

Harmony PSA6

Windows System Setting

User Guide

EIO0000005686.00
08/2025

Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this document are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owner.

This document and its content are protected under applicable copyright laws and provided for informative use only. No part of this document may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.

Table of Contents

Safety Information	4
About the Document	5
Cybersecurity	7
Cybersecurity Guideline	7
System Settings	8
Main Features	8
At First Startup.....	8
Windows Update	9
How to Enable Automatic Updates.....	10
How to Enable Security Intelligence Updates.....	11
User Account.....	13
How to Create a Standard User Account.....	13
UEFI BIOS	16
UEFI BIOS Setup Menu.....	16
Changing the UEFI BIOS Password	17
In-Band ECC (only Atom model)	17
Launcher.....	17
Starting the Launcher	17
Buzzer.....	18
Write Filter.....	19
Shell	20
Power	21
System.....	22
Recovery USB	22
Window Locker	23
Edit	25
TPM.....	26
Trellix Software	26
Introduction	26
Installation	27
Searching for the Manual	27
Uninstallation.....	28
System Backup.....	29
System Recovery.....	31

Safety Information

Important Information


Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.





The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.



This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

 DANGER
DANGER indicates a hazardous situation which, if not avoided, will result in death or serious injury.

 WARNING
WARNING indicates a hazardous situation which, if not avoided, could result in death or serious injury.

 CAUTION
CAUTION indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

NOTICE
NOTICE is used to address practices not related to physical injury.

Please Note

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

About the Document

Document Scope

This document describes how to set up the system configuration of the Harmony PSA6, which is used in industrial or factory automation systems.

This document is intended for users who design systems, or install and maintain components.

Validity Note

This document is valid for Harmony PSA6.

The characteristics of the products described in this document are intended to match the characteristics that are available on www.se.com. As part of our corporate strategy for constant improvement, we may revise the content over time to enhance clarity and accuracy. If you see a difference between the characteristics in this document and the characteristics on www.se.com, consider www.se.com to contain the latest information.

Product Related Information

Refer to Harmony PSA6 Hardware Guide.

General Cybersecurity Information

In recent years, the growing number of networked machines and production plants has seen a corresponding increase in the potential for cyber threats, such as unauthorized access, data breaches, and operational disruptions. You must, therefore, consider all possible cybersecurity measures to help protect assets and systems against such threats.

To help keep your Schneider Electric products secure and protected, it is in your best interest to implement the cybersecurity best practices as described in the [Cybersecurity Best Practices](#) document.

Schneider Electric provides additional information and assistance:

- Subscribe to the Schneider Electric [security newsletter](#).
- Visit the [Cybersecurity Support Portal](#) web page to:
 - Find Security Notifications.
 - Report vulnerabilities and incidents.
- Visit the [Schneider Electric Cybersecurity and Data Protection Posture](#) web page to:
 - Access the cybersecurity posture.
 - Learn more about cybersecurity in the cybersecurity academy.
 - Explore the cybersecurity services from Schneider Electric.

Product Related Cybersecurity Information

Refer to [Cybersecurity](#), page 7.

Related Documents

Title of documentation	Reference number
Cybersecurity Best Practices	Refer to General Cybersecurity Information, page 5.
HMI/IPC Cybersecurity Guide	EIO0000004948 (ENG)
Harmony PSA6 Hardware Guide	EIO0000005603 (ENG) EIO0000005604 (FRE) EIO0000005605 (GER) EIO0000005606 (SPA) EIO0000005607 (ITA) EIO0000005608 (CHS)

You can download the manuals related to this product, such as the software manual, from the Schneider Electric download center (www.se.com/ww/en/download).

Information on Non-Inclusive or Insensitive Terminology

As a responsible, inclusive company, Schneider Electric is constantly updating its communications and products that contain non-inclusive or insensitive terminology. However, despite these efforts, our content may still contain terms that are deemed inappropriate by some customers.

Trademarks

Microsoft® and Windows® are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Intel®, Core™ and Atom® are registered trademark of Intel Corporation.

QR Code is a registered trademark of DENSO WAVE INCORPORATED in Japan and other countries.

Product names used in this manual may be the registered trademarks owned by the respective proprietors.

Cybersecurity

Cybersecurity Guideline

Use this product inside a secure industrial automation and control system. Total protection of components (equipment/devices), systems, organizations, and networks from cyber attack threats requires multi-layered cyber risk mitigation measures, early detection of incidents, and appropriate response and recovery plans when incidents occur. For more information about cybersecurity, refer to the Harmony HMI/iPC Cybersecurity Guide.

<https://www.se.com/ww/en/download/document/EIO0000004948/>

WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Change default passwords at first use to help prevent unauthorized access to device settings, controls and information.
- Disable unused ports/services and default accounts, where possible, to minimize pathways for malicious attacks.
- Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).
- Apply the latest updates and hotfixes to your Operating System and software.
- Use cybersecurity best practices (for example: least privilege, separation of duties) to help prevent unauthorized exposure, loss, modification of data and logs, interruption of services, or unintended operation.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

System Settings

What's in This Chapter

Main Features	8
At First Startup	8
Windows Update	9
User Account	13
UEFI BIOS.....	16
In-Band ECC (only Atom model).....	17
Launcher	17
TPM	26
Trellix Software	26
System Backup	29
System Recovery	31

Main Features

Multilanguage Support

The operating system is installed with the following languages.

English (default), Japanese, French, German, Spanish, Italian, Portuguese, Russian, Swedish, Simplified Chinese and Traditional Chinese.

UEFI BIOS

This product is equipped with the UEFI BIOS. Refer to UEFI BIOS, page 16.

Launcher

Utility that displays icons for registered files, programs, and various settings, which you can start with a simple touch operation. The Launcher already includes the icons of necessary settings for this product such as Write Filter. Refer to Launcher, page 17.

Security Support

Secure Boot is enabled on this product. Additionally, as TPM comes as part of this product, it can easily support an encryption tool, BitLocker. Furthermore, by purchasing a Trellix license you can realize a more secure environment. Refer to TPM, page 26 and Trellix Software, page 26.

NOTE: Enable BitLocker to make your system more secure.

At First Startup

The first time you start up the product, the initial settings for the operating system is executed. Connect a keyboard and mouse before powering up, then follow the on-screen instructions to define the settings.

NOTE:

This product requires the sign-in password to be set in order to reduce the risks of unauthorized access, intrusion and infection of malicious software. The conditions for the sign-in password are as follows.

No. of characters: From the usable characters below, at least 3 types and at least 8 characters are required. The sign-in password should not contain the character strings used in the account name.

Usable characters:

- Uppercase letters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
- Lowercase letters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
- Base 10 digits (0 through 9)
- Non-alphanumeric characters (special characters): (~!@#\$%^&* _+=`|()\{} []:;"<>,.?/) Currency symbols such as the Euro or British Pound are not counted as special characters for this policy setting.
- Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.
- It is not possible to recover a lost username and password.

⚠ CAUTION**EQUIPMENT DAMAGE**

Regardless of the Write Filter setting, do not turn off the power immediately after turning on the product.

Failure to follow these instructions can result in injury or equipment damage.

NOTICE**LOSS OF DATA**

Do not turn off the power during initial setup.

Failure to follow these instructions can result in equipment damage.

NOTICE**ACCESS LOSS**

Store your device's username and password information in a secure location.

Failure to follow these instructions can result in equipment damage.

Windows Update

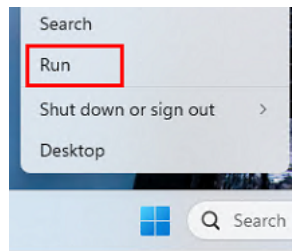
For safer use of this product, use Windows Update to keep the operating system up to date. In the factory default state, the automatic security update function is disabled. For the procedure on how to enable it, refer to the following.

NOTE:

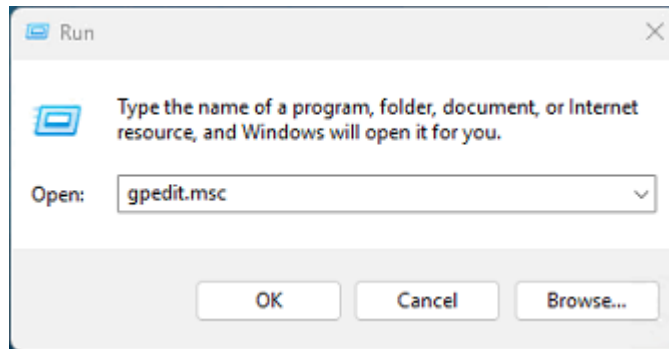
- If Write Filter is enabled, disable the Write Filter and update the operating system.
- For environments where security updates cannot be applied regularly, we recommend purchasing the optional Trellix license and implementing the permission list method for security protection.

