HAGIWARA Solutions

Portable Malware Scanner

Vaccine USB3

VaccineUSB Boot Scan Manual

Thank you for purchasing Vaccine USB3 (hereinafter referred to as this product).

This manual explains how to use the Vaccine USB boot scan function of this product.

Please read this manual carefully to ensure proper use of this product.

CE FC VCCI

Table of contents

1 Before Use

The Vaccine USB is a licensed product that contains anti-malware application program with the scan engine of Trellix of the United States (hereinafter called “Trellix”) and updates, including virus definition files (hereinafter called “Trellix Programs”).Before start to use your Vaccine USB, we ask you to read and acknowledge the license conditions (including definition of Vaccine USB, licensing, prohibitions and limitations, disclaimers, and warrantee) bundled with Vaccine USB that provides the terms of use between Hagiwara Solutions Co., Ltd., and you on Trellix Programs contained on Vaccine USB. The start of your using Vaccine USB shall constitute your agreement to the license conditions.

Precaution Instructions for Use

For proper use of Vaccine USB, be sure to read the precaution instructions given below and thoroughly understand the instructions when using Vaccine USB. Be advised beforehand that malfunctions, problems, or loss/damage of data of the devices to which Vaccine USB is connected for use, as well as malfunctions or problems of Vaccine USB caused by improper use are out of the scope of warranty.

Indications of Warning Signs

Caution	This sign indicates possibilities of causing human death or injuries.
Warning	This sign indicates possibilities of causing human injuries or damage to property.

Caution

- When using Vaccine USB while connecting it to a device, follow the warnings and cautions provided by the manufacturer of the device to which Vaccine USB is connected.
- Never use at voltages other than instructed. Ignition, fire, heat generation, or electric shock can result.
- Do not use Vaccine USB while the device for which Vaccine USB is applied for virus scan, deletion, or isolation is in operation. The performance of the device might be affected
- Do not use Vaccine USB with wet hands. Electric shock or malfunctions can result.
- Do not leave Vaccine USB within reach of small children or infants. Swallowing it or its cap poses danger of choking. If swallowed, immediately seek medical consultation
- Do not use while walking or driving. Accidents might result.
- Do not use Vaccine USB where water is used or humidity is high. Electric shock, fire, or malfunctions can result.
- In case liquids or foreign objects enter Vaccine USB or the device to which Vaccine USB is connected, or in case smoke or an unusual smell comes out of Vaccine USB or the connected device, immediately turn off the power supply to the device and plug off the power cable from the outlet. Continued use can result in electric shock or fire.
- Before touching Vaccine USB, remove the static electricity from the body by touching metals, etc. The static electricity can cause damage or erase the data.
- Do not bend forcibly, drop, scratch, or load down with heavy objects. Malfunctions can result.
- In case the connector of Vaccine USB is soiled or dusted, remove with a dry, clean cloth. Use in the soiled state can result in malfunctions.
- Do not remove Vaccine USB from the device or turn the device off while data is written on or read from Vaccine USB. The data can be damaged or deleted, and Vaccine USB can be out of order.

Warning

- When using Vaccine USB while connecting it to a device, follow the warnings and cautions provided by the manufacturer of the device to which Vaccine USB is connected.
- Be sure to back up the data that is saved or to be saved on Vaccine USB. Be advised that Hagiwara Solutions Co., Ltd. bears no responsibility for the loss or damage of the programs or data saved in Vaccine USB.
- The Vaccine USB has a lifespan due to its use of flash memory. (Warranty is valid for the licensed period of Vaccine USB. The maximum warranty period is five years.) After use over a long period of time, data will not be saved or retrieved properly.
- When formatting Vaccine USB, be sure that necessary data is not saved on Vaccine USB.
- We grant you a nonexclusive, nontransferable right to use the Product containing the Trellix programs. The Product is provided solely for your use.or any affiliated company to which you may authorize us or our distributors to perform the audits set forth in the License Agreement. In no event, whether in Japan or abroad. The Product may not be rented or transferred to any third party under any circumstances, whether in Japan or abroad. If you intend to export the Product overseas, you must comply with all applicable export laws, regulations, and procedures, both domestic and international.,If you should export the Product overseas, you must fully comply with all relevant export laws, regulations, and procedures, both domestic and foreign.
- The Vaccine USB is packaged for delivery inside Japan. When exporting overseas, be advised that you package the goods for exporting.
- When you are to execute virus scan on your own, be sure to download the latest virus definition files. The latest virus information shall be confirmed on Trellix's or other related websites.
- The Trellix Programs embedded in Vaccine USB do not remove the detected computer viruses but instead delete or isolate the infected files. (The infected files will not be deleted when it was set to Virus Scan Only mode.) If the OS was infected, the program deletes or isolates the infected OS file, and the host device may be left unusable until it is reinstalled with an uninfected OS.
- Viruses that have infected a system file cannot be deleted or isolated at times. However, dedicated deletion tools available for download at Trellix's Website might be able to delete such viruses.
- Viruses that have infected the system memory cannot be deleted or isolated. Confirm the deletion method on Trellix's Website.
- New viruses are being discovered on a daily basis. Execute virus scans with the latest definition files, otherwise viruses may not be detected, deleted or isolated.
- In case the registry has been overwritten by a virus and such virus has been deleted or isolated, the system may not reboot properly since Vaccine USB does not have a function for restoring the registry.
- Once the licensed period of Vaccine USB has expired, the latest virus definition file will no longer be available for download. After the termination of the license period, Trellix Programs provide no protection and will not be guaranteed. Hagiwara Solutions Co., Ltd., or the retailer bears no responsibility for any damage caused by continued use of Vaccine USB after the license period
- There are viruses that cannot be deleted or isolated by Vaccine USB. For such viruses, check the Trellix database and other information to take necessary actions.
- The Vaccine USB can detect the viruses addressed by Trellix when the pattern files were updated to the latest ones. It does not guarantee the detection of every virus. There are cases where it fails to detect a virus in some files including encrypted files or compressed files with password.

Cautions for Storage

Do not keep the product in the following locations. The Vaccine USB can be deteriorated, or electric shock or fire can result.

- Where exposed to direct sunlight
- Where water might leak and wet
- Around heating equipment or fire
- Under high temperatures (over 50°C) and high humidity (over 85%) where dew condensation can occur or temperature can change drastically
- Where it is not level, or the foundation is unstable, or vibration is generated.
- Where strong magnetic field or static electricity can be generated
- Dusty place

Product Warranty Regulations

For defects found within the warranty period of Vaccine USB, free repair or replacement is available provided such defect is determined to be attributed to Vaccine USB. For damage or malfunctions caused during delivery transport, free repair or replacement is available provided such damage or malfunction is clearly attributed to Hagiwara Solutions Co., Ltd.
The compatibility of Application Programs with your specific purposes cannot be warranted.
Hagiwara Solutions Co., Ltd. shall not be liable for any of the following situations.
Malfunctions or damage due to your mishandling such as drops or impacts during transporting after delivery
Malfunctions or damage due to such natural disasters as earthquakes, lightning, wind, and flood damage or fire for which Hagiwara Solutions Co., Ltd. is not responsible.
Repairs or modification performed by persons other than Hagiwara Solutions Co., Ltd. staff
Hagiwara Solutions Co., Ltd. Malfunctions or damage due to handling that disregards the appriopriate methods of use or precautions described in this Manual
Malfunctions or damage due to the malfunctions or problems of the target device to which Vaccine USB is connected
Loss of or damage to the programs or data recorded on Vaccine USB (Hagiwara Solutions Co., Ltd. shall assume no liability for loss of or damage to the programs or data recorded in the memory, even in case such damage or deletion was caused by a defect in Vaccine USB.)
In case Vaccine USB is lost or stolen and comes into possession of third parties, the recorded data can be leaked. Be sure to secure Vaccine USB since Hagiwara Solutions Co., Ltd. takes no responsibility for indemnifying any loss and damage arising out of such a situation.

