

blacha podtrzymująca stacji obsługi do SCALANCE XF204G do montażu na stacji obsługi Siemens ,



pozostałe informacje / łącza internetowe

- łącze internetowe / do strony: poradnik wyboru TIA Selection Tool
- łącze internetowe / do strony: komunikacja przemysłowa
- łącze internetowe / do strony: IWLAN
- łącze internetowe / do strony: bank obrazów
- łącze internetowe / do strony: CAX-Download-Manager
- link internetowy / do strony internetowej: Industry Online Support

<https://www.siemens.com/tstcloud>

<https://www.siemens.com/simatic-net>

<https://www.siemens.com/iwlan>

<https://www.automation.siemens.com/bilddb>

<https://www.siemens.com/cax>

<https://support.industry.siemens.com>

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)

Ostatnia zmiana:

4.12.2025