How to Enable Automatic Updates

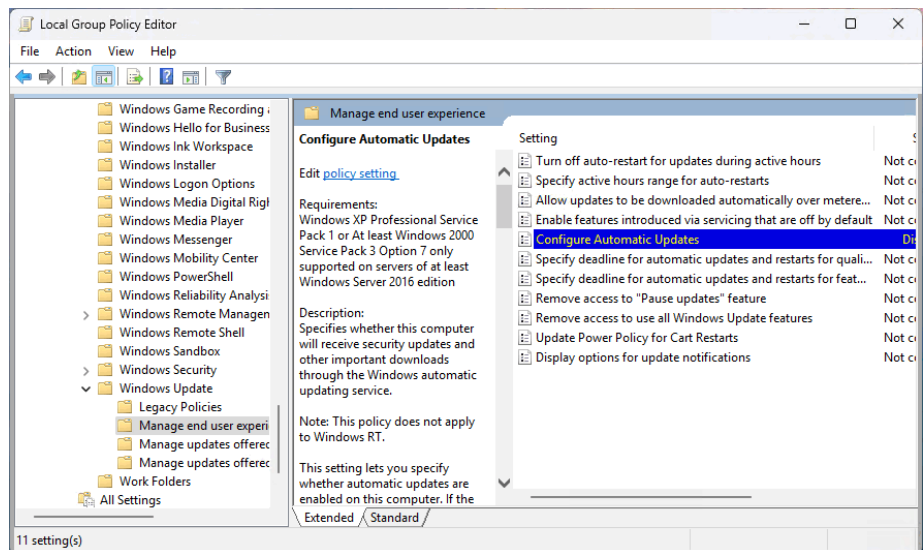
1. Right-click the **Start** button, and Select **Run**.



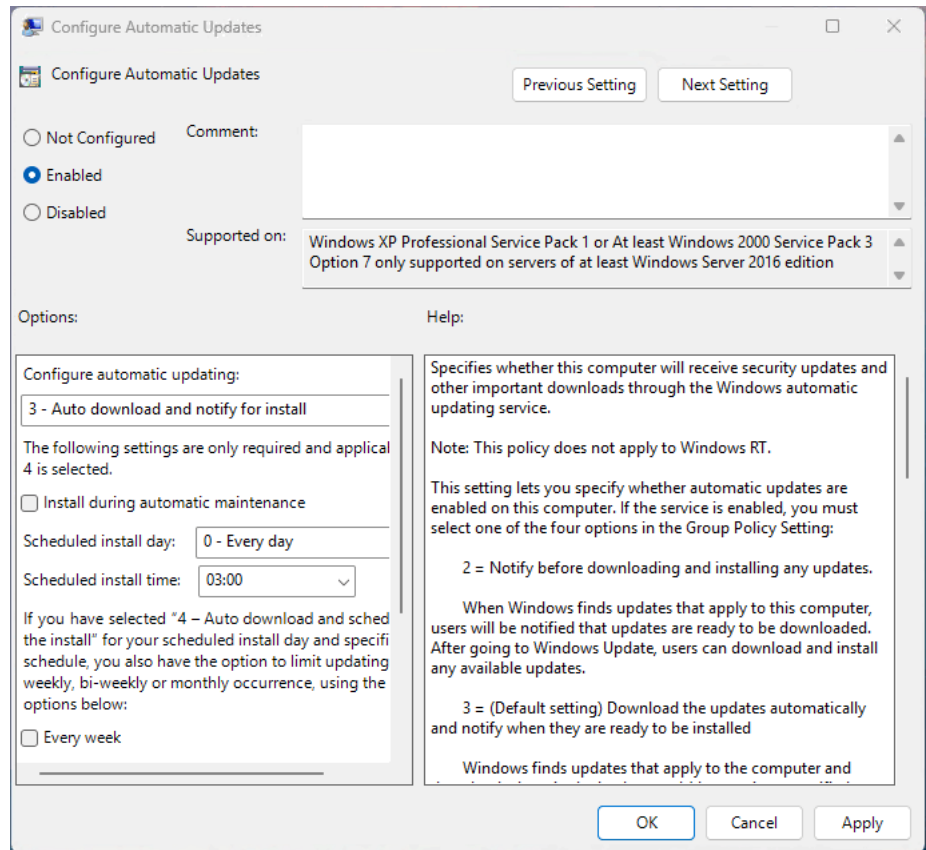
2. Enter `gpedit.msc`, and select **OK**.



3. Open **Computer Configuration > Administrative Templates > Windows Components > Windows Update > Manage end user experience > Configure Automatic Update**.

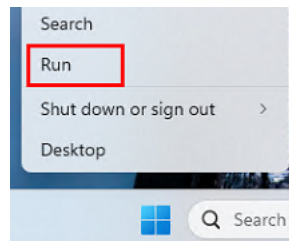


4. Change the setting from **Disabled** to **Enabled**, select the settings in **Options** for your environment, and select **OK**.

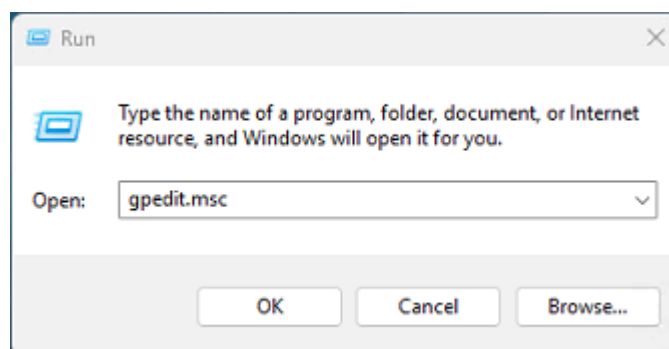


How to Enable Security Intelligence Updates

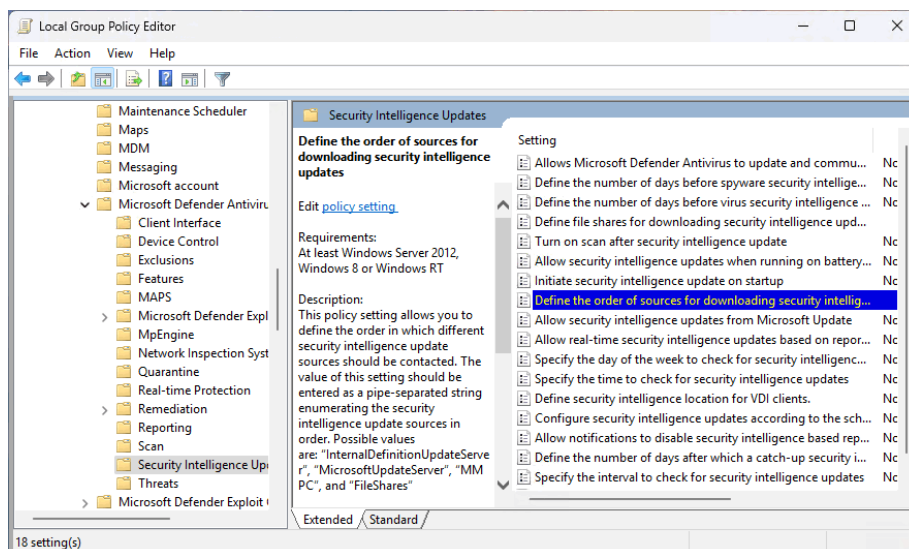
1. Right-click the **Start** button, and Select **Run**.



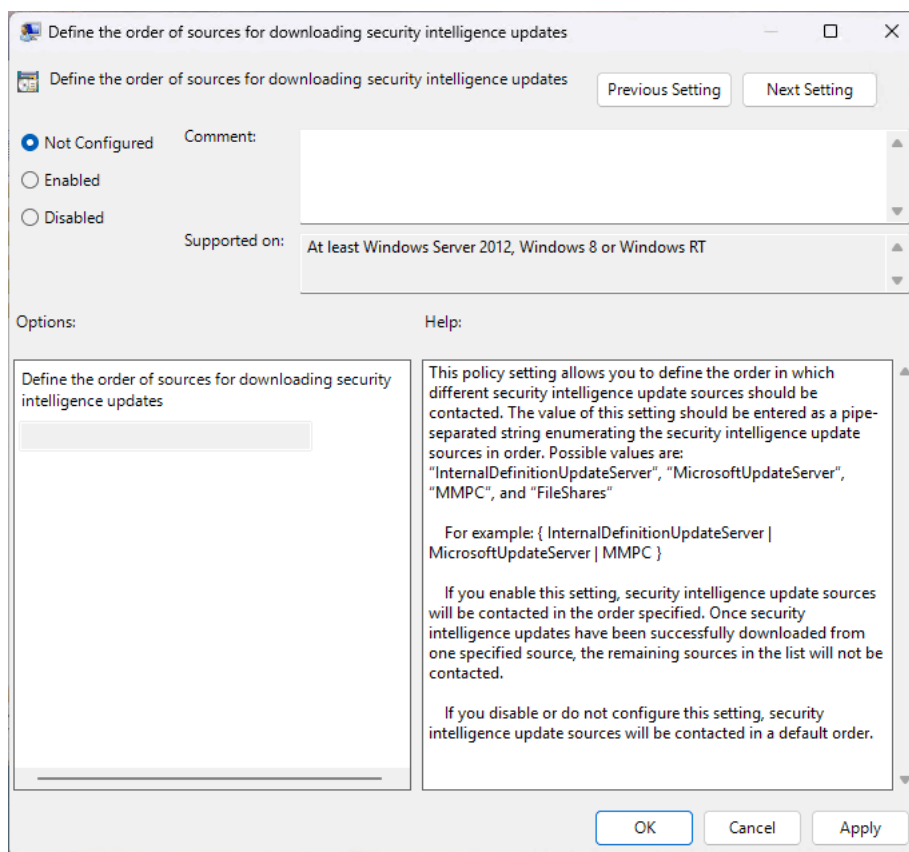
2. Enter `gpedit.msc`, and select **OK**.



