SIEMENS

SIMATIC

SIMATIC IPC Image & Partition Creator V3.6

Operating Manual

05/2020
A5E50132312-AA

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

> ⚠️ **DANGER**
>
> indicates that death or severe personal injury **will** result if proper precautions are not taken.

> ⚠️ **WARNING**
>
> indicates that death or severe personal injury **may** result if proper precautions are not taken.

> ⚠️ **CAUTION**
>
> indicates that minor personal injury can result if proper precautions are not taken.

> **NOTICE**
>
> indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

> ⚠️ **WARNING**
>
> Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Table of contents

Safety instructions 1

> ⚠️ **CAUTION**
>
> **Warning notices in the documentation**
>
> Please read the warning notices in the documentation because incorrect operation of the program may damage the operating system, programs and stored data.

> **NOTICE**
>
> **Perform backups at regular intervals**
>
> You should back up at regular intervals. This is the only way to ensure that you can quickly restore system operation when a problem occurs.

Note

Contrary to statements made in the "Paragon Hard Disk Manager ™ Suite" manual, you cannot create a Linux rescue medium with the "SIMATIC Image & Partition Creator".

Instead use the function "Create a USB memory drive with Image & Partition Creator".

Industrial Security

<div style="text-align: right; font-size: 3em;">2</div>

Industrial Security

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit (http://www.siemens.com/industrialsecurity).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under (https://support.industry.siemens.com/cs/ww/en/).

Disclaimer for third-party software updates

This product includes third-party software. Siemens AG only provides a warranty for updates/patches of the third-party software, if these have been distributed as part of a Siemens software update service contract or officially released by Siemens AG. Otherwise, updates/patches are undertaken at your own risk. You can find more information about our Software Update Service offer on the Internet at Software Update Service (http://www.automation.siemens.com/mcms/automation-software/en/software-update-service).

Notes on protecting administrator accounts

A user with administrator privileges has extensive access and manipulation options in the system.

Therefore, ensure there are adequate safeguards for protecting the administrator accounts to prevent unauthorized changes. To do this, use secure passwords and a standard user account for normal operation. Other measures, such as the use of security policies, should be applied as needed.

System requirements 3

- SIMATIC IPC or SIMATIC ITP or SIMATIC Field PG
- For runtime environments under Windows operating systems:
  - Windows®7
  - Windows®10
  - Windows® Embedded Standard 7
  - Windows® Server 2008 R2
  - Windows® Server 2012 R2
  - Windows® Server 2016
  - Windows® Server 2019

SIMATIC IPC Image & Partition Creator and Paragon Hard Disk Manager™ Suite

4

"SIMATIC IPC Image & Partition Creator" and "Paragon Hard Disk Manager™ Suite"

"SIMATIC IPC Image & Partition Creator V3.6" contains the "Paragon Hard Disk Manager™ 17 Suite" and also provides additional functions for your SIMATIC IPC.

You can back up or restore files, directories, partitions or entire drives in various runtime environments.

You avoid time-consuming new installations and thus reduce the downtime of your SIMATIC IPC significantly. This increases system availability and reduces resulting costs.

With the partitioning functions of the "Paragon Hard Disk Manager™ 17 Suite" you can also easily and quickly customize the partitioning of drives to meet your requirements without re-installation.

Data backup by creating images (1ClickImage function)

You create backups (images) to protect your device and thus your plant from loss of data that can be caused, for example, by hardware failure, installation problems, operation errors or external influences (viruses, hackers).

The particularly easy backup is performed:

- To a different partition or drive (mirroring)

  or

- To image files

  – CD-R/CD-RW or DVD-R/DVD+R/DVD+RW

  – A network drive

  – An external drive connected via USB

Runtime environments

<div style="text-align: right; font-size: 3em;">5</div>

5.1 Start Paragon Hard Disk Manager™ Suite (without installation)

Select this runtime environment for functions that do not require a restart of the operating system.

Select the following runtime environment for functions that do require a restart of the operating system:

