v24.2.0
Drivers

eScada.Drivers.SiemensTcp

eScada.Drivers.SiemensTcp
(S7 Protocol)

OS availability
Windows, Linux, RaspBian

Atomic data type
Bit, Byte oriented protocol.

Hardware and documentation reference
www.siemens.com

Parameters available in every section

Channel: none

Device: IP address   It can be only IPV4 type
                                          Multiple addresses can be expressed using multiple rows or a
                                          comma
                                          e.g. 192.168.1.10,192.168.1.11
              TCP Port   A valid TCP port number. Default 102
              Reconnect timeout [ms]   Waiting time before a reconnection after COMM break-down
              Response timeout [ms]   Timeout interval used to wait for a response.
              Protocol type   ISO over TCP - CPs 243, 343 and 443 or
                                          VIPA Speed7 with built in Ethernet support
              Rack number   Rack number where the CPU is mounted, default 0
              Slot number   Slot number where the CPU is mounted, default 2
              Communication type   PG, OP, S7Basic

Group: none

Tag: Chunk mode   None, no chunks
                                          System, tries to use a default value for chunks size.
                                          Custom, permits to set a custom size for every chunk.
              Bytes per chunk   Only with custom mode
                                          Amount of bytes, admitted by the protocol, for each communication
                                          frame to get or set data. It depends on the protocol and device
                                          you are using, please refer to the protocol documentation.
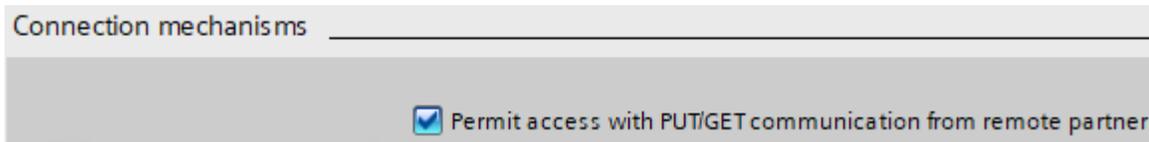   0=No data chunks used.

Remarks for devices

The following attributes can be expressed for each device.

Bytes order actions   None, Swap bytes order, Swap bytes order in DWords, Swap words order,
                             Swap bytes order in DWords then words order

String actions   None, Swap bytes in words

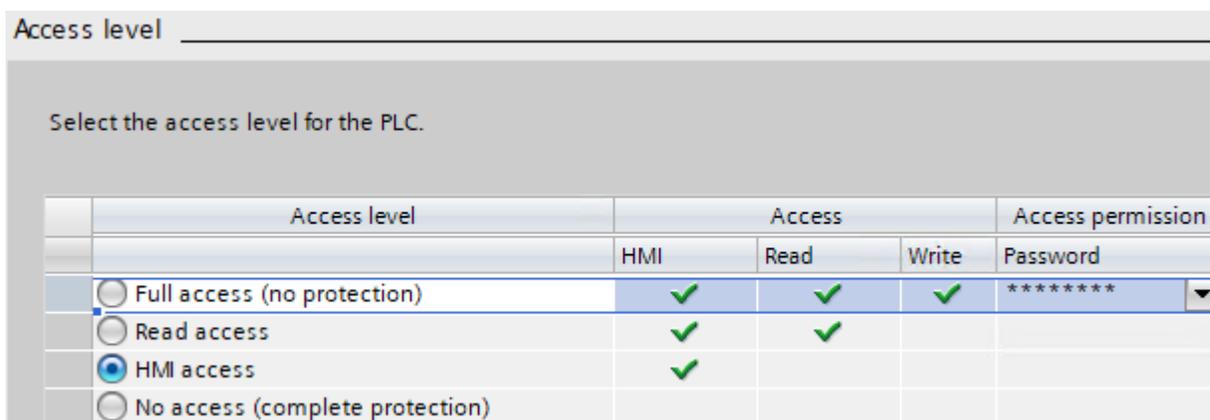**Remarks for CPUs belonging to 1200 and 1500 series**

- Rack and slot device parameters must be set to zero.
- For DB blocks you want to reach, the optimized flag must be disabled.
- Get and Put functions must be enabled
  CPU Properties\Protection & Security\Connection mechanisms

Connection mechanisms _____

☑ Permit access with PUT/GET communication from remote partner

- The access level must be set minimum to HMI access.
  A password can be expressed, if you want to protect your CPU from a download or an upload action.
  CPU Properties\Protection & Security\Access level

Access level _____

Select the access level for the PLC.