Limited Indemnity

In any case, Hagiwara Solutions Co., Ltd. or the retailer accepts no liability for any incidental, indirect, special, or consequential damage, including the loss of profit, use, data, trust or confidence, business interruption, or other similar damage caused in relation to Vaccine USB or liability for lost profit.

2 License Agreement

This document outlines the conditions under which VaccineUSB Software (hereinafter referred to as "the Software") is provided for customer use. Please read this document carefully before installing the Software. This agreement establishes the terms under which the use of the software provided by Hagiwara Solutions Co., Ltd. (hereinafter referred to as "the Company") to the customer (hereinafter referred to as "the Customer") is licensed. The Company grants the Customer the right to use the licensed software in accordance with the following terms. The Customer should read the content of this agreement carefully and may use the licensed software at their own risk only if they agree to the content of this agreement. By using the licensed software, the Customer is deemed to have agreed to each term of this agreement. If the Customer does not agree to each term of this agreement, the Company cannot grant the Customer the right to use the licensed software.

Article 1 (General Provisions)
The licensed software is protected by copyright and other intellectual property laws and treaties, both domestically and internationally. The licensed software is licensed to the Customer by the Company under the terms of this agreement, and the intellectual property rights of the licensed software, including copyrights, belong to the Company and are not transferred to the Customer.

Article 2 (License)
1. The Company grants the Customer a non-exclusive right to use the licensed software.
2. The right to use the licensed software arising from this agreement refers to the right to use the licensed software on electronic devices that support the licensed software, for the Customer's devices, etc.
3. The Customer may not modify, add to, or otherwise alter any part of the licensed software.

Article 3 (Restrictions on Rights)
1. The Customer shall not re-license, transfer, lend, lease, or in any other way allow a third party to use the licensed software.
2. The Customer shall not use the licensed software to infringe on the copyright or other rights of the Company or any third party.
3. The Customer shall not engage in reverse engineering, disassembling, decompiling, or any other source code analysis work in relation to the licensed software.
4. Based on this agreement, the Customer may transfer all rights related to the licensed software, as an integral part of the electronic device on which it is installed, to a transferee, provided that the transferee agrees to the terms of this agreement. However, in such cases, the Customer may not retain any copies of the licensed software and must transfer all aspects of the licensed software (including all components, media, electronic documents, and this agreement).

Article 4 (Rights to the Licensed Software)
All rights related to the licensed software, including copyrights, belong to the Company or the original rights holder (hereinafter referred to as the "Original Rights Holder") who has granted the Company the right to license the use of the software to the Customer under this agreement. The Customer shall not have any rights to the licensed software other than the rights to use granted under this agreement.

Article 5 (Scope of Liability)

1. The Company and the Original Rights Holder do not guarantee that the update data defined in Article 6, Section 2 can be installed correctly, nor do they guarantee that the installation of such update data will not cause damage to the Customer.
2. The Company and the Original Rights Holder do not guarantee that the licensed software is free from errors, bugs, or other defects, that it will operate without interruption, or that its use will not cause damage to the Customer or third parties. They also do not guarantee that the licensed software does not infringe on the intellectual property rights of third parties or that manuals and other documents are error-free.
3. Products, software, or network services other than the licensed software on which the operation of the licensed software depends (including those provided by third parties, the Company, or the Original Rights Holder) may be discontinued or interrupted at the discretion of the provider of such software or network services. The Company and the Original Rights Holder do not guarantee that these products, software, or network services will operate without interruption and normally in the future.
4. The liability of the Company and the Original Rights Holder for damage to the Customer is limited to direct and actual ordinary damages that have occurred to the Customer, except in cases of intentional or gross negligence by the Company or the Original Rights Holder, and is limited to the purchase price of the licensed software that the Customer can prove.
5. The Company and the Original Rights Holder shall not be liable for any lost profits, consequential damages, indirect damages, or damages related to data loss or corruption, regardless of the cause of the obligation or tort.
6. The Company provides technical support related to the licensed software licensed to the Customer only through the Company's designated inquiry contact point. However, the Company may change the reception hours of the contact point and the availability of support at any time without the consent of the Customer. Furthermore, unless a separate contract is concluded between the Customer and the Company, the Company is under no obligation to provide or continue to provide such support.

Article 6 (Copyright Protection and Automatic Updates)

1. The Customer agrees to comply with all relevant domestic and international copyright and other intellectual property laws and treaties when using the licensed software.
2. The Customer must update the licensed software within 90 days following the publication of update data (hereinafter "Update Data") by the Company or a third party designated by the Company on the web for the purpose of improving security features, correcting errors, enhancing update functions, etc. of the licensed software. If more than 90 days pass after the Update Data has been published, the Customer cannot use the old version of the licensed software for any purpose other than updating it. The Customer agrees that (i) the functionality of the licensed software may be added, changed, or removed as a result of such updates, and (ii) the updated licensed software will also be subject to this agreement.

Article 7 (Termination of Agreement)

1. The Company may immediately terminate this agreement if the Customer violates any terms set forth in this agreement.
2. Upon termination of this agreement pursuant to the provisions of the preceding paragraph, the Customer must dispose of or return all of the licensed software to the Company within two weeks from the date of termination. If the Customer disposes of the licensed software, they must immediately submit documentation proving such disposal to the Company.

3. The provisions of Articles 4 and 5, Sections 2 and 3 of Article 7, and Sections 1, 3, 4, and 5 of Article 8 shall remain in effect even if this agreement is terminated pursuant to Section 1 of this Article.

Article 8 (Consent to Use of Data)

The Customer agrees that the Company may collect and use technical information related to the usage of this product (excluding information about the Customer's devices), which is not limited to these, for the purposes of software updates related to the Company's products, product support, and other services to be smoothly provided to the Customer. This information will be collected on a regular basis. The Company may use this information in a manner that does not personally identify the Customer, for the purpose of improving products or providing services or technology to the Customer.

Article 9 (Miscellaneous)

1. This agreement shall be governed by the laws of Japan.
2. If the Customer takes the licensed software outside of the country, they must comply with the applicable ordinances, laws, export control regulations, and orders.
3. Any disputes related to this agreement shall be subject to the exclusive jurisdiction of the district court or summary court located at the Company's head office location in the first instance.
4. If any provision of this agreement is rendered invalid by law, such provision shall remain effective to the extent that it is deemed valid by law.
5. If there are any matters not stipulated in this agreement or any doubts arise regarding the interpretation of this agreement, the Customer and the Company shall discuss and resolve the matter in good faith.

