

RUCKUS® IoT Suite



KORZYŚCI

WYKORZYSTANIE POSIADANEJ INFRASTRUKTURY

Zmniejszenie wydatków na infrastrukturę dzięki połączeniu obsługujących i nieobsługujących Wi-Fi urządzeń IoT z jedną bezprzewodową siecią obsługującą wiele standardów.

WIELOPOZIOMOWA OCHRONA

Zabezpieczenia między poszczególnymi elementami IoT Suite chronią przesyłane dane i bronią przed fizycznymi atakami.

ZABEZPIECZENIA OPARTE NA STANDARDACH

Sieć dostępowa dla urządzeń IoT jest chroniona z wykorzystaniem szyfrowania AES dla połączeń bezprzewodowych oraz SSL dla komunikacji MQTT i REST API.

UPROSZCZONY ONBOARDING URZĄDZEŃ

Obsługujące i nieobsługujące Wi-Fi urządzenia końcowe łączą się szybko z kontrolerem RUCKUS® IoT.

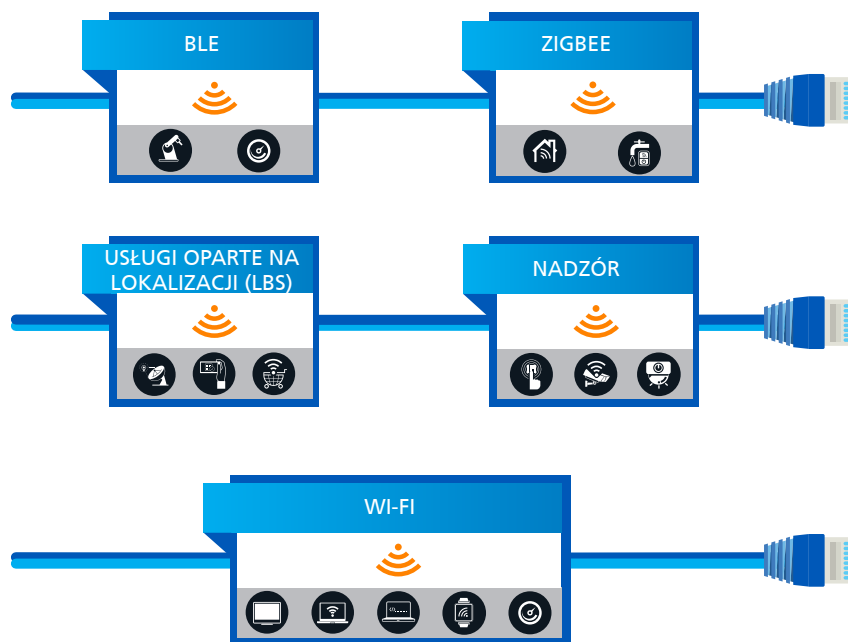
SZYBSZE WDROŻENIE

Punkty dostępowe posiadające status „IoT-Ready” można doposażyć w moduł IoT podłączany do portu USB, umożliwiając wzbogacenie sieci bezprzewodowej o obsługę standardów BLE, Zigbee 3.0, iBeacon oraz urządzeń IoT opartych o Eddystone.

Organizacje chcące wdrożyć rozwiązania IoT napotykają zawiły, sfragmentaryzowany ekosystem standardów, urządzeń i usług, który często spowalnia lub zatrzymuje wdrożenia IoT w przedsiębiorstwach.

Dostawcy rozwiązań IoT klasy korporacyjnej opracowują zintegrowane pionowo autorskie silosy infrastrukturalne, które często eliminują tylko jeden problem, ale nie są gotowe do integracji z innymi silosami, a także oferują bardzo mało możliwości wykorzystania infrastruktury do innych celów. W rezultacie nawet względnie udane wdrożenia IoT wymagają nadmiarowej infrastruktury sieciowej, dodatkowych narzędzi bezpieczeństwa i rozbudowanych usług integracyjnych.

RUCKUS IoT Suite to kolekcja sprzętowych i programowych elementów infrastrukturalnych, które umożliwiają organizacjom utworzenie bezpiecznej sieci dostępu do urządzeń IoT, która eliminuje te problemy. RUCKUS IoT Suite konsoliduje wiele fizycznych warstw sieci IoT w jednej sieci, umożliwiając organizacjom szybszą realizację korzyści z inwestycji w IoT.