- Booting the SIMATIC Image & Partition Creator from the data storage medium (operating under Windows® PE) (Page 11)
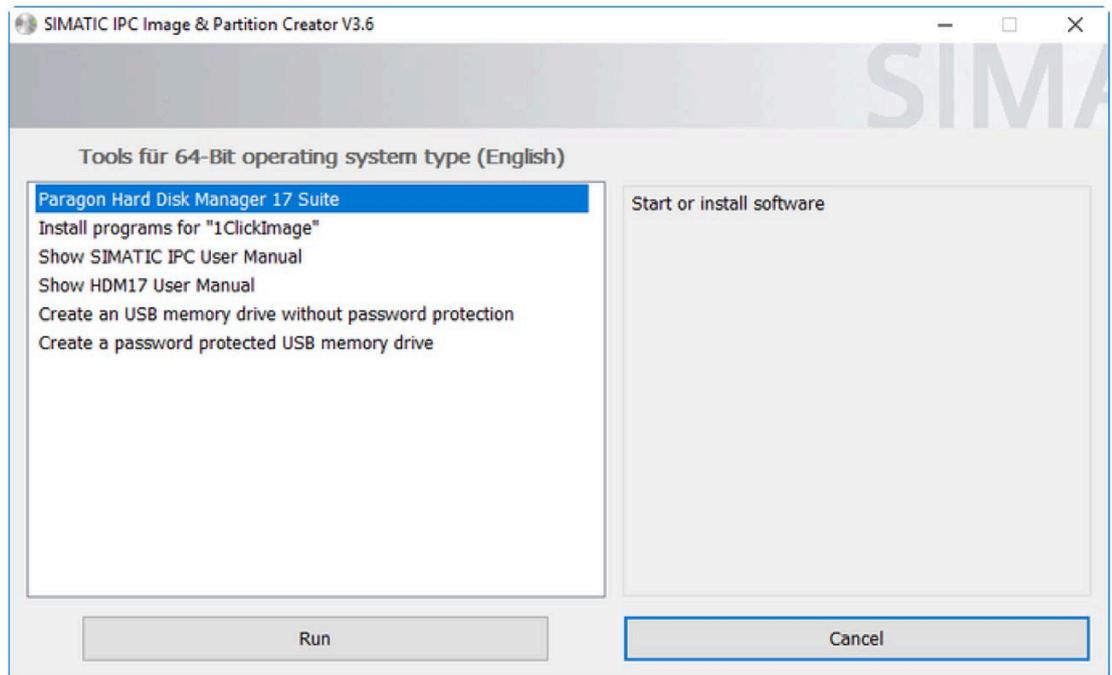- Installing Paragon Hard Disk Manager™ Suite (Page 15)

Requirement

- A keyboard and a mouse are connected to the SIMATIC device.

Procedure

1. Start the Windows® operating system on your SIMATIC device.
2. Connect the USB stick with the "SIMATIC Image & Partition Creator" to your device.
3. Open Windows® Explorer and select the connected USB stick.
4. Run the following batch file with a double-click:
   - Start_Image&PartitionCreator
5. Confirm the subsequent security prompt with "Yes".
6. Depending on the target operating system (operating system of the device), select the following in the next dialog window:
   - System type: 32-bit or 64-bit
   - Language version: English or German

7. The program user interface of the "SIMATIC IPC Image & Partition Creator" is displayed.

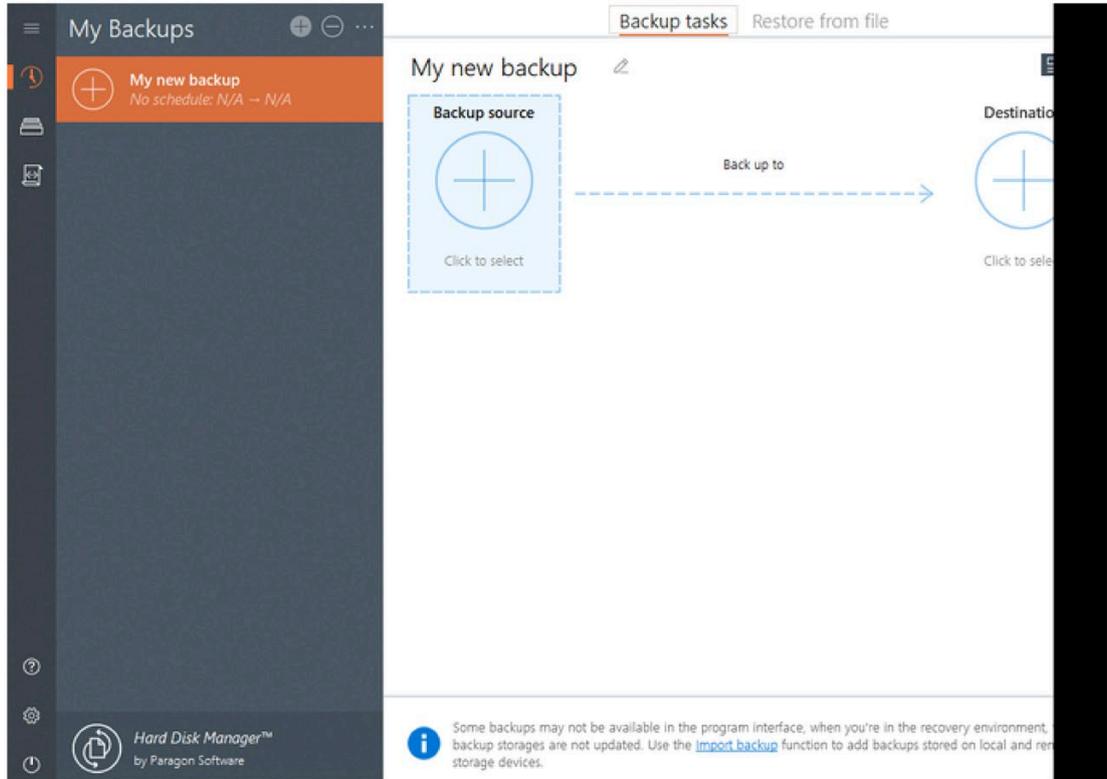   Select the option "Paragon Hard Disk Manager 17 Suite" and click on "Run".