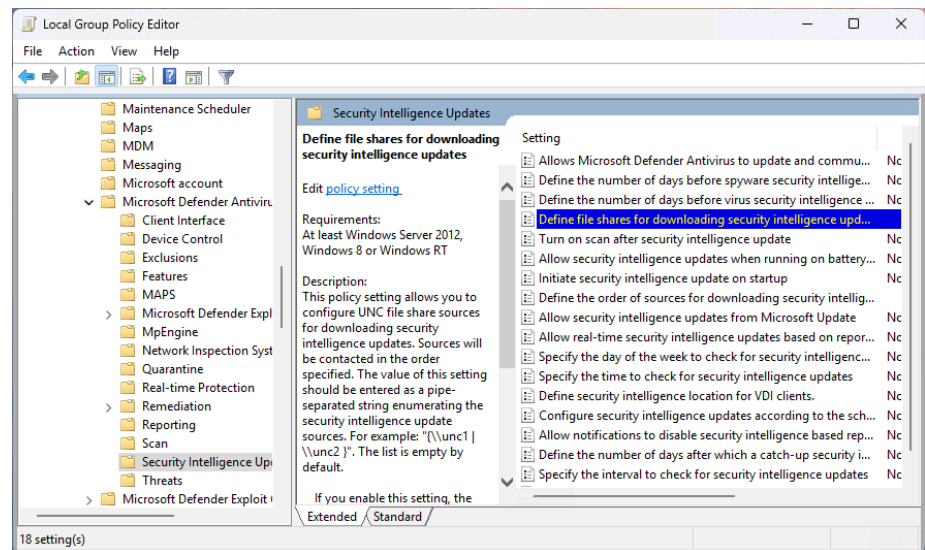
- Open **Computer Configuration > Administrative Templates > Windows Components > Microsoft Defender Antivirus > Security Intelligence Updates > Define the order of sources for downloading security intelligence updates**.



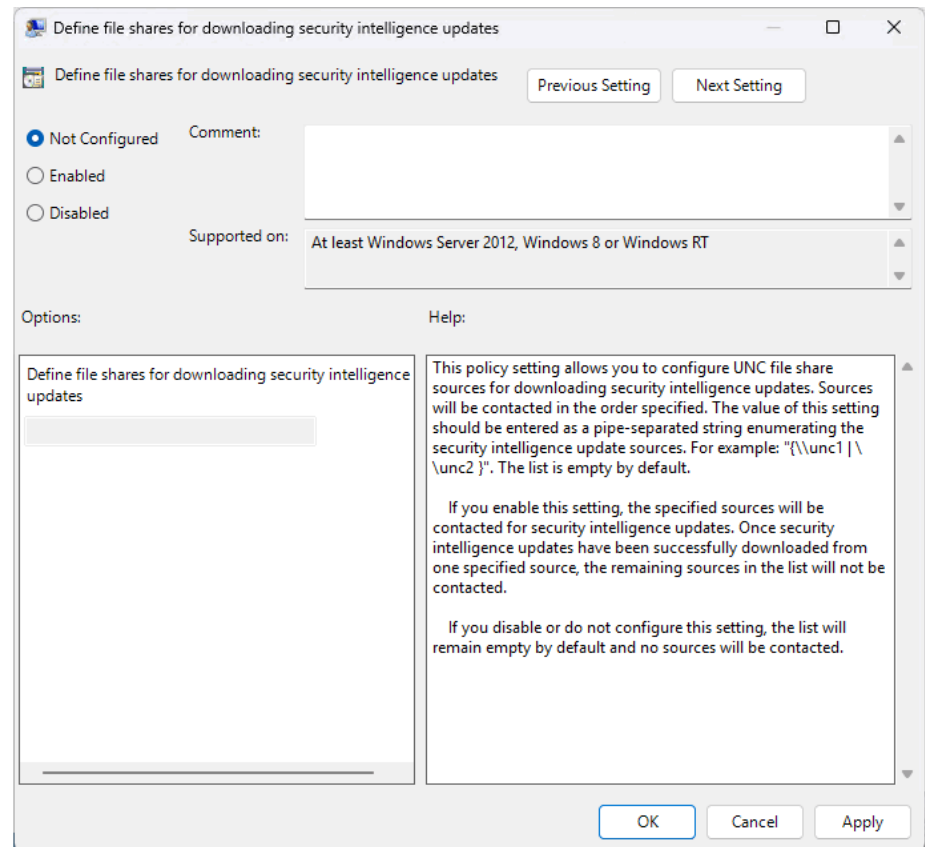
- Change the setting from **Disabled** to **Not Configured**, and select **OK**.



- Open **Computer Configuration > Administrative Templates > Windows Components > Microsoft Defender Antivirus > Security Intelligence Updates > Define the file shares for downloading security intelligence updates**.



- Change the setting from **Disabled** to **Not Configured**, and select **OK**.



User Account

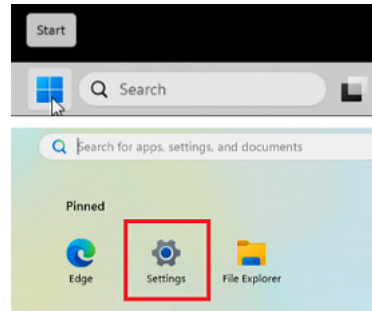
How to Create a Standard User Account

A user account with an Administrator account type should only be used when system configuration changes are required.

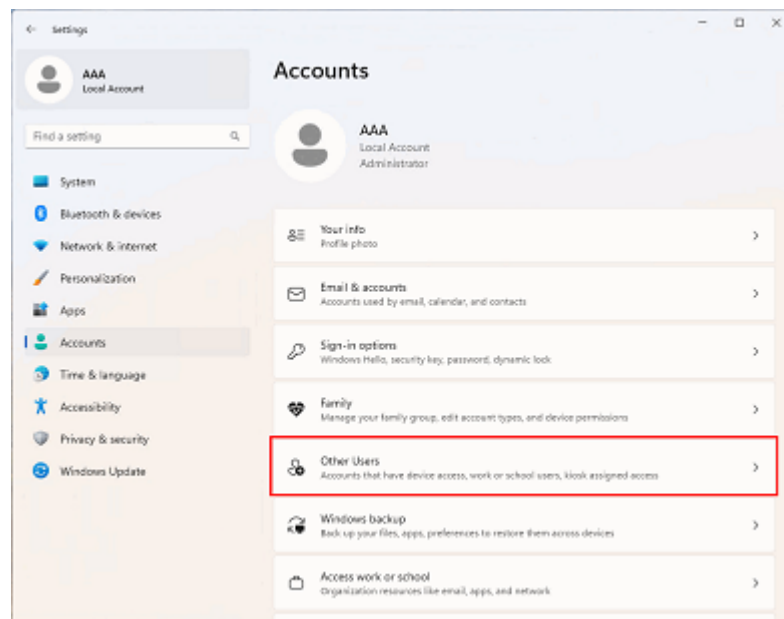
For normal operations, use a user account with a Standard User account type.

The following shows how to create an account with a Standard User account type.

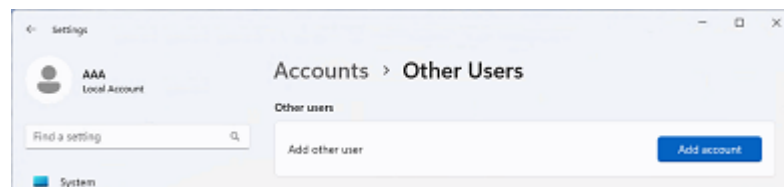
1. Open **Settings**.



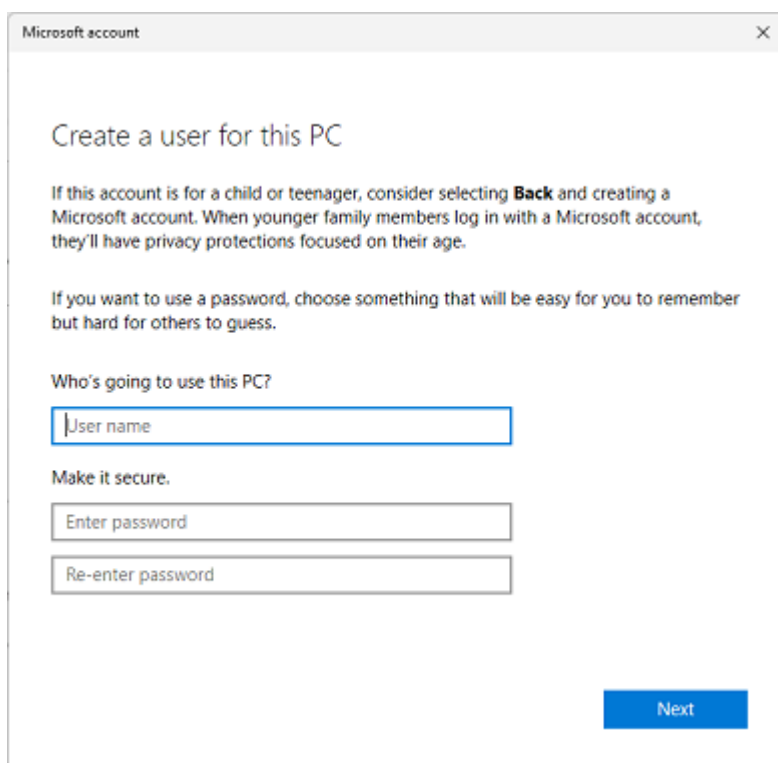
2. Select **Accounts**.
3. Select **Other Users**.