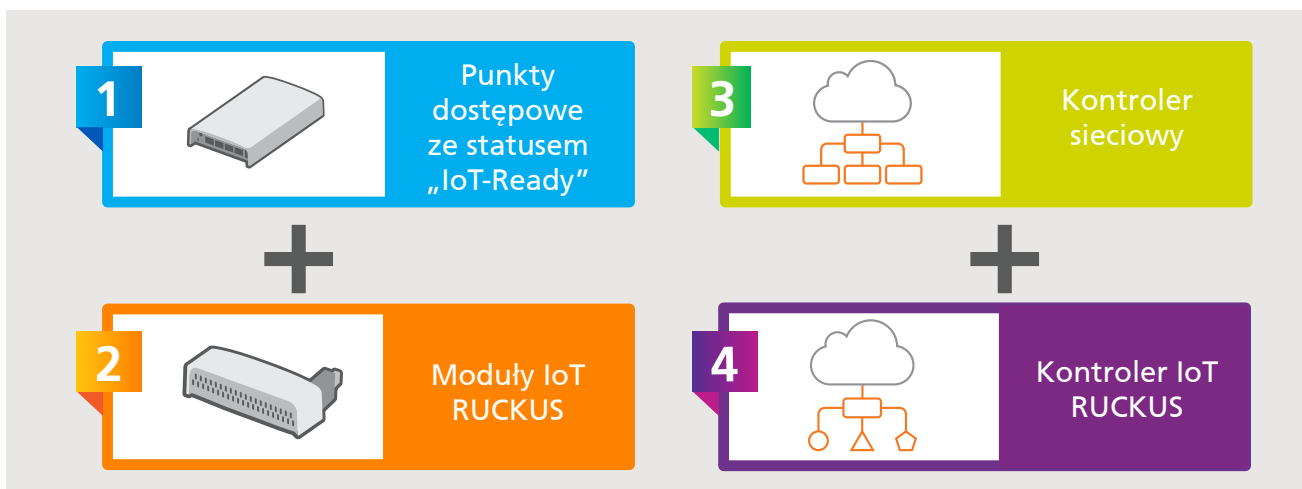
Wdrożenie IoT w formie silosów

RUCKUS IoT Suite

RUCKUS IoT Suite to kolekcja sprzętowych i programowych elementów infrastrukturalnych służących do tworzenia konwergentnej, obsługującej wiele standardów sieci dostępu dla urządzeń IoT.

- **Punkty dostępowe RUCKUS ze statusem „IoT-Ready”** — wbudowane urządzenia radiowe IoT umożliwiają nawiązywanie połączenia bezprzewodowego z punktami końcowymi obsługującymi i nieobsługującymi Wi-Fi.
- **Moduły IoT RUCKUS** — urządzenia radiowe lub radiowo-czujnikowe, które łączą się z punktem dostępowym RUCKUS ze statusem „IoT-Ready”, aby umożliwić łączność z urządzeniami końcowymi za pomocą takich protokołów, jak Bluetooth Low Energy (BLE) i Zigbee.
- **Kontroler RUCKUS SmartZone™** — kontroler sieciowy stanowiący interfejs zarządzania siecią WLAN.
- **Kontroler IoT RUCKUS** — wirtualny kontroler, wdrażany wraz z kontrolerem z systemem operacyjnym RUCKUS SmartZone, który wykonuje funkcje zarządzania łącznością, urządzeniami i zabezpieczeniami dla urządzeń bez Wi-Fi, a także ułatwia koordynację zarządzania różnymi urządzeniami końcowymi i korzystanie z API do integracji z programami analitycznymi i usługami chmury IoT.

RUCKUS IoT Suite



Moduł IoT RUCKUS

Punkty dostępowe Wi-Fi 6 posiadają wbudowany w urządzeniach moduł radiowy IoT i nie wymagają żadnego dodatkowego sprzętu. Za pomocą punktów dostępowych RUCKUS jest możliwe równoczesne wykonywanie operacji Zigbee i BLE. Moduł IoT RUCKUS (I100) to moduł podłączany do punktu dostępowego RUCKUS ze statusem „IoT-Ready”, zazwyczaj modelu Wi-Fi 5 lub starszego. I100 zapewnia połączenie z urządzeniem końcowym IoT w protokole Bluetooth Low Energy (BLE) i Zigbee. I100 służy jako centralny punkt połączenia między różnymi urządzeniami IoT korzystającymi z różnych protokołów a punktem dostępowym RUCKUS ze statusem „IoT-Ready”.

