00)
Perform "Secure Erase"/"Sanitize" process and then write values to the whole disk drive as follows.
2nd, 3rd process are normal write processes.

1st time: Secure Erase/Sanitize
2nd time: Write a random value
3rd time: Write 00 (hexary) / 00000000 (binary)

Secure Erase Method
Normally, you can leave it as "-Auto-".
The process is executed using the most secure method among all executable processes.
You can also choose any method.

Only methods supported by the disk drive will be displayed as options.

Processing priority for "-Auto-"
ATA drive
Sanitize (block erase)
Sanitize (over write)
Sanitize (crypto)
Secure Erase (enhanced)
Secure Erase

NVMe drive
Sanitize (block erase)
Sanitize (over write)
Sanitize (crypto)
Secure Erase

However, if Sanitize (crypto) and Sanitize (block erase)/Sanitize (over write) are supported,
  Sanitize (crypto)+Sanitize (block erase)
  Sanitize (crypto)+Sanitize(over write)
is execute in combination.

Verify after erase
After the erasing process is completed, read the whole disk and verify that all sectors have been erased.
This process is normal read process.

Stop when error
If a write error tf a write error to the disk occurs in the middle, you can choose to interrupt the process or ignore it and continue. If you ignore it and continue, the number of errors is counted.
Error counts are for normal read/write process only.

Confirm

It is provided for confirmation so that it will not work even if you accidentally press the "execute ERASE" button.
Please enter "YES" ("yes" is also possible).

execute ERASE

Press this button to start the process.

Interrupt

You cannot interrupt during the secure erase step.
For normal read/write process, you can interrupt the process with the "Interrupt" button at the bottom right.

Close

Click the "Close" button to close the Report screen.

Errors that may occur during the secure erase process

Secure Erase - ATA(SATA)

Error Code	Description
-3	Frozen state
-2	Secure Erase not supported
-1	Secure Erase not supported
1	Open error for the Disk
2	Disk identify error
3, 4, 6	Error when removing HDD password The currently set password is different from the Windows standard password (*), or the password cannot be reset.
5, 9	Disk identify error
7, 8, 10	Error when removing HDD password The currently set password is different from the Windows standard password (*), or the password cannot be reset.
15, 16, 17 18, 19, 20	Error when setting HDD passowrd Tried to set a password for secure erasure, but an error occurred.
25	Secure Erase preparation error
26	Secure Erase Test error
28	Secure Erase preparation error
30	Secure Erase execution error
31	Secure erasure process completed in much shorter time than expected
32	Confirmation error after Secure Erase process *Password cannot be deleted
40	Disk open error, after Secure Erase. (SecureErase is finished)
41	Disk open error, after Secure Erase. (SecureErase is finished in much shorter time than expected)
42	Disk identify error (SecureErase is finished)

*Windows standard password "AutoATAWindowsString12345678901"

Sanitize - ATA(SATA)

Error Code	Description
-8	BLOCK ERASE is not supported
-7	OVERWRITE is not supported
-6	CRYPT ERASE is not supported
-5	Unsupported erase type
-4	Sanitize is not supported
-3	Disk identify error
-2	Disk open error
1	Error getting Sanitize status
2	Sanitize frozen state
3	Sanitize is executing
10	Sanitize execution error (CRYPTO_SCRAMBLE)
11	Sanitize execution error (OVERWRITE)
12	Sanitize execution error (BLOCK_ERASE)

Secure Erase - NVMe

Error Code	Description
-10	Secure Erase(format) execution error
-8	Memory allocation error
-7	Disk identify(identify ns) error
-4	Secure Erase (format) is not supported
-3	Disk identify error
-2	Disk open error
>0	Secure Erase processing error

Sanitize - NVMe

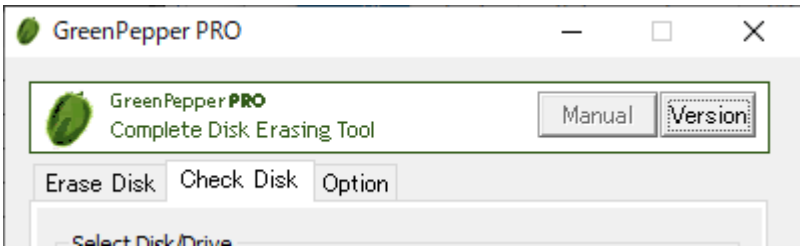
Error Code	Description
-10	Sanitize execution error
-9	Memory allocation error
-8	Sanitize is executiong
-7	OVERWRITE is not supported
-6	BLOCK ERASE is not supported

-5	CRYPT ERASE is not supported
-4	Sanitize is not supported
-3	Disk identify error
-2	Disk open error
>0	Sanitize processing error

Check disk

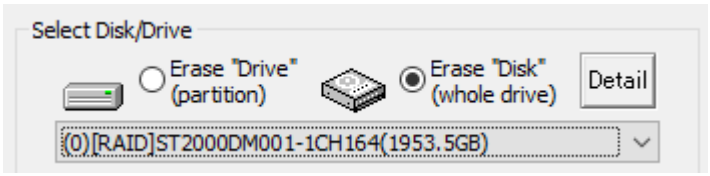
"Check Disk" checks the reading of hard disk, floppy disk, memory card, etc. connected to the Windows PC.
It can be used to check if there are any read failures on the disk, and to check if all the data on the disk is zero after erasing.

*"Disk" refers to a whole physical disk unit.
*"Drive" refers to a partition within a disk drive. Usually a drive letter "A"-"Z" is assigned.



* This function is equivalent to "Verify after erase" when "Erase disk".
* This process does not change any data on the disk / drive.
* You may also be able to check the system drive (C: drive, etc.).

Select Disk / Drive



Select whether to check on a drive (C,D,..., a partition) or on a whole physical disk.

Windows10/11 etc.

check Drive

In Windows, drive letters such as A, C, D, etc. are basically assigned to each disk (whole physical disk) for removable disks (such as floppy disks ,USB flash drives), and to each partition for hard disk drives.
If you want to check this drive unit, select "check Drive".
* on WindowsPE, you cannot select "check Drive"

Windows10/11 etc.

check Disk

For hard disk drives, etc. (include removable drive), you can check entire disk regardless of the partition state. In that case, all data on the disk, including partition information, will be checked.

* For a single disk, it is a physical disk unit, and for a RAID configuration, it is a logical disk unit.

Disks with no drive letter assigned or unformatted disks can also be selected.

Select Drive / Disk to check

After specifying "check Drive" or "check Disk", select the drive/disk to check.

Disk information

See "Erase Disk".

Disk Detail information

See "Erase Disk".

Additional information for "Report"

See "Erase Disk".

Options

Select processing option.

Stop when error
If a read error to the disk occurs in the middle, you can choose to interrupt the process or ignore it and continue.
If you ignore it and continue, the number of errors is counted.

Stop when non-zero
The disk is read sequentially, and if there is a non-zero location, the process is interrupted.
If it is not interrupted, it will be counted up and displayed as VR (Verify Error).

However, if you select "Compare with 1st sector" in the following options, it will be compared with the contents of the first sector instead of zero, and if there is a difference, interruption / VR(verify error) count up will be performed.

Compare with 1st sector
Checks if the contents of the disk are the same as the contents of the first sector.
This is used to verify a disk that has a specific pattern written on it, rather than zero. In "Enhanced Secure Erase", a specific pattern may be written.
First, the first sector (512 bytes) is read, and the subsequent sectors are compared in units of 512 bytes.
The count displayed as VR (Verify Error) is the number of sectors with different contents from the first sector.

Execute CHECK

Press this button to start the process.

Errors that can occur at the start

Disk is locked (Secure Locked)
Since the HDD password is set on the disk, read / write processing cannot be performed.
To cancel, use "Remove HDD Password" in "Boot up Erase Program"/"Utility".

Cannot lock drive / Cannot open drive
The specified drive / disk cannot be opened. Lock processing for exclusive use is not possible.
It is displayed when the program or file on the drive / disk is used by any process, including the case where the folder is displayed in Explorer.

For removable media such as USB flash drive, try removing it once. Check if the files are not used on the hard disk, including the service program in the background.

Display during erasure

You can check the start / end time and the number of errors.

RD: count of READ errors
VR: count of VERIFY errors

About the count of errors

The number of errors is counted for each of read, and verify.
The unit is the number of sectors per sector = 512 bytes.

READ error	This is the number of cases that could not be read. The contents of the disk are unknown for this number x 512 bytes.
VERIFY error	Only when read verification is performed. The number of sectors where the read data had a non-zero value. Or not same as the 1st sector, when "Compare with 1st sector" is selected. The part of the READ error is not included in the VERIFY error.

Interrupt

You can interrupt the process with the "Interrupt" button at the bottom right.

Report

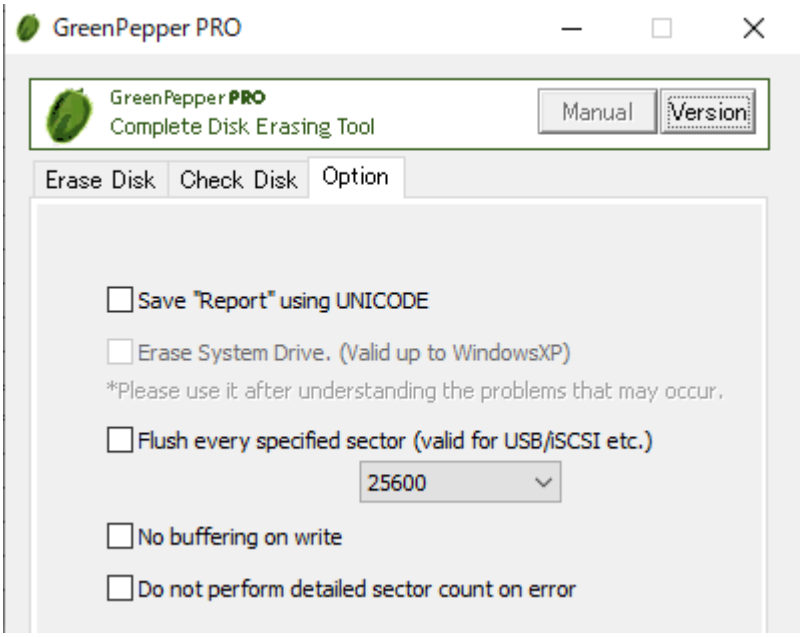
When the process is completed, the following End "Report" will be displayed.
For details, see "erase Disk".

Close

Click the "Close" button to close the Report screen.

Option

On the "Option" page, specify processing options for "Erase Disk" and "Check Disk".



Option specification

Save "Report" using UNICODE

When saving the report at the end of processing with the "Save" button, save it with UNICODE (UTF-16).
"BOM (Byte Order Mark)" is added to the beginning, and you can open it as it is with Notepad on Windows.
If you do not specify this option, it is saved with ANSI.

Erase system drive

In normal "Erase Disk", the Windows system drive and the disk including the Windows system drive cannot be selected.
This option is intended to allow erasing even if it is recognized as a system drive.

However, this option is only available for WindowsXP and earlier.

If you specify this option to erase the system drive, you may be able to erase "some" of the disk.
However, Windows may stop or some data may remain.

Flush every specified sector (Effective for USB/iSCSI etc.)

In normal erasing, the entire disk is written continuously.
When this option is specified, the writing contents are flushed to the disk for each processing of the selected number of sectors.
The processing speed will be slower, but continuous writing may not be performed correctly unless this option is specified, especially for disks / memory connected via USB / iSCSI.

No buffering on write

In normal erasing, Windows buffers when writing, causing a delay in writing to disk.
If you have problems with normal write operations, you may be able to work around the problem by specifying this option.
The processing speed will be slightly slower.

Do not perform detailed sector count on error

If a write / read error occurs during erasure / check, normally, a retry is attempted in detail for each sector, and the error is counted for each sector.
If this option is specified, each larger processing unit will be treated as an error and counted.
For drives with a lot of errors, this will speed up the process.

Setting initial and fixed values using the command line

Command line option details

In "Windows Erase Program", you can set the initial value and fix the value by using the command line at startup of "gppro4.exe".

Example:
gppro4.exe /M:3E /R:InfoDep. /T:E

Specify options by configuration file

By putting the "config.gp4" file in the same folder as gppro4.exe, you can specify the same contents as the command line.
"config.gp4" is a text file (ANSI) with the contents of the command line.

Example: contents of "config.gp4"

/M:3E /R:InfoDep. /T:E

Using with WindowsPE environment

When using gppro4.exe on WindowsPE, you can also perform automatic deletion operations, specify Secure Erase operations, specify network logs, etc. on the command line or configuration file (config.gp4).
The "WindowsPE configuration file" (config.gp4;contains command line options) used in this case can be created using the "Startup Environment Creation Tool'' (gpset4.exe) -"Create WindowsPE Configuration File''.

Item	How to specify	Description
Specify the Drive to be erased ("erase Drive/partition")	/d:[Drive specification] *specifying the initial value	A,B,C,D,・・・,Z: Specify drive RM: Specify 1st removable drive HD: Specify 1st HDD drive, exclude system drive If only "/d:" is specified, the initial value is "erase Drive".
	/D:[Drive specification] * Fixed at the specified value, cannot be changed	Same as above If only "/D:" is specified, "erase Drive" is fixed, cannot be changed.
	ex: /d:f /D:E /D:RM /D:	
Specify the Disk to be erased ("erase Disk/whole drive")	/p:[Disk specification] *specifying the initial value	0.1.2.3.・・・: Specify disk. RM: Specify 1st removable disk HD: Specify 1st HDD disk, exclude system drive. If only "/p:" is specified, the initial value is "erase Disk".
	/P:[Disk specification] * Fixed at the specified value, cannot be changed	Same as above If only "/P:" is specified, "erase Disk" is fixed, cannot be changed.
	ex: /P:1 /P:RM	
	/m:[1,2,3,4][E][V][H][Z][C] *specifying the initial value (WindowsPE only) [6,7,8][L][N][R]	1-4: Erase count 1-4 times E: Stop when error V: Verify after erase H: Log(HDD) Z: Stop when non-zero C: Compare with 1st sector
		WindowsPE
		6-8: Erase count for Secure Erase 6: sec(1time) 7:sec+1(2times) 8:sec+2(3times) L: Log to removable drive(USB flash drive) N: Log to network share R: Verify after erase, for Secure Erase
		Items not specified below are not fixed

Erase method	/M:[1,2,3,4[E][e][V][v] [H][h][Z][z][C][c] * Fixed at the specified value, cannot be changed	1-4: Erase count 1-4 times E: enable - "Stop when error" e: disable - "Stop when error" V: enable - "Verify after erase" v: disable - "Verify after erase" H: enable - "Log(HDD)" h: disable - "Log(HDD)" Z: enable - "Stop when error" z: disable - "Stop when error" C: enable - "Compare with 1st sector" c: enable - "Compare with 1st sector"
	(WindowsPE only) [6,7,8][L][l][N][n][R][r]	WindowsPE
		6-8: Erase count for Secure Erase 6: sec(1time) 7:sec+1(2times) 8:sec+2(3times) L: enable - Log to removable drive l: disable - Log to removable drive N: enable - Log to network share n: disable - Log to network share R: enable - Verify after erase, for Secure Erase r: disable - Verify after erase, for Secure Erase
	ex: /M:3EVHe	
	/s:[1,2,3,4][V] *specifying the initial value	<u>Initial value when the drive is an SSD</u> 1-4: Erase count 1-4 times V: Verify after erase
	(WindowsPE only) [6,7,8][R]	WindowsPE
		6-8: Erase count for Secure Erase 6: sec(1time) 7:sec+1(2times) 8:sec+2(3times) R: Verify after erase, for Secure Erase
	/S:[1,2,3,4][V][v] * Fixed at the specified value, cannot be changed	<u>Fixed value when the drive is an SSD</u> 1-4: Erase count 1-4 times V: enable - "Verify after erase" v: disable - "Verify after erase"
	(WindowsPE only) [6,7,8][R][r]	WindowsPE
		6-8: Erase count for Secure Erase 6: sec(1time) 7:sec+1(2times) 8:sec+2(3times) R: enable - Verify after erase, for Secure Erase r: disable - Verify after erase, for Secure Erase
Erasure Pattern	/E:[P1],[P2],[P3],[P4]:[t]	Erasure Pattern for 1-4times erasure. *If you use the default value, specify only ",". [P1]: for 1-time, Two hexadecimal digits. "RD" for random. [P2]: for 2-times, Two+Two hex digits. "RD" for random. [P3]: for 3-times, Two+Two+Two hex digits. "RD" for random. [P4]: for 4-times, Two+Two+Two+Two hex digits. "RD" for random. If you do not want to perform TRIM on the SSD, add ":t".
	ex: /E:00,AA,00,RDRD00,AAFFRD00 /E:,,RDRD00,:t	
Additional information for "Report"	/R:"[additional information]" * same as /r	"" is not required if spaces are not included.
	ex: /R:"my report info" /R:MyReport	
WinPE Additional information Item	/i1:"[Item1]" /I2:"[Item1]" /i2:"[Item2]" /I3:"[Item2]"	i1,i2: specify item name I1,i2: specify item name, make it "input required". up to 16 single-byte alphanumeric characters (spaces allowed)
	ex: /I1:"PC name" /2:USERID	
	/o:[U][S][C1-5][E][B] *specifying the initial value	U: Save "Report" using UNICODE S: Erase system drive C1-5: Flush every specified sector C1: 256, C2: 2560, C3: 25600 C4: 256000 C5:

Option			2560000 B: No buffering on write E: Do not perform detailed sector count on error
		/O:[U][S][C1-5][E][B] * Fixed at the specified value, cannot be changed	Same as above
		ex: /O:C3 /O:UC3E	
Specifying page (tab) display		/T:[E][C][O] * same as /t	E: "Erase disk" page C: "Check disk" page O: "Option" page
		(WindowsPE only) [S]	WindowsPE
			S: "Secure Erase" page
		ex: /T:E /T:CO	
Button display on the report screen when erasing and disk check processing is completed		/F:[C][S][Ftext to Display] * same as /f	C: If specified, hide the "Copy" button S: If specified, hide the "Save" button FIf [text to Display] is specified, replace the text of the "Confirm" button with the specified text.
		ex: /F:CSFclose /F:S	
WinPE	Network specification	/N:server=[server],share=[share], directory=[directry],userid=[userid], password=[pass], passwordc=[pass_encrypt], fnformat=[format],fnprefix=[prefix]	[server]: IP address (ipv4) of the server [share]: share name [directry]: folder name to save log [userid]: user name to connect to the share [pass]: password to connect to the share (plain text) [pass_encrypt]: encrtpted password *Specify either [pass] or [pass_encrypt] *Set the encryption password using the "Start up Environment Creation Tool" (gpset4.exe). [format]: 0:default, 1:fixed prefix, 2: use addtional info1 as prefix, 3: use addtional info2 as prefix [prefix]: fixed prefix value
		ex: /N:server=192.168.0.1,share=erase,userid=test,password=testpass	
WinPE	Auto-Execution	/AUTO	Automatic Erase process execution. Start erase processes for the number of disk drives and perform parallel erasing. (up to 9 disk drives) Final confirmation "yes" input and operation of "Execute Erase" button are required.
		/AUTOPASS:[passwrod]	Auto erase with password. After startup, a password entry screen will be displayed. If the value specified in [Password] is entered correctly, automatic execution will be performed in the same way as "/AUTO".
		/AUTOPASSTTL:[Title] /AUTOPASSCM1:[Comment1] /AUTOPASSCM2:[Comment2] /AUTOPASSCM3:[Comment3] /AUTOPASSCM4:[Comment4]	Spesify with "/AUTOPASS" Specify the display text on the initial password input screen.
		/AUTOBUTEXEC	Use with /AUTO or /AUTOPASS Omit the input of "yes" to confirm erasing, and start erasing only by pressing the "Execute erase" button. *If automatic execution is specified with the "Start up Environment Creation Tool" (gpset4.exe), this specification will be used.
		/AUTOFULLEXEC	Use with /AUTO or /AUTOPASS Entering "Yes" to confirm erasing and clicking the "Execute deletion" button are also omitted. Start erasing at startup without user interaction.

How to run "gppro4.exe" in Windows PE environment using "System Repair Disc" (easy way)

If you want to create a WindowsPE execution environment that boots from a CD/USB flash drive and automatically launches the erase program, you need to use the method described in "Building WindowsPE boot environment" below.
However, if you want to start the erase program and erase manually in a Windows PE environment, you can do it easily by following the steps below.

Create "System Repair disc" on Windows10/11

This can be done from "Control Panel" -> "Backup and Restore".
Please see the Windows manual for detailed instructions.

Boot your PC with the "System Repair Disc"

·After booting with the "System Repair Disc", select "Command Prompt" from the screen.
·Replace the "System Repair disc" with a CD containing the Windows erasure program "gppro4.exe", or insert a USB flash drive containing "gppro4.exe".
·Run "gppro4.exe" from the CD or USB flash drive at "Command Prompt".

* Normally, the drive assignments is as shown below. However, depending on the system.

X: Windows system deployed in memory
C: Internal disk drive
D:,E:,F: etc. CD drives, USB flash drives, etc.

Example:
If the USB flash is the D: drive and "gppro4.exe" is in the root folder of the USB flash drive, enter the following to start it.

D:\gppro4.exe

Building WindowsPE boot environment

In order to use the "Windows Erase Program" (gppro4.exe) in a WindowsPE environment, you must create the WindowsPE environment yourself.
Below are the steps for the latest version (10.0.226.21.1) as of August 2023.
For other versions, the steps may be different.

Note on WindowsPE

WindowsPE is an OS that is highly compatible with Windows and is provided free of charge by Microsoft, but it is for temporary use, including disk erasure.
Therefore, if continuous use exceeds 72 hours, it is designed to automatically stop. Please be careful when erasing large size disks.
Please see Microsoft's website for details.

Download/install WindowsPE environment

Download
Download "Windows ADK for WindowsXX" and "Windows PE Add-on" from the Microsoft site.

Install ADK, WindowsPE Add-on
When installing "Windows ADK", it is necessary to enable [Deployment tool] feature.
*Even if all other options are OFF, it will still work for this purpose only.
After installing "Windows ADK", install "WindowsPE Add-on".

Creating a base WinPE image

Run "Deployment and Imaging Tools Environment"
From start menu, find [Windows Kits]->[Deployment and Imaging Tools Environment], run it as Administrator.

Create base WinPE image

At the [Deployment and Imaging Tools Environment] command prompt, run the following command.
The files required to run WindowsPE will be created under the specified folder.

```
copype amd64 C:\WinPE_amd64
```

amd64: Specifies the construction of a 64-bit environment.
Windows PE equivalent to Windows 11 only provides a 64-bit environment.
*When building in a 32-bit environment with an earlier version, it will be "x86".

"C:\WinPE_amd64": Created under this folder. Any folder can be specified.
*This folder name will be used in the following explanation.

Configure WinPE image and embed the program

Run "Deployment and Imaging Tools Environment"

From start menu, find [Windows Kits]->[Deployment and Imaging Tools Environment], run it as Administrator.

Mounting WinPE boot disk image file

At the [Deployment and Imaging Tools Environment] command prompt, run the following command.
By mounting, the contents of the boot disk image file [boot.wim] can be accessed under the [mount] folder.

```
Dism /Mount-Image /ImageFile:"C:\WinPE_amd64\media\sources\boot.wim" /index:1
/MountDir:"C:\WinPE_amd64\mount"
```

Adding required packages and drivers

At the [Deployment and Imaging Tools Environment] command prompt, run the following command.
Add the necessary packages to run "gppro4.exe".

*In the standard state, disk drivers and network drivers for general desktop and notebook PCs are included, but if you need additional drivers for servers etc., install them here.

required package
·WMI WinPE-WMI.cab

```
Dism /image:C:\winPE_amd64\mount /add-package /packagepath:"C:\Program Files
(x86)\Windows Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-WMI.cab"
```

If you need to add drivers.

```
Dism /Add-Driver /Image:"C:\WinPE_amd64\mount" /Driver:"C:\SampleDriver\driver.inf"
```

Specify the required driver file (*.inf) in the "C:\SampleDriver\driver.inf" part.

Time zone and keyboard settings

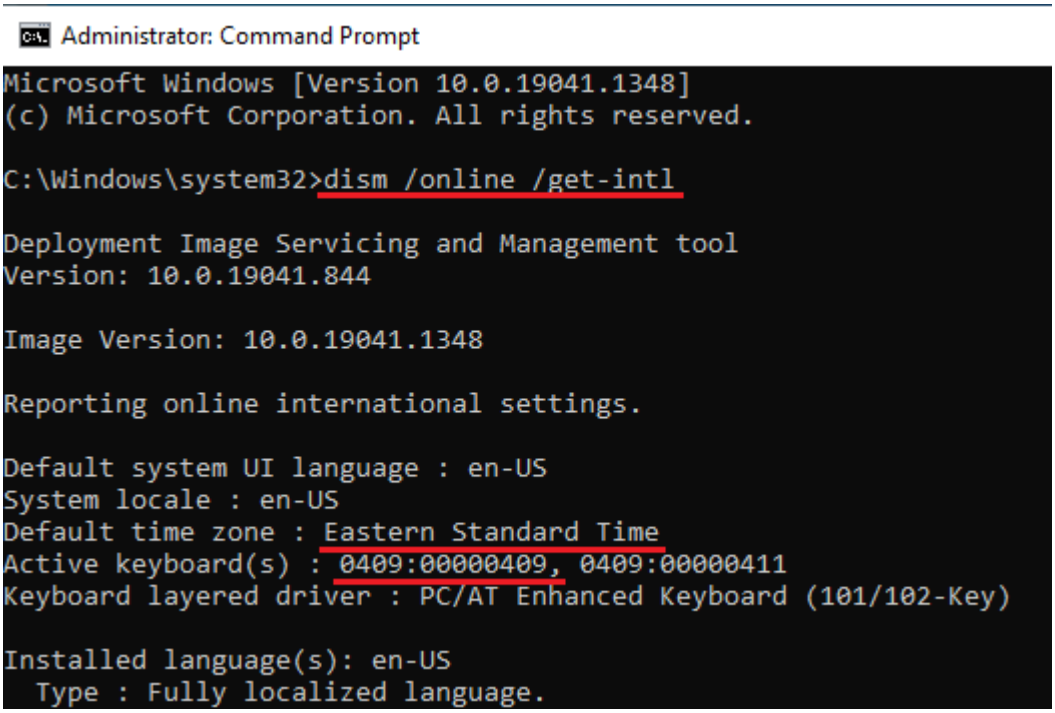
At the [Deployment and Imaging Tools Environment] command prompt, run the following command.

```
Dism /image:C:\winPE_amd64J\mount /Set-Timezone:<Time zone name>
Dism /image:C:\winPE_amd64J\mount /Set-InputLocale:<input_locale>:<keyboard_layout>
```

You can check the current timezone and locale:keyboard settings using the following command.

```
Dism /Image:"C:\WinPE_amd64\mount" /Get-intl
```

The timezone and locale:keyboard_layout values that should be set can be obtained from the PC currently used for configuration using the following method.
*"/online" indicates the currently running Windows,
and "/image" indicates the specified Windows image file.



If you want to set it up like in the example above, run the following command.

```
Dism /image:C:\winPE_amd64\mount /Set-Timezone:"Eastern Standard Time"
Dism /image:C:\winPE_amd64\mount /Set-InputLocale:0409:00000409
```

Embedding "gppro4.exe"
Perform the steps below with the boot disk image file [boot.wim] mounted.

"C:\WinPE_amd64\mount\program files"

Copy the following to this folder. (Copy with regular Windows Explorer)

gppro4.exe : "Windows Erase program". **For 64bit WindowsPE, use the 64bit version "gppro4.exe"**.
config.gp4 : Configuration file created using the "Startup Environment Creation Tool"/"Creating WindowsPE configuration File". (Copy required only if used)
license.gp4 : License file required when using "gppro4.exe"

Settings for automatic execution of the program ("gppro4.exe")
Perform the steps below with the boot disk image file [boot.wim] mounted.

"C:\WinPE_amd64\mount\Windows\System32"

Create a text file named "Winpeshl.ini" in this folder.
Write the following as the contents of the file.
*Please be careful not to add ".txt" etc. to the end of the file name.

```
[LaunchApps]
startnet.cmd
"%systemdrive%\Program Files\gppro4.exe"
wpeutil shutdown
```

Unmounting WinPE boot disk image file
At the [Deployment and Imaging Tools Environment] command prompt, run the following command.

```
Dism /unmount-image /mountdir:C:\WinPE_amd64\mount /commit
```

If you change the contents of the boot disk image file [boot.wim], be sure to unmount and close the boot disk image file.
Before unmounting, please make sure that no other program is accessing the folder under "mount".
It is also not possible to open the folder in Explorer.

If an error occurs when unmounting, please do the following command.
In that case, mount it again and check the contents.

Dism /unmount-image /mountdir:C:\WinPE_amd64\mount /discard

Creating a bootable CD image file, configuring a bootable USB flash drive

CD Image file

At the [Deployment and Imaging Tools Environment] command prompt, run the following command.
*WinPE boot disk image file must be UNmounted.

```
MakeWinPEMedia /ISO C:\WinPE_amd64 "C:\anyfolder\WinPE_amd64.iso"
```

Here, "c:\anyfolder\WinPE_amd64.iso" is the output CD image file name. Please specify any file.
Create a CD-R from the created ISO file. See "How to create a CD from an image file".

USB flash drive

At the [Deployment and Imaging Tools Environment] command prompt, run the following command.
*WinPE boot disk image file must be UNmounted.

```
MakeWinPEMedia /UFD C:\WinPE_amd64 X:
```

Here, replace "X:" with the drive letter of the USB flash drive to be written.

Abstract of "Startup environment creation tool"

The "Startup Environment Creation Tool" is a tool for creating an environment for starting and executing the "Boot up Erase Program" and creating a configuration file when running the "Windows Erase Program" on WindowsPE.
Use this program to distribute the erasure program to general users in your company.

Also, if you want to **use the network log function**, you need to create a boot environment/configuration file using this program.

The boot environment/configuration file that can be created by this program is as follows.

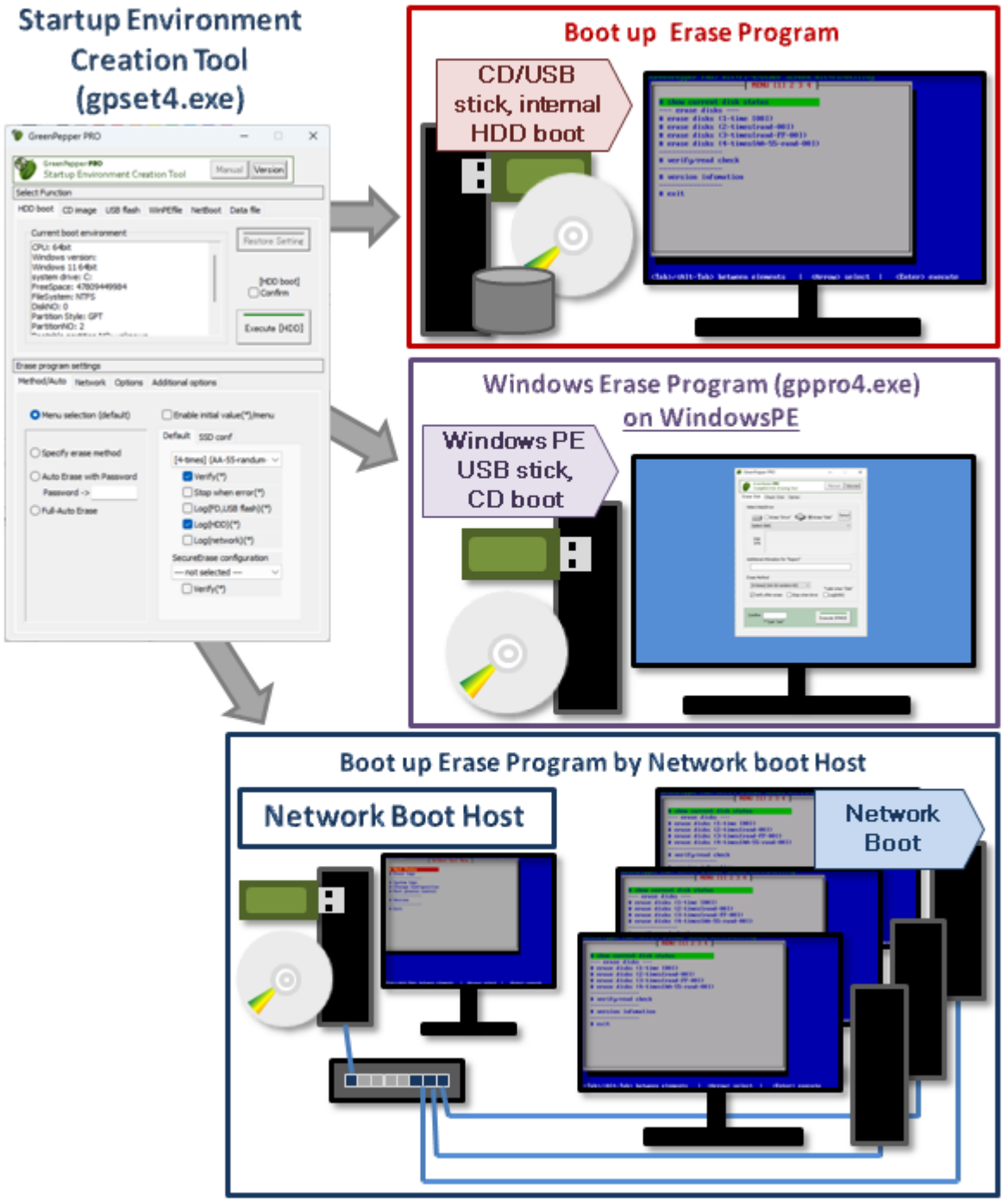
Hard disk (HDD) settings
Execute the "Startup Environment Creation Tool" **on the PC you want to erase**, and install the "Startup Erase Program" on the system hard disk of that PC.
When you restart your PC, the "Boot up Erase Program" will start and you can erase the hard disk of that PC.

Create bootable CD image file
Create a CD-ROM image file (ISO9660 format) that can start the "Boot up Erase Program".
By writing this file to a CD-R, it becomes a bootable CD.

Setting bootable USB flash drive
This is a process to incorporate a "Boot up erase program" into a commonly available USB flash drive.
You can start the PC from the set USB flash drive and use the "Boot up Erase Program".

Creating WindowsPE configuration file
Create a configuration file to enable automatic execution, specify processing methods, and use network logs when running the "Windows Erase Program" on Windows PE.
It becomes effective by installing the created configuration file in the same folder as "gppro4.exe" in the WindowsPE execution environment.

Creating a network boot host (CD image, USB flash drive settings)
*"Site License"/"Company License" is needed to use.
* With "Single user license", the program is executed in evaluation mode.
* A network boot data file (gpdataost.pac) is required for execution.
You can create a host function to use the erase program with network boot (PXE).
By using the CD or USB flash drive created with this function and starting the PC, you can use it as a host PC.



Distribution of erasing environment within the company

When distributing the erasing environment within the company using each function, the following methods are possible.
When distributing, you can use the "Customizing/Setting data file" and "Customizing/setting by command line" functions to unify the erasing method, etc. within the company, and reduce the learning burden of general users' operations.

* A corporate license, etc. are required to distribute in your company.

Using "Operation of 'HDD boot'"

Allow general users to run the "Startup Environment Creation Tool" (gpset4.exe) using the network drive of the company server.
The user can launch the program, embed it on the disk of the PC, and then erase it.

Using "Creating bootable 'CD image' file

Create a CD-ROM image (ISO9660 format) with appropriate options set in the management department in

advance.
Create a CD-R and distribute the CD-R itself, or distribute the CD image file on a network drive, intranet, etc.
If distributed as an image file, users can create a CD-R and erase HDD drives with it.
"Startup environment creation tool" is not required for users.

Using Setting "bootable 'USB flash drive'"

Setting USB flash drive with appropriate options set in the management department in advance and distribute the USB flash drive itself.

In order to allow users to set the USB flash drive by themselves,
allow general users to run the "Startup Environment Creation Tool" (gpset4.exe) using the network drive of the company server. In this case, we recommend using the "Customizing/Setting data file" function to fix the available tab pages and setting items.
The user can launch the program, setting USB flash drive, and erase HDD drives with it.

You can also distribute the USB boot environment using the following method.
However, only UEFI booting is supported (BIOS/Legacy booting is not possible) by this method.
* Compress a set of internal files of the configured USB flash drive into a zip file. Save it to a file server.
* The user must format the USB memory in FAT/FAT32 (NTFS, exFat is not possible). Extract the contents of the zip file and copy to the USB memory.

Distributing WindowsPE boot images

CD image files can be distributed in the same way as "bootable CD image" above.
The USB memory itself will be distributed as the configured USB memory.

Centralized erasure task using network boot host

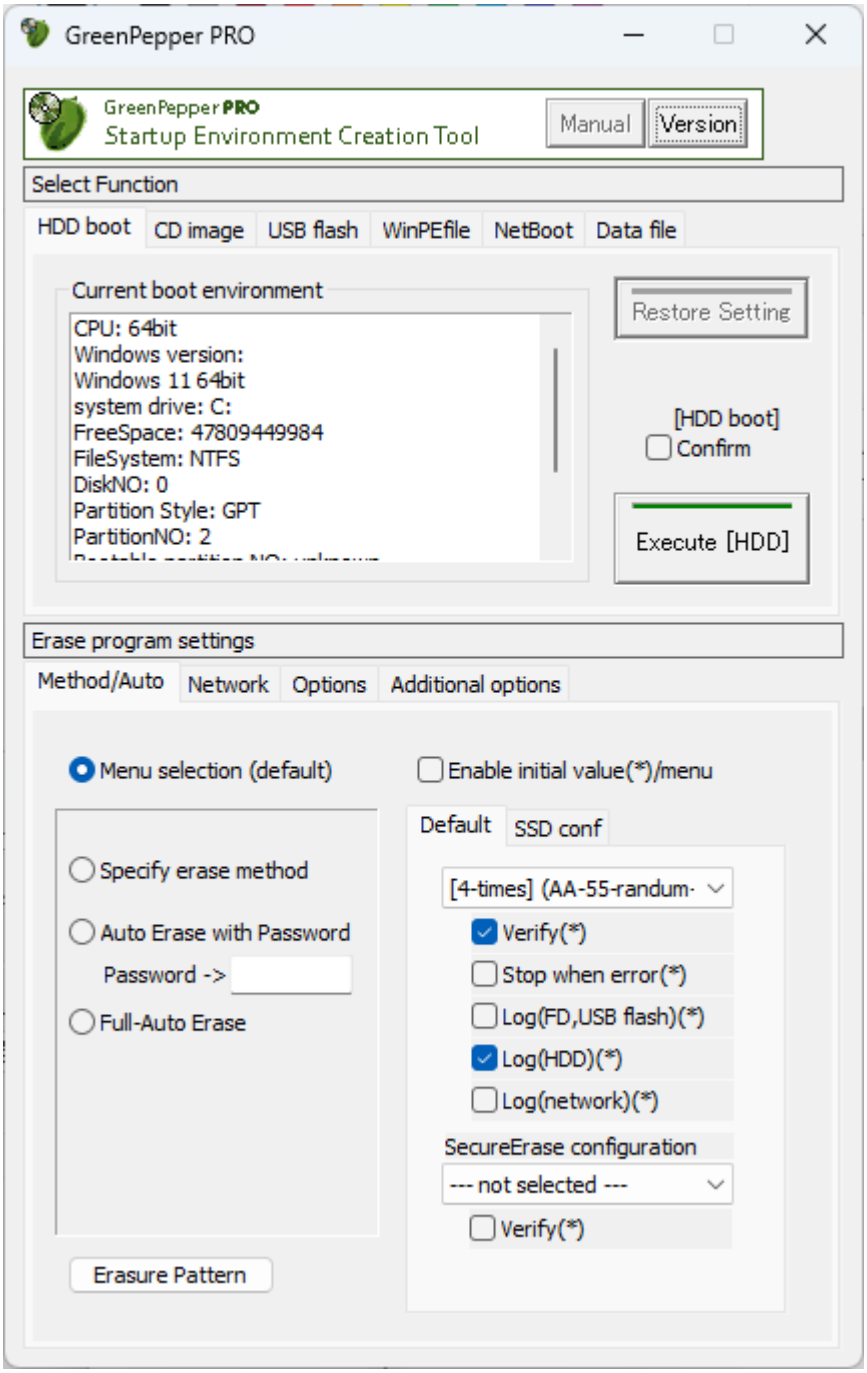
A network boot host that can be booted using only a CD/USB flash drive has the following functions:
·Host function for network boot
·Loading the erase program on network booted PC's
·FTP server for the erasure program to write logs
·NTP server for time synchronization with network booted PC's

Even if there are dozens or hundreds of PCs to be erased, simply by connecting them to the network, you can start the erasure program over the network and leave the erasure log on the host PC. There is no need to prepare media such as CDs or USB flash drive.
Furthermore, by using "gputil4.exe"'s "log conversion" function, a large number of log files can be converted into a TEXT(CSV) file at once, making it easier to manage them in databases, etc.

Executing "Startup environment creation tool"

The "Startup Environment Creation Tool"(gpset4.exe) that runs on Windows can be easily started and executed without any installation work.
* You can boot directly from a CD-ROM, network folder, etc.

***License file "license.gp4" is requierd in the same folder as "gpset4.exe".**



Double-click [gpset4.exe] to start it

· For online download, it is in the unzipped folder.
· If provided on a CD-ROM, it is located on the product CD-ROM (root).

You can boot directly from the product CD-ROM, or copy it to a hard disk, network drive, etc. for use.

Confirmation of "Data file" existence

The "Data file" (gpdata.pac) is required in the same folder as gpset4.exe or in the [data] folder at the same level as gpset4.exe.

* You can also specify a data file in another location. See "Customizing/setting by command line" for details.

In addition, when using the "netboot" function, the network boot data file (gpdatahost.pac) is also required.

"Data file" type

There are the following three types of "Data file"s.
[1]. Not supports network log ... When network log is not needed.
[2]. Supports network log (LAN, USB-LAN) ... When using only LAN(wired) for network log.
[3]. Supports network log (LAN, USB-LAN, WiFi) ... When using LAN, WiFi for network log.

It is also possible to use the "Data file"s of [2] [3] and not use the network log.
Therefore, if you always use the data file of [3], you will be able to select all the functions.
However, the size of the data file becomes large as [1] <[2] <[3], and it takes time to transfer the data file, especially when the setting environment is distributed via the network.
Therefore, please use the necessary "Data file" according to the function to be used.

For the type of data file you are currently using, see the version information displayed by the "Version" button.
* See "Data file version" below.

"Data file"location · For online download, it is in the unzipped folder. · If provided on a CD-ROM, it is located on the product CD-ROM (root).	File size	Settings that do not use the network	Settings using LAN, USB-LAN (wired)	Settings using Wi-Fi, LAN, USB-LAN
[1]gpdata.pac.nonet * If you want to use it, you need to rename it to "gpdata.pac".	small	*		
[2]gpdata.pac.net * If you want to use it, you need to rename it to "gpdata.pac".	medium	*	*	
[3]gpdata.pac	large	*	*	*

*There is only one type of network boot data file (gpdatahost.pac).

Administrator privileges required to run

Vista/7/2008 or later (include Windows10)

The following message will be displayed.

Do you want to allow this app to make changes to your device?
---
* The message varies depending on the Windows version.

* If you are logged on as a non-administrator,
  You will be required to enter the administrator user password.

Click (continue) "Yes" to boot.

About the [manual] folder

The "Manual" button on the upper right of the screen is enabled when the [manual] folder exists in the same folder as [gppro4.exe], and the manual will be displayed when the button is pressed.
If you want to display the manual with this button, you need to copy the [manual] folder along with [gppro4.exe].

*"index.html" in the [manual] folder is called. It is also possible to display any document.

when "disabled" when "enabled"

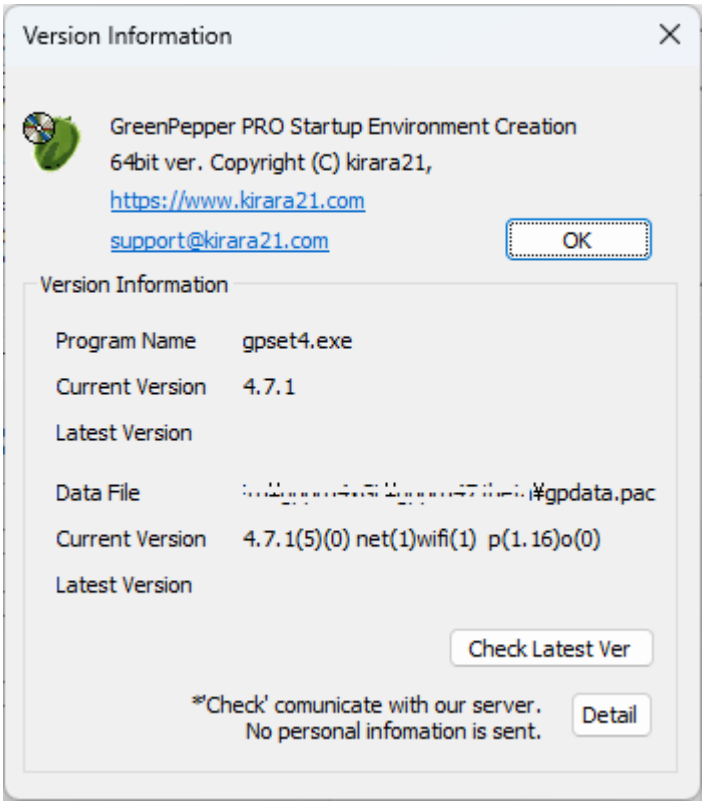
[Version] button

You can check the version currently in use and the latest version by clicking the [Version] button on the upper right of the screen.

"64bit ver." indicates a 64bit program, and "32bit ver." indicates a 32bit program.

"Data file" version

The "Data File" section shows the currently valid version of the "Data file".
net (0) ... Data file with network log settings (LAN, USB-LAN) disabled.
net (1) ... Data file with network log settings (LAN, USB-LAN) enabled.
wifi (0) ... Data file with network log setting (Wi-Fi) disabled
wifi (1) ... Data file with network log setting (Wi-Fi) enabled



Check Latest Ver

When you press this button, it communicates with our (kirala21) server and displays the latest version information on the screen.

* Customer-specific information (PC information, Windows information, etc.) will NOT be sent in this communication.
* Communicate via http. Please use it in an environment where you can access the Internet via http.

Detail

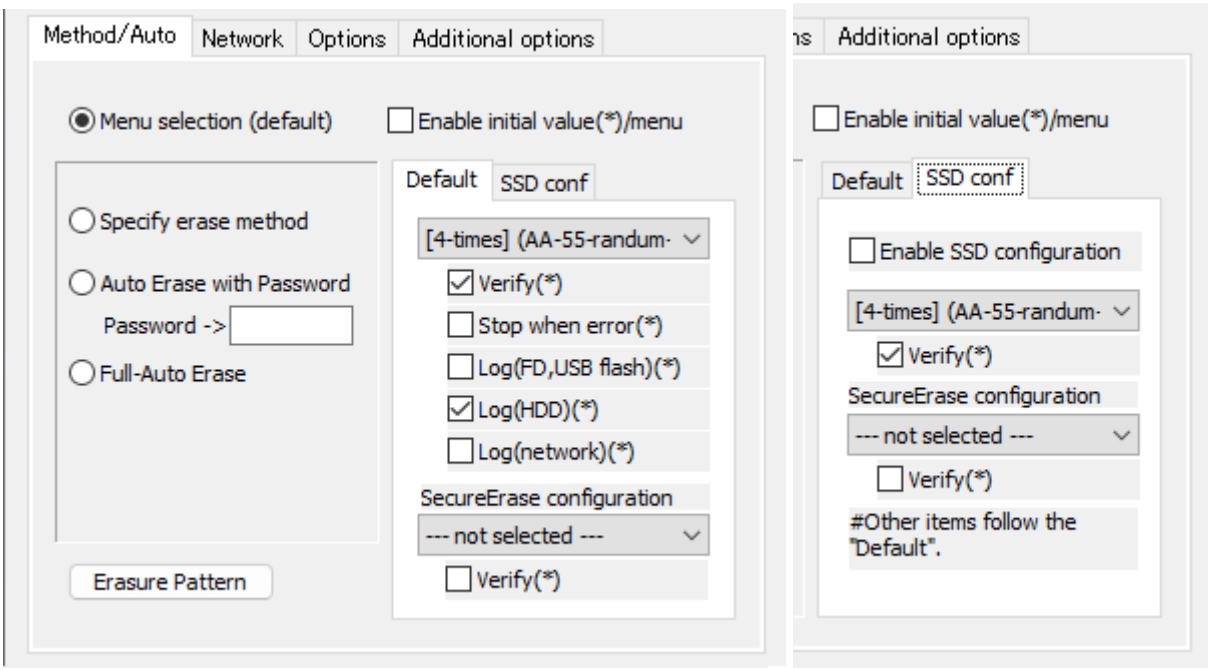
Click the [Detail] button to see the details of what is sent to the server.
No further information will be sent.

Common options for "Startup environment creation tool"

Various option settings are possible when embedding in a hard disk, creating a CD image, and setting a USB flash drive.
By setting various options here, it is possible to realize an erasing environment with a unified policy within the company, such as fixing the erasing method and fixing the processing options in the "Boot up erase program".

The following common options are also effective when installing the "Windows Erase Program" in WindowsPE. For an explanation of the operation by specifying options, see "Creating WindowsPE configuration file".

Method / Auto



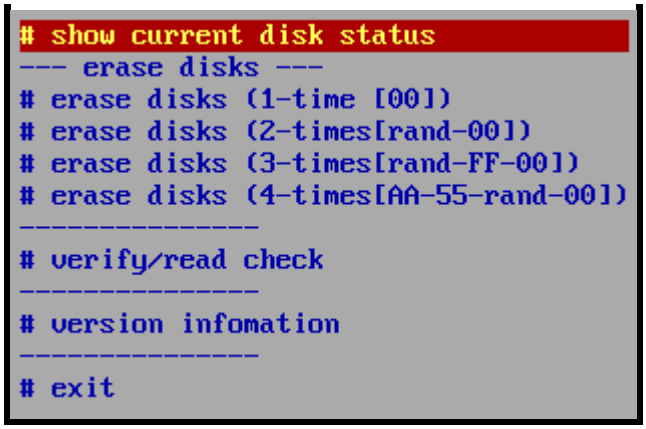
Menu selection

Start "Boot up Erase Program" in the normal menu selection format.

MEMO
The image on this page, which is surrounded by a black frame as shown below, is the screen of the "Boot up Erase Program".
Other than that, it is the screen of the "Startup environment creation tool" of Windows.

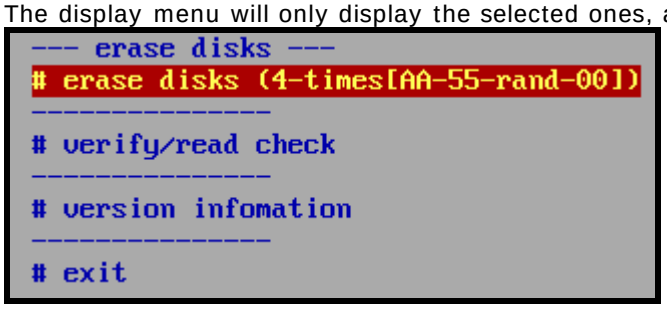
Enable initial value (*) /menu
If checked, you can specify the initial values for the following items. This is valid only in the "Menu selection".
If unchecked, it will be the system default value.

· Verify (Default, SecureErase, SSD conf, SSD SecureErase)
· Stop when error
· Log(FD, USB stick)
· Log(HDD)
· Log(Network)

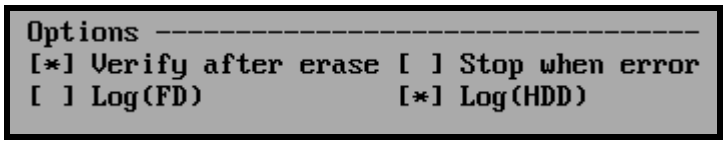


Specify erase method

Shows only the specified erase method.
The display menu will only display the selected ones, as shown below.