4. Select **Add account**.



5. Enter a username and a password, and select **Next**.



Microsoft account

Create a user for this PC

If this account is for a child or teenager, consider selecting **Back** and creating a Microsoft account. When younger family members log in with a Microsoft account, they'll have privacy protections focused on their age.

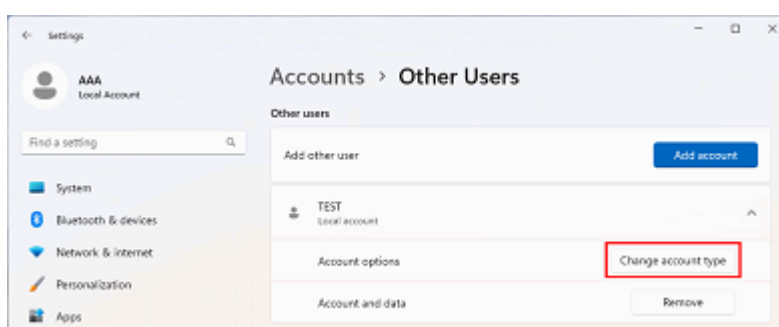
If you want to use a password, choose something that will be easy for you to remember but hard for others to guess.

Who's going to use this PC?

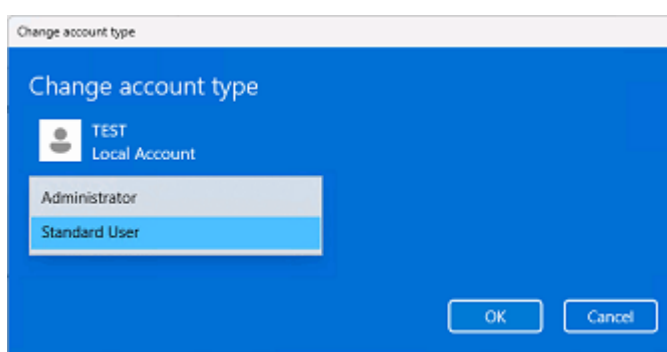
Make it secure.

Next

6. Select the user account created, and then **Change account type**.

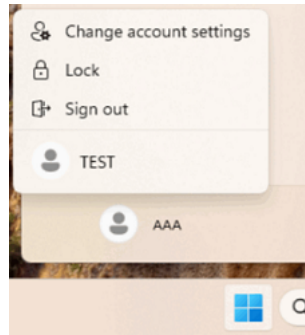


7. Select **Standard User**.



8. Select **Start** and then the account icon.

9. You can select the user account created.



UEFI BIOS

UEFI BIOS Setup Menu

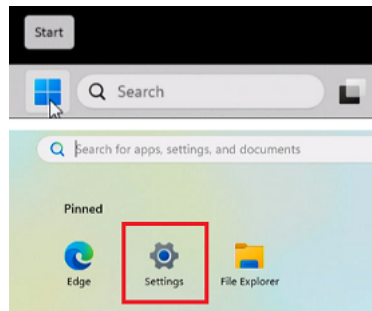
To enter the UEFI BIOS setup menu:

1. Turn on the product.
2. While the boot screen is displayed, press the [DEL] key.
3. Enter the password (default password: Pw#12345)*¹.
4. The BIOS screen will display.

*¹ Make sure you change the default password. Refer to [Changing the UEFI BIOS Password](#), page 17.

Depending on the settings, such as Fast Boot, you may not be able to enter the BIOS setup menu using the above procedure. If that is the case, display the setup menu using the following steps.

1. Turn on the product and start up normally.
2. Open **Settings**.



3. Select **Recovery**.
4. From **Advanced startup**, select **Restart now**.
5. Select **Troubleshoot**.
6. Select **Advanced options**.
7. Select **UEFI Firmware Settings**.
8. Select **Restart**.
9. Enter the password (default password: Pw#12345)*¹.

*¹ Make sure you change the default password. Refer to [Changing the UEFI BIOS Password](#), page 17.

Changing the UEFI BIOS Password

For security reasons, make sure you change the default password (Pw#12345). The following describes the procedure for changing the password.

NOTE:

- The password requires at least 8 characters.
- Even if the battery is removed for replacement or any other reason, the UEFI BIOS password will not reset.

NOTICE

ACCESS LOSS

Store your UEFI BIOS password information in a secure location.

Failure to follow these instructions can result in equipment damage.

1. Display the BIOS screen. Refer to UEFI BIOS Setup Menu, page 16.
2. Select **Security**.
3. Select **Administrator Password**.
4. The **Enter Current password** dialog box appears. Enter the current password.
5. The **Create New Password** dialog box appears. Enter the new password.
6. The **Confirm New Password** dialog box appears. Enter the same password as step 5.
7. Press the [F4] key.
8. Select **Yes** in the **Save & Exit Setup** dialog box.
9. The product is restarted.

In-Band ECC (only Atom model)

The CPU in this product supports In-Band ECC. The following describes the procedure for enabling and disabling In-Band ECC (default: **Disabled**).

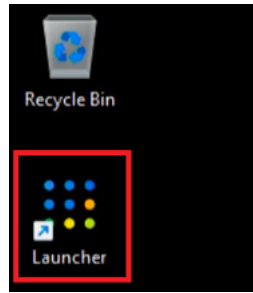
1. Display the BIOS screen. Refer to UEFI BIOS Setup Menu, page 16.
2. Select **Advanced > CPU Configuration > In-Band ECC Support**.
3. Select **Enabled** or **Disabled**.
4. Press the [F4] key.
5. Select **Yes** in the **Save & Exit Setup** dialog box.
6. The product is restarted.

Launcher

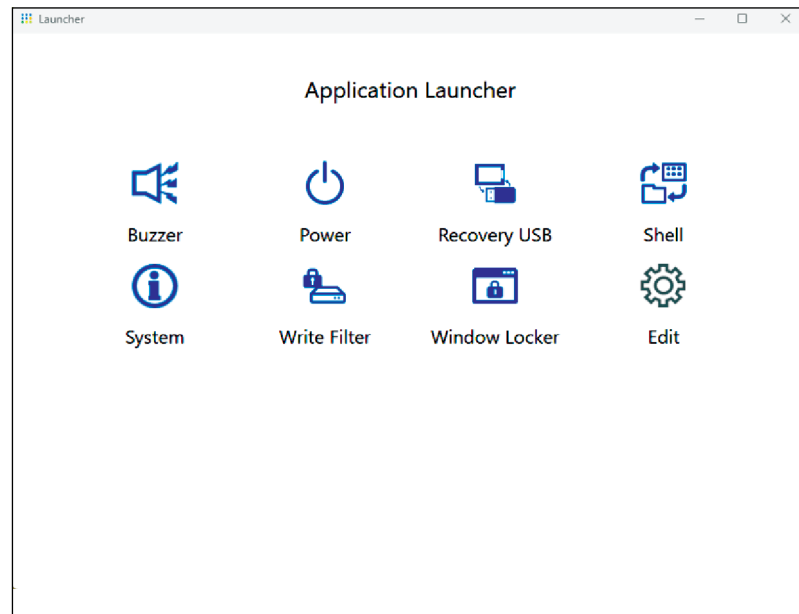
Starting the Launcher

The Launcher is a utility that you can set up to start programs and settings. The Launcher allows for convenient touch-screen operation by displaying icons for registered various settings.

You can start the Launcher from the shortcut icon on the desktop.



Launcher top screen

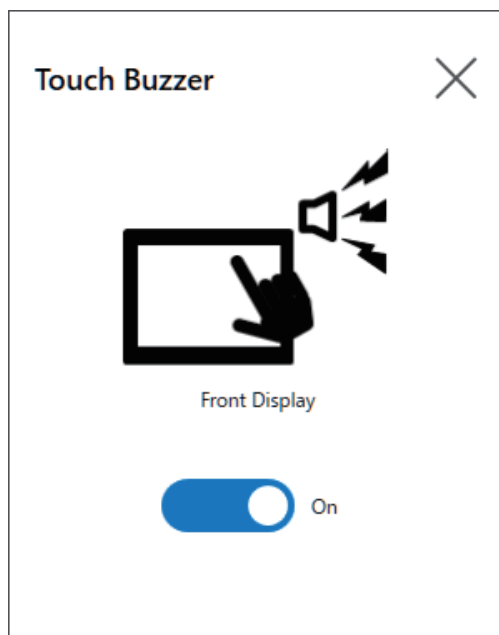
**NOTE:**

- To customize the Launcher, refer to [Edit](#), page 25.
- Download the latest version of the utility for Harmony PSA6 from the following URL to keep the Launcher up to date.
www.se.com/ww/en/download
- When the Launcher is already installed, it is overwritten. If you used **Edit** to customize the Launcher, customize again.

Buzzer

Sets the sound on/off when you perform touch-panel operations.

