

S7-PLCSIM Readme

Readme

Improvements in S7-PLCSIM V21

This release of S7-PLCSIM includes the following new key features:

- The "Activity Log" provides a chronological record of significant events and status changes that occur as you use S7-PLCSIM.
- The "Global Properties" tab provides access to the functionality and centralized control found in the S7-PLCSIM Advanced control panel.

Additionally, this release offers the following changes and enhancements:

- Sequences feature a table format and support additional time formats and action types.
- The Essentials view offers expanded options and functionality.
- Overall performance is improved.

View the most recent product information online

Siemens updates this readme file as needed and publishes it on the Siemens Industry Online Support (<https://support.industry.siemens.com/cs/us/en/view/109826195>) ("SIOS") Web site. Each readme file on the SIOS site contains the contents of this readme file as well as additional information about S7-PLCSIM that was not available when the product was released.

If you encounter unexpected behavior in S7-PLCSIM, check the SIOS site and search for "S7-PLCSIM Readme" to see whether there is a newer version that addresses your issue.

Operating system support

S7-PLCSIM supports the same operating systems, virtualization, antivirus, and hard disk encryption technology as the corresponding TIA Portal version.

See the TIA Portal readme for a full list of supported technologies.

Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity 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 cybersecurity 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 cybersecurity measures that may be implemented, please visit <https://www.siemens.com/cybersecurity-industry>.

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 the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under <https://new.siemens.com/cert>.

Known issues

Restriction for using "Upload as new station" in STEP 7 with an S7-1200 G2 CPU

You must set the communication mode for your simulated S7-1200 G2 instance (1212/1214, V4.1) to "TCP/IP" to "Upload device as new station" in STEP 7.