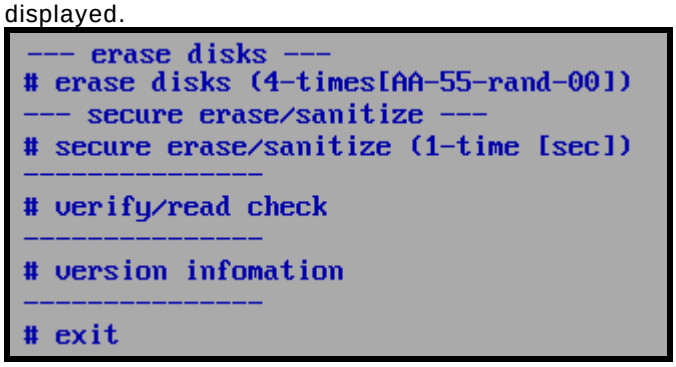
On the erase screen, the specified options such as "Stop when error" and "Log" are fixedly displayed, so that the user cannot change them.



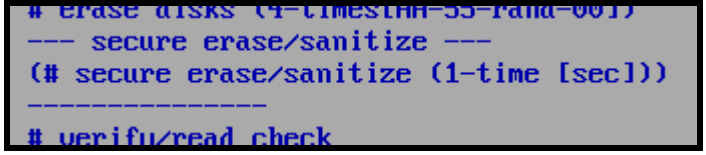
* For details on the erasing method and processing options, see "Erase disks".

SecureErase configuration

If you select a process other than "--- not selected ---", the specified secure erase menu is additionally displayed.



However, if a disk that can execute "Secure Erase"/"Sanitize" is not connected (including the frozen state) on the booted computer, the Secure Erase menu will be displayed and cannot be selected as shown below.



SSD configuration

If an SSD (including ATA-SSD, eMMC, NVMe) disk is connected to the booted computer, you can specify a different process for the SSD than for the HDD.

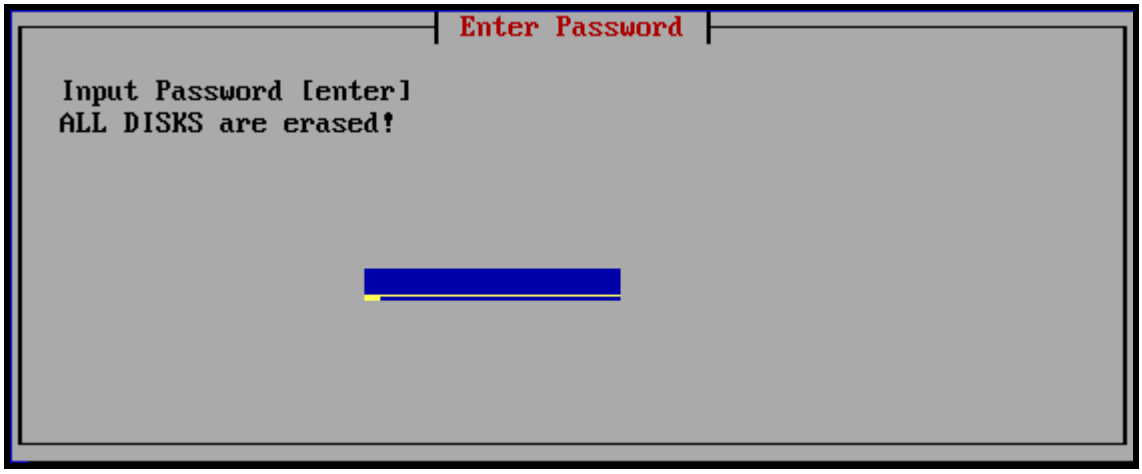
· When only the HDD is connected ... Only the processing menu specified in the [Default] settings is displayed.
· When only SSD is connected ... Only the processing menu specified in the [SSD conf] settings is displayed.
· When both HDD / SSD are connected ... Both of the processing menus specified in the [Default] settings / [SSD conf] settings are displayed.

Auto erase with password

If you make this selection, when the "Boot up Erase Program" starts, the password entry screen will be displayed as shown below.
If you do not enter the specified password here, you will not be able to proceed.
If you specify the correct password, **the menu selection screen will not be displayed** after that, and **all connected disks (up to 4) will be erased automatically**.
Different disks are processed in parallel on each screen displayed by ALT + F1-F4.

As with "Specify Erase Method", the erase method and erase options (such as "Stop when Error") are fixed to the specified values.

The text "Enter password", "Input Password [enter]", and "ALL DISKS are erased!" can be customized as desired.
See "Additional options" at the bottom of this page.



* Password can be up to 10 characters. Half-width alphanumeric characters can be used.
* The password is not for security purposes, but is for confirming the erasure, avoiding that the erasure starts automatically just by turning on the power.
* The password is saved in a text file that can be easily viewed on the boot CD or USB flash drive.

SecureErase configuration

If you select a process other than "---- not selected ---", the specified Secure Erase will be executed if a disk that is ready for Secure erase/Sanitize is connected.

SSD configuration

If an SSD (including ATA-SSD, eMMC, NVMe) disk is connected to the computer, the process specified in the SSD configuration will be automatically performed for the SSD.

· When only the HDD is connected ... Processing specified in the "Default" settings.
· When only SSD is connected ... Processing specified in the "SSD conf" settings
· When both HDD / SSD are connected ... Processing specified in the "Default" settings for HDD, "SSD conf" settings for SSD.

Full-auto erase

If you make this selection, when the "Boot up Erase Program" is started,
all connected disks (up to 4) will be erased automatically without waiting for any operator input.

As with "Specify Erase Method", the erase method and erase options (such as "Stop when Error") are fixed to the specified values.

Warning!
If you unintentionally leave the created CD or USB flash drive on the PC,
the next time you turn on the power, it will boot from the CD, etc.,
and all the disks on that PC will be erased.

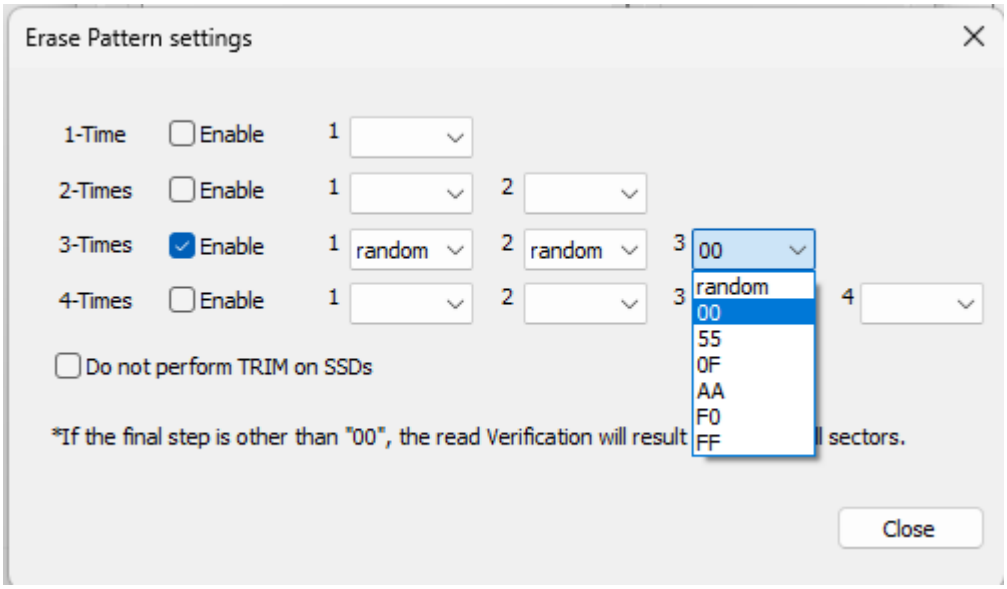
Remove the CD or USB flash drive immediately that incorporates fully automatic execution after creating it.

Erasure Pattern

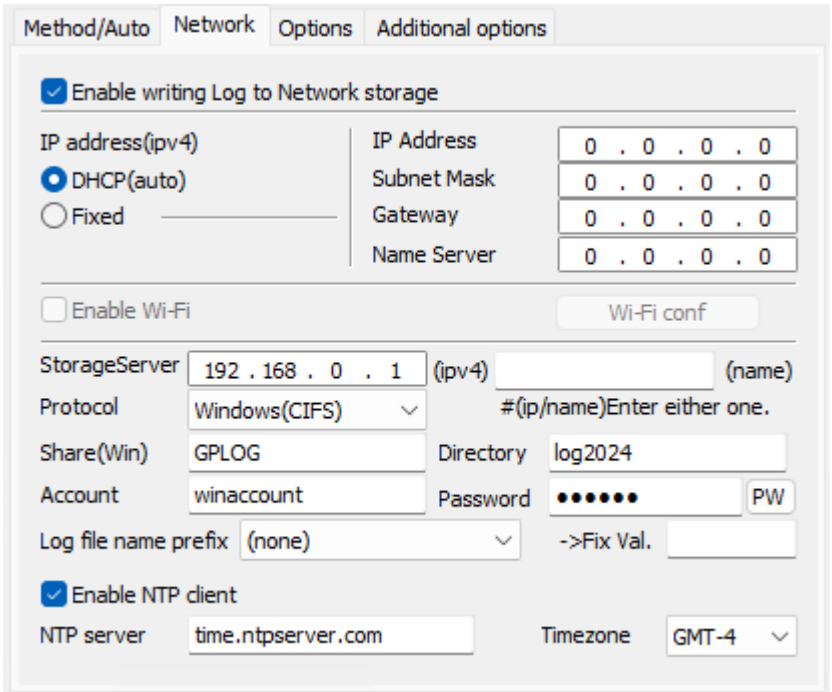
Specifies the erasure pattern for erasing 1-4 times.
If you want to use a pattern different from the standard pattern, set it here.
*If the final step is anything other than "00", "Read Verification" will result in a verification error.

Check "Enable" and specify the write value for each erase step.

Also, for SSD drives, TRIM processing is performed if erasing more than twice,
but if you do not want to perform this processing,
check "Do not perform TRIM on SSDs".



Network



Enable writing Log to network storage

When using the network log function, **check here and specify the following items**.
If you do not want to use network logs, uncheck it.

* If the data file (gpdata.pac) you are using does not support the network function, it cannot be enabled.

IP address (ipv4)

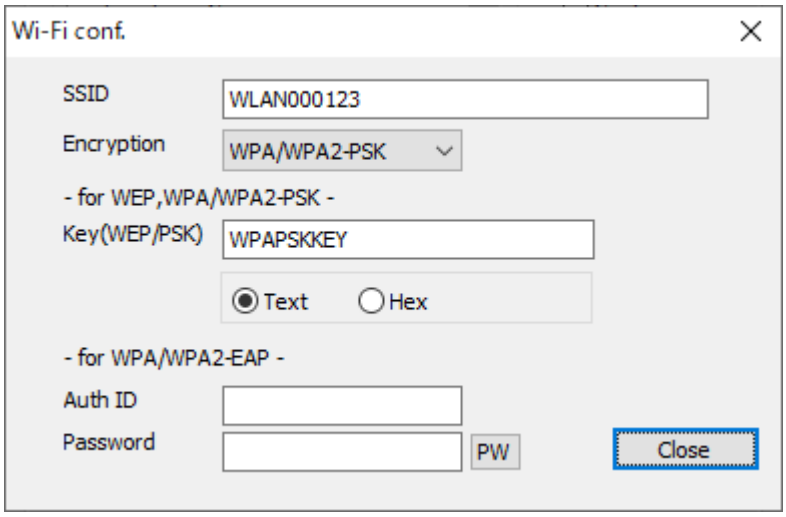
Specify the IP address (ipv4). Select "DHCP" to get it automatically from the DHCP server, select "Fixed Value" to use a fixed value and specify the following address.

The following does not need to be entered in the case of "DHCP".
"IP address" --- IP address
"Subnet mask" --- Subnet mask (255.255.255.0, etc.)
"Gateway" --- Gateway address. No input is required when not in use.
"Name server" --- Name server address. Required only if "Storage Server" is specified by "(name)".

Enable Wi-Fi

When using wireless LAN(Wi-Fi) for connection, check this box and set "Wi-Fi conf.".

* If the data file (gpdata.pac) you are using does not support the Wi-Fi network function, it cannot be enabled.



SSID

Enter the SSID for Wi-Fi connection.

Encryption

Specify the authentication encryption method for Wi-Fi connection.
You can select from the following.

(none)
WEP
WPA/WPA2-PSK (TKIP)
WPA/WPA2-EAP (EAP-PEAP,TKIP)

Key(WEP/PSK)

Specify KEY for WEP, WPA/WPA2-PSK.
When entering in hexadecimal, select "Hex".

Auth ID/Password

Enter the authentication ID and password used for WPA / WPA2-EAP (EAP-PEAP).
When you press the "PW" button, the password you entered will be displayed. Press it again to display "*".
However, "PW" can be displayed only when entering a new character or after clearing all characters.

The password is encrypted and stored in the created CD or USB flash drive, but it may be decrypted.
If it is widely distributed, please be careful about its management.

Storage Server

Enter the IP address or server name of the server.
It is is a FTP server or a server with Windows shared folder.
Enter only either the IP address (ipv4) or the server name.

Protocol

Select "Windows (CIFS)" when writing to a Windows shared folder, or "FTP" when writing to an FTP server.
* Supports SMB 3.0, 2.1, 2.0, 1.0.
FTP is connected in Passive mode (PASV mode).

Share(Win)

Required only for "Windows" connections.
Specify the Windows share name to connect to.
Write permission is required for the shared folder .

Directory

Specify the name of the directory (folder) to write the log to.
If left blank, it will be written to the shared folder for Windows shares and to the home directory for FTP.
It is not necessary to add "\", "/" at the beginning and end. (Even if it is attached, it will be ignored)
Specify the directory delimiter with "\" or "/".

example:
gp\2012\log
gplog/2012

For the specified directory, create / write a file, read the file size, and delete the written file (during a write test) are performed. Please set the authority appropriately.
Since file data read permission is not required, write-only operation is also possible.

* Even if you do not have permission to delete the file, the process will continue,
but the file written in the write test (that is automatically performed before the erase process) will remain unerased.

Account/Password

Enter the authentication ID (user name) and password used for connection.

The password is encrypted and stored in the created CD or USB flash drive, but it may be decrypted.
Please be careful about management when it is widely distributed.
For example, creating an authentication ID dedicated to log storage that can be written only to the specified folder.

When you press the "PW" button, the password you entered will be displayed. Press it again to display "*".
However, "PW" can be displayed only when entering a new character or after clearing all characters.

log file name prefix

It is possible to add special characters to the beginning of the log file name to be written.

(none) · · · It will be a normal file name.

[date(month,day)][hour][minute][second].log
ex: Log created at 13:08:12 on June 5th -> 0605130812.log

Fixed val · · · The character entered in the "Fixed val" field is added to the beginning.

[Fixed val]_[date(month,day)][hour][minute][second].log
ex:
Fixed val: SZ
Log created at 13:08:12 on June 5th -> SZ_0605130812.log

[Additional info1]/[Additional info2]
· · · The value entered by the operator in "Option"/"Additional info" is added to the beginning.

ex:
When "nomura" is entered in "Additional info1"
Log created at 13:08:12 on June 5th -> nomura_0605130812.log

If the input value contains characters that cannot be used as a file name, it will be replaced with "_".

For "Additional info", see "Options" / "Enter additional info" below.

Enable NTP client

If enabled, the time will be synchronized with the specified NTP server when the erase program starts.
"Enable writting log to network storage" must be enabled.

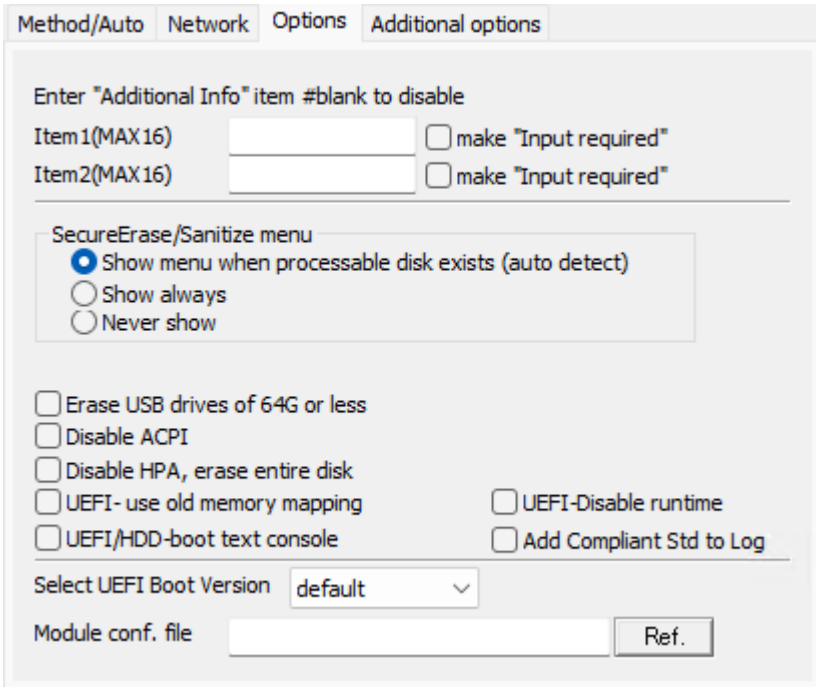
NTP server

If you check "Enable NTP client", specify the server to synchronize time with.
Specify by IP address (IPv4) or server name.
When using a server name, it is necessary to specify a "Name server".

Timezone

If you check "Enable NTP client", specify the time zone of the PC.
Specify between GMT-12 and GMT+12.
For example,
San Francisco (USA) , "GMT-7"
New York (USA) , "GMT-4"
Berlin (Germany) , "GMT+2"
New Delhi (India) , "GMT+5"
Tokyo (Japan) , "GMT+9"

Options

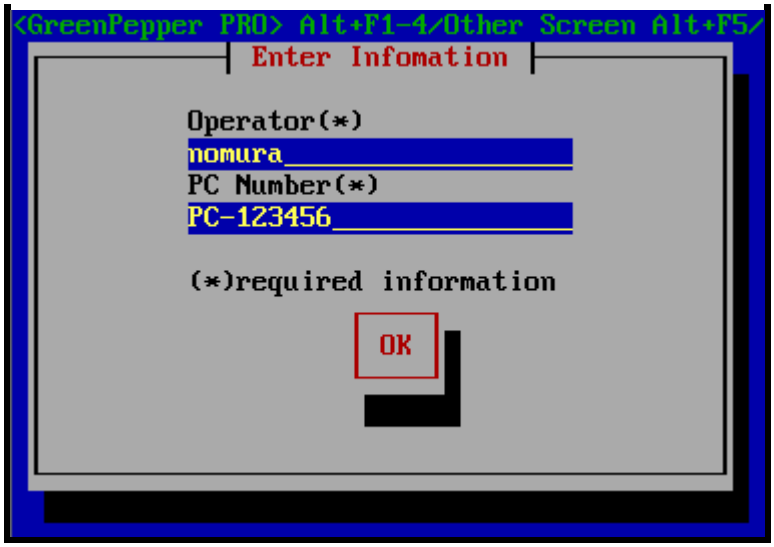


Enter "Additional Info" item #blank to disable

If you specify a value for the "Item1"/"Item2", the following screen will be displayed before the erase menu is displayed, prompting the operator for input.
If you select "make 'input required'", you will not be able to proceed unless you enter some value in that item.
If it is not " input required", you can move to the next even if it is left blank.
The "Item1"/"Item2" can be up to 16 single-byte alphanumeric characters (spaces allowed).

You can disable it by leaving the them blank.

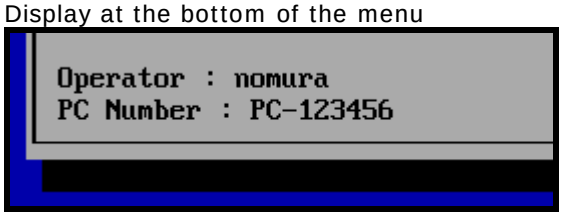
It is convenient to use it for the person in charge of processing, the in-house management number of the PC, etc.



In the example of this screen,
Item1: "Operator" Required
Item2: "PC Number" Required

The entered content is displayed at the bottom of the menu and written to the erasure log.

Display at the bottom of the menu



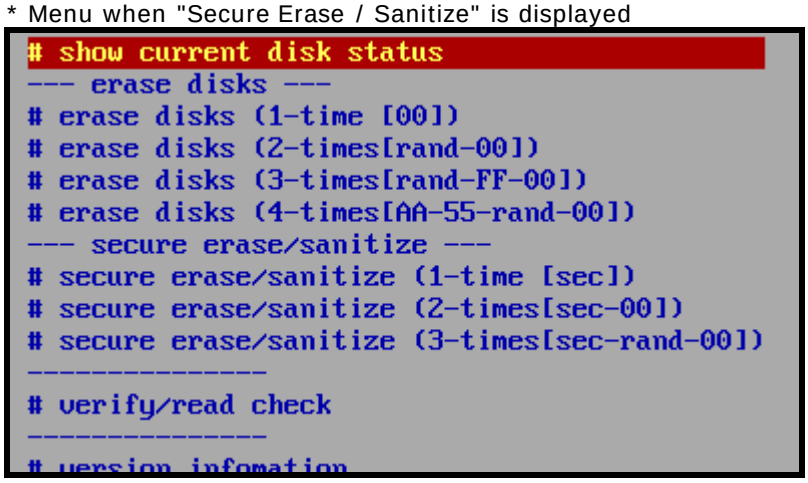
Write to Log
* Written in the area subject to tampering check.

```
===
--- disk erase log ----------------------------
Operator : nomura
PC Number : PC-123456
disk : ATA ST3160813AS (156290904 kbyte) rev:SD2B
ser:9SY082C5
method : 4-times[AA-55-rand-00] -> verify
..... omitted below
===
92ae1655be5a5b95977863ac87c637a5
```

SecureErase/Sanitize menu

Specify when to display "Secure Erase / Sanitize" in the menu.

* Menu when "Secure Erase / Sanitize" is displayed



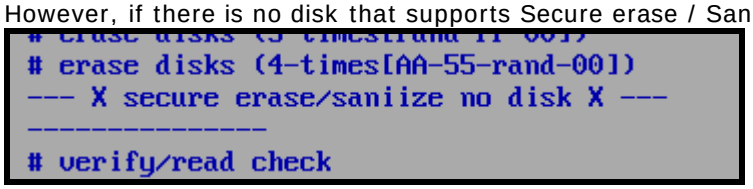
Show menu when processable disk exists
In the following cases, "Secure Erase / Sanitize" is displayed.

* When there is a disk that supports Secure erase and is not in a Frozen state.
* When there is a disk that supports Sanitize.

This is the default value for the "Product CD-ROM".

Show always
"Secure Erase / Sanitize" is always displayed.
* Even if it is Frozen state, it will be displayed in the menu.

However, if there is no disk that supports Secure erase / Sanitize, the following will be displayed.



Never show
"Secure Erase / Sanitize" is not displayed in any case.

Erase USB drives of 64G or less

Normally, a USB drive of 64 Giga bytes or less is interpreted as a USB drive used for writing logs and booting, and is excluded from erasure.
When this option is enabled, no such exclusion is made and all USB drives are also subject to erasure.
Especially when erasing by automatic execution, if the USB flash drive is the target of erasure, the USB flash drive used for startup will also be automatically erased.
Therefore, when booting from USB flash drive, use a USB flash drive of 64GB or less and do not check this.

Disable ACPI

Generally, it does not need to be set.
On some PCs, if this option is not enabled, it may stop during startup and not proceed to the menu display.

First, try booting with ACPI disabled by specifying options at startup of "GreenPepper PRO". If you can start it that way and you need to erase many of the same PC models, it is convenient to check here.
Refer to "Boot from CD/USB flash drive" for how to boot with ACPI disabled.

If ACPI is disabled, general PCs may not be able to recognize the disk or the power may not be turned off automatically.

Disable HPA, erase entire disk

For HPA (Host Protected Area), see "Points to consider about erasing method".
If you want to temporarily disable HPA, it is convenient to specify options at startup to disable HPA.
For the boot method with HPA disabled, refer to "Boot from CD / USB flash drive".
It can also be disabled by the "Utility"/"Remove HPA / Reset DCO" process after startup.

If you need to disable HPA and erase many of the same PC models, it is convenient to check here.

* HPA specifications may not be valid, such as when connecting to a USB interface.

UEFI - use old memory mapping

Generally, it does not need to be set.
This setting is valid only at startup in UEFI.
If there is a problem such as stopping in the middle without completing the startup, please try this option

UEFI - disable runtime

Generally, it does not need to be set.
This setting is valid only at startup in UEFI.
If there is a problem such as stopping in the middle without completing the startup, please try this option

If you make this specification, other problems may occur, such as the computer name not being displayed or the power not turning off automatically.

UEFI/HDD - boot text console

This setting is valid only at startup in UEFI.
If checked, the initial screen at startup will be a text display. That is unlikely to cause problems on many models.
If the startup screen is not displayed at all and "Green Pepper PRO" starts automatically after a while, or

the screen is too small to see, try this specification.

Add Compliant Std to Log

The erasing standard that complies with is displayed in the erasing log as shown below.
Only when there are no errors in the erasure process and verification process.

Log example:

```
===
--- disk erase log ----------------------------
disk : xxxxx
method : 2-times[rand-00] -> verify
start: xxxxxxxx
end: xxxxxxx
error : write(0) read(0) verify(0)
status : finished (no error)
standard : NIST.SP.800-88.Rev1(clear) compliant
-----------------------------------------------
```

Disk type	Erase method	Description
ATA(SATA,PATA) HDD	1time-4times erase + verify	NIST.SP.800-88.Rev1(clear)
	4times erase + verify	DoD 5220.22-M Sup1(1995)
	Secure Erase/Sanitize(1time-3times)+verify when following method is executed. *Secure Erase/Enhanced Secure Erase *Sanitize(OVER_WRITE).	NIST.SP.800-88.Rev1(purge)
	3times erase + verify *random-random-00 is specified	NSA 130-1
ATA(SATA,PATA) SSD	1time-4times erase + verify Secure Erase/Sanitize(1time-3times)+verify when following method is executed. *Secure Erase/Enhanced Secure Erase	NIST.SP.800-88.Rev1(clear)
	4times erase + verify	DoD 5220.22-M Sup1(1995)
	Secure Erase/Sanitize(1time-3times)+verify when following method is executed. *Sanitize(BLOCK_ERASE)	NIST.SP.800-88.Rev1(purge)
	3times erase + verify *random-random-00 is specified	NSA 130-1
NVMe (SSD)	1time-4times erase + verify	NIST.SP.800-88.Rev1(clear)
	4times erase + verify	DoD 5220.22-M Sup1(1995)
	Secure Erase/Sanitize(1time-3times)+verify when following method is executed. *Secure Erase *Sanitize	NIST.SP.800-88.Rev1(purge)
	3times erase + verify *random-random-00 is specified	NSA 130-1
SCSI(SCSI/SAS)	1time-4times erase + verify	NIST.SP.800-88.Rev1(clear)
	4times erase + verify	DoD 5220.22-M Sup1(1995)
	3times erase + verify *random-random-00 is specified	NSA 130-1
eMMC,USB Flash etc.	1time-4times erase + verify	NIST.SP.800-88.Rev1(clear)
	4times erase + verify	DoD 5220.22-M Sup1(1995)
	3times erase + verify *random-random-00 is specified	NSA 130-1

Select UEFI Boot Version

Generally, it does not need to be set, select "defult".
For some older PCs, it may not boot properly.
When such cases, select "old ver-1" or other.
For example, some old Fujitsu LIFEBOOK need to set "old ver-1".

Module conf. file

Generally, it does not need to be set.

The "module configuration file" is a file that describes the driver modules for the disk interface and network interface.
It is used in the following cases.
* When specifying parameters different from normal
* When installing a driver that is not automatically installed
* If you do not want to install the automatically installed driver

If there is a problem with the standard settings, use the file provided by us, or please create and use the file yourself.
The file format is as follows.

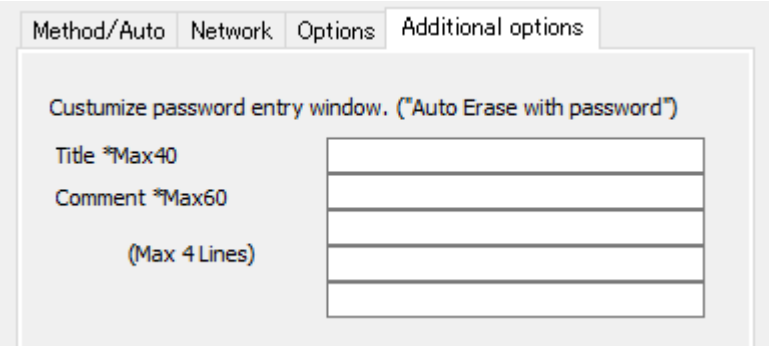
[before]
(A module that is forcibly loaded before loading a system-recognized module)
[match]
(Use the specified parameters when loading a system-recognized module)
[noload]
(If the module recognized by the system matches the specified one, it will not be loaded)
[after]
(Module to be forcibly loaded after the system -recognized modules have been loaded)
---

* ASCII text file. Line breaks are CR + LF or LF.
* Lines starting with "#" are ignored as comments
* Describe only the necessary sections
* The module description is only the module name, excluding ".ko", path, etc.
* Only modules that can be described are those in "Supported SCSI / RAID cards" and "Supported network interface card".
* Describe the parameters according to the kernel version. You can see kernel version in "Technical Specifications" page.
* Describe parameters after the module name with a space.

Example: When specifying the "topology=2" for the Fibre Channel module, "lpfc"

[match]
lpfc topology=2

Additional options



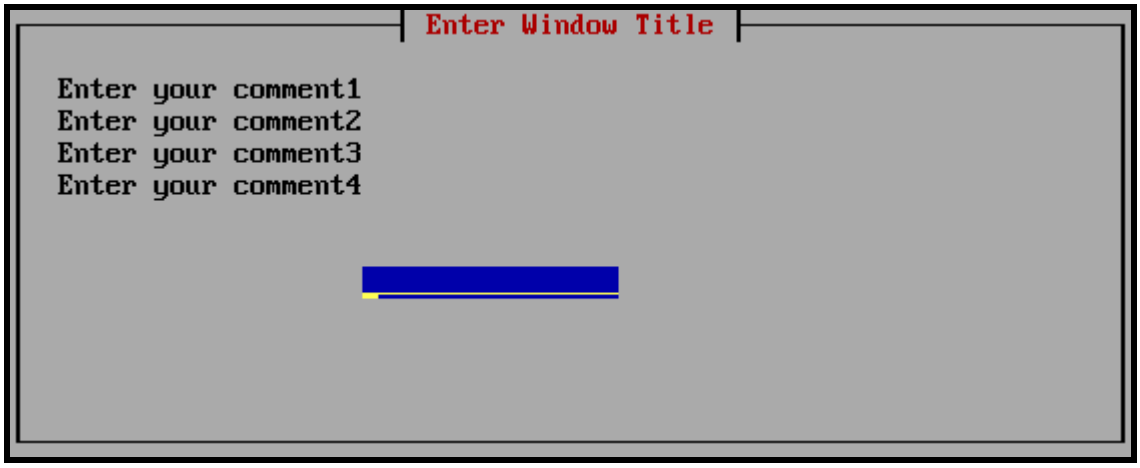
Title / comment

Specify the display text on the initial password input screen during "Auto erase with password".

Example:

Title: Enter Window Title
Comment:
Enter your comment1
Enter your comment2
Enter your comment3
Enter your comment4

When set in this way, the following screen will be displayed.

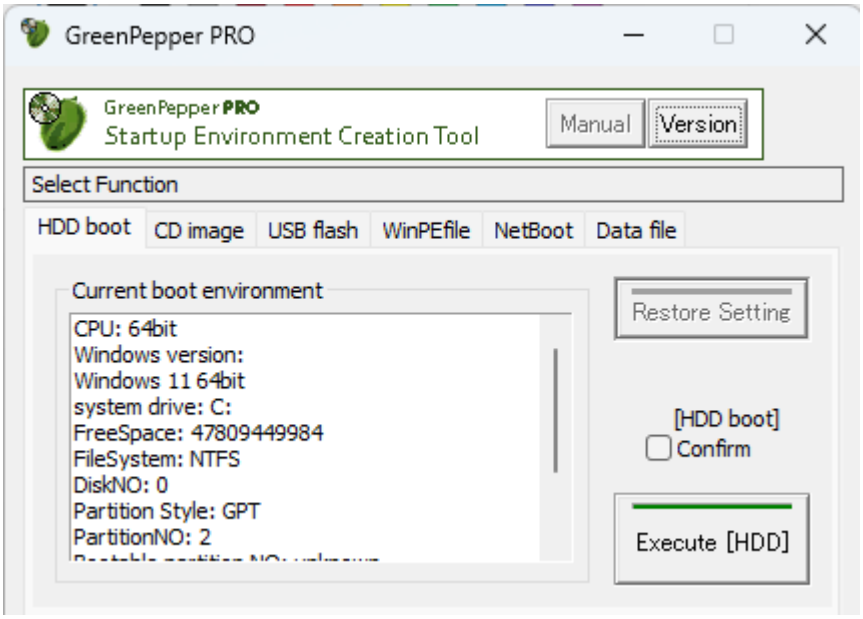

Enter Window Title
Enter your comment1
Enter your comment2
Enter your comment3
Enter your comment4

Operation of "HDD boot"

Execute the "Startup Environment Creation Tool" **on the PC you want to erase**, and install the "Boot up Erase Program" on the system hard disk of that PC.
When you restart your PC, the "Boot up Erase Program" will start and you can erase the hard disk of that PC.

Even if the HDD installation is completed and the "Boot up Erase Program" is started, the disk interface may not be supported or the network card may not be supported.
In that case, the disk cannot be erased or the network log cannot be written. Please use it on a PC with a model number whose operation has been confirmed in advance.

If the disk is not recognized by the "Boot up Erase Program" or cannot be started, start it with a CD / USB flash drive and erase the PC.



* This process rewrites the startup environment. By incorporating the erase program, you may not be able to start up Windows. Perform the process on the assumption that it will be deleted.
* If you are using 64-bit Windows and GPT partition / UEFI boot, use the UEFI boot system to boot.
* If you are using 32bit UEFI, 32bit Windows and GPT partition / UEFI boot, the CPU must be 64-bit compatible.
* When booting with the Legacy/BIOS, write the boot file to the system drive.
If the file system is encrypted (NTFS encryption or other software encryption), you will not be able to boot.

Current boot environment

Shows the current Windows boot environment. Based on the environment recognized here, it is judged whether or not the setting is possible when performing the embedded processing.
* Please let us know this information if you have any problems with the embedded process.

Options

For the options , see "Common options".

Execute [HDD]

Check "[HDD] boot confirm" and then click "Execute [HDD]". Executes the process of embedding in the hard disk.
* Processing will take some time. Please wait until the end message appears.

Items to check in the boot environment

The following items are checked. If a check error occurs,
boot "Boot up erase program" from the CD / USB flash drive and erase it.

Legacy(BIOS) boot	
system drive	System drive is "C"
file system	File system on the system drive is NTFS

disk containing system drive	The disk must be the first disk (0) on the system
partition style	Partition style is MBR, not GPT.
partition NO.	System is on partition 0-3.
bootable	One of 0-3 partitions are bootable (It may be different from the system)
Free space on C drive	65M or more free space
UEFI boot	
Windows	64bit Windows or When 32bit Windows, 32bit UEFI and 64bit CPU.
disk containing system drive	The disk must be the first disk (0) on the system
partition style	Partition style is GPT, not MBR
Free space on UEFI partition	65M or more free space

Folder to be created

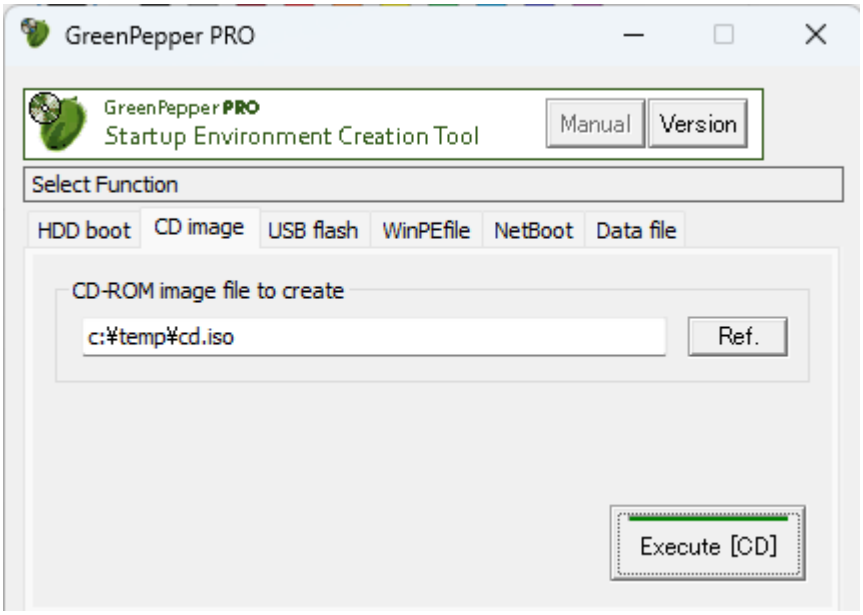
In the BIOS(Legacy) boot environment
c: \gp_boot
folder will be created to save the current Windows startup environment as well as the erase program startup environment.
Do not delete or rewrite this folder if you have the possibility of returning to the previous Windows boot environment.
* If this folder is compressed or encrypted, it will not be able to start.

Restore setting

You can use this button in an environment where a boot environment for erasing has been set.
If you want to revert to the previous Windows boot environment, perform this process.
* Depending on the environment, it may not be possible to recover correctly.
Perform the installation work on the assumption that it will be erased.

Creating bootable "CD image" file

Create a CD-ROM image file (ISO9660 format) that can boot PC and start the "Boot up Erase Program".
By writing (burning) this file to a CD-R, it becomes a bootable CD.
The created CD can be booted in both the BIOS and UEFI environments.



CD-ROM image file to create

Specify the file to create. Enter the file name (full path) directly from the keyboard, or press the "Ref." button to specify the file.

Options

For the options , see "Common options".

Execute [CD]

Execute creating a CD-ROM image file.
* Processing will take some time. Please wait until the end message appears.

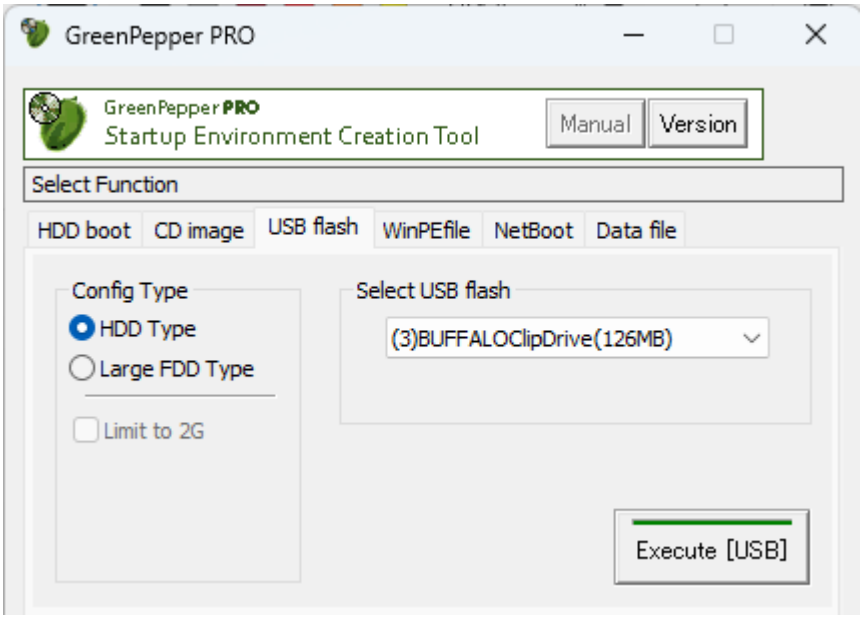
Writing (burning) the created file to a CD-R

To Write (burn) a CD image file to a CD-R, see "How to create a CD from an image file".

Setting bootable "USB flash drive"

This is a process to incorporate a "Boot up erase program" into a commercially available USB flash drive.
You can start the PC from the set USB flash drive and use the "Boot up Erase Program".
The created USB flash drive can be booted in both the BIOS and UEFI environments.

* Another program for configuring USB flash drives is the "USB stick Boot configuration tool" (gpusbst4.exe).
This does not require administrator privileges and can be used with user privileges.
Please see "Abstract, Executing , Functions" for details.



Warning !
* Please note that the USB flash drive is initialized by the setting process and **the inside is erased**.
* Please use a **USB flash drive of 64GB or less**.
Anything larger than 64GB will be treated as an erase target drive and you will not be able to write logs.
Also, when automatic erase is set, it will be erased automatically.
* USB flash drives that are encrypted and those require a password at the time of use cannot be used for booting.

* The USB flash drive can be set if it has a capacity of about 128MB.

Select USB stick

Select the USB flash drive to be set from the list.
* A list of USB removable drives is displayed.

When you make a selection, information such as the current setting type is displayed.

Config type

Select the method for setting the USB flash drive.
Normally, select "HDD type".
Depending on the PC, it may not be possible to boot with the "HDD type".
In that case, please try with "Large FDD type".

If you check "Limit to 2G", the USB flash drive larger than 2GB will be limited to the capacity of 2GB.
This is an option when you cannot boot with a large capacity one on an old PC.
* Even if you set "Limit to 2GB", if you format it in Windows, you can use it with normal capacity.

You may need to change the BIOS settings to boot from a USB flash drive.
For information on changing the BIOS settings, see "Setting the boot environment on BIOS/UEFI".

Options

For the options , see "Common options".

Execute [USB]

Execute setting USB flash drive.
* Please note that the inside of the USB flash drive will be erased.
* Processing will take some time. Please wait until the end message appears.

Points to note in the setting procedure

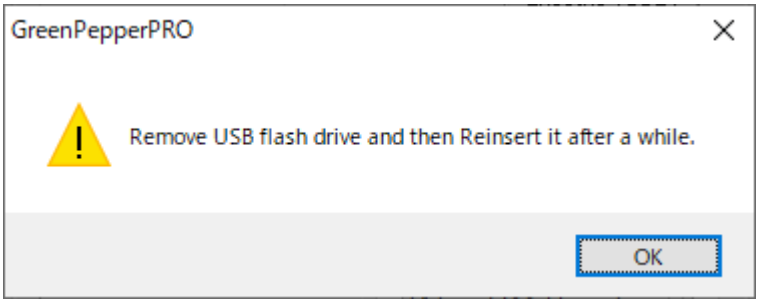
The setting procedure is as follows. Follow the on-screen messages to proceed.

1. Confirmation of execution

You will be asked if you want to execute it. Click "OK" if you want to proceed.

2. Remove the USB flash drive and then reinsert it.

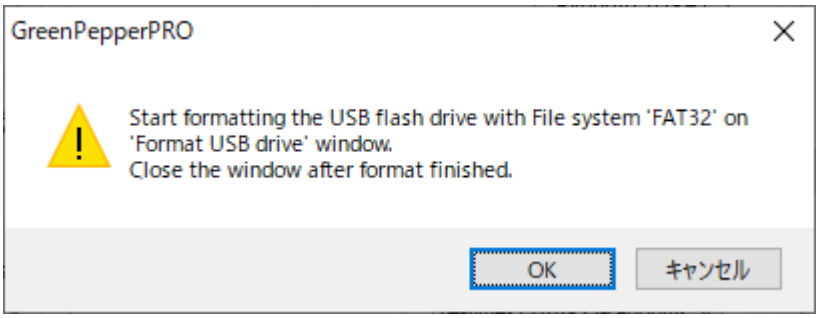
If the following message appears, remove the USB flash drive once, wait a few seconds, and then insert it again. After reinserting, click "OK".



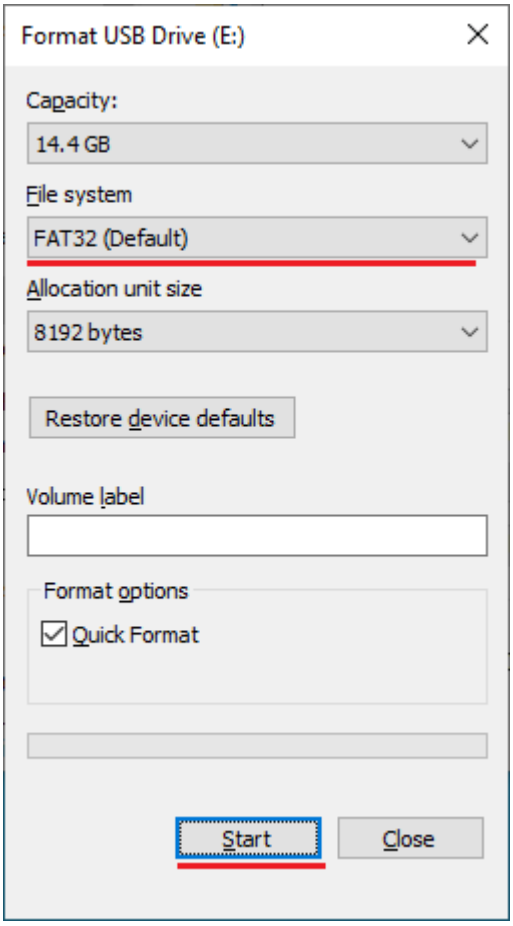
3. Format the USB flash drive

Before you start formatting, you will get a message like the one below.
On this screen, you can specify whether file system is "FAT" or "FAT32".
* FAT for 2GB or less, and FAT32 for larger capacities.

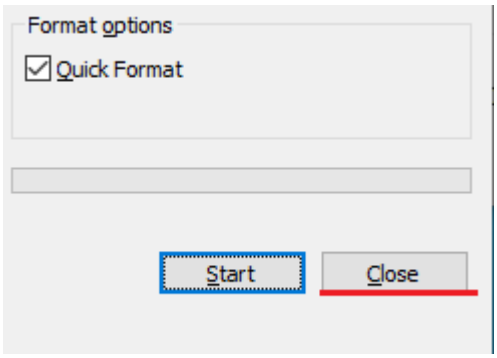
On the next format screen, **be sure to select the indicated file system** and format it.



On the format screen, check "File system" and press the "Start" button.
* "Quick format" can be checked or unchecked.

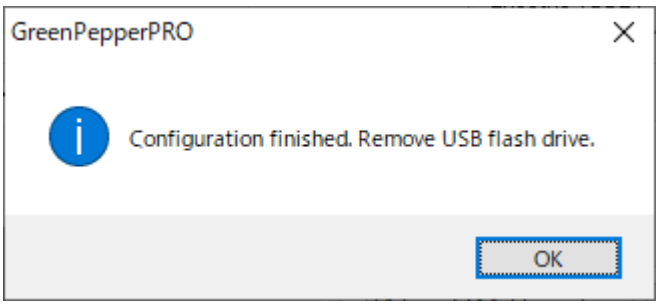


After formatting is complete, click the "Close" button to close the format screen.



4. End message

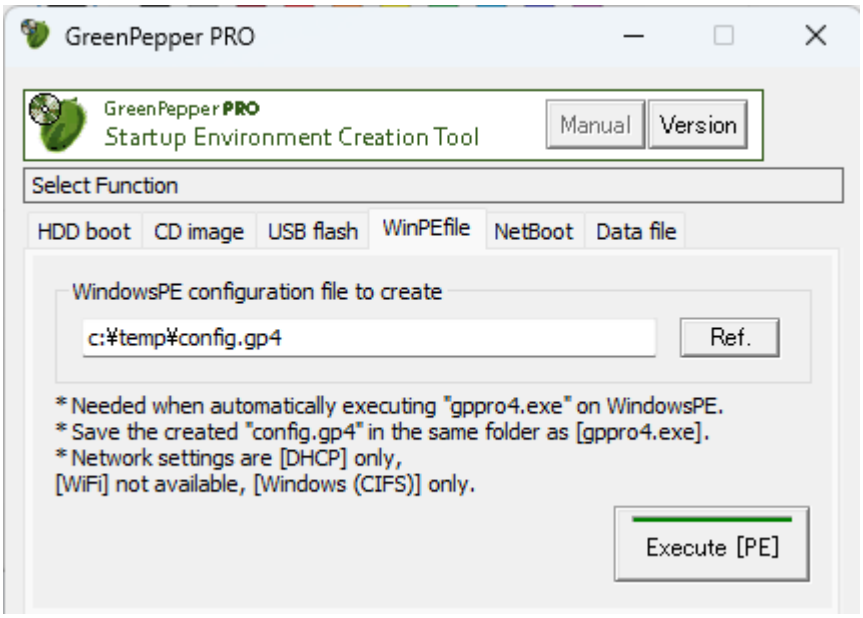
It is complete when the following end message appears.
Even if you want to check the inside of the USB flash drive, please use it after removing and reinserting it.



Creating WindowsPE configuration file

When running the "Windows executable program" (gppro4.exe) on a WindowsPE environment, you can specify various options by using the configuration file (config.gp4) created below.
The created configuration file (config.gp4) must be installed in the same folder as "gppro4.exe".
For detail information on WindowsPE environment, see "Building WindowsPE boot environment".

Additionally, "config.gp4" is a file in which the contents described in "Setting initial and fixed values using the command line" are automatically set.
You can also edit the content yourself.



WindowsPE configuraition file to create

Specify the file to create. Enter the file name (full path) directly from the keyboard, or press the "Ref." button to specify the file.
The file name when installing must be "config.gp4".

Options

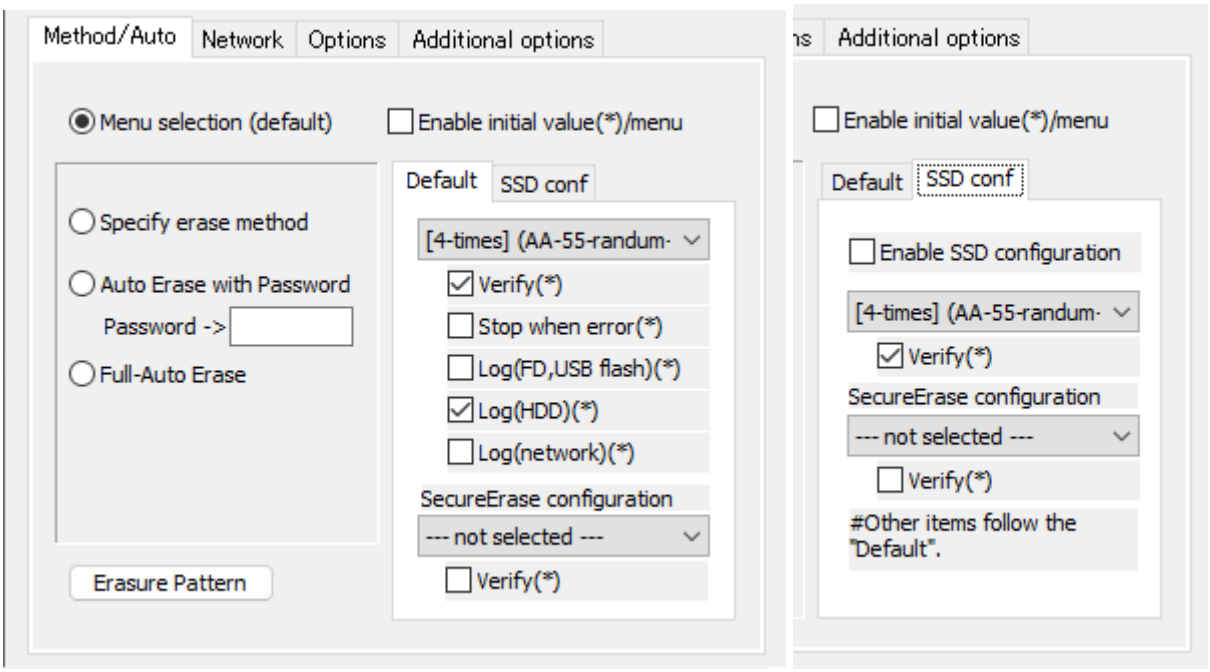
For the options , see "Common options".

Execute [PE]

Execute creating a WindowsPE configuration file.

Options for WindowsPE configuration file

Method / Auto



Menu selection

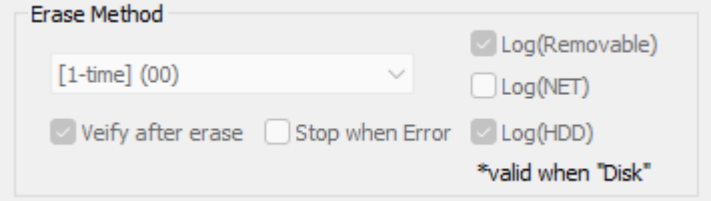
Start "Windows Erase Program" in the normal menu selection format.

[Enable initial value (*) /menu]
If checked, you can specify the initial values for the following items. This is valid only in the "Menu selection(default)".
If unchecked, it will be the system default value.