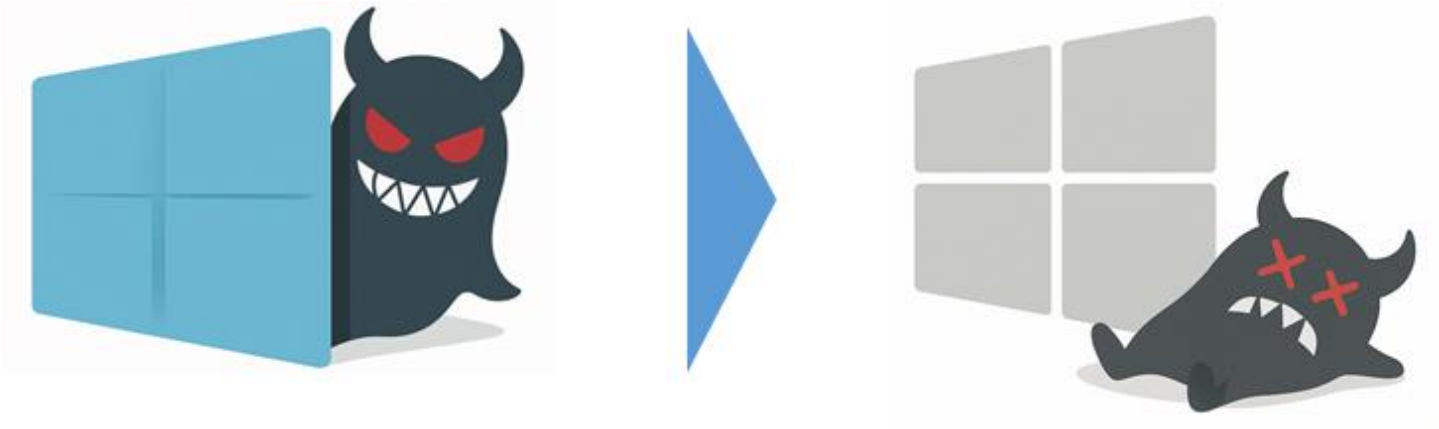
3 About USB Boot Scan

"Vaccine USB Boot Scan" is a malware detection and removal mode that operates in an environment completely independent from your device's OS.

Standard malware protection software runs on operating systems like Windows, which may make it difficult to access malware that is deeply embedded in the OS.

"Vaccine USB Boot Scan" boots the PC directly from a USB memory device. It accesses disks and file systems directly without going through the device's OS, detecting and removing malware hidden in the OS or malware that activates when the OS starts.

It can also be expected to work with devices running older operating systems.



Boot Scan Use Cases

-Use on devices with malware that cannot be removed by regular antivirus software or Vaccine USB
-Use on devices where regular antivirus software or Vaccine USB no longer supports the OS (such as Windows XP)

Boot Scan Usage Video

You can check the Vaccine USB Boot Scan usage video here.

Note:

-We do not guarantee the removal of all malware.

-We do not guarantee operation in all environments.

Vaccine USB Boot Scan Features

Malware Scanning Function Independent from the Device's OS

Boot the PC directly from the USB memory device. Access disks and file systems directly without going through the OS to detect and remove malware hidden in the OS or malware that activates when the OS starts.

Uses Trellix (formerly McAfee) Malware Scan Engine and Definition Files

Uses the Trellix malware scan engine used in the regular Vaccine USB3.

Also uses the latest definition files downloaded to the Vaccine USB.

File Scanning and Deletion Functions

Similar to the regular Vaccine USB3, it scans files within the device and deletes them when malware is detected.

You can select from settings for scan only, deletion.

-Scan only:Only performs malware scanning. Does not delete when malware is detected.

-Scan + Delete:Performs malware scanning and deletes malware when detected.

Displays Scan Results with LED

Similar to the regular Vaccine USB3, it displays status/results using LED.

-During scanning: The red LED and blue LED on the main unit alternate flashing

-When malware is detected: The red LED on the main unit lights up

-When no malware is detected: The blue LED on the main unit lights up

-When malware deletion is successful: The blue LED on the main unit lights up

-When an error occurs: The red LED on the main unit flashes

Log Saving Function

Similar to the regular Vaccine USB3, it saves scan results, discovered virus information, executed PC information, etc. as log files in this product.

Virus Infection Prevention Function for This Product

This product is designed so that nothing can be written to the removable disk area.

It has a function to prevent virus infection to this product, including unknown viruses, even when connected to a virus-

USB Boot Scan Operating Environment

The operating environment for Vaccine USB Boot Scan is as follows:
Note: This is not the operating environment for regular Vaccine USB3.

USB Interface	USB 2.0 (High Speed/Full Speed) / USB3.0 (Super Speed)
Operating Environment	- CPU: Intel 64 and x86 architecture CPU *Does not support arm environmen - Memory: 1GB or more ※2GB or more recommended - Display resolution: VGA (640x480) or higher - Must be able to boot from USB CD/DVD
Compatible Device OS	Windows OLinux OS
Compatible Device File Systems	EXT, EXT2, EXT3, EXT4, XFS, Btrfs NTFS, FAT16, FAT32, exFAT
Verified Storage	SATA HDD, SATA SSD, NVMe SSD, USB memory

Note: Even with an environment that meets all of the above, operation is not guaranteed.

5 About Limitations

When Drive Encryption by BitLocker/TCG-OPAL, etc. is Performed

When a drive is entirely encrypted by Windows' BitLocker, equivalent third-party encryption software, or TCG-OPAL, etc., malware scanning cannot be performed.

When Windows Access Control (Permission Settings) is Set

When special access permissions (Access Control List: ACL) are set for folders or files in Windows,
Vaccine USB may be restricted from accessing specific files depending on the permission settings.

Access to Windows Special System Files or System Folders

Windows system files (e.g., parts of the Windows folder, parts of Program Files, etc.) may have access restrictions.

When Fast Startup is Enabled

When Windows' Fast Startup feature is enabled, the system does not completely shut down, and some information remains saved on the disk.
Using the product in this state may corrupt the file system. Always disable Fast Startup before use.

***-How to disable Fast Startup (operation on Windows side)*:**

1: Open Control Panel and select "Power Options."

2: Click "Choose what the power button does."

3: Click "Change settings that are currently unavailable."

4: Uncheck "Turn on fast startup (recommended)" and click "Save changes."

When Using Secure Boot/TPM

When UEFI Secure Boot/TPM is enabled, Vaccine USB Boot Scan may not start.

Limitations Related to USB CD-ROM Boot

If the UEFI/BIOS of the device (PC) being used does not support booting from a USB CD-ROM, Vaccine USB Boot Scan cannot start.
Even if the UEFI/BIOS supports booting from a USB CD-ROM, Vaccine USB Boot Scan may not necessarily start properly depending on the model or settings.

Target USB Memory

Vaccine USB Boot Scan scans files within the USB memory connected to the device being scanned.
However, connect the USB memory to be scanned to the device before starting Vaccine USB Boot Scan (before powering ON the device).
Any USB memory not connected before startup will not be included in the scan targets.

Limitations Related to Virtual Environments and LVM2 (Logical Volume Manager 2)

Systems that virtualize or abstract disks or partitions (such as LVM2) are not supported.

6 Usage Flow (Overview)

The flow from setup to use of Vaccine USB Boot Scan is outlined below. For details, please refer to section 7.

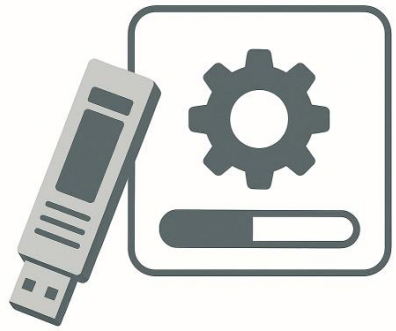
STEP1: Preliminary Setup

1-1: Definition File Update

Update the definition files with the regular Vaccine USB3.
The updated definition files will be used during Vaccine USB Boot Scan.