Default: **On**



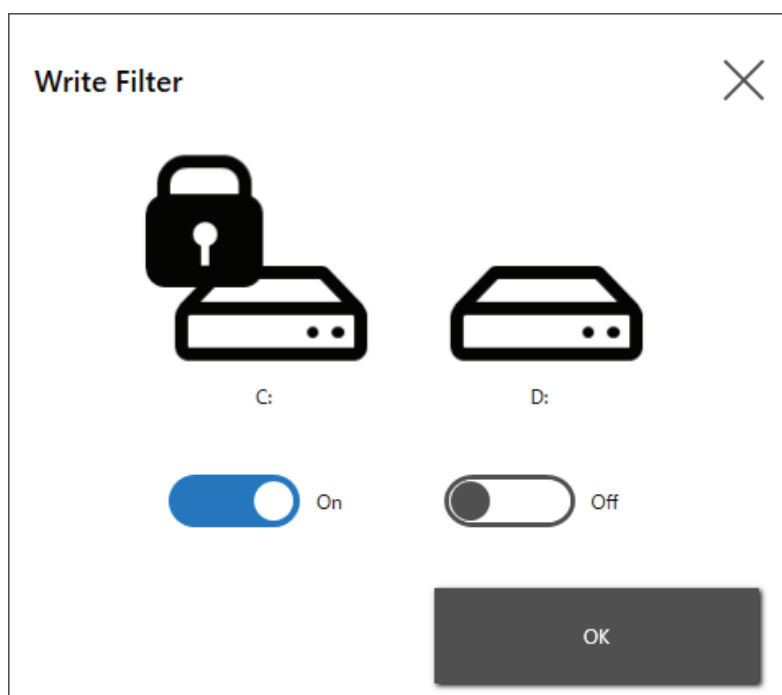
NOTE: The buzzer sound is prioritized by the UEFI BIOS settings over the Launcher's **Buzzer** setting. Make sure the setting is **Enabled** in **Advanced > Onboard Device > Beep On** (default: **Enabled**). Otherwise, even if the setting for the Launcher's **Buzzer** is **ON**, the buzzer will not make a sound.

Write Filter

This function prevents writing to the system disk.

By enabling the Write Filter, you can prevent damage to the system disk and shortened life of disk due to excessive writes.

Default: **Off** (Disable)



NOTE:

- When only one volume is set to the Write Filter, the screen displays just that one volume.
- When changing settings (such as settings in the Launcher, and when adding drivers, changing the registry, or installing applications), disable the Write Filter. If the Write Filter is enabled, any changes to settings will be erased when the operating system is restarted. After changes to settings are complete, we recommend that you re-enable the Write Filter.
- If the Write Filter is enabled, the fast startup function is disabled.

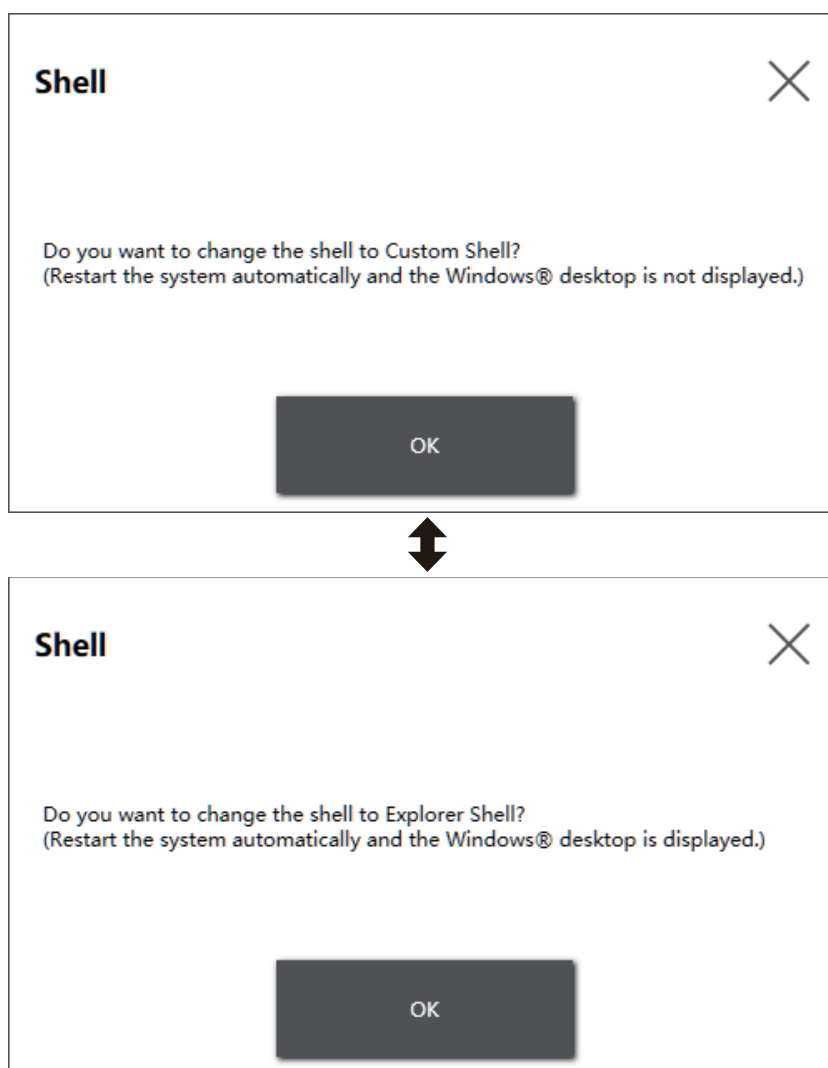
⚠ CAUTION
EQUIPMENT DAMAGE Regardless of the Write Filter setting, do not turn off the power immediately after turning on the product. Failure to follow these instructions can result in injury or equipment damage.

NOTICE
LOSS OF DATA Do not turn off the power while writing to a storage device that is not protected by the Write Filter. Failure to follow these instructions can result in equipment damage.

Shell

You can hide the Windows® desktop by switching from the Explorer Shell to the Custom Shell. By doing so, you can suppress Windows® functions such as the Control Panel.

Custom Shell: The Windows® desktop is not displayed. After the product starts up, the Launcher landing page is displayed.
Explorer Shell: The Windows® desktop is displayed.

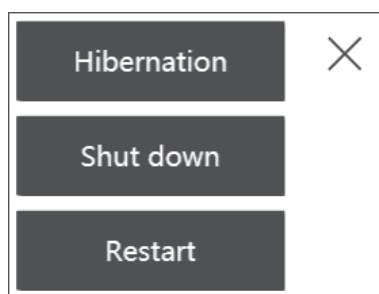


NOTE:

- Install applications in the Explorer Shell.
- When changing to the custom shell, the features shown in the Explorer Shell (such as Windows® desktop, Start menu, taskbar) cannot be used.

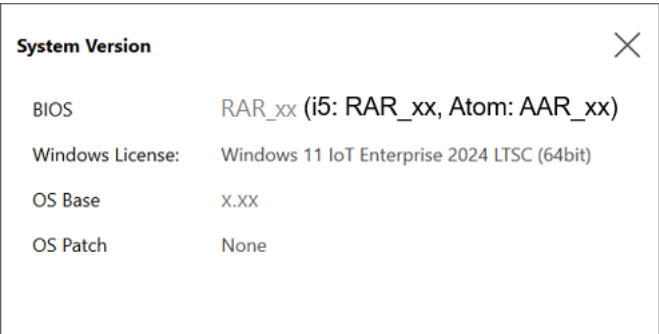
Power

Use this feature to operate the product's power supply.



System

Displays the version of the product firmware, BIOS, and operating system.

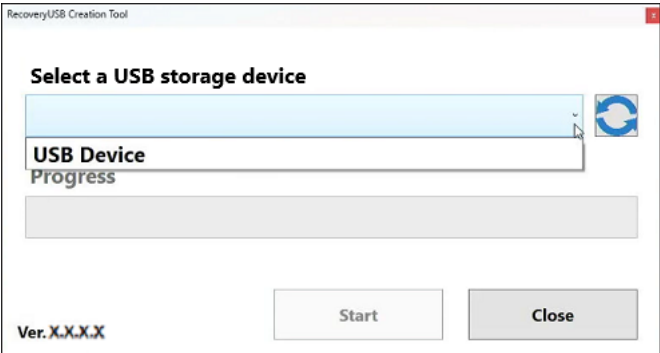


Recovery USB

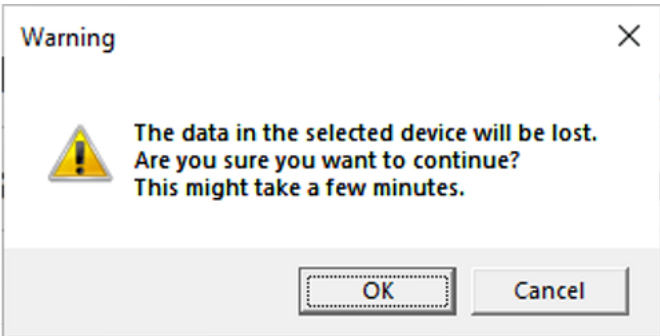
This feature is to create a recovery USB to restore and back up the system. During the creation of the recovery USB, the operating system image at the factory default is automatically stored in the USB. With this image, you can restore the factory default image, refer to [System Recovery](#), page 31. If you need to back up your current system, refer to [System Backup](#), page 29.