8. The installation window of the "Paragon Hard Disk Manager™ 17 Suite" is displayed.

9. Click "Execute directly".

Result

The program window of the "Paragon Hard Disk Manager™ 17 Suite" opens.

You can start individual functions of the program directly using the icons on the left.

5.2 Booting the SIMATIC Image & Partition Creator from the data storage medium (operating under Windows® PE)

You can boot the "SIMATIC IPC Image & Partition Creator" directly from the data storage medium.

The program is subsequently operated independently of the target operating system (operating system of the device) in the runtime environment "Windows® PE (Preinstallation Environment)".

NOTICE
License provision
The Windows® Preinstallation Environment may only be used with Siemens SIMATIC IPCs or SIMATIC Field PGs in combination with Windows® operating systems.

NOTICE
Unannounced restart of the device after 72 hours of continuous operation
Note the safety function of "Windows® PE".
After 72 hours of continuous operation of your SIMATIC device under "Windows® PE", the device is restarted directly and **without** advance warning.
This means you should only use the "Windows® PE (Preinstallation Environment)" runtime environment for booting, to restore the operating system or for diagnostics purposes.

Note

Using SIMATIC IPC227D or IPC277D

Microsoft® Windows® Preinstallation Environment does not support the "Topcliff" network adapter. Use the Intel I82574L NIC instead.

Requirement

- The SIMATIC device is switched off.
- A keyboard and a mouse are connected to the SIMATIC device.
- If the drives of your target operating system are encrypted with BitLocker, you need the BitLocker recovery password.

Procedure

1. Switch on your SIMATIC device with the on/off switch and/or on/off button.

2. Immediately after switching on the device, press the <Esc> key and hold it down.

   The firmware selection menu opens.

Note

Windows®10 operating systems: Alternative procedure for opening the firmware selection menu

If after starting the device the firmware selection menu does not open with the <Esc> key, follow these steps:

- Start Windows®10.
- Press the <Shift> key and keep it pressed.
- Select "Restart."
  The "Chose an Option" window opens.
- Select the "Troubleshoot" option.
- Select "UEFI / Firmware Settings."
- Click "Restart".

---

3. Select "Boot Manager."

4. Select the data storage medium with the "SIMATIC Image & Partition Creator" in the "Boot Manager" and confirm the entry.