1-2: USB Boot Scan Settings

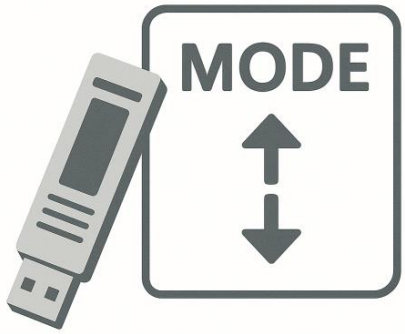
Determine the operation mode for Vaccine USB Boot Scan from the settings screen of the regular Vaccine USB3.



Setting	Operation
Scan only (default)	- Scan operation: Only performs scanning *Does not delete when malware is detected. - Scan range: All files on all drives of the device. - Scan timing: Scanning starts automatically after startup.
Scan + Delete	- Scan operation: Performs scanning and deletes when malware is detected. - Scan range: All files on all drives of the device. - Scan timing: Scanning starts automatically after startup.

1-3: Switch to USB Boot Scan

Perform the update (switch) to Vaccine USB Boot Scan mode.



[Vaccine USB Boot Scan Updater Download Site] https://www.hagisol.co.jp/products/offline/usb3_boot_update.html

STEP2: Using Vaccine USB Boot Scan

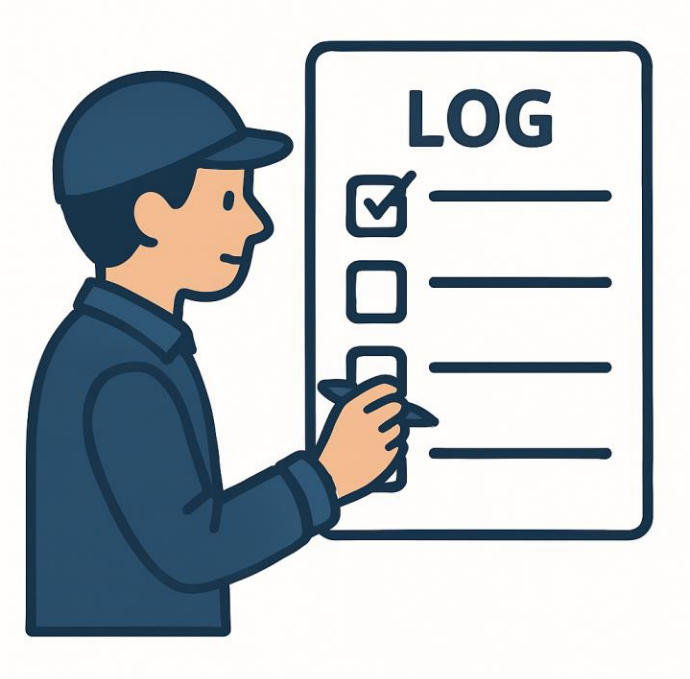
Connect the Vaccine USB to the device to be scanned and restart the device*. Vaccine USB Boot Scan will start, and the scan set in 1-2 will be performed automatically.
*If the power is already off, power on the device.

STEP3: Return to Regular Vaccine USB Mode and Check Logs

To use as a regular Vaccine USB3 again, apply the following update software.
Check the USB Boot Scan logs from [View Logs] in the regular Vaccine USB3.

[Vaccine USB3 Updater Download Site]
https://www.hagisol.co.jp/products/offline/usb3_update.html

Then launch Vaccine USB and check the logs.



7 Preliminary Setup (STEP1)

The following preliminary setup is necessary to use Vaccine USB Boot Scan:

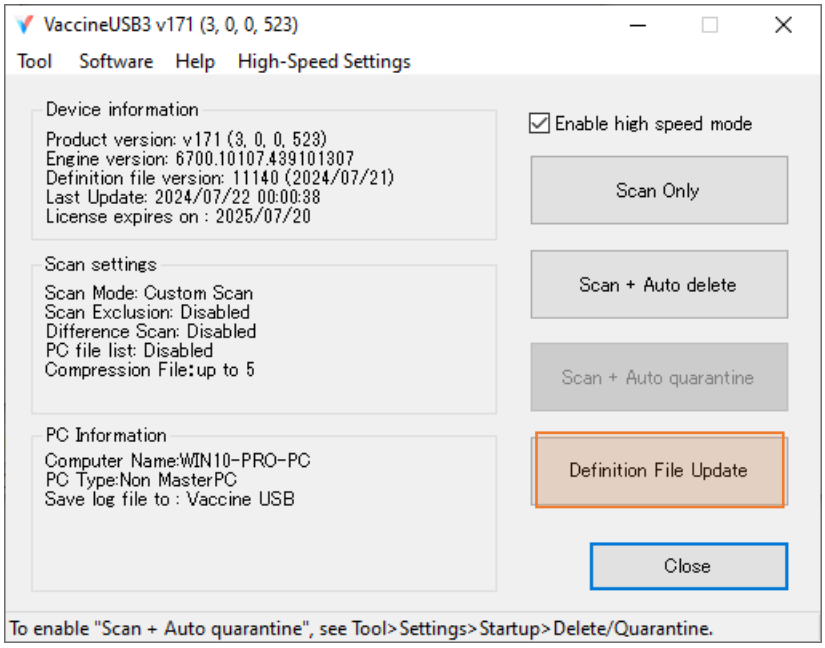
7-1: Definition File Update

7-2: USB Boot Scan Settings

7-3: Switch to USB Boot Scan

Definition File Update

Connect this product to a PC with internet connection, start Vaccine USB, and update the definition files from the main screen.



Note	Depending on the communication environment, downloading the virus definition files may take time. Do not remove this product from the target device or PC while downloading the virus definition files. Confirm that the access LED (green) is not flashing before removing. Forcibly removing it can damage the data and cause the product to malfunction.

USB Boot Scan Settings

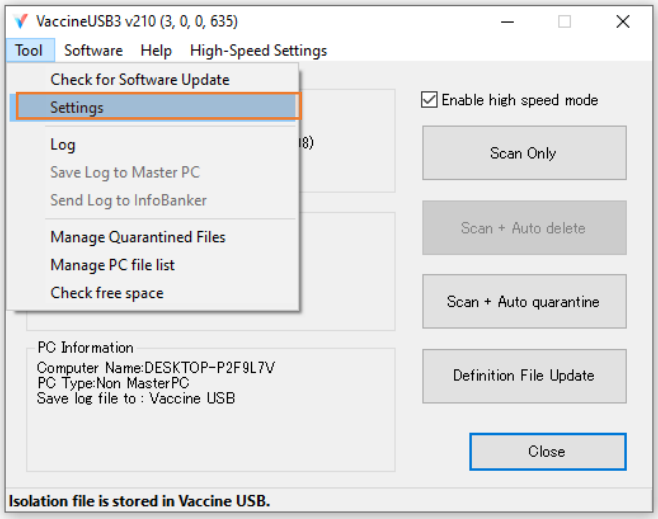
Set the operation mode for Vaccine USB Boot Scan. There are two modes:

Setting	Operation
Scan only (default)	- Scan operation: Only performs scanning *Does not delete when malware is detected. - Scan range: All files on all drives of the device. - Scan timing: Scanning starts automatically after startup.
Scan + Delete	- Scan operation: Performs scanning and deletes when malware is detected. - Scan range: All files on all drives of the device. - Scan timing: Scanning starts automatically after startup.