· Erase Method
· Verify (Default, SecureErase, SSD conf, SSD SecureErase)
· Stop when error
· Log(FD, USB stick)
· Log(HDD)
· Log(Network)

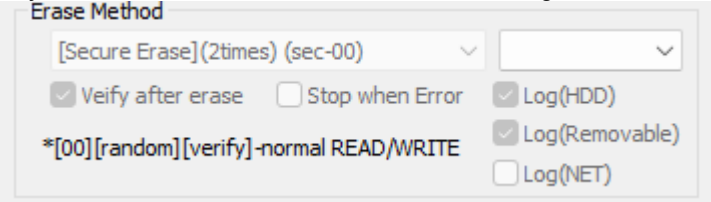
Specify erase method

Fixes to only the specified erasure method and disables selection of others.
In addition, the "Verify after Erase" and log writing specifications are also fixed and cannot be changed.
When the program is executed, the screen will be displayed in an unchangeable state as shown below.



SecureErase configuration

Specify the erase method for Secure Erase, which is displayed on the "Secure Erase" tab (page) when running the "Windows Erase Program".
If you select "---not selected---", the erasing method is not fixed and can be selected at runtime.



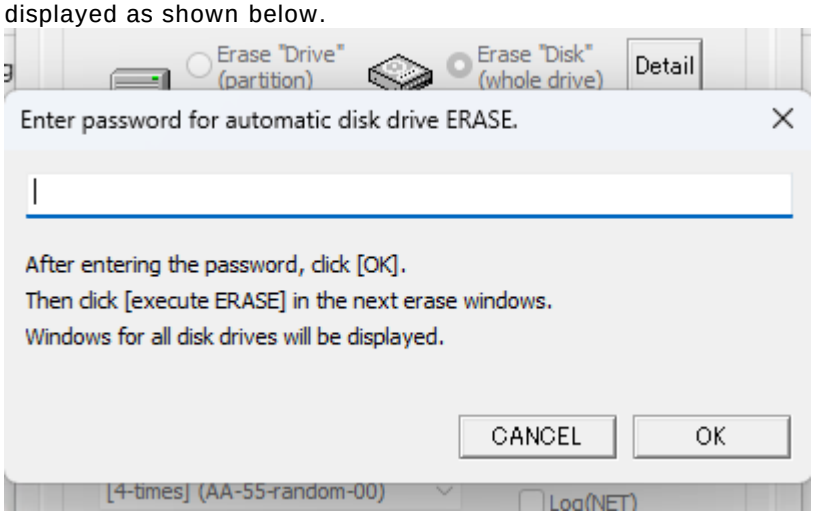
SSD configuration

If an SSD (including ATA-SSD, NVMe) disk is connected to the booted computer,
you can specify a different process for the SSD than for the HDD.

At runtime, the specifications for the HDD are displayed in the initial state. When selecting a disk drive, if it is recognized as an SSD, it will change to the contents specified in the SSD settings.

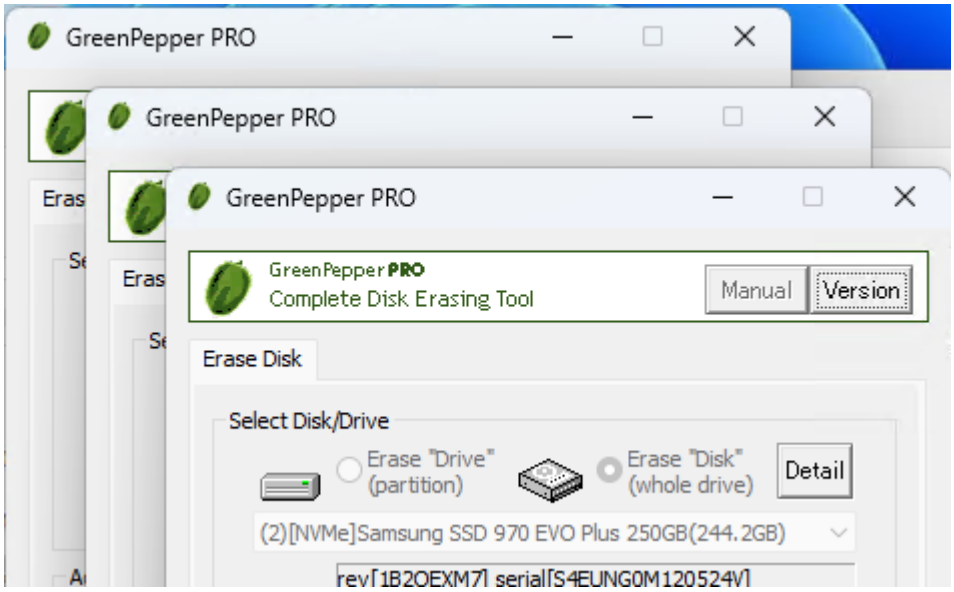
Auto erase with password

If you make this selection, when the "Windows Erase Program" starts, the password entry screen will be displayed as shown below.

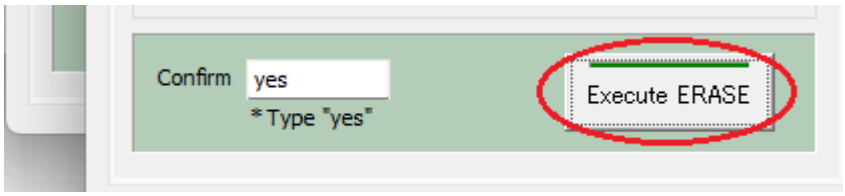


You cannot proceed further unless you enter the specified password. “Cancel” ends the program.
If you specify the correct password, the erase program for all disks (up to 9 disks) will start automatically. Each screen will have a different disk selected.

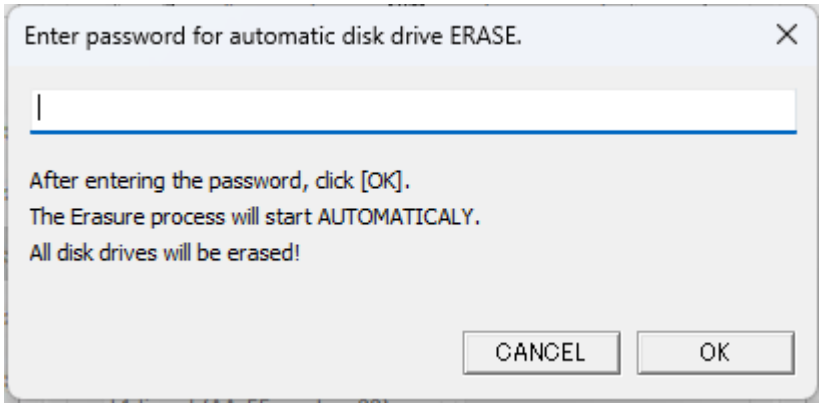
When "Auto Erase with Password"/"Full-Auto Erase" is performed, only the "Erase Disk" or "Secure Erase" tab (page) is displayed on the erase program screen. If you do not enter the specified



If you use "config.gp4" automatically created by this "Creating WindowsPE configuration file", the program will wait for operation with "yes" automatically entered in the "Confirm" field as shown below.
When the operator clicks "Execute Erase," erasing (using the specified erasing method) begins.
*You must click "Execute Erase" on all the screens that are launched.



If you want to run completely automatically without clicking "Execute Erase", edit the created "config.gp4" with Notepad etc. "/AUTOBUTEXEC" must be replaced with "/AUTOFULLEXEC".
If specified so, the following screen will be displayed and
all disk drives will be automatically erased immediately after entering the password.



* Password can be up to 10 characters. Half-width alphanumeric characters can be used.
* The password is not for security purposes, but is for confirming the erasure, avoiding that the erasure starts automatically just by turning on the power.
* The password is saved in a text file that can be easily viewed on the boot CD or USB flash drive.

SecureErase configuration

If you select a method other than "---- not selected ---", the specified Secure Erase will be executed if a disk drive that is ready for Secure erase/Sanitize is connected.

SSD configuration

If an SSD (including ATA-SSD, NVMe) disk drive is connected, the method specified in the SSD settings will be automatically performed for the SSD.

Full-auto erase

If you select this, the password entry screen for "Auto Erase with Password" will be omitted and the erasure execution screen will be displayed immediately.

If you use "config.gp4" automatically created by this "Creating WindowsPE configuration file", the program will wait for operation with "yes" automatically entered in the "Confirm" field.
When the operator clicks "Execute Erase," erasing (using the specified erasing method) begins.
*You must click "Execute Erase" on all the screens that are launched.

If you want to run completely automatically without clicking "Execute Erase", edit the created "config.gp4" with Notepad etc. "/AUTOBUTEXEC" must be replaced with "/AUTOFULLEXEC".

Example: contents of "config.gp4" created by "gpset4.exe"

/M:17eVRLHn /S:47VR /AUTO /AUTOBUTEXEC

After change:

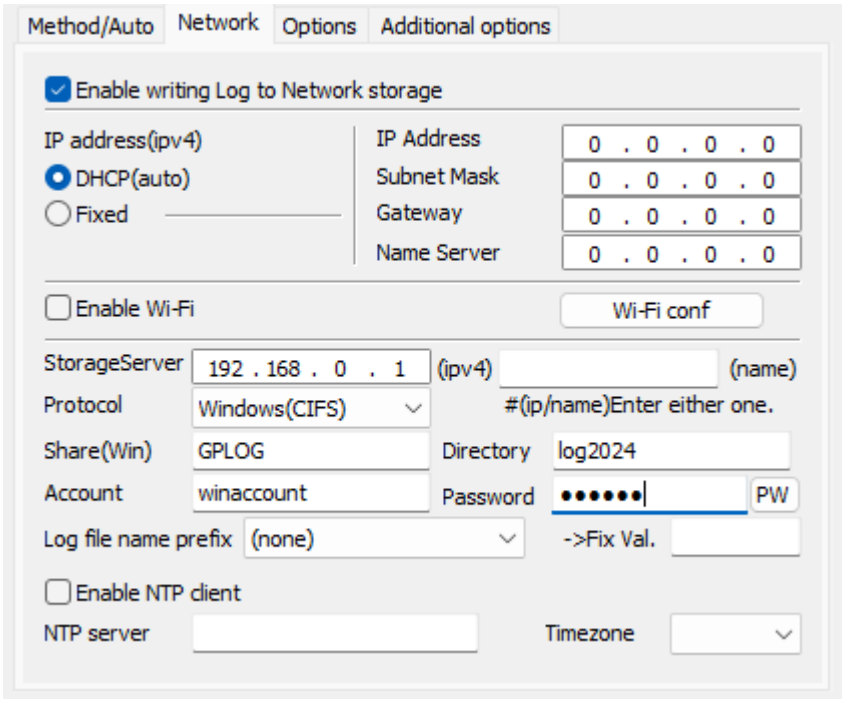
/M:17eVRLHn /S:47VR /AUTO **/AUTOFULLEXEC**

If specified so,
all disk drives will be automatically erased immediately without any operation.
*If "gppro4.exe" is set to start automatically.

Warning!
If you unintentionally leave the created CD or USB flash drive on the PC,
the next time you turn on the power, it will boot from the CD, etc.,
and all the disks on that PC will be erased.

Remove the CD or USB flash drive immediately that incorporates fully automatic execution after creating it.

Network



Enable writing Log to network storage

When using the network log function, **check here and specify the following items**.
If you do not want to use network logs, uncheck it.

* If the data file (gpdata.pac) you are using does not support the network function, it cannot be enabled.

IP address (ipv4)

Specify the IP address (ipv4).
On WindowsPE environment, only DHCP is supported. Select "DHCP (Auto)".

The following does not need to be entered.
"IP address","Subnet mask", "Gateway", "Name server".

Enable Wi-Fi

On WindowsPE environment, Wi-Fi is not supported.
Uncheck "Enable Wi-Fi".

Storage Server

Enter the IP address or server name of the server. with windows Shared folder.
Enter only either the IP address (ipv4) or the server name.
On WindowsPE environment, only Windows Share(CIFS) is supported.

Protocol

Select "Windows (CIFS)".
On WindowsPE environment, only Windows Share(CIFS) is supported.

Share(Win)

Required only for "Windows" connections.
Specify the Windows share name to connect to.
Write permission is required for the shared folder .

Directory

Specify the name of the directory (folder) to write the log to.
If left blank, it will be written to the shared folder for Windows share.
It is not necessary to add "\", at the beginning and end. (Even if it is attached, it will be ignored)
Specify the directory delimiter with "\".

example:
gplog/2012

For the specified directory, create / write a file, read the file size, and delete the written file (during a write test) are performed. Please set the authority appropriately.
Since file data read permission is not required, write-only operation is also possible.

* Even if you do not have permission to delete the file, the process will continue,
but the file written in the write test (that is automatically performed before the erase process) will remain unerased.

Account/Password

Enter the authentication ID (user name) and password used for connection.

The password is encrypted and stored in the created CD or USB flash drive, but it may be decrypted.
Please be careful about management when it is widely distributed.
For example, creating an authentication ID dedicated to log storage that can be written only to the specified folder.

When you press the "PW" button, the password you entered will be displayed. Press it again to display "*".
However, "PW" can be displayed only when entering a new character or after clearing all characters.

log file name prefix

It is possible to add special characters to the beginning of the log file name to be written.

(none) · · · It will be a normal file name.

[date(month,day)][hour][minute][second].log
ex: Log created at 13:08:12 on June 5th -> 0605130812.log

Fixed val · · · The character entered in the "Fixed val" field is added to the beginning.

[Fixed val]_[date(month,day)][hour][minute][second].log
ex:
Fixed val: SZ
Log created at 13:08:12 on June 5th -> SZ_0605130812.log

[Additional info1]/[Additional info2]
· · · The value entered by the operator in "Option"/"Additional info" is added to the beginning.

ex:
When "nomura" is entered in "Additional info1"
Log created at 13:08:12 on June 5th -> nomura_0605130812.log

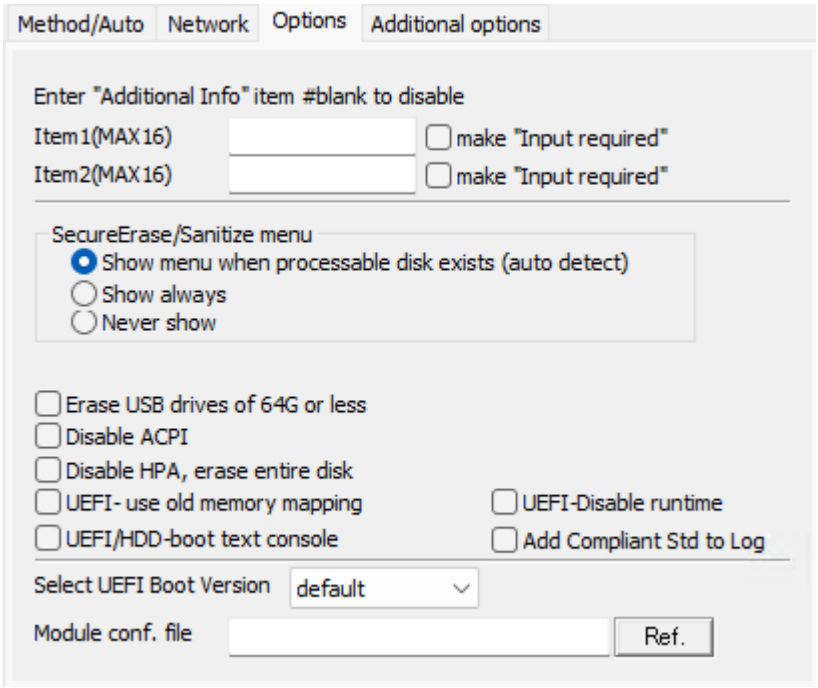
If the input value contains characters that cannot be used as a file name, it will be replaced with "_".

For "Additional info", see "Options" / "Enter additional info" below.

Enable NTP client

On WindowsPE environment, NTP client is not supported.

Options

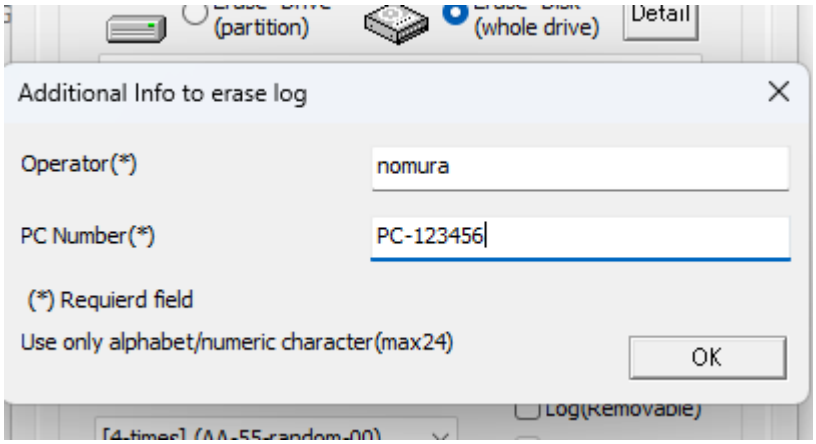


Enter "Additional Info" item #blank to disable

If you specify a value for the "Item1"/"Item2", the following screen will be displayed before the erase Windows is displayed, prompting the operator for input.
If you select "make 'input required'", you will not be able to proceed unless you enter some value in that item.
If it is not " input required", you can move to the next even if it is left blank.
The "Item1"/"Item2" can be up to 16 single-byte alphanumeric characters (spaces allowed).

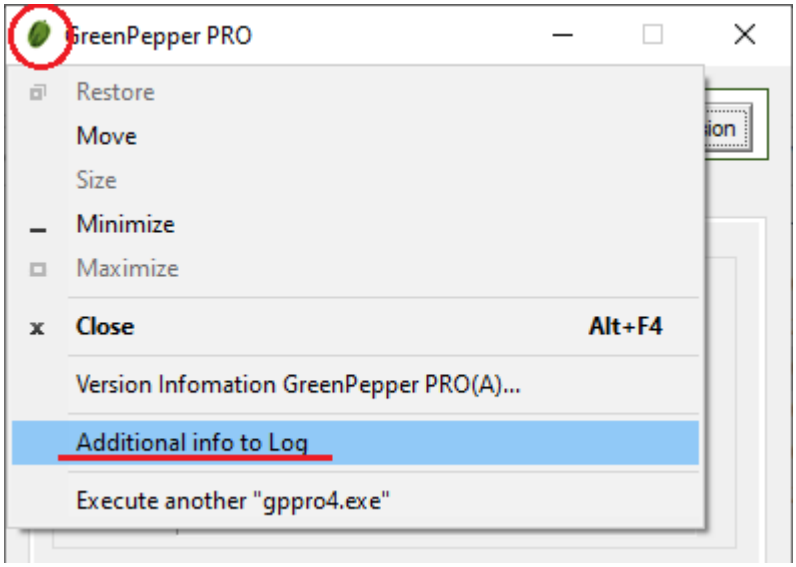
You can disable it by leaving the them blank.

It is convenient to use it for the person in charge of processing, the in-house management number of the PC, etc.



In the example of this screen,
Item1: "Operator" Required
Item2: "PC Number" Required

You can check and reset the entered information by clicking on the icon at the top left of the program and selecting "Additional info to log" from the system menu that appears.



Write to Log
* Written in the area subject to tampering check.

```
===
--- disk erase log ---------------------------
Operator : nomura
PC Number : PC-123456
disk : ATA ST3160813AS (156290904 kbyte) rev:SD2B
ser:9SY082C5
method : 4-times[AA-55-rand-00] -> verify
..... omitted below
===
92ae1655be5a5b95977863ac87c637a5
```

SecureErase / Sanitize menu

Not used on WindowsPE environment.

Erase USB drives of 64G or less

Not used on WindowsPE environment.
On Windows PE environment, removable drives of 128 Gbyte or less are always excluded from erasing.

Disable ACPI

Not used on WindowsPE environment.

Disable HPA, erase entire disk

Not used on WindowsPE environment.

UEFI - use old memory mapping

Not used on WindowsPE environment.

UEFI - disable runtime

Not used on WindowsPE environment.

UEFI / HDD - boot text console

Not used on WindowsPE environment.

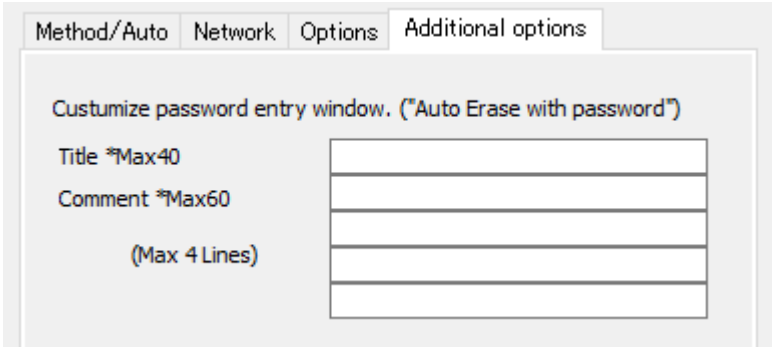
Add Compliant Std to Log

Not used on WindowsPE environment.

Module conf. file

Not used on WindowsPE environment.

Additional options



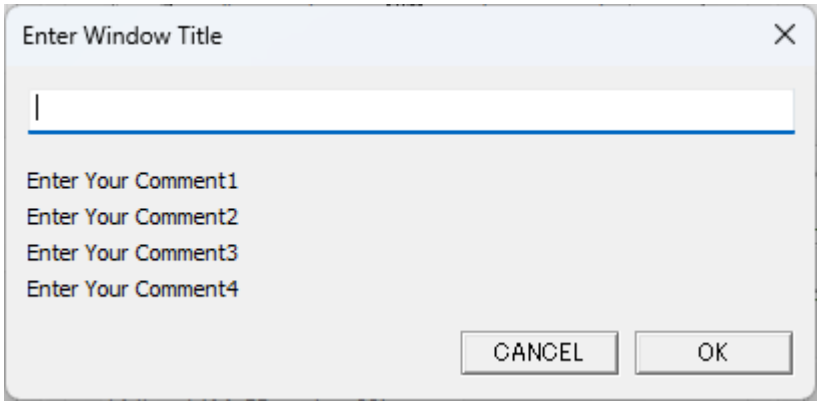
Title / comment

Specify the display text on the initial password input screen during "Auto erase with password".

Example:

Title: Enter Window Title
Comment:
Enter your comment1
Enter your comment2
Enter your comment3
Enter your comment4

When set in this way, the following screen will be displayed as password entry screen.

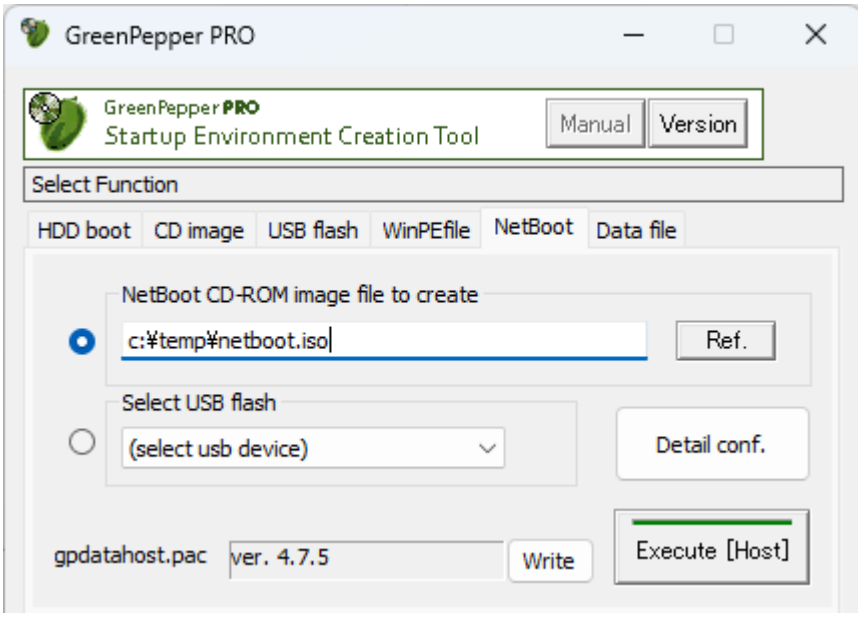


Creating Network boot host image / USB flash drive

Warning !
* "Site License"/"Company License" is requierd to use.
* With "Single user license", the program is executed in evaluation mode.
* A network boot data file (gpdataost.pac) is required for execution.

Set up and create the host function to start PC's to be erased using network boot (PXE) and execute the erase program.
Here you can create a bootable CD image file or configure USB flash drive.
Just by booting your PC using this CD/USB flash drive, you can build a host (server) that includes all of the following functions.

·Host function for network boot
·Loading the erase program on network booted PC's
·FTP server for the erasure program to write logs
·NTP server for time synchronization with network booted PC's



Please set one of the following.

*A check will be placed to the left of the currently valid item.

NetBoot CD-Rom image file to create

Specify the file to create. Enter the file name (full path) directly from the keyboard, or press the "Ref." button to specify the file.

Select USB flash

Select the USB flash drive to be set from the list.
* A list of USB removable drives is displayed.

When you make a selection, information such as the current setting type is displayed.

* Please note that the USB flash drive is initialized by the setting process and **the inside is erased**.

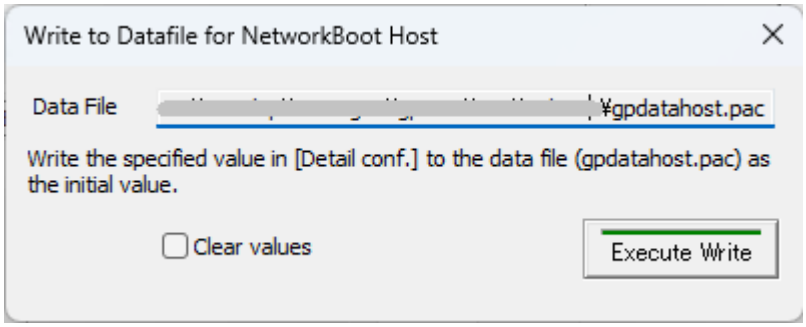
gpdatahost.pac - [Write]

When there is a valid network boot data file, the version will be displayed as shown in the image above.

The [Write] button allows you to write the values set in [Detaile conf.] to the data file (gpdatahost.pac).

The written value will be displayed as the initial value/fixed value the next time you start the "Startup Environment Settings Tool". Whether to use a changeable initial value or a fixed value depends on the "Fixed value" specification in "Customizing/Setting data file".

This is a convenient function when you use it frequently or when you want to specify a value and distribute it. *Here, only data related to "Network boot host settings" is written to (gpdatahost.pac). Other setting values are written to (gpdata.pac) by operating from the "Customizing/Setting data file" screen.



Data file

The currently valid data files are displayed.

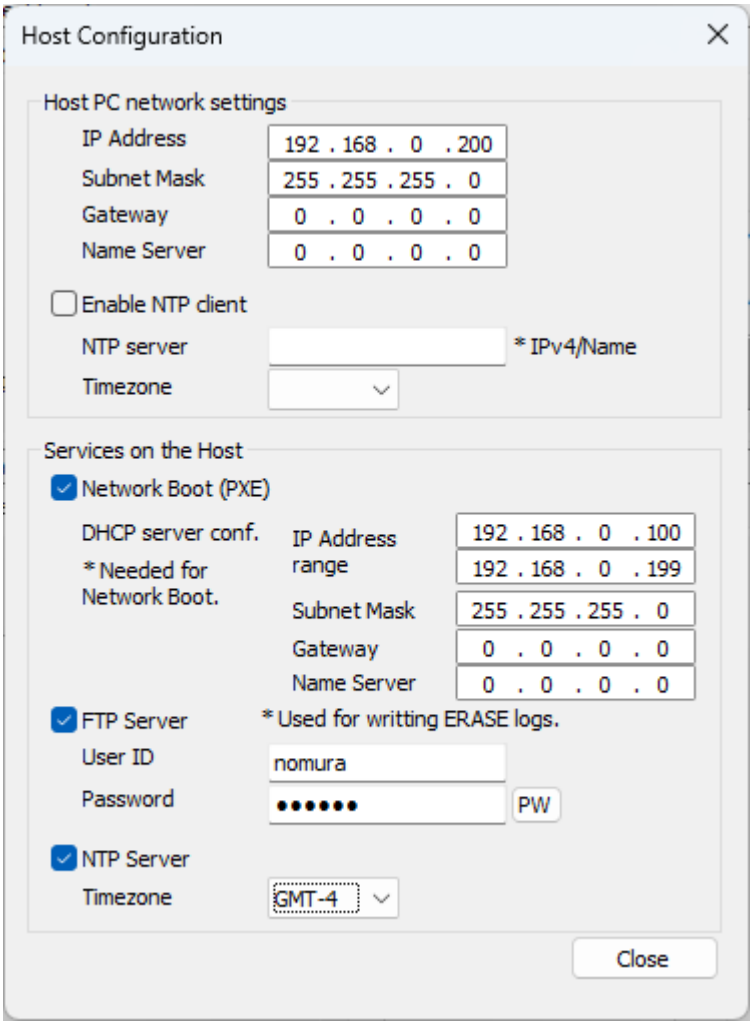
Clear Values

If you check and execute "Execute Write", the values written in the data file will be deleted.

Execute Write

Writes values to the currently valid data file.

Detail conf.



Host PC network settings

Settings for the host(server) PC itself.

IP Address/Subnet mask/Gateway/Name server

These are address settings for network boot host PC.
Please specify the IP address (IPv4), subnet mask, default gateway, and name server.
Default gateway and name server are not required. Please specify only if necessary.

Enable NTP client

Check this box if you want to synchronize the host time with an NTP server.

NTP server

If you check "Enable NTP client", specify the server to synchronize time with.
Specify by IP address (IPv4) or server name.
When using a server name, it is necessary to specify a "Name server".

Timezone

If you check "Enable NTP client", specify the time zone of the PC.
Specify between GMT-12 and GMT+12.
For example,
- San Francisco (USA) , "GMT-7"
- New York (USA) , "GMT-4"
- Berlin (Germany) , "GMT+2"
- New Delhi (India) , "GMT+5"
- Tokyo (Japan) , "GMT+9"

Services on the host

Service settings for network-connected client PCs.

Network boot (PXE)

Network booting uses a DHCP server to distribute IP addresses and other information necessary for booting. Therefore, if you want to use the network boot function, you must enable it and set the DHCP server information.
Here, set the IP address range (IPv4), subnet mask, gateway, and name server information distributed by the DHCP server. Gateway and name server are not required, but should be configured as needed.

FTP server

It can be used as an FTP server for saving erase logs over the network.
There is no need to enable it if you do not use it. Network booting is possible without enabling it.
If used, please specify User ID and Password for connecting to the FTP server.

When you press the "PW" button, the password you entered will be displayed. Press it again to display "*".
However, "PW" can be displayed only when entering a new character or after clearing all characters.

NTP server

It can be used as an NTP server when synchronizing the time with the PC to be erased using network boot.
There is no need to enable it if you do not use it. Network booting is possible without enabling it.

Timezone

If you use NTP server, specify the time zone, between GMT-12 and GMT+12.
For example,
- San Francisco (USA) , "GMT-7"
- New York (USA) , "GMT-4"
- Berlin (Germany) , "GMT+2"
- New Delhi (India) , "GMT+5"
- Tokyo (Japan) , "GMT+9"

If you check "Enable NTP client", please use the same time zone as NTP client.

Execute [Host]

Execute creating a CD-ROM image file/setting USB flash drive.
* Processing will take some time. Please wait until the end message appears.

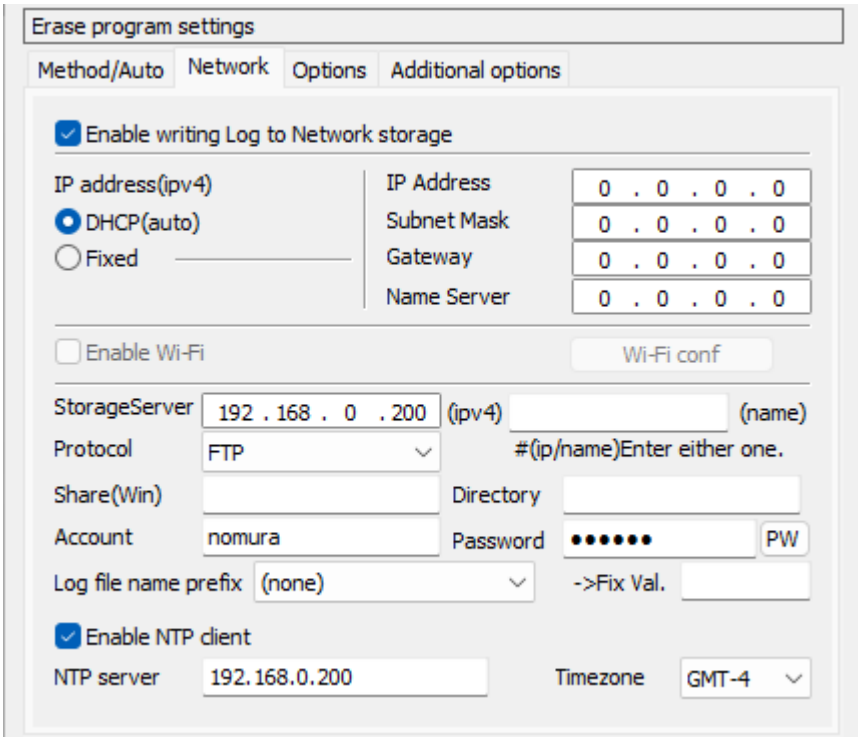
For "Points to note in the setting procedure", see Setting bootable "USB flash drive".
The procedure will be similar.

Specifying erase program options

This network boot host can boot network-connected PC's and let ths PC's execute the erase program.
The erase program to be executed is the same as "Boot from CD/USB flash drive", and options can be specified in the same way. For details on specifying options, see "Common options".

For example, when you set the network boot host address etc. in "Detail conf." as shown in the image above, and specifying the "Network" option of the erasure program as shown in the image below, the following feature will be enabled.

·Obtain address by DHCP from the network boot host
·Write log to the network boot host using FTP
·Time synchronization with the network boot host using NTP

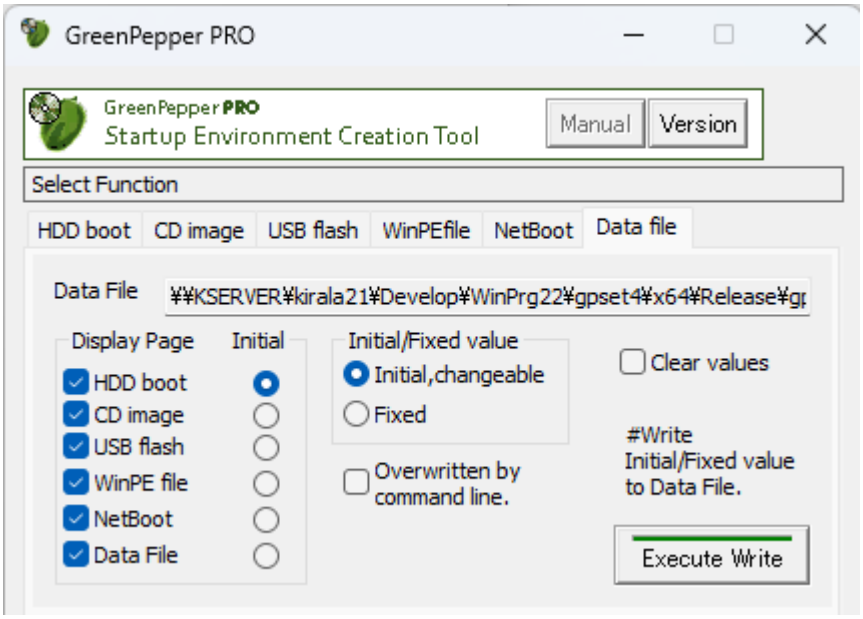


Customizing/Setting data file

In the data file settings, various customization information can be saved for the data file used by the "Startup Environment Creation Tool". These include erasing methods, changing the initial value of erasing options, fixing values, and specifying the display page.
The customized information saved in the data file is read when the "Startup Environment Creation Tool" is started, and the customized information becomes effective.

This function is based on the assumption that the system department, etc. will create a data file in which the erasing method etc. are set in advance, and distribute this program together with the data file within the company.
It is possible to establish a unified erasing method within the company and minimize the learning of operations by general users.

* Since it is saved in units of data files, you can use files with different environments properly.
* Unlike the settings in the registry etc., the environment can be realized simply by placing gpset4.exe and customized gpdata.pac on the network drive.



Data file

The currently valid data file is displayed.
The data file used is in the same folder as gpset4.exe or in the [data] folder at the same level as gpset4.exe.

Also, from the command line, it is also possible to specify in the form of,

gpset4.exe / d:[data file]

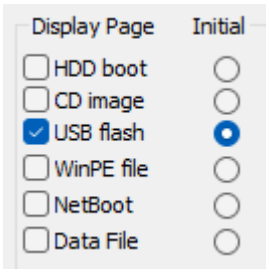
Options

For the options , see "Common options".
The contents of the set options are saved.

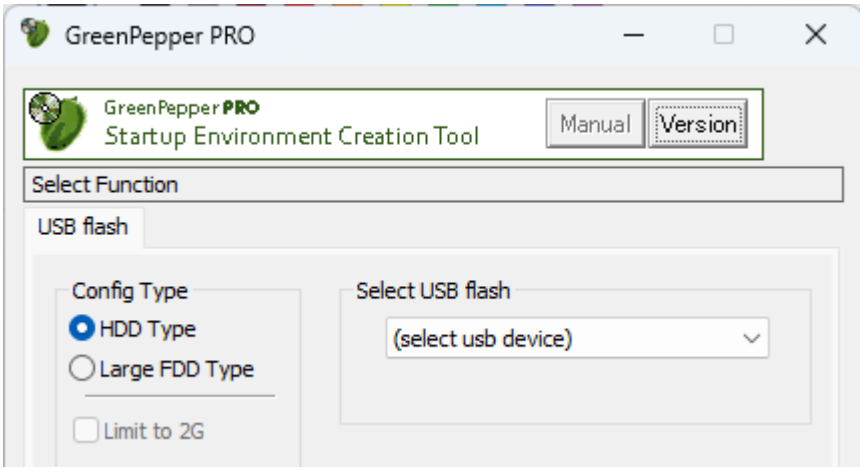
Display page / Initial

You can specify the page to be displayed from the pages of "HDD boot", "CD image", "USB flash", "WinPE file" and "Data file", and hide the other pages.
You can also specify the page ("initial" selection) that will be displayed immediately after starting the program.

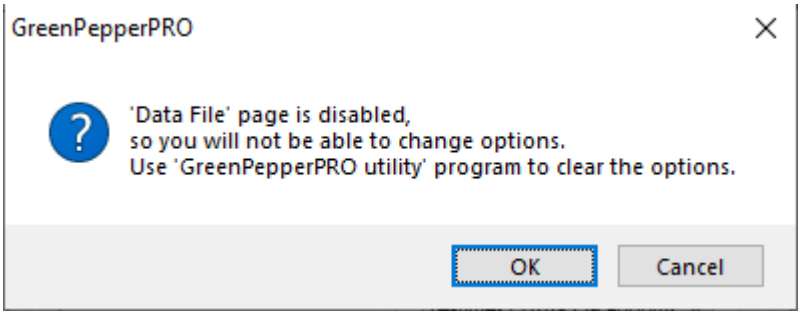
For example, if you specify only "USB flash".



The next time you start up, only "USB flash" will be displayed as shown below, and you can use it as a program dedicated to configure USB flash drive.
This is a convenient function when distributing an erase environment using USB flash drive to end users.



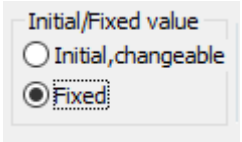
If you do not display the Data File page, **you will not be able to change options stored in that data file**.
If you uncheck "Data file" and use the settings, the following message will be displayed for confirmation.



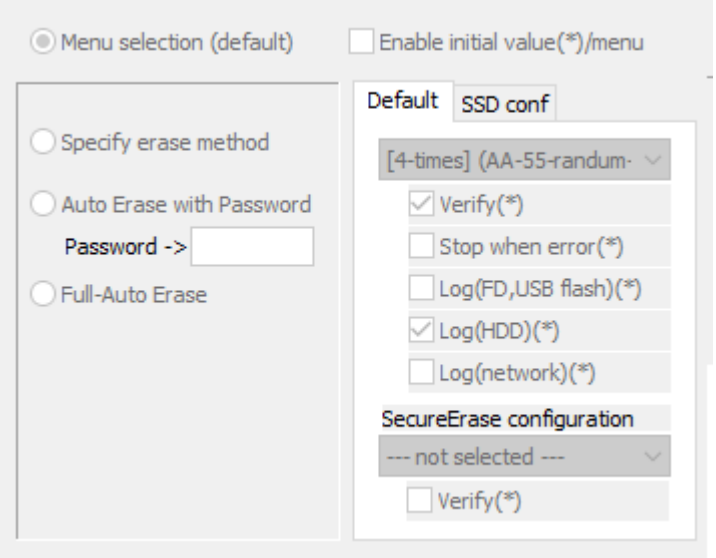
To clear the settings of the data file and return it to the initial state, use "Data file" in "Utilities for administrator" /"Operation of each function".

Initial/Fixed value

In the case of "Initial, changeable", only the initial value can be set and the user can freely change the value.
In the case of "Fixed", the value is fixed and cannot be changed by the user.



When "Fixed" is set, the screen display is grayed out as shown below, and the value cannot be changed.



Overwritten by command line

Initial values, fixed values, etc. can be specified in the data file or command line to gpset4.exe.
If you check here, even if the value is set in the data file, if there is a command line specification when executing gpset4.exe, the command line specification has priority.
If unchecked, the value in the data file takes precedence and cannot be changed by command line specification at runtime.

For example, if you do not want to allow the user to change the value of the data file, you can leave it unchecked, and if you want to be able to flexibly change it from the command line each time, you can check it.

Clear values

By checking this and pressing "Execute Write", you can clear the value written in the data file and return it to the initial state.
However, if you hide the "Data file" page, clear it by using "Utilities for administrator" / "operation of each function".

Execute Write

Writes the specified options to the data file. It will be enabled the next time you start the "Startup Environment Creation Tool".

Customizing/setting by command line

In "Customizing/setting data file", you can use the data file to specify the processing contents in a fixed manner.
The command line specification allows you to more flexibly specify the initial state, processing content, etc.

Initially, **the data file settings take precedence over the command line settings**.
This is from the idea of preventing users from being able to change it freely on the command line.
Which one to prioritize can be changed by "Overwritten by command line" in the data file.

Details of command line options

The command line options are as follows.
For individual meanings and screen display when set, see "Customizing/Setting data file".

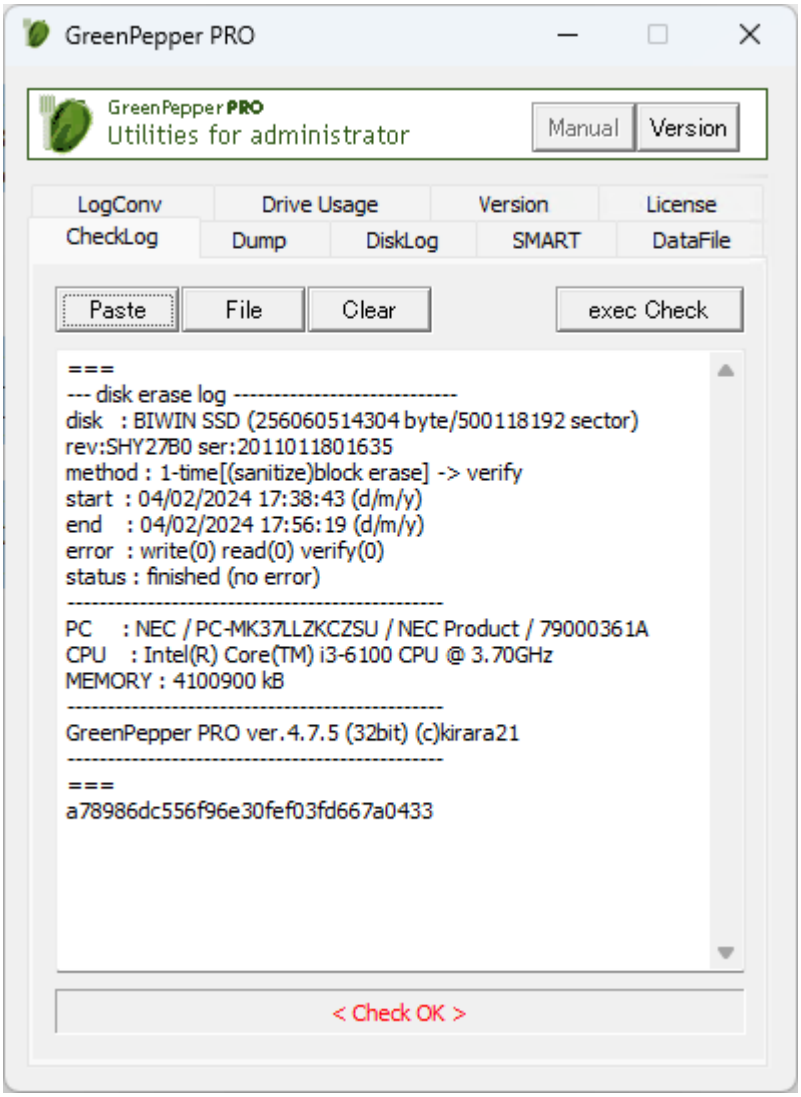
Item	Settings	Description
Data file	/D:[data file]	Specify the data file. If the data file name contains spaces, enclose it in "" (double quotation marks).
Fixed Erase method, Auto erase	/A:D	Specify fixed erase method
	/A:P[password]	Auto erase with password
	/A:A	Full-auto erase
	ex. /A:P1234 Auto erase with password, using password "1234".	
Erase method	/M:[1,2,3,4][6,7,8][E][L][H][N][V][v]	1-4: Number of erasures, 1-4 times 6-8: Secure Erase, 1-3 times (If not specified, it will be "--- not selected ---". ') E: Stop when error L: Write log to FD/USB flash drive H: Write log to HDD N: Write log to network share V: Verify v: Verify(Secure Erase)
	/S:[1,2,3,4][6,7,8][V][v]	/S If specified, "Enable SSD configuration" 1-4: Number of erasures, 1-4 times 6-8: Secure Erase, 1-3 times (If not specified, it will be "--- not selected ---". ') V: Verify v: Verify(Secure Erase)
	ex. /A:D /M:3VH Fixed erase method. Erase 3times, Verify, Log(HDD). /A:Ppass /M:16LHVv Auto erase with password(pass), erase 1time, Log(USB stick,HDD), Verify, Secure erase 1time, Verify. SSD configuration not specified.	
Erasure Pattern	/E:[P1],[P2],[P3],[P4]:[t]	Erasure Pattern for 1-4times erasure. *If you use the default value, specify only ",". [P1]: for 1-time, Two hexadecimal digits. "RD" for random. [P2]: for 2-times, Two+Two hex digits. "RD" for random. [P3]: for 3-times, Two+Two+Two hex digits. "RD" for random. [P4]: for 4-times, Two+Two+Two+Two hex digits. "RD" for random. If you do not want to perform TRIM on the SSD, add ":t".
	ex. /E:00,AA,00,RDRD00,AAFFRD00 /E:,,RDRD00,:t	
USB flash drive, Config type	/U:[H][F][2]	H: HDD type F: Large FDD type 2: Limit to 2G
	ex. /U:H Set to HDD type	
	/L:[en,jp]	en: English jp: Japanese

Language	ex. /L:jp Set language to Japanese	
Options	/O:[U][P][S][H][V][E][T][D][B]	U: Erase USB drives of 64G or less P: Disable ACPI S0: SecureErase/Sanitize menu: Auto S1: Show always S2:Never show H: Disable HPA, erase entire disk V: UEFI- use old memory mapping E: UEFI- disable runtime T: UEFI/HDD- boot text console D: Add compliant std to log B: Select UEFI boot program version. B0:default B1:old-ver1 B2:old-ver2
	ex. /O:HS1 Disable HPA, Show Secure Erase menu always.	
Additional info	/N:title1,0/1,title2,0/1	Specify the following separated by commas Item1 title text (space character should be replaced by "_" underscore) 1 if specify input required, 0 otherwise Item2 title text (space character should be replaced by "_" underscore) 1 if specify input required, 0 otherwise
	ex. /N:Operater,1,PC_Number,0 Set "Operator" as a required input item and "PC Number" as an optional input item	
Display page	/T:[H][U][C][P][S]	The specified page is displayed H: HDD boot U: USB stick C: CD image P: WinPE config file S: Data file The first specified page will be the initial display page.
	/T:H Display only "HDD boot" page /T:CU Display "USB stick","CD image" page. Set the initial display page to the "CD image" page.	
Fixed value	/F	If specified, the value will be fixed. Cannot be changed.
Module configuration file	/J:[file path]	Specify the module configuration file to use. If the file path contains spaces, enclose it in "" (double quotation marks).
Network specifications		
Enable writing log to Network Storage	/NE	Enabled if specified
IP address	/NI:D /NI:I[x.x.x.x,x.x.x.x,x.x.x.x ,x.x.x.x]	D: DHCP I: Specify fixed value (IP,subnetmask, default gateway, nameserver) (Gateway and name server can be omitted)
	ex. /NI:D DHCP /NI:I192.168.0.10,255.255.255.0,192.168.0.1 IP:192.168.0.10, netmask: 255.255.255.0, gateway: 192.168.0.1	
Protocol	/NW:[W][F]	W: Windows share (SMB/CIFS) F: FTP
	ex. /NW:W Windows share	
Storage Serevr	/NV:[x.x.x.x] /NV:[server name]	Specify IP address of the server, or server name
	ex. /NV:192.168.0.5 Specify server address 192.168.0.5	
Share (WIN)	/NS:[share name]	Specify share name
	ex. /NS:TEST Specify share name TEST	
Directory	/ND:[directory]	Specify directory name. If the directory name contains spaces , enclose in "" (double quotation marks). (WIN only)
	ex. /ND:gplog/2012 Specify directory name "gplog/2012"	

Account	/NU:[account]	Specify the account/authentication ID
	ex. /NU:nomura	
Password	/NP:[password]	Specify password (plain text)
	/NP:password	
Password(encrypted)	/NC:[encrypt password]	Specify the encrypted password * Please contact us for information on how to create an encrypted password.
Log file name prefix	/NX:[0-3](fixed value)	0: none 1[fixed value]: fixed value 2:"additional info1" input value 3:"additional info2" input value
	ex. /NX:1GP Specify fixed value "GP" /NX:2 Specify input value of "additional info1"	
NTP client	/NT:[NTP server],[Time zone]	Specify NTP server. Server Name or IP(v4) assress. Spicify Time zone. "GMT-4","GMT+3" style.
	ex. /NT:time.ntpserver.com,GMT-4	
Network (Wi-Fi) specifications		
Enable Wi-Fi	/WE	Enabled if specified
SSID	/WS:[SSID]	Specify SSID
Encryption	/WA:[W/P/E]	W:WEP P:WPA/WPA2-PSK E:WPA/WPA2-EAP
Key(WEP/PSK)	/WK:"[text]" /WK:[hex key]	Specify the authentication key for WEP, WPA / WPA2-PSK. Enclose in double quotes for text. For hexadecimal, specify without double quotation.
	ex. /WK:"WPAPSKKEY" Specify key in text, "WPAPSKKEY" /WK:0506AF4D5DD0B33E Specify key in hexadecimal, 0506AF4D5DD0B33E	
Auth ID(EAP)	/WU:[authentication ID]	Specify authentication ID for WPA/WPA2-EAP.
Password(EAP)	/WP:[password]	Specify password (plain text) for WPA/WPA2-EAP
Password(encrypted)	/WC:[encrypt password]	Specify encrypted password for WPA/WPA2-EAP. * Please contact us for information on how to create an encrypted password.

Executing "Utilities for administrator"

The "Utilities for Administrator"(gputil4.exe) can be easily executed without any prior installation work.
Follow the procedure below to execute it.



Double-click [gputil4.exe] to start it.

· **For online download, it is in the unzipped folder.**
· **If provided on a CD-ROM, it is located on the product CD-ROM (root).**

You can boot directly from the product CD-ROM, or copy it to a hard disk, network drive, etc. for use.

Administrator privileges required to run

Vista/7/2008 or later (include Windows10)
The following message will be displayed.

Do you want to allow this app to make changes to your device?
---
* The message varies depending on the Windows version.

* If you are logged on as a non-administrator,
You will be required to enter the administrator user password.

Click (continue) "Yes" to boot.

