OMRON

Industrial PC Platform

NY-series

NYB/NYP Industrial PC

Security Guidelines User's Manual

NYB□□
NYP□□

SYSMAC
always in control

W661-E2-01

NOTE

No patent liability is assumed with respect to the use of the information contained herein. Moreover, because OMRON is constantly striving to improve its high-quality products, the information contained in this manual is subject to change without notice. Every precaution has been taken in the preparation of this manual. Nevertheless, OMRON assumes no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained in this publication.

Trademarks

- Sysmac and SYSMAC are trademarks or registered trademarks of OMRON Corporation in Japan and other countries for OMRON factory automation products.
- Windows is a registered trademark of Microsoft Corporation in the USA and other countries.
- The SD and SDHC logos are trademarks of SD-3C, LLC.
- CFAST is a registered trademark of CompactFlash Association.
- Intel, the Intel Logo, Celeron and Intel Core are trademarks of Intel Corporation in the U.S. and/or other countries.

Other company names and product names in this document are the trademarks or registered trademarks of their respective companies.

Copyrights

Microsoft product screen shots reprinted with permission from Microsoft Corporation.

Introduction

Thank you for using the OMRON Industrial PC Platform.
This manual contains information to understand the security initiatives of OMRON for its NYB/NYP IPC products.This document proposes the security measures that users of an IPC products should take on their own. It describes the security measures that you can implement using NYB/NYP series IPC Units.
Please read this document together with the Security Guideline for Factory Automation System and related manuals. Please read this manual and make sure you understand the Security Guidelines before implementing your IPC to a network.
Keep this manual in a safe place where it will be available for reference during operation.

Intended Audience

This manual is intended for the following personnel, who must also have knowledge of software programming (a software engineer or the equivalent).

- Personnel in charge of introducing Factory Automation systems.
- Personnel in charge of designing Factory Automation systems.
- Personnel in charge of software design for Factory Automation systems.
- Personnel in charge of installing and maintaining and programming Factory Automation systems.
- Personnel in charge of managing Factory Automation systems and facilities.

Applicable Products

This manual covers the following Industrial PC products:

Product	Model
Industrial Box PC	NYB□□
Industrial Panel PC	NYP□□

Sections in this Manual

CONTENTS

Section 5 Safely Disposing of Equipment

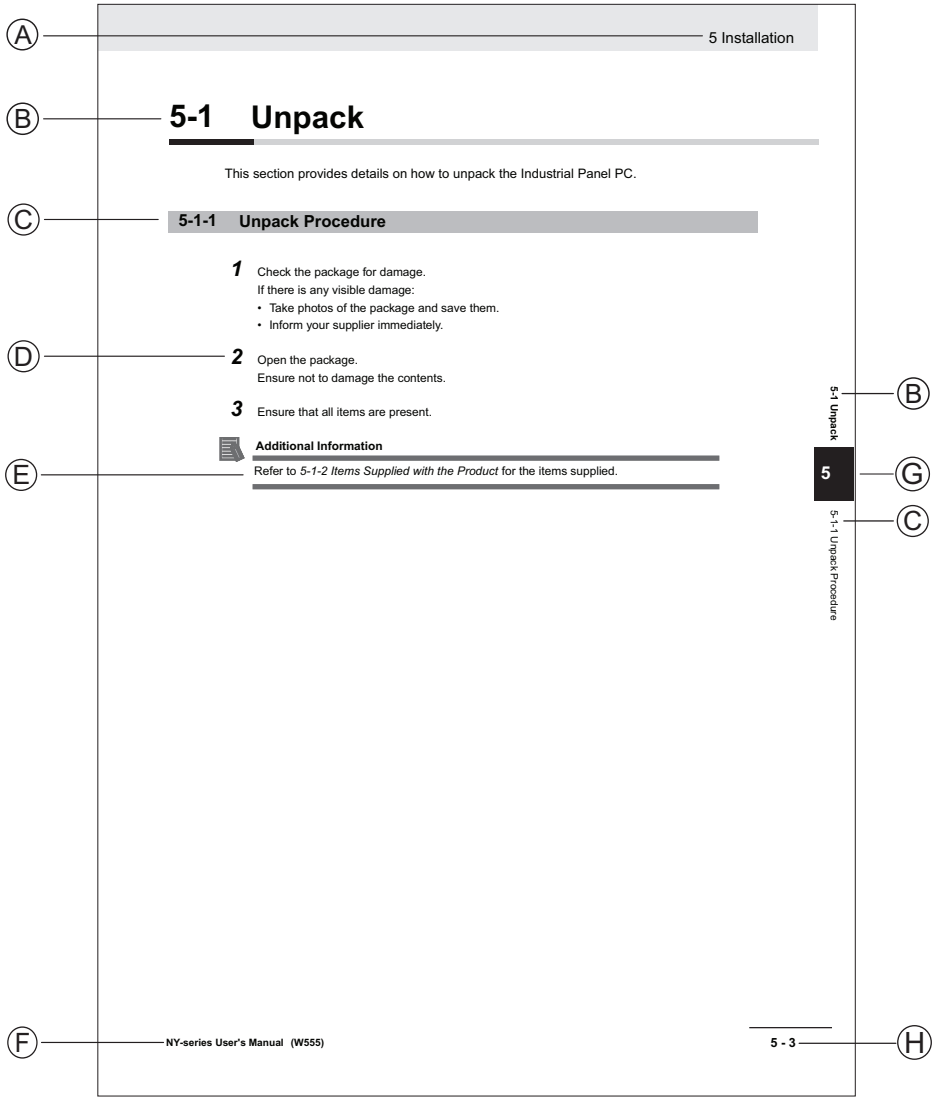
Index

Manual Information

This section provides information about this manual.

Page Structure

The following page structure is used in this manual.



Note: This illustration is provided as a sample. It will not literally appear in this manual.

Item	Explanation	Item	Explanation
A	Level 1 heading	E	Special Information
B	Level 2 heading	F	Manual name
C	Level 3 heading	G	Page tab with the number of the main section
D	Step in a procedure	H	Page number

Special Information

Special information in this manual is classified as follows:

Precautions for Safe Use

Precautions on what to do and what not to do to ensure safe usage of the product.

Precautions for Correct Use

Precautions on what to do and what not to do to ensure proper operation and performance.

Additional Information

Additional information to read as required.
This information is provided to increase understanding or make operation easier.

Version Information

Information on differences in specifications and functionality between different versions.

Related Manuals

The following manuals are related. Use these manuals for reference.

Related Industrial PC Manuals

This table contains the related manuals of Industrial PC products.

Manual name	Cat. No.	Model numbers	Application	Description
NY-series Industrial Box PC Hardware User's Manual	W553	NYB	Learning all basic information about the Industrial Box PC. This includes introductory information with features, hardware overview, software overview, specifications, mounting, wiring, connecting, operating and maintaining the Industrial Box PC. Mainly hardware information is provided.	An introduction to the Industrial Box PC is provided along with the following information: • Overview • Hardware • Software • Specifications • Installation • Operating Procedures • Maintenance
NY-series Industrial Panel PC Hardware User's Manual	W555	NYP	Learning all basic information about the Industrial Panel PC. This includes introductory information with features, hardware overview, software overview, specifications, mounting, wiring, connecting, operating and maintaining the Industrial Panel PC. Mainly hardware information is provided.	An introduction to the Industrial Panel PC is provided along with the following information: • Overview • Hardware • Software • Specifications • Installation • Operating Procedures • Maintenance
NY-series Operating Systems and Software Utilities Manual	W616	NYB NYP	Learning all software related information about the Industrial PC. This includes introductory information, installation, operating procedures and maintenance. Mainly software information is provided.	An introduction to the IPC is provided along with the following information: • Overview • Software • Specifications • Installation • Operating Procedures • Maintenance
NY-series Software Development Kit User's Manual	W633	NYB NYP	Learning all basic information and features of the SDK for the OMRON IPCs. Mainly API function details are provided.	An introduction to the SDK is provided along with the following information: • Software for developers • Industrial PC System API • Industrial Monitor API • Installation • Operating Procedures

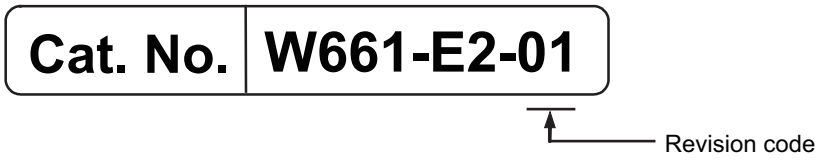
Related Security Manuals

This table contains the related OMRON Security manuals.