5. Confirm the subsequent message for "Windows® Preinstallation Environment".
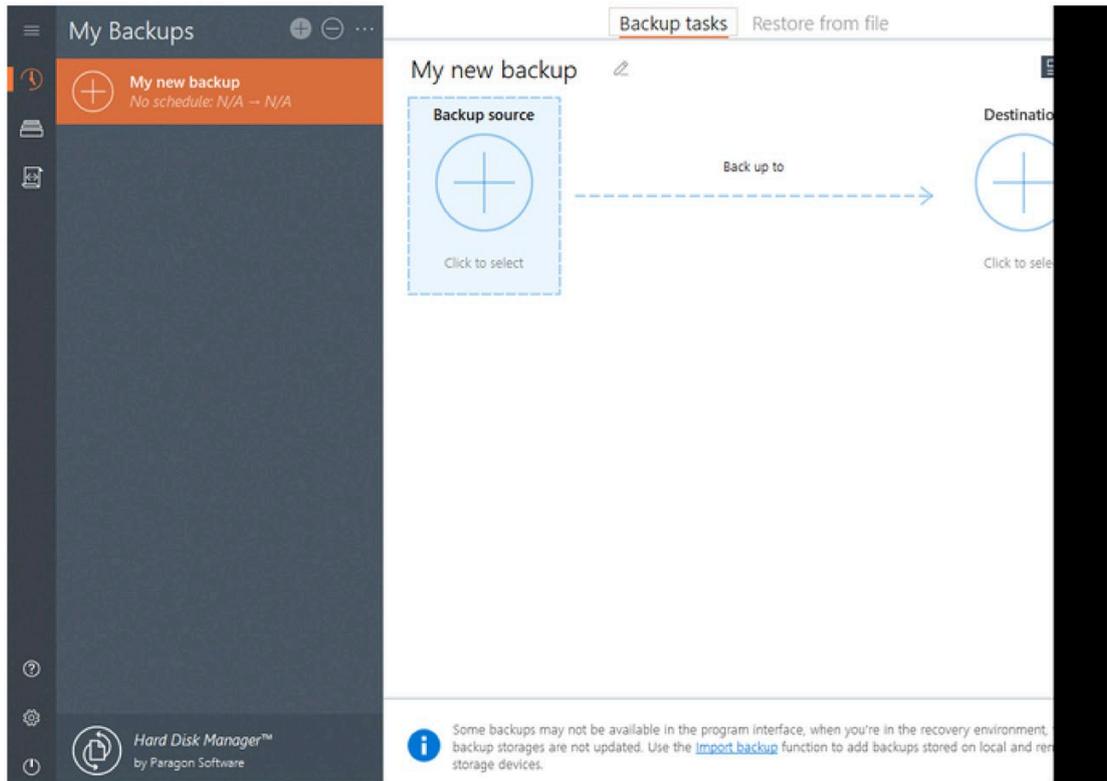
6. The program user interface of the "SIMATIC IPC Image & Partition Creator" is displayed under "Windows® PE".
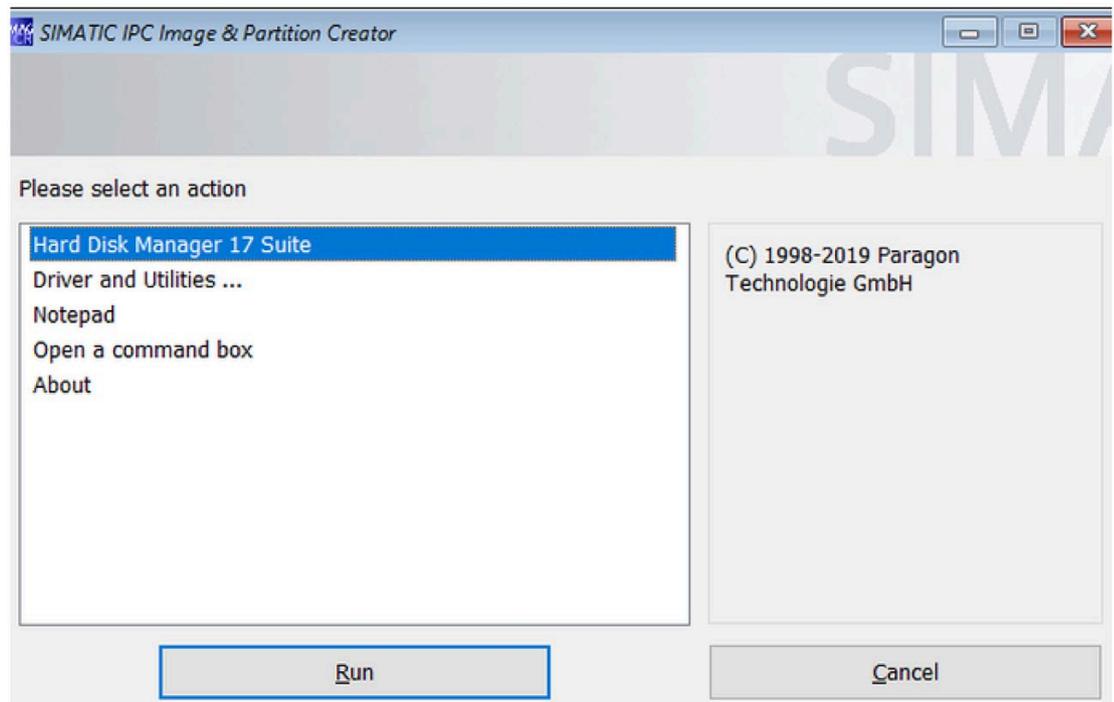
7. Select the option "Paragon Hard Disk Manager 17 Suite" and click on "Run".

Result

The program window of the "Paragon Hard Disk Manager™ 17 Suite" opens.

You can start individual functions of the program directly using the icons on the left.

Note

Unlocking encrypted drives

If the drives of your target operating system are encrypted with BitLocker, select the "Unlock Drives" function.

5.3 Installing Paragon Hard Disk Manager™ Suite

Select this runtime environment if you want to execute time-controlled functions.

Requirement

- You have backed up the data of all running applications.
- A keyboard and a mouse are connected to the SIMATIC device.