About the [manual] folder

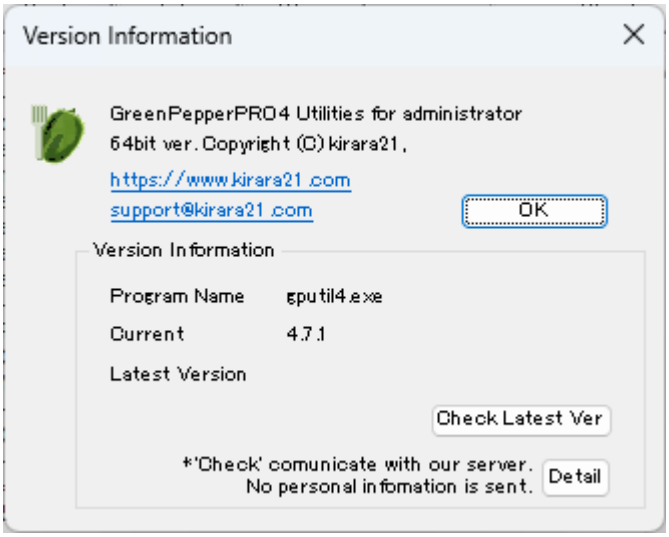
The "Manual" button on the upper right of the screen is enabled when the [manual] folder exists in the same folder as [gputil4.exe], and the manual will be displayed when the button is pressed.
If you want to display the manual with this button, you need to copy the [manual] folder along with [gputil4.exe].

*"index.html" in the [manual] folder is called. It is also possible to display any document.

when "disabled" when "enabled"

[Version] button

You can check the version currently in use and the latest version by clicking the [Version] button on the upper right of the screen.



Check Latest Ver

When you press this button, it communicates with our (kirala21) server and displays the latest version information on the screen.

* Customer-specific information (PC information, Windows information, etc.) will NOT be sent in this communication.
* Communicate via http. Please use it in an environment where you can access the Internet via http.

Detail

Click the [Detail] button to see the details of what is sent to the server.
No further information will be sent.

Check log

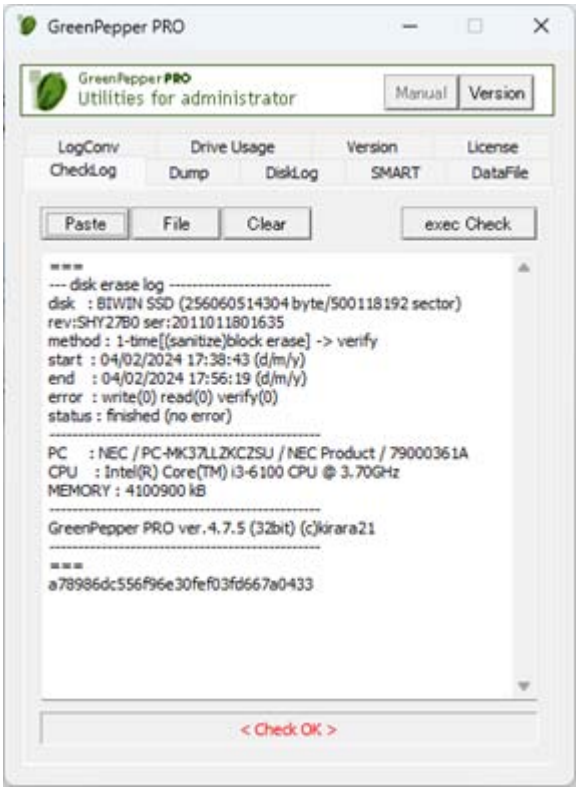
"Check Log" checks the validity of the log file created by the "Green Pepper PRO" system.

Log file output

In the "Boot up erase program", the log is written to the hard disk, floppy disk, and USB flash drive after the erase process is completed.
The "Windows Erase Program" writes to the hard disk after the erase process is completed. In addition, it is output as a "End Report" in the erase process and read check process.

They are prepended with a "checksum" string (eg "92ae1655be5a5b95977863ac87c637a5").
This is to check that the log contents are output by "Green Pepper PRO" and that no single character has been changed since then.
If even one character in the log is changed, the internal characters and the checksum will be inconsistent, and it will be known that the log has been tampered with.

* Handle the log file in units of the contents between "===" (including itself) and the checksum character string on the next line.



Operation on the screen

Paste
Paste the log file that has been "copied" in advance to the screen.

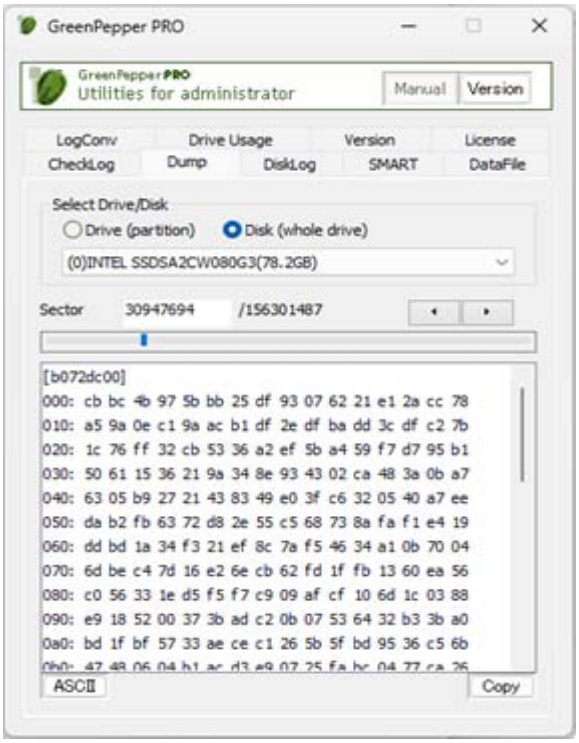
File
Read the log file saved in the disk drive.

Clear
Clear the screen.

exec Check
Check the validity of the log file displayed on the screen.

Dump disk

"Dump disk" is a function that displays the contents of the connected disk as they are.
You can actually see what the contents of the disk are now.



Operation on the screen

Select Drive / Disk
Select "Drive" unit (C, D, E, ...) or "Disk" unit (physical / RAID logical disk) unit.
From the drives / disks displayed in the list, select the disk you want to display.

Sector
The currently displayed sector number is displayed.
You can also display the contents of the specified sector by entering the sector number here.

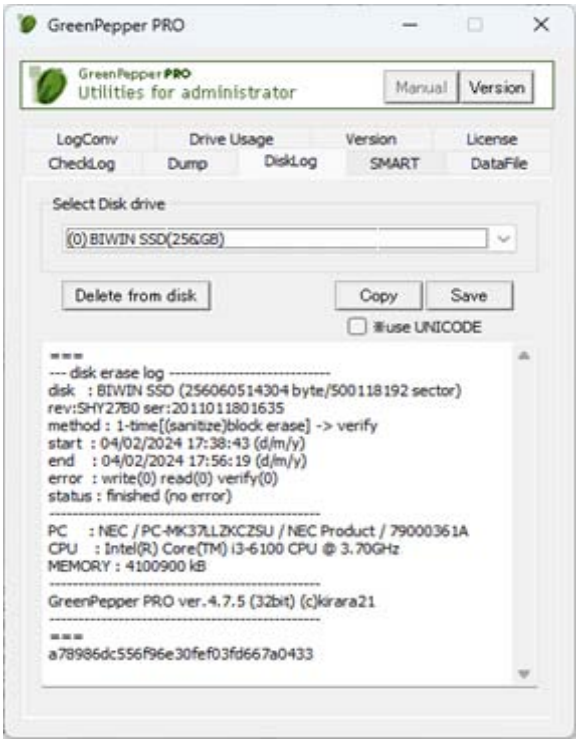
Move Sector
You can move sector by any of the following methods.
*Enter the sector number you want to display in "Sector"
*Right of "Sector", press the left / right move button
*Operate the slider bar with the mouse under "Sector".

ASCII / HEX
Switches between ASCII: character display and HEX: hexadecimal display.

Copy
Copies the information displayed on the screen to the clipboard. You can then "paste" it into Notepad or other programs.

Disk log

"Disk log" is a function to read the log written to the hard disk drive.
The log is a file that was written directly to the hard disk drive by the "Boot up Erase Program" or "Windows Erase Program" after the erase process. It is written to the beginning area of the disk drive.



Operation on the screen

Select disk
Select the disk drive for which you want to view the logs.
If the log has been written, the contents will be displayed on the screen

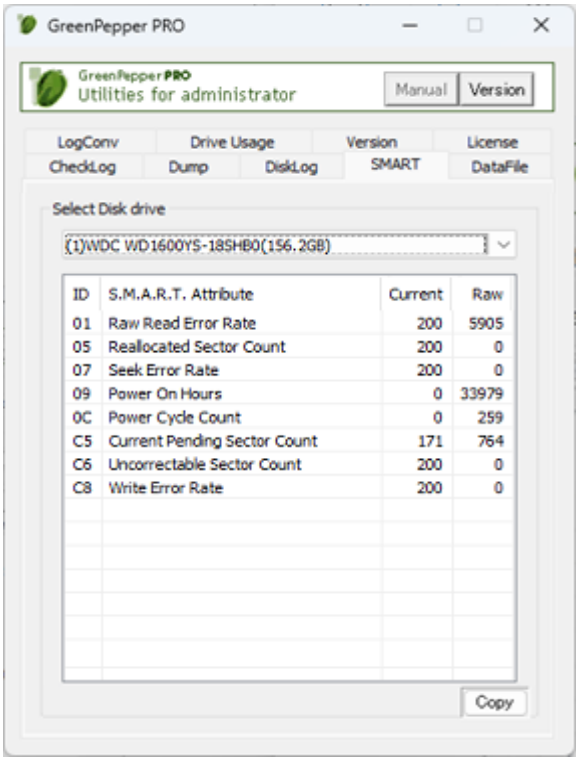
Delete from disk
Erase the log from disk. Only the written part of the disk log is overwritten with zero.

Copy
Copy (to clipboard) the contents of the log.

Save
Save the contents of the log to a file.
If you check [* use UNICODE], the file will be saved with [UNICODE]. If unchecked, it will be [ANSI].

S.M.A.R.T.

"SMART" displays the contents of S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology), which is information that can lead to failures in the disk drive itself.



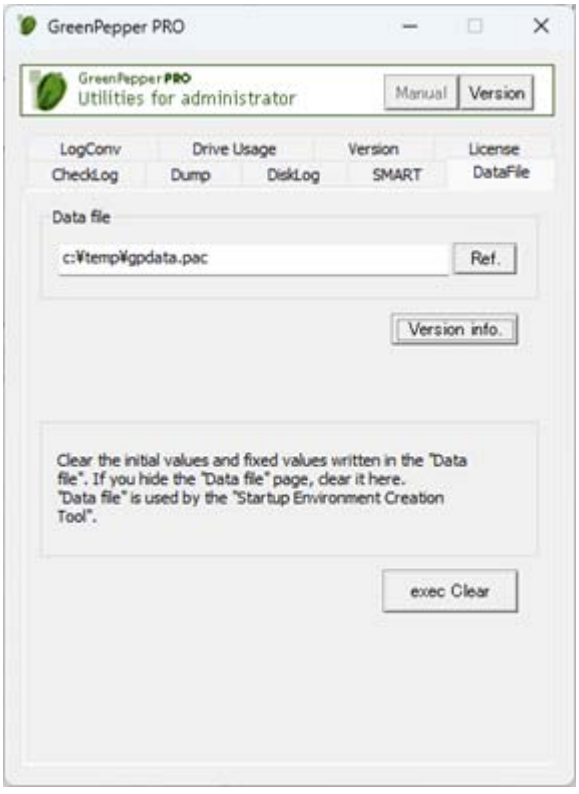
Operation on the screen

Select disk
Select the disk drive for which you want to view the S.M.A.R.T. information.

Copy
Copies the information displayed on the screen to the clipboard. You can then "paste" it into Notepad or other programs.

Data file

In "Data file", operate the data file (gpdata.pac) used in "Startup environment creation tool".
* You can also use for Network boot data file (gpdatahost.pac).



Operation on the screen

Data file
Specify the data file you want to operate. It can also be specified by clicking the "Ref." button.

Version Info.
Displays the version of the specified data file.

Net (0/1) · · · 1: Network (LAN, USB-LAN) log compatible data file 0: Not supported
WiFi (0/1) · · · 1: Network (WiFi) log compatible data file 0: Not supported

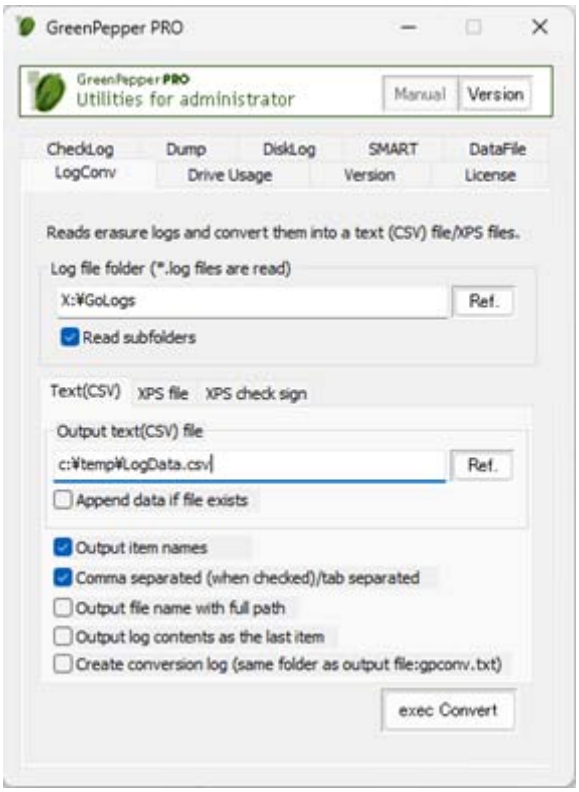
See Executing "Startup environment creation tool"/ "Data file" type

exec Clear
Clears the customization information written by the "Customizing/Setting data file " operation and returns the data to the initial state.
If you hide the "Data file" page of the "Startup environment creation tool", clear it by this operation, and then use the "Startup environment creation tool" again to set the data file.

Log Conv

In "Log Conv" (Log Conversion), reads erasure log files, convert them into a text (CSV) file.
You can also create a "Disk Erasure Report" in XPS file format from the log file.

When reading, checksums are checked and only valid log files are converted.
The text file can be used in Excel, databases, etc.



Operation on the screen

Text(CSV) ----------

Log file folder (*.log files are read)
Specify the folder where the erasure log is saved. You can also specify a folder using the "Ref" button.
Read files with the extension ".log" in the specified folder.
If you check "**Read subfolders**", files in subfolders will also be included.

Output text (CSV) file
Specify a file name of output text (CSV) file. You can also specify a file name using the "Ref" button.
If you check "**Append data if file exists**", when the specified file already exists, the data to be processed this time will be added to the end of the file. If not checked, existing file will be deleted.

Output file format
Comma or tab seperated. Line seperate code is CR+LF.
* Items may change in future versions.

Item Name	Description	Example
MODEL	Disk drive Model	"Samsung SSD 970 EVO Plus 250GB"
SIZE	Disk Drive Size (bytes)	250059350016
SECTOR	Disk Drive Size in Sector(512byte)	488397168
REV	Disk Drive Revision	"1B2QEXM7"
SER	Disk Drive Serial Number	"S4EUNG0M120524V"
HPA	HPA/AMA configuration	"HPA enabled." "AMA enabled."
DCO	DCO configuration	"DCO enabled."
METHOD	Erase method	"2-times[(sanitize)block erase-00] -> verify"
START	Process start Date/Time	"October 14, 2023 15:03:04"
END	Process end Date/Time	"October 14, 2023 15:58:48"
ERR_WRITE	Write Error Count (total)	46
ERR_WRITE1	Write Error Count in Step1	12
ERR_WRITE2	Write Error Count in Step2	8
ERR_WRITE3	Write Error Count in Step3	16
ERR_WRITE4	Write Error Count in Step4	10
ERR_READ	Read Error Count	156
ERR_VERIFY	Verify Error Count	1054
RETRY_WRITE	Retry Count in Write Process (total)	201
RETRY_WRITE1	Retry Count in Write Step1	48
RETRY_WRITE2	Retry Count in Write Step2	32
RETRY_WRITE3	Retry Count in Write Step3	56
RETRY_WRITE4	Retry Count in Write Step4	65
RETRY_READ	Retry Count in Read Process	358
STATUS	Erase Process Status	"OK" or "ERR"
STATUS_TEXT	Erase Process Status in Text	"finished (no error)", "finished (verify error)"
STANDARD	Compliant standard	"NIST.SP.800-88.Rev1(clear) compliant"
OS	Operation System (when Windows)	"WindowsPE(10.0.22621.1)"
PC	PC information	"NEC PC-MK37LLZKCZSU 79000361A"
PCVEND	PC Vender (>= Gppro 4.7.5)	"NEC"
PCPROD	PC Product name (>= Gppro 4.7.5)	"PC-MK37LLZKCZSU"
PCVER	PC Version (>= Gppro 4.7.5)	"NEC Product"
PCSER	PC Serial NUmber (>= Gppro 4.7.5)	"79000361A"
CPU	CPU infomation	"Intel(R) Core(TM) i3-6100 CPU @ 3.70GHz"
MEMORY	Memory(RAM) size	"4100900 kB"
PROG	Process program name	"GreenPepper PRO Ver.4.7.5 (c)kirara21"
ADDINFO1	Additional infomation1, title	"PC-NO"
ADDINFO1_VAL	Additional infomation1, input value	"CB1234"
ADDINFO2	Additional infomation2, title	"USER"
ADDINFO2_VAL	Additional infomation2, input value	"nomura"
FILENAME	Log file name	"26140307.log","c:\GPlog\2024\26140307.log"
LOG	The log file itself, including line breaks	"===\r\ndisk : ATA ....."

Output item names
If checked, item names will be output as the first line.
However, if "**Append data if file exists**" is specified and the output file already exists, item names will not be output.

Comma seperated (when checked)/tab seperated
If checked, items are separated by commas. If unchecked, separated by tab code.

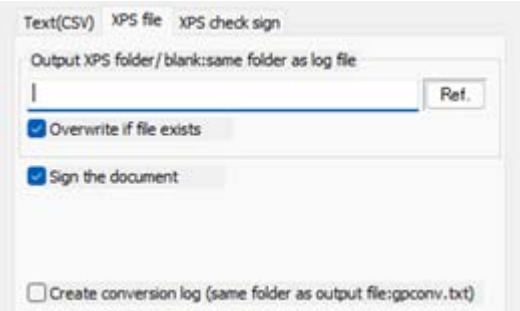
Output file name with full path
Specifies the output method for the "FILENAME" item of the output file.
If checked, the file name will be output as the full path from the root. If not checked, only the file name without the path will be output.

Output log contents as the last item
If checked, the contents of the log file will be output as is as the final item of the output file.
The entire log file is enclosed in double quotes, but it contains line breaks.

Create Conversion log (same folder as output file:gpconv.txt)
Create a processing log file to check the processing status of individual files.
A file will be created with the name "gpconv.txt" in the same folder as the output file.
[OK], [Format Error], and [Checksum Error] are recorded for each file.

exec Convert
Perform the conversion.

XPS file ----------



Log file folder (*.log files are read)
Specify the folder where the erasure log is saved. You can also specify a folder using the "Ref" button.
Read files with the extension ".log" in the specified folder.
If you check "**Read subfolders**", files in subfolders will also be included.

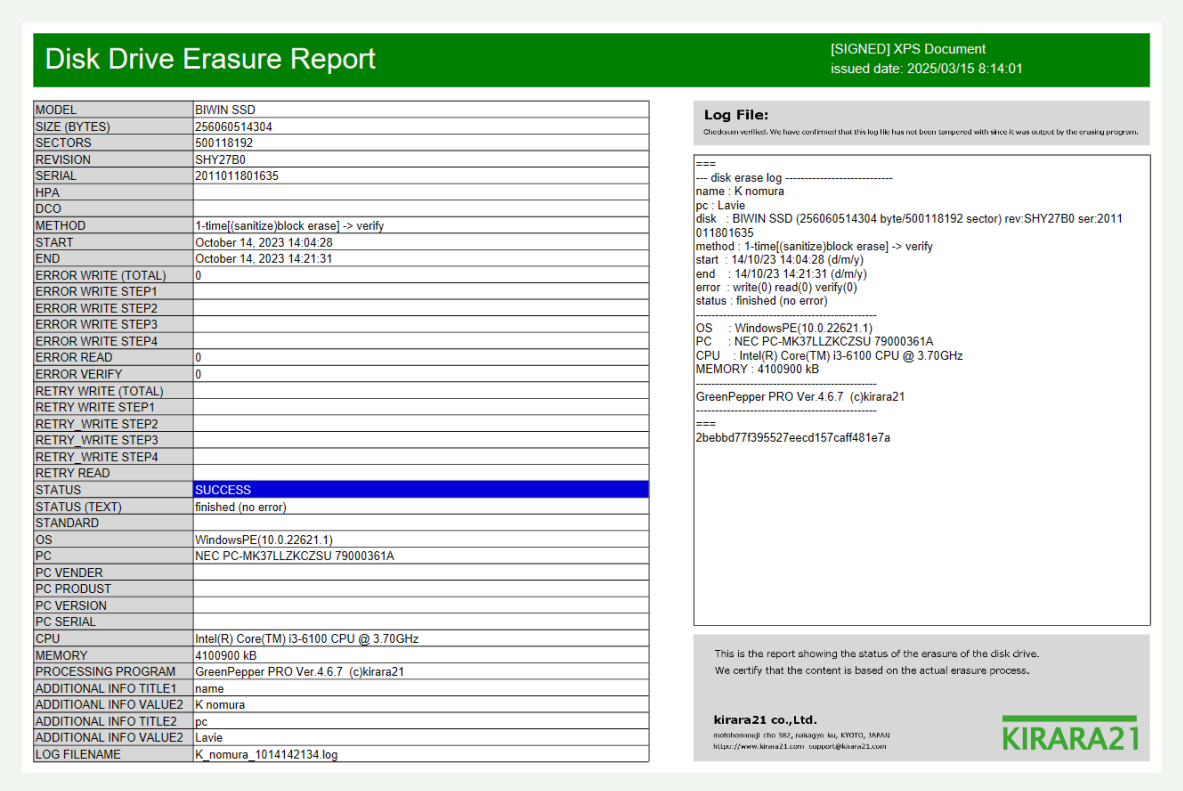
Output XPS folder
Specify a folder name of output XPS files. You can also specify a folder name using the "Ref" button.
If it is blank, the output will be in the same folder as the log files.

If you check "**Overwrite if file exists**", the file will be overwritten if a file with the same name already exists. If you do not check this, the file will be output with a different file name.

Sign the Document
XPS files are signed to ensure that it has not been altered since it was output.

Create Conversion log (same folder as output file:gpconv.txt)
Create a processing log file to check the processing status of individual files.
A file will be created with the name "gpconv.txt" in the same folder as the output file.
[OK], [Format Error], and [Checksum Error] are recorded for each file.

XPS file sample (enlargeable)



Disk Drive Erasure Report

[SIGNED] XPS Document
issued date: 2025/03/15 8:14:01

MODEL	BIWIN SSD
SIZE (BYTES)	256060514304
SECTORS	500118192
REVISION	SHY27B0
SERIAL	2011011801635
HPA	
DCO	
METHOD	1-time[(sanitize)block erase] -> verify
START	October 14, 2023 14:04:28
END	October 14, 2023 14:21:31
ERROR WRITE (TOTAL)	0
ERROR WRITE STEP1	
ERROR WRITE STEP2	
ERROR WRITE STEP3	
ERROR WRITE STEP4	
ERROR READ	0
ERROR VERIFY	0
RETRY WRITE (TOTAL)	
RETRY WRITE STEP1	
RETRY_WRITE STEP2	
RETRY_WRITE STEP3	
RETRY_WRITE STEP4	
RETRY READ	
STATUS	SUCCESS
STATUS (TEXT)	finished (no error)
STANDARD	
OS	WindowsPE(10.0.22621.1)
PC	NEC PC-MK37LLZKCZSU 79000361A
PC VENDER	
PC PRODUST	
PC VERSION	
PC SERIAL	
CPU	Intel(R) Core(TM) i3-6100 CPU @ 3.70GHz
MEMORY	4100900 kB
PROCESSING PROGRAM	GreenPepper PRO Ver.4.6.7 (c)kirara21
ADDITIONAL INFO TITLE1	name
ADDITIOANL INFO VALUE2	K nomura
ADDITIONAL INFO TITLE2	pc
ADDITIONAL INFO VALUE2	Lavie
LOG FILENAME	K_nomura_1014142134.log

Log File:
Checksum verified. We have confirmed that this log file has not been tampered with since it was output by the erasing program.

```
===
--- disk erase log -------------------------
name : K nomura
pc : Lavie
disk   : BIWIN SSD (256060514304 byte/500118192 sector) rev:SHY27B0 ser:2011
011801635
method : 1-time[(sanitize)block erase] -> verify
start  : 14/10/23 14:04:28 (d/m/y)
end    : 14/10/23 14:21:31 (d/m/y)
error  : write(0) read(0) verify(0)
status : finished (no error)
----------------------------------------------
OS     : WindowsPE(10.0.22621.1)
PC     : NEC PC-MK37LLZKCZSU 79000361A
CPU    : Intel(R) Core(TM) i3-6100 CPU @ 3.70GHz
MEMORY : 4100900 kB
----------------------------------------------
GreenPepper PRO Ver.4.6.7  (c)kirara21
----------------------------------------------
===
2bebbd77f395527eecd157caff481e7a
```

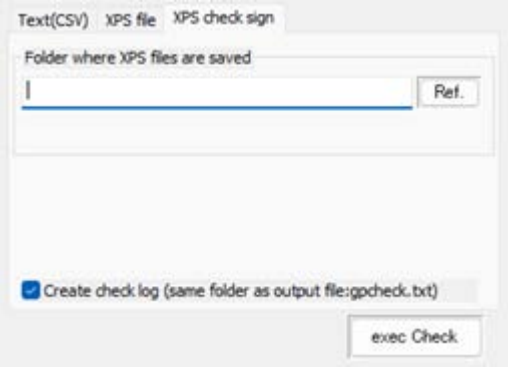
This is the report showing the status of the erasure of the disk drive.
We certify that the content is based on the actual erasure process.

kirara21 co.,Ltd.
motohonnouji cho 382, nakagyo ku, KYOTO, JAPAN
https://www.kirara21.com support@kirara21.com

KIRARA21

exec Convert
Perform the conversion.

XPS check sign ----------



Folder where XPS files are saved (*.xps files are read)
Specify the folder where the XPS files is saved. You can also specify a folder using the "Ref" button.
Read files with the extension ".xps" in the specified folder.

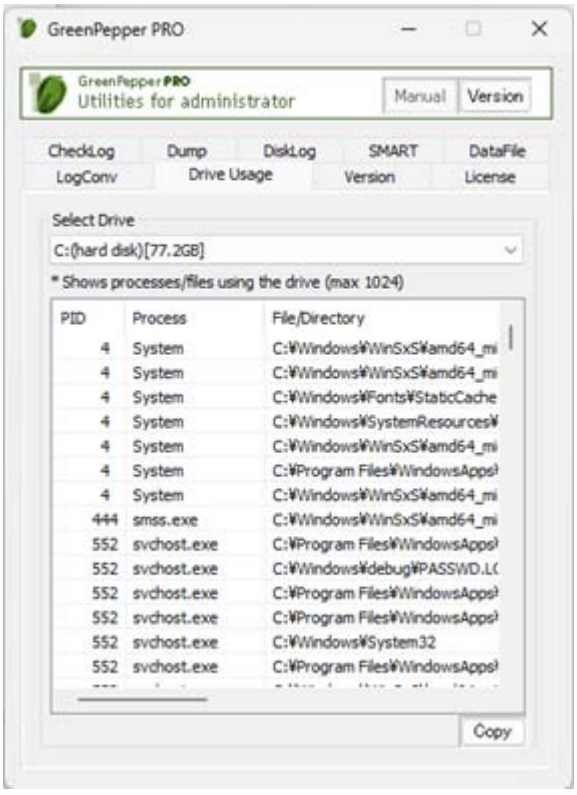
Create check log (same folder as output file:gpcheck.txt)
Create a processing log file to check the processing status of individual files.
A file will be created with the name "gpcheck.txt" in the same folder as the sepcified XPS folder.

exec Check
Perform the check process.

Drive Usage

Displays a list of processes that are using programs/files on the drive specified in "Select Drive".
This can be used to investigate cases where the drive cannot be locked when erasing the drive or setting up a USB flash drive.

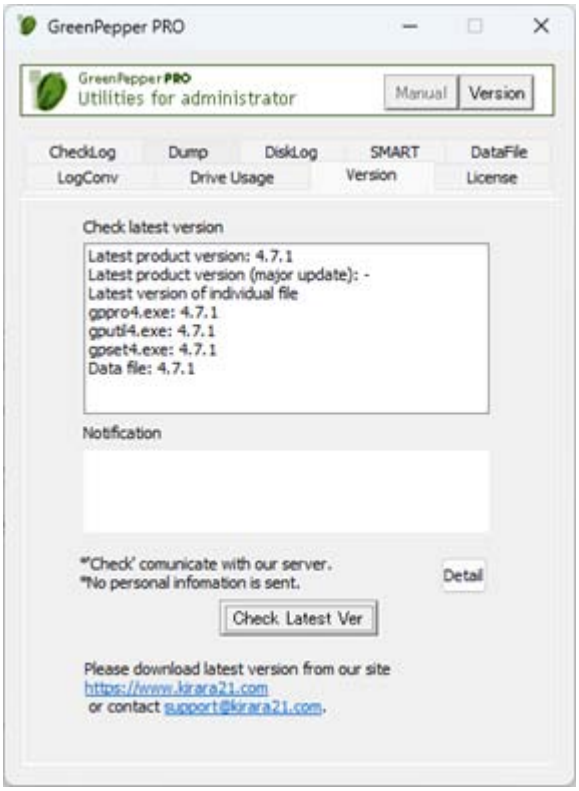
Warning!
This function scans all processes running on your PC, so some antivirus/EDR software may warn you about it as harfull software. "gputil4.exe" is created and signed by our company. The signature checks for program tampering, so when the signature is valid, the program will not harm your PC.



Copy
Copies the information displayed on the screen to the clipboard. You can then "paste" it into Notepad or other programs.

Version>

"Version" confirms the latest version of the current "Green Pepper PRO" system.



Operation on the screen

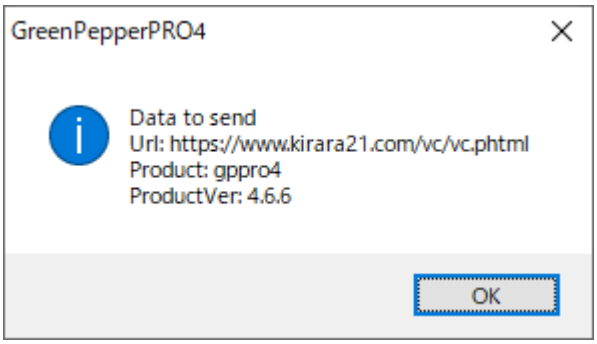
Check Latest Ver

When you press this button, it communicates with our (kirala21) server and displays the latest version information on the screen.

*** Customer-specific information (PC information, Windows information, etc.) will NOT be sent in this communication.**
*** Communicate via http. Please use it in an environment where you can access the Internet via http.**

Detail

Click the [Detail] button to see the details of what is sent to the server.
No further information will be sent.



E-mail link for update

When you click the link of the e-mail address, your e-mail software will start and the recipient and subject will be set automatically.
As the text, the item name etc. of the content to be filled in will be displayed.
Please fill in the required information and send us an email.

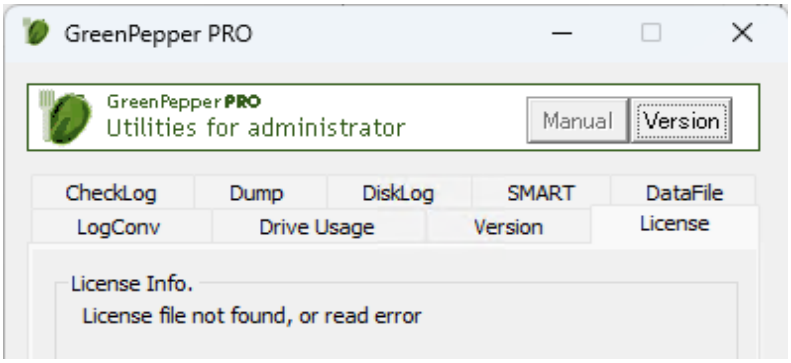
You can also send us an email as usual instead of using this link. * It will not be sent by just clicking the link. To send, you need to send an email as usual.

License

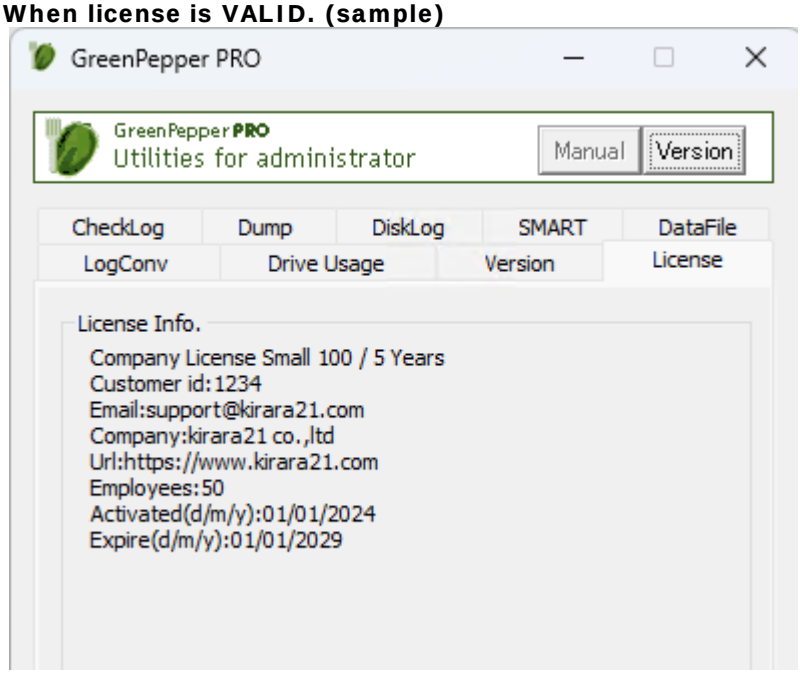
In "License", you can check the currnet license status, activate / renew / reissue license file.

License status

When NO valid license. Initial state / No license / or license file read error.



When license is VALID. (sample)



License Activation / Renew / Reissue

Please see 'About license, license activation' for details.

Abstract of "USB stick Boot configuration tool"

The "USB stick Boot configuration tool"(gpusbst4.exe) is a tool for configuring USB flash drive for starting and executing the "Boot up Erase Program".

As you know, "gpset4.exe" has same function, but this program can be executed **with user privileges** (administrator privileg is not required) and is useful for distributing USB flash drive boot environments within your company.

Options for "Boot up erase program" are loaded from the data file "gpdata.pac" and you can not set with this program.

If the USB flash drive has partition like usual HDD ("HDD type"), legacy (BIOS) booting with the USB flash drive is NOT possible. Only UEFI startup is possible.
If legacy (BIOS) booting is required, run "gpusbst4.exe" with "administrator privileges" and configure.

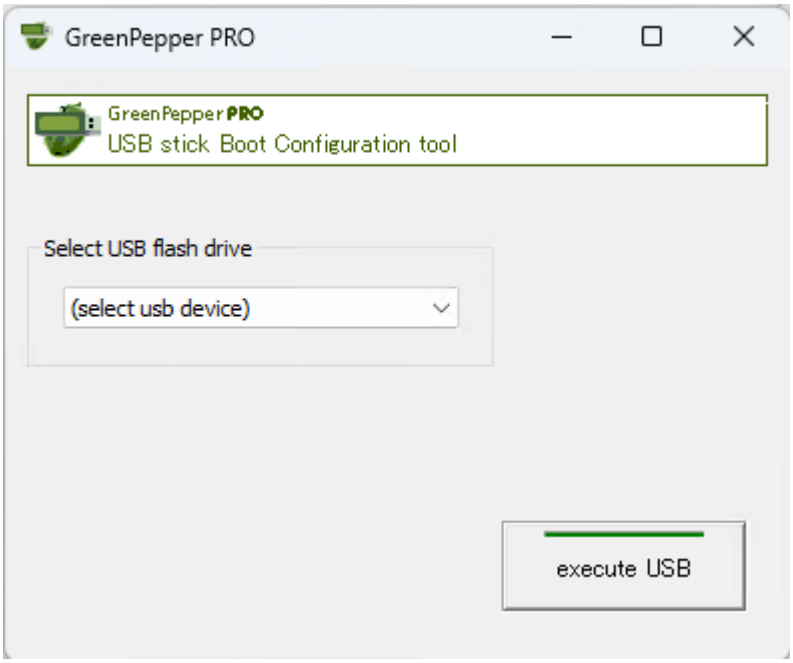
*If the USB flash drive is "large FDD type" with no partitions, legacy (BIOS) boot configuration is possible with general user privileges.
*The difference between "HDD type" and "large FDD type" is the difference in whether or not partitions are created, and is not specific to USB flash drive hardware.
*Depending on your PC, you may not be able to start the PC if it is either an "HDD type" or a "large FDD type."

Executing "USB stick Boot configuration tool"

The "USB stick Boot configuration tool"(gpusbst4.exe) that runs on Windows can be easily started and executed without any installation work.

You can boot directly from a CD-ROM, network folder, etc., double click "gpusbst4.exe" to start it.

***License file "license.gp4" is requierd in the same folder as "gpusbst4.exe".**



Confirmation of "Data file" existence

The "Data file" (gpdata.pac) is required in the same folder as gpusbst4.exe or in the [data] folder at the same level as gpusbst4.exe.

For details about "Data file", see "Executing "Startup environment creation tool" .

Storing option values for "Boot up Erase program" to the Data file

If you want to specify options for the "Boot up erase program", you must save them in the data file (gpdata.pac) in advance.
This program configures the USB flash drive using the saved option values.

By specifying and storing options in advance in the System department, internal users can create USB flash drives with the same specifications without having to be aware of the options.

For details on how to specify and save option values, see "Customizing/Setting data file".
Whether "Initial, changeable'' or "Fixed", have no effect on this program.

*However, when running with administrator privileges, the settings of "Initial, changeable'' or "Fixed" will be valid for the USB flash drive type.

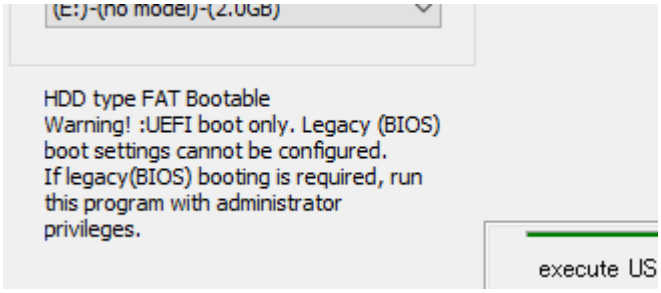
Operation of configuring USB flash drive

Select the USB flash drive to be set from the list.
* A list of USB removable drives is displayed. When you make a selection, information such as the current setting type is displayed.
Then click [Execute USB].

Warning !
* Please note that the USB flash drive is initialized by the setting process and **the inside is erased**.
* Please use a **USB flash drive of 64GB or less**.
Anything larger than 64GB will be treated as an erase target drive and you will not be able to write logs.
Also, when automatic erase is set, it will be erased automatically.
* USB flash drives that are encrypted and those require a password at the time of use cannot be used for booting.

Other settings procedures are almost the same as "Setting bootable "USB flash drive".
Please have a look at this.

After selecting a USB flash drive, the following message may appear.



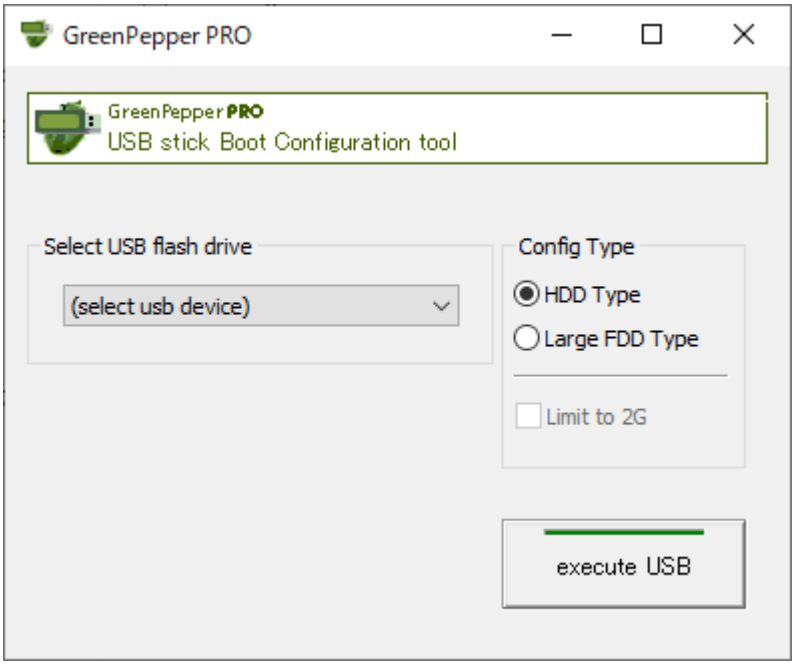
In this case, legacy (BIOS) booting using the configured USB flash drive is not possible. UEFI boot only.

If legacy (BIOS) booting is required, settings must be made using one of the following methods.
·Run "gpusbst4.exe" as administrator and configure. (Both "HDD type" and "large FDD type" are possible)
·Run "gpusbst4.exe" as administrator and configure for "Large FDD type". After that, settings can be made with general user privileges with this USB flash drive.

*Depending on your PC, you may not be able to start the PC if it is either an "HDD type" or a "large FDD type." In that case, you will need to "Run as administrator" and change it to a bootable type.
*These operations can also be performed using "gpset4.exe".

"Run as administrator"

If you run "gpusbst4.exe" as administrator, the flowing screen is displayed.



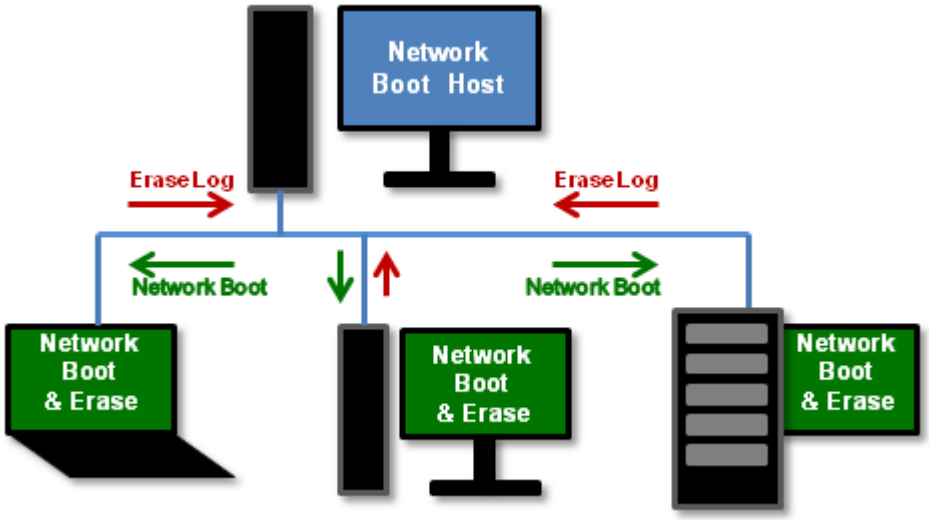
The "Config Type" selection will be displayed, and you can specify it as you like.
For details on "Config Type", see "Setting bootable "USB flash drive".

Abstract of Network Boot Host

Warning !
* "Site License"/"Company License" is requierd to use.
* With "Single user license", the program is executed in evaluation mode.

This is a host (server) function that starts and executes the erase program via network boot (PXE).
By simply inserting the CD or USB flash drive created in "Creating Network boot host image/ USB flash drive" into your PC and booting it, you can build a host (server) that includes all of the following functions.

·Host function for network boot
·Loading the erase program on network booted PC's
·FTP server for the erasure program to write logs
·NTP server for time synchronization with network booted PC's



Preparing the host PC

One PC is required to use a network boot host. It does not require many resources, so a PC 2-3 generations old is sufficient.
It can also be executed in virtual environments such as Microsoft's Hyper-V.

Basically, you can use it without making any settings, just by booting with the CD/USB flash drive created in "Creating Network boot host image/ USB flash drive".
However, if you want to leave erase logs using the FTP server function, please check and configure the storage settings (menu screen "Storage Configuration").

About disk drives

The OS, programs, and necessary data are loaded from the CD/USB flash drive, so it can be executed even if there is no disk drive (diskless).
If you only use the network boot function, there is no problem with a diskless system.
Disk (or other) storage is required only if you enable the FTP server function and store the erasure log.

The following can be used as storage.
·HDD/SSD (internal/USB connection)
When you assign a disk as storage, the disk must be initialized, so its contents are erased.
*It will not be deleted automatically. It will be cleared only if you perform an assignment operation.
·Boot USB flash drive
The USB flash drive used for boot can be used as storage. In that case, diskless operation is possible.
·Memory (RAM) area
It is also possible to assign memory (RAM) as storage, but the contents will be erased when the power is turned off.

Preparing the network environment

When performing an erase operation using network boot, the network boot host PC and the PC to be erased must be connected via a network (Ethernet).
Since the network boot host has a DHCP server function, it may conflict with the DHCP server in the existing network. Also to avoid the risk that the PC you use on a daily basis will be erased by network boot, **we recommend that you separate it from your existing network**.

Preparing the PC to be erased

Make the PC to be erased network bootable and connect it to the network boot host.
When the power is turned on, the boot program and erase program are loaded from the network boot host, allowing erasure to be performed.

·Network boot (PXE/IPv4) must be enabled in the PC's BIOS/UEFI settings.
*Supports both Legacy (BIOS) boot and UEFI boot.
·Set the boot priority for network boot higher than the internal drive, or select network boot in the temporary boot settings.
·Many models can boot even with Secure Boot enabled. However, if this is not possible, please disable secure boot.
·If you enable the erase program's network log and specify the log write target as the network boot host (FTP), the erase log will be written to the network boot host.
* The network interface of the PC must be compatible.
* Network logging must be enabled when erasing.
·If you enable the NTP server of the network boot host and enable the NTP client function of the erase program, the time will be synchronized when the erase program is started.
* The NTP server specification in the erase program must be the address of the network boot host.

Boot from CD / USB flash drive

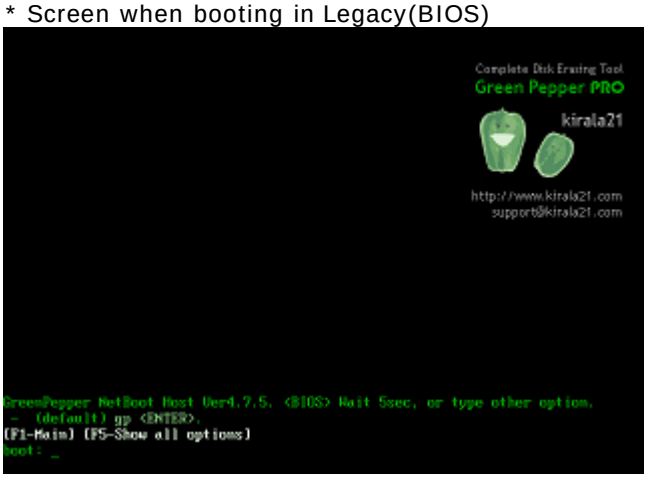
Boot

Insert the "Green Pepper Pro" product CD-ROM or the created bootable CD / USB flash drive into your computer, and turn on the power.
The system will start and the screen will look like the one below.

* To create bootable CD, see "Creating bootable "CD image" file"
* To create bootable USB flash drive, see "Setting bootable "USB flash drive""

The boot screen differs depending on the Legacy(BIOS) / UEFI boot. The processing after startup is exactly the same.

* Screen when booting in Legacy(BIOS)



* Screen when booting for UEFI (In the case of secure boot, the background image may not be displayed)

If the PC does not boot or the OS installed on the hard disk boots

· Check the Legacy(BIOS) / UEFI settings. The boot priority of the CD / USB flash drive may be low.
see "Setting the boot environment on BIOS/UEFI"
· The created CD-R may not have been created correctly for booting.
see "How to create a CD from an image file"
· The type of USB flash drive you have set may not match your PC.
see "Setting the boot environment on BIOS/UEFI""Setting bootable "USB flash drive""
· Your PC may not support booting from the CD / USB flash drive.
see "Setting the boot environment on BIOS/UEFI"
· A message will be displayed at startup, and some models will not start from a CD unless the specified key is pressed at that timing.
example: "Press any key to boot from CD..." message appear at boot time.

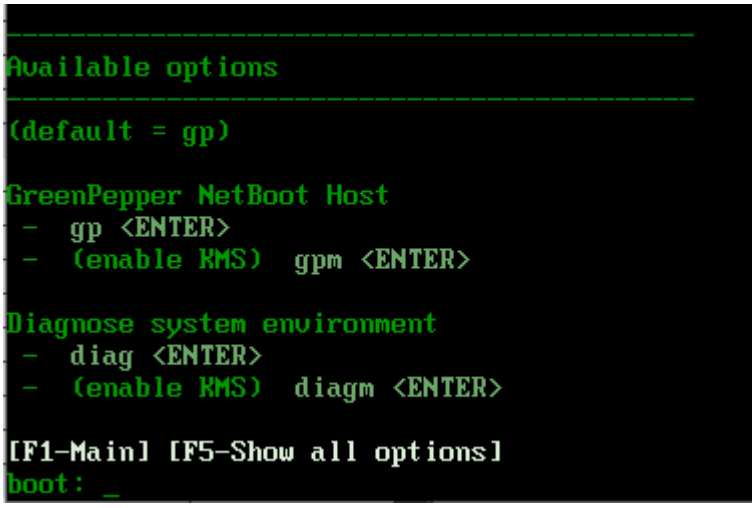
Operation on the boot screen - Legacy(BIOS) boot

Normally, even if you do nothing, it will automatically start the startup process after 5 seconds.
Press the [enter] key to start immediately.

* The screen may not switch immediately after [enter], such as when media access is slow, but please wait for a while.
* If you enter one character within 5 seconds, the automatic startup will stop.

Select other option

The available options are displayed by pressing the "F5" key within 5 seconds.
* Once the screen is switched, the automatic startup will be stopped.



input	contents
gp	Display normal erase screen
gpm	Enable Kernel Mode Setting (KMS). If there is a problem with the display, please try it.
diag	Diagnose: Problem investigation screen to check the status when startup is not completed or disk is not recognized.
diagm	Diagnose: Enable Kernel Mode Setting (KMS). If there is a problem with the display, please try it.

If the startup is not completed

If the startup is not completed and the menu screen is not displayed, the following causes are possible.

· The hardware is not compatible with this product.
  * Not compatible CPU, motherboard, and peripheral devices.
  * Please remove peripheral devices and try again.
  * If there is a device that can be separated by the BIOS, try disconnecting it.
· Media failure (CD-ROM, USB flash drive)
· Other hardware failures

Start with "diag" and let us know the contents of the screen at the time of stop.

If the startup stops halfway and the menu is not displayed, there is no function to get the screen.
Please take a picture of the screen with a digital camera and send it to us.

For the operation of the screen displayed by the "diag" option, see "Using diagnose screen".

Operation on the boot screen - UEFI boot

"Green Pepper PRO" supports Secure Boot of many PCs, but if the Secure Boot specification of your PC is not

supported , the following boot screen will not be displayed and a message such as a Security error will be displayed.
In that case, try disabling Secure Boot in the BIOS (UEFI) settings.

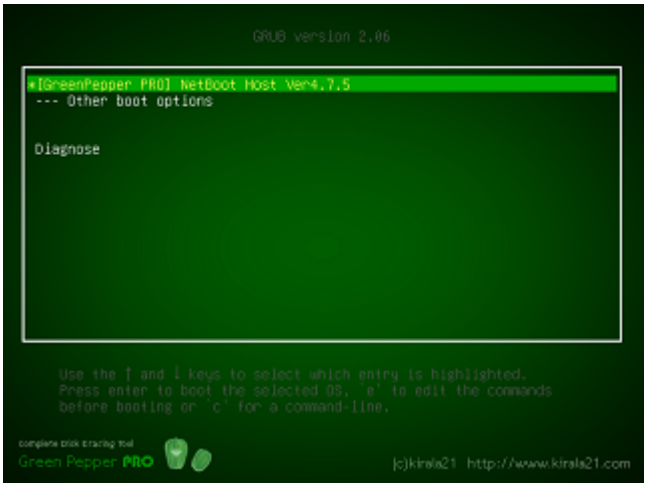
Normally, even if you do nothing, it will automatically start the startup process after 5 seconds.