Prepare a commercially available USB memory with a size of 32 GB or more, to create a backup USB.

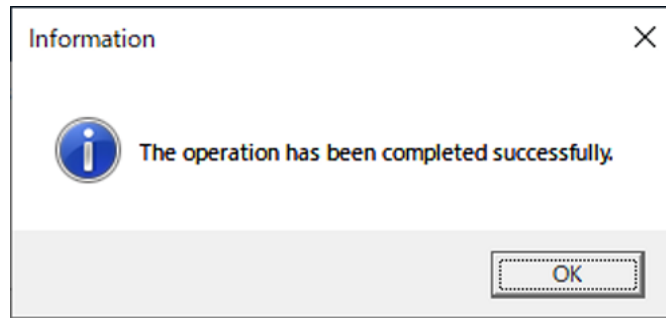
- 1. Disconnect all connected devices from the product.
- 2. Insert a commercially available USB memory.
- 3. Open the Launcher.
- 4. Select the **Recovery USB** icon.
- 5. Select the USB memory in **Select a USB storage device**.



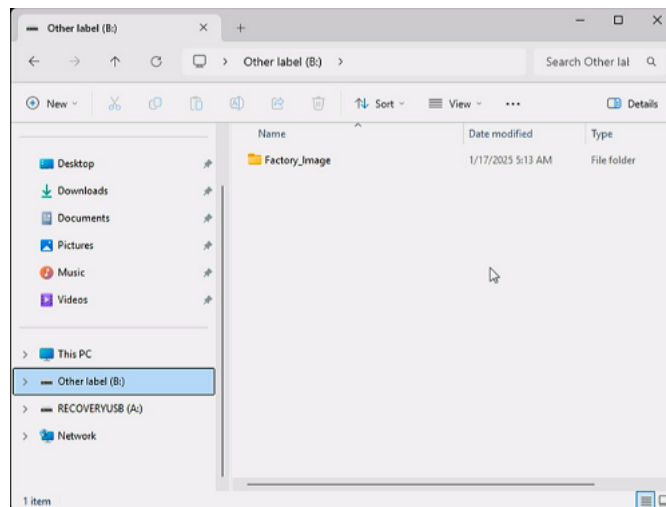
- 6. Select **Start**.
- 7. In the confirmation screen, select **OK**.



8. When completed, the following message appears and select **OK**.

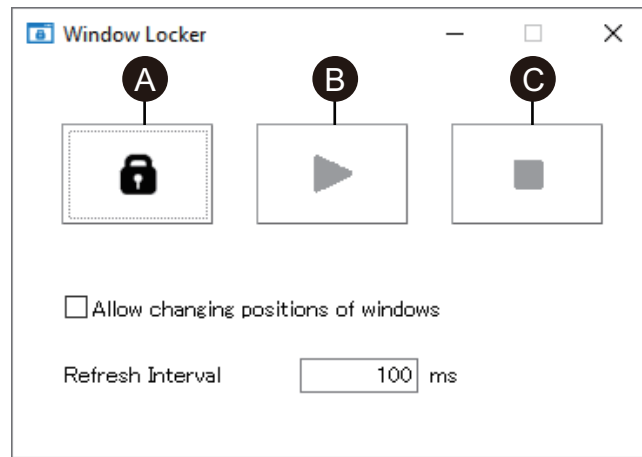


9. Close the **Recovery USB** screen.
10. After the operation, the drive labeled "Other label" is create in the USB. The operating system image at the factory default is stored in the folder named "Factory image" in the drive.



Window Locker

If for some reason the connection to the external display is disconnected, the displayed application window may move to a different position or to a different display altogether. By using the Window Locker, when applications start up you can display them in a fixed position, so that after reconnecting external displays you can view the application window in the same display and position as before being disconnected.



- A. LOCK
- B. PLAY
- C. STOP

1. Start up all application windows to define their display positions and which display to use.

NOTE: If you save the display position while the application is in full screen mode, the window may not display properly.

2. Move each window to the desired display position.
3. Run Window Locker from the Launcher.
4. Select **LOCK** to save the display position.

NOTE:

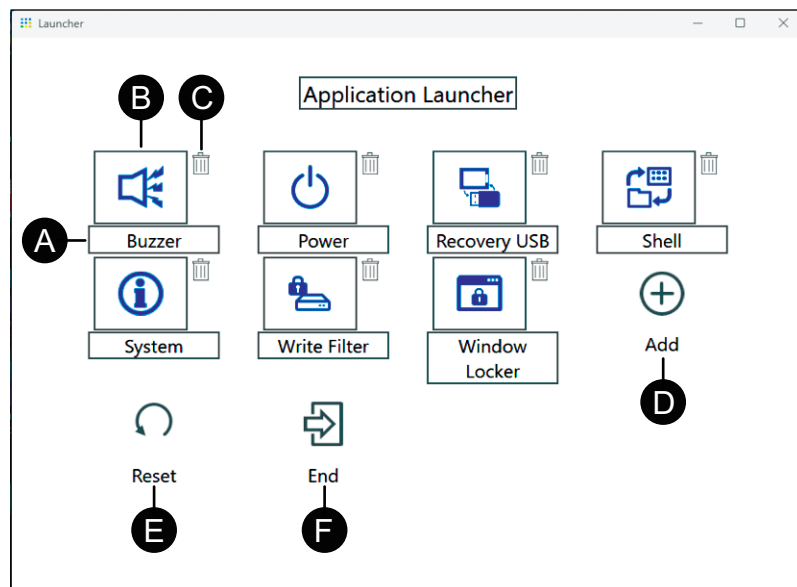
- Window sizes are fixed to the size when **LOCK** is pressed.
 - By entering an amount of time in the **Refresh Interval**, if you change the window size or position after **PLAY** is pressed, the window will return to its original size and position when the time elapses. If you select the **Allow changing positions of windows** check box, after **PLAY** is pressed, even when the entered time elapses the window will remain in the changed position, but the window will return to its original size.
 - The **Refresh Interval** input range is from 100 ms to 86,400,000 ms (24 hours).
5. Select **PLAY**. Every time the application window opens, it automatically appears in the saved position.

NOTE:

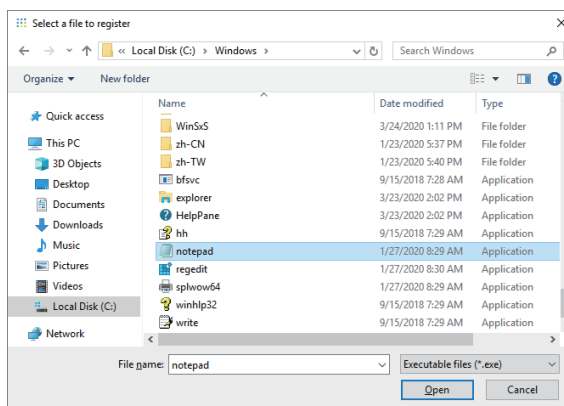
- When saving window positions, ensure that the Write Filter is disabled. If the Write Filter is enabled, the saved information will be erased when the operating system is restarted. After you finish saving, we recommend that you re-enable the Write Filter.
- To temporarily release the fixed position, select **STOP**. To return to the fixed position, select **PLAY**.
- After saving the window display position, connecting or disconnecting an external display loses the display positions. If you add a connection or disconnect, save the display position again. However, if you return to the same configuration as before connecting or disconnecting the external display, the saved display position information is applied so you do not have to set the display information again.
- You may not be able to normally save the display position of windows with the same name, or applications such as Windows® Media Player, which have multiple internal windows.
- After saving the window display position with Window Locker, changing the screen placement or resolution could cause the window to display incorrectly. If you change the screen settings, save the window display position again.

Edit

You can use this function to customize the icons displayed on the Launcher. You can also add any application to the display.



- You can change the name of the icon.
- You can change the application displayed. Click to display a screen where you can select the application's exe file. Select the exe file of the application you want to display.



- C. Click this mark to remove the icon.
- D. Add the application displayed. Click to display a screen where you can select the application's exe file. Select the exe file of the application you want to display.
- E. Returns the icon display to the factory default settings.
- F. This button releases Edit mode.

TPM

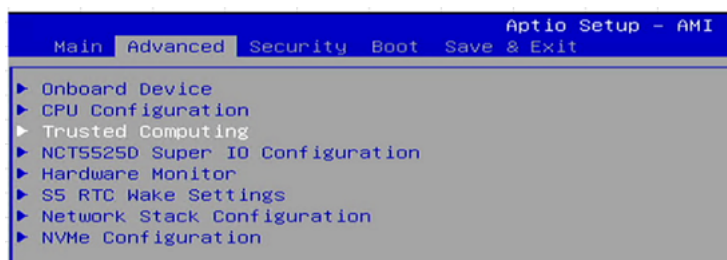
This product comes equipped with the TPM 2.0 module.

Enable or disable TPM in accordance with the laws, regulations, and standards of each country.

TPM is enabled by default.

NOTE: Enable BitLocker to make your system more secure.