Manual name	Cat. No.	Model numbers	Application	Description
Security Guideline for Factory Automation System	P162	NYB NYP	Learning the concept of security for FA systems in general.	An introduction to the security guidelines is provided along with the following information: • Product Security Initiatives at OMRON • Necessity and Purpose of Security Response • Implementation of Risk Assessment • Security Measures

Revision History

A manual revision code appears as a suffix to the catalog number on the front and back covers of the manual.



Revision code	Date	Revised content
01	November 2025	First release

1

Overview

This section provides general information about the Security Guidelines for your Industrial PC.

1-1 Intended Use

This Security Guidelines User's Manual is intended to be used as a guideline for the safe installation and use of an Omron Industrial PC in an automation environment.
A user can use these Guidelines to implement and maintain security measures to protect Industrial PCs and their network environment.

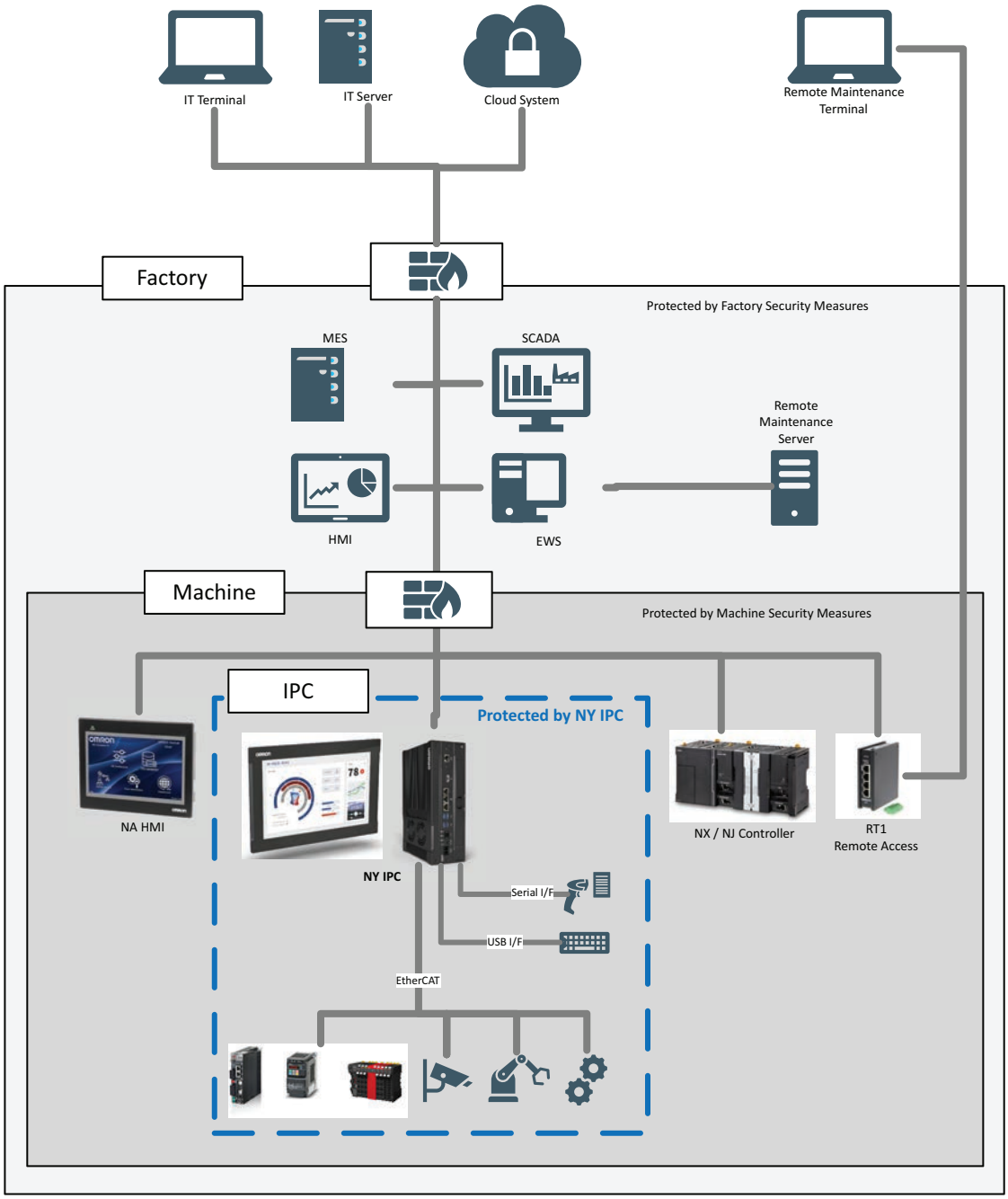
2

Defence-in-Depth

Defence-in-depth is a cybersecurity strategy that employs multiple layers of security controls to protect the Industrial PC Platform systems and data, ensuring that if one layer fails, others remain to defend against threats.

2-1 Operating Environment

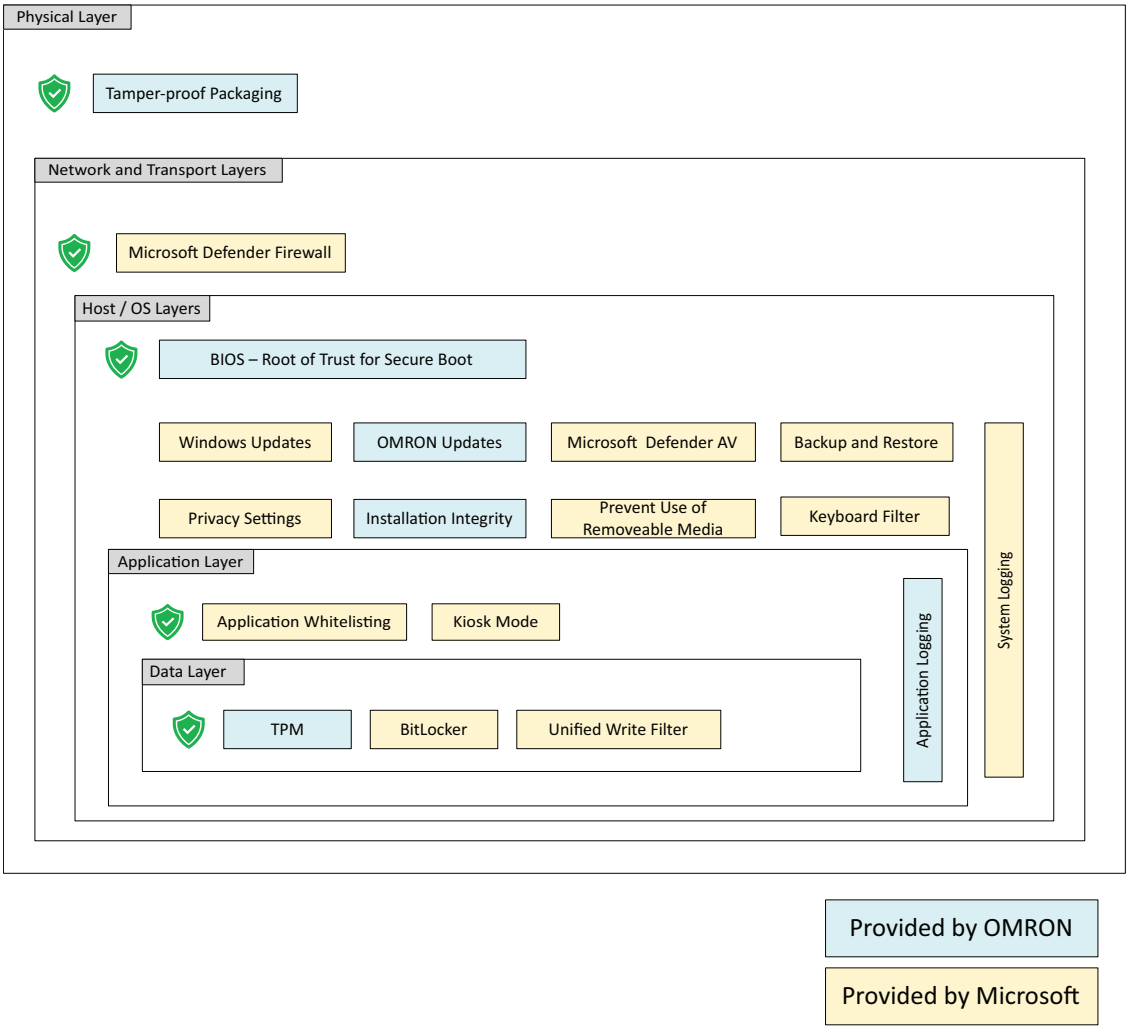
The NYB/NYP Series IPC models provide security protection to devices connected over the fieldbus and peripheral connections directly controlled by the IPC. Security at the higher networking level is provided by the factory or machine system. Security devices such as firewalls and remote connection devices, such as the OMRON RT1 Remote Access Solution provide additional security.