[ESC]key for menu .....
4

If you want to start with other options, press the [ESC] key before the 5-second countdown ends.
The following option menu screen is displayed.

If the "[ESC]key for menu" screen is not displayed and "loading system..." is displayed

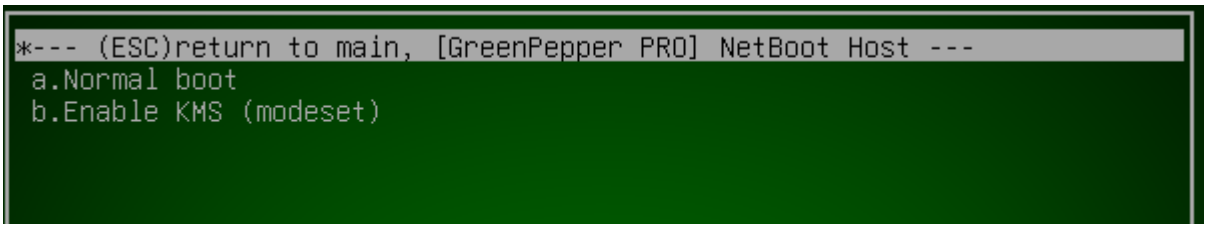
·If you do not need to select any other options at startup, the program will run until the menu is displayed, so please use it as is.
· If you need to select an option at startup, press and hold the [Esc] key immediately after the PC starts booting.
A boot option selection menu will be displayed.



Operation on the option menu screen

Use the "Down" and "Up" keys to select a function, and the [enter] key to execute the option menu.
Under "---- Other boot options", a submenu will be displayed that allows you to select more detailed options.

1. Under the "[GreenPepper PRO] NetBoot Host ver4.xx" menu, when "--- Other boot options" is selected.



From this screen, press the [ESC] key to return to the first option menu screen.

Menu Structure

In the standard state, the menu structure is as follows.

Option menu structure

selection menu	contents
[GreenPepper PRO] NetBoot Host Ver 4.x.x	Normal Boot
--- Other boot options	Boot option submenu
Diagnose	Diagnose: Problem investigation screen to check the status when startup is not completed or disk is not recognized.

Boot option submenu

selection menu	contents
*--- (ESC)return to main, [GreenPepper PRO]	* press the [ESC] key to return to the first option

NetBoot Host	menu screen.
a.Normal boot	Normal Boot
b:Enable KMS (nodeset)	Enable Kernel Mode Setting (KMS). If there is a problem with the display, please try it.

Boot option submenu (diagnose)

selection menu	contents
*--- (ESC)return to main, diagnose ---	* press the [ESC] key to return to the first option menu screen.
a.Normal boot	Diagnose: Problem investigation screen to check the status when startup is not completed or disk is not recognized.
g:Enable KMS (nodeset)	Diagnose: Enable Kernel Mode Setting (KMS). If there is a problem with the display, please try it.

If the startup is not completed

If the startup is not completed and the erase screen is not displayed, the following causes are possible.

· The hardware is not compatible with this product.
  * Not compatible CPU, motherboard, and peripheral devices.
  * Please remove peripheral devices and try again.
  * If there is a device that can be separated by the BIOS, try disconnecting it.
· Media failure (CD-ROM, USB flash drive)
· Other hardware failures

· Unsupported Secure Boot specification
  * Try disabling Secure Boot in the BIOS (UEFI) settings.
  * If you see the "disable SecureBoot if stops here" message on the screen and it stops, try disabling Secure Boot.

Also, start with "diagnose" menu and let us know the contents of the screen at the time of stop.

If the startup stops halfway and the menu is not displayed, there is no function to get the screen.
Please take a picture of the screen with a digital camera and send it to us.

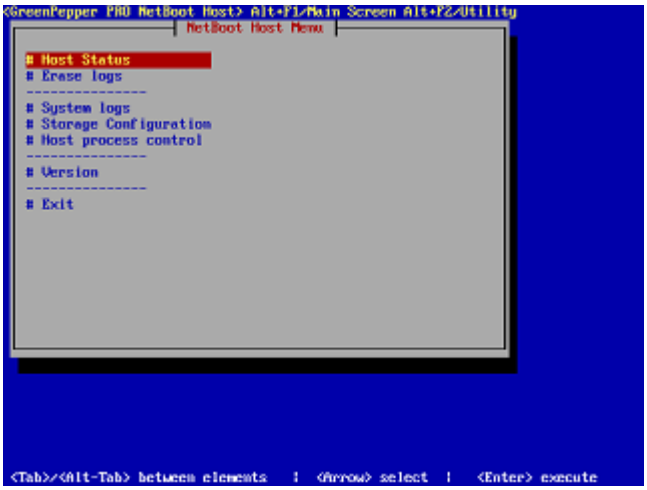
For the operation of the screen displayed by the "diag" option, see "Using diagnose screen".

Basic operation of Network Boot Host

Menu screen

If you start the Network Boot Host from the bootable CD, USB flash drive, the following menu will be displayed.

Normal menu screen



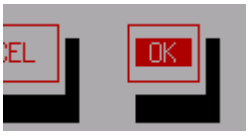
Key operation

Move choices: Arrow keys
Move between input items: [tab] / [alt] + [tab] keys
Select / execute choice: [enter] key
Check / uncheck check items: [space] key

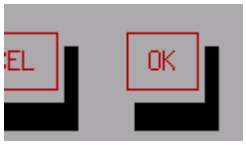
Cursor position

Check the current position of the cursor as follows.

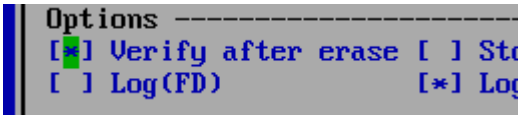
cursor is on "OK" button



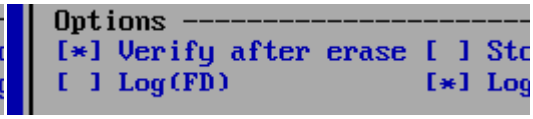
no cursor on "OK" button



cursor is on "Verify after erase"

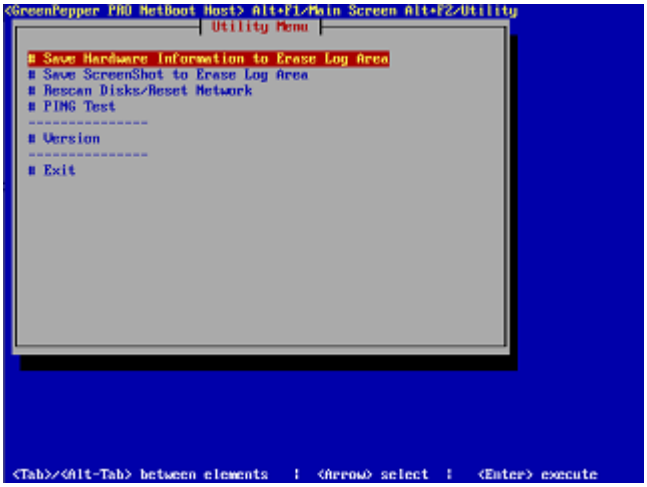


no cursor on "Verify after erase"



Switch to another screen

In addition to the menu that is displayed by default, the "Utilities" menu will be displayed by pressing Alt+F2 (Hold down Alt and press the F2 key). To return to the normal menu screen, press Alt+F1.



Outline of menu contents

Host Status
Show the current setting status of each function.

Erase Logs
When the FTP server function is enabled and erase logs of the erase program are saved, a list and contents of erase logs will be displayed.

System Logs
Check logs related to the system, such as DHCP lease status, TFTP (network boot) download status, host/network settings/error status, etc.

Storage Configuration
Configure storage for erasure logs. **When starting up for the first time, please check and configure the settings**.

Host Porcess Control
This function temporarily stops and restarts the network boot process (DHCP/TFTP), FTP, and NTP process.
FTP can be changed to run in debug mode to investigate any problems.

version information
Display version information.

exit
Shut down the system and turn off the power..

---Utility Menu ---
Save Hardware Information to Erase Log Area
Writes detailed hardware information to the erase log area for problem investigation.

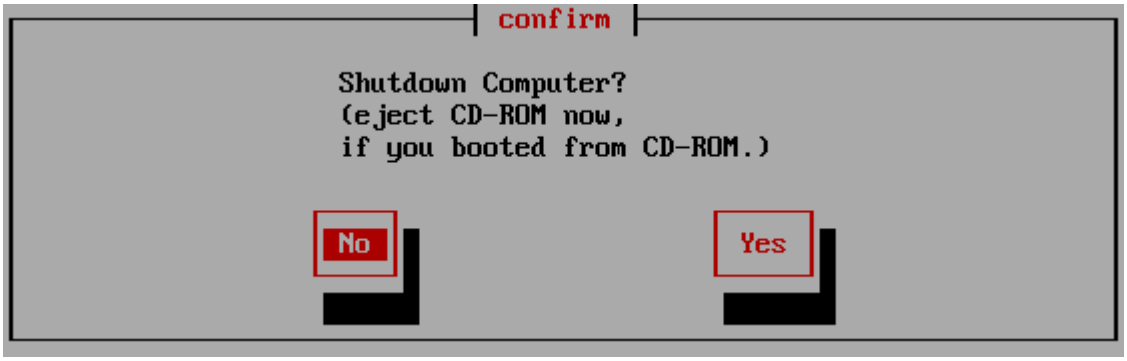
Save Screenshot to Erase Log Area
Take a screenshot and write the file to the erase log area.

Rescan Disks/Reset Network
Execute this command to reconfigure the settings when the disk/net environment changes, such as by connecting or disconnecting a USB disk drive or reconnecting a network cable.

PING Test
Perform a PING test to confirm network connectivity.

System shutdown

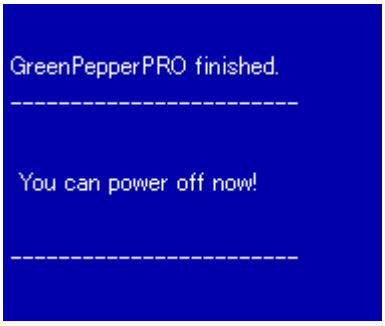
Select "Exit" from the menu and press [enter]..
On the screen below, select [Yes] and press [enter]..



any PCs will turn off automatically after this.Many PCs will turn off automatically after this.
Therefore, if you are booting from the CD-ROM, it is convenient to remove the CD at this timing.

If the power does not turn off automatically

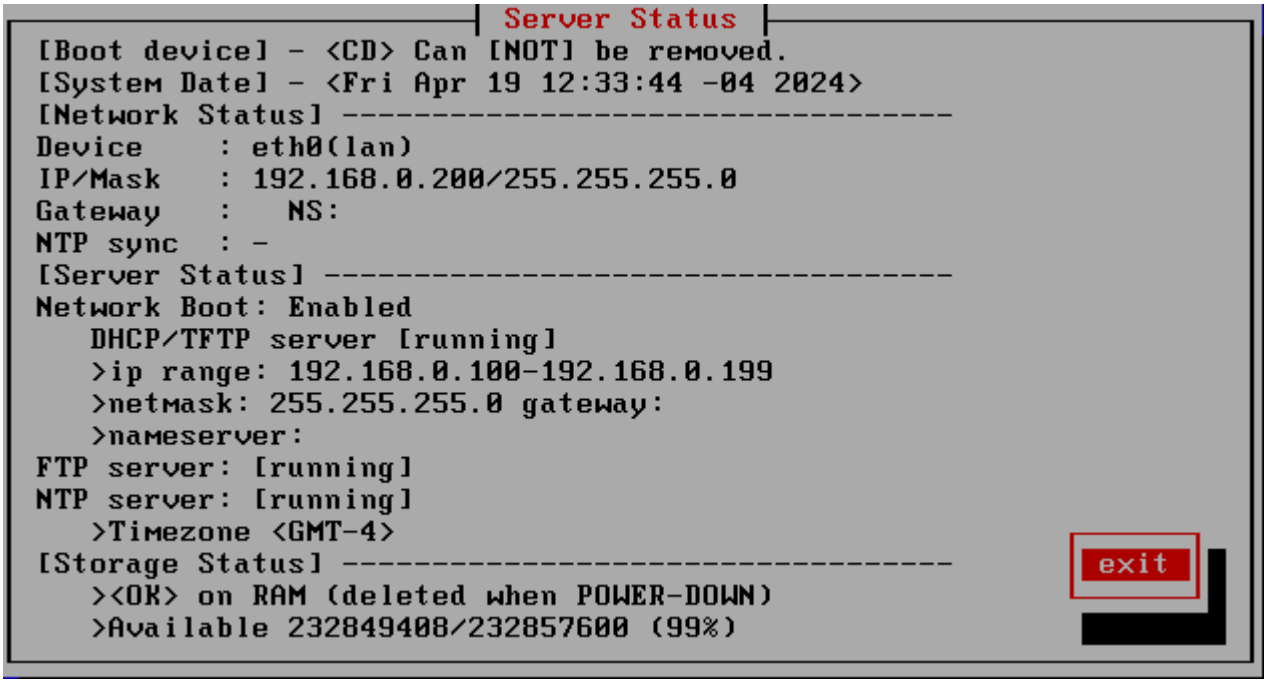
If the power does not turn off automatically, etc.,
after the following screen is displayed, press the power button (may be a long press) to turn off the power.



Operation of Each function

Host Status

Show the current setting status of each function.



[Boot Device]
Displays the boot device and information on whether it can be removed .

<CD>: Booting from CD
<usb flash>: Booting from USB flash drive

Can be Removed: The boot CD/USB memory can be removed. The system will continue to operate even if it is removed.
Can [NOT] be removed: The boot CD/USB memory cannot be removed. It is used for network boot programs, log writing, etc.

[System Date]
Current system date and time. "-04"(example) before the year is the time zone.

[Network Status]
Displays the current network address settings, etc.
Also, if the NTP client is enabled, the setting status as an NTP client will be displayed.

If "Status:NG (N:Error code)", an error has occurred in the network settings.

Error code	Contents	Troubleshooting
Error that may occurs		
(N3) No network device found	The network device is not enabled because there is no corresponding network driver.	The network interface card installed in your PC may not be supported by your "Green Pepper PRO" version. Or, no valid network interface was found.
(N20)	The IP address could not be set.	When specifying an IP address by DHCP, it often occurs when the IP address cannot be obtained because the DHCP server cannot be found or the DHCP server does not respond. Please check the network route to the DHCP server and check the operation of the DHCP server.

Address is not set(DHCP) Address is not set(static)	In the case of DHCP, the address cannot be obtained because the network cable is not connected or the DHCP server cannot be found.	If you change the network route (cable, hub, etc.) or DHCP server side and try to connect again, restart "Green Pepper PRO" system or perform "Utilities"/"Rescan disks /Reset network". In the case of IP address setting with a fixed value, the specified address is incorrect, etc. Check the IP address / subnet mask settings.
The following rarely occurs		
(N1) Confing file not found	The network configuration file cannot be found.	
(N2) Confing file read error	An error occurred while reading the network configuration file.	
(N10) No ip/netmask in config	The fixed IP address (ipv4) and subnet mask values are not set.	
(N11) Bad ip(ipv4) address	Specified fixed IP address (ipv4) is incorrect.	
(N12) Bad subnet mask(ipv4)	Specified subnet mask (ipv4) is incorrect.	
(N13) Bad gateway address(ipv4)	Specified gateway address (ipv4) is incorrect.	

[Server Status]
Displays the execution status of server processes.

Network Boot:
Enabled / Disabled

DHCP/TFTP server [runiing]:
The server process required for network boot is running.
The IP address distributed by the DHCP server will be displayed.

Error: An error has occurred. An error message will be displayed.

FTP server:
Disabled/ Running

Error: An error has occurred. An error message will be displayed.

NTP server:
Disabled/ Running
Timezone is displayed

Error: An error has occurred. An error message will be displayed.

[Storage Status]
Displays the storage status.

<OK> on XXXXX:
Settings are being made. The currently assigned device is displayed in XXXX.

USB flash drive (boot): Assigned to the USB flash drive used for booting
RAM (deleted when POWER-DOWN): Assigned to memory (RAM) as storage.
Saved log files, etc. will be deleted when the power is turned off.
[HDD/SSD model number]: Assign HDD/SSD as storage.

Available xxxxx/xxxxxxx (xx%):
Indicates the available capacity/total capacity (usage rate) of storage.
However, in the case of a RAM drive, it cannot be used to its full capacity because it is shared with other systems and execution programs.

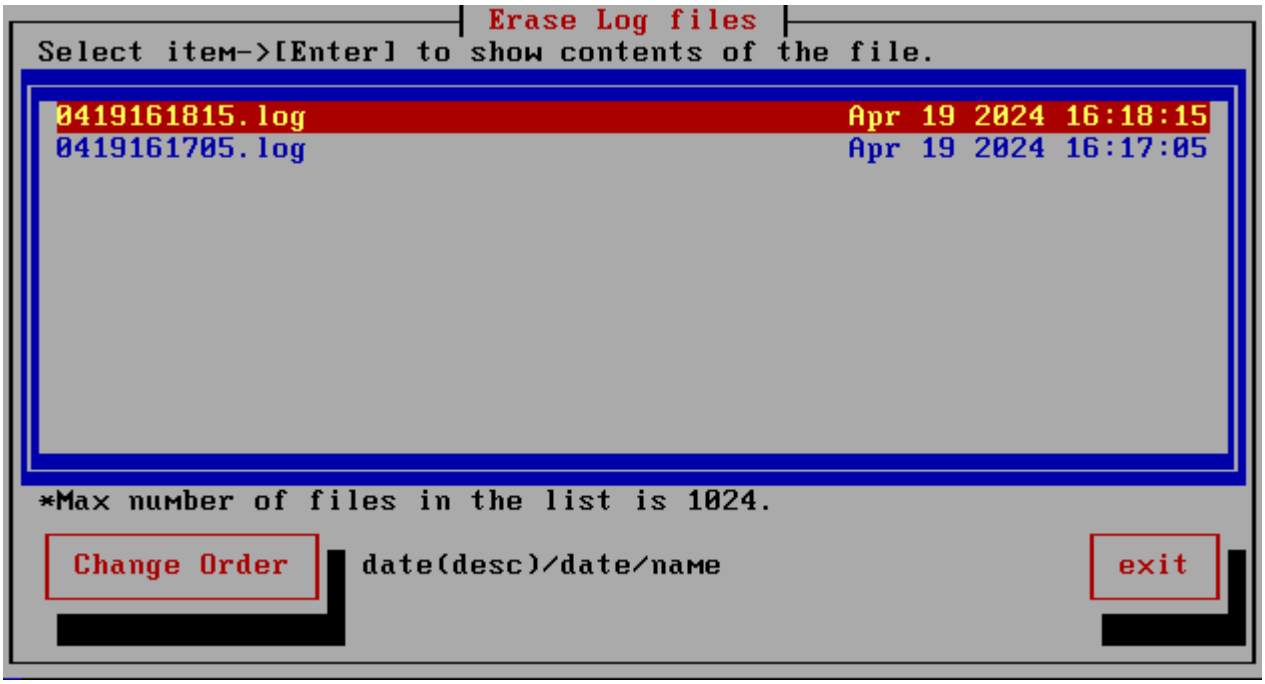
Erase Logs

When the FTP server function is enabled and erase logs of the erase program are saved, a list and contents of

erase logs will be displayed.

If you are using a USB flash drive as storage, you can remove the USB flash drive, connect it to a Windows PC, etc., and copy or delete the contents.
If you are using an internal disk, you will need to connect another PC via FTP to copy or delete.

*The maximum number of files displayed is 1024.



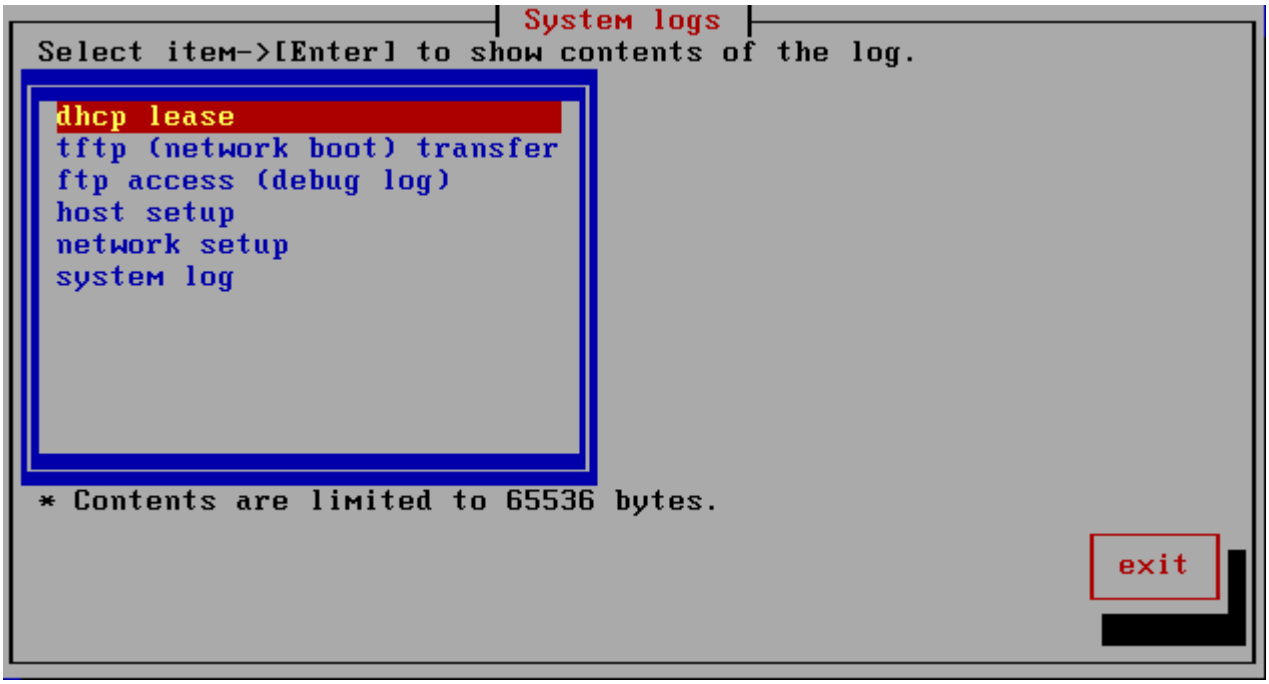
File selection / display
Select a file using the up and down arrow keys and press [enter] to display the file contents.

Change order
When you press [Change order], sorted by,
Date (descending)->Date (ascending)->File name

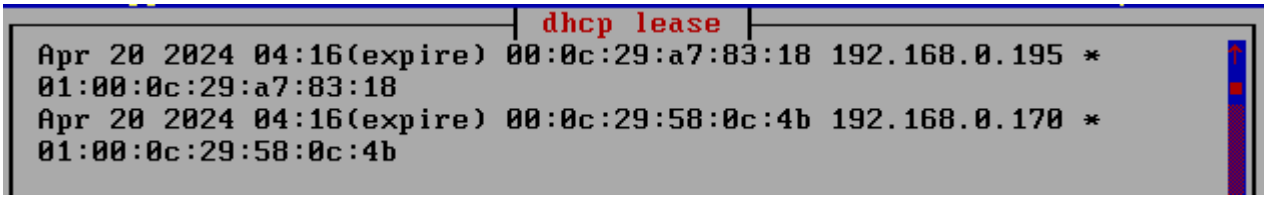
System Logs

Check logs related to the system, such as DHCP lease status, TFTP (network boot) download status, host/network settings/error status, etc.
Select the log to display and press [enter] to display the contents.

*The displayed file content is up to 65536 bytes.



DHCP lease
Displays the address distribution status on the DHCP server.



The date and time (time of expiry: 12 hours after distribution), distribution destination MAC address, distribution IP address, etc. are displayed.

tftp (network boot) transfer
Displays the file transfer status using tftp used for network boot.

ftp access (debug log)
Display detailed ftp access logs.
However, nothing is displayed in the initial state.
In "Host process control", temporarily [stop] the FTP process and then select [Debug Run] to obtain access logs.

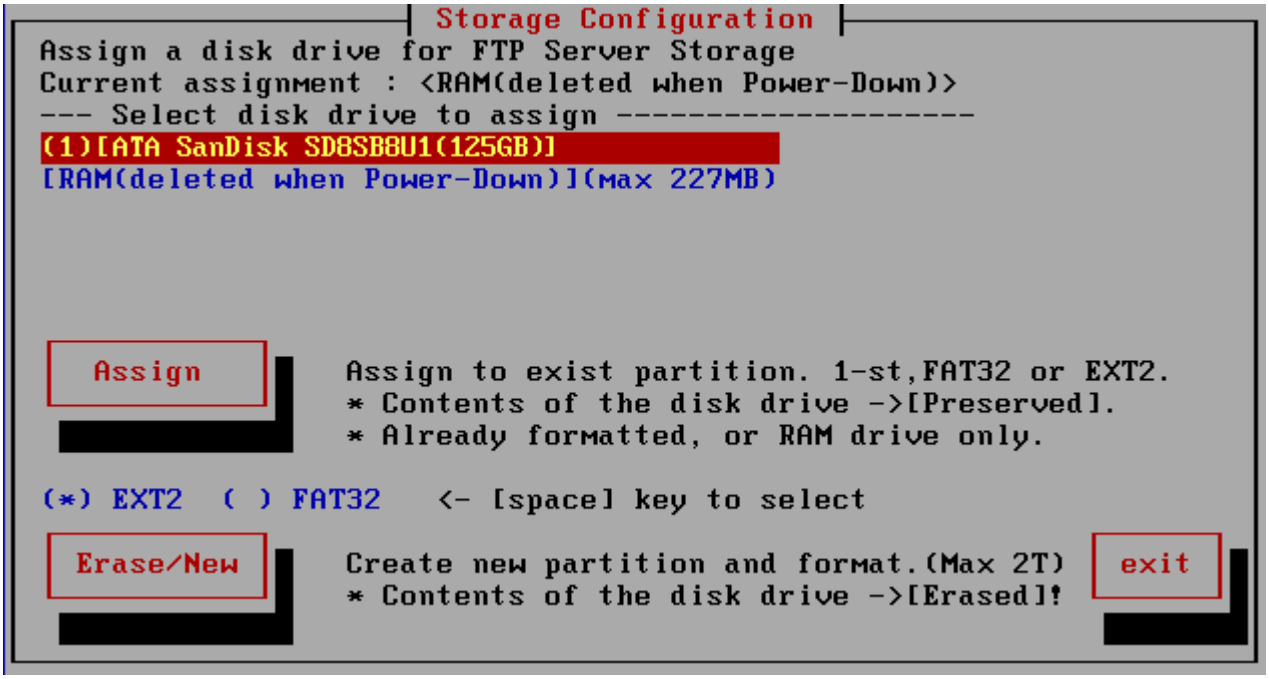
Host setup
This is the setting status of the network boot host. If you have any problems, please let us know.

Network setup
This is the setting status of the network. If you have any problems, please let us know.

System Log
Detailed log for the entire system.

Storage Configuration

Configure storage to be used to store erase logs on the FTP server.
If you do not use an FTP server, leave it in its initial state and do not need to make any settings.



The following devices can be used as storage.

·USB flash drive used for startup.
The notation is "USB flash drive (boot)".
·Uses memory (RAM) as storage. Saved log files, etc. will be deleted when the power is turned off.
The notation is "RAM (deleted when POWER-DOWN)".
·HDD/SSD such as SATA, NVMe, USB connection.
The notation is the model number of the disk drive.
When used, it will be formatted as EXT2/FAT32 and its contents will be erased.

Also, the maximum capacity is limited to 2T (2 terabytes).
(Disk drives of 2T or more can also be used, but the capacity used will be 2T)

Current Assignment
Displaying currently assigned devices.

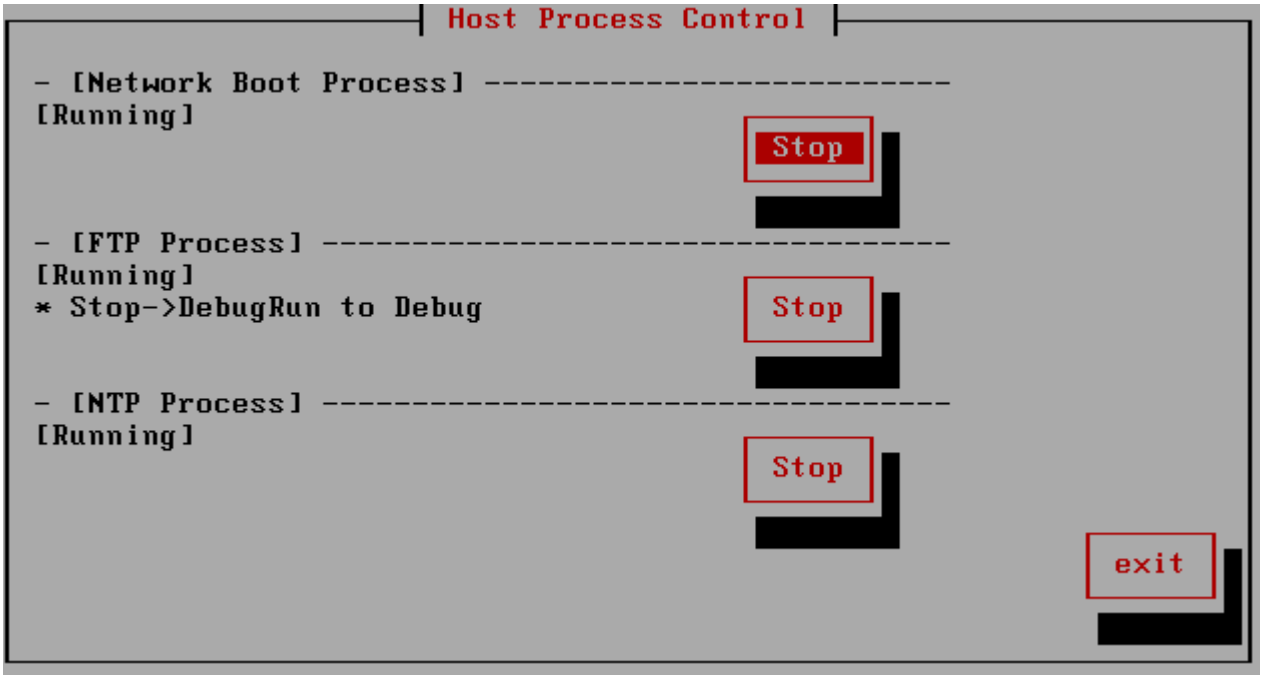
[Assign]
When assigning to "USB flash drive (boot)", "RAM (deleted when POWER-DOWN)", or if the first partition of the disk is already formatted as FAT32/EXT2, do "Assign " process.
The current disk contents are preserved (not erased), except for assigning to RAM.

[Erase/New]
Perform this process when newly assigning to HDD/SSD.
Please note that **the contents of the disk drive will be erased**.

Select EXT2 or FAT32 as the formatting method. EXT2 is a format commonly used on Linux, but cannot be read from Windows. FAT32 can be read from Windows, so if you want to retrieve log files by connecting to Windows PC, please select FAT32.
The partitions will be created and the first partition will be used.

Host Process Control

Controls the suspension and restart of host processes running on the network boot host.
It can be used to temporarily stop [Network Boot Process] (DHCP) when connecting to an existing network.
FTP also allows you to leave detailed access logs by selecting [Stop]->[DebugRun].



Operation of Each function - Utility

Save Hardware Information to Erase Log Area
Writes detailed hardware information to the erase log area for problem investigation.

The written hardware information can be accessed from the "Erase Logs" menu as shown above.

hwinfo_xxxx.txt
will be the name.

Save Screenshot to Erase Log Area

Take a screenshot and write the file to the erase log area.

It is used when there is a problem with processing, when you want to save screen information in-house as a processing record, or when you want to prepare manuals, etc.

If written, the file name will be "ddhhMMss.stx" (day, hours, minutes, seconds).
This file is a Linux hardcopy file. Please use the "stx2bmp.exe" program included with the product to convert it to an image file (*.bmp).

Rescan Disks/Reset Network

Execute this command to reconfigure the settings when the disk/net environment changes, such as by connecting or disconnecting a USB disk drive or reconnecting a network cable.

The installation status of drivers and network status are displayed on the screen, so you can use it to check the status.
When the process is finished, "press[enter]" will be displayed at the end, so press the [enter] key.

PING Test

Perform a PING test to confirm network connectivity.

Enter the IP address or host name for which you want to test the connection, and select [PING].
If "ping test OK" is displayed, a basic connection with the PC has been established.

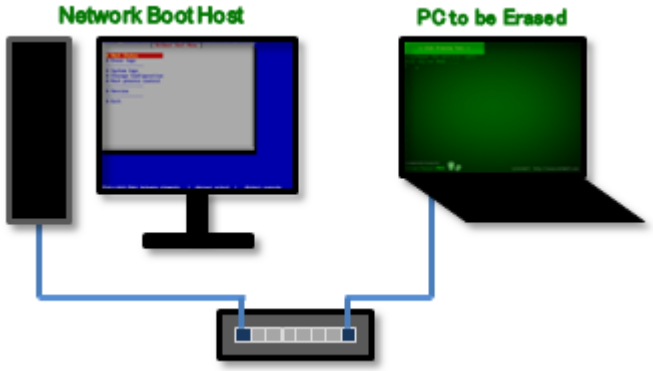
* When connecting by host name, the name server must be set correctly and the name server must be able to resolve the name.
* Note: Some PC firewalls may block PING responses. In that case, you may be able to connect even if the connection fails here.

Preparing PC

Preparing network and the PC to be erased

Connect Network boot Host and the PC to be erased by network (ethernet).
*Basically, a wired LAN connection is required. However, for models that support WiFi at the BIOS/UEFI level, network booting via WiFi is possible.

Since the network boot host has a DHCP server function, it may conflict with the DHCP server in the existing network. Also to avoid the risk that the PC you use on a daily basis will be erased by network boot, **we recommend that you separate it from your existing network**.



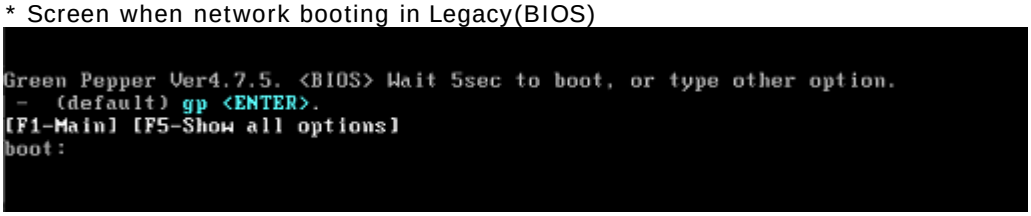
Booting PC

Boot

In the BIOS/UEFI settings of the PC to be erased, enable network boot (PXE IPv4) and raise the boot order of network boot, or display the boot menu (display with F9, F12, etc.) and select network boot. A network boot will be performed.
The system will start and a screen like the one below will appear.

The boot screen differs depending on the Legacy(BIOS) / UEFI boot. The processing after startup is exactly the same.

* Screen when network booting in Legacy(BIOS)



* Screen when network booting for UEFI (In the case of secure boot, the background image may not be displayed)

The operations after booting are exactly the same as booting from a CD/USB flash drive.

Please refer to "Operation of Boot Erase Program" - "Boot from CD/USB flash drive".

Programs using in "Boot up Erase program", Windows applications (GPL,GPL2)

	kernel	Linux kernel 6.3.12 (64bit) Linux kernel 4.20.13 (32bit)
	buildroot (uclibc,busybox)	basic build package
	bogl-bterm	UTF terminal
	newt	user interface
	grub	boot loader
	syslinuix, isolinux, pxelinux	boot loader
	mkisofs	creating ISO image file

Time required to erase the disk

* Measured by us

Bootup Erase Program

Specifications of the PC used for measurement

CPU: Intel Core i3-6100 CPU @ 3.70GHz
Memory: 4GB
Disk interface:
Intel H110 chipset/SATA 6.0 Gb/s

Intel SSD D3-S4510 series SSDSC2KB24 240GB SATA 6.0Gbs		
Sanitize (block+crypt)	20sec	0.08sec/Gbyte
Sanitize (over write)	24min	6.1sec/Gbyte
Secure Erase (Specification value 2min)	10sec	0.04sec/Gbyte
Normal Erase (zero write)	18min	4.5sec/Gbyte
Read verify	20min	4.8sec/Gbyte
SAMSUNG MZVLB1T0HBLR-000L7 1TB NVMe		
Sanitize (block+crypt)	15sec	0.015sec/Gbyte
Normal Erase (zero write)	17min	1sec/Gbyte
Read verify	6min	0.37sec/Gbyte
SAMSUNG 970 EVO PLUS 250GB NVMe		
Secure Erase	12sec	0.048sec/Gbyte
Normal Erase (zero write)	9min	2.2sec/Gbyte
Read verify	94sec	0.37sec/Gbyte

Specifications of the PC used for measurement

CPU: Intel(R) Celeron(R) CPU N2807 @ 1.58GHz
Memory: 2GB
Disk Interface:
eMMC

Toshiba 064GE2 64GB eMMC		
Sanitize (block+sanitize)	34sec	0.54sec/Gbyte
Secure Erase	112min	108sec/Gbyte
Normal Erase (zero write)	111min	106sec/Gbyte
Read verify	9min	8.6sec/Gbyte

Specifications of the PC used for measurement

CPU: Intel Pentium D 2.807GHz
Memory: 2GB
Disk interface:
Intel 3000/ICH7 chipset/SATA 3.0 Gb/s

Seagate ST3160813AS 160GB 7200 rpm cache 8MB SATA 3.0Gbs		
Secure Erase (Specification value 30min)	28min	10.5sec/Gbyte
Normal Erase (zero write)	34min	12.8sec/Gbyte
Read verify	28min	10.5sec/Gbyte
WesternDigital WD1600YS 160GB 7200rpm cache 16MB SATA 3.0Gbs		
Secure Erase (Specification value 54min)	51min	19.1sec/Gbyte
Normal Erase (zero write)	51min	19.1sec/Gbyte
Read verify	51min	19.1sec/Gbyte
WesternDigital WD25EZRX 2.5TB 5400rpm cache 64MB SATA 6.0Gbs		
Secure Erase (Specification value 490min)	480min	11.5sec/Gbyte
Normal Erase (zero write)	532min	12.8sec/Gbyte
Read verify	480min	11.5sec/Gbyte

Specifications of the PC used for measurement

CPU: Intel Pentium D 2.807GHz
Memory: 2GB
Disk interface:
Dell SAS 6/i (LSI SAS 1078)

IBM-ESXS(Seagate) ST936701SS 36.4G 10,000rpm cache 8MB SAS 3Gbs RAID configuration: 1 logical disk = 1 physical disk		
Secure Erase	-	-
Normal Erase (zero erase) **Write Cache OFF** (write through)	234min	386sec/Gbyte
Normal Erase (zero erase) **Write Cache ON** (write back)	11min	18.1sec/Gbyte
Read verify	11min	18.1sec/Gbyte
HP DF072ABAA8 72G 15,000rpm SAS 3Gbs RAID configuration: 1 logical disk = 1 physical disk		
Secure Erase	-	-
Normal Erase (zero write)	310min	258sec/Gbyte
Read verify	11min	9.2sec/Gbyte

Specifications of the PC used for measurement

CPU: Intel Pentium D 2.807GHz
Memory: 2GB
Disk interface:
HP SmartArray E200

IBM-ESXS(Seagate) ST936701SS 36.4G 10,000rpm cache 8MB

SAS 3Gbs RAID configuration: 1 logical disk = 1 physical disk		
Secure Erase	-	-
Normal Erase (zero write)	13min	21.4sec/Gbyte
Read verify	11min	18.1sec/Gbyte

Specifications of the PC used for measurement

CPU: Intel Core i5 750 2.67GHz
Memory: 4GB
Disk interface:
Intel P55 chipset/SATA 3.0 Gb/s

Seagate ST3160813AS 160GB 7200 rpm cache 8MB SATA 3.0Gbs		
Secure Erase (Specification value 30min)	28min	10.5sec/Gbyte
Normal Erase (zero write)	37min	13.9sec/Gbyte
Read verify	28min	10.5sec/Gbyte
WesternDigital WD1600YS 160GB 7200rpm cache 16MB SATA 3.0Gbs		
Secure Erase (Specification value 54min)	51min	19.1sec/Gbyte
Normal Erase (zero write)	51min	19.1sec/Gbyte
Read verify	51min	19.1sec/Gbyte
WesternDigital WD25EZRX 2.5TB 5400rpm cache 64MB SATA 6.0Gbs		
Secure Erase (Specification value 490min)	480min	11.5sec/Gbyte
Normal Erase (zero write)	504min	12.0sec/Gbyte
Read verify	480min	11.5sec/Gbyte

Specifications of the PC used for measurement

CPU: Intel Pentium 4 3.00GHz
Memory: 512MB
Disk Interface:
Intel 955X/ICH7R/Ultra DMA 100

Seagate ST3120026A 120GB 7200 rpm cache 8MB IDE Ultra ATA100		
Secure Erase (No specification value)	50min	25.0sec/Gbyte
Normal Erase (zero write)	45min	22.5sec/Gbyte
Read verify	45min	22.5sec/Gbyte

Windows Erase program

Specifications of the PC used for measurement

CPU: Intel Core i5 750 2.67GHz
Memory: 4GB
Disk interface:

Intel P55 chipset/SATA 3.0 Gb/s

OS: Windows7(64bit)

Seagate ST3160813AS 160GB 7200 rpm cache 8MB SATA 3.0Gbs		
Normal Erase (zero write)	28min	10.5sec/Gbyte
Read verify	28min	10.5sec/Gbyte
WesternDigital WD1600YS 160GB 7200rpm cache 16MB SATA 3.0Gbs		
Normal Erase (zero write)	51min	19.1sec/Gbyte
Read verify	51min	19.1sec/Gbyte
WesternDigital WD25EZRX 2.5TB 5400rpm cache 64MB SATA 6.0Gbs		
Normal Erase (zero write)	480min	11.5sec/Gbyte
Read verify	480min	11.5sec/Gbyte

Supported ATA/SCSI/SAS/RAID/NVMe/eMMC interface (PCI/PCIe)

* Basically, the model number of the chip is used instead of the product name. To confirm, you need to find out the chip model number of the interface.
* The table shows the corresponding product notation for each driver. We have not confirmed the operation.
* Even the ones listed in the table may not work due to firmware version, driver defect, hardware environment, version difference, etc.
* Please be sure to check the operation before purchasing.
*Yellow green is added after Ver4.6.x. Gray is obsolete after Ver4.6.x.
*In a 32-bit execution, the contents has not changed after Ver4.6.x.

64bit execution			
Manufacturer	Product name	Interface	Driver used
3ware	5xxx/6xxx PATA-RAID	IDE	3w-xxxx
	7xxx/8xxx PATA/SATA-RAID	SATA	3w-xxxx
	9xxx SATA-RAID, 9550sx,9650SE SATAII RAID 9690SA SAS/SATAII RAID	SATA	3w-9xxx
	9750 SAS2/SATA-II	SAS	3w-sas
Adaptec	Themisto, Catapult, Tomcat, Callisto AAC-RAID series ASR-2020ZCR, ASR-2025ZCR, ASR-2130S, ASR-2230S, ASR-2240S Legend S220,S230, 2120S, 2200S, 3230S, 3240S	SCSI	aacraid
	ASR-4005SAS, ASR-4000, ASR-4800S, AS4805SAS, SRC 8x6G SAS, Series 7 6G SAS, Series 8 12G SAS, Series 9	SAS	aacraid
	ASR-2020SA, ASR-2025SA, ASR-2420SA, ASR-2620SA, ASR-2820SA AAR-2610SA, AAR-2410SA, AAR-2810SA, AAR-21610SA	SATA	aacraid
	ASC-29320/A/B/LP/ALP/LPE, ASC-39320/A/B/D, AIC-7901/A, AIC-7902/B	SCSI	aic79xx
	AHA-2940/U/W/UW/D/U2/U2W/U2B, AHA-2930CU/UW/U2, AHA-2904, AHA-294x, AHA-2950U2B, AHA-39xx, AHA-3940/U/UW/W/AU/AUW/AUWD/UWD/U2x, AHA-3950U2B/U2x/U2D, AHA-3985, AHA-2944/W/UW, AHA-3944/U/W//UW/AUWD, AHA-4944W/UW, AHA-29160/C/N/LP, AHA-19160, AHA-3960D, AAA-131U2 AIC-7815, AIC-7810, AIC-7821, AIC-7850, AIC-7855, AIC-3860, AIC-1480, AIC-7860, AIC-7861, AIC-7870, AIC-7871, AIC-7872, AIC-7873, AIC-7874, AIC-7875, AIC-7875, AIC-7876, AIC-7880U, AIC-7890, AIC-7891, AIC-7895, AIC-7881U, AIC-7882U, AIC-7883U, AIC-7884U, AIC-7885, AIC-7886, AIC-788x, AIC-7888, AIC-7896, AIC-7896U2, AIC-7897U2,AIC-7892A/B/D/P, AIC-7899B/D/P	SCSI	aic7xxx
	SCSI Adaptor (571E,571F)	SCSI	ipr
	SAS Adapter (572A,572C,572B,572D,572F)	SAS	ipr
	ServeRAID	SCSI	ips
	1420SA, 1430SA	SATA	sata_mv
	AAR-1210SA	SATA	sata_sil
	ASC-1405	SAS	mvsas
	Series 9, PQI 12G SAS, QS-8204-8i, QS-8238-16i, QS-8236-16i, QS-8240-24i, QS-8242-24i, SmartRAID 3162-8i /e, martRAID 3100, SmartRAID 3162-8i, SmartRAID 3154-24i, SmartRAID 3154-8i16e, SmartRAID 3154-8i8e, SmartRAID 3154-16i, HBA 1100, HBA 1100-16i, HBA 1100-16i, HBA 1100-8i8e, |HBA 1100-24i, SmartHBA 2100, SmartHBA 2100A-8i,	SAS	smartpqi
	SmartHBA-SA(8i, 8e, 16i, 4i4e)	SAS	hpsa
	PMC-Sierra PM8001, PM8018, PM8019	SAS	pm80xx
Adaptec (ICP vortex)	ICP9085LI, ICP5085BR, ICP5445AU,	SAS	aacraid
	ICP9024RO, ICP9014RO	SCSI	aacraid
	ICP9047MA, ICP9087MA, ICP9067MA	SATA	aacraid

ADATA Technology	XPG SX8200, XPG GAMMIX S50, IM2P33F8ABR1	NVMe	nvme
Advanced System	ASC1100/1200/1300, ABP940-U, ABP940-UW, ABP940-U2W, ABP960-U, ABP3950-U3W	SCSI	advansys
ALi	M5228, M5229	IDE	pata_ali
	ULi M5288 SATA(AHCI)	SATA	ahci
	ALi M5281, ULi 5287, ULi 5289	SATA	sata_uli
	ALi M5281 SATA RAID	SATA	sata_via
Amazon.com	NVMe Controller	NVMe	nvme
AMD	CS5536	IDE	pata_cs5536
	CS5536, AMD-755,756,766,768,2092,81111 IDE	IDE	pata_amd
	Hudson IDE Controller	IDE	pata_atiixp
	Hudson SATA Controller, CZ SATA, AMD ahci Controller	SATA	ahci
	53c974	SCSI	tmscsim
	AMD sdhci Controller	MMC	sdhci_pci
AMI/LSI Logic	MegaRAID 428, 434 MegaRAID 438, 466, 467	SCSI	megaraid
Apple	S1X, S3X, ANS2	NVMe	nvme
Areca Technology	ARC-1110, ARC-1120, ARC-1130, ARC-1160, ARC-1170, ARC-1200, ARC-1210, ARC-1220, ARC-1230, ARC-1231, ARC-1260, ARC-1680, ARC-1880, ARC-1203, ARC-12x4, ARC-1884, ARC-1886	SATA	arcmsr
	ARC-1300ix-16, 1320	SAS	mvsas
Artop Electronic	ATP867	IDE	pata_atp867x
	ATP850UF, ATP860, ATP865	IDE	pata_artop
	AEC6710, AEC6712/UW/U/S/D/SUW, AEC67160/S, AEC16712	SCSI	atp870u
	ATP8620	SATA	acard_ahci
ASMedia Technology	ASM1060, ASM1061, ASM1062	SATA	ahci
ATI	Dual Channel BusMater IDE, 3xx PATA, SB400, SB600, SB700, SB800 IDE	IDE	pata_atiixp
	SB600, SB700, SB800 SATA	SATA	ahci
	436E, IXP SB400 SATA	SATA	sata_sil
Atto	Ultra320 SCSI	SCSI	mptspi
	ExpressSAS R680,R608,R60F,R6F0,R644,R648	SAS	esas2r
	ExpressSAS H1280,H1208,H1244,H12F0,H120F,H1288	SAS	pm80xx
	ExpressSAS GT 12Gb/s SAS/SATA HBA	SAS	mpt3sas
	Celerity FC-161E, FC-161P, FC-162E, FC-161P, FC-164E, FC-164P, FC-321E, FC-321P, FC-322E, FC-322P, FC-324P, FC-324E	FC	lpfc
Broadcom	OSB4, OSB5, OSB6, BCM5785	IDE	pata_serverworks
	K2, RAIDCore RC4000, BCM5785 [HT1000], HT1100	SATA	sata_svw
	Fusion-MPT 24GSAS, PCIe SAS40xx	SAS	mpi3mr
	MegaRAID SAS38xx ,SAS39xx	SAS	megaraid_sas
	Fusion-MPT SAS38x, SAS39xx	SAS	mpt3sas
Brocade	400	FC	mtpfc
	415/815/41B/81B, 425/825/42B/82B, 804 8Gbps, 1860 16Gbps, 1867/1869 16Gbps	FC	bfa
BusLogic	BT-946C, Flashpoint LT	SCSI	BusLogic
CNEX	LightNVM, 8800 series NVMe SSD	NVMe	nvme
Compaq	Smart-2/P, Smart-2SL, Smart Array 221, 3100ES, 3200 (DEC) Smart Array 4200, 4250ES, 431	SCSI	cpqarray
DEC	NetRAID-4M, 5400S	SCSI	aacraid
Dell	PowerEdge 2/SC, 2/DC,	SCSI	megaraid
	PowerEdge 4/DC, 4/SC, 4/Di, 4e/Si, 4e/Di PowerEdge 3/QC, 3/SC, 3/DC, 4/QC PowerEdge 1750	SCSI	megaraid_mbox
	CERC RAID ATA100/4CH	IDE	megaraid_mbox
	PowerEdge 2, 320/DC, 2/Si PowerEdge 2400, 2450, 4400 PowerEdge 3/Si, 3/DiV, 3/DiL, 3/Di, 3/DiJ, 3/DiD, 3/DiB	SCSI	aacraid
	CERC SATA 6ch	SATA	aacraid
	PowerEdge PERC 5i, 6i	SAS	megaraid_sas
DTC	Domex 536	SCSI	dmx3191d
	Domex DMX3194UP	SCSI	initio
Emulex	LP6000, Proteus-X, Saturn, LP952, Thor, Helios, Zephyr, Neptune, Saturn-X, LP7000, LP8000, LP9000, LP9802, Thor-X, Viper, Herios-X, Zephyr-X, Saturn-X, Proteus-X, Helios-X,	FC	lpfc