Procedure

1. Follow the action steps as described in "Start Paragon Hard Disk Manager™ Suite (without installation) (Page 8) " until the installation window of the "Paragon Hard Disk Manager™ 17 Suite" is displayed:

2. Click "Installation".
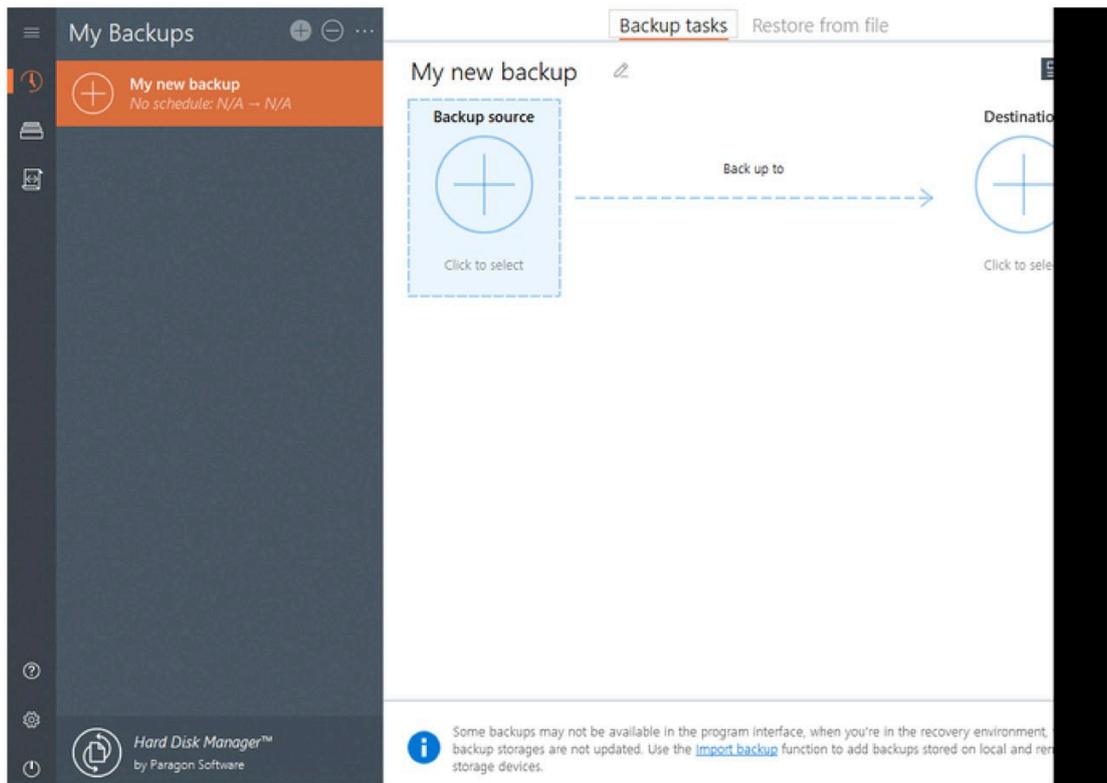3. Accept the licensing conditions and run the installation.

Result

The icon for opening the "Paragon Hard Disk Manager™ 17 Suite" has been added to your desktop. Click on this icon.

The program window of the "Paragon Hard Disk Manager™ 17 Suite" opens.

You can start individual functions of the program directly using the icons on the left.

Configuring and creating "1ClickImage backup" 6

With 1ClickImage you create an automatic backup of the operating system according to a previously defined configuration.

By installing the programs for "1ClickImage", you create two desktop icons for quick access to the following functions:

- Parameter configuration for a 1ClickImage backup
- Creating a 1ClickImage backup with the previously defined configuration.

Requirement

- "Paragon Hard Disk Manager™ Suite" is installed.