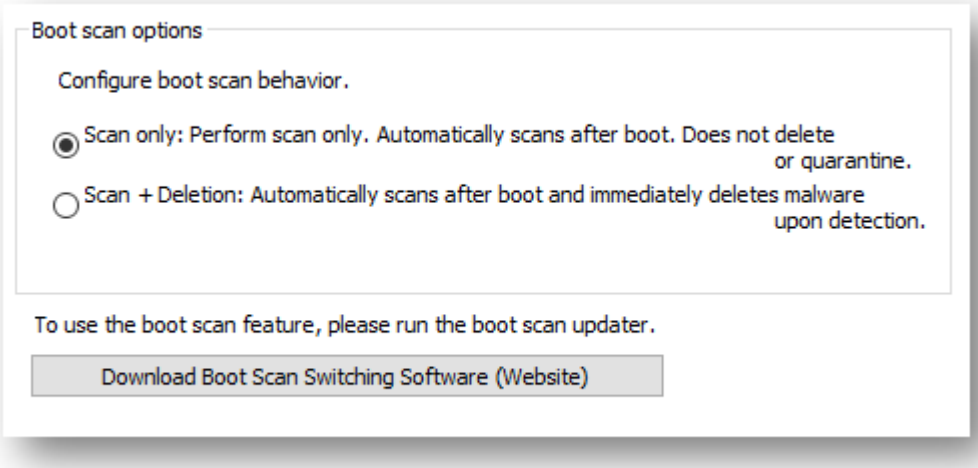
*The default setting is to only perform scanning.
*This setting does not affect the settings of Vaccine USB3 in normal mode.

Setting Method

1: Start Vaccine USB, select [Tools] from the toolbar on the main screen, and click [Settings].



2: Select the tab: USB Boot Scan on the settings screen and make your settings.

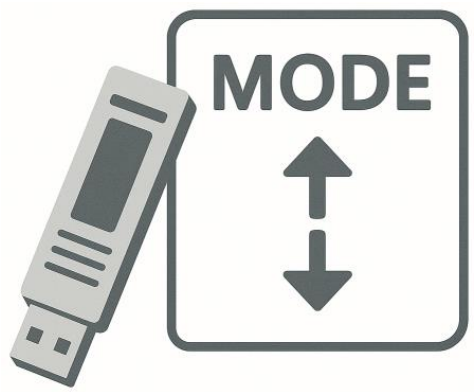


Switch to USB Boot Scan Mode

To use Vaccine USB Boot Scan, you need to update (switch) to Vaccine USB Boot Scan mode.

Download the Vaccine USB Boot Scan Updater from the site below and apply it to your Vaccine USB.

[Vaccine USB Boot Scan Updater Download Site]
https://www.hagisol.co.jp/products/offline/usb3_boot_update.html

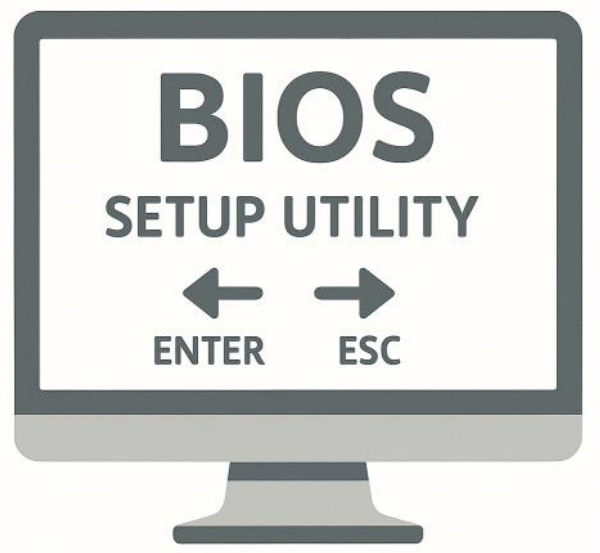


Note: When you switch to Vaccine USB Boot Scan mode, the normal Vaccine USB mode becomes temporarily unavailable.
You can return to normal Vaccine USB mode at any time. See here for how to return.

8 Using Vaccine USB Boot Scan (STEP2)

1: Connect the Vaccine USB3 in Boot Scan mode to the device to be scanned.
Restart the device. *If the power is already off, power on the device.

2: While the device is starting up, move to the BIOS or UEFI boot menu.
Generally, pressing the [Del], [F2], or [F10] key immediately after restart will take you to the menu.The BIOS or UEFI boot menu varies in screen and items depending on the device.In the menu, look for the boot settings item, set "VUSB_BOOT" of Vaccine USB as the first product to boot, and exit the BIOS/UEFI.

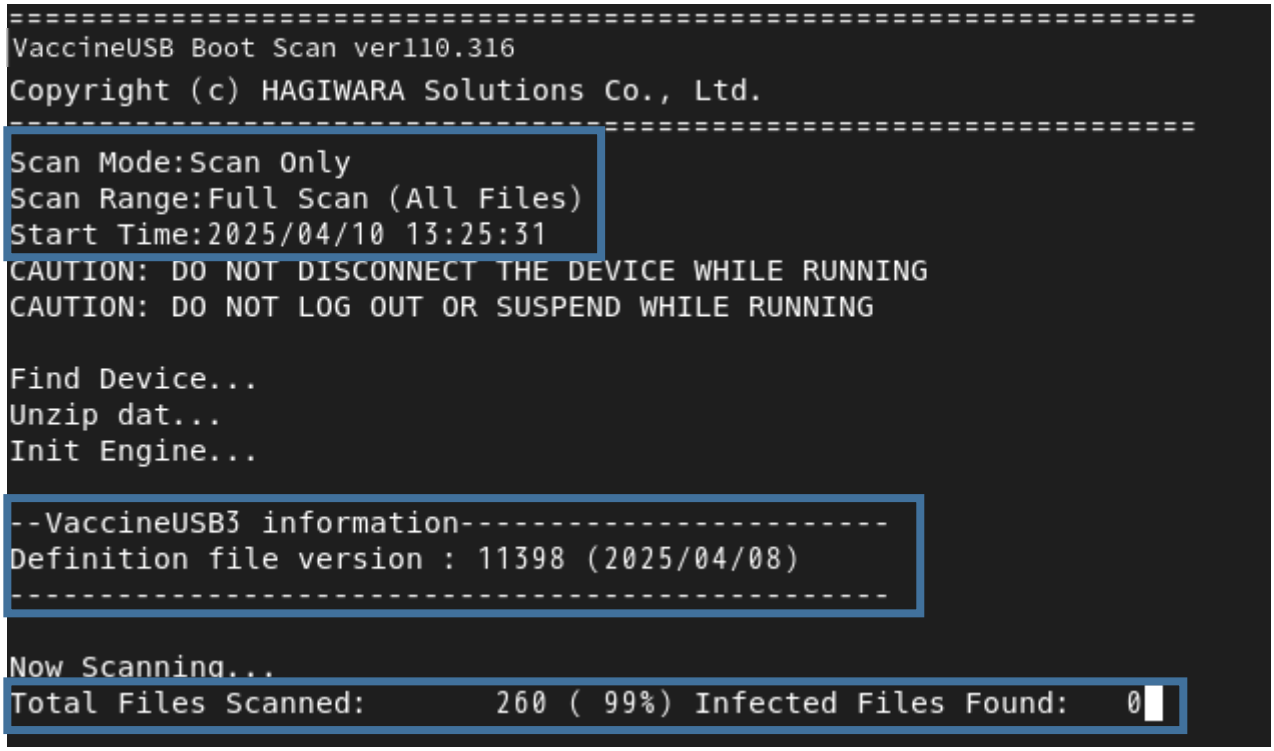


Note: There are BIOS and UEFI where the boot settings item does not exist. Please check with the device manufacturer regarding the BIOS and UEFI menu.

