SIEMENS

Datenblatt 6GK8751-1BA01-0BK0

Produkttyp-Bezeichnung	**SINEC INS Basic 50 DL**
	SINEC INS Basic 50 DL Lieferform Download Dienste zur Verwaltung von industriellen Netzwerken, RADIUS-, Syslog-, NTP-, DHCP-, TFTP-, SFTP-, DNS-Server, Lizenztyp Single überwachbare IP-Geräte 50 Ubuntu Linux 20.4.4 LTS Ubuntu Linux Server 20.4.4 LTS Debian 9.6.0 SIMATIC OS 1.3.

Software-Version	V1.0
Normen, Spezifikationen, Zulassungen	
Referenzkennzeichen	
● gemäß IEC 81346-2:2019	010307
Weitere Informationen / Internet-Links	
Internet-Link	
● zur Webseite: Auswahlhilfe TIA Selection Tool	https://www.siemens.com/tstcloud
● zur Webseite: Industrielle Kommunikation	https://www.siemens.com/simatic-net
● zur Webseite: SiePortal	https://sieportal.siemens.com/
● zur Webseite: Bilddatenbank	https://www.automation.siemens.com/bilddb
● zur Webseite: CAx-Download-Manager	https://www.siemens.com/cax
● zur Webseite: Industry Online Support	https://support.industry.siemens.com
Securityhinweise	
Securityhinweis	Siemens bietet Produkte und Lösungen mit Industrial Cybersecurity-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen. Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Cybersecurity-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen einen Bestandteil eines solchen Konzepts. Die Kunden sind dafür verantwortlich, unbefugten Zugriff auf ihre Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Diese Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und nur wenn entsprechende Schutzmaßnahmen (z.B. Firewalls und/oder Netzwerksegmentierung) ergriffen wurden. Weiterführende Informationen zu möglichen Schutzmaßnahmen im Bereich Industrial Cybersecurity finden Sie unter www.siemens.com/cybersecurity-industry. Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Produkt-Updates anzuwenden, sobald sie zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen. Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Cybersecurity RSS Feed unter https://www.siemens.com/cert. (V4.7)

letzte Änderung: 07.06.2025