2-2 Security for the Technical Layer

The NYB/NYP IPC Models provide security functions to protect your assets as part of a Defence-in-Depth approach. If an attacker is able to break through one layer of defence, security functions in the layer closest to the assets will maintain the protection of those assets.

The security measures provided by the NYB/NYP IPC Models can have a functional impact on the intended operation of the end system. Some of the provided security measures are not enabled by default. It is recommended that a risk assessment is prepared for the operating environment, to determine which of the security measures provided should be utilised for each use case.
Depending on the operating goal and the identified threat, provide additional Defence-in-Depth by combining the measures described in Security Guideline for Factory Automation System (Cat. No. P162) and the security measures described in this document.



3

Security Functions

Security functions can be divided in general Windows security functions and OMRON specific security functions.

3-1 Windows Security Functions and Configuration

Information on windows Security Functions and the use and configuration of security related software.

3-1-1 Windows Configuration

To ensure optimal security for an industrial product, OMRON has limited the behaviour of some default windows tasks and services. The affected services are either disabled by default or adjusted to run manually rather than automatically in the NYB/NYP Series IPC Models.

Related tasks and services for Windows 11:

Type	Name	Adjusted Status
Service	Connected User Experiences and Telemetry	Manual
Scheduled Task	\Microsoft\Windows\Application Experience\Microsoft Compatibility Appraiser	Disabled
	\Microsoft\Windows\Application Experience\Microsoft Compatibility Appraiser Exp	
	\Microsoft\Windows\Application Experience\Pca-PatchDbTask	
	\Microsoft\Windows\Application Experience\Startu-pAppTask	
	\Microsoft\Windows\ApplicationData\appuriverifierdaily	
	\Microsoft\Windows\ApplicationData\appuriverifierin-stall	
	\Microsoft\Windows\Customer Experience Improve-ment Program\UsbCeip	
	\Microsoft\Windows\Defrag\ScheduledDefrag	
	\Microsoft\Windows\Device Information\Device User	
	\Microsoft\Windows\DiskCleanup\SilentCleanup	
	\Microsoft\Windows\DiskDiagnostic\Microsoft-Win-dows-DiskDiagnosticDataCollector	
	\Microsoft\Windows\Speech\SpeechModelDownload-Task	
	\Microsoft\XblGameSave\XblGameSaveTask	
	\Microsoft\XblGameSave\XblGameSaveTaskLogon	

3-1-2 Microsoft Defender

Microsoft Defender tasks:

- Protection against virus, ransomware and spyware
- Reduces attack surfaces
- Provides managed system maintenance

Microsoft Defender is a powerful tool that offers many security functions including virus and threat protection, firewall and network protections and user account protections.

Microsoft Defender can be configured as part of standard IT integration within your organisation. Ensure that corporate IT governance is met by applying your group policies and typical configuration settings in Microsoft Defender.

In particular, ensure that:

- Microsoft Defender Antivirus is enabled and kept up to date with the latest virus definitions.
- Microsoft Defender Firewall should be enabled to control inbound and outbound traffic to the system.

Microsoft Defender Firewall

In the BIOS of your Industrial PC the section Security changeable BIOS parameters and their factory default values are available.
Microsoft Defender Firewall is enabled by default, with default configuration, in the NYB/NYP Series IPC Models.
Additional settings in Microsoft Defender Firewall:

- Allow an app through firewall.
  If the firewall is blocking an app you need, you can add an exception for that app, or open a specific port
- Firewall notification settings.
  Get notifications when your firewall blocks something
- Advanced settings.
  Allows you to edit or create inbound or outbound rules, connection security rules, and see monitoring logs for the firewall

To view or change settings of Microsoft Defender Firewall:

1 In the Windows Security app on your NYB/NYP IPC, select “Firewall & network protection”

2 Windows Security shows you which type of network you're currently connected to. Usually, your device will only be connected to one network at a time. Select a network profile: “Domain network”, “Private network”, or “Public network”

3 Under “Microsoft Defender Firewall”, confirm that the setting to is set to “On” to enable Windows Firewall. Turning off Windows Firewall could make your device more vulnerable to unauthorized access. If there's an app you need to use that's being blocked, you can allow it through the firewall, instead of turning the firewall off.

4 Under the Incoming connections section, there's a checkbox for Blocks all incoming connections, including those in the list of allowed apps. Checking this box tells the Windows Firewall to ignore the allowed apps list and block everything. Turning this on increases your security but might cause some apps to stop working

Microsoft Defender Firewall is configured.

NOTE: These steps have been taken from: https://support.microsoft.com/

Microsoft Defender Antivirus

Microsoft Defender Antivirus is enabled by default, with default configuration, in the NYB/NYP Series IPC Models.
Capabilities in Microsoft Defender Antivirus:

- View Current threats. This allows you to see any threats currently found on your device, the last time a scan was run on your device, how long it took, and how many files were scanned, and to see threats that have been quarantined. You can also manually start a new scan.
- Virus & threat protection settings. This allows you to customize your level of protection, or exclude trusted files and folders from repeated scanning.

- Virus & threat protection updates. Windows automatically downloads the latest security intelligence as part of Windows Update, but you can also manually check for it. Ensure that a network connection is available for this feature.
- Ransomware Protection. The “Controlled folder access” feature checks apps against a list of known, trusted apps and blocking unauthorized or unsafe apps from accessing or changing files in protected folders. You can add or remove folders in the protected folders list.

To view the status of Microsoft Defender Antivirus:

1 Open the Windows Security app on your Industrial PC

2 Select “Virus & threat protection”

3 Select “Virus & threat protection > Manage settings”

4 Select “Virus & threat protection> Protection updates > Check for updates”

5 Select “Virus & threat protection> Manage ransomware protection”

The status of Microsoft Defender Antivirus is known.

NOTE: These steps have been taken from: https://support.microsoft.com/

3-1-3 PowerShell Script Execution

This section provides details on the use of PowerShell and PowerShell script execution.
PowerShell is a useful tool to configure settings in an IPC but an incorrect setting of PowerShell can allow unwanted execution of scripts. PowerShell can be configured with the following Execution Policy Options:

- Restricted = No scripts allowed to run. This is the default and recommended setting.
- AllSigned = Only scripts signed by a trusted publisher may be run
- RemoteSigned = Local scripts can run without being signed, remote scripts must be signed
- Unrestricted = All scripts allowed to run. This is not recommended.

The active Execution Policy is shown with the command **Get-ExecutionPolicy -List**

To allow local scripts without signing, the Execution Policy can be temporarily changed to a less secure state.
To temporarily allow a locally-made script:

1 Open PowerShell as Administrator.

2 Run **Set-ExecutionPolicy RemoteSigned -Scope LocalMachine**.
The security level is lowered and allows execution of local scripts.

3 Run your local script.

4 Open PowerShell as Administrator.

5 Run **Set-ExecutionPolicy Restricted -Scope LocalMachine**.
The IPC is restored to its secure state.

The local script was used and the IPC is restored to a secure state.

3-1-4 Application Whitelisting

Windows 11 provides capabilities to whitelist specific software applications.
Application Whitelisting:

- Prevents unauthorised software from running
- Reduces attack surface

This ensures that only those applications you allow to execute are able to be run on the system.
AppLocker uses rules and the properties of files to provide access control for applications. If rules are present in a rule collection, only the files included in those rules will be permitted to run.
If, for example, IPC is used to run only few certain apps, AppLocker can help to make system more secure.

AppLocker supports rules for: executables, installers, scripts, DLLs and Packaged apps. Also it has option to create Allow or Deny rule type and with Publisher, Path or File Hash condition.
Enable the AppLocker and Create Rules to run executables digitally signed by Microsoft only. This can also apply to other files, rule types and conditions.
See also:

- *Enable the Application Identity Service* on page 3-8
- *Create "Allow" Rules* on page 3-9
- *Test using Audit-Only mode* on page 3-10

Enable the Application Identity Service

AppLocker will only work when the Application Identity service is running.
The Application Identity service can not be enabled automatically from the Services menu.
To start the Application Identity service using Task Scheduler:

1 Open **Task Scheduler**

2 Select **Create Task**

3 In the **General** tab:

1) Name the task
2) Check **Run with highest privileges**
3) Configure for: **Windows 11**

4 In the **Trigger** tab:

1) Click **New**
2) Begin the task: **At startup**
3) Delay task for **2 seconds**
4) Check **"Enabled"** in Advance settings

5 In the **Actions** tab:

1) Click **New**
2) Action: **Start a program**
3) Program/script:**powershell.exe**
4) Add arguments: **-Command "Start-Service AppIDSvc"**

6 Save the task

7 Restart the IPC

The Application Identity Service is enabled.
Use the above information to create a PowerShell script if required.