Opatentowane technologie RUCKUS koordynują wykorzystanie widma częstotliwości, automatycznie wybierając kanały tak, aby różne standardy częstotliwości mogły w inteligentny sposób współistnieć i optymalnie działać. RUCKUS koordynuje wybór kanałów tak, aby zapobiec rywalizowaniu o nie przez Wi-Fi i Zigbee.



Kontroler IoT RUCKUS

Kontroler IoT RUCKUS to wirtualny kontroler zintegrowany z kontrolerem SmartZone, który wykonuje funkcje zarządzania łącznością, urządzeniami i zabezpieczeniami dla urządzeń bez Wi-Fi. Umożliwia on zarządzanie urządzeniami IoT klasy korporacyjnej i upraszcza dodawanie nowych usług do rozwiązania IoT.

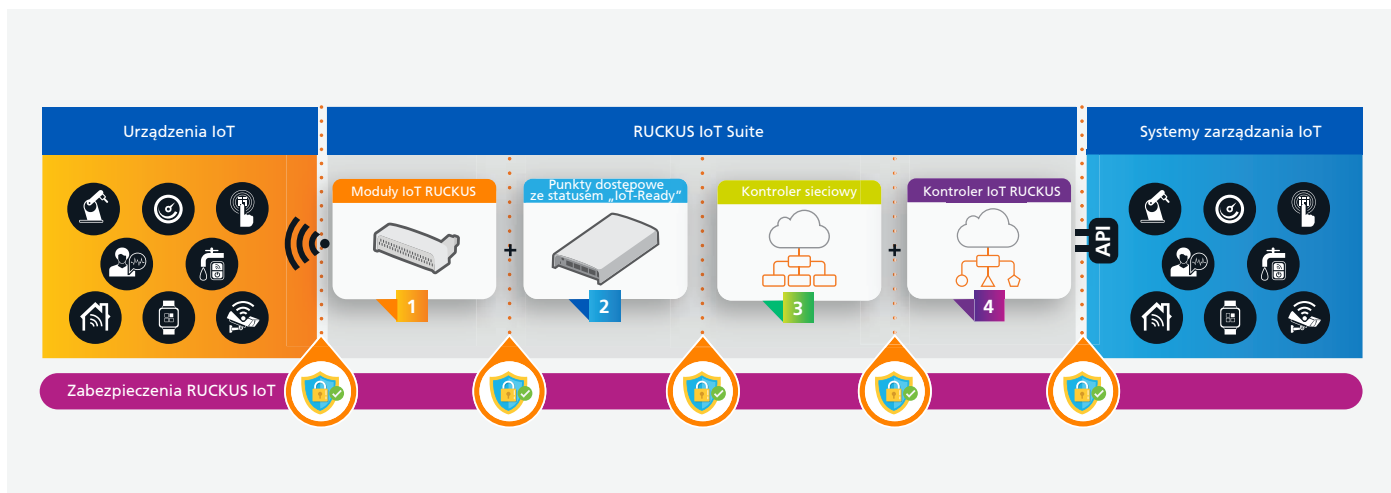
Kontroler IoT RUCKUS zawiera silnik reguł do zarządzania politykami między urządzeniami IoT. Jego otwarte interfejsy API mogą posłużyć do integracji systemów zarządzania IoT innych firm z programami analitycznymi i usługami chmury IoT.

Zabezpieczenia

Zabezpieczenia zajmują pierwsze miejsce na liście czynników, które spowalniają wdrażanie rozwiązań IoT. W RUCKUS IoT Suite przyjęto wielopoziomowe podejście w tej kwestii, które obejmuje następujące elementy:

- **Certyfikaty cyfrowe** — bezpieczne certyfikaty zamieniają punkty dostępowe ze statusem „IoT-Ready” i kontrolery IoT w zaufane platformy.
- **Separacja ruchu** — komunikacja w sieci IT i OT jest odseparowana za pomocą wirtualnej sieci LAN (VLAN).
- **Zabezpieczenia fizyczne** — moduły IoT są na stałe połączone z punktami dostępowymi ze statusem „IoT-Ready” w zabezpieczonej obudowie.
- **Szyfrowanie** — szyfrowanie na poziomie urządzenia radiowego lub aplikacji chroni przesyłane dane przez urządzenie końcowe IoT bez adresu IP; MQTT-over-SSL zabezpiecza przesyłane dane między punktami dostępowymi ze statusem „IoT-Ready” a kontrolerem IoT; uwierzytelniony protokół HTTPS i bezpieczne zarządzanie sesją chronią wychodzące wywołania REST API.