	LightPulse 8Gb/s PCIe, LPSe12002 EmulexSecure, Lancer-X, LightPulse 16Gb, Lancer Gen6: LPe32000, LPe36000, LPe37000/LPe38000 Series 32Gb/64Gb		
ENE Technology	SD/MMC Card Reader Controller	MMC	sdhci_pci
Enmotus	8000 Storage	SATA	ahci
Future Domain	TMC-3260/AHA-2920A	SCSI	fdomain_pci
Genesys Logic	GL9763E, GL9750 eMMC Controller	MMC	sdhci-pci
HGST	Ultrastar SN100,SN200 Series NVMe SSD, NVMe	NVMe	nvme
HP(Compaq)	Smart Array 5300, 5i, 532, 5312, 6i, 641, 642, 6400, 6400EM	SCSI	cciss
	3Gb/s SAS RAID, P800, P400, P400i, E200i, E200, E500, P700m	SAS	cciss
	P212, P410, P410i, P411, P711m, 712m, P812, P230i, P430, P431, P731m, P830, P830i, Generation 6, Generation 8 controlles, Generation 9 controlles P240nr, H240nr, H244br, P246br, P430i, P840, StorageWorks 1210m, P1224, P1228, P1224e, P1228e	SAS	hpsa
	NetRAID-1Si, NetRAID-3Si MegaRAID 438, MegaRAID T5	SCSI	megaraid
HighPoint	RocketRAID 3120, 3220, 3320 361x, 362x, 364x, 366x, 368x, 369x, 452x	SATA	hptiop
	RocketRAID 644L	SATA	ahci
	RocketRAID 2710,2720,2721,2722,2740,2744	SAS	mvsas
	RocketRAID 1720, 1740, 1742, 230x, 2310, 2640	SATA	sata_mv
IBM	ServeRAID 8i, 8k/8k-l4, 8k/8k-l8	SAS	aacraid
	SCSI Adapter (2780,571B,571A)	SCSI	ipr
	SAS Adapter (2CCA,2CD2,2CCD, 572E,572A,572C,572B,571D,574D,574E,57B1,57B2,57B3, 57B4,57B5,57C3,57C4,57C6,57C8,57CC,57CE,57D7,57D8, 57EB,57EC,57ED,580A,580B IPR SAS Adapter (ASIC)	SAS	ipr
	ServeRAID controller II, 3H, 3L, 4H, 4M, 4L, 4Mx, 4Lx, 5i , 5i, 6M , 6i, 7t, 7k, 7M	SCSI	ips
ICP Vortex(intel)	GDT Raid Controller	SCSI	gdth
Initio	INI-920, 935, 940, 950	SCSI	initio
	INI-A100U2W	SCSI	a100u2w
	INI-1623	SATA	sata_inic162x
Intel	SCH IDE	IDE	pata_sch
	82371FB	IDE	pata_oldpiix
	82801, ICH4, ICH5, ICH6, ICH7, ICH8, 6300ESB, 631xESB, 632xESB, 82371SB PIIX3, 82371AB/EB/MB PIIX4, 82440MX, 82372FB PIIX5, Virtual PC, 82801DBL (ICH4-L)	IDE	ata_piix
	430MX - 82371MX	IDE	pata_mpiix
	ICH6, ICH7, ICH8, ICH9, ICH10, 631xESB, 632xESB, EP80579 5 Series, 3400 Series, Ibex Peak, 6 Series, C600/X79 series, 7 Series, Panther Point, DH89xxCC, C2000, Wellsburg sSATA, Lynx Point-LP, 8 Series/C220, 9 Series ValleyView, Coleto Creek, Wildcat Point-LP, Sunrise Point-LP, Sunrise Point-H, DNV AHCI, Lewisburg AHCI, 6th,7th,8th Gen CPU AHCI, other newer AHCI	SATA	ahci
	ICH5, ICH6, ICH7, ICH8, ICH9, ICH10, 6300ESB, 631xESB, 632xESB, EP80579, 3100, 5 Series, 3400 Series, 6 Series, C600/X79 series, 7 Series C2000, Wellsburg sSATA, DH89xxCC, Lynx Point-LP. 8 Series/C220, 9 Series,	SATA	ata_piix
	C600/X79 series, C602, C604/X79 series, C606, C608	SAS	isci
	80960RP (i960RP)	SCSI	megaraid
	GD31244	SATA	sata_vsc
	Atom Z36xxx/Z37xxx SDIO, Atom E3800 eMMC, Atom/Celeron/Pentium x5-E8000/J3xxx/N3xxx N4200/N3350/E3900 MMC, EG20T SDIO, SD Host, Comet Lake PCH-LP SCS3	MMC	sdhci_pci
	PCIe Data Center SSD, NVMe, QEMU NVM Express, 600P, 7600p/760p/E, 6100p	NVMe	nvme

	Volume Management Device NVMe RAID Controller	NVMe	vmd
	ATA Generic	IDE	ata_generic
ITE	IT8213	IDE	pata_it8213
	IT8211F, IT8212	IDE	pata_it821x
JMicron Technology	JMB362, AHCI Controller	SATA	ahci
	PATA Controller	IDE	pata_jmicron
	SD/MMC Host Controller	MMC	sdhci_pci
Kingston Technology	NVMe controller	NVMe	nvme
LSI Logic	Integrated Smart Array, RAID LC2	SCSI	cpqarray
	MegaRAID	SATA	megaraid_mbox
	MegaRAID	SCSI	megaraid_mbox
	MagaRAID SAS 1078, 1078DE, 9240, 9260, Verde ZCR, 2208, SAS-3 3108, SAS-3 3008 SAS 2208, SAS3404, SAS3408, SAS3416, SAS3504, SAS3508, SAS3516, SAS-3 3216/3224, SAS-3 3316, SAS-3 3324	SAS	megaraid_sas
	SAS1064, SAS4068, SAS1064ET, SAS1068E, SAS1078, SAS8208ELP, SAS8208ELP	SAS	mptsas
	SAS2116, SAS2004, SAS2008, SAS2108, SAS2208, SAS2308, SSS6200, SAS3108, SAS3004, SAS3008	SAS	mpt2sas
	SAS3216, SAS3224, SAS3316, SAS3324, SAS3408, SAS3416, SAS3508, SAS3516, SAS3616	SAS	mpt3sas
	53c1030, 53c1035	SCSI	mptspi
Marvell	88SE6440,MV64460/64461/64462, 9180, 9480, 88SE644 88SE9445, 88SE9480, 88SE9485	SAS	mvsas
	88SE6121, 88SE6414 SATA, 88SE9123, 88SE9125 88SE912x, 88SE9170, 88SE9172, 88SE9230	SATA	ahci
	88SE6101, 88SE6121, 88SE6145, 88SE912x	IDE	pata_marvell
	MV88SX5040, MV88SX5041, MV88SX5080, MV88SX5081, MV88SX6041, 88SX6042, 88SX6042, MV88SX6081, 88SX7042	SATA	sata_mv
	OLPC Cafe Controller	MMC	sdhci_pci
	NVMe controller	NVMe	nvme
MAXIO Technology	NVMe controller	NVMe	nvme
Microchip Technology	SLC90E66	IDE	pata_efar
Micron	Samurai_IDE	IDE	ata_generic
	RealSSD P320h, P320m, P320s, P325m, P420h, P420m, P425m	PCIe	mtip32xx
	NVMe controller	NVMe	nvme
Mylex	DAC960P, DAC960PD, DAC960PG, eXtremeRAID 2000/3000 AcceleRAID 352/170/160	SCSI	DAC960
	U320 SCSI/RAID	SCSI	ipr
National Semiconductor	87410	IDE	pata_ns87410
	87415, 87560	IDE	pata_ns87415
Netac Technology	NVMe controller	NVMe	nvme
nVidia	CK804, CK8S, MCP04, MCP2A, MCP51, MCP55, MCP61, MCP65, MCP67, MCP73, MCP78S, nForce, nForce2, nForce3	IDE	pata_amd
	MCP65, MCP67, MCP73, MCP77, MCP7B, MCP78S, MCP79, MCP89, MCP SATA2 GeForce 7100/nForce 630i, GeForce 8200	SATA	ahci
	MCP04 , CK804, nForce2, nForce3, MCP51, MCP55, MCP61	SATA	sata_nv
	MCP89	SATA	ata_generic
O2 Micro	OZ600FJ1/OZ900FJ1, OZ600FJ0/OZ900FJ0/OZ600FJS, OZ600RJ1/OZ900RJ1, OZ600RJ0/OZ900RJ0/OZ600RJS	MMC	sdhci_pci
OCZ Technology	MVSAS, RevoDrive 3 X2 PCI-Express SSD	SAS	mvsas
OPTi	82C558	IDE	ata_generic
	82C621, 82C825	IDE	pata_opti
	82C825	IDE	pata_optidma
Pacific Digital	ADMA-100 DiscStaQ	IDE	pdc_adma
	QMaster Controller	SATA	sata_qstor
Phison Electronics	NVMe controller	NVMe	nvme
PMC-Sierra	BR522x [PMC-Sierra maxRAID SAS Controller]	SAS	pmcraid
	PM80xx, PM8009	SAS	pm80xx
	PDC20246, PDC20263, PDC20262 (FastTrak66/Ultra66), PDC20265(FastTrak100 Lite/Ultra100), PDC20267	IDE	pata_pdc202xx_old

	(FastTrak100/Ultra100),		
	PDC20275, PDC20268 (Ultra100 TX2), PDC20269, PDC20276 (MBFastTrak133 Lite), PDC20270 (FastTrak100 LP/TX2/TX4), PDC20271 (FastTrak TX2000), PDC20277 (SBFastTrak133 Lite)	IDE	pata_pdc2027x
Promise	PDC20318 (SATA150 TX4), PDC20319 (FastTrak S150 TX4), PDC20371 (FastTrak S150 TX2plus), PDC20378 (FastTrak 378/SATA 378), PDC20375 (SATA150 TX2plus), PDC20376 (FastTrak 376), PDC40719 [FastTrak TX4300/TX4310], PDC40519 (FastTrak TX4200), 20771 (FastTrak TX2300), PDC20571 (FastTrak TX2200), PDC20579 SATAII 150 IDE Controller, PDC40779 (SATA 300 779), PDC40718 (SATA 300 TX4), PDC20518/PDC40518 (SATAII 150 TX4), PDC40775 (SATA 300 TX2plus), PDC20575 (SATAII150 TX2plus), PDC20619 (FastTrak TX4000)	SATA	sata_promise
	PDC42819 [FastTrak TX2650/TX4650] FastTrak TX8660	SATA	ahci
	PDC20621 [SATA150 SX4]	SATA	sata_sx4
	80333 [SuperTrak EX4350][SuperTrak EX24350][SuperTrak EX8350/EX16350][SuperTrak EX12350][SuperTrak EX24350], 80331 [SuperTrak EX8300/EX16300], 8870(p3), 8871(p3)	SATA	stex
	81384 [SuperTrak EX SAS and SATA RAID Controller], PM8010 [SuperTrak EX SAS and SATA 6G RAID Controller]	SAS	stex
	SATAII 150 SX8	SATA	sx8
QLogic	ISP10160, ISP1020, ISP1080, ISP12160, ISP1240, ISP1280	SCSI	qla1280
	QLA2100, QLA200, QLA2300, ISP2312, ISP2322, ISP2422, ISP2432, ISP2532, ISP2432M SP232, SP202, SP212, ISP2714, ISP2722, ISP2852, ISP2854, ISP2812, ISP2814	FC	qla2xxx
RDC	R1010	IDE	pata_it821x
Realtek	RTS5250	MMC	sdhci_pci
	RTS5763DL NVMe SSD	NVMe	nvme
Ricoh	R5C822, R5C843 MMC/SD	MMC	sdhci_pci
Samsung Electronics	Apple PCIe SSD, XP941 PCIe SSD, SM951 PCIe SSD	SATA	ahci
	172X,172Xa,172Xb, PM9B1, 980	NVMe	nvme
Sandisk	Skyhawk Series NVME SSD	NVMe	nvme
Seagate	Nytro Flash Storage	NVMe	nvme
Shenzhen Longsys Electronics	NVMe controller	NVMe	nvme
SiliconImage	PCI0643, PCI0646, PCI0648, PCI0649	IDE	pata_cmd64x
	PCI0680	IDE	pata_sil680
	PCI0640	IDE	pata_cmd640
	3112, 3114, 3512	SATA	sata_sil
	3132, 3124, 3531	SATA	sata_sil24
Silicon Motion	SM2263EN/SM2263XT SSD Controller	NVMe	nvme
SiS	AHCI Controller	SATA	ahci
	180, 182 SATA Controller	SATA	sata_sis
	5513 [IDE]	IDE	pata_sis
SK hynix	NVMe controller	NVMe	nvme
ST Microelectronics	ST ConneXt	SATA	ahci
Symbios/LSI	53c810, 53c820, 53c825, 53c815, 53c810AP, 53c860, 53c1510, 53C896/897, 53c895, 53c885, 53c875, 53C1510, 53c895a, 53c875a, 53c1010, 53c875J	SCSI	sym53c8xx
Synopsys	c202	MMC	sdhci-pci
Tekram	TRM-S1040 (DC395/DC315)	SCSI	dc395x
Toshiba America	EX-IDE	IDE	ata_generic
United Microelectronics [UMC]	UM8673F, UM8886BF, UM8886A	IDE	ata_generic
VIA	VT82C576MV	IDE	ata_generic
	VT82C586A/B/VT82C686/A/B/VT823x/A/C, CX700/VX700, VT82C576M/VT82C586, VT6410, VX800, VX855/VX875, 9000	IDE	pata_via

	VT8237A, VT6420 , VT6421, VT8251, VT6421, 9000	SATA	sata_via
Vitesse	VSC-7174	SATA	sata_vsc
VMWare	PVSCSI SCSI Controller	SCSI	vmw_pvscsi
WorkBit	Ninja(0x8008,f008,f02c)	IDE	pata_ninja32

32bit execution

Manufacturer	Product name	Interface	Driver used
3ware	5xxx/6xxx PATA-RAID	IDE	3w-xxxx
	7xxx/8xxx PATA/SATA-RAID	SATA	3w-xxxx
	9xxx SATA-RAID, 9550sx,9650SE SATAII RAID 9690SA SAS/SATAII RAID	SATA	3w-9xxx
	9750 SAS2/SATA-II	SAS	3w-sas
Adaptec	Themisto, Catapult, Tomcat, Callisto AAC-RAID series ASR-2020ZCR, ASR-2025ZCR, ASR-2130S, ASR-2230S, ASR-2240S Legend S220,S230, 2120S, 2200S, 3230S, 3240S	SCSI	aacraid
	ASR-4005SAS, ASR-4000, ASR-4800S, AS4805SAS, SRC 8x6G SAS, Series 7 6G SAS, Series 8 12G SAS, Series 9	SAS	aacraid
	ASR-2020SA, ASR-2025SA, ASR-2420SA, ASR-2620SA, ASR-2820SA AAR-2610SA, AAR-2410SA, AAR-2810SA, AAR-21610SA	SATA	aacraid
	ASC-29320/A/B/LP/ALP/LPE, ASC-39320/A/B/D, AIC-7901/A, AIC-7902/B	SCSI	aic79xx
	AHA-2940/U/W/UW/D/U2/U2W/U2B, AHA-2930CU/UW/U2, AHA-2904, AHA-294x, AHA-2950U2B, AHA-39xx, AHA-3940/U/UW/W/AU/AUW/AUWD/UWD/U2x, AHA-3950U2B/U2x/U2D, AHA-3985, AHA-2944/W/UW, AHA-3944/U/W//UW/AUWD, AHA-4944W/UW, AHA-29160/C/N/LP, AHA-19160, AHA-3960D, AAA-131U2 AIC-7815, AIC-7810, AIC-7821, AIC-7850, AIC-7855, AIC-3860, AIC-1480, AIC-7860, AIC-7861, AIC-7870, AIC-7871, AIC-7872, AIC-7873, AIC-7874, AIC-7875, AIC-7875, AIC-7876, AIC-7880U, AIC-7890, AIC-7891, AIC-7895, AIC-7881U, AIC-7882U, AIC-7883U, AIC-7884U, AIC-7885, AIC-7886, AIC-788x, AIC-7888, AIC-7896, AIC-7896U2, AIC-7897U2,AIC-7892A/B/D/P, AIC-7899B/D/P	SCSI	aic7xxx
	SCSI Adaptor (571E,571F)	SCSI	ipr
	SAS Adapter (572A,572C,572B,572D,572F)	SAS	ipr
	ServeRAID	SCSI	ips
	1420SA, 1430SA	SATA	sata_mv
	AAR-1210SA	SATA	sata_sil
	ASC-1405	SAS	mvsas
	Series 9, PQI 12G SAS, QS-8204-8i, QS-8238-16i, QS-8236-16i, QS-8240-24i, QS-8242-24i, SmartRAID 3162-8i /e, martRAID 3100, SmartRAID 3162-8i, SmartRAID 3154-24i, SmartRAID 3154-8i16e, SmartRAID 3154-8i8e, SmartRAID 3154-16i, HBA 1100, HBA 1100-16i, HBA 1100-16i, HBA 1100-8i8e, |HBA 1100-24i, SmartHBA 2100, SmartHBA 2100A-8i,	SAS	smartpqi
	SmartHBA-SA(8i, 8e, 16i, 4i4e)	SAS	hpsa
	PMC-Sierra PM8001, PM8018, PM8019	SAS	pm80xx
Adaptec (ICP vortex)	ICP9085LI, ICP5085BR, ICP5445AU,	SAS	aacraid
	ICP9024RO, ICP9014RO	SCSI	aacraid
	ICP9047MA, ICP9087MA, ICP9067MA	SATA	aacraid
Advanced System	ASC1100/1200/1300, ABP940-U, ABP940-UW, ABP940-U2W, ABP960-U, ABP3950-U3W	SCSI	advansys
ALi	M5228, M5229	IDE	pata_ali
	ULi M5288 SATA(AHCI)	SATA	ahci
	ALi M5281, ULi 5287, ULi 5289	SATA	sata_uli
	ALi M5281 SATA RAID	SATA	sata_via
AMD	CS5536	IDE	pata_cs5536
	CS5536, AMD-755,756,766,768,2092,81111 IDE	IDE	pata_amd
	Hudson IDE Controller	IDE	pata_atiixp
	Hudson SATA Controller, CZ SATA, AMD ahci Controller	SATA	ahci
	53c974	SCSI	tmscsim

	AMD sdhci Controller	MMC	sdhci_pci
AMI/LSI Logic	MegaRAID 428, 434 MegaRAID 438, 466, 467	SCSI	megaraid
Apple	S1X, S3X	NVMe	nvme
Areca Technology	ARC-1110, ARC-1120, ARC-1130, ARC-1160, ARC-1170, ARC-1200, ARC-1210, ARC-1220, ARC-1230, ARC-1231, ARC-1260, ARC-1680, ARC-1880, ARC-1203, ARC-12x4, ARC-1884	SATA	arcmsr
	ARC-1300ix-16, 1320	SAS	mvsas
Artop Electronic	ATP867	IDE	pata_atp867x
	ATP850UF, ATP860, ATP865	IDE	pata_artop
	AEC6710, AEC6712/UW/U/S/D/SUW, AEC67160/S, AEC16712	SCSI	atp870u
	ATP8620	SATA	acard_ahci
ASMedia Technology	ASM1060, ASM1061, ASM1062	SATA	ahci
ATI	Dual Channel BusMater IDE, 3xx PATA, SB400, SB600, SB700, SB800 IDE	IDE	pata_atiixp
	SB600, SB700, SB800 SATA	SATA	ahci
	436E, IXP SB400 SATA	SATA	sata_sil
Atto	Ultra320 SCSI	SCSI	mptspi
	ExpressSAS R680,R608,R60F,R6F0,R644,R648	SAS	esas2r
	ExpressSAS H1280,H1208,H1244,H12F0,H120F,H1288	SAS	pm80xx
Broadcom	OSB4, OSB5, OSB6, BCM5785	IDE	pata_serverworks
	K2, RAIDCore RC4000, BCM5785 [HT1000], HT1100	SATA	sata_svw
Brocade	400	FC	mtpfc
	415/815/41B/81B, 425/825/42B/82B, 804 8Gbps, 1860 16Gbps, 1867/1869 16Gbps	FC	bfa
BusLogic	BT-946C, Flashpoint LT	SCSI	BusLogic
CNEX	LightNVM, 8800 series NVMe SSD	NVMe	nvme
Compaq	Smart-2/P, Smart-2SL, Smart Array 221, 3100ES, 3200 (DEC) Smart Array 4200, 4250ES, 431	SCSI	cpqarray
DEC	NetRAID-4M, 5400S	SCSI	aacraid
Dell	PowerEdge 2/SC, 2/DC,	SCSI	megaraid
	PowerEdge 4/DC, 4/SC, 4/Di, 4e/Si, 4e/Di PowerEdge 3/QC, 3/SC, 3/DC, 4/QC PowerEdge 1750	SCSI	megaraid_mbox
	CERC RAID ATA100/4CH	IDE	megaraid_mbox
	PowerEdge 2, 320/DC, 2/Si PowerEdge 2400, 2450, 4400 PowerEdge 3/Si, 3/DiV, 3/DiL, 3/Di, 3/DiJ, 3/DiD, 3/DiB	SCSI	aacraid
	CERC SATA 6ch	SATA	aacraid
	PowerEdge PERC 5i, 6i	SAS	megaraid_sas
DTC	Domex 536	SCSI	dmx3191d
	Domex DMX3194UP	SCSI	initio
Emulex	LP6000, Proteus-X, Saturn, LP952, Thor, Helios, Zephyr, Neptune, Saturn-X, LP7000, LP8000, LP9000, LP9802, Thor-X, Viper, Herios-X, Zephyr-X, Saturn-X, Proteus-X, Helios-X, LightPulse 8Gb/s PCIe, LPSe12002 EmulexSecure, Lancer-X, LightPulse 16Gb, Lancer Gen6: LPe32000, LPe36000	FC	lpfc
ENE Technology	SD/MMC Card Reader Controller	MMC	sdhci_pci
Enmotus	8000 Storage	SATA	ahci
HGST	Ultrastar SN100,SN200 Series NVMe SSD, NVMe	NVMe	nvme
HP(Compaq)	Smart Array 5300, 5i, 532, 5312, 6i, 641, 642, 6400, 6400EM	SCSI	cciss
	3Gb/s SAS RAID, P800, P400, P400i, E200i, E200, E500, P700m	SAS	cciss
	P212, P410, P410i, P411, P711m, 712m, P812, P230i, P430, P431, P731m, P830, P830i, Generation 6, Generation 8 controlles, Generation 9 controlles P240nr, H240nr, H244br, P246br, P430i, P840, StorageWorks 1210m, P1224, P1228, P1224e, P1228e	SAS	hpsa
	NetRAID-1Si, NetRAID-3Si MegaRAID 438, MegaRAID T5	SCSI	megaraid
HighPoint	RocketRAID 3120, 3220, 3320 361x, 362x, 364x, 366x, 368x, 369x, 452x	SATA	hptiop
	RocketRAID 644L	SATA	ahci
	RocketRAID 2710,2720,2721,2722,2740,2744	SAS	mvsas
	RocketRAID 1720, 1740, 1742, 230x, 2310	SATA	sata_mv

IBM	ServeRAID 8i, 8k/8k-l4, 8k/8k-l8	SAS	aacraid
	SCSI Adapter (2780,571B,571A)	SCSI	ipr
	SAS Adapter (2CCA,2CD2,2CCD, 572E,572A,572C,572B,571D,574D,574E,57B1,57B2,57B3, 57B4,57B5,57C3,57C4,57C6,57C8,57CC,57CE,57D7,57D8, 57EB,57EC,57ED,580A,580B) IPR SAS Adapter (ASIC)	SAS	ipr
	ServeRAID controller II, 3H, 3L, 4H, 4M, 4L, 4Mx, 4Lx, 5i , 5i, 6M , 6i, 7t, 7k, 7M	SCSI	ips
ICP Vortex(intel)	GDT Raid Controller	SCSI	gdth
Initio	INI-920, 935, 940, 950	SCSI	initio
	INI-A100U2W	SCSI	a100u2w
	INI-1623	SATA	sata_inic162x
Intel	SCH IDE	IDE	pata_sch
	82371FB	IDE	pata_oldpiix
	82801, ICH4, ICH5, ICH6, ICH7, ICH8, 6300ESB, 631xESB, 632xESB, 82371SB PIIX3, 82371AB/EB/MB PIIX4, 82440MX, 82372FB PIIX5, Virtual PC, 82801DBL (ICH4-L)	IDE	ata_piix
	430MX - 82371MX	IDE	pata_mpiix
	ICH6, ICH7, ICH8, ICH9, ICH10, 631xESB, 632xESB, EP80579 5 Series, 3400 Series, Ibex Peak, 6 Series, C600/X79 series, 7 Series, Panther Point, DH89xxCC, C2000, Wellsburg sSATA, Lynx Point-LP, 8 Series/C220, 9 Series ValleyView, Coleto Creek, Wildcat Point-LP, Sunrise Point- LP, Sunrise Point-H, DNV AHCI, Lewisburg AHCI, 6th,7h,8rh Gen CPU AHCI, 他AHCI	SATA	ahci
	ICH5, ICH6, ICH7, ICH8, ICH9, ICH10, 6300ESB, 631xESB, 632xESB, EP80579, 3100, 5 Series, 3400 Series, 6 Series, C600/X79 series, 7 Series C2000, Wellsburg sSATA, DH89xxCC, Lynx Point-LP. 8 Series/C220, 9 Series,	SATA	ata_piix
	C600/X79 series, C602, C604/X79 series, C606, C608	SAS	isci
	80960RP (i960RP)	SCSI	megaraid
	GD31244	SATA	sata_vsc
	Atom Z36xxx/Z37xxx SDIO, Atom E3800 eMMC, Atom/Celeron/Pentium x5-E8000/J3xxx/N3xxx N4200/N3350/E3900 MMC, EG20T SDIO, SD Host	MMC	sdhci_pci
	PCIe Data Center SSD, NVMe, QEMU NVM Express, 600P, 7600p/760p/E, 6100p	NVMe	nvme
	ATA Generic	IDE	ata_generic
ITE	IT8213	IDE	pata_it8213
	IT8211F, IT8212	IDE	pata_it821x
JMicron Technology	JMB362, AHCI Controller	SATA	ahci
	PATA Controller	IDE	pata_jmicron
	SD/MMC Host Controller	MMC	sdhci_pci
LSI Logic	Integrated Smart Array, RAID LC2	SCSI	cpqarray
	MegaRAID	SATA	megaraid_mbox
	MegaRAID	SCSI	megaraid_mbox
	MagaRAID SAS 1078, 1078DE, 9240, 9260, Verde ZCR, 2208, SAS-3 3108, SAS-3 3008 SAS 2208, SAS3404, SAS3408, SAS3416, SAS3504, SAS3508, SAS3516, SAS-3 3216/3224, SAS-3 3316, SAS-3 3324	SAS	megaraid_sas
	SAS1064, SAS4068, SAS1064ET, SAS1068E, SAS1078, SAS8208ELP, SAS8208ELP	SAS	mptsas
	SAS2116, SAS2004, SAS2008, SAS2108, SAS2208, SAS2308, SSS6200, SAS3108, SAS3004, SAS3008	SAS	mpt2sas
	SAS3216, SAS3224, SAS3316, SAS3324, SAS3408, SAS3416, SAS3508, SAS3516, SAS3616	SAS	mpt3sas
	FC909, FC929, FC919, FC929X, FC919X, FC949X, FC939X, FC949ES	FC	mptfc
	53c1030, 53c1035	SCSI	mptspi
	88SE6440,MV64460/64461/64462, 9180, 9480, 88SE644 88SE9445, 88SE9480, 88SE9485	SAS	mvsas

Marvell	88SE6121, 88SE6414 SATA, 88SE9123, 88SE9125 88SE912x, 88SE9170, 88SE9172, 88SE9230	SATA	ahci
	88SE6101, 88SE6121, 88SE6145, 88SE912x	IDE	pata_marvell
	MV88SX5040, MV88SX5041, MV88SX5080, MV88SX5081, MV88SX6041, 88SX6042, 88SX6042, MV88SX6081, 88SX7042	SATA	sata_mv
	OLPC Cafe Controller	MMC	sdhci_pci
Microchip Technology	SLC90E66	IDE	pata_efar
Micron	Samurai_IDE	IDE	ata_generic
	RealSSD P320h, P320m, P320s, P325m, P420h, P420m, P425m	PCIe	mtip32xx
Mylex	DAC960P, DAC960PD, DAC960PG, eXtremeRAID 2000/3000 AcceleRAID 352/170/160	SCSI	DAC960
	U320 SCSI/RAID	SCSI	ipr
nVidia	CK804, CK8S, MCP04, MCP2A, MCP51, MCP55, MCP61, MCP65, MCP67, MCP73, MCP78S, nForce, nForce2, nForce3	IDE	pata_amd
	MCP65, MCP67, MCP73, MCP77, MCP7B, MCP78S, MCP79, MCP89, MCP SATA2 GeForce 7100/nForce 630i, GeForce 8200	SATA	ahci
	MCP04 , CK804, nForce2, nForce3, MCP51, MCP55, MCP61	SATA	sata_nv
	MCP89	SATA	ata_generic
O2 Micro	OZ600FJ1/OZ900FJ1, OZ600FJ0/OZ900FJ0/OZ600FJS, OZ600RJ1/OZ900RJ1, OZ600RJ0/OZ900RJ0/OZ600RJS	MMC	sdhci_pci
OCZ Technology	MVSAS, RevoDrive 3 X2 PCI-Express SSD	SAS	mvsas
OPTi	82C558	IDE	ata_generic
Pacific Digital	ADMA-100 DiscStaQ	IDE	pdc_adma
	QMaster Controller	SATA	sata_qstor
PMC-Sierra	BR522x [PMC-Sierra maxRAID SAS Controller]	SAS	pmcraid
	PM80xx, PM8009	SAS	pm80xx
Promise	PDC20246, PDC20263, PDC20262 (FastTrak66/Ultra66), PDC20265(FastTrak100 Lite/Ultra100), PDC20267 (FastTrak100/Ultra100),	IDE	pata_pdc202xx_old
	PDC20275, PDC20268 (Ultra100 TX2), PDC20269, PDC20276 (MBFastTrak133 Lite), PDC20270 (FastTrak100 LP/TX2/TX4), PDC20271 (FastTrak TX2000), PDC20277 (SBFastTrak133 Lite)	IDE	pata_pdc2027x
	PDC20318 (SATA150 TX4), PDC20319 (FastTrak S150 TX4), PDC20371 (FastTrak S150 TX2plus), PDC20378 (FastTrak 378/SATA 378), PDC20375 (SATA150 TX2plus), PDC20376 (FastTrak 376), PDC40719 [FastTrak TX4300/TX4310], PDC40519 (FastTrak TX4200), 20771 (FastTrak TX2300), PDC20571 (FastTrak TX2200), PDC20579 SATAII 150 IDE Controller, PDC40779 (SATA 300 779), PDC40718 (SATA 300 TX4), PDC20518/PDC40518 (SATAII 150 TX4), PDC40775 (SATA 300 TX2plus), PDC20575 (SATAII150 TX2plus), PDC20619 (FastTrak TX4000)	SATA	sata_promise
	PDC42819 [FastTrak TX2650/TX4650] FastTrak TX8660	SATA	ahci
	PDC20621 [SATA150 SX4]	SATA	sata_sx4
	80333 [SuperTrak EX4350][SuperTrak EX24350][SuperTrak EX8350/EX16350][SuperTrak EX12350][SuperTrak EX24350], 80331 [SuperTrak EX8300/EX16300], 8870(p3), 8871(p3)	SATA	stex
	81384 [SuperTrak EX SAS and SATA RAID Controller], PM8010 [SuperTrak EX SAS and SATA 6G RAID Controller]	SAS	stex
	SATAII 150 SX8	SATA	sx8
QLogic	ISP10160, ISP1020, ISP1080, ISP12160, ISP1240, ISP1280	SCSI	qla1280
	QLA2100, QLA200, QLA2300, ISP2312, ISP2322, ISP2422, ISP2432, ISP2532, ISP2432M SP232, SP202, SP212, ISP2714, ISP2722	FC	qla2xxx
RDC	R1010	IDE	pata_it821x
Realtek	RTS5250	MMC	sdhci_pci
Ricoh	R5C822, R5C843 MMC/SD	MMC	sdhci_pci

Samsung Electronics	Apple PCIe SSD, XP941 PCIe SSD, SM951 PCIe SSD	SATA	ahci
	172X,172Xa,172Xb	NVMe	nvme
Seagate	Nytro Flash Storage	NVMe	nvme
SiliconImage	PCI0643, PCI0646, PCI0648, PCI0649	IDE	pata_cmd64x
	PCI0680	IDE	pata_sil680
	PCI0640	IDE	pata_cmd640
	3112, 3114, 3512	SATA	sata_sil
	3132, 3124, 3531	SATA	sata_sil24
SiS	AHCI Controller	SATA	ahci
	180, 182 SATA Controller	SATA	sata_sis
	5513 [IDE]	IDE	pata_sis
ST Microelectronics	ST ConneXt	SATA	ahci
Symbios/LSI	53c810, 53c820, 53c825, 53c815, 53c810AP, 53c860, 53c1510, 53C896/897, 53c895, 53c885, 53c875, 53C1510, 53c895a, 53c875a, 53c1010, 53c875J	SCSI	sym53c8xx
Synopsys	c202	MMC	sdhci-pci
Tekram	TRM-S1040 (DC395/DC315)	SCSI	dc395x
Toshiba America	EX-IDE	IDE	ata_generic
United Microelectronics [UMC]	UM8673F, UM8886BF, UM8886A	IDE	ata_generic
VIA	VT82C576MV	IDE	ata_generic
	VT82C586A/B/VT82C686/A/B/VT823x/A/C, CX700/VX700, VT82C576M/VT82C586, VT6410, VX800, VX855/VX875, 9000	IDE	pata_via
	VT8237A, VT6420 , VT6421, VT8251, VT6421, 9000	SATA	sata_via
Vitesse	VSC-7174	SATA	sata_vsc
VMWare	PVSCSI SCSI Controller	SCSI	vmw_pvscsi
WorkBit	Ninja(0x8008,f008,f02c)	IDE	pata_ninja32

Supported eMMC interface (acpi)

* Basically, the model number of the chip is used instead of the product name. To confirm, you need to find out the chip model number of the interface.
* The table shows the corresponding product notation for each driver. We have not confirmed the operation.
* Even the ones listed in the table may not work due to firmware version, driver defect, hardware environment, version difference, etc.
* Please be sure to check the operation before purchasing.
* Yellow green is added after Ver4.6.x. Gray is obsolete after Ver4.6.x.
* In a 32-bit execution, the contents has not changed after Ver4.6.x.

64bit execution			
Manufacturer	Product name	Interface	Driver used
AMD	SD Host Controller (AMDI0040, AMDI0041)	MMC	sdhci-acpi
Intel	SD Host controller (80860F14, 80860F16, 80865ACA, 80865AD0, INT33BB, INT33C6, INT3436, INT344D, PNP0D40)	MMC	sdhci-acpi
Qualcomm	SD Host controller (QCOM8051, QCOM8052)	MMC	sdhci-acpi

32bit execution			
Manufacturer	Product name	Interface	Driver used
Intel	SD Host controller (80860F14, 80860F16, 80865ACA, 80865AD0, INT33BB, INT33C6, INT3436, INT344D, PNP0D40)	MMC	sdhci-acpi
Qualcomm	SD Host controller (QCOM8051, QCOM8052)	MMC	sdhci-acpi

Supported Network Interface (Ethernet PCI/PCIe)

* Basically, the model number of the chip is used instead of the product name. To confirm, you need to find out the chip model number of the interface.
* The table shows the corresponding product notation for each driver. We have not confirmed the operation.
* Even the ones listed in the table may not work due to firmware version, driver defect, hardware environment, version difference, etc.
* Please be sure to check the operation before purchasing.
*Yellow green is added after Ver4.6.x. Gray is obsolete after Ver4.6.x.
*In a 32-bit execution, the contents has not changed after Ver4.6.x.

64bit execution		
Manufacturer	Product name	Driver used
3com	3c450,3c555,3c590,3c595,3c900,3c905,3C920,3c980, 3c982,3CSOHO100	3c59x
	3c940	skge
	3c985	acenic
	3C990,3CR990	typhoon
	3CSOHO100B	tulip
Abocom	21x4x DEC-Tulip,ADMtek Centaur-C	tulip
Accton	21x4x DEC-Tulip,EN-1216,EN-1217	tulip
	SMC2-1211TX	8139too
Adaptec	ANA620xx, ANA69011A	starfire
Addtron	RTL8139	8139too
ADMtek	21x4x DEC-Tulip,NC100	tulip
AMD	79c970,79c978	pcnet32
	AMD-8111	amd8111e
	10GB Ethernet	amd-xgbe
	DSC Ethernet	ionic
ALi	M5261,ULi 1689,ULi 1573	uli526x
Allied Telesyn	21x4x DEC-Tulip	tulip
	RTL81xx	8139too
		r8169
Alteon Networks	AceNIC,Farallon PN9100-T	acenic
Altima	AC1000,AC1001,AC1003,AC9100	tg3
Apple	Intrepid2,K2,Shasta,UniNorth, UniNorth 2,Pangea	sungem
	Tigon3	tg3
Aquantia	AQC107, AQC108, AQC111, AQC112, AQC100, AQC113CS	atlantic
Asix	AX88141	tulip
Beijing Wangxun Technology	|WX1860, RP1000, RP2000	ngbe
Broadcom	570x, (NetLink) BCM57780,BCM57781,BCM57785,BCM57788, BCM57790,BCM57791,BCM57795, BCM5781,BCM5784,BCM5785,BCM5786,BCM5787, BCM5789,BCM5906, (NetXtreme) 5714S,BCM5700,BCM5701,BCM5702,BCM5703, BCM5704,BCM5705,BCM5714,BCM5715,BCM5717, BCM5718,BCM5719,BCM5720,BCM5721,BCM5722, BCM5723,BCM5751,BCM5752,BCM5753,BCM5754, BCM5755,BCM5756,BCM5761,BCM5764, BCM57760,BCM57761,BCM57765,BCM5780, BCM5782,BCM5788,BCM5901, BCM5725, BCM5727, BCM5762, BCM57762, BCM57766, BCM57780, BCM5787M, BCM57764, BCM57767, BCM57782, BCM57786, BCM57787,	tg3
	BCM4401,BCM4402	b44
	NC370 (NetXtreme II) BCM5706,BCM5708,BCM5709,BCM5716	bnx2
	(NetXtreme II)	bnx2x

	BCM57710,BCM57711,BCM57712,BCM57800, BCM57810,BCM57840, BCM57811	
	BCM57301, BCM57302, BCM57304, BCM57417, BCM57311,BCM57312, BCM57314, BCM57402, BCM57404, BCM57406, BCM57407, BCM57412, BCM57414, BCM57416, BCM57417, BCM57452, BCM57454, BCM5745X, BCM58802, BCM58804, BCM57502, BCM57504, BCM57508, BCM5750X	bnxt_en
Brocade	-	bna
Cavium	PCI Endpoint NIC	octeon_ep
Chelsio	T210, other	cxgb
	S310-CR,N320-G2-CR,S320-LP-CR, T302,T310,T320	cxgb3
	PE10K,T404-BT,T420-BCH,T420-BT,T420-CR, T420-CX,T420-SO,T422-CR,T440-BCH, T440-CH,T440-CR, T440-LP-CR, T480 B404, B420, B504, B520, T404, T420, T420X, T440, T440F, T480, T502, T504, T520, T522, T540, T560, T580, T6225, T6240, T62100, T64100, T62100-608a, T62100-KR,	cxgb4
	B404, B420, B504, B520, T420, T422, T440, T440F, T440T, T480, T504, T520, T522, T540, T570, T580, T6225, T6240, T62100, T64100, T62100-608a	cxgb4vf
Cisco	VIC Ethernet NIC	enic
CNet	GigaCard	skge
Compaq	HNE-300	8139too
	NetFlex-3/P,Netelligent 10/100,	tlan
Compex	RL100-ATX 10/100	winbond-840
	RL100TX	tulip
Conexant	HCF 56k Modem	tulip
Corega	PCI NIC	r8192e_pci
Corigine	NIC	nfp
Davicom	Ethernet 100/10 MBit	dmfe
	21x4x DEC-Tulip	tulip
DELTA Electronics	RTL81xx	8139too
DEC	DECchip 21040,21041	de2104x
	DECchip 21140,21142,21143	tulip
	Farallon PN9000SX	acenic
D-Link	-	tulip
	DFE-550TX/FX,DFE-580TX,DL10050	sundance
	RTL8139	8139too
	DGE-528T, DGE-560T	r8169
	DGE-530T	skge
	DGE-550SX,DGE-550T,DGE-560SX,DGE-560T	sky2
	DL2000	dl2k
Edimax	RTL81xx	8139too
Efar	LAN9420/LAN9420i	smsc9420
Emulex	BladeEngine2,BladeEngine3,OneConnect,OneConnect(Skyhawk-VF)	be2net
Exar	X3100 Series	vxge
	Xframe,Xframe II	s2io
Fujitsu	-	tg3
Fungible	NIC	funeth
Hangzhou Silan	SC92031,RTL8139D	sc92031
Hawking	PN672TX	tulip
LSI	ET-131x	et131x
	21145	tulip
	80003ES2LAN, 82562G/GT/V,82566DC/DM/MC/MM, 82567LF/LM/V/,82571EB/PT,82572EI, 82573E/L/V,82574L,82577LC/LM,8258DC/DM, 82579LM/V,82583V,I217-LM,I217-V,I218-V,I218-LM,I219-V,I219-LM	e1000e
	82540EM/EP,82541EI/ER/GI/PI, 82542,82543GC,82544EI/GC, 82545EM/GM,82546EB/GB,82547EI/GI	e1000
	82551QM,82552,82557/8/9/0/1, 82559,8255xER,82551IT,	e100

Intel	82562EM/EX/GX/ET/EZ/GT/GZ/G, 82801BA/BAM/CA/CAM/DB/E/EB/ER, N10,PRO100VE/VM	
	82575EB/GB,82576/NS,82580,DH8900CC,I350, I210,I211,I354	igb
	82597EX	ixgb
	82598/EB,82599/EB/ES,X540-AT2,X520-4,X520-Q1,X540, X550T, X552, X557,	ixgbe
	X552, XL710, X710, X722	i40evf
	X550	ixgbevf
	X557, X710, XL710, X722, XXV710, I710,	i40e
	E810-C, E810-XXV, E822-L, E822-C, E823-L, E823-C	ice
	2.5G, I225-IT, I226-LM, I226-V, I225-LMvP	igc
Intersil	ISL3877, ISL3886, ISL3890, ISL3886IK	p54pci
JMicron	JMC250,JMC260	jme
LevelOne	FPC-0106TX	8139too
Linksys	21x4x DEC-Tulip	tulip
	Gigabit	skge
	Gigabit	r8169
Lite-On	LNE100TX	tulip
LSI Logic	83C885 NT50 DigitalScape Fast Ethernet, Yellowfin G-NIC gigabit	yellowfin
Macronix	MX98713,MX987x5	tulip
Marvell	88E8001,F5D5005	skge
	88E8021,88E8022,88E8035,88E8036,88E8038, 88E8039,88E8040,88E8042,88E8048,88E8050, 88E8052,88E8053,88E8055,88E8056,88E8057, 88E8058,88E8061,88E8062,88E8070,88E8071, 88E8072,88E8075,88EC032,88EC033,88EC034, 88EC036,88EC042, 88E8059	sky2
Mellanox	MT25400,MT25408,MT25418,MT25448,MT26418, MT26428,MT26438,MT26448,MT26468,MT26478, MT27500,MT27510,MT27520,MT27521,MT27530, MT27531,MT27540,MT27541,MT27550,MT27551, MT27560,MT27561	mlx4_en
	MT27600, MT27700, MT27710, MT27800, MT28800, MT28908, MT416842, MT2892, MT2894, MT2894, MT42822, MT43244	mlx5_core
Micrel-Kendin	KSZ8842-PMQL	ksz884x
Microcomputer	(2031)	sc92031
Microsoft	MN-130, MN-120	tulip
MYRICOM	Myri-10G	myri10ge
MYSON	MTD-8xx,EP-320X-S	fealnx
National Semiconductor	Aculab E1/T1 PMXc,DP83815	natsemi
	DP83065	cassini
	DP83820	ns83820
Netgear	GA620,GA630	acenic
Netronome Systems	NFP4000/NFP6000	nfp
NetXen	NX3031,NXB-10GCX4,NXB-10GXSR, NXB-4GCU,XG Mgmt	netxen_nic
Northern Telecom	RTL81xx	8139too
NVIDIA	CK804,CK8S,MCP04,MCP2A,MCP51,MCP55,MCP61, MCP65,MCP67,MCP73,MCP77,MCP79,MCP89, nForce,nForce2,nForce3	forcedeth
Olicom	OC-2183,OC-2185,OC-2325,OC-2326	tlan
Oracle/SUN	Cassini	cassini
	GEM	sungem
	Happy Meal	sunhme
	Multithreaded	niu
Packet Engines	GNIC-II	hamachi
Peppercon	ROL/F-100	8139too
Planex	-	tulip
	RTL81xx	8139too
QLogic	10GbE Converged	qlge
	cLOM8214, ISP8324 1/10GbE	qlcnic
	ISP4022-based,ISP4032-based	qla3xxx
	FastLinQ QL45000	qede
Qualcomm Atheros	Attansic L1	atl1
	Attansic L2	atl2
	AR8131,AR8132,AR8151,AR8152	atl1c

	AR8121,AR8113,AR8114	atl1e
	AR8161,AR8162,QCA8171,QCA8172,E2200, E2400	alx
	AR5008, AR922x	ath9k_pci_owl_loader
RDC Semiconductor	R6040	r6040
Realtek	RTL-8129,RTL-8139/8139C/8139C+	8139too
	RTL-8101E,RTL-8102E,RTL-8110SC,RTL-8111, RTL-8129,RTL-8168B,RTL-8169,,RTL-8169SC, E3000, RTL8125,	r8169
	RTL-8139/8139C/8139C+	8139cp
Sega	-	8139too
Silicon Graphics	AceNIC	acenic
SiS	190,191	sis190
	SiS7016,SiS900	sis900
Solarflare	[64] SFC4000,SFC9020,SFL9021 SFC9120, SFC9140, SFC9220, SFC9250	sfc
SMC	83c170,83c175	epic100
STMicroelectronics	21x4x DEC-Tulip	tulip
Sundance	IP100A,ST201	sundance
	TC902x	dl2k
SysKonnect|	SK-9871,SK-9872	skge
	SK-9Dxx,SK-9Mxx	tg3
	SK-9E21D,SK-9S21, SK-9E21M	sky2
TDK	RTL81xx	tulip
Tehuti Networks	10-Giga TOE	tehuti
Trident	4DWave DX	pcnet32
TTTech AG	TTP-Monitoring Card V2.0	8139cp
U.S. Robotics	USR997902	r8169
VIA	VT6102,VT6105,VT6106S,VT6105M,VT86C100A	via-rhine
	VT6120,VT6121,VT6122	via-velocity
Winbond	W89C840	winbond-840
Xilinx	Solarflare SFC9000/SFC9100-family	sfc

32bit execution		
Manufacturer	Product name	Driver used
3com	3c450,3c555,3c590,3c595,3c900,3c905,3C920,3c980, 3c982,3CSOHO100	3c59x
	3c940	skge
	3c985	acenic
	3C990,3CR990	typhoon
	3CSOHO100B	tulip
Abocom	21x4x DEC-Tulip,ADMtek Centaur-C	tulip
Accton	21x4x DEC-Tulip,EN-1216,EN-1217	tulip
	SMC2-1211TX	8139too
Addtron	RTL8139	8139too
ADMtek	21x4x DEC-Tulip,NC100	tulip
AMD	79c970,79c978	pcnet32
	AMD-8111	amd8111e
	10GB Ethernet	amd-xgbe
ALi	M5261,ULi 1689,ULi 1573	uli526x
Allied Telesyn	21x4x DEC-Tulip	tulip
	RTL81xx	8139too
		r8169
Alteon Networks	AceNIC,Farallon PN9100-T	acenic
Altima	AC1000,AC1001,AC1003,AC9100	tg3
Apple	Intrepid2,K2,Shasta,UniNorth, UniNorth 2,Pangea	sungem
	Tigon3	tg3
Aquantia	[64] AQC107, AQC108, AQC111, AQC112	atlantic
Asix	AX88141	tulip
AT&T	100VG ethernet	hp100
	570x, (NetLink) BCM57780,BCM57781,BCM57785,BCM57788, BCM57790,BCM57791,BCM57795, BCM5781,BCM5784,BCM5785,BCM5786,BCM5787, BCM5789,BCM5906, (NetXtreme) 5714S,BCM5700,BCM5701,BCM5702,BCM5703, BCM5704,BCM5705,BCM5714,BCM5715,BCM5717,	tg3

Broadcom	BCM5718,BCM5719,BCM5720,BCM5721,BCM5722, BCM5723,BCM5751,BCM5752,BCM5753,BCM5754, BCM5755,BCM5756,BCM5761,BCM5764, BCM57760,BCM57761,BCM57765,BCM5780, BCM5782,BCM5788,BCM5901, BCM5725, BCM5727, BCM5762, BCM57762, BCM57766, BCM57780, BCM5787M, BCM57764, BCM57767, BCM57782, BCM57786, BCM57787,	
	BCM4401,BCM4402	b44
	NC370 (NetXtreme II) BCM5706,BCM5708,BCM5709,BCM5716	bnx2
	(NetXtreme II) BCM57710,BCM57711,BCM57712,BCM57800, BCM57810,BCM57840, BCM57811	bnx2x
	BCM57301, BCM57302, BCM57304, BCM57417, BCM57311,BCM57312, BCM57314, BCM57402, BCM57404, BCM57406, BCM57407, BCM57412, BCM57414, BCM57416, BCM57417, BCM57452, BCM57454, BCM5745X, BCM58802, BCM58804	bnxt_en
Brocade	-	bna
Chelsio	T210, other	cxgb
	S310-CR,N320-G2-CR,S320-LP-CR, T302,T310,T320	cxgb3
	PE10K,T404-BT,T420-BCH,T420-BT,T420-CR, T420-CX,T420-SO,T422-CR,T440-BCH, T440-CH,T440-CR, T440-LP-CR, T480 B404, B420, B504, B520, T404, T420, T420X, T440, T440F, T480, T502, T504, T520, T522, T540, T560, T580, T6225, T6240, T62100, T64100,	cxgb4
	B404, B420, B504, B520, T420, T422, T440, T440F, T440T, T480, T504, T520, T522, T540, T570, T580, T6225, T6240, T62100, T64100,	cxgb4vf
Cisco	VIC Ethernet NIC	enic
CNet	GigaCard	skge
Compaq	HNE-300	8139too
	NetFlex-3/P,Netelligent 10/100,	tlan
Compex	RL100-ATX 10/100	winbond-840
	RL100TX	tulip
	ENet100VG4	hp100
Conexant	HCF 56k Modem	tulip
Davicom	Ethernet 100/10 MBit	dmfe
	21x4x DEC-Tulip	tulip
DELTA Electronics	RTL81xx	8139too
DEC	DECchip 21040,21041	de2104x
	DECchip 21140,21142,21143	tulip
	Farallon PN9000SX	acenic
D-Link	-	tulip
	DFE-550TX/FX,DFE-580TX,DL10050	sundance
	RTL8139	8139too
	DGE-528T, DGE-560T	r8169
	DGE-530T	skge
	DGE-550SX,DGE-550T,DGE-560SX,DGE-560T	sky2
	DL2000	dl2k
Edimax	RTL81xx	8139too
Efar	LAN9420/LAN9420i	smsc9420
Emulex	BladeEngine2,BladeEngine3,OneConnect,OneConnect(Skyhawk-VF)	be2net
Exar	X3100 Series	vxge
	Xframe,Xframe II	s2io
Fujitsu	-	tg3
Hangzhou Silan	SC92031,RTL8139D	sc92031
Hawking	PN672TX	tulip
LSI	ET-131x	et131x
	21145	tulip
	80003ES2LAN, 82562G/GT/V,82566DC/DM/MC/MM, 82567LF/LM/V/,82571EB/PT,82572EI, 82573E/L/V,82574L,82577LC/LM,8258DC/DM,	e1000e

Intel	82579LM/V,82583V,I217-LM,I217-V,I218-V,I218-LM,I219-V,I219-LM	
	82540EM/EP,82541EI/ER/GI/PI, 82542,82543GC,82544EI/GC, 82545EM/GM,82546EB/GB,82547EI/GI	e1000
	82551QM,82552,82557/8/9/0/1, 82559,8255xER,82551IT, 82562EM/EX/GX/ET/EZ/GT/GZ/G, 82801BA/BAM/CA/CAM/DB/E/EB/ER, N10,PRO100VE/VM	e100
	82575EB/GB,82576/NS,82580,DH8900CC,I350, I210,I211,I354	igb
	82597EX	ixgb
	82598/EB,82599/EB/ES,X540-AT2,X520-4,X520-Q1,X540, X550T, X552, X557,	ixgbe
	X552, XL710, X710, X722	i40evf
	X550	ixgbevf
	X557, X710, XL710, X722,	i40e
	E810-C	ice
	2.5G	igc
Intersil	ISL3877, ISL3886, ISL3890, ISL3886IK	p54pci
JMicron	JMC250,JMC260	jme
LevelOne	FPC-0106TX	8139too
Linksys	21x4x DEC-Tulip	tulip
	Gigabit	skge
	Gigabit	r8169
Lite-On	LNE100TX	tulip
LSI Logic	83C885 NT50 DigitalScape Fast Ethernet, Yellowfin G-NIC gigabit	yellowfin
Macronix	MX98713,MX987x5	tulip
Marvell	88E8001,F5D5005	skge
	88E8021,88E8022,88E8035,88E8036,88E8038, 88E8039,88E8040,88E8042,88E8048,88E8050, 88E8052,88E8053,88E8055,88E8056,88E8057, 88E8058,88E8061,88E8062,88E8070,88E8071, 88E8072,88E8075,88EC032,88EC033,88EC034, 88EC036,88EC042, 88E8059	sky2
Mellanox	MT25400,MT25408,MT25418,MT25448,MT26418, MT26428,MT26438,MT26448,MT26468,MT26478, MT27500,MT27510,MT27520,MT27521,MT27530, MT27531,MT27540,MT27541,MT27550,MT27551, MT27560,MT27561	mlx4_en
	MT27600, MT27700, MT27710, MT27800, MT28800, MT28908, MT416842	mlx5_core
Microcomputer	(2031)	sc92031
Microsoft	MN-130, MN-120	tulip
MYRICOM	Myri-10G	myri10ge
MYSON	MTD-8xx,EP-320X-S	fealnx
National Semiconductor	Aculab E1/T1 PMXc,DP83815	natsemi
	DP83065	cassini
	DP83820	ns83820
Netgear	GA620,GA630	acenic
NetXen	NX3031,NXB-10GCX4,NXB-10GXSR, NXB-4GCU,XG Mgmt	netxen_nic
Northern Telecom	RTL81xx	8139too
NVIDIA	CK804,CK8S,MCP04,MCP2A,MCP51,MCP55,MCP61, MCP65,MCP67,MCP73,MCP77,MCP79,MCP89, nForce,nForce2,nForce3	forcedeth
Olicom	OC-2183,OC-2185,OC-2325,OC-2326	tlan
Oracle/SUN	Cassini	cassini
	GEM	sungem
	Happy Meal	sunhme
	Multithreaded	niu
Packet Engines	GNIC-II	hamachi
Peppercon	ROL/F-100	8139too
Planex	-	tulip
	RTL81xx	8139too
QLogic	10GbE Converged	qlge
	cLOM8214, ISP8324 1/10GbE	qlcnic
	ISP4022-based,ISP4032-based	qla3xxx
	FastLinQ QL45000	qede

Qualcomm Atheros	Attansic L1	atl1
	Attansic L2	atl2
	AR8131,AR8132,AR8151,AR8152	atl1c
	AR8121,AR8113,AR8114	atl1e
	AR8161,AR8162,QCA8171,QCA8172,E2200, E2400	alx
RDC Semiconductor	R6040	r6040
Realtek	RTL-8129,RTL-8139/8139C/8139C+	8139too
	RTL-8101E,RTL-8102E,RTL-8110SC,RTL-8111, RTL-8129,RTL-8168B,RTL-8169,,RTL-8169SC	r8169
	RTL-8139/8139C/8139C+	8139cp
Rohm	-	pch_gbe
Sega	-	8139too
Silicon Graphics	AceNIC	acenic
SiS	190,191	sis190
	SiS7016,SiS900	sis900
Solarflare	[64] SFC4000,SFC9020,SFL9021 SFC9120, SFC9140, SFC9220, SFC9250	sfc
SMC	83c170,83c175	epic100
STMicroelectronics	21x4x DEC-Tulip	tulip
Sundance	IP100A,ST201	sundance
	TC902x	dl2k
SysKonnect|	SK-9871,SK-9872	skge
	SK-9Dxx,SK-9Mxx	tg3
	SK-9E21D,SK-9S21, SK-9E21M	sky2
TDK	RTL81xx	tulip
Tehuti Networks	10-Giga TOE	tehuti
Trident	4DWave DX	pcnet32
TTTech AG	TTP-Monitoring Card V2.0	8139cp
U.S. Robotics	USR997902	r8169
VIA	VT6102,VT6105,VT6106S,VT6105M,VT86C100A	via-rhine
	VT6120,VT6121,VT6122	via-velocity
Winbond	W89C840	winbond-840

Supported Network Interface (Wi-Fi PCI/PCIe)

* Basically, the model number of the chip is used instead of the product name. To confirm, you need to find out the chip model number of the interface.
* The table shows the corresponding product notation for each driver. We have not confirmed the operation.
* Even the ones listed in the table may not work due to firmware version, driver defect, hardware environment, version difference, etc.
* Please be sure to check the operation before purchasing.
*Yellow green is added after Ver4.6.x. Gray is obsolete after Ver4.6.x.
*In a 32-bit execution, the contents has not changed after Ver4.6.x.