Create "Allow" Rules

To use executables in a safe way we create "Allow" Rules.
To create Allow Rules:

1 Go to **Local Security Policy** → **Application Control Policies** → **AppLocker**

2 Right-click **Executable Rules** → **Create New Rule...**

3 Create Executable Rules using the wizard:

1) Action: **Allow**, User or group: **Everyone**, select **Next**
2) Conditions: **Publisher**, select **Next**
3) Click Browse and navigate to known Microsoft-signed executable e.g.: ***C:\Windows\System32\notepad.exe*** and then select **Next**
4) Drag the slider to **Publisher** and select **Next**
5) Add exceptions if needed and then select **Next**
6) Name the rule and then select **Create**

The created rule allows all EXE files signed by Microsoft to run for all users.
To keep Windows 10 fully functional also the next steps are required because they will allow the use of packaged apps.

4 Create "Allow" rules for the other file types signed by Microsoft (Script, Windows Installer, etc.) using the same wizard.

5 Create "Allow" rules for file types signed by Omron Europe B.V. using the same wizard.
This is required to run Omron IPC software.
For an Omron Europe B.V. signed reference file use: C:\Program Files (x86)\OMRON\Industrial PC\Industrial PC Support Utility\IndustrialPCSupportUtility.exe
Sysmac Studio has different digital signature. "Allow" rule for Sysmac Studio needs to be created separately from IPC software rule.

6 Create "Allow" rules for **Sysmac Studio** using the same wizard.
This is required to use Sysmac Studio because it has a different digital signature.

The required Allow Rules are created.

Test using Audit-Only mode

Precautions for Correct Use

First test which executables would be allowed or blocked **without enforcing** the policy using **Audit only** mode.

To test using Audit-Only mode:

1. Right-click **AppLocker** and select **Properties**
2. For **Executable rules** select: **Audit only**
3. Select **Apply** and then **OK**
4. Ensure that **Application Identity** service is running. Restart the system if needed.
5. Confirm:
   - Launching a Microsoft-signed executable (e.g., Notepad) will run.
   - Launching a non-Microsoft executable (e.g., a portable tool) does not run, it generates an **audit logs**
6. **Check AppLocker logs:**
   - Open **Event Viewer**
   - Navigate to **Applications and Services Logs** → **Microsoft** → **Windows** → **AppLocker** → **EXE and DLL**
   - Ensure that allowed and blocked events are registered

The test using Audit mode succeeded.

Enable AppLocker Enforcement

Ensure the created rules behaves correctly.
Refer to *Test using Audit-Only mode* on page 3-10 for details.

To start AppLocker Enforcement:

1. Select **Security Policy** and then **AppLocker**.
2. Select **Configure Rule Enforcement**.
3. For **Executable Rules**, select **Enforce rules**.
4. Select **Apply** and then **OK**.

AppLocker is enabled.

Additional Information

Note that:
- **Deny rules** override **Allow rules**.
- The **Exceptions** tab in the **Rule menu** can be used to avoid conflicts.

3-1-5 Unified Write Filter

An OMRON Industrial PC can be protected with a Unified Write Filter (UWF). The UWF intercepts disk changes and stores them into a memory overlay in RAM memory instead of applying them to disk. The UWF ensures the integrity of the disk at system startup.
All changes made to the system will be lost at the next reboot. This includes installation of new software, Windows updates and other software updates.

Additional Information

Refer to *Install and Update Software* on page 3-14 for the procedure to install and update software.

Determine Status Unified Write Filter

The status of the Unified Write Filter can be determined.

To confirm the status of the write filter:

1. Run the Command Prompt as an administrator.
2. Enter command **uwfmgr.exe get-config**
   Following screen will appear.

```
C:\Windows\System32>uwfmgr.exe get-config
Unified Write Filter Configuration Utility version 10.0.26100
Copyright (C) Microsoft Corporation. All rights reserved.

Current Session Settings


FILTER SETTINGS
    Filter state:     OFF
    Commit pending:   N/A
    Shutdown pending: N/A
    HORM mode:        N/A

SERVICING SETTINGS
    Servicing State: OFF
```

3. By default, all devices have UWF disabled.

The status of the Unified Write Filter is known.

Enable Unified Write Filter

The Unified Write Filter (UWF) can be enabled to store changes into a memory overlay in RAM memory.

Additional Information

With the write filter enabled windows updates will not be applied to your Industrial PC. Windows updates should be installed regularly to prevent security risks. Refer to *Install and Update Software* on page 3-14 for details.

To enable the Unified Write Filter:

1. Run the Command Prompt as administrator
2. Enter command *uwfmgr.exe filter enable*
3. Reboot the Industrial PC.
4. Run the Command Prompt as administrator
5. Enter command *uwfmgr.exe volume protect C:*
6. Reboot the Industrial PC.

The Unified Write Filter is enabled.

Disable Unified Write Filter

To disable the Unified Write Filter:

1. Run the Command Prompt as administrator
2. Enter command *uwfmgr.exe filter disable*
3. Reboot the Industrial PC.

The Unified Write Filter is disabled.

Install and Update Software

The When the IPC is protected with a Unified Write Filter (UWF), newly installed software and updates will be lost on the next system startup.

Additional Information

Refer to *3-1-5 Unified Write Filter* on page 3-12 for detailed information.

To install new software and updates use the following procedure:

1. Disable the write filter.
   Refer to *Disable Unified Write Filter* on page 3-13 for details.
2. Manually install new software and (Windows) updates.
3. Reboot the Industrial PC to ensure the installation is finalized.
   Recheck for new updates manually when installing Windows updates to ensure all updates are installed.
4. Enable the write filter.
   Refer to *Enable Unified Write Filter* on page 3-13 for details.
5. Ensure the status of the Unified Write Filter is enabled.
   Refer to *Determine Status Unified Write Filter* on page 3-12 for details.

The installed software and updates are preserved at the next system startup.

Additional Information

Windows updates can also be installed using the procedure as described by Microsoft.

3-1-6 Privacy Settings

Privacy settings can prevent personal, usage and system data from being shared.

Windows privacy settings control how much personal data your device sends to Microsoft and third parties, as well as how apps access your location, camera, microphone, contacts, files, and more. These settings are especially important for protecting your personal information, usage habits, and device behaviour.
To configure Privacy settings:

1 In **Settings / Privacy & Security / General**
Confirm the settings:
- Let apps use advertising ID to make ads...= OFF
- Let websites provide locally relevant content by accessing my language list = OFF
- Let Windows track app launches to improve Start and search results = OFF

2 In **Settings / Privacy & Security / Location**
Allow apps to access your location = OFF

3 In **Settings / Privacy & Security / Speech**
Online speech recognition = OFF

4 In **Settings / Privacy & Security / Inking & typing personalization**
Getting to know you = OFF

5 In **Settings / Privacy & Security / Diagnostics & feedback**
Diagnostic data / Send optional diagnostic data = OFF

The Privacy settings are configured.

3-1-7 Removable media

Removable media, such as USB devices or external SD cards can often be used to transfer malware to system, either intentionally or accidentally. These devices are also used as a mechanism to exfiltrate data from a system. USB devices can be supplied with hidden malware embedded in them. It is best practise to limit USB ports from being accessible, and therefore vulnerable to risks from external media. USB ports can be disabled, or be limited in their functionality.
Prevent the use of removable media to:

- Reduces attack surface
- Prevent malware infections
- Prevent data theft / data loss

To disable access to removable storage devices:

1 Open the Group Policy by typing **Gpedit.msc** to the Windows Run and then Navigate to **Computer Configuration, Administrative Templates, System, Removable Storage Access**
The Group Policy editor is displayed.

2 Doubleclick **All Removable Storage classes: Deny all access**
The Settings are displayed.

3 Select **Enable** and then Close the window.
The setting is enabled.

4 Restart the IPC to restart Windows.

Removable media can not be accessed.
An **Access denied** message box will appear when trying to use removable media.

