SIEMENS

Data sheet 6GT2780-1EA30

product type designation	**Locating Manager Professional, 10000**
product description	For position determination and tracking in localization system SIMATIC RTLS with license for 10000 transponders, all add-on functions and 5 instances in a site/factory
	SIMATIC RTLS Locating Manager Professional 10,000 for 10,000 transponders, single license for 5 instances/ installations in one plant, software and license key download - - email address required for delivery .



product brand name	SIMATIC RTLS
Technical Product Detail Page	https://i.siemens.com/1P6GT2780-1EA30
software version	V2.13.0.0
product functions	
product version	localization and communication server application for SIMATIC RTLS
product description	For position determination and tracking in localization system SIMATIC RTLS with license for 10000 transponders, all add-on functions and 5 instances in a site/factory
product options	Server applications: Network Communication Service, Network Management Service, Localization Service, Client Communication Service, Logging Service / administration tools: Network Configuration, Localization Configuration, User Configuration / Management and Visualization: System Management, 2D view / integration wizard: Automatic detection of new transponders in the wireless network, assignment to TAG groups, AutoConfig of new TAGs with customer-specific parameters, verification of all TAG functions, testing incl. all connections, creation of a test protocol with documented test results and file storage in the archive folder, logoff of TAGs from systems, device replacement of infrastructure incl. automated configuration for routing and positioning / message management: 1. Detection and retaining of events for further processing, 2. Configuration of reactions to events: Database entry, emailing, local information window, SNMP traps, 3. EventLogViewer for filtering, searching and display of database entries /system requirement server: Microsoft Windows 2016/2019 Server, system requirement clients: Microsoft Windows 2016/2019 Server and Microsoft Windows 10 Pro 64-bit / system requirement database: Microsoft SQL Server 2017 / 2019, Oracle 18c / 19c / PostgreSQL 11.11 / 13.2, Microsoft SQL Server 2017 Express Edition included (only for evaluation, not for operation)
PROFINET conformity class	F
product function	
● web-based management	No
● MIB support	No
● TRAPs via email	Yes
● configuration with STEP 7	No
● PROFINET IO diagnosis	No
protocol / is supported	
● SSH	No
● HTTP	No
● HTTPS	No
● NETCONF	No
● DCP	No
● LLDP	No

Subject to change without notice
© Copyright Siemens

● SNMP v1	No
● SNMP v2	No
● SNMP v2c	No
● SNMP v3	No
● IGMP (snooping/querier)	No
national language	
● of the software	German
● of the documentation / German	Yes
● of the documentation / English	Yes
● of the documentation / French	No
● of the documentation / Chinese (simplified)	Yes
software requirements / header	
operating system	
● usable / Windows 10	Yes; clients
● usable / Windows 7	No; nur für Clients
● usable / Windows 2016 Server	Yes; server and clients
● usable / Windows 2012 Server	No
● usable / Windows 2008 Server	No; As of R2
● usable / Windows Server 2019	Yes; server and clients
browser software / required	no
hardware requirements	
processor clock frequency / minimum	2 Hz; GHz (dual core processor)
storage capacity	
● of the work memory / required / minimum	2000 Mibyte
● on hard disk / required	2 Gibyte
● on hard disk / recommended	100 Gibyte
further information / internet links	
internet link	
● to web page: selection aid TIA Selection Tool	https://www.siemens.com/tstcloud
● to web page: identification and localization systems	https://www.siemens.com/ident
● to web page: SiePortal	https://sieportal.siemens.com/
● to website: Image database	https://www.automation.siemens.com/bilddb
● to website: CAx-Download-Manager	https://www.siemens.com/cax
● to website: Industry Online Support	https://support.industry.siemens.com
security information	
security 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 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://www.siemens.com/cert. (V4.7)

last modified: 3/10/2026

Subject to change without notice
© Copyright Siemens