Installing programs for 1ClickImage backup

1. Start the "SIMATIC IPC Image & Partition Creator" under Windows®.

2. Follow the action steps until the program user interface of the "SIMATIC IPC Image & Partition Creator" is displayed.

3. Select the function "Install programs for "1ClickImage"".

"SIMATIC IPC Image Creator - InstallShield Wizard" opens.
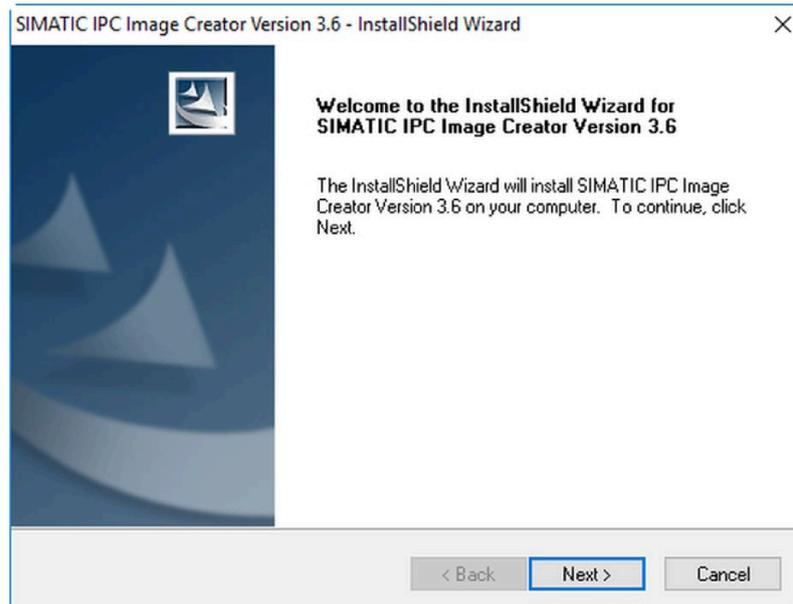
4. Follow the instructions of the InstallShield Wizard.

   The following two icons have been added to your desktop.

Configuration	1ClickImage

5. Now configure the parameters for the 1ClickImage backup.

Configuring parameters for the 1ClickImage backup

1. Click on the "Configuration" icon.

2. Confirm the subsequent security prompt.

3. In the next dialog window, select the "Specify 1ClickImage backup" option.

4. In the next dialog window, configure the parameters for the 1ClickImage backup:
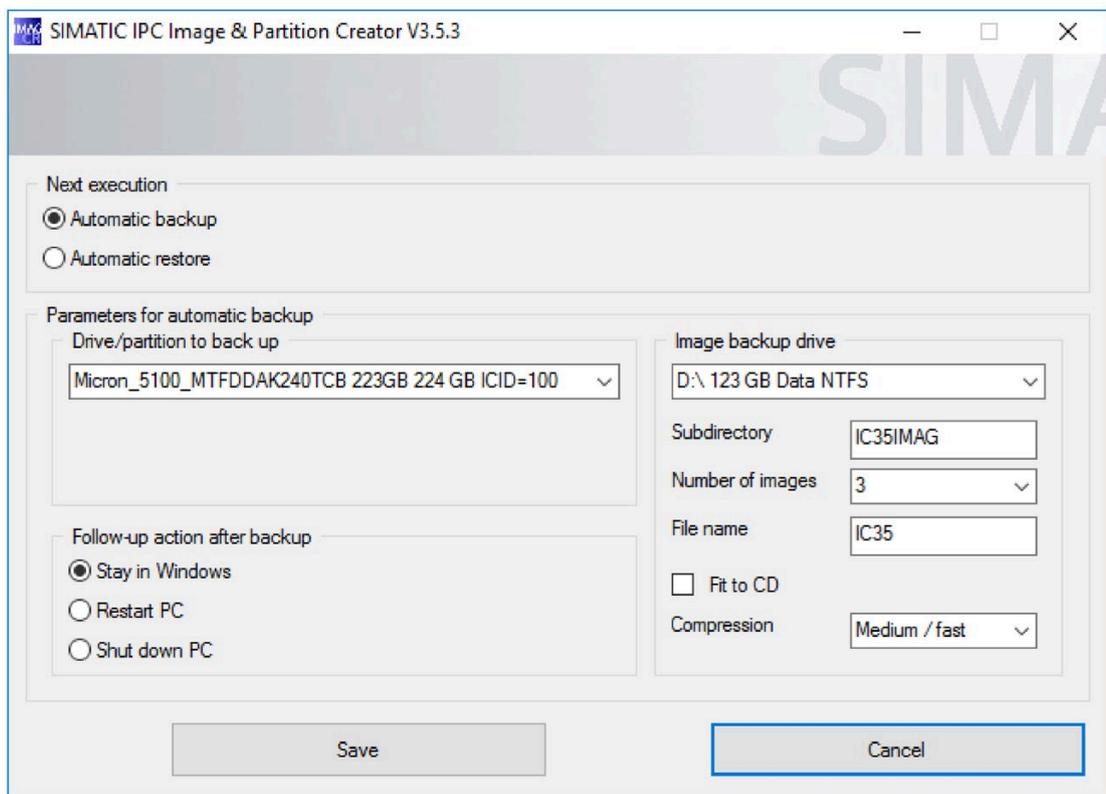
5. Save the settings.

Result

You can now create a backup with the configured parameters with a mouse click. To do so, click on the "1ClickImage" icon on your desktop.

Creating USB memory drives 7

7.1 Drive types and access authorizations for USB memory drives

A USB memory drive is an external, bootable drive that you connect to your SIMATIC IPC via a USB port.