3: When you restart the device, the Vaccine USB Boot Scan will launch and begin scanning.

USB Boot Scan Display Screen

Scan Screen



Scan Screen Explanation

Scan Mode	Vaccine USB Boot Scan operation mode - Scan Only: Only performs malware scanning. - Scan + Auto delete: Performs scanning and deletes when malware is detected.
Scan Range	Scan range - Full Scan (All Files): Scans all drives.
Start Time	Scan start date and time
Definition file version	Definition file version
Total Files Scanned	Number of scanned files (progress [%])
Infected Files Found	Number of detected malware

Scan Result Screen

```
--Scan Summary----------------------------------
Status:WARNING (Malware was found)
Total Files Scanned:731
Infected Files Found:1
Files Removed:0
Scan End Time:2025/04/10 13:34:19
Total Duration:528 s
-----------------------------------------------
```

Scan Result Screen Explanation

Status	Status Scan result (4 types) **[1]SAFETY (Scan completed successfully. No malware found)** Scan result: No malware was found **[2]SAFETY (Scan completed successfully. All detected malware was removed)** Scan result: Malware was detected and all was removed **[3]WARNING (Malware was found)** Scan result: Malware was detected **[4]WARNING (Some malware could not be removed)** Scan result: Malware was detected but could not be removed
Total Files Scanned	Total number of files scanned
Infected File Found	Number of detected malware
File Removed	Number of malware deleted
Scan End Time	Date and time when scanning was completed
Total Duration	Time (seconds) spent scanning

Detected Malware Information Explanation

When malware is detected, malware information is displayed.

```
[Virus001]
Path=/media/user1/SECURE/eicar.com
InfectType=AVT_TEST
VirusName=EICAR test file
Hash=3395856ce81f2b7382dee72602f798b642f14140
CleanAction=0x29AA0024:CleanActionNoAction
```

Path	Full path of the malware
Infect type	Type of malware (including viruses) defined by Trellix
VirusName	Name of malware (including viruses) defined by Trellix
Hash	Hash of the malware
CleanAction	Result of malware scanning - **CleanActionNoAction**: Virus found (no deletion/quarantine process performed) - **CleanActionDeleteFail**: Failed to delete the virus. - **CleanActionQuarantineFail**: Failed to quarantine the virus.

4: Please shut down the device after confirming the scan results. Then remove the vaccineUSB.

This completes the implementation of the boot scan.

LED Specifications

Vaccine USB also displays the inspection status and results using the built-in LEDs. You can check even when implementing on a device without a monitor.

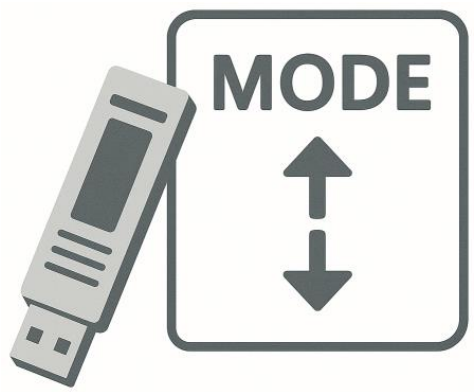
Status	Blue LED	Red LED
Idle (before scanning)	Off	Off
During scanning	Flashing	Flashing
[1]Scan result: No malware was found	On	Off
[2]Scan result: Malware was detected and all was removed	On	Off
[3]Scan result: Malware was detected	Off	On
[4]Scan result: Malware was detected but could not be removed	Off	On
Other errors occurred	Off	Flashing

9 Returning to Normal Vaccine USB Mode (STEP3-1)

To return the Vaccine USB to normal Vaccine USB mode (for scanning in Windows, updating definition files, checking logs, etc.),

Download the Vaccine USB Updater from the site below and apply it to your Vaccine USB.

[Vaccine USB Software Update Software Download Site]
https://www.hagisol.co.jp/products/offline/usb3_update.html



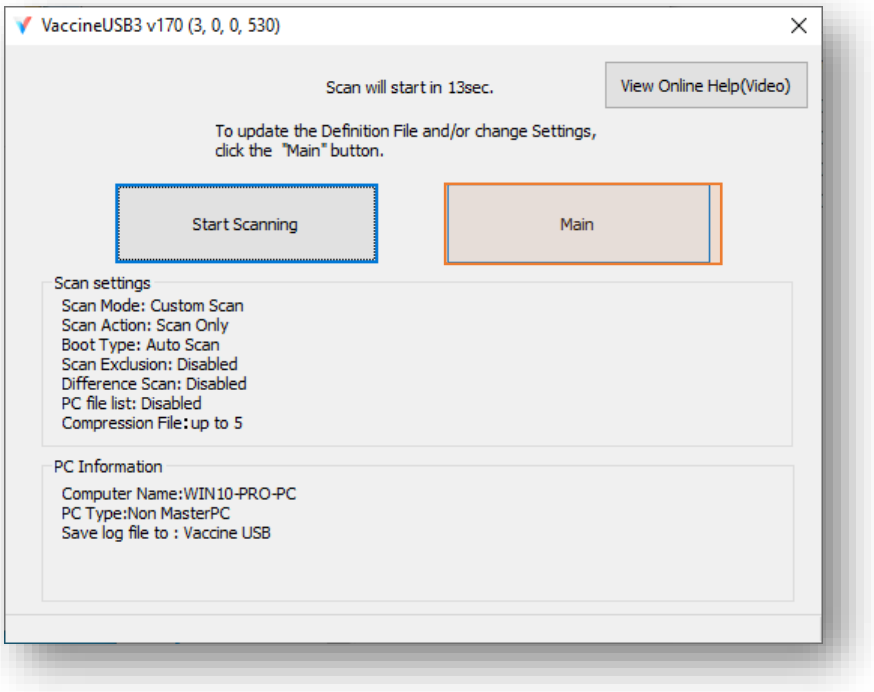
10 Checking Logs (STEP3-2)

Logs saved during boot scanning can be checked using the same method as viewing logs in normal Vaccine USB mode. The scan results are saved as log files within the Vaccine USB. A log file is generated each time a scan is performed.