3-1-8 Kiosk Mode

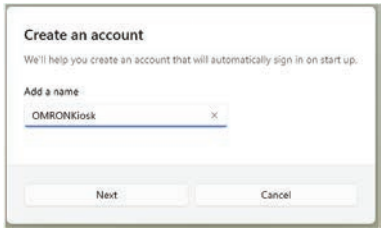
With Kiosk Mode tasks you can:

- Prevents misuse or tampering
- Reduces attack surface

Kiosk mode in Windows 11 allows administrators to configure the system to run a limited set of applications in a locked down environment. This prevents end users from accessing anything outside of the intended digital workspace.
To activate an application in Kiosk Mode:

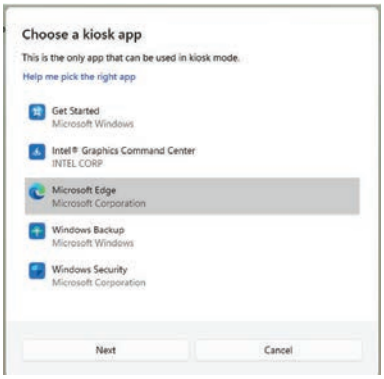
1 Open Windows **Settings** and there select **Setup a kiosk (assigned access)**.
The Setup up a kiosk window appears.

2 Select the **Get Started** button.

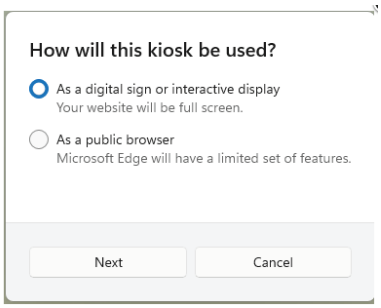


3 Enter a name for the new account you want to use for the kiosk (for example "OMRONKiosk").
Then select Next

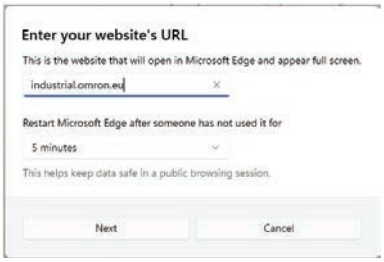
4 Select **Microsoft Edge** as example of the app to launch



5 Select **As a digital sign or interactive display** on how the kiosk will be used.



6 Put in a valid URL



7 Restart the IPC and log into the OMRON Kiosk account.

Kiosk mode is active with only the selected URL in Microsoft Edge active.

3-1-9 Keyboard Filter

Keyboard Filter prevents misuse or tampering.

Windows keyboard filter allows administrators to block the use of specific key combinations or individual key presses to prevent users from performing specific actions that could disrupt or compromise the systems.

To enable Keyboard Filters:

1. Retrieve the script **Add blocked key combinations**
   This script can be found at
   http://learn.microsoft.com/en-us/windows/configuration/keyboard-filter/keyboardfilter-powershell-script-samples
2. Create your own script file with the content of **Add blocked key combinations.**
3. Edit the bottom of your script file to activate the Keyboard Filter combinations you want.
   Example:
   Enable-Predefined-Key "Ctrl+Alt+Del" = The Ctrl+Alt+Del submenu will not appear.
   Enable-Predefined-Key "Ctrl+Esc" = Using Ctrl+Esc the Windows Start Menu is not displayed
   Enable-Custom-Key "Ctrl+V" = Using Ctrl+V no information is copied to the clipboard
   Enable-Custom-Key "Numpad1" = The 1 on the Numpad keyboard is enabled.
   Enable-Custom-Key "Shift+Numpad8" = Blocks the Shift+Numpad8 combination.
   Enable-Scancode "Ctrl" 37 = Enable filtering of the Ctrl + keyboard scancode 37 sequence.
4. Start Windows PowerShell ISE as administrator.
5. Run the created script

Additional Information

Ensure PowerShell script execution is enabled.
Refer to *3-1-3 PowerShell Script Execution* on page 3-6 for details.

6. Restart the IPC

Keyboard filtering is now disabled / enabled for the set combinations.

3-1-10 Encryption using BitLocker

BitLocker protects data at rest in the system from unauthorised access by applying full disk encryption.
BitLocker tasks:

- Ensure compliance with regulations
- Prevent data loss

BitLocker protects data at rest in the system from unauthorised access by applying full disk encryption.
To encrypt the system C drive with the provided script:

1 Make sure a back-up of your data is available.

2 Ensure the TPM status is **The TPM is ready to use**, and that the version is 2.0 or higher.
To check this select Windows+R to open a run dialog window.
Type **tpm.msc** into it and press **Enter** to launch the tool.
The status should say, **The TPM is ready for use** and the specification version should be 2.0 or higher.

3 Run following .bat script as an administrator.

```
@echo off
TITLE Bitlocker Encryption
:: encryption command for windows
manage-bde -on C:
echo.
echo README
echo Check if you ran this batch file with administrator rights.
echo If prompted, restart for a hardware test, after that, run this batch fil
e again. Encryption will then be executed.
echo Encryption will finish by itself.
pause
```

4 Restart the IPC.

After the restart BitLocker is active.
Encryption will start in the background.

3-1-11 Windows Backup and Restore

Ensure the operating system, software and data can always be restored when required.
There are different software tools to create a backup and repair data.
Windows Backup and Retore utilities help you back up your files and system, and restore them if something goes wrong, such as in the event of hardware failure, accidental deletion, malware infection, or system corruption.
Select the Backup and Repair procedure or procedures that are most suitable for your situation.

Overview of Recover, Restore and Repair Methods

Depending on the goal and depending on the available backup and repair data an applicable backup and recover, restore or repair action can be selected.

An overview of the different methods to restore and repair Windows and custom files:

Tool	Goal	Preparation in advance	Restore details	Refer to
Windows Recovery disk	Restore Windows 10 or 11 to a previous state	Create a Windows Recovery disk	• A partial recovery or recovery of user data is not possible • Windows recovers to the state of the previously created Recovery image • Uses a USB storage device • The IPC can boot with this USB	**Create**: *Create a Windows Recovery Drive* on page 3-22 **Restore**: *Recover Windows with the Recovery Drive* on page 3-24
Windows Backup and Restore	Restore a user's selection of folders	Create a Windows Backup	• The data is restored to the state of the previously created backup • Recovery of specific folders is possible. Backups can be created automatically at predefined intervals • No recovery of the Windows operating system • Uses any type of storage device	**Create**: *Create a Custom Backup with Windows Backup* on page 3-25 **Check**: *Check the Custom Backup Storage Device (Windows)* on page 3-27 **Restore**: *Restore a Custom Backup with Windows* on page 3-28

*1. Rescue Disk Creator 1.4.11 or higher.

Additional Information

Contact your OMRON representative when the IPC needs to be restored and you do not have any restore or recover possibility.

Create a Windows Recovery Drive

A Windows recovery drive can repair Windows if a serious error occurs.
Prepare:

- A USB storage device that has sufficient capacity to backup the content of the IPC. The capacity should be at least the Windows partition size + 16 GB. The recommended minimum read/write speed is 190 MB/s.
  Note that all content on this USB storage device will be erased.

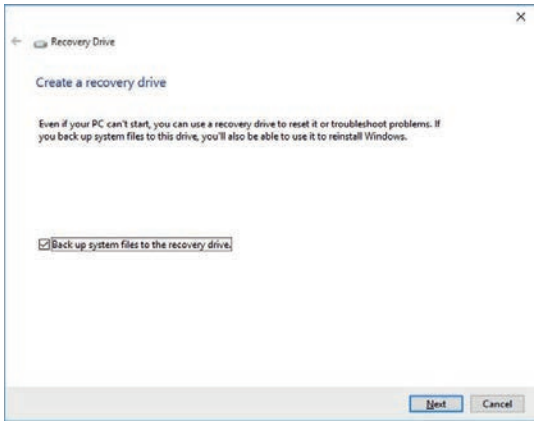
Use the following procedure to create a Windows recovery drive:

1 Insert the USB storage device in a USB 3.0 connector.

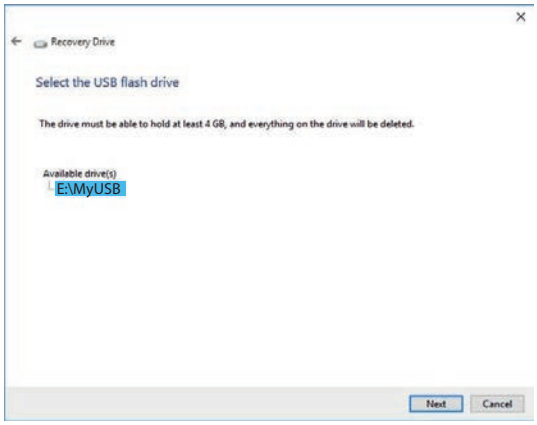
2 Select the Windows **Start** Button.