You need the USB memory drive when:

- A system partition in use cannot be restored via a network drive under Windows®.
- The system partition cannot be backed up to a network drive under Windows® Embedded Standard.

The USB drive memory is repartitioned when it is created.

Drive types for creating a USB memory drive

You can create a USB memory drive with the following drives:

- USB HDD
- USB SSD
- USB stick

Access authorization to the USB memory drive

You can create the USB memory drive with one of the following access authorizations ("Specialist" or "Technician"):

"Specialist" (not password protected)

- Access to the partitions of the USB memory drive is not protected by a password.
- Access to the "Paragon Hard Disk™ Suite" is not protected by a password.
- Access to the BIOS Manager (if available) is not protected by a password.
- Access to the "Paragon Hard Disk™ Suite" is allowed.

"Technician" (password protected)

- Access to the partitions of the USB memory drive is protected by a password.
- Access to the "Paragon Hard Disk™ Suite" is protected by a password.
- Access to the BIOS Manager (if available) is protected by a password.
- Backup of the current system can be configured.
- Backup of the current system can be executed.
- USB flash drive for end user can be created from a previously stored backup.
- Access to the "Paragon Hard Disk™ Suite" is **not** allowed.

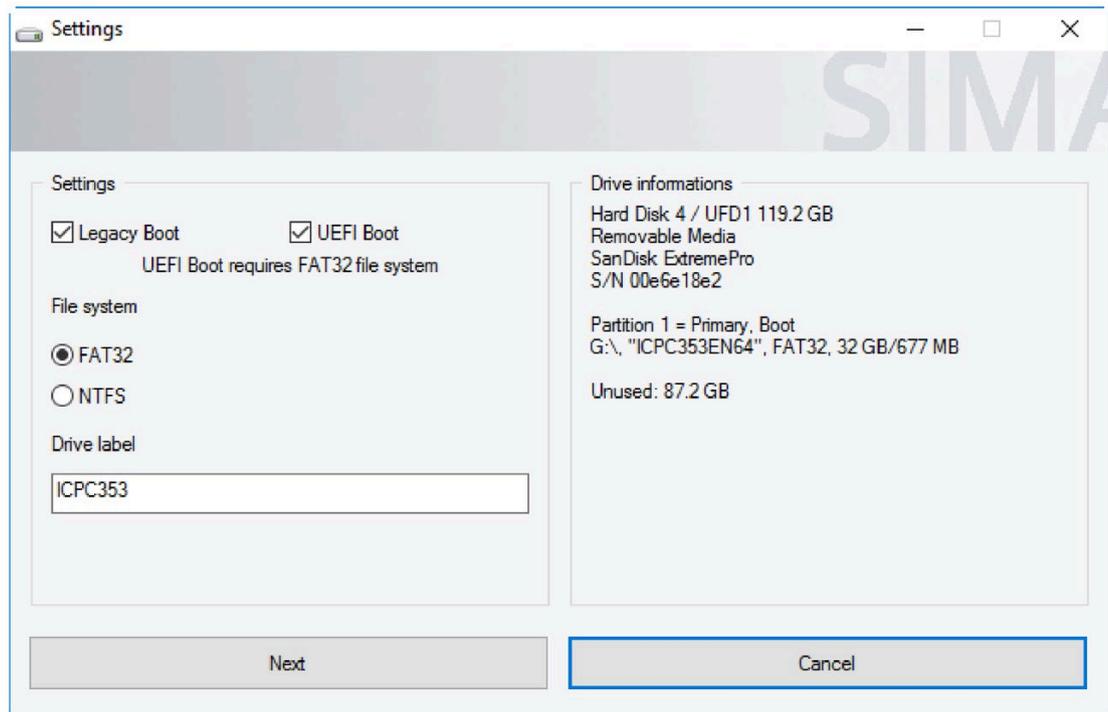## 7.2 Creating a USB memory drive without password protection

Requirements

⚠ WARNING
Risk of data loss
All data is deleted when you create a USB memory drive .
Back up all data on the drive.

- Get more information on the drive types that can be used and the access authorizations to the USB memory drive without password protection. (Page 19)
- "SIMATIC IPC Image & Partition Creator" is started under Windows®.

Procedure

1. Connect a drive to your SIMATIC IPC via USB.

2. Select the function "Create a USB memory drive without password protection" and click on "Run".

3. Depending on the connected drive, make the desired settings in the next dialog window.

    The necessary settings are already selected by default.

4. In the "Drive label" field, enter a name for the USB memory drive and click "Next".

5. Confirm the subsequent security prompt.

Result

A bootable USB memory drive without password protection has been created with the corresponding access authorizations (Page 19).