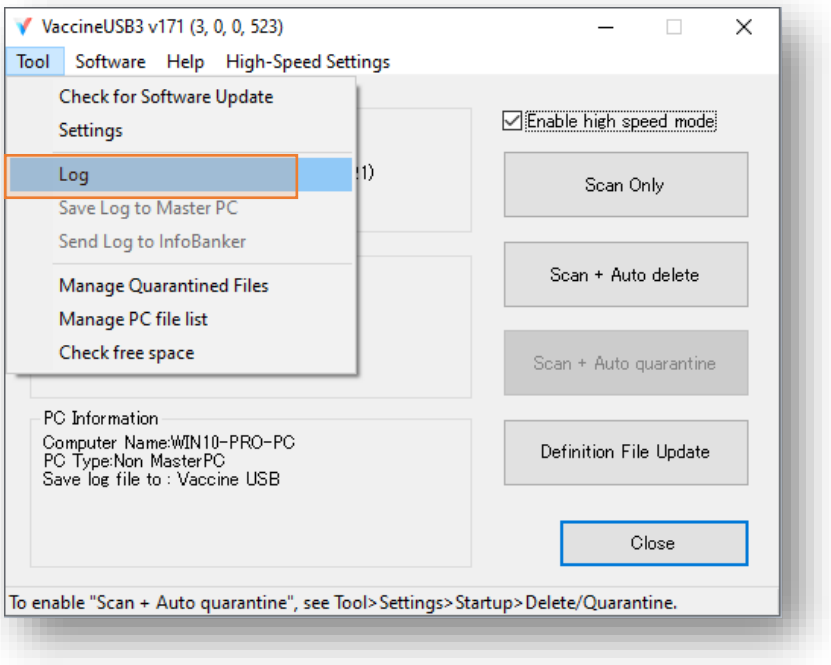
Please check the following for how to view logs.

1:Connect this product to a PC and click the [Main] button on the startup screen.

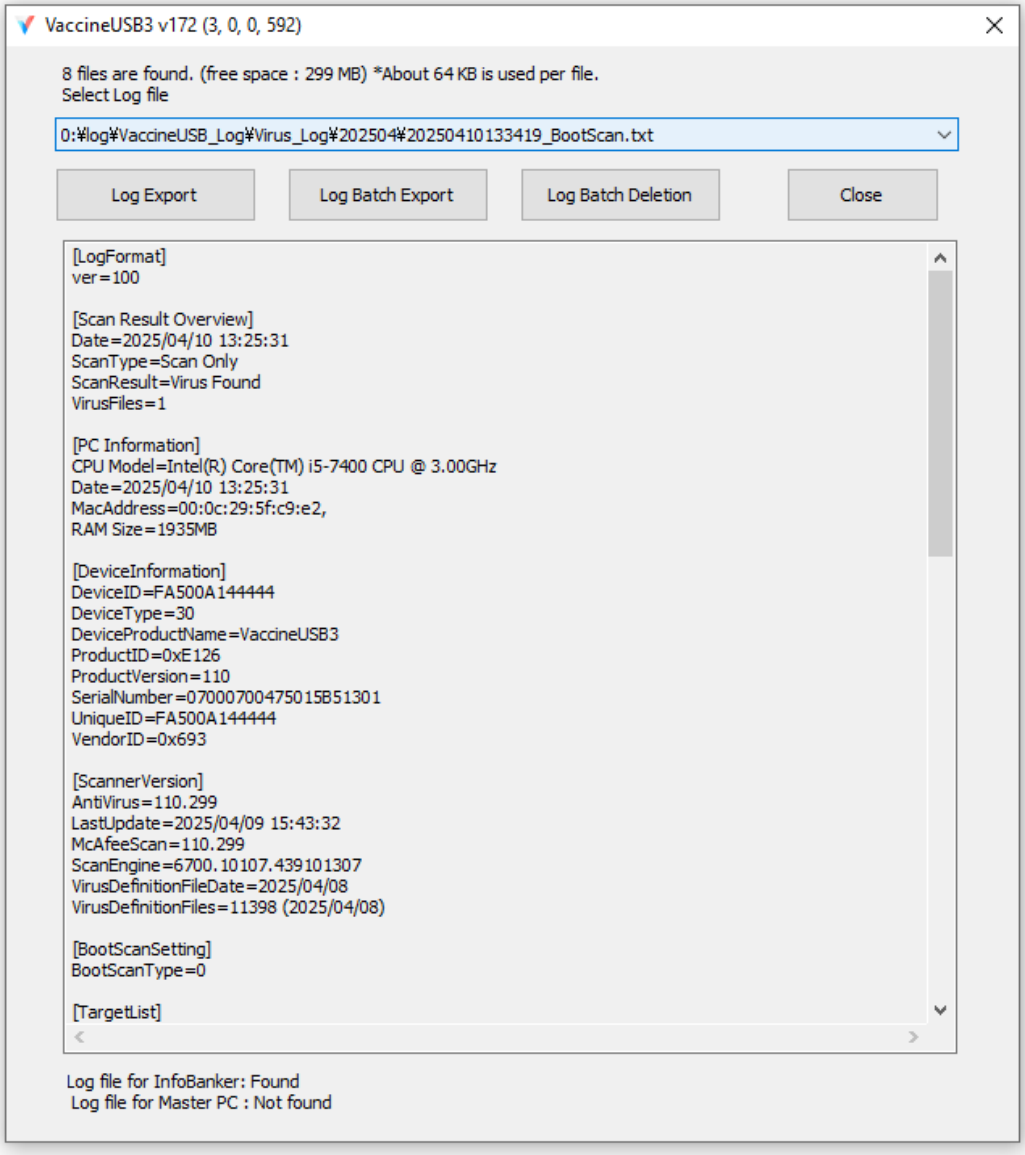
Note:If about 15 seconds pass after this screen is displayed, scanning will start automatically, so please perform operations before that.



2:Select [Tools] from the toolbar and click [Log].



3:The log screen will be displayed. The log file name for boot scan is "YYYYMMDDHHMMSS_BootScan.txt".



Log Contents

Key	Content
Section [LogFormat] Log Format information	
ver	Log Format version
Section [Scan Result Overview] Scan results overview	
Date	Start date and time of vaccine USB scan
ScanType	Scan type (0: Scan only, 1: Scan + immediate deletion, 3: Scan + immediate quarantine)
ScanResult	Final scan result - No virus: No Virus - Virus found: Virus Found
VirusFiles	Number of viruses detected
Section [PC_Information] PC Information	
CPU Model	CPU Model
Date	Log file creation date/time
MacAddress	MAC address
RAM Size	Memory Capacity
Section[DeviceInformation] Device Information	
DeviceID	Number on device case (same as USB serial)
DeviceType	Fixed at 30
DeviceProductName	Fixed at VaccineUSB3
ProductID	Device ProductID
ProductVersion	Product version
SerialNumber	Device USB serial number
UniqueID	Reserved for internal purposes.
VendorID	Device VendorID
Section[ScannerVersion] Scan App Information	
AntiVirus	Anti-virus software version
LastUpdate	Virus definition file update date
McAfeeScan	Anti-virus software library version
ScanEngine	Scan engine version
VirusDefinitionFileDate	Virus definition file date/time
VirusDefinitionFiles	Virus definition file version
Section[BootScanSetting] Boot Scan Settings	
BootScanType	Scan type during boot scan (0: Scan only, 1: Scan + auto Delete, 4: User selection)
Section[TargetList] Scan Target List	
Target#	Scan location path (# is number) *Multiple entries for multiple locations
Section [CustomInformation]Custom information ※Customer can set arbitrarily	
CompanyNameReport	Issuing company name