3 In the search field, input *recovery drive*.

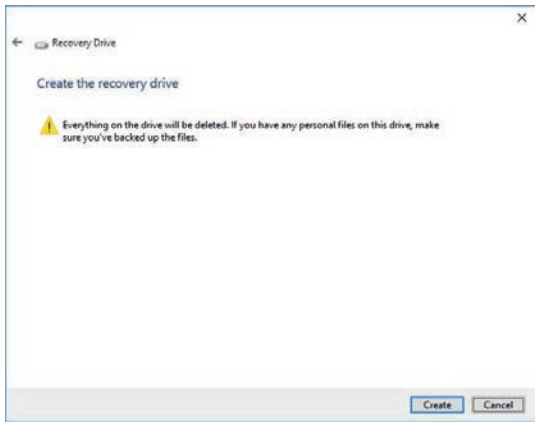
4 Select **Create a recovery drive**.
The recovery drive window opens.



5 Check the checkbox **Back up system files to the recovery drive** and then select **Next**.
The drive selection window opens.

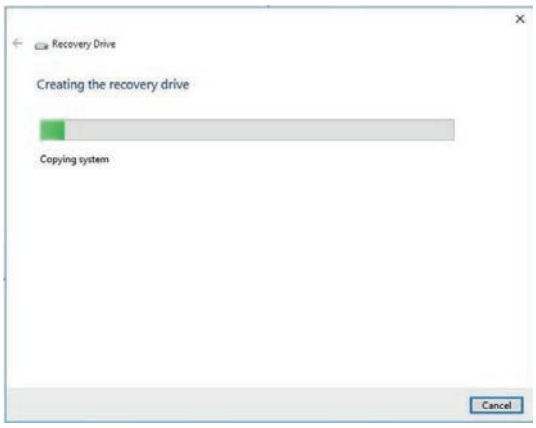


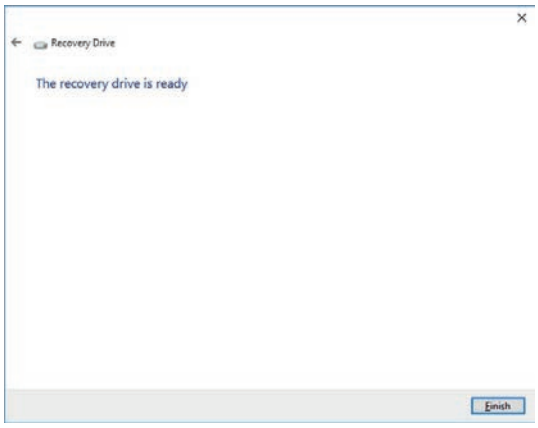
6 Select the applicable drive letter and then select **Next**.
The Create window will appear.



7 Read the warning and if your personal files are safe then select **Create**.

8 Wait until the progress bar is finished and the message **The recovery drive is ready** appears.





9 Remove the USB storage device and store it in a safe place.

The Windows recovery drive is ready.

Additional Information

Refer to http://windows.microsoft.com/ for recovery drive details.

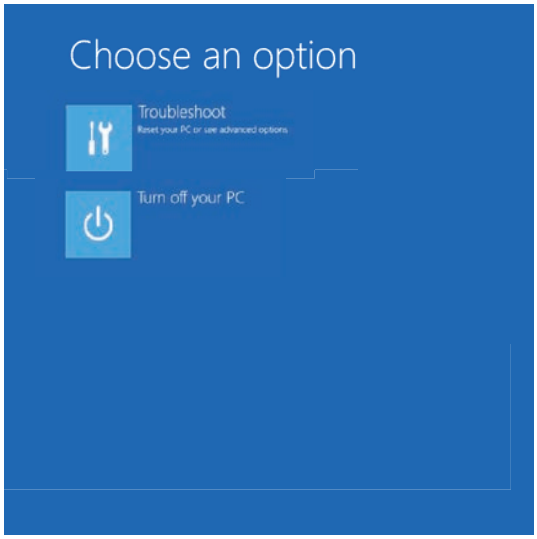
Recover Windows with the Recovery Drive

Use the following procedure to recover Windows to a previous state using a Recovery Drive.

Ensure a Windows Recovery Drive is created earlier and it is available:

To recover Windows:

1. Connect the USB storage device to the IPC.
2. Power ON the IPC and press **F11** repeatedly to display the Boot Selection Popup menu.
3. Select your boot device and then select **Enter**.
   The IPC will reboot.
4. When requested choose your keyboard layout.
   The window *Choose an option* will appear.



5. Select **Troubleshoot**
   The window *Troubleshoot* will appear.
6. Select **Recover from a drive**.

Additional Information

Windows will be restored to the state the recovery disk was created!

Follow the instruction and wait while Windows reinstalls.

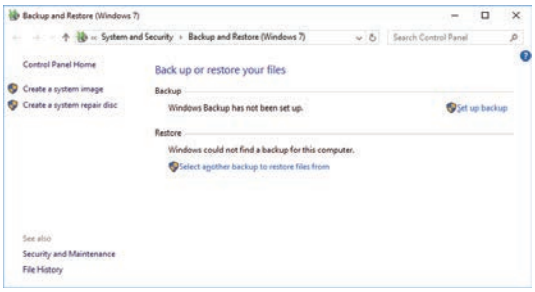
Windows is restored.

Create a Custom Backup with Windows Backup

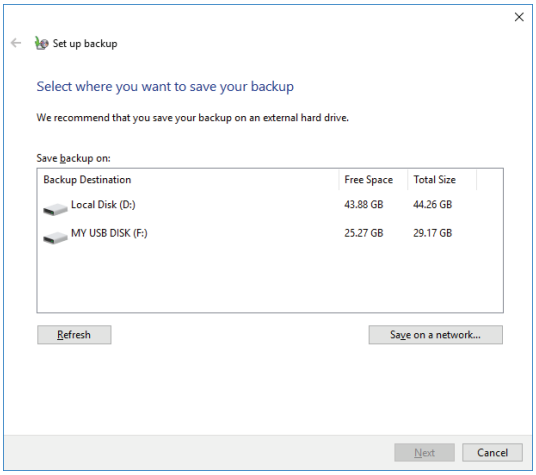
Use the following procedure to create a custom backup of the Industrial PC with the Windows Backup and Restore mechanism.

To manually or automatically create a customized backup:

1. Select the Windows **Start** Button.
2. In search field, input *Backup settings*.
3. Select **Backup settings**.
   The Backup window opens.
4. If available select the option **Go to Backup and Restore**.
   The **Backup and Restore** window is now visible.



5. Select **Set up backup**.
   The Set up backup window opens.

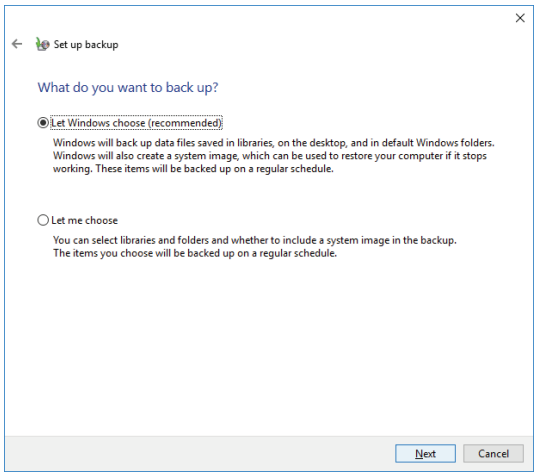


6. Select the backup destination.
   A network location can be added with **Save on a network**.

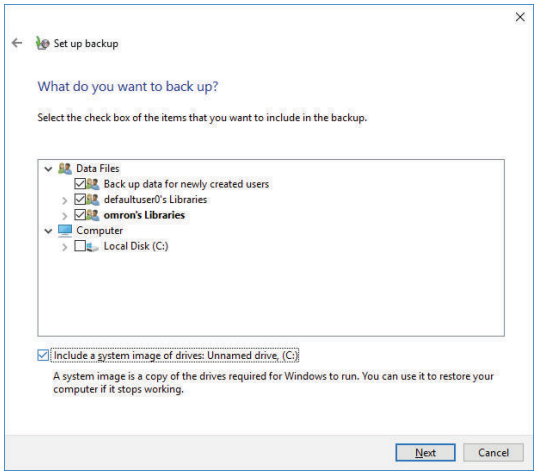
Additional Information

Preferred locations for an automatic backup are:
- A network drive
- The local drive in drive bay B, when installed.