1. Turn on the product.
2. While the boot screen is displayed, to disable TPM, press [CTRL]+[D]; to enable TPM, press [CTRL]+[E].
3. The product is restarted.
4. After the setting is updated, when TPM is enabled, **Trusted Computing** is displayed in the BIOS **Advanced** menu. When it is disabled, **Trusted Computing** is not displayed.



Trellix Software

Introduction

By purchasing the optional Trellix license (HMIYP6LSMCA) and using the Trellix software, you can increase the security on this product. For the software functions and how to use the software, refer to the following URL and search for the associated manual.

<https://docs.trellix.com/bundle>

The following describes how to install the software and search for the manual.

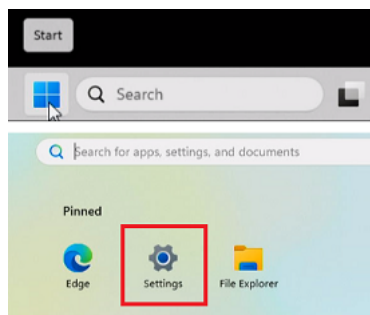
Installation

1. Insert the Trellix license USB storage to the product.
2. Run **setup.exe** in USB storage.
3. The installer is executed.

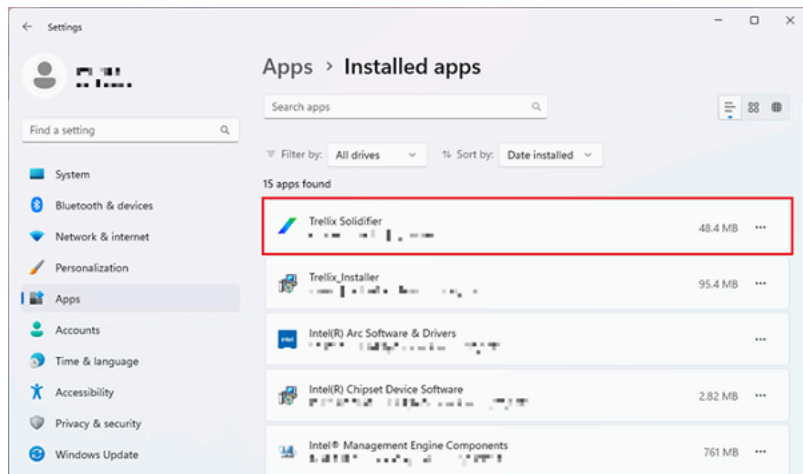
Searching for the Manual

The following describes how to search for the Trellix software manual. Check the software version beforehand.

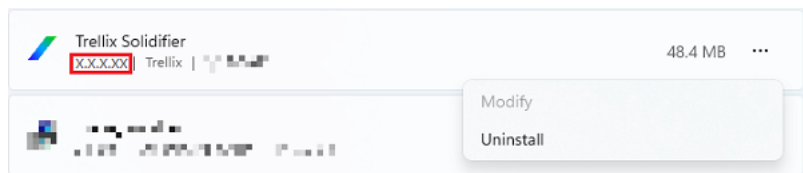
1. Select the **Settings** button.



2. Select **Apps**.
3. In **Apps**, select **Trellix Solidifier**.



4. Confirm the version.



5. Close the **Apps** screen.
6. Display <https://docs.trellix.com/bundle> in the web browser.

- Search for **Application and Change Control** corresponding to the version confirmed in step 4.

NOTE: The Trellix provided on our optional Trellix license USB storage supports an unmanaged environment (called standalone or self-managed) as defined by Trellix. It does not support a managed Trellix ePolicy Orchestrator - On-prem environment. Please be aware of this when reading the manuals.

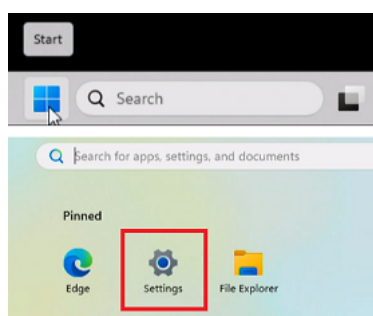
Uninstallation

When uninstalling, you need to uninstall the following two applications.

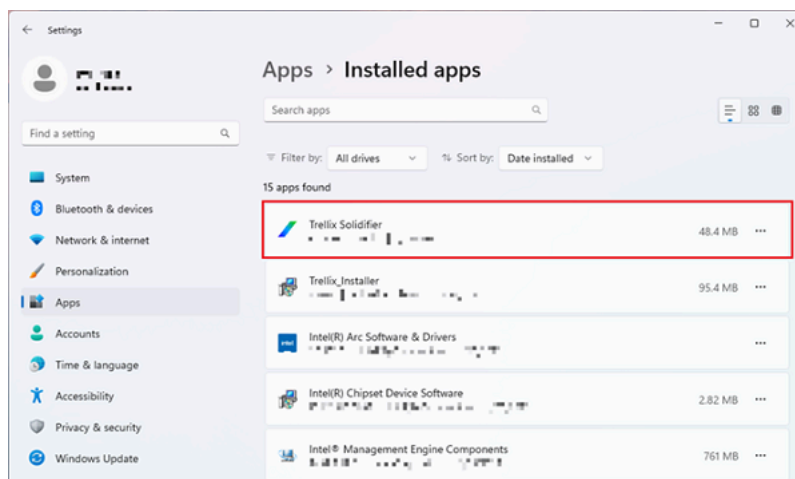
- Trellix Solidifier
- Trellix Installer

Steps for uninstalling is as follows.

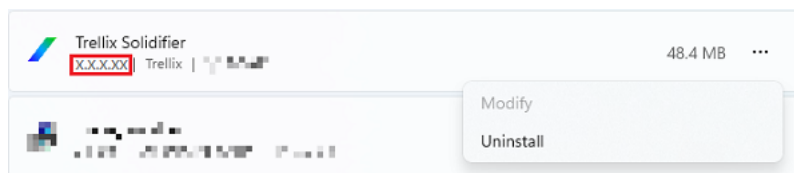
- Select the **Settings** button.



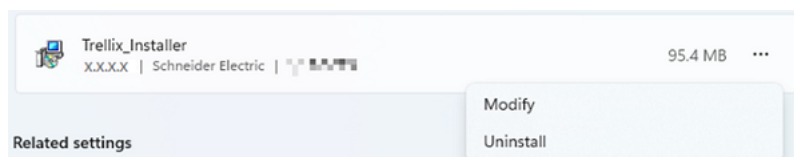
- Select **Apps**.
- In **Apps**, select **Trellix Solidifier**.



- Select **Uninstall**.



- Follow the same steps and select **Trellix_Installer**, and then **Uninstall**.

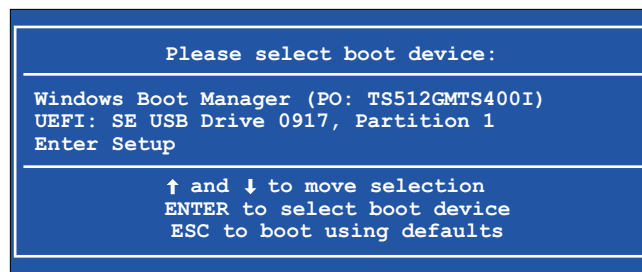


System Backup

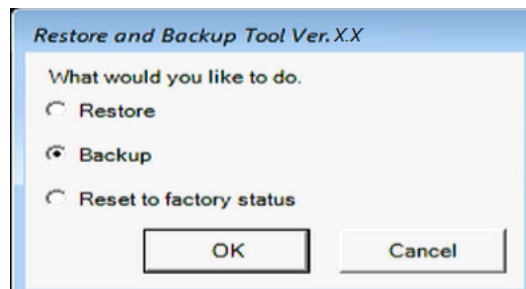
After product setup, backing up the system is recommended. Prepare a commercially available USB memory with a size of 32 GB or more, to create a backup USB.

NOTE: Right after the hibernation is performed, system backup or recovery will not run properly. Perform system backup or recovery after shutting down the product.

1. Prepare a commercially available USB memory.
2. Create a recovery USB with the **Recovery USB** in the Launcher. Refer to Recovery USB, page 22.
3. Insert the recovery USB created in step 2 into the product.
4. Turn on the product.
5. While the boot screen is displayed, press the [F7] key.
6. Enter the password (default password: Pw#12345).
7. From the following screen, select the recovery USB.



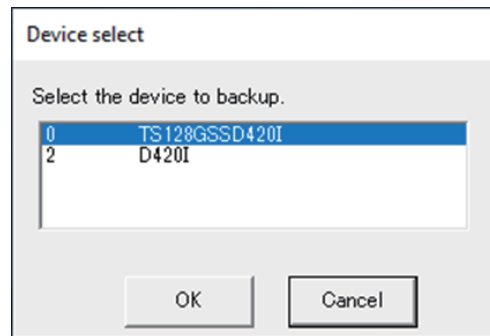
8. Select **Backup > OK**.



