SIEMENS

SIMATIC
S7-1200
S7-1200 Firmware update V4.5.1
Product Information

Description

The S7-1200 CPU firmware update V4.5.1 is now available.

This firmware update provides the following corrections:

- Retentive memory is retained after a firmware upgrade from V4.x to V4.5.1.
- CPU password protection is enforced correctly with TIA Portal V13 and earlier.
- The SET_TIMEZONE instruction can be executed any number of times.
- You no longer need to power cycle after a firmware update to V4.3.x or older version.

For more information about the S7-1200 products, see the S7-1200 System Manual, edition 05/2021.

Table 1 CPU models affected by firmware update V4.5.1

CPU model	Description	Article number
CPU 1211C	CPU 1211C DC/DC/DC	6ES7211-1AE40-0XB0
	CPU 1211C AC/DC/Relay	6ES7211-1BE40-0XB0
	CPU 1211C DC/DC/Relay	6ES7211-1HE40-0XB0
CPU 1212C	CPU 1212C DC/DC/DC	6ES7212-1AE40-0XB0
	CPU 1212C AC/DC/Relay	6ES7212-1BE40-0XB0
	CPU 1212C DC/DC/Relay	6ES7212-1HE40-0XB0
CPU 1214C	CPU 1214C DC/DC/DC	6ES7214-1AG40-0XB0
	CPU 1214C AC/DC/Relay	6ES7214-1BG40-0XB0
	CPU 1214C DC/DC/Relay	6ES7214-1HG40-0XB0
CPU 1215C	CPU 1215C DC/DC/DC	6ES7215-1AG40-0XB0
	CPU 1215C AC/DC/Relay	6ES7215-1BG40-0XB0
	CPU 1215C DC/DC/Relay	6ES7215-1HG40-0XB0
CPU 1217C	CPU 1217C DC/DC/DC	6ES7217-1AG40-0XB0
Fail-Safe CPUs		
CPU 1212FC	CPU 1212FC DC/DC/DC	6ES7212-1AF40-0XB0
	CPU 1212FC DC/DC/Relay	6ES7212-1HF40-0XB0
CPU 1214FC	CPU 1214FC DC/DC/DC	6ES7214-1AF40-0XB0
	CPU 1214FC DC/DC/Relay	6ES7214-1HF40-0XB0
CPU 1215FC	CPU 1215FC DC/DC/DC	6ES7215-1AF40-0XB0
	CPU 1215FC DC/DC/Relay	6ES7215-1HF40-0XB0

Required user action

You can install the CPU firmware using one of the following methods:

- Update from the Web server
- The online diagnostic functions of STEP 7
- The SIMATIC Automation Tool
- Make a SIMATIC S7 Memory Card using the Siemens Industry Online Support site that contains the firmware update

The S7-1200 System Manual and the SIMATIC Automation Tool User Guide documents these methods.

Security information

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 (https://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 the latest updates may increase customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed visit (https://www.siemens.com/industrialsecurity).

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

S7-1200 Firmware update V4.5.1
A5E44115569-AH, V4.5.1, 07/2021