

### designazione del tipo di prodotto

descrizione del prodotto

### Meldungsmanagement fuer Locating Manager Basic, 1000

La Gestione segnalazioni informa l'utente su determinati eventi che si sono verificati

SIMATIC RTLS Locating Manager gestione delle segnalazioni 1000 per 1.000 transponder, opzione per licenza Basic, Single License, software e download di License Key - - l'indirizzo e-mail è obbligatorio per la fornitura .



pagina di informazioni tecniche sul prodotto

<https://i.siemens.com/1P6GT2780-0DB20>

versione di software

V2.13.0.0

### funzioni del prodotto

variante di prodotto

licenza Add-On per Locating Manager Basic 1000

descrizione del prodotto

La Gestione segnalazioni informa l'utente su determinati eventi che si sono verificati

opzioni di prodotto

Eventi importanti vengono riconosciuti nel sistema e registrati per l'ulteriore elaborazione (ad es. interruzioni del collegamento, riavvio del server) / Possono essere configurate reazioni agli eventi: immissione in banca dati, invio di e-mail, Windows Messaging, SNMP-Traps / EventLogViewer per il filtraggio, la ricerca e la visualizzazione di voci di banca dati

classe di conformità PROFINET

F

funzione del prodotto

- Web-based Management
- supporto di MIB
- TRAPs via e-mail
- configurazione con STEP 7
- diagnostica PROFINET IO

No  
No  
Sì  
No  
No

protocollo / viene supportato

- SSH
- HTTP
- HTTPS
- NETCONF
- DCP
- LLDP
- SNMP v1
- SNMP v2
- SNMP v2c
- SNMP v3
- IGMP (Snooping/Querier)

No  
No  
No  
No  
No  
No  
No  
No  
No  
No  
No

lingua nazionale

- del software
- della documentazione / tedesco
- della documentazione / inglese
- della documentazione / francese
- della documentazione / cinese (semplificato)

Tedesco  
Sì  
Sì  
No  
Sì

### requisiti software / intestazione

sistema operativo

<ul style="list-style-type: none"> <li>• impiegabile / Windows 10</li> <li>• impiegabile / Windows 7</li> <li>• impiegabile / Windows 2016 Server</li> <li>• impiegabile / Windows 2012 Server</li> <li>• impiegabile / Windows 2008 Server</li> <li>• impiegabile / Windows Server 2019</li> </ul>	<p>Si; Client</p> <p>No; nur für Clients</p> <p>Si; server e clients</p> <p>No</p> <p>No; Da R2</p> <p>Si; server e clients</p>
software browser / necessario	no
<b>requisiti hardware</b>	
frequenza di clock del processore / min.	2 Hz; GHz (processore Dual Core)
capacità di memoria	
<ul style="list-style-type: none"> <li>• della memoria di lavoro / necessario / min.</li> <li>• su disco fisso / necessario</li> <li>• su disco fisso / consigliato</li> </ul>	<p>2000 Mibyte</p> <p>2 Gibyte</p> <p>100 Gibyte</p>
<b>ulteriori informazioni / links Internet</b>	
link Internet	
<ul style="list-style-type: none"> <li>• alla pagina web: supporto per la scelta TIA Selection Tool</li> <li>• alla pagina web: sistemi di identificazione e localizzazione</li> <li>• alla pagina web: SiePortal</li> <li>• alla pagina web: Banca dati di immagini</li> <li>• alla pagina web: Download Manager CAx</li> <li>• alla pagina web: Industry Online Support</li> </ul>	<p><a href="https://www.siemens.com/tstcloud">https://www.siemens.com/tstcloud</a></p> <p><a href="https://www.siemens.com/ident">https://www.siemens.com/ident</a></p> <p><a href="https://sieportal.siemens.com/">https://sieportal.siemens.com/</a></p> <p><a href="https://www.automation.siemens.com/bilddb">https://www.automation.siemens.com/bilddb</a></p> <p><a href="https://www.siemens.com/cax">https://www.siemens.com/cax</a></p> <p><a href="https://support.industry.siemens.com">https://support.industry.siemens.com</a></p>
<b>avvertenze di security</b>	
avvertenze di security	<p>Siemens commercializza prodotti e soluzioni dotati di funzioni di cybersecurity industriale che contribuiscono al funzionamento sicuro di impianti, soluzioni, macchine e reti. Al fine di proteggere impianti, sistemi, macchine e reti da minacce cibernetiche, è necessario implementare - e mantenere continuamente - un concetto di cybersecurity industriale globale ed all'avanguardia. I prodotti e le soluzioni Siemens costituiscono soltanto una componente di questo concetto. È responsabilità dei clienti prevenire accessi non autorizzati ai propri impianti, sistemi, macchine e reti. Tali sistemi, macchine e componenti dovrebbero essere connessi unicamente a una rete aziendale o a Internet se e nella misura in cui detta connessione sia necessaria e solo quando siano attive appropriate misure di sicurezza (ad es. impiego di firewall e segmentazione della rete). Per ulteriori informazioni inerenti alle misure di cybersecurity industriale che possono essere implementabili potete visitare il sito <a href="http://www.siemens.com/cybersecurity-industry">www.siemens.com/cybersecurity-industry</a>. I prodotti e le soluzioni Siemens vengono costantemente perfezionati per incrementarne la sicurezza. Siemens raccomanda espressamente che gli aggiornamenti dei prodotti siano effettuati non appena disponibili e che siano utilizzate le versioni più aggiornate. L'utilizzo di versioni di prodotti non più supportate ed il mancato aggiornamento degli stessi incrementa il rischio di attacchi cibernetiche. Per essere informati riguardo agli aggiornamenti dei prodotti, potete iscrivervi a Siemens Industrial Cybersecurity RSS Feed al sito <a href="https://www.siemens.com/cert">https://www.siemens.com/cert</a>. (V4.7)</p>

Ultima modifica:

29/10/2025 