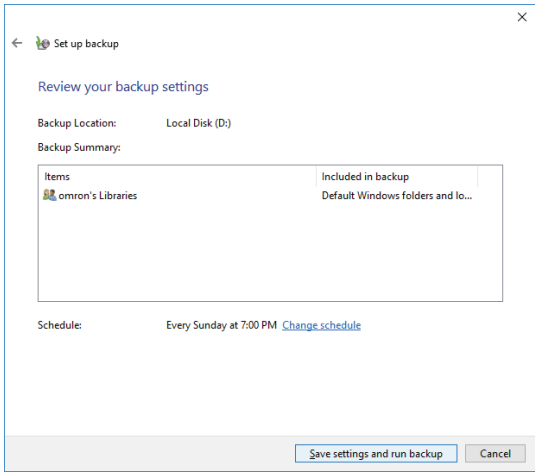
7 Select **Next**.
The following window will appear:



8 Select **Let me choose** and then select **Next**.
The following window will appear:



9 Select all directories you want to include in the backup.



10 Select **Next**.

11 Select **Configure schedule** or **Change schedule** and change the backup schedule.
Ensure:
- The interval is short enough to minimize data loss when a restore is required
- The Industrial PC is powered ON during the backup periods
- The time the backup is scheduled does not interfere with normal operation

or uncheck **Run backup on a schedule** if an automatic backup is not possible.

12 Select **OK**.

13 Select **Save settings and run backup** to create the first backup.

A Custom Backup is available.

Precautions for Correct Use

Create backups according to the preventive maintenance schedule to prevent data loss and system integrity issues.

Additional Information

- Check your backup to ensure it contains all data required for a restore.
- Refer to http://windows.microsoft.com/ for Backup and Restore details.
- Refer to *Restore a Custom Backup with Windows* on page 3-28 for the Restore Procedure.

Check the Custom Backup Storage Device (Windows)

Use the following procedure to check the custom backup storage device.

1 Insert the storage device with the backup in the Industrial PC that created the backup.

2 Follow the first few steps of the restore procedure to display the 'Restore files' screen.
Refer to *Restore a Custom Backup with Windows* on page 3-28 for details.

3 Browse the storage device and ensure at least one backup is displayed.

4 Select **Cancel** to cancel the restore procedure.

The storage device with the custom backup is approved.

Restore and Repair Data

Depending on the goal and depending on the available backup and repair data an applicable restore or repair action can be selected.

Use the *Overview of Recover, Restore and Repair Methods* on page 3-21 to determine the method that is applicable to your situation.
Refer to the mentioned procedure to perform the restore or repair procedure.

● Restore a Custom Backup with Windows

Use the following procedure to restore a custom backup of user files with Windows Backup and Restore.

Additional Information

- Refer to *Create a Custom Backup with Windows Backup* on page 3-25 for Custom Backup details.
- With Windows Backup and Restore it is not possible to restore the complete boot disk or the operating system. Use the Windows Repair Disk to repair the Windows operating system. Refer to http://windows.microsoft.com/ for Backup and Restore details.
- Use the Windows System Repair Disk to repair the Windows operating system when Windows can not be started.

Ensure:

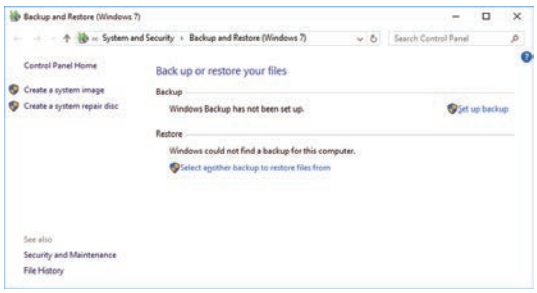
- The Industrial PC is ON
- You are logged in
- A backup is created earlier and it is available

To restore a backup:

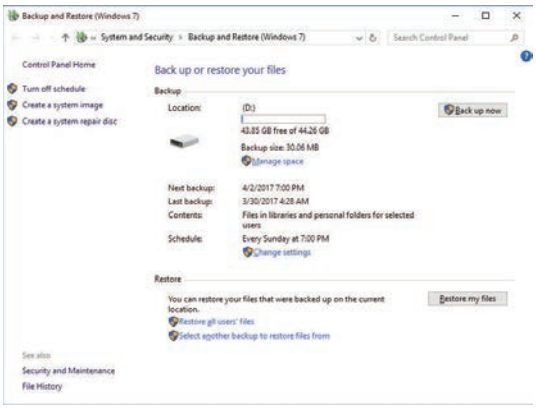
1 Select the Windows **Start** Button.

2 In the search field, input *Backup*.

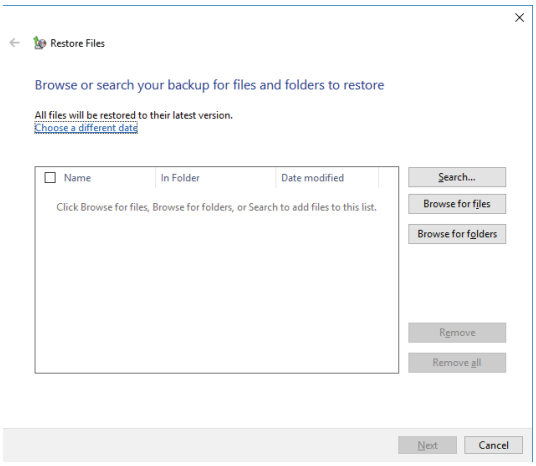
3 Select **Backup and Restore**.
The Backup and Restore window opens.



4 Select **Restore my files**.
The restore files window opens.



5 Use the buttons **Search** and **Browse for files** or **Browse for folders** to find the created back-up.

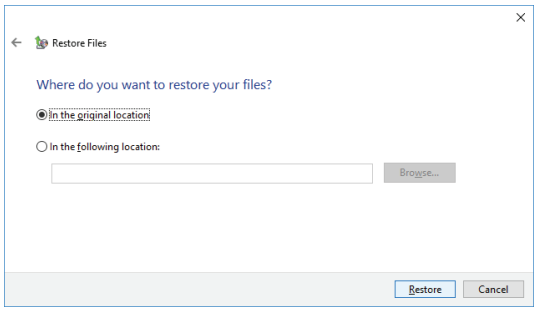


6 Add the files and folders to be restored and then select **Next**.

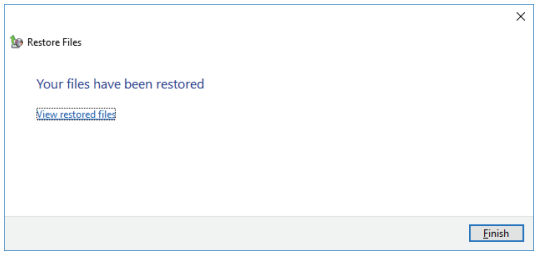
Additional Information

With this Windows Restore procedure it is not possible to restore files that are in use. This means system files and files of the logged in user can not be restored with this procedure.

7 Select **In the original location** and then select **Next**.
The progress window will appear.



8 Wait until the message **Your files have been restored** appears and then select **Finish**.



The files are restored.

3-2 OMRON NY Security Functions

3-2-1 Installation Integrity

To be able to guarantee the integrity of the installation procedure on the NYB/NYP Series IPC Models, the installation process generates hashes of the configuration files used to deploy the system.These hashes can be compared to the expected hashes, to determine if the configuration has been manipulated since leaving the factory.

1 Confirm following hash files are present in folder **C:/OMRON**
- **OmronScripts**
- **OOBE_Execute_ps1**
- **OOBE_Install_cmd**
- **OOBE_PostInstall_cmd**
- **OOBE_PreInstall_cmd**
- **SchedulerScript_cmd**
- **SetServiceConfig_cmd**

2 Open file OmronScripts with Notepad.

3 Open file OOBE_Execute_ps1 and the other files with Notepad
Ensure the hash values are identical to the values in **OmronScripts**.

4 Open file **OOBE_Install_cmd**
Ensure the hash values are identical to the values in **OmronScripts**.

5 Open file **OOBE_PostInstall_cmd**
Ensure the hash values are identical to the values in **OmronScripts**.

6 Open file **OOBE_PreInstall_cmd**
Ensure the hash values are identical to the values in **OmronScripts**.

7 Open file **SchedulerScript_cmd**
Ensure the hash values are identical to the values in **OmronScripts**.

8 Open file **SetServiceConfig_cmd**
Ensure the hash values are identical to the values in **OmronScripts**.

The hash values are confirmed to be identical.

3-2-2 System Watchdog

The System Watchdog identifies system interruptions and performance issues.
The NYB/NYP Series IPC Models includes a hardware-based Watchdog feature that can be integrated into your application to help maintain security in your system.
The System Watchdog is a timer mechanism that needs to be periodically "kicked" by software to prevent a system-level reboot action. If the app or system becomes unresponsive and fails to reset the timer, the watchdog assumes something is wrong and triggers a corrective system reboot. The System Watchdog relies on the OMRON IPC System Service to be running in order to function correctly.

Combined with another Windows 11 hardening feature, the Unified Write Filter, it is possible to improve resilience in your system in the event of a cyberattack. The Unified Write Filter ensures that changes are made only in RAM, and therefore, combined with the watchdog feature to reboot the system after an interruption, the system can quickly be back up and running in its intended operational state.
Refer to *3-1-5 Unified Write Filter* on page 3-12 for details.