64bit execution		
Manufacturer	Product name	Driver used
3com	AR5212	ath5k
	3CRWE154G72 [Office Connect Wireless LAN Adapter]	p54pci
Belkin	F5D6001, F5D6020, F5D7000, F5D7010	rtl818x_pci
Broadcom	BCM4311, BCM4313, BCM4331, BCM4352, BCM4360, BCM43131, BCM43217, BCM43224, BCM43225, BCM43227, BCM43228, BCM43142 Wireless 1704	bcma
	BCM4350, BCM4356, BCM4358, BCM43142, BCM43567, BCM43570, BCM43602, BCM4355, BCM4359, BCM4364, BCM4377b, BCM4378	brcmfmac
D-Link	DWL-510, DWL-610	rtl818x_pci
Intel	Advanced-N 6200, Advanced-N 6205, Advanced-N + WiMAX 6250, Advanced-N 6230, Advanced-N 6235, Wireless-N 100, Wireless-N 105, Wireless-N 130, Wireless-N 135, Wireless-N 1000, Wireless-N 1030, Wireless-N 2200, Wireless-N 2230, Wireless-N + WiMAX 6150, Wireless 3160, Wireless 3165, Wireless 5350, Wireless 7260, Wireless 7265, Wireless 8260, Wireless-AC 3165, Wireless 5100, Wireless 8260, Wireless 8265, Wireless 8275, Wireless-AC	iwlwifi

	9260, Wireless-AC 9560, Ultimate-N 6300, WiFi Link 5100, WiFi Link 5150, WiFi Link 5300, AX200, AX210, AX211, AX41, Alder Lake-P PCH CNVi	
	Wireless 3945ABG	iwl3945
	Wireless 4965	iwl4965
Marvell	88W8363, 88W8687, 88W8366, 88W8764,	rmwl8k
	88W8897,	mwifiex_pcie
MEDIATEK	MT7630e, MT7662E	mt76x2e
	MT7615E, MT7915E, MT7921, MT7922	mt7915e
Qualcomm Atheros	AR5210, AR5211, AR5212/5213/2414, AR2413/AR2414, AR5413/AR5414, AR242x / AR542x, AR2417,	ath5h
	AR2427, AR5416, AR5418, AR9160, AR9227, AR922X, AR9285, AR9287, AR928X , AR93xx, AR9462, AR9485, AR9565, AR958x, QCA9565, AW-NB037H, AW-NE186H, EM306, WLM200NX, T77H047.31, N1102, N1103, Wireless 1601, Wireless 1802	ath9k
	QCA6164, QCA6174, QCA9377, QCA986x, QCA9887, QCA988x, QCA9980,QCA9990,	ath10k_pci
	WIL6210	wil6210
Ralink	RT61, RT2561, RT2600	rt61pci
	RT2760, RT2800, RT2890, RT3060, RT3062, RT3090, RT3091, RT3092, RT3290, RT3592, RT5360, RT5362, RT5390, RT5392,	rt2800pci
	RT2400 / RT2460	rt2400pci
	RT2500	rt2500pci
Realtek	RTL8191SEvA, RTL8191SEvB, RTL8192SE, RTL8192E,	rtl8192se
	RTL8188CE, RTL8191CE, RTL8192CE,	rtl8192ce
	RTL8188EE, RTL8192EE,	rtl8188ee
	RTL8192DE	rtl8192de
	RTL8723AE	rtl8723ae
	RTL8812AE, RTL8821AE	rtl8821ae
	RTL8723BE	rtl8723be
	RTL8180L, RTL-8185, RTL8187SE	rtl818x_pci
	RTL8821CE	rtw88_8821ce
	RTL8822CE	rtw88_8822ce
	RTL8723DE	rtw88_8723de
	RTL8852AE	rtw89_8852ae
Ubiquiti Networks	(11ac)	ath10k_pci
Wilocity	Wil6200	wil6210

32bit execution		
Manufacturer	Product name	Driver used
3com	AR5212	ath5k
	3CRWE154G72 [Office Connect Wireless LAN Adapter]	p54pci
Broadcom	BCM4311, BCM4313, BCM4331, BCM4352, BCM4360, BCM43131, BCM43217, BCM43224, BCM43225, BCM43227, BCM43228, BCM43142 Wireless 1704	bcma
	BCM4350, BCM4356, BCM4358, BCM43142, BCM43567, BCM43570, BCM43602,	brcmfmac
Intel	Advanced-N 6200, Advanced-N 6205, Advanced-N + WiMAX 6250, Advanced-N 6230, Advanced-N 6235, Wireless-N 100, Wireless-N 105, Wireless-N 130, Wireless-N 135, Wireless-N 1000, Wireless-N 1030, Wireless-N 2200, Wireless-N 2230, Wireless-N + WiMAX 6150, Wireless 3160, Wireless 3165, Wireless 5350, Wireless 7260, Wireless 7265, Wireless 8260, Wireless-AC 3165, Wireless 5100, Wireless 8260, Wireless 8265, Wireless 8275, Wireless-AC 9260, Wireless-AC 9560, Ultimate-N 6300, WiFi Link 5100, WiFi Link 5150, WiFi Link 5300,	iwlwifi
	Wireless 3945ABG	iwl3945
	Wireless 4965	iwl4965
Marvell	88W8363, 88W8687, 88W8366, 88W8764,	rmwl8k
	88W8897,	mwifiex_pcie

MEDIATEK	MT7630e, MT7662E	mt76x2e
Qualcomm Atheros	AR5210, AR5211, AR5212/5213/2414, AR2413/AR2414, AR5413/AR5414, AR242x / AR542x, AR2417,	ath5h
	AR2427, AR5416, AR5418, AR9160, AR9227, AR922X, AR9285, AR9287, AR928X , AR93xx, AR9462, AR9485, AR9565, AR958x, QCA9565, AW-NB037H, AW-NE186H, EM306, WLM200NX, T77H047.31, N1102, N1103, Wireless 1601, Wireless 1802	ath9k
	QCA6164, QCA6174, QCA9377, QCA986x, QCA9887, QCA988x, QCA9980,QCA9990,	ath10k_pci
	WIL6210	wil6210
Ralink	RT61, RT2561, RT2600	rt61pci
	RT2760, RT2800, RT2890, RT3060, RT3062, RT3090, RT3091, RT3092, RT3290, RT3592, RT5360, RT5362, RT5390, RT5392,	rt2800pci
	RT2400 / RT2460	rt2400pci
	RT2500	rt2500pci
Realtek	RTL8191SEvA, RTL8191SEvB, RTL8192SE, RTL8192E,	rtl8192se
	RTL8188CE, RTL8191CE, RTL8192CE,	rtl8192ce
	RTL8188EE, RTL8192EE,	rtl8188ee
	RTL8192DE	rtl8192de
	RTL8723AE	rtl8723ae
	RTL8812AE, RTL8821AE	rtl8821ae
	RTL8723BE	rtl8723be
Ubiquiti Networks	(11ac)	ath10k_pci
Wilocity	Wil6200	wil6210

Supported Network Interface (USB connected, ethernet,Wi-Fi)

* Basically, the model number of the chip is used instead of the product name. To confirm, you need to find out the chip model number of the interface.
* The table shows the corresponding product notation for each driver. We have not confirmed the operation.
* Even the ones listed in the table may not work due to firmware version, driver defect, hardware environment, version difference, etc.
* Please be sure to check the operation before purchasing.
*Yellow green is added after Ver4.6.x. Gray is obsolete after Ver4.6.x.
*In a 32-bit execution, the contents has not changed after Ver4.6.x.

64bit execution			
Manufacturer	Product name	Wi-Fi	Driver used
3com	3C19250, HomeConnect 3C460		kaweth
	3C460B		pegasus
	3CRWE254G72	*	p54usb
	3CRUSB10075	*	zd1211rw
AboCom Systems	XX1, XX2, XX4, XX5, XX6, XX7, XX9, DU-E10, DU-E100, USB 1.1 10/100M		pegasus
	Mini Wireless LAN USB2.0, Wireless LAN USB2.0	*	rt2800usb
	DU-E10		kaweth
	RTL8151		rtl8150
	UF200 Ethernet		asix
	Prolink Wireless-N Nano	*	rtl8192cu
	HWU54DM, RT2573, WUG2700	*	rt73usb
	-	*	mt76x0u
	-	*	ath9k_htc
	Wireless	*	rtl8xxxu
Accton Technology	SpeedStream, CPWUE001,		pegasus
	Arcadyan, SMCWUSBS-N, SMCWUSBS-N2, SMCWUSBS-N3, Speedport W 102 Stick	*	rt2800usb
	Arcadyan WN7512	*	carl9170
	T-Sinus 154data, Siemens S30853-S1016-R107, Zoom 4410	*	p54usb
	SMCWUSB-G, ZD1211B, Arcadyan WN4501, WUS-201	*	zd1211rw
	-	*	rt2800usb
	SMCWUSBT-G2	*	ar5523
Acer	EP-1427X-2		asix
Actiontec Electronics	802AIN	*	ath9k_htc
	802AIN	*	carl9170
ADS Technologies	|UBS-10BT		kaweth

ADMtek	AN986A, AN986, ADM8511, AN8513, AN8515		pegasus
AirTies Wireless Networks	Air2210, Air2310	*	rt2800usb
Allied Telesys International	AT-USB100		pegasus
	Ethernet		ax88179_178a
	Ethernet		lan78xx
A-Max Technology	Wireless 802.11g 54Mbps	*	rtl8187
Amigo Technology	802.11n Wireless USB Card	*	rt2800usb
AMIT	WL532U, CG-WLUSB2GNR, CG-WLUSB10	*	rt2800usb
	CG-WLUSB2GO	*	rt73usb
Apple	Ethernet Adapter[A1277]		asix
ASIX Electronics	AX88178, AX88179, AX88772, AX88772A, AX88772B		asix
	Ethernet		aqc111
	Ethernet		cdc_ether
Askey Computer	RT2573	*	rt73usb
	802.11n Wireless LAN	*	rt2800usb
	SMCWUSBT-G, AR5523	*	ar5523
	Voyager 1055	*	rndis_wlan
	Wireless	*	r8712u
ASUSTek Computer	WL-167G v2, RT2573	*	rt73usb
	USB-N11, USB-N13, USB-N53,	*	rt2800usb
	USB-N13, N10 Nano	*	rtl8192cu
	WL-167G	*	rt2500usb
	WL-159g, A9T	*	zd1211rw
	AC51, USB-AC50	*	mt76x0u
	USB-N10	*	mt7601u
	USB-AC55	*	mt76x2u
	WL169gE	*	rndis_wlan
	USB-N10, WL-167G	*	r8712u
	Wireless	*	rtw88_8822bu
	Realtek 8188EUS	*	rtl8xxxu
ATEN International	10Mbps Ethernet		kaweth
	UC-110T 100Mbps Ethernet		pegasus
	DSB-650 10Mbps Ethernet		kaweth
Atheros Communications	AR5523	*	ar5523
AVM GmbH	Fritz!WLAN /2.4	*	carl9170
	Fritz!WLAN N v2	*	ath9k_htc
	FRITZ WLAN N v2	*	rt2800usb
	-	*	mt76x0u
	-	*	mt76x2u
Belkin Components	F5D5050		pegasus
	F9L1004, F7D1102, F7D2102, IWL 2000	*	rtl8192cu
	F5D5055 Gigabit		asix
	F5D7050 v1000/v2000/v3000, F5D9050,	*	rt73usb
	F5D7050 v5000	*	rtl8187
	|F5D8053, F5D8055, F7D1101, F9L1103	*	rt2800usb
	F5D7051	*	rt2500usb
	-		ax88179_178a
	F5D7050	*	zd1211rw
	F5D8053, F7D210, F7D1101	*	r8712u
Billionton Systems	USB-100N, USBLP-100, USBEL-100, USBE-100		pegasus
	USB2AR		asix
BUFFALO	LUA-TX, LUA2-TX,		pegasus
	LUA-KTX,		rtl8150
	LUA-U2-KTX, LUA-U2-GT,		asix
	WLI-U2-SG54HP, WLI-U2-G54HP,	*	rt73usb
	WLI-UC-G300N, WLI-UC-AG300N, WLI-UC-G300HP, WLP-UC-AG300、WLI-UC-GNHP, WLI-UC-GN, WLI-UC-G301N, WLI-UC-GNM, WLI-UC-GNM2, WLI-UC-G450	*	rt2800usb
	Sony UWA-BR100	*	ath9k_htc
	WLI2-USB2-G54	*	p54usb
	WLI-U2-KG54, WLI-U2-KG54-AI, WLI-U2-KG54-YB, WLI-U2-KG54-BB, intendo Wi-Fi	*	rt2500usb
	WLI-U2-KG54L	*	zd1211rw
	WLI-USB-G54, WLI-U2-KG125S	*	rndis_wlan
Broadcom	BCM43236	*	brcmfmac
	EM4045	*	rndis_wlan
CACE Technologies	AirPcap NX	*	carl9170
	GN-BR402W		pegasus

Chu Yuen Enterprise	GN-WB01GS, GN-WI05GS	*	rt73usb
	GN-WB30N, GN-WB31N, GN-WB32L	*	rt2800usb
	GN-54G, GN-WBKG	*	rt2500usb
CNet Technology	CWD-854 [RT2573], CWD-854 rev F	*	rt73usb
	CWD-854 Wireless 802.11g 54Mbps	*	rtl8187
Compaq Computer	iPAQ Networking 10/100 Ethernet		pegasus
Computer Access	NetMate, NetMate2		catc
Conexant Systems	SoftGate 802.11 Adapter	*	p54usb
Corega	Ether USB-T		kaweth
	FEther USB-TX, FEther USB-TXS		pegasus
	FEther USB2-TX		asix
	CG-WLUSB2GPX	*	rt73usb
	CG-WLUSB2GNL, CG-WLUSB300AGN, CG-WLUSB300GNS, CG-WLUSB300GNM	*	rt2800usb
	FEther USB-TXC		dm9601
	CG-WLUSB2GT, CG-WLUSB2GTST	*	p54usb
	CG-WLUSBNM, CG-WLUSB300NM	*	r8712u
CyberTAN Technology	Gigaset USB Adapter 300		rt2800usb
Cypress Semiconductor	-	*	brcmfmac
Davicom Semiconductor	ZT6688, ADM8515, DM9000E, DM9601	*	dm9601
Dell	WLA3310, TrueMobile 1300, Wireless 1450	*	p54usb
D-Link System	DWA-160, DWA-130	*	carl9170
	DWA-126	*	ath9k_htc
	DWL-G122, WUA-1340, DWA-111, DWA-110	*	rt73usb
	EH103, DUB-E100, DUB-E100		asix
	DWA-110, DWA-123, DWA-125, DWA-127, DWA-140, DWA-160, DWL-G122,	*	rt2800usb
	DWA-121, DWA-133, DWA-135	*	rtl8192cu
	DSB-650C		kaweth
	DSB-650, DSB-650TX		pegasus
	WUA-2340, DWL-AG132, DWL-G132, DWL-AG122	*	ar5523
	DWA-125, DWA-123	*	rtl8xxxu
	DWL-G120, DWL-G122,	*	p54usb
	DWL-G122	*	rt2500usb
	-	*	mt76x0u
	-	*	mt7601u
	DWA-130, DWA-131 ,DWL-G122	*	r8712u
	Wireless	*	rtw88_8822bu
Edimax Technology	EW-7711UTn, EW-7717UN, EW-7718UN, EW-7722UTn	*	rt2800usb
	EW-7811Un	*	rtl8192cu
	-	*	mt7601u
	-	*	mt76x0u
	Wireless	*	r8712u
	EW-7611ULB	*	rtl8xxxu
	Wireless	*	rtw88_8822bu
Efficient Networks	Siemens SpeedStream 100MBps Ethernet		pegasus
Elecom	LD-USB/TX, LD-USB/TX, LD-USBL/TX, LD-USB20		pegasus
	Wireless	*	rtl8xxxu
ELCON Systemtechnik	Goldpfeil P-LAN		pegasus
ELSA AG	Micolink USB2Ethernet		pegasus
Encore Electronics	ENUWI-N3	*	rt2800usb
EndPoints	101 Ethernet		kaweth
Entrega	E45 Ethernet		kaweth
Fujitsu Siemens Computers	Connect2Air E-5400	*	p54usb
Gemtek	WUBR-177G	*	rt73usb
	WUBR-208N	*	rt2800usb
Good Way Technology	GWUSB2E		asix
	RT2573	*	rt73usb
Global Sun Technology	AR5523	*	ar5523
	Cohiba 802.11g Wireless Mini adapter	*	p54usb
Guillemot	HWGUSB2-54-LB, HWGUSB2-54V2-AP	*	rt73usb
	Hercules HWNUp-150	*	rtl8192cu
	HWNUm-300, HWGUm-54	*	r8712u
Hawking Technologies	HWUN1, HWUN2, HWUN3, HAWNU1	*	rt2800usb
	UF100		pegasus
	HWDN2	*	r8712u
	Wireless	*	rtw88_8822bu

HP	Ethernet HN210E		pegasus
Huawei-3Com	Aolynk WUB320g	*	rt73usb
IMC Networks	802.11 n/g/b Wireless	*	rt2800usb
	-	*	mt7601u
	Wireless	*	r8712u
Intellon	MicroLink dLAN		int51x1
I-O Data	ET/TX Ethernet, ET/TX-S Ethernet		pegasus
	ETG-US2		asix
	WNGDNUS2	*	carl9170
	WHG-AGDN/US, WN-GDN/US3, WN-G150U, WN-G300U	*	rt2800usb
	USB ETT		kaweth
	-	*	rtl8xxxu
	-	*	mt76x0u
Jaton	Ethernet		kaweth
K2L GmbH	Ethernet		smsc95xx
Kawasaki LSI	KL5KUSB101B,		kaweth
Kingston Technology	Ethernet		kaweth
	KNU101		pegasus
Kontron	DM9601		dm9601
Lenovo	AX88179		ax88179_178a
	U2L 100P-Y1		asix
	Ethernet		r8152
	Ethernet		cdc_ether
	Ethernet		r8153_ecm
Linksys	USB10TX, USB100TX,		pegasus
	USB200M, USB1000		asix
	Gigabit Ethernet		r8152
	WUSB54GC, WUSB54GR, WUSB200	*	rt73usb
	AE1000, AM10, WUSB100 v1/v2, WUSB600N v1/v2, WUSB54GC v3, AE3000	*	rt2800usb
	WUSB54GC v2	*	rtl8187
	WUSB54G, WUSB54AG	*	p54usb
	WUSB54G, WUSB54GP, HU200TS,	*	rt2500usb
	WUSBF54G,	*	zd1211rw
	AE1200	*	brcmfmac
	AE6000	*	mt76x0u
	WUSB6100M	*	ath10k_usb
	Wireless	*	rtw88_8822cu
LG Electronics	Ethernet		mt7663u
Logitec	Realtek RTL8187	*	rtl8187
	LAN-GTJ/U2A		asix
	LAN-WN22/U2, LAN-WN12/U2, LAN-W150/U2M, LAN-W300N/U2, LAN-W150N/U2, LAN-W300AN/U2	*	rt2800usb
	-	*	rtl8xxxu
MediaTek	-	*	mt7601u
	-	*	mt76x0u
	-	*	mt76x2u
	Wireless	*	mt7663u
	Wireless	*	mt7921u
Mobility	Ethernet		kaweth
	EasiDock Ethernet		pegasus
Microsoft	10/100 USB NIC		pegasus
	RTL8153 GigE [Surface Dock Ethernet], RTL8153B		r8152
	RTL8153 GigE [Surface Dock Ethernet]		cdc_ether
	MN-710	*	p54usb
	Wireless XBox Controller Dongle	*	mt76x2u
Micro Star International	RT2573	*	rt73usb
	1T1R Mini Card	*	rt2800usb
	IEEE 802.11g Wireless	*	p54usb
	RT2570, MSI-6861	*	rt2500usb
MosChip Semiconductor	MCS7730, MCS7830, MCS7832		mcs7830
NEC	Aterm WL300NU-G, WL300NU-AG	*	carl9170
	Aterm PA-WL54GU	*	zd1211rw
	WL300NU-GS	*	r8712u
	EA101,		kaweth
	FA101		pegasus
	FA120		asix

NetGear	WG111v2	*	rtl8187
	WN111(v2), WNDA3100v1, WNA1000	*	carl9170
	WNDA3200, WNA1100	*	ath9k_htc
	WNA3100M(v1), WNA1000M, WNA1000Mv2, N300MA, N150MA	*	rtl8192cu
	WG111, WG111	*	p54usb
	WG111U, WPN111, WG111T	*	ar5523
	WNDA4100	*	rt2800usb
Netopia	Motorola 802.11n	*	rt2800usb
NovaTech	RT2573	*	rt73usb
	NV-902W	*	rt2500usb
	Wireless	*	r8712u
Omnidirectional Control Technology	USB TO Ethernet, OCT To Fast Ethernet		pegasus
OQO	model 01+ Ethernet		asix
	model 01 Ethernet		rtl8150
Ovislink	AirLive WN-360USB, AirLive WN-200USB	*	rt2800usb
	AirLive WL-1600USB	*	rtl8187
	AirLive X	*	carl9170
Panasonic	DY-WL10	*	rt2800usb
	N5HBZ0000055	*	ath9k_htc
PEGATRON	RT2770, RT2720, RT3070	*	rt2800usb
Peracom	Enet, Enet2, @Home Networks		kaweth
Philips	|Wireless Network Adapter	*	rt73usb
	802.11n Wireless Adapter	*	rt2800usb
	PTA01 Wireless Adapter	*	ath9k_htc
	Wireless Adapter 11g	*	p54usb
	SNU5600, SNU5630NS/05	*	zd1211rw
Planex Communications	GU-1000T		asix
	GWUS300	*	carl9170
	GW-US54HP, GW-US54Mini2	*	rt73usb
	GW-US300MiniS, GW-USMini2N, GW-USMicro300, GW-US300MiniW	*	rt2800usb
	GW-USNano2, GW-USEco300, GW-USValue-EZ	*	rtl8192cu
	GW-US54ZGL, GW-US54GZ, GW-US54Mini	*	zd1211rw
	-	*	mt76x0u
	-	*	rtl8xxxu
	GW-USSuper300, GW-USNano, GW-USMicroN2W, GW-USHyper300	*	r8712u
	GW-USMicroN	*	rt2800usb
Portsmith	Express Ethernet		kaweth
Qcom	RT2573	*	rt73usb
	RTL8187	*	rtl8187
QNAP System	Enet, Enet2, @Home Networks		kaweth
	Ethernet		cdc_ether
	Ethernet		aqc111
Qualcomm Atheros Communications	Thomson TG121N, TL-WN822N v1, TP-Link TL-WN821N v2, 3Com 3CRUSBN275, AR9170	*	carl9170
	TL-WN422G v2, TP-Link TL-WN322G v3, TP-Link TL-WN821N v3, TL-WN822N v2, AR9271, Ubiquiti WiFiStation, Ubiquiti WiFiStationEXT	*	ath9k_htc
	AR5523	*	ar5523
	-	*	ath6kl_usb
Quanta Microsystems	802.11n Wireless LAN Card	*	rt2800usb
Ralink Technology	RT2070, RT2770, RT2870, RT3070, RT3071, RT3072, RT3370, RT3572, RT3573, RT5370, RT5372, RT5572, Conceptronic C300RU v1/v2, Airlink101 AWLL6080, DrayTek Vigor N61, Airlink101 AWLL6070, Keebox W150NU	*	rt2800usb
	RT2501, RT2573, RT2601, RT2671, RT2501, Conceptronic C54RU v3	*	rt73usb
	RT2500USB, RT2570	*	rt2500usb
	MT7601U	*	mt7601u
	MT7610U	*	mt76x0u
	Wireless	*	r8712u
	RTL8150		rtl8150
	RTL8152, RTL8153		r8152
	RTL8188CUS, RTL8192CU, RTL8188RU	*	rtl8192cu

Realtek Semiconductor	RTL8187, RTL8187B	*	rtl8187
	RTL8723AU, RTL8188ETV, RTL8188EUS, RTL8188FTV	*	rtl8xxxu
	Wireless	*	rtw88_8821cu
	RTL88x2bu	*	rtw88_8822bu
	Wireless	*	rtw88_8822cu
	Wireless	*	rtw88_8723du
	RTL8188SU, RTL8191SU, RTL8192SU, RTL8191SU	*	r8712u
Sagem	XG-76NA, XG-760NA	*	zd1211rw
	Wi-Fi 11g	*	rt2500usb
Samsung	WIS09ABGN LinkStick	*	rt2800usb
Senao	EUB600v1, WUA-0605, WUA-0615, EnGenius, EUB9706, EUB9801	*	rt2800usb
	EUB-3701	*	rt73usb
	NUB-350	*	p54usb
	NUB-8301	*	zd1211rw
	RTL8188S	*	r8712u
Shark Multimedia	Pocket Ethernet		kaweth
SohoWare	NUB100 Ethernet		pegasus
Silicom	U2E, Psion Gold Port Ethernet		kaweth
Sitecom Europe B.V.	WL-168	*	rtl8187
	WL-182, WL-188, WL-301, WL-302, WL-315, WL-321, WL-323, WL-324, WL-329, WL-343, WL-344, WL-345, WL-349v1, WL-349v4, WL-352v1, WL-609, WLA-4000, WLA-5000, WLA-5100,	*	rt2800usb
	LN-028, LN-031,		asix
	AX88179		ax88179_178a
	WL-113, WL-172	*	rt73usb
	WL-603, WL-113 , WL-117	*	zd1211rw
	-	*	mt76x0u
	WL-353, WL-356, WL-349v3, WL-352, WLA-2000	*	r8712u
	Wireless	*	rtl8xxxu
smartBridges	smartNIC		catc
	smartNIC 2		pegasus
Sphairon Access Systems	Turbolink UB801RE Wireless	*	rtl8187
	Turbolink UB801R WLAN	*	rt2500usb
Standard Microsystems	LAN7500		smsc75xx
	LAN9512, LAN9514, SMSC9512, SMSC9514		smsc95xx
	2202		kaweth
	2202, EZ Connect		pegasus
	LAN78xx		lan78xx
	SMC2862W-G	*	p54usb
	SMC2862W-G	*	rt2500usb
Surecom Technology	EP-9001-g	*	rtl8187
	RT2573	*	rt73usb
Sweex	LW153, LW313	*	rt2800usb
	LW154	*	r8712u
Tekram Technology	QuickWLAN,	*	zd1211rw
TMT Technology	Ethernet		kaweth
Toshiba	WLM-10U1	*	rt2800usb
	WLM-20U2, GN-1080	*	ath9k_htc
	AX88179		ax88179_178a
TP-Link	Archer T1U, Archer T2UHP	*	mt76x0u
	TL-WN821N, TL-WN822N, TL-WN823N, TL-WN722N v2/v3	*	rtl8xxxu
	Archer T3U, Archer T4U ver.3	*	rtw88_8822bu
TRENDnet	SMC SMCWUSB-N, TEW-645UB	*	rt2800usb
	TEW-648UBM	*	rtl8192cu
	TEW-444UB, ALL0283	*	ar5523
	TEW-429UB, ALL0298, TEW-509UB	*	zd1211rw
	TEW-646UBH	*	r8712u
	Wireless	*	rtw88_8822bu
	Ethernet		aqc111
Trust International	NW-3100	*	zd1211rw
U.S. Robotics	U5	*	p54usb
	USR5423	*	zd1211rw
	USR5420,Wireless MAXg	*	rndis_wlan
Victor	MP-PRX1		asix
	AR9170+AR9104 802.11abgn	*	carl9170

Wistron NeWeb	UR054g	*	p54usb
	UR055G	*	zd1211rw
	AR5523	*	ar5523
Xircom	Ethernet		kaweth
ZyDAS	ZD1221	*	carl9170
	ZD1211	*	zd1211rw
ZyXEL	G-210H	*	rt73usb
	NWD-210N, NWD211AN, NWD-270N, NWD2105, N220	*	rt2800usb
	NWD271N	*	carl9170
	NWD2205	*	rtl8192cu
	G-200, G-202, G-220, G-220F, AG-225H, M-202,	*	zd1211rw
	NWD6505	*	mt76x0u
	Ethernet		dm9601
Z-Com	802.11b/g Wireless	*	rt73usb
	|802.11b/g/n Wireless	*	rt2800usb
	UB81, UB82, Sphairon Homelink 1202	*	carl9170
	XG-300, XG-703A, XG-705A	*	p54usb
	AR5523	*	ar5523

32bit execution

Manufacturer	Product name	Wi-Fi	Driver used
3com	3C19250, HomeConnect 3C460		kaweth
	3C460B		pegasus
	3CRWE254G72	*	p54usb
	3CRUSB10075	*	zd1211rw
AboCom Systems	XX1, XX2, XX4, XX5, XX6, XX7, XX9, DU-E10, DU-E100, USB 1.1 10/100M		pegasus
	Mini Wireless LAN USB2.0, Wireless LAN USB2.0	*	rt2800usb
	DU-E10		kaweth
	RTL8151		rtl8150
	UF200 Ethernet		asix
	Prolink Wireless-N Nano	*	rtl8192cu
	HWU54DM, RT2573, WUG2700	*	rt73usb
	-	*	mt76x0u
	-	*	ath9k_htc
Accton Technology	SpeedStream, CPWUE001,		pegasus
	Arcadyan, SMCWUSBS-N, SMCWUSBS-N2, SMCWUSBS-N3, Speedport W 102 Stick	*	rt2800usb
	Arcadyan WN7512	*	carl9170
	T-Sinus 154data, Siemens S30853-S1016-R107, Zoom 4410	*	p54usb
	SMCWUSB-G, ZD1211B, Arcadyan WN4501, WUS-201	*	zd1211rw
	-	*	rt2800usb
Acer	EP-1427X-2		asix
Actiontec Electronics	802AIN	*	ath9k_htc
	802AIN	*	carl9170
ADS Technologies	|UBS-10BT		kaweth
ADMtek	AN986A, AN986, ADM8511, AN8513, AN8515		pegasus
AirTies Wireless Networks	Air2210, Air2310	*	rt2800usb
Allied Telesyn International	AT-USB100		pegasus
A-Max Technology	Wireless 802.11g 54Mbps	*	rtl8187
Amigo Technology	802.11n Wireless USB Card	*	rt2800usb
AMIT	WL532U, CG-WLUSB2GNR, CG-WLUSB10	*	rt2800usb
	CG-WLUSB2GO	*	rt73usb
Apple	Ethernet Adapter[A1277]		asix
ASIX Electronics	AX88178, AX88179, AX88772, AX88772A, AX88772B		asix
Askey Computer	RT2573	*	rt73usb
	802.11n Wireless LAN	*	rt2800usb
	SMCWUSBT-G, AR5523	*	ar5523
ASUSTek Computer	WL-167G v2, RT2573	*	rt73usb
	USB-N11, USB-N13, USB-N53,	*	rt2800usb
	USB-N13, N10 Nano	*	rtl8192cu
	WL-167G	*	rt2500usb
	WL-159g, A9T	*	zd1211rw
	AC51, USB-AC50	*	mt76x0u
	USB-N10	*	mt7601u
	USB-AC55	*	mt76x2u

ATEN International	10Mbps Ethernet		kaweth
	UC-110T 100Mbps Ethernet		pegasus
	DSB-650 10Mbps Ethernet		kaweth
Atheros Communications	AR5523	*	ar5523
AVM GmbH	Fritz!WLAN /2.4	*	carl9170
	Fritz!WLAN N v2	*	ath9k_htc
	FRITZ WLAN N v2	*	rt2800usb
	-	*	mt76x0u
	-	*	mt76x2u
Belkin Components	F5D5050		pegasus
	F9L1004, F7D1102, F7D2102, IWL 2000	*	rtl8192cu
	F5D5055 Gigabit		asix
	F5D7050 v1000/v2000/v3000, F5D9050,	*	rt73usb
	F5D7050 v5000	*	rtl8187
	|F5D8053, F5D8055, F7D1101, F9L1103	*	rt2800usb
	F5D7051	*	rt2500usb
	-		ax88179_178a
	F5D7050	*	zd1211rw
Billionton Systems	USB-100N, USBLP-100, USBEL-100, USBE-100		pegasus
	USB2AR		asix
BUFFALO	LUA-TX, LUA2-TX,		pegasus
	LUA-KTX,		rtl8150
	LUA-U2-KTX, LUA-U2-GT,		asix
	WLI-U2-SG54HP, WLI-U2-G54HP,	*	rt73usb
	WLI-UC-G300N, WLI-UC-AG300N, WLI-UC-G300HP, WLP-UC-AG300, AWLI-UC-GNHP, WLI-UC-GN, WLI-UC-G301N, WLI-UC-GNM, WLI-UC-GNM2, WLI-UC-G450	*	rt2800usb
	Sony UWA-BR100	*	ath9k_htc
	WLI2-USB2-G54	*	p54usb
	WLI-U2-KG54, WLI-U2-KG54-AI, WLI-U2-KG54-YB, WLI-U2-KG54-BB, intendo Wi-Fi	*	rt2500usb
	WLI-U2-KG54L	*	zd1211rw
Broadcom	BCM43236	*	brcmfmac
CACE Technologies	AirPcap NX	*	carl9170
Chu Yuen Enterprise	GN-BR402W		pegasus
	GN-WB01GS, GN-WI05GS	*	rt73usb
	GN-WB30N, GN-WB31N, GN-WB32L	*	rt2800usb
	GN-54G, GN-WBKG	*	rt2500usb
CNet Technology	CWD-854 [RT2573], CWD-854 rev F	*	rt73usb
	CWD-854 Wireless 802.11g 54Mbps	*	rtl8187
Compaq Computer	iPAQ Networking 10/100 Ethernet		pegasus
Computer Access	NetMate, NetMate2		catc
Conexant Systems	SoftGate 802.11 Adapter	*	p54usb
Corega	Ether USB-T		kaweth
	FEther USB-TX, FEther USB-TXS		pegasus
	FEther USB2-TX		asix
	CG-WLUSB2GPX	*	rt73usb
	CG-WLUSB2GNL, CG-WLUSB300AGN, CG-WLUSB300GNS, CG-WLUSB300GNM	*	rt2800usb
	FEther USB-TXC		dm9601
	CG-WLUSB2GT, CG-WLUSB2GTST	*	p54usb
CyberTAN Technology	Gigaset USB Adapter 300		rt2800usb
Cypress Semiconductor	-	*	brcmfmac
Davicom Semiconductor	ZT6688, ADM8515, DM9000E, DM9601	*	dm9601
Dell	WLA3310, TrueMobile 1300, Wireless 1450	*	p54usb
D-Link System	DWA-160, DWA-130	*	carl9170
	DWA-126	*	ath9k_htc
	DWL-G122, WUA-1340, DWA-111, DWA-110	*	rt73usb
	EH103, DUB-E100, DUB-E100		asix
	DWA-110, DWA-123, DWA-125, DWA-127, DWA-140, DWA-160, DWL-G122,	*	rt2800usb
	DWA-121, DWA-133, DWA-135	*	rtl8192cu
	DSB-650C		kaweth
	DSB-650, DSB-650TX		pegasus
	WUA-2340, DWL-AG132, DWL-G132, DWL-AG122	*	ar5523
	-	*	rtl8xxxu

	DWL-G120, DWL-G122,	*	p54usb
	DWL-G122	*	rt2500usb
	-	*	mt76x0u
	-	*	mt7601u
Edimax Technology	EW-7711UTn, EW-7717UN, EW-7718UN, EW-7722UTn	*	rt2800usb
	EW-7811Un	*	rtl8192cu
	-	*	mt7601u
	-	*	mt76x0u
Efficient Networks	Siemens SpeedStream 100MBps Ethernet		pegasus
Elecom	LD-USB/TX, LD-USB/TX, LD-USBL/TX, LD-USB20		pegasus
ELCON Systemtechnik	Goldpfeil P-LAN		pegasus
ELSA AG	Micolink USB2Ethernet		pegasus
Encore Electronics	ENUWI-N3	*	rt2800usb
EndPoints	101 Ethernet		kaweth
Entrega	E45 Ethernet		kaweth
Fujitsu Siemens Computers	Connect2Air E-5400	*	p54usb
Gemtek	WUBR-177G	*	rt73usb
	WUBR-208N	*	rt2800usb
Good Way Technology	GWUSB2E		asix
	RT2573	*	rt73usb
Global Sun Technology	AR5523	*	ar5523
	Cohiba 802.11g Wireless Mini adapter	*	p54usb
Guillemot	HWGUSB2-54-LB, HWGUSB2-54V2-AP	*	rt73usb
	Hercules HWNUp-150	*	rtl8192cu
Hawking Technologies	HWUN1, HWUN2, HWUN3, HAWNU1	*	rt2800usb
	UF100		pegasus
HP	Ethernet HN210E		pegasus
Huawei-3Com	Aolynk WUB320g	*	rt73usb
IMC Networks	802.11 n/g/b Wireless	*	rt2800usb
	-	*	mt7601u
Intellon	MicroLink dLAN		int51x1
I-O Data	ET/TX Ethernet, ET/TX-S Ethernet		pegasus
	ETG-US2		asix
	WNGDNUS2	*	carl9170
	WHG-AGDN/US, WN-GDN/US3, WN-G150U, WN-G300U	*	rt2800usb
	USB ETT		kaweth
	-	*	rtl8xxxu
	-	*	mt76x0u
Jaton	Ethernet		kaweth
Kawasaki LSI	KL5KUSB101B,		kaweth
Kingston Technology	Ethernet		kaweth
	KNU101		pegasus
Kontron	DM9601		dm9601
Lenovo	AX88179		ax88179_178a
	U2L 100P-Y1		asix
Linksys	USB10TX, USB100TX,		pegasus
	USB200M, USB1000		asix
	Gigabit Ethernet		r8152
	WUSB54GC, WUSB54GR, WUSB200	*	rt73usb
	AE1000, AM10, WUSB100 v1/v2, WUSB600N v1/v2, WUSB54GC v3, AE3000	*	rt2800usb
	WUSB54GC v2	*	rtl8187
	WUSB54G, WUSB54AG	*	p54usb
	WUSB54G, WUSB54GP, HU200TS,	*	rt2500usb
	WUSBF54G,	*	zd1211rw
	AE1200	*	brcmfmac
	AE6000	*	mt76x0u
	WUSB6100M	*	ath10k_usb
Logitec	Realtek RTL8187	*	rtl8187
	LAN-GTJ/U2A		asix
	LAN-WN22/U2, LAN-WN12/U2, LAN-W150/U2M, LAN-W300N/U2, LAN-W150N/U2, LAN-W300AN/U2	*	rt2800usb
	-	*	rtl8xxxu
MediaTek	-	*	mt7601u
	-	*	mt76x0u
	-	*	mt76x2u
Mobility	Ethernet		kaweth

	EasiDock Ethernet		pegasus
Microsoft	10/100 USB NIC		pegasus
	RTL8153 GigE [Surface Dock Ethernet]		r8152
	RTL8153 GigE [Surface Dock Ethernet]		cdc_ether
	MN-710	*	p54usb
	Wireless XBox Controller Dongle	*	mt76x2u
Micro Star International	RT2573	*	rt73usb
	1T1R Mini Card	*	rt2800usb
	IEEE 802.11g Wireless	*	p54usb
	RT2570, MSI-6861	*	rt2500usb
MosChip Semiconductor	MCS7730, MCS7830, MCS7832		mcs7830
NEC	Aterm WL300NU-G, WL300NU-AG	*	carl9170
	Aterm PA-WL54GU	*	zd1211rw
NetGear	EA101,		kaweth
	FA101		pegasus
	FA120		asix
	WG111v2	*	rtl8187
	WN111(v2), WNDA3100v1, WNA1000	*	carl9170
	WNDA3200, WNA1100	*	ath9k_htc
	WNA3100M(v1), WNA1000M, WNA1000Mv2, N300MA	*	rtl8192cu
	WG111, WG111	*	p54usb
	WG111U, WPN111, WG111T	*	ar5523
	WNDA4100	*	rt2800usb
Netopia	Motorola 802.11n	*	rt2800usb
NovaTech	RT2573	*	rt73usb
	NV-902W	*	rt2500usb
Omnidirectional Control Technology	USB TO Ethernet, OCT To Fast Ethernet		pegasus
OQO	model 01+ Ethernet		asix
	model 01 Ethernet		rtl8150
Ovislink	AirLive WN-360USB, AirLive WN-200USB	*	rt2800usb
	AirLive WL-1600USB	*	rtl8187
	AirLive X	*	carl9170
Panasonic	DY-WL10	*	rt2800usb
	N5HBZ0000055	*	ath9k_htc
PEGATRON	RT2770, RT2720, RT3070	*	rt2800usb
Peracom	Enet, Enet2, @Home Networks		kaweth
Philips	]Wireless Network Adapter	*	rt73usb
	802.11n Wireless Adapter	*	rt2800usb
	PTA01 Wireless Adapter	*	ath9k_htc
	Wireless Adapter 11g	*	p54usb
	SNU5600, SNU5630NS/05	*	zd1211rw
Planex Communications	GU-1000T		asix
	GWUS300	*	carl9170
	GW-US54HP, GW-US54Mini2	*	rt73usb
	GW-US300MiniS, GW-USMini2N, GW-USMicro300, GW-US300MiniW	*	rt2800usb
	GW-USNano2, GW-USEco300, GW-USValue-EZ	*	rtl8192cu
	GW-US54ZGL, GW-US54GZ, GW-US54Mini	*	zd1211rw
	-	*	mt76x0u
	-	*	rtl8xxxu
Portsmith	Express Ethernet		kaweth
Qcom	RT2573	*	rt73usb
	RTL8187	*	rtl8187
Qualcomm Atheros Communications	Thomson TG121N, TL-WN822N v1, TP-Link TL-WN821N v2, 3Com 3CRUSBN275, AR9170	*	carl9170
	TL-WN422G v2, TP-Link TL-WN322G v3, TP-Link TL-WN821N v3, TL-WN822N v2, AR9271, Ubiquiti WiFiStation, Ubiquiti WiFiStationEXT	*	ath9k_htc
	AR5523	*	ar5523
	-	*	ath6kl_usb
Quanta Microsystems	802.11n Wireless LAN Card	*	rt2800usb
Ralink Technology	RT2070, RT2770, RT2870, RT3070, RT3071, RT3072, RT3370, RT3572, RT3573, RT5370, RT5372, RT5572, Conceptronic C300RU v1/v2, Airlink101 AWLL6080, DrayTek Vigor N61, Airlink101 AWLL6070, Keebox W150NU	*	rt2800usb
	RT2501, RT2573, RT2601, RT2671, RT2501,	*	rt73usb

	Conceptronic C54RU v3		
	RT2500USB, RT2570	*	rt2500usb
	MT7601U	*	mt7601u
	MT7610U	*	mt76x0u
Realtek Semiconductor	RTL8150		rtl8150
	RTL8152, RTL8153		r8152
	RTL8188CUS, RTL8192CU, RTL8188RU	*	rtl8192cu
	RTL8187, RTL8187B	*	rtl8187
	RTL8723AU	*	rtl8xxxu
Sagem	XG-76NA, XG-760NA	*	zd1211rw
	Wi-Fi 11g	*	rt2500usb
Samsung	WIS09ABGN LinkStick	*	rt2800usb
Senao	EUB600v1, WUA-0605, WUA-0615, EnGenius, EUB9706, EUB9801	*	rt2800usb
	EUB-3701	*	rt73usb
	NUB-350	*	p54usb
	NUB-8301	*	zd1211rw
Shark Multimedia	Pocket Ethernet		kaweth
SohoWare	NUB100 Ethernet		pegasus
Silicom	U2E, Psion Gold Port Ethernet		kaweth
Sitecom Europe B.V.	WL-168	*	rtl8187
	WL-182, WL-188, WL-301, WL-302, WL-315, WL-321, WL-323, WL-324, WL-329, WL-343, WL-344, WL-345, WL-349v1, WL-349v4, WL-352v1, WL-609, WLA-4000, WLA-5000, WLA-5100,	*	rt2800usb
	LN-028, LN-031,		asix
	AX88179		ax88179_178a
	WL-113, WL-172	*	rt73usb
	WL-603, WL-113 , WL-117	*	zd1211rw
	-	*	mt76x0u
smartBridges	smartNIC		catc
	smartNIC 2		pegasus
Sphairon Access Systems	Turbolink UB801RE Wireless	*	rtl8187
	Turbolink UB801R WLAN	*	rt2500usb
Standard Microsystems	LAN7500		smsc75xx
	LAN9512, LAN9514, SMSC9512, SMSC9514		smsc95xx
	2202		kaweth
	2202, EZ Connect		pegasus
	LAN78xx		lan78xx
	SMC2862W-G	*	p54usb
	SMC2862W-G	*	rt2500usb
Surecom Technology	EP-9001-g	*	rtl8187
	RT2573	*	rt73usb
Sweex	LW153, LW313	*	rt2800usb
Tekram Technology	QuickWLAN,	*	zd1211rw
TMT Technology	Ethernet		kaweth
Toshiba	WLM-10U1	*	rt2800usb
	WLM-20U2, GN-1080	*	ath9k_htc
TP-Link	Archer T1U	*	mt76x0u
	TL-WN821N, TL-WN822N, TL-WN823N	*	rtl8xxxu
TRENDnet	SMC SMCWUSB-N, TEW-645UB	*	rt2800usb
	TEW-648UBM	*	rtl8192cu
	TEW-444UB, ALL0283	*	ar5523
	TEW-429UB, ALL0298, TEW-509UB	*	zd1211rw
Trust International	NW-3100	*	zd1211rw
U.S. Robotics	U5	*	p54usb
	USR5423	*	zd1211rw
Victor	MP-PRX1		asix
Wistron NeWeb	AR9170+AR9104 802.11abgn	*	carl9170
	UR054g	*	p54usb
	UR055G	*	zd1211rw
	AR5523	*	ar5523
Xircom	Ethernet		kaweth
ZyDAS	ZD1221	*	carl9170
	ZD1211	*	zd1211rw
ZyXEL	G-210H	*	rt73usb
	NWD-210N, NWD211AN, NWD-270N, NWD2105, N220	*	rt2800usb
	NWD271N	*	carl9170

	NWD2205	*	rtl8192cu
	G-200, G-202, G-220, G-220F, AG-225H, M-202,	*	zd1211rw
	NWD6505	*	mt76x0u
Z-Com	802.11b/g Wireless	*	rt73usb
	]802.11b/g/n Wireless	*	rt2800usb
	UB81, UB82, Sphairon Homelink 1202	*	carl9170
	XG-300, XG-703A, XG-705A	*	p54usb
	AR5523	*	ar5523

Supported Display Chips (PCI/PCIe)

*Display chip support is only required for the "unfreeze" process. Regular erasure operations are possible even in unsupported environments.
* Basically, the model number of the chip is used instead of the product name. To confirm, you need to find out the chip model number of the interface.
* The table shows the corresponding product notation for each driver. We have not confirmed the operation.
* Even the ones listed in the table may not work due to firmware version, driver defect, hardware environment, version difference, etc.
* Please be sure to check the operation before purchasing.

