

KEY-PLUG W740, nośnik wymienny do odłączenia iFeatures do SCALANCE W w trybie klient, pozwala na prostą wymianę urządzeń w przypadku błędu oraz na rejestrowanie danych konfiguracyjnych; lub danych projektowych i aplikacji, do wszystkich urządzeń SCALANCE W ze slotem PLUG.



oznaczenie typu produktu	
Nazwa markowa produktu	SCALANCE
oznaczenie typu produktu	KEY-PLUG W740 iFeatures
opis produktu	nośnik wymienny do aktywacji iFeatures dla SCALANCE W w trybie klienta i do prostej wymiany urządzenia w przypadku awarii
możliwość zastosowania	aktywacja trybu klienta iPCF, trybu klienta iPCF-MC, trybu klienta iPRP
możliwość zainstalowania	SCALANCE W780/W770 (tryb klienta), SCALANCE W740/W730
warunki otoczenia	
temperatura otoczenia	
• podczas pracy	-40 ... +75 °C
• podczas magazynowania	-40 ... +80 °C
• podczas transportu	-40 ... +80 °C
wilgotność względna	
• przy 25 °C / bez kondensacji / podczas pracy / maksymalna	95 %
Stopień ochrony IP	IP20
konstrukcja, wymiary i waga	
szerokość	24,3 mm
wysokość	17 mm
głębokość	8,1 mm
masa netto	5 g
rodzaj nośnika wymiennego	
• C-PLUG	Nie
• KEY-PLUG	Tak
cechy produktu, funkcje produktu, elementy składowe produktu / ogólne	
pojemność pamięci	256 Mibyte
normy, specyfikacje, dopuszczenia / deklaracja środowiskowa produktu	
deklaracja środowiskowa produktu	Tak
współczynnik ocieplenia globalnego [eq CO ₂]	
• ogółem	1264 kg
• podczas produkcji	0,92 kg
• podczas eksploatacji	0,34 kg
• po End of Life	0,0042 kg
pozostałe informacje / łącza internetowe	
• łącze internetowe / do strony: poradnik wyboru TIA Selection Tool	https://www.siemens.com/tstcloud
• łącze internetowe / do strony: komunikacja przemysłowa	https://www.siemens.com/simatic-net
• łącze internetowe / do strony: bank obrazów	https://www.automation.siemens.com/bilddb
• łącze internetowe / do strony: CAX-Download-Manager	https://www.siemens.com/cax

wskazówka bezpieczeństwa

wskazówka bezpieczeństwa

Siemens oferuje produkty i rozwiązania z funkcjami cyberbezpieczeństwa przemysłowego, które wspierają bezpieczne działanie instalacji, systemów, maszyn i sieci. Aby zabezpieczyć instalacje, systemy, maszyny i sieci przed zagrożeniami w cyberprzestrzeni, konieczna jest implementacja – oraz ciągłe utrzymanie – kompleksowej koncepcji cyberbezpieczeństwa przemysłowego dostosowanej do obecnego stanu wiedzy technicznej. Produkty i rozwiązania firmy Siemens są tylko jednym z elementów takiej koncepcji. Klienci są odpowiedzialni za zapobieganie nieuprawnionemu dostępowi do swoich instalacji, systemów, maszyn i sieci. Takie systemy, maszyny i komponenty powinny być podłączone do sieci korporacyjnej lub Internetu tylko w niezbędnym zakresie, jeśli jest to konieczne oraz gdy podjęto odpowiednie środki ochronne (np. wykorzystanie zapory sieciowej i/lub segmentacji sieci). Dodatkowe informacje dotyczące środków cyberbezpieczeństwa przemysłowego, które można wdrożyć, znajdują się na stronie www.siemens.com/cybersecurity-industry. Produkty i rozwiązania firmy Siemens są nieustannie rozwijane, aby zapewnić jeszcze lepszą ochronę. Siemens usilnie zaleca aktualizowanie produktów, gdy tylko odpowiednie aktualizacje będą dostępne, oraz używanie wyłącznie najnowszych wersji produktów. Używanie produktów w niewspieranych już wersjach, jak również zaniechanie aktualizacji może zwiększyć podatność klientów na zagrożenia w cyberprzestrzeni. Aby być zawsze informowanym o aktualizacjach produktów, zasubskrybuj kanał RSS Siemens Industrial Cybersecurity pod adresem <https://www.siemens.com/cert.> (V4.7)

Zezwolenia / Certyfikaty

General Product Approval

[Declaration of Conformity](#)



[China RoHS](#)

[Manufacturer Declaration](#)



General Product Approval

Environment

[China RoHS](#)



Ostatnia zmiana:

28.06.2026