To ensure that your system is protected from unauthorised access that could lead to the System Watchdog being misused:
- Regularly confirm that the OMRON IPC System Service is active and running
- Ensure only authorized apps can access the system (Application Whitelisting)
- Use code signing to protect your application from tampering
- Run the Watchdog interaction under a service account with restricted permissions

Configure the Watchdog

To periodically kick the Watchdog from your app:

1. Configure the Watchdog timeout of X seconds in the System API.
   Refer to NY-series Software Development Kit User's Manual for details.
2. In your application start a background thread or timer
3. Within the configured timeout period of X seconds, send a Kick command to the Watchdog
   Refer to NY-series Software Development Kit User's Manual for details.

The Watchdog is configured. If the application crashes, freezes, or is tampered with, the reset fails and the watchdog reboot is triggered.

3-2-3 Secure Boot

The Secure Boot function restricts what software can be started during the boot process of your Industrial PC. The settings are available in BIOS.

BIOS Setup Program

Press the **DEL** key repeatedly directly after Power ON to access the BIOS Setup Program.

BIOS - Security

In the BIOS of your Industrial PC the section Security changeable BIOS parameters and their factory default values are available.

⚠ WARNING

Security setting adjustments should only be performed by the engineer in charge that possesses a thorough understanding of the security settings. Selecting non-recommended security settings can put your system at risk.

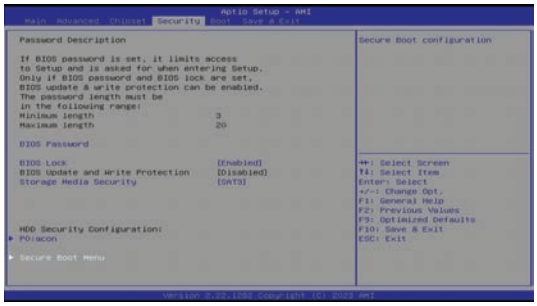
Changeable BIOS Security parameters and their factory defaults:

Item	Default / Remark
Security	
BIOS Lock	Enabled
Storage Media Security	SAT3
Security / Secure Boot Menu	
Secure Boot	Disabled
Secure Boot Mode	Standard

Configure Secure Boot

In the BIOS of your Industrial PC Secure Boot can be configured.
To enable Secure Boot:

1 Select in the BIOS the **Security** page.
Following page will appear:



2 Select the option **Secure Boot Menu**.
Following page will appear:

3 Ensure **Secure Boot** = **Enabled** and **Secure Boot Mode** = **Standard**.

4 Select **F10** to Save and Exit the BIOS.

Additional Information

The Windows Bootloader will use Secure Boot after it has been enabled.

Secure Boot is enabled.

4

Apply Security Patches

Vulnerabilities in products and software libraries are uncovered daily. To protect your assets and production systems from cyberattacks, it is essential to maintain your devices with the latest software and security updates.
This section describes the functions that the NYB/NYP Seres IPC Models provide for updating the system.

4-1 Windows Security Updates

Always keep software at the latest released version to ensure stable operation.
This is specifically important for:

- Anti-virus software
- Firewall software
- Internet browser
- Windows security patches

Precautions for Correct Use

After an OS update or a peripheral device driver update for the product is executed, the product behaviour might be different. Confirm that operation is correct before you start actual operation.

4-2 OMRON Security Updates

Keep your OMRON IPC software up to date to protect your system.
Software can be updated for multiple reasons:

- Security fixes
- Improved Performance
- New Features and enhancements
- Compatibility with other products

Security fixes may be related to reported product vulnerabilities. The OMRON website displays Vulnerability advisories for products. It is also possible to register for the Vulnerability Advisory RSS feed.

- Vulnerability advisory information, including RSS feed, is available at: https://www.fa.omron.co.jp/product/security/en/vulnerability/
- The Industrial PC Platform Software downloads can be found on the OMRON website: https://www.ia.omron.com/product/tool/ipc-platform/index.htm

OMRON recommends that IPC Software should be checked regularly for updates.

Additional Information

Refer to **Preventive Maintenance** in NY-series Operating Systems and Software Utilities Manual (Cat. No. W616) for details.

5

Safely Disposing of Equipment

Disposing of or transferring your OMRON products poses the risk of information disclosure, allowing
third parties to view user data and other information saved in the devices. Before disposing of or transferring the products, it is your responsibility to erase the user data.

5-1 Backup Data

Before disposing of your system, ensure that relevant data is backed up to a secure location.
After disposal, the data will no longer be accessible.

5-2 Wipe User Accounts

Depending on how they were configured, user accounts can expose personal information about system users. It is recommended that you delete user accounts before disposing of the IPC. You must be logged in with an administrator account to perform this action.
To delete a User Account:

1. Select the **Start** button (the Windows icon) on your taskbar.
2. Select **Settings** from the menu.
3. In the Settings window, select **Accounts**.
4. From the left-hand menu, select **Other users**.
5. Under the **Other users** section, select the account you wish to delete.
6. Select the **Remove** button.
   A confirmation prompt will appear.
7. Select **Delete account and data** to permanently remove the account and all its files.

The User Account and associated data is wiped.

5-3 Reset Windows

If you intend to reuse the IPC for another installation, or offer the system for resale, it is recommended that you reset Windows 11 to the application defaults.
To reset Windows 11:

1. Open the Start menu and click the **Settings** app.
2. Navigate through the settings window to **System Recovery**.
3. Under **Reset this PC**, click **Reset PC**.
4. Select the **Remove everything** option to remove all personal files, app data and settings
5. Select **Local Install** to perform a fast reset, for systems that will not be reused.
   If you have security issues in the system and would like to repurpose the system later, then instead select Cloud reinstall to clean the system of any existing data. This option requires an internet connection.
6. In the **Additional settings** window, select **Next**.
7. On the Ready to Reset this PC screen, select the **Reset** button.
   The reset will start.

Windows is reset.
After reset, the Windows Out-Of-The-Box status will be displayed.

5-4 Wipe Storage Devices

Disk drives should be fully wiped on disposing either the system or the specific drive. There are multiple ways to clean your drives.
We recommend one of the following two methods:

Method 1: Use Windows Reset
Selecting the option “Remove everything” during the Windows Reset process will clean the installed drives.
Refer to *5-3 Reset Windows* on page 5-4 for details.

Method 2: Use the “Disk Partition” application.
To use the DiskPart application:

1 In the Windows 11 search bar search **cmd**
The option Command Prompt will appear.

2 right-click Command Prompt, and select **Run as administrator**.
A Command prompt window will appear.

3 Type **diskpart:** and press **Enter**.
The disk partitioning utility will start

4 Type **List Disks:** and press **Enter**.
All available drives are shown.

5 Type **select disk X** (replace X with your target drive number) and press **Enter**.
The chosen drive is selected.

6 Type **clean all** and press **Enter** to securely wipe the disk.
Secure Erase will start and wipe the disk.

The storage device is wiped.

5-5 Dispose of Hardware

Follow the regulations in your region to environmentally dispose your system.

Ensure that the measures to backup data, wipe user accounts, reset windows and wipe storage devices have been correctly executed before environmentally disposing your system.
See also:

- *5-1 Backup Data* on page 5-2
- *5-2 Wipe User Accounts* on page 5-3
- *5-3 Reset Windows* on page 5-4
- *5-4 Wipe Storage Devices* on page 5-5

In case of doubt or for systems with highly sensitive data, physically remove storage devices and mechanically destroy them before disposing your system.

I

Index

Index

OMRON Corporation **Industrial Automation Company**

Kyoto, JAPAN **Contact : www.ia.omron.com**

Regional Headquarters

OMRON EUROPE B.V.
Wegalaan 67-69, 2132 JD Hoofddorp
The Netherlands
Tel: (31) 2356-81-300 Fax: (31) 2356-81-388

OMRON ELECTRONICS LLC
2895 Greenspoint Parkway, Suite 200
Hoffman Estates, IL 60169 U.S.A.
Tel: (1) 847-843-7900 Fax: (1) 847-843-7787

OMRON ASIA PACIFIC PTE. LTD.
438B Alexandra Road, #08-01/02 Alexandra
Technopark, Singapore 119968
Tel: (65) 6835-3011 Fax: (65) 6835-3011

OMRON (CHINA) CO., LTD.
Room 2211, Bank of China Tower,
200 Yin Cheng Zhong Road,
PuDong New Area, Shanghai, 200120, China
Tel: (86) 21-6023-0333 Fax: (86) 21-5037-2388

Authorized Distributor:

Cat. No. W661-E2-01 1125