64bit Execution		
Manufacturer	Product name	Driver used
	BC-250, FirePro S7150, FirePro S7150V, FirePro W7100, Instinct MI100, Instinct MI210, Instinct MI25 MxGPU/MI25x2 MxGPU/V340 MxGPU/V340L MxGPU, Instinct MI25/MI25x2/V340/V320, Instinct MI250X, Instinct MI250X/MI250, Polaris10, Polaris11, Radeon 540/540X/550/550X / RX 540X/550/550X, Radeon 540X/550X/630 / RX 640 / E9171 MCM, Radeon 680M, Radeon Instinct, Radeon Pro 5600M/V520/BC-160, Radeon Pro 5700 XT, Radeon Pro 5700, Radeon PRO SSG, Radeon Pro V340/Instinct MI25x2, Radeon Pro V520/V540, Radeon Pro V5300X, Radeon Pro V620 MxGPU, Radeon Pro V620, Radeon Pro V7300X / V7350x2, Radeon Pro Vega 20, Radeon Pro Vega 48, Radeon Pro Vega 56, Radeon Pro Vega 64X, Radeon Pro Vega II/Radeon Pro Vega II Duo, Radeon Pro VII/Radeon Instinct MI50 32GB, Radeon Pro W5300M, Radeon Pro W5500, Radeon Pro W5500M, Radeon Pro W5700, Radeon Pro W5700X, Radeon PRO W6300/W6300M, Radeon PRO W6400, Radeon PRO W6500M, Radeon PRO W6600, Radeon PRO W6600M, Radeon PRO W6800, Radeon Pro W6800X/Radeon Pro W6800X Duo, Radeon Pro W6900X, Radeon PRO WX 2100, Radeon PRO WX 3100, Radeon PRO WX 3200, Radeon Pro WX 4100, Radeon Pro WX 4130/4150, Radeon Pro WX 4170, Radeon Pro WX 5100, Radeon Pro WX 7100 Mobile, Radeon Pro WX 7100, Radeon PRO WX 8100/8200, Radeon PRO WX 9100, Radeon Pro WX Vega M GL, Radeon R2/R3/R4/R5 Graphics, Radeon R5 M255, Radeon R5 M315, Radeon R5/R6/R7 Graphics, Radeon R7 M260/M265 / M340/M360 / M440/M445 / 530/535 / 620/625 Mobile, Radeon R9 285/380, Radeon R9 380X / R9 M295X, Radeon R9 FURY / NANO Series, Radeon R9 M295X / M390X, Radeon R9 M395/ M395X Mac Edition, Radeon RX 460/560D / Pro 450/455/460/555/555X/560/560X, Radeon RX 470/480/570/570X/580/580X/590, Radeon RX 550 640SP / RX 560/560X, Radeon RX 5500/5500M / Pro 5500M, Radeon RX 5600 OEM/5600 XT / 5700/5700 XT, Radeon RX 580 2048SP, Radeon RX 6300, Radeon RX 6400/6500 XT/6500M, Radeon RX 6600/6600 XT/6600M, Radeon RX 6650 XT / 6700S / 6800S, Radeon RX 6700/6700 XT/6750 XT / 6800M/6850M XT, Radeon RX 6800/6800 XT / 6900 XT, Radeon RX 6900 XT, Radeon RX 6950 XT, Radeon RX Vega 56/64, Radeon RX Vega M GH, Radeon RX Vega M GL, Radeon Vega Frontier Edition, Radeon Vega Series / Radeon Vega Mobile Series, Radeon VII,	amdgpu
	All-In-Wonder Radeon 8500 DV, All-In-Wonder X800 GT, ATI FirePro (FireGL) Graphics Adapter, FireGL 8800, FireGL T2, FireGL V3100, FireGL V3200, FireGL V3300, FireGL V3350, FireGL V3400, FireGL V3600, FireGL V5000, FireGL V5100, FireGL V5600, FireGL V7100, FireGL V7200, FireGL V7300, FireGL V7350, FireGL V7600, FireGL V7700, FireGL V8600, FireGL V8650, FireGL X1, FireGL X2 AGP Pro, FireGL X3-256, FireGL Z1, FireMV 2200 PCI, FireMV 2200, FireMV 2250, FireMV 2400, FirePro 2260, FirePro 2270, FirePro 2450, FirePro 2460, FirePro A300, FirePro A320, FirePro M4000,	radeon

AMD (AMD/ATI)	FirePro M6100, FirePro M7740, FirePro M7750, FirePro RG220, FirePro Series Graphics Adapter, FirePro Series, FirePro V3700, FirePro V3750, FirePro V3800, FirePro V3900, FirePro V4800, FirePro V4900, FirePro V5700, FirePro V5800, FirePro V5900, FirePro V7750, FirePro V7760, FirePro V7800, FirePro V7900, FirePro V8700, FirePro V8750, FirePro V8800, FirePro V9800, FirePro W2100, FirePro W4100, FirePro W5000, FirePro W5100, FirePro W600, FirePro W7000, FirePro W8100, FirePro W9000, FirePro W9100, FireStream 9170, FireStream 9250, FireStream 9270, FireStream 9350, FireStream 9370, Mobility FireGL 7800, Mobility FireGL 9000/Radeon 9000, Mobility FireGL T2, Mobility FireGL V3100, Mobility FireGL V3200, Mobility FireGL V5000, Mobility FireGL V5100, Mobility FireGL V5200, Mobility FireGL V5250, Mobility FireGL V5700, Mobility FireGL V5725, Mobility IGP 320M, Mobility Radeon 7000 IGP, Mobility Radeon 7500, Mobility Radeon 9000 IGP, Mobility Radeon 9100 IGP, Mobility Radeon 9200 AGP, Mobility Radeon 9500/9700 SE, Mobility Radeon 9550, Mobility Radeon 9600 (PRO) / 9700, Mobility Radeon 9800, Mobility Radeon HD 2300, Mobility Radeon HD 2400 XT, Mobility Radeon HD 2400, Mobility Radeon HD 2600 XT, Mobility Radeon HD 2600 XT/2700, Mobility Radeon HD 2600, Mobility Radeon HD 3100, Mobility Radeon HD 3200, Mobility Radeon HD 3410/3430, Mobility Radeon HD 3450/3470, Mobility Radeon HD 3650, Mobility Radeon HD 3670, Mobility Radeon HD 3850 X2, Mobility Radeon HD 3850, Mobility Radeon HD 3870 X2, Mobility Radeon HD 3870, Mobility Radeon HD 4100, Mobility Radeon HD 4225/4250, Mobility Radeon HD 4330, Mobility Radeon HD 4330/4350/4550, Mobility Radeon HD 4350/4550/530v/540v/545v / FirePro RG220, Mobility Radeon HD 4530/4570/5145/530v/540v/545v, Mobility Radeon HD 4650/5165, Mobility Radeon HD 4670, Mobility Radeon HD 4830, Mobility Radeon HD 4850 X2, Mobility Radeon HD 4850, Mobility Radeon HD 4860, Mobility Radeon HD 4870, Mobility Radeon HD 5430, Mobility Radeon HD 5430/5450/5470, Mobility Radeon HD 5570/6550A, Mobility Radeon HD 5650/5750 / 6530M/6550M, Mobility Radeon HD 5730 / 6570M, Mobility Radeon HD 5850, Mobility Radeon HD 5870, Mobility Radeon X1300, Mobility Radeon X1350, Mobility Radeon X1400, Mobility Radeon X1450, Mobility Radeon X1600, Mobility Radeon X1700, Mobility Radeon X1700/X2500, Mobility Radeon X1800 XT, Mobility Radeon X1800, Mobility Radeon X2300 HD, Mobility Radeon X2300, Mobility Radeon X300, Mobility Radeon X300, Mobility Radeon X600 SE, Mobility Radeon X600, Mobility Radeon X700 XL, Mobility Radeon X700, Mobility Radeon X800 XT, Mobility Radeon X800, Mobility Radeon Xpress 200, Mobility Radeon Xpress 200M, Radeon 2100, Radeon 3000, Radeon 3100, Radeon 7000 / Radeon VE, Radeon 7200 / All-In-Wonder Radeon, Radeon 7500/7500 LE, Radeon 8500/8500 LE, Radeon 9000 Series, Radeon 9100 IGP, Radeon 9100 PRO/XT IGP, Radeon 9100, Radeon 9200 PRO / 9250, Radeon 9200 SE, Radeon 9200, Radeon 9500 PRO/9700, Radeon 9500, Radeon 9550, Radeon 9550/9600/X1050 Series, Radeon 9550/9600/X1050 Series, Radeon 9600 Series, Radeon 9600 TX, Radeon 9600, Radeon 9600/X1050 Series, Radeon 9700 PRO, Radeon 9700/9700 PRO, Radeon 9800 Series, Radeon 9800 XXL/XT, Radeon 9800, Radeon 9800/9800 SE, Radeon APU XX-2200M with R2 Graphics, Radeon E2400, Radeon E4690, Radeon E6460, Radeon E6760, Radeon E8860, Radeon HD 2350, Radeon HD 2400 LE, Radeon HD 2400 PRO AGP, Radeon HD 2400 PRO PCI, Radeon HD 2400 PRO, Radeon HD 2400 PRO/XT, Radeon HD 2600 PRO AGP, Radeon HD 2600 PRO, Radeon HD 2600 X2, Radeon HD 2600 XT AGP, Radeon HD 2600 XT, Radeon HD 2900 GT, Radeon HD 2900 PRO, Radeon HD 2900 PRO/XT, Radeon HD 2900 XT, Radeon HD 3200, Radeon HD 3300, Radeon HD 3450 AGP, Radeon HD 3450 PCI, Radeon HD 3450, Radeon HD 3470, Radeon HD 3650 AGP, Radeon HD 3650/3750/4570/4580, Radeon HD 3690/3850, Radeon HD 3830, Radeon HD 3850 AGP, Radeon HD 3850 X2, Radeon HD 3870 X2, Radeon HD 3870, Radeon HD 4200, Radeon HD 4250, Radeon HD 4290, Radeon HD 4350/4550, Radeon HD 4550, Radeon HD 4600 AGP Series, Radeon HD 4650, Radeon HD 4670, Radeon HD 4710, Radeon

HD 4750, Radeon HD 4770, Radeon HD 4830, Radeon HD 4850 X2, Radeon HD 4850, Radeon HD 4860, Radeon HD 4870 X2, Radeon HD 4870, Radeon HD 4890, Radeon HD 5000/6000/7350/8350 Series, Radeon HD 5550/5570/5630/6390/6490/7570, Radeon HD 5550/5570/5630/6510/6610/7570, Radeon HD 5570/6510/7510/8510, Radeon HD 5670 640SP Edition, Radeon HD 5670/5690/5730, Radeon HD 5750, Radeon HD 5770, Radeon HD 5830, Radeon HD 5850, Radeon HD 5870, Radeon HD 5970, Radeon HD 5970, Radeon HD 6250, Radeon HD 6250, Radeon HD 6290, Radeon HD 6310, Radeon HD 6310, Radeon HD 6320, Radeon HD 6330M, Radeon HD 6370D, Radeon HD 6370M/7370M, Radeon HD 6380G, Radeon HD 6400M Series, Radeon HD 6400M Series, Radeon HD 6400M/7400M Series, Radeon HD 6410D, Radeon HD 6410D, Radeon HD 6430M, Radeon HD 6450/7450/8450 / R5 230 OEM, Radeon HD 6450A/7450A, Radeon HD 6480G, Radeon HD 6480G, Radeon HD 6520G, Radeon HD 6530D, Radeon HD 6550D, Radeon HD 6550M, Radeon HD 6570/7570/8550 / R5 230, Radeon HD 6610M/7610M, Radeon HD 6620G, Radeon HD 6630M/6650M/6750M/7670M/7690M, Radeon HD 6650A/7650A, Radeon HD 6670/7670, Radeon HD 6730M/6770M/7690M XT, Radeon HD 6750, Radeon HD 6770, Radeon HD 6790, Radeon HD 6800 Series, Radeon HD 6850, Radeon HD 6850M/6870M, Radeon HD 6870, Radeon HD 6930, Radeon HD 6950, Radeon HD 6970, Radeon HD 6970M/6990M, Radeon HD 6990, Radeon HD 6990, Radeon HD 7000M Series, Radeon HD 7290, Radeon HD 7300 Series, Radeon HD 7310, Radeon HD 7340, Radeon HD 7350/8350 / R5 220, Radeon HD 7400G, Radeon HD 7400G, Radeon HD 7420G, Radeon HD 7420G, Radeon HD 7450, Radeon HD 7450A, Radeon HD 7470/8470 / R5 235/310 OEM, Radeon HD 7480D, Radeon HD 7500G, Radeon HD 7500G, Radeon HD 7500G, Radeon HD 7500M/7600M Series, Radeon HD 7520G, Radeon HD 7520G, Radeon HD 7540D, Radeon HD 7550M/7570M/7650M, Radeon HD 7560D, Radeon HD 7570, Radeon HD 7600 Series, Radeon HD 7600G, Radeon HD 7620G, Radeon HD 7640G, Radeon HD 7650A/7670A, Radeon HD 7660D, Radeon HD 7660G, Radeon HD 7670M, Radeon HD 7700M Series, Radeon HD 7730/8730, Radeon HD 7730M, Radeon HD 7750/8740 / R7 250E, Radeon HD 7770/8760 / R7 250X, Radeon HD 7790/8770 / R7 360 / R9 260/360 OEM, Radeon HD 7850 / R7 265 / R9 270 1024SP, Radeon HD 7850M/8850M, Radeon HD 7870 GHz Edition, Radeon HD 7870 XT, Radeon HD 7870M, Radeon HD 7950/8950 OEM / R9 280, Radeon HD 7970/8970 OEM / R9 280X, Radeon HD 7970M, Radeon HD 7990/8990 OEM, Radeon HD 8180, Radeon HD 8210, Radeon HD 8240 / R3 Series, Radeon HD 8250/8280G, Radeon HD 8280 / R3 Series, Radeon HD 8280E, Radeon HD 8310E, Radeon HD 8310G, Radeon HD 8330, Radeon HD 8330E, Radeon HD 8350G, Radeon HD 8370D, Radeon HD 8400 / R3 Series, Radeon HD 8400E, Radeon HD 8410G, Radeon HD 8450G, Radeon HD 8470D, Radeon HD 8490 / R5 235X OEM, Radeon HD 8510G, Radeon HD 8530M / R5 M240, Radeon HD 8550D, Radeon HD 8550G, Radeon HD 8550M / R5 M230, Radeon HD 8570 / R5 430 OEM / R7 240/340 / Radeon 520 OEM, Radeon HD 8570A/8570M, Radeon HD 8570D, Radeon HD 8610G, Radeon HD 8650D, Radeon HD 8650G, Radeon HD 8670 / R5 340X OEM / R7 250/350/350X OEM, Radeon HD 8670A/8670M/8690M / R5 M330 / M430 / Radeon 520 Mobile, Radeon HD 8670A/8670M/8750M / R7 M370, Radeon HD 8670D, Radeon HD 8730M, Radeon HD 8790M, Radeon HD 8830M / R7 250 / R7 M465X, Radeon HD 8850M / R9 M265X, Radeon HD 8870M / R9 M270X/M370X, Radeon HD 8890M / R9 M275X/M375X, Radeon HD 8930M, Radeon HD 8970M, Radeon IGP 320M, Radeon IGP 330M/340M/345M/350M, Radeon IGP 340, Radeon R1E/R2E Graphics, Radeon R2 Graphics, Radeon R3 Graphics, Radeon R3E Graphics, Radeon R4 Graphics, Radeon R4/R5 Graphics, Radeon R5 Graphics, Radeon R5 M230 / R7 M260DX / Radeon 520/610 Mobile, Radeon R5 M230, Radeon R5 M240, Radeon R6 Graphics, Radeon R6 Graphics, Radeon R6/R7 Graphics, Radeon R7 200 Series, Radeon R7 240,

	Radeon R7 240/340 / Radeon 520, Radeon R7 260X/360, Radeon R7 360 / R9 360 OEM, Radeon R7 370 / R9 270/370 OEM, Radeon R7 370 / R9 270X/370X, Radeon R7 Graphics, Radeon R7 M260X, Radeon R7 M265/M365X/M465, Radeon R9 255 OEM, Radeon R9 290/390, Radeon R9 290X Engineering Sample, Radeon R9 290X/390X, Radeon R9 295X2, Radeon R9 M270X/M280X, Radeon R9 M280X, Radeon X1200, Radeon X1300 XT/X1600 PRO, Radeon X1300/X1550 Series, Radeon X1300/X1550/X1600 Series, Radeon X1550 64-bit, Radeon X1600 PRO, Radeon X1600 PRO, Radeon X1600 XT/X1650 GTO, Radeon X1600/X1650 PRO, Radeon X1600/X1650 Series, Radeon X1650 GT, Radeon X1650 PRO, Radeon X1650 PRO, Radeon X1650 XT, Radeon X1800 GTO, Radeon X1800 GTO, Radeon X1800 XL, Radeon X1800 XT, Radeon X1900 GT, Radeon X1900 XT, Radeon X1950 GT, Radeon X1950 PRO, Radeon X1950 XT, Radeon X1950 XTX, Radeon X1950, Radeon X300, Radeon X300/X550/X1050 Series, Radeon X550 XTX / X700, Radeon X550/X600, Radeon X600/X600 SE, Radeon X700 PRO, Radeon X700 SE, Radeon X700 XT, Radeon X700, Radeon X800 AGP Series, Radeon X800 GT AGP, Radeon X800 GT/SE, Radeon X800 GTO, Radeon X800 GTO, Radeon X800 GTO2/XL, Radeon X800 PRO/GTO AGP, Radeon X800 VE AGP, Radeon X800 XT Platinum Edition AGP, Radeon X800 XT Platinum Edition, Radeon X800 XT, Radeon X800, Radeon X850 AGP, Radeon X850 PRO AGP, Radeon X850 SE, Radeon X850 XT AGP, Radeon X850 XT Platinum Edition AGP, Radeon X850 XT Platinum Edition, Radeon X850 XT, Radeon Xpress 1100/1150, Radeon Xpress 1200/1250/1270, Radeon Xpress 1200/1250/1270, Radeon Xpress 1250, Radeon Xpress 200 Series, Radeon Xpress 200, Radeon Xpress 200/1100, Radeon Xpress 200M, Rage/Radeon Mobility Series,	
ASPEED Technology	ASPEED Graphics Family	ast
Tata Power Strategic Electronics Division		bochs
Cirrus Logic	GD 5446	cirrus
Intel Corporation	Atom Processor D2xxx/N2xxx Integrated Graphics Controller, Atom Processor E6xx Integrated Graphics Controller, US15W/US15X SCH, US15L/UL11L SCH, Moorestown Graphics and Video	gma500_gfx
	Chipset, CPU Integrated Graphics Controller HD/UHD/Iris graphics Up to 13th-Gen CPU Integrated Graphics Controller	i915
Matrox Electronics Systems	MGA G200, G200 AGP, G200e , G200EV, G200eW, G200EH, G200eR2, G200eW3, G200eH3	mgag200
NVIDIA	NVIDIA Graphics Controller	nouveau

32bit Execution		
Manufacturer	Product name	Driver used
	FirePro S7150, FirePro S7150V, FirePro W7100, Polaris10, Polaris11, Radeon E9171 MCM, Radeon Instinct MI25 MxGPU, Radeon Instinct MI25, Radeon Instinct, Radeon PRO SSG, Radeon Pro V5300X, Radeon Pro V7300X / V7350x2, Radeon Pro Vega 20, Radeon Pro Vega 56, Radeon PRO WX 2100, Radeon PRO WX 3100, Radeon Pro WX 4100, Radeon Pro WX 4130/4150, Radeon Pro WX 4170, Radeon Pro WX 5100, Radeon Pro WX 7100 Mobile, Radeon Pro WX 7100, Radeon PRO WX 8100/8200, Radeon PRO WX 9100, Radeon Pro WX Vega M GL, Radeon R2/R3/R4/R5 Graphics, Radeon R5 M255, Radeon R5 M315, Radeon R5/R6/R7 Graphics, Radeon R7 M260/M265 / M340/M360 / M440/M445, Radeon R9 285/380, Radeon R9 380X / R9 M295X, Radeon R9 FURY / NANO Series, Radeon R9 M295X, Radeon RX 460/560D / Pro 450/455/460/555/555X/560/560X, Radeon RX 470/480/570/570X/580/580X/590, Radeon RX 550 640SP / RX 560/560X, Radeon RX 550/550X, Radeon RX 580 2048SP, Radeon RX Vega 56/64, Radeon RX Vega M GH, Radeon RX Vega M GL, Radeon Vega Frontier Edition, Radeon Vega Series / Radeon Vega Mobile Series, Radeon VII,	amdgpu
	All-In-Wonder Radeon 8500 DV, All-In-Wonder X800 GT, ATI FirePro (FireGL) Graphics Adapter, FireGL 8800, FireGL T2, FireGL V3100, FireGL V3200, FireGL V3300, FireGL V3350,	radeon

	FireGL V3400, FireGL V3600, FireGL V5000, FireGL V5100, FireGL V5600, FireGL V7100, FireGL V7200, FireGL V7300, FireGL V7350, FireGL V7350, FireGL V7600, FireGL V7700, FireGL V8600, FireGL V8650, FireGL X1, FireGL X2 AGP Pro, FireGL X3-256, FireGL Z1, FireMV 2200 PCI, FireMV 2200, FireMV 2250, FireMV 2400, FirePro 2260, FirePro 2270, FirePro 2450, FirePro 2460, FirePro A300, FirePro A320, FirePro M4000, FirePro M6100, FirePro M7740, FirePro M7750, FirePro RG220, FirePro Series, FirePro V3700, FirePro V3750, FirePro V3800, FirePro V3900, FirePro V4800, FirePro V4900, FirePro V5700, FirePro V5800, FirePro V5900, FirePro V7750, FirePro V7760, FirePro V7800, FirePro V7900, FirePro V8700, FirePro V8750, FirePro V8800, FirePro V9800, FirePro W2100, FirePro W4100, FirePro W5000, FirePro W5100, FirePro W600, FirePro W7000, FirePro W8100, FirePro W9000, FirePro W9100, FireStream 9170, FireStream 9250, FireStream 9270, FireStream 9350, FireStream 9370, Mobility FireGL 7800, Mobility FireGL 9000/Radeon 9000, Mobility FireGL T2, Mobility FireGL V3100, Mobility FireGL V3200, Mobility FireGL V5000, Mobility FireGL V5100, Mobility FireGL V5200, Mobility FireGL V5250, Mobility FireGL V5700, Mobility FireGL V5725, Mobility IGP 320M, Mobility Radeon 7000 IGP, Mobility Radeon 7500, Mobility Radeon 9000 IGP, Mobility Radeon 9100 IGP, Mobility Radeon 9200 AGP, Mobility Radeon 9500/9700 SE, Mobility Radeon 9550, Mobility Radeon 9600 (PRO) / 9700, Mobility Radeon 9800, Mobility Radeon HD 2300, Mobility Radeon HD 2400 XT, Mobility Radeon HD 2400, Mobility Radeon HD 2600 XT, Mobility Radeon HD 2600 XT/2700, Mobility Radeon HD 2600, Mobility Radeon HD 3100, Mobility Radeon HD 3200, Mobility Radeon HD 3410/3430, Mobility Radeon HD 3450/3470, Mobility Radeon HD 3650, Mobility Radeon HD 3670, Mobility Radeon HD 3850 X2, Mobility Radeon HD 3850, Mobility Radeon HD 3870 X2, Mobility Radeon HD 3870, Mobility Radeon HD 4100, Mobility Radeon HD 4225/4250, Mobility Radeon HD 4330, Mobility Radeon HD 4330/4350/4550, Mobility Radeon HD 4350/4550, Mobility Radeon HD 4530/4570/545v, Mobility Radeon HD 4650/5165, Mobility Radeon HD 4670, Mobility Radeon HD 4830, Mobility Radeon HD 4850 X2, Mobility Radeon HD 4850, Mobility Radeon HD 4860, Mobility Radeon HD 4870, Mobility Radeon HD 5430, Mobility Radeon HD 5430/5450/5470, Mobility Radeon HD 5570/6550A, Mobility Radeon HD 5650/5750 / 6530M/6550M, Mobility Radeon HD 5730 / 6570M, Mobility Radeon HD 5850, Mobility Radeon HD 5870, Mobility Radeon X1300, Mobility Radeon X1350, Mobility Radeon X1350, Mobility Radeon X1400, Mobility Radeon X1450, Mobility Radeon X1600, Mobility Radeon X1700, Mobility Radeon X1700/X2500, Mobility Radeon X1800 XT, Mobility Radeon X1800, Mobility Radeon X2300 HD, Mobility Radeon X2300, Mobility Radeon X300, Mobility Radeon X600 SE, Mobility Radeon X600, Mobility Radeon X700 XL, Mobility Radeon X700, Mobility Radeon X800 XT, Mobility Radeon X800, Mobility Radeon Xpress 200, Mobility Radeon Xpress 200M, Radeon 2100, Radeon 3000, Radeon 3100, Radeon 7000 / Radeon VE, Radeon 7200 / All-In-Wonder Radeon, Radeon 7500/7500 LE, Radeon 8500/8500 LE, Radeon 9000 Series, Radeon 9100 IGP, Radeon 9100 PRO/XT IGP, Radeon 9100, Radeon 9200 PRO, Radeon 9200 SE, Radeon 9200, Radeon 9500 PRO/9700, Radeon 9500, Radeon 9550/9600/X1050 Series, Radeon 9600 Series, Radeon 9600 TX, Radeon 9600, Radeon 9600/X1050 Series, Radeon 9700/9700 PRO, Radeon 9800 Series, Radeon 9800 XXL/XT, Radeon 9800, Radeon 9800/9800 SE, Radeon APU XX-2200M with R2 Graphics, Radeon E2400, Radeon E4690, Radeon E6460, Radeon E6760, Radeon E8860, Radeon HD 2350, Radeon HD 2400 LE, Radeon HD 2400 PRO AGP, Radeon HD 2400 PRO PCI, Radeon HD 2400 PRO, Radeon HD 2400 PRO/XT, Radeon HD 2600 PRO AGP, Radeon HD 2600 PRO, Radeon HD 2600 PRO, Radeon HD 2600 X2, Radeon HD 2600 XT AGP, Radeon HD 2600 XT, Radeon HD 2900 GT, Radeon HD 2900 PRO, Radeon HD 2900 PRO/XT, Radeon HD 2900 XT, Radeon HD 3200, Radeon HD 3300, Radeon HD 3450 AGP, Radeon HD 3450 PCI, Radeon HD 3450, Radeon HD 3470, Radeon HD 3650 AGP, Radeon HD 3650 AGP, Radeon HD 3650 AGP, Radeon HD	

AMD (AMD/ATI)	3650/3750/4570/4580, Radeon HD 3690/3850, Radeon HD 3830, Radeon HD 3850 AGP, Radeon HD 3850 X2, Radeon HD 3870 X2, Radeon HD 3870, Radeon HD 4200, Radeon HD 4250, Radeon HD 4290, Radeon HD 4350/4550, Radeon HD 4550, Radeon HD 4600 AGP Series, Radeon HD 4650, Radeon HD 4670, Radeon HD 4710, Radeon HD 4750, Radeon HD 4770, Radeon HD 4830, Radeon HD 4850 X2, Radeon HD 4850, Radeon HD 4860, Radeon HD 4870 X2, Radeon HD 4870, Radeon HD 4890, Radeon HD 5000/6000/7350/8350 Series, Radeon HD 5550/5570/5630/6390/6490/7570, Radeon HD 5550/5570/5630/6510/6610/7570, Radeon HD 5570/6510/7510/8510, Radeon HD 5670 640SP Edition, Radeon HD 5670/5690/5730, Radeon HD 5750, Radeon HD 5770, Radeon HD 5830, Radeon HD 5850, Radeon HD 5870, Radeon HD 5970, Radeon HD 6250, Radeon HD 6250, Radeon HD 6290, Radeon HD 6310, Radeon HD 6310, Radeon HD 6320, Radeon HD 6330M, Radeon HD 6370D, Radeon HD 6370M/7370M, Radeon HD 6380G, Radeon HD 6400M Series, Radeon HD 6400M/7400M Series, Radeon HD 6410D, Radeon HD 6430M, Radeon HD 6450/7450/8450 / R5 230 OEM, Radeon HD 6450A/7450A, Radeon HD 6480G, Radeon HD 6520G, Radeon HD 6530D, Radeon HD 6550D, Radeon HD 6550M, Radeon HD 6570/7570/8550, Radeon HD 6610M/7610M, Radeon HD 6620G, Radeon HD 6630M/6650M/6750M/7670M/7690M, Radeon HD 6650A/7650A, Radeon HD 6670/7670, Radeon HD 6730M/6770M/7690M XT, Radeon HD 6750, Radeon HD 6770, Radeon HD 6790, Radeon HD 6800 Series, Radeon HD 6850, Radeon HD 6850M/6870M, Radeon HD 6870, Radeon HD 6930, Radeon HD 6950, Radeon HD 6970, Radeon HD 6970M/6990M, Radeon HD 6990, Radeon HD 6990, Radeon HD 7000M Series, Radeon HD 7290, Radeon HD 7300 Series, Radeon HD 7310, Radeon HD 7340, Radeon HD 7350/8350 / R5 220, Radeon HD 7400G, Radeon HD 7420G, Radeon HD 7450, Radeon HD 7450A, Radeon HD 7470/8470 / R5 235/310 OEM, Radeon HD 7480D, Radeon HD 7500G, Radeon HD 7500M/7600M Series, Radeon HD 7520G, Radeon HD 7540D, Radeon HD 7550M/7570M/7650M, Radeon HD 7560D, Radeon HD 7570, Radeon HD 7600 Series, Radeon HD 7600G, Radeon HD 7620G, Radeon HD 7640G, Radeon HD 7650A/7670A, Radeon HD 7660D, Radeon HD 7660G, Radeon HD 7670M, Radeon HD 7700M Series, Radeon HD 7730/8730, Radeon HD 7730M, Radeon HD 7750/8740 / R7 250E, Radeon HD 7770/8760 / R7 250X, Radeon HD 7790/8770 / R7 360 / R9 260/360 OEM, Radeon HD 7850 / R7 265 / R9 270 1024SP, Radeon HD 7850M/8850M, Radeon HD 7870 GHz Edition, Radeon HD 7870 XT, Radeon HD 7870M, Radeon HD 7950/8950 OEM / R9 280, Radeon HD 7970/8970 OEM / R9 280X, Radeon HD 7970M, Radeon HD 7990/8990 OEM, Radeon HD 8180, Radeon HD 8210, Radeon HD 8240 / R3 Series, Radeon HD 8250/8280G, Radeon HD 8280 / R3 Series, Radeon HD 8280E, Radeon HD 8310E, Radeon HD 8310G, Radeon HD 8330, Radeon HD 8330E, Radeon HD 8350G, Radeon HD 8370D, Radeon HD 8400 / R3 Series, Radeon HD 8400E, Radeon HD 8410G, Radeon HD 8450G, Radeon HD 8470D, Radeon HD 8490 / R5 235X OEM, Radeon HD 8510G, Radeon HD 8530M / R5 M240, Radeon HD 8550D, Radeon HD 8550G, Radeon HD 8550M / R5 M230, Radeon HD 8570 / R7 240/340 OEM, Radeon HD 8570A/8570M, Radeon HD 8570D, Radeon HD 8610G, Radeon HD 8650G, Radeon HD 8670 / R7 250/350, Radeon HD 8670A/8670M/8690M / R5 M330 / M430 / Radeon 520 Mobile, Radeon HD 8670A/8670M/8750M, Radeon HD 8670D, Radeon HD 8730M, Radeon HD 8790M, Radeon HD 8830M / R7 250 / R7 M465X, Radeon HD 8850M / R9 M265X, Radeon HD 8870M / R9 M270X/M370X, Radeon HD 8890M / R9 M275X/M375X, Radeon HD 8930M, Radeon HD 8970M, Radeon IGP 320M, Radeon IGP 330M/340M/345M/350M, Radeon IGP 340, Radeon R1E/R2E Graphics, Radeon R2 Graphics, Radeon R3 Graphics, Radeon R3E Graphics, Radeon R4 Graphics, Radeon R4/R5 Graphics, Radeon R5 Graphics, Radeon R5 M230 / R7 M260DX / Radeon 520 Mobile, Radeon R5 M230, Radeon R5 M240, Radeon R6 Graphics, Radeon R6/R7 Graphics, Radeon R7 200 Series, Radeon R7 240/340, Radeon R7 260X/360, Radeon R7 360 /	

	R9 360 OEM, Radeon R7 370 / R9 270/370 OEM, Radeon R7 370 / R9 270X/370X, Radeon R7 Graphics, Radeon R7 M260X, Radeon R7 M265/M365X/M465, Radeon R9 255 OEM, Radeon R9 290/390, Radeon R9 290X/390X, Radeon R9 295X2, Radeon R9 M270X/M280X, Radeon R9 M280X, Radeon X1200, Radeon X1300 XT/X1600 PRO, Radeon X1300/X1550 Series, Radeon X1300/X1550, Radeon X1300/X1550/X1600 Series, Radeon X1550 64-bit, Radeon X1550 Series, Radeon X1600 PRO, Radeon X1600 XT/X1650 GTO, Radeon X1600/X1650 PRO, Radeon X1600/X1650 Series, Radeon X1650 GT, Radeon X1650 PRO, Radeon X1650 XT, Radeon X1800 GTO, Radeon X1800 XL, Radeon X1800 XT, Radeon X1900 GT, Radeon X1900 XT, Radeon X1950 GT, Radeon X1950 PRO, Radeon X1950 XT, Radeon X1950 XTX, Radeon X1950, Radeon X300, Radeon X300/X550/X1050 Series, Radeon X550 XTX / X700, Radeon X600, Radeon X600/X600 SE, Radeon X700 PRO, Radeon X700 SE, Radeon X700 XT, Radeon X700, Radeon X800 AGP Series, Radeon X800 GT AGP, Radeon X800 GT/SE, Radeon X800 GTO, Radeon X800 PRO/GTO AGP, Radeon X800 VE AGP, Radeon X800 XL, Radeon X800 XT Platinum Edition AGP, Radeon X800 XT Platinum Edition, Radeon X800 XT, Radeon X800, Radeon X850 AGP, Radeon X850 PRO AGP, Radeon X850 SE, Radeon X850 XT AGP, Radeon X850 XT Platinum Edition AGP, Radeon X850 XT Platinum Edition, Radeon X850 XT, Radeon Xpress 1100/1150, Radeon Xpress 1200/1250/1270, Radeon Xpress 1250, Radeon Xpress 200 Series, Radeon Xpress 200, Radeon Xpress 200/1100, Radeon Xpress 200M, Rage/Radeon Mobility Series,	
ASPEED Technology	ASPEED Graphics Family	ast
Tata Power Strategic Electronics Division		bochs-drm
Cirrus Logic	GD 5446	cirrus
Intel Corporation	Chipset, CPU Integrated Graphics Controller HD/UHD/Iris graphics Up to 8th-Gen CPU Integrated Graphics Controller	i915
Matrox Electronics Systems	MGA G200e , G200EV, G200eW, G200EH, G200eR2, G200eW3, G200eH3	mgag200
NVIDIA	NVIDIA Graphics Controller	nouveau

4.7.8 (March 24th, 2025)

Individual version included in this version
gppro4.exe 4.7.5
gpset4.exe 4.7.8
gputil.exe 4.7.8
gpusbst4.exe 4.7.8
gpdata.pac 4.7.8
gpdatahost.pac 4.7.8
---
gpdata.pac (Boot up Erase program)
·Make it possible to change the write value for erasure.
·Added TRIM processing for SSDs (ATA, NVMe) when erasing more than 2-times.
·Displays the configured value of AMA (Accessible MAX Address) for ATA drives. Added a warning display when it is set. Added AMA removal function.
·Added display of non-allocated and other memory information for NVMe drives.
·Added "NSA 130-1 compliant" message to the log when processing "random-random-00-verify".
·Changed timeout processing for HDDs that do not return processing time in ATA secure erase.
·Supports PCs that cannot perform "secure boot" due to the August 2024 Windows Update (KB5041585 (Windows 11), KB5041580 (Windows 10)).
·Supports writing to the log after removing and reinserting a USB flush drive after erasure process has started.

gpdatahost.pac (Data for Network boot function)
·Supports PCs that cannot perform "secure boot" due to the August 2024 Windows Update (KB5041585 (Windows 11), KB5041580 (Windows 10)).

gppro4.exe
·Make it possible to change the write value for erasure.
·Displays the configured value of AMA (Accessible MAX Address) for ATA drives. Added a warning display when it is set.
·WinPE: Added TRIM processing for SSDs (ATA, NVMe) when erasing more than 2-times.
·WinPE: Changed timeout processing for HDDs that do not return processing time in ATA secure erase.
·WinPE: NVMe sanitize and namespace processing improvements
·WinPE: ATA command processing improvements

gpset4.exe
·Newly added "Erasure Pattern" settings.
·Newly added "Select UEFI boot Version", to support models only older boot programs can be used.

gputil4.exe
·"Log Conv"(Log Conversion) supports changed AMA status and erasure standard output message.
·"Log Conv" newly supports creating a "Disk Drive Erasure Report" in XPS format.
·Added "Drive Usage" tab page. Ability to display processes using the drive.
·Added "ASCII" display to "Dump".
·Added "COPY" function to "Dump"/"SMART" page.

gpusbst4.exe
·Basically no changes. Recompile in new environment.

4.7.5 (May 24th, 2024)

Individual version included in this version
gppro4.exe 4.7.5
gpset4.exe 4.7.5
gputil.exe 4.7.5
gpusbst4.exe 4.7.5
gpdata.pac 4.7.5
gpdatahost.pac 4.7.5
---
gpdata.pac (Boot up Erase program)
· Changing the UEFI initial boot program.
· Avoid the issue where SecureErase cannot be executed on some old HDDs (Error: 28)
· Fixed the issue when there are two or more USB flash drives, and the issue when booting from a CD when there is a USB flash drive.
· Addition of time synchronization function using ntp.
· Fixed a problem in obtaining HPA values for some HDDs.
· Fixed issue with hyper-v gen2 not recognizing keyboard.
Fixed issue with suspend process, "suspend to RAM unsupported[6]" error occurred.

.
· Changed erasure log format with "PC:" item.

gpdatahost.pac (Data for Network boot function)
· New addition of network boot host function.

gppro4.exe
·WindowsPE: Avoid locking errors caused by drive recognition issues.
·WindowsPE: Changed to additionally set master password when processing SecureErase.

gpset4.exe
· Interface changes.
· Addition of host creation function for Network boot.
· Addition of ntp client function to the erase program.

gputil4.exe
· Addition of log conversion function.
· Support for gpdatahost.pac version display and saved data deletion.

gpusbst4.exe
· New addition of USB flash drive boot configuration tool that can be used with user privileges.

4.7.1 (Oct. 19th, 2023)
Individual version included in this version
gppro4.exe 4.7.1
gpset4.exe 4.7.1
gputil.exe 4.7.1
gpdata.pac 4.7.1
---
gpdata.pac (Boot up Erase program)
· Major update of Linux 64bit kernel (32bit kernel is same as ver4.6.x).
· Addition / update of device driver (support for new models).
· Added suspend processing to unfreeze the ATA drive (at startup and menu processing) .
· Font switching for high resolution display.
· Fixed the problem of menu screen display disorder.
· Changes to namespace handling for NVMe drives. Troubleshooting issues during secure erase.
· Updated bootloader. (support newer PCs secure boot).

gppro4.exe, gpset4.exe, gputil4.exe common
· Addition of 64bit version.
· Updating the compilation environment.

gppro4.exe
· Supports operation on Windows PE.
Secure erase, log to USB flash drive, log to network share, automatic execution,
automatic processing of multiple disks, SSD processing switching, additional information input, etc.

gpset4.exe
· Addition of "WindowsPE configuration file" creation function.
· Supports "HDD boot" in Windows 11/UEFI environment.

gputil4.exe
· Added S.M.A.R.T. information display function

4.6.6 (Aug. 6th, 2022)
Individual version included in this version
gppro4.exe 4.6.6
gpset4.exe 4.6.6
gputil.exe 4.6.6
gpdata.pac 4.6.6
---

gpdata.pac (Boot up Erase program)
·Updated bootloader. (support newer PCs secure boot).
·Added Compliant erasure standard display option.
·Fixed a problem with pci bus sdhci (eMMC drive) recognition.
·License processing support, added license display.
·Evaluation mode support.

gppro4.exe
·Deleted DoD5220.22-M notation.

·License processing support, added license display.
·Evaluation mode support.
·Support English mode.

gpset4.exe
·Supports "Windows11" display.
·Added Compliant erasure standard display option.
·Supports widely for secure boot on HDD boot.
·License processing support, added license display.
·Evaluation mode support.
·Support English mode.

gputil4.exe
·License processing support, added license display.
·Support English mode.

4.6.5 (Oct. 1st, 2021)

Individual version included in this version
gppro4.exe 4.6.4
gpset4.exe 4.6.4
gpset4x.ocx 4.6.4
gputil.exe 4.6.4
gpdata.pac 4.6.5
---

gpdata.pac (Boot up Erase program)
·Fixed a problem in the processing of Sanitize / CRYPTO SCRAMBLE EXT of ATA drive.
·Added automatic ON control for write cache of ATA / SCSI (SAS) drive.
·Added the display of the write cache status of the ATA / SCSI (SAS) drive in "Show current disk status".
·Added "Write cache control" to "Utilities".
·Added "Set Secure Erase Method / Test" to "Utility". The processing method in "Secure Erase / Sanitize" can be selected.

4.6.4 (Mar. 31th, 2021)

Individual version included in this version
gppro4.exe 4.6.4
gpset4.exe 4.6.4
gpset4x.ocx 4.6.4
gputil.exe 4.6.4
gpdata.pac 4.6.4
---

gppro4.exe
· Avoid the problem of "interruption due to error" that occurred mainly in windows7.
· Supports NVMe OPAL information display.

gpset4.exe
· Improved acquisition of UEFI startup information.

gputil4.exe
· Compile in a new environment.

gpdata.pac (Boot up Erase program)
· Supports NVMe Sanitize erase processing.
· Supports NVMe OPAL information acquisition.
· Change of device check method.
· Supports module compression in 64-bit environment.
· Fixed the problem that a part of the second and subsequent disks is erased when exiting with [ESC] etc. from the password specification screen during automatic erase specification.

Other
· Added screenshot image conversion program (stx2bmp.exe)

4.6.3 (Aug. 9th, 2020)

Individual version included in this version
gppro4.exe 4.6.3
gpset4.exe 4.6.3
gpset4x.ocx 4.6.3
gputil.exe 4.6.3
gpdata.pac 4.6.3

Common to *.exe
· Enhancement of program safety with "EV Code Signing".

gppro4.exe
· Fixed the problem that the "Copy" and "Save" buttons were not displayed on the end confirmation screen.
· For Windows dynamic disk, a warning message is issued and processing is disabled.

gputil4.exe
· Fixed the problem that the "File" reading function could not read UNICODE files correctly in "Log Check".

gpset4.exe
· Fixed the problem that the USB flash drive could not be processed by "Cannot write to drive (partition deletion)" when it was formatted with FD type.

gpdata.pac (Boot up Erase program)
· Fixed the problem that "SSD setting" (read verification etc.) did not work properly in the boot environment creation tool (gpset4.exe).
· Fixed an issue where SSD was not working properly when "Secure Erase" was specified for automatic execution
· Change information etc. for NVMe drive by "Write hardware information to FD / USBmem / Net".

4.6.1 (May 8th, 2019)
Individual version included in this version
gppro4.exe 4.6.1
gpset4.exe 4.6.1
gpset4x.ocx 4.6.1
gputil.exe 4.6.1
gpdata.pac 4.6.1
---

gppro4.exe
· Displaying the startup splash screen.
· Enables button display and character customization on the end confirmation screen.
· Added fixed value setting to command line options.
· Addition of command line configuration file function.
· Cancel program termination with ESC button.

gpset4.exe
gpset4x.ocx
· Displaying the startup splash screen.
· Secure erase processing in automatic execution can be set separately.
· SSD erasing process in automatic execution can be set separately.
· Read verification specification in automatic execution can be set individually for secure erase / SSD.
· Added "Additional Options". Password specification screen can be customized.
· Added "UEFI / HDD-boot Text console" option.
· Added "[HDD boot] confirm" check when "HDD boot" configuration.
· USB flash drive type value can be fixed.
· Change of command line options due to function addition.
· The initial display page can be specified by setting the value in the data file or specifying the command line.
· It is possible to specify whether to prioritize the command line by setting the value in the data file.
· If the data file does not support network or Wi-Fi, the related button cannot be selected.
· Added network support status to the data file version display.
· Cancel program termination with ESC button.

gputil4.exe
· Displaying the startup splash screen
· Added network support status to the data file version display.
· Cancel program termination with ESC button.

gpdata.pac (Boot up Erase program)
· Major update of Linux kernel (8th Gen CPU compatible).
· Addition / update of device driver (support for new models).
· More support for secure boot.
· Support for models that could not display the secure erase time.
· Supports secure erase of NVMe drives.
· Show detailed "Show current disk status" for NVMe drives.
· Change password handling for secure erase (change to user-> master password).
· Added erase check mechanism during secure erase / sanitize.
· At the time of automatic execution, the shutdown screen is displayed immediately after the end confirmation

screen. Also, when processing is being performed on another screen, the screen switching button is displayed.
· Separate network / WiFi compatible data file (gpdata.pac).
· When the BIOS boots (USB flash drive, CD), the system read status is displayed on the screen.
· Added 64-bit kernel read option when booting オon BIOS (USB flash drive, CD).
· Added exit with ESC key on password entry screen.
· Hide "OK" and "CANCEL" buttons while executing the erase / verification process.

4.5.0 (Jun. 22th, 2018)
Individual version included in this version
gppro4.exe 4.5.0
gpset4.exe 4.5.0
gpset4x.ocx 4.5.0
gputil.exe 4.5.0
gpdata.pac 4.5.0
---
gppro4.exe
· Added "No buffering on write" option.
· Added "sanitize" information to disk "detail".
· Added a process to periodically flush the buffer during the erase process.
· Command line changes due to option addition.

gpset4.exe
gpset4x.ocx
· Change network settings.
  Wi-Fi setting items added
  Add Name server
  Add Server Name
  Added password display button.
· Change of option contents.
  Specifying the secure erase / sanitize menu
  Change the size of the USB drive to be erased to 32G-> 64G
  Added "UEFI- use old Memory Mapping"
· Command line changes due to addition of setting items.
· Support for 32bit UEFI startup.
· Display of CPU bits.
· Change data file version notation.
· Support for new boot erase program configuration.

gputil4.exe
· Change data file version notation.

gpdata.pac (Boot up Erase program)
· Major update of Linux kernel.
· Support for eMMC and NVMe drives.
· Addition / update of device driver (support for new models).
· Support for models that cannot boot on UEFI in the previous version.
· Supports wireless LAN and USB-LAN.
· Support for server names / name servers on the network.
· Support for SMB3.0, 2.1, 2.0 on Windows sharing.
· Support for read-only drive.
· Addition of ATA sanitization processing.
· Add eMMC secure erase / sanitize processing.
· Automatic display of secure erase / sanitize processing menu.
· Addition of sanitization information in the information display of the disk. Add eMMC information.
· Support for 32bit UEFI (tablet, etc.) startup.
· Change menu options.
· Change the screen size when starting on UEFI.
· Change to 64bit kernel / 64bit system when UEFI boots, 32bit kernel / 32bit system when BIOS boots.
· Support for exFat format of log writing USB flash drive.

4.3.2 (Feb. 14th, 2017)
Individual version included in this version
gppro4.exe 4.3.2
gpset4.exe 4.3.2
gpset4x.ocx 4.3.2
gputil.exe 4.3.2
gpdata.pac 4.3.2
---
gppro4.exe
· Change the write buffer size for removable media (speed up processing of some USB flash drive).
· Limited selection of "Erase system drive" option to Windows XP or earlier.

· Addressing an issue where regular reports are displayed when interrupted due to an error.
· Fixed an issue where the Windows version was not displayed correctly on Winodws8.1 or later.

gpset4.exe
gpset4x.ocx
· Changed to display the progress during processing.
· Fixed an issue where the Windows version was not displayed correctly on Winodws8.1 or later.

gputil4.exe
· Fixed an issue where the Windows version was not displayed correctly on Winodws8.1 or later.

gpdata.pac (Boot up Erase program)
· Addition / update of device driver (support for new models).

4.3.0 (Nov. 27th, 2015)
Individual version included in this version
gppro4.exe 4.3.0
gpset4.exe 4.3.0
gpset4x.ocx 4.3.0
gputil.exe 4.3.0
gpdata.pac 4.3.0
---
gppro4.exe
· Fixed an issue where the progress was not updated after 2TB during the erase process.
· Support for OPAL (self-encrypting disk). Display OPAL information in the detailed information of the disk.
· Improvement of acquisition of HPA / DCO information.
· Change buffer size when erasing removable media.
· Supports Windows 10 notation.

gpset4.exe
· Dealing with NTFS compression (to be uncompressed) and encryption (error) in the BIOS boot environment when configuring the HDD boot.
· Added "UEFI-disable runtime" option.

gputil4.exe
· Partial changes to the common basic library.

gpdata.pac (Boot up Erase program)
· Addition / update of device driver (support for new models).
· Change the screen display to a fixed size.
· Change of initial option at UEFI boot (Fixed the problem that processing may stop at the second erase process at UEFI boot).
· Added options when booting UEFI (VirtualMemory Mode, disable efi).
· Support for OPAL (self-encrypting disk). The OPAL status is displayed on the disk status display. Added processing warning in OPAL mode. Added encryption key deletion process to the utility.

4.2.0 (Dec. 14th, 2014)
Individual version included in this version
gppro4.exe 4.2.0
gpset4.exe 4.2.0
gpset4x.ocx 4.2.0
gputil.exe 4.2.0
gpdata.pac 4.2.0
---
gppro4.exe
· Supports disk size information by DCO (Device Configuration Overlay)
· Added a function to count the number of retries when a Read / Write error occurs.
· Expansion of functions for acquiring serial numbers of USB memory.
· Change of end report (DCO, retry item added).
· Correction of processing at the time of abnormal termination.

gpset4.exe
· Support for UEFI (Secure Boot) on CD / USB flash drive boot.
· Support for UEFI(Secure Boot) on HDD boot.
· Expansion of functions for acquiring serial numbers of USB memory.
· Fixed the problem that some USB memory could not be written correctly.

gputil4.exe
· Partial changes to the disk access basic library.

gpdata.pac (Boot up Erase program)
· Addition / update of kernel, device driver (support for new models).

· Supports UEFI boot (Secure Boot). Added 64-bit version.
· Supports disk size information / deletion by DCO (Device Configuration Overlay).
· Added a function to count the number of retries when a Read / Write error occurs.
· End screen, log change (DCO, retry item added).

4.1.0 (Oct. 1st, 2012)
Individual version included in this version
gppro4.exe 4.1.0
gpset4.exe 4.1.0
gpset4x.ocx 4.1.0
gputil.exe 4.1.0
gpdata.pac 4.1.0
---
gppro4.exe
· Support for 4096 sector drives
· Added display of sector size.
· Add command line processing.

gpset4.exe,gpset4x.ocx
· Add network setting.
· Add network log specification item.
· Addition of module configuration file.
· Addition of initial value specification at menu processing.
· Add network etc. to command line processing.

gputil4.exe
· Support for Ver4.1.x data files.

gpdata.pac (Boot up Erase program)
· Addition / update of kernel, device driver (support for new models).
· Added network log write.
· Added file save to network.
· Fixed device recognition issue.
· Support for 4096 sector drives.
· Added display of sector size.
· Addition of module configuration file.
· Addition of initial value specification at menu processing.
· Add log write check process before erasing.
· Added network related processing to the utility.
· The log writing status is displayed on the end screen.

4.0.2 (Apr. 9th, 2012)
Individual version included in this version
gppro4.exe 4.0.1
gpset4.exe 4.0.2
gpset4x.ocx 4.0.2
gputil.exe 4.0.1
gpdata.pac 4.0.2
---
gpset4.exe,gpset4x.ocx
· Solved the problem that an error occurred when creating a CD image by booting from a device other than the c: drive.
· Fixed the problem that an error occurred when the file name was specified as a relative path when creating a CD image. Changed to allow input only for absolute paths.
· Added a writable check for CD image files before processing when creating a CD image.

gpdata.pac (Boot up Erase program)
· HP SmartArray Driver Update (cciss, hpsa).
· Emulex FC driver (lpfc) initial parameter change.
· Display the disk number on the processing end screen. Change the number of displayed lines.

4.0.1 (Feb. 28th, 2012)
Individual version included in this version
gppro4.exe 4.0.1
gpset4.exe 4.0.1
gpset4x.ocx 4.0.1
gputil.exe 4.0.1
gpdata.pac 4.0.1

3.0.1 (Jul. 7th, 2006)

2.0.1 (Jun. 12th, 2004)

Contact / Support
support@kirara21.com

GreenPepper PRO online manual
Ver4.7.8 - updated March 24th, 2025

Kirara21. Co., Ltd.
https://www.kirara21.com (Global site)
https://www.kirala21.com (Japanese site)

Privacy Policy and Other Policies
https://www.kirara21.com/policy/