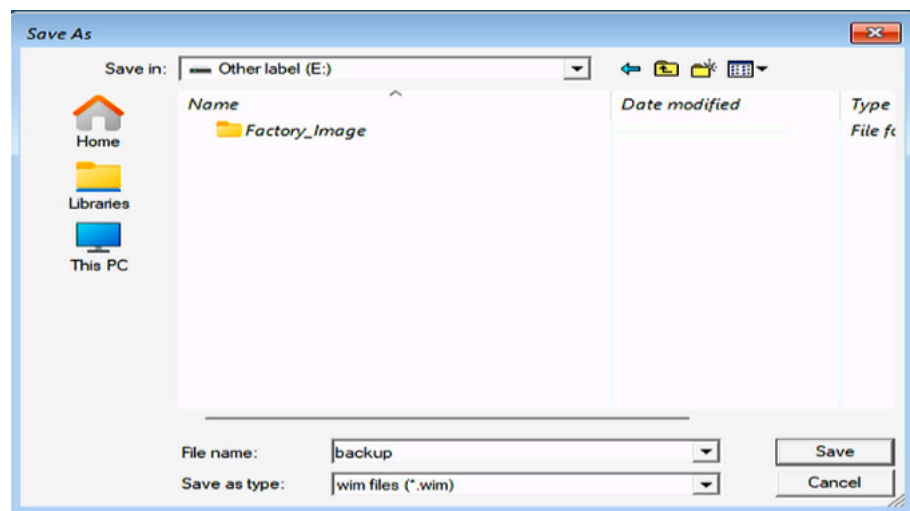
NOTE:

- If the "Factory image" folder where the factory default image is stored remains in the USB under the "Other label" drive, **Reset to factory status** is displayed.
- After restoring your system image in the product, the factory default image will be lost. Even if you perform **Recovery USB** in the Launcher, the factory default image will be no longer created in the USB.

9. Select the disk to backup. Only C drive can be backed up. If several storage devices are shown in the dialog box, select the storage device of C drive. If there is only one storage device, the following screen does not appear and skip to step 10.

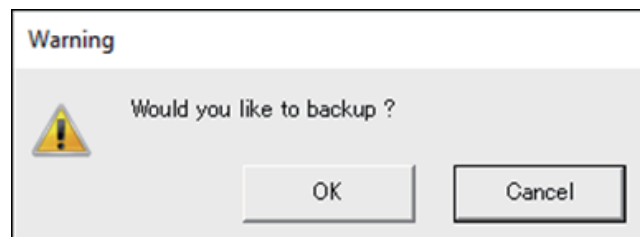


10. Select the drive labeled "Other label", enter a file name, and select either **Save** or **Open**.

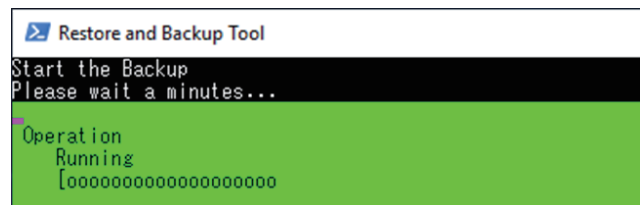


NOTE: Do not create the backup image in the "Factory image" folder.

11. In the confirmation screen, select **OK**.



12. Backup begins.



13. After backup is complete, the following screen is displayed. Remove the backup USB from the product, and then select **Restart** or **Shutdown**.

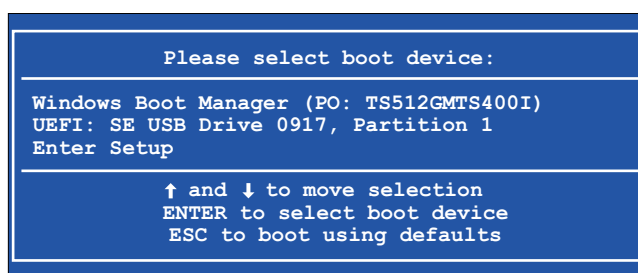


System Recovery

To restore the system, a recovery USB is required. Prepare a recovery USB created with **Recovery USB** in the Launcher. Refer to *Recovery USB*, page 22.

NOTE: Right after the hibernation is performed, system backup or recovery will not run properly. Perform system backup or recovery after shutting down the product.

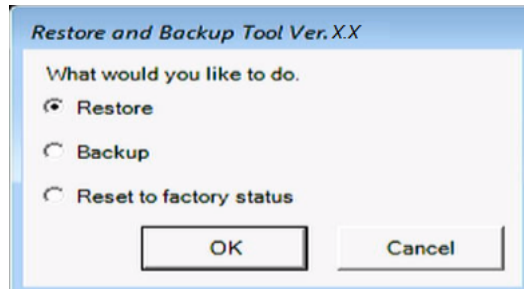
1. Insert the recovery USB to this product.
2. Turn on the product.
3. While the boot screen is displayed, press the [F7] key.
4. Enter the password (default password: Pw#12345).
5. Select the recovery USB.



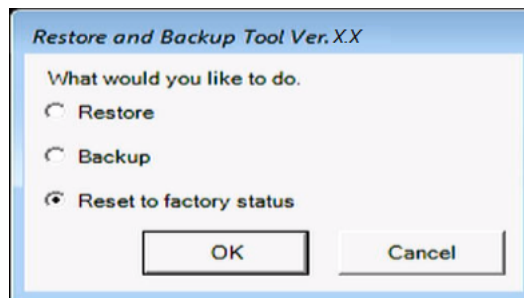
6. To restore the system image backed up with **Recovery USB** in the Launcher, select **Restore** > **OK**.

NOTE:

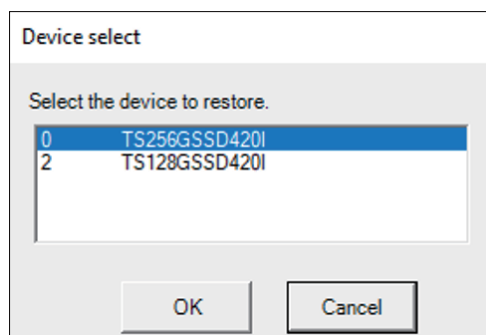
- If the "Factory image" folder where the factory default image is stored remains in the USB under the "Other label" drive, **Reset to factory status** is displayed.
- **Reset to factory status** resets only the operating system image. It does not reset the UEFI BIOS settings.
- After restoring your system image in the product, the factory default image will be lost. Even if you perform **Recovery USB** in the Launcher, the factory default image will be no longer created in the USB.



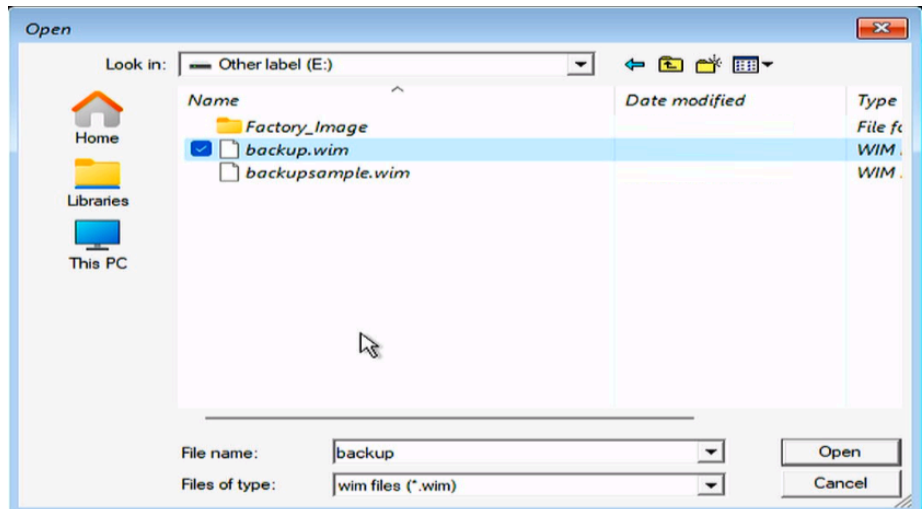
To restore the factory default image, select **Reset to factory status** > **OK**.



7. Select the disk to recover. If there is only one storage, the following screen does not appear and skip to step 8.



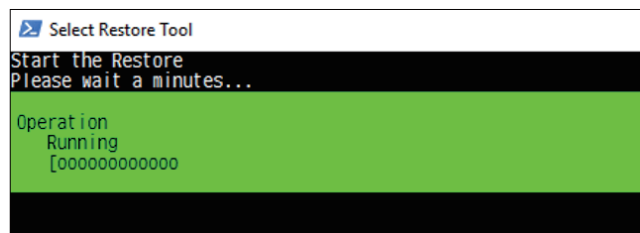
8. If there is one wim file stored directly under "Other label", or restore the factory default, go to step 9. If there are two or more wim files stored directly under "Other label", select the "Other label" > the wim file to restore > select **Open**.



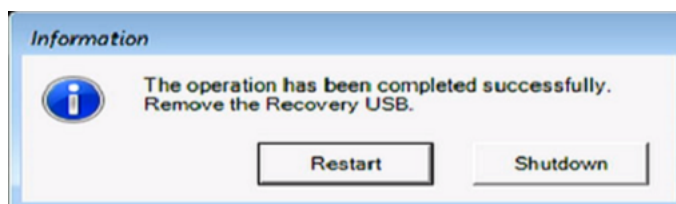
9. In the confirmation screen, select **OK**.



10. Recovery begins.



11. After recovery is complete and the following screen is displayed, remove the recovery media from the product and select either **Restart** or **Shutdown**.



Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

As standards, specifications, and design change from time to time, please ask for confirmation of the information given in this publication.

© 2025 – Schneider Electric. All rights reserved.

EIO0000005686.00