Access level	Access			Access permission
	HMI	Read	Write	Password
○ Full access (no protection)	✔	✔	✔	******** ▼
○ Read access	✔	✔		
◉ HMI access	✔			
○ No access (complete protection)				

Remarks for CP-1243

Protocol / function	Port number (protocol)	Default of the port	Port status	Authentication
DNP3	20000 (TCP/UDP)	Closed	Open after configuration	Yes, when Secure Authentication is enabled.
IEC	2404 (TCP)	Closed	Open after configuration	No
S7 and online connections	102 (TCP)	Closed Change to open	Open after configuration *	No
Online security diagnostics (if supported)	102 (TCP)	Open	Open after configuration *	No
Communication via SINEMA RC (if supported)	443 (TCP)	Closed	Open after configuration	Yes
HTTP	80 (TCP)	Closed	Open after configuration	Yes
HTTPS	443 (TCP)	Closed	Open after configuration	Yes
SNMP (if supported)	161 (UDP)	Open	Open after configuration	Yes (with SNMPv3)
Syslog	514 (UDP)	Closed	Open after configuration	No

* Some service providers consider the opening of port 102 a security vulnerability.
To avoid opening port 102 during online diagnostics, see section Online security diagnostics via port 8448 (Page 91).

Addressing

Variable type	Type	Address type	chunks	Items
Boolean				
Single bit	Bit	Mx.b, Ex.b, Ax.b, DBx.DBXy.b Fx.b, Ix.b, Qx.b	NO	1680
Byte				
Unsigned 8 bit	UInt8	MBx, EBx, ABx, DBx.DBBy FBx, IBx, QBx	YES	210
Signed 8 bit	Int8			
16 bit				
Unsigned integer 16 bit	UInt16	MWx, EWx, AWx, DBx.DBWy FWx, IWx, QWx	YES	105
Signed integer 16 bit	Int16			
32 bit				
Unsigned integer 32 bit	UInt32	MDx, EDx, ADx, DBx.DBDy FDx, IDx, QDx	YES	52
Signed integer 32 bit	Int32			
Single precision 32 bit - (IEEE 754)	Float			
64 bit				
Unsigned integer 64 bit	UInt64	MBx, EBx, ABx, DBx.DBBy	YES	26
Signed integer 64 bit	Int64			
Double precision 64 bit - (IEEE 754)	Double			
Strings String bytes can be interpreted as ASCII, UTF-7, UTF-8, UTF-16 or UTF-32 encoding				
Array of bytes	String	MBx, EBx, ABx, DBx.DBBy FBx, IBx, QBx	YES	(A)
Array of bytes. (Siemens S7) Array of bytes. (AllenBradley style)	S7String ABString	MBx, EBx, ABx, DBx.DBBy FBx, IBx, QBx	YES	(B)
(A) It depends on the strings length: e.g. if you want to read strings with a length of 20 chars each string, you can set a number of items of 210 / 20 = 10 consecutive items.				
(B) It depends on the strings length: e.g. if you want to read strings with a length of 20 chars each string, you can set a number of items of 210 / (20+2) = 9 consecutive items.				

remark:
When using chunks, there are no limits on the amount of items.

S7 strings format
They have got two bytes at the beginning.
The first byte is for max allowed string length, the second one is for the real string length.
These types of strings can be declared with a length of 255 bytes max.

AB Strings format
They have got one word (16 bit) at the beginning, it contains the string length.

Consecutive items
The number of consecutive read/write items could be different, because it depends on CPU model, protocol and other things. Values expressed below are referred to a CPU315 connected using CP343