TargetProductName	Scanned device name/product name
VaccineUSBManagementNumber	VaccineUSB management number
Section[License] License Information	
LicenseAlert	Company management number
LicenseLast	License end date
LicenseStart	License start date
LicenseTerm	License duration in days
Section[Result] Scan Result	
StartTime	Scan start date/time
EndTime	Scan end time
TotalTime	Scan duration (seconds)
TotalScanFiles	Total files scanned
VirusFiles	Number of malware detected
DeleteVirusFiles	Number of malware successfully deleted
IsolateVirusFiles	Number of malware successfully quarantined
NoDeleteOrNotIsolateVirusFiles	Number of malware failed to delete/quarantine
ScanResult	Final scan result - No virus: No Virus - Virus found: Virus Found
BootScanExecutionType	Scan type performed during boot scan (0: Scan only, 1: Scan + deletion)
BootScanExecutionMode	Scan range performed during boot scan 0: Complete scan
BootScanExecuted	0: Boot scan not performed 1: Boot scan performed
TotalThread	Number of threads when scanning
Section[Virus***] Detected Malware Information (***:Virus number 001~)	
Path	Malware full path
InfectType	The infect type defined by Trellix.
VirusName	The virus name defined by Trellix.
CleanAction	The malware scan result -CleanActionNoAction : Malware found (no deletion performed) -CleanActionVirusDeleteSuccess : Malware deletion successful -CleanActionVirusQuarantineSuccess : Malware quarantine successful -CleanActionDeleteFail : Malware deletion failed -CleanActionQuarantineFail : Malware quarantine failed
Result	Reserved for internal purposes
Detected Malware Information Example	
Detected Malware Information Example	[Virus001] Path=/home/user/Desktop/eicar.txt InfectType=AVT_TEST VirusName=EICAR test file

	CleanAction=0x29AA0025:CleanActionVirusDeleteSuccess Result=0x710f0003:KEY_AV_SUMMARY_INFECTED

Key	Content
Section [PC Information in detail] Detailed PC Information (****: (0001~))	
BIOSVersion	BIOS Version
CPUTotal	Number of CPUs
CPUTotalCore	Number of CPU cores
DiskTotal	Number of drives
SystemHostName	Host name
SystemManufacturer	Computer manufacturer
SystemModel	Computer model name
SystemProductIdentifyingNumber	Computer serial number
SystemProductUUID	Motherboard UUID
Section [PC Drive] PC Drive Information (:** (01~))	
DriveLetter**	Drive mount point
DriveCapacity**	Drive capacity (GB)
DriveFreeCapacity**	Drive free capacity (GB)

11 Comparison with Normal Vaccine USB Mode

Since "Vaccine USB Boot Scan" mode is specialized for boot scanning, what it can do is limited compared to normal Vaccine USB mode(over version200).

Item	Vaccine USB Boot Scan Mode	Normal Vaccine USB Mode
Boot Scan	✓	
Windows PC Scan	-	✓
Linux PC Scan	✓	✓
Creating Logs	✓	✓
Definition File Update	-	✓
Log Viewing	-	✓
Settings Change	-	✓
Software Update	-	✓
Quarantined File Management	-	✓
Creating logs for the management service	-	✓
Log Transmission to Management Service	-	✓

-This product incorporates "UDRW Technology," a USB storage technology combining CD-ROM and removable storage areas (patented):

Japan: Patent No. 3914949, Patent No. 3699717, Patent No. 3513147

U.S.A.: Patent No. 7,111,121 B2

China: Patent No. ZL200410038475.6

Hong Kong: Patent No. HK1068990 B

Taiwan: Invention Patent No. I 261757

Korea: Patent No. 589521

European Patent: (Italy, France, Germany, United Kingdom) Patent No. 149182

-Product specifications, appearance, and service contents are subject to change without prior notice. Thank you for your understanding.

-Microsoft Windows is a trademark or registered trademark of Microsoft Corporation in the United States and other countries.

-All other company names and product names mentioned are trademarks or registered trademarks of their respective companies. The © and ™ marks are not explicitly stated in this document.

-Third-Party Library Notice

This software uses GNU libstdc++ (libstdc++.so.5). GNU libstdc++ is distributed under the terms of GNU General Public License version 2 with the "Runtime Library Exception. The full text of the GNU GPL can be obtained from the following URL:https://www.gnu.org/licenses/old-licenses/gpl-2.0.html

How to Obtain the Source Code

The source code for GNU libstdc++ is provided as part of GNU GCC (GNU Compiler Collection). It can be obtained through the following methods:

GNU GCC Official Website:

https://gcc.gnu.org/pub/gcc/releases/

*Note: libstdc++.so.5 is included in the gcc-3.2.x series

GNU FTP Mirror:

https://ftp.gnu.org/gnu/gcc/

User Rights

Under the GNU GPL, users are guaranteed the following rights.:

The right to obtain and modify the library source code

The right to relink this software using a modified version of the library

This software is designed to allow users to relink with newer versions of libstdc++. For information about relinking procedures, please contact us.

Note: This software uses libstdc++ as a dynamic link library. The license of this software itself is not affected by the libstdc++ LGPL license.

[Disclaimer Regarding the Use of Debian GNU/Linux]

This product utilizes Debian GNU/Linux as a Live OS environment that boots from a USB memory device. Our proprietary software, VaccineUSB3 Boot Scan, operates within this environment. The following is a disclaimer regarding the use of Debian GNU/Linux.

1. About the Debian Distribution

This product includes the Debian GNU/Linux distribution, which consists of numerous independent open-source software packages.

-Hagiwara Solutions makes no guarantees regarding the operation, performance, or compatibility of Debian or its included packages.

2. Source Code Availability

For packages included in this product that are subject to copyleft licenses such as the GPL, source code is made available under the following conditions:

-The source code will be provided upon request from the customer.

-Please contact the following email address for requests:vsolsupport@hagisol.co.jp

-Actual expenses such as media and shipping costs may be charged for source code distribution.

-The source code will be available for a period of **three (3) years** from the date the product is sold or distributed.

-Hagiwara Solutions does not guarantee the performance or operation of the provided source code.

-We bear no responsibility for any modifications made to the source code by the customer.

3. License Compliance

-It is the customer’s responsibility to comply with the license terms of Debian and its included packages.

-The obligation to fulfill redistribution requirements for licenses such as the GPL and LGPL lies with the customer.

-Hagiwara Solutions assumes no legal responsibility for any license violations.

4. Security Updates

-No security updates will be provided for the Debian environment included in this product.

-Hagiwara Solutions is not liable for any damage caused by security vulnerabilities.

-Customers are responsible for implementing appropriate security measures.

5. Package Operation

-Hagiwara Solutions is not liable for any damage caused by malfunctions of open-source packages included in this product.

-We are also not responsible for issues arising from incompatibilities between packages.

6. Scope of Support

-Technical support is not provided for Debian or any of its included packages.

-Our support covers **VaccineUSB3 Boot Scan** only.

-For questions regarding Debian, please consult the Debian Project or community support resources.

7. System Modifications

-Hagiwara Solutions is not responsible for any malfunctions caused by changes to the Debian system included in this product (e.g., package installation/removal, configuration changes).

8. Redistribution Notice

-If this product is redistributed or sold to a third party, you must comply with the license terms of the included open-source software.

-In particular, redistribution of GPL-covered packages may require the distributor (i.e., the customer) to also provide the source code.

[Copyright Notice]

-Debian GNU/Linux

Debian GNU/Linux and related packages included in this product are distributed in accordance with their respective license terms. For details, please refer to the documentation for each package under `/usr/share/doc/`.

-VaccineUSB3 Boot Scan

This software is provided under a proprietary license by Hagiwara Solutions.

Vaccine USB3 USB Boot Scan
Manual
Published May 2025
Publisher: Hagiwara Solutions Co., Ltd.