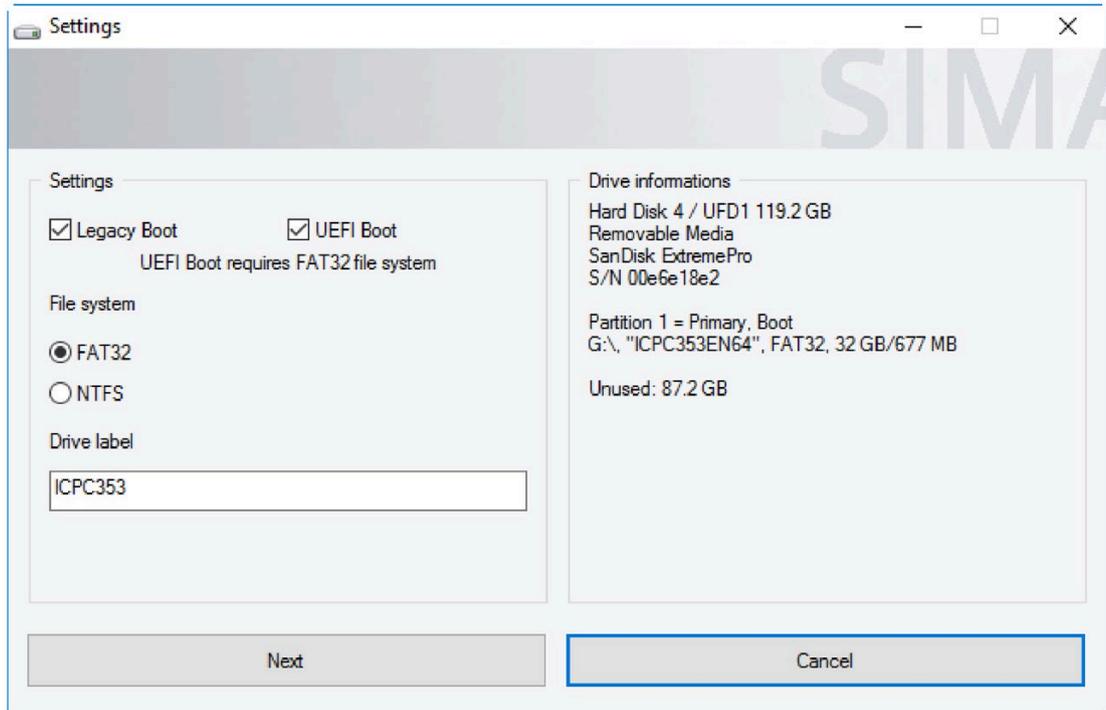## 7.3 Creating a USB memory drive with password protection

Requirements

⚠ WARNING
Risk of data loss
All data is deleted when you create a USB memory drive .
Back up all data on the drive.

- Get more information on the drive types that can be used and the access authorizations to the USB memory drive with password protection. (Page 19)
- "SIMATIC IPC Image & Partition Creator" is started under Windows®.

Procedure

1. Connect a drive to your SIMATIC IPC via USB.
2. Select the function "Create a password protected USB memory drive" and click on "Run".
3. Depending on the connected drive, make the desired settings in the next dialog window.

   The necessary settings are already selected by default.

4. In the "Drive label" field, enter a name for the USB memory drive and click "Next".
5. Confirm the subsequent security prompt.

Result

A bootable USB memory drive with password protection has been created with the corresponding access authorizations (Page 19).

Backing up write-protected operating systems

<div align="right" style="font-size:48px">8</div>

Windows®10 and Windows® Embedded Standard 7 provide configurable write filters:

● Enhanced Write Filter (EWF)

 or

● File Based Write Filter (FBWF)

 or

● Unified Write Filter (UWF)

With these configurable write filters you can give write protection to individual partitions of data storage media (for EWF and UWF) or individual files on data storage media (for FBWF and UWF).

To create a backup of your write-protected operating system or restore a previously created backup, follow these steps:

Creating a backup of the write-protected operating system

1. Start the "SIMATIC IPC Image & Partition Creator" without installation directly from the data storage medium.

2. Then create a backup of the operating system with the "Paragon Hard Disk Manager™ 17 Suite".

Restoring the write-protected operating system

1. Disable the write filter "Enhanced Write Filter (EWF)", "File Based Write Filter (FBWF)" or "Unified Write Filter (UWF)".

 For information on deactivation, refer to the operating instructions for your operating system.

2. Boot the "SIMATIC IPC Image & Partition Creator" from the data storage medium.

3. Then restore a previously created backup of the operating system with the "Paragon Hard Disk Manager™ 17 Suite".