Wielopoziomowa filozofia zabezpieczeń RUCKUS chroni przesyłane dane i broni przed fizycznym włamaniem poprzez szyfrowanie komunikacji między punktem dostępowym a urządzeniami IoT, klamry bezpieczeństwa między modulem IoT a punktem dostępowym, szyfrowanie ruchu SSL oraz ochronę HTTPS między punktem dostępowym przez kontroler IoT do dowolnego zewnętrznego systemu zarządzania.



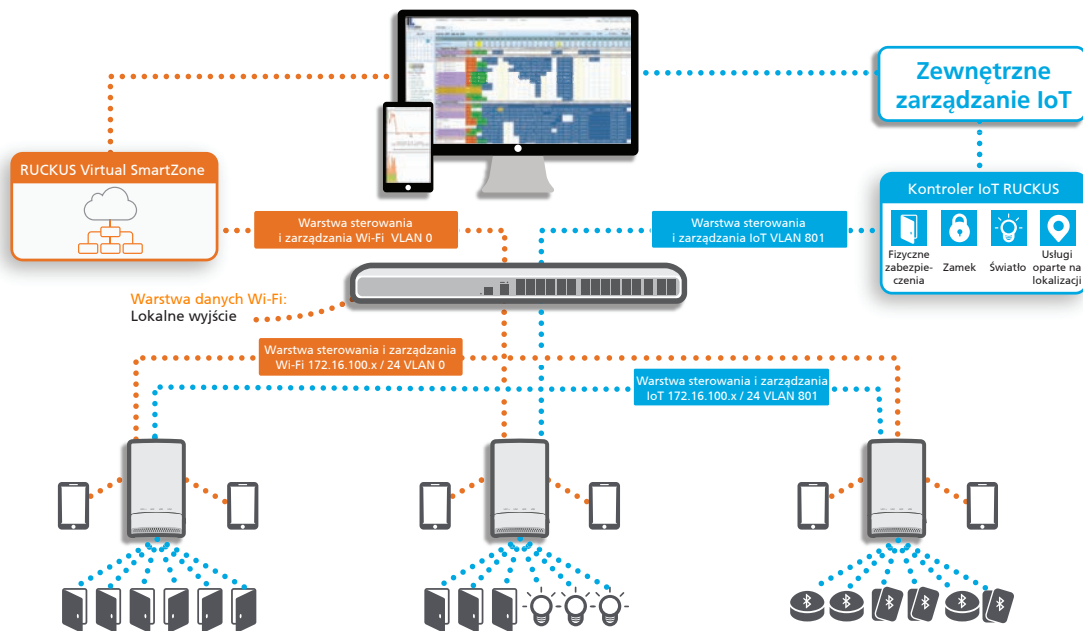
Przypadki użycia i ekosystem RUCKUS IoT Suite

Współpraca z najlepszymi na rynku dostawcami rozwiązań technologii przemysłowej (OT) i technologii klienta (CT) umożliwia organizacjom ustanowienie w kontrolerze IoT RUCKUS polityk obejmujących różne rozwiązania, a także łatwe korzystanie z zewnętrznych narzędzi analitycznych i usług, aby uzyskać większe korzyści z inwestycji w IoT.

RUCKUS IoT Suite służy jako sieć dostępu między urządzeniami IoT a ich systemami zarządzania IoT. Wykorzystanie i rozszerzenie istniejącej infrastruktury sieci za pomocą obsługi wielu standardów komunikacji radiowej i wielopoziomowych zabezpieczeń IoT sprawia, że RUCKUS IoT Suite jest w stanie spełnić różne wymagania w zakresie IoT.

Wdrożenie IoT

- Wi-Fi
- IoT



Przykładowe wdrożenia

Hotelarstwo

Właściciele hoteli i apartamentów zyskują łatwiejszy sposób na poprawę bezpieczeństwa i zwiększenie wygody gości i kierowników obiektu za pomocą zdalnego zarządzania kartami dostępu, zarządzania energią i innych udogodnień podnoszących poziom zadowolenia gości. Ponadto funkcje takie, jak rejestrowanie operacji przy zamku, anulowanie lub zmienianie karty dostępu do pokoju i alarmowanie personelu o włamaniu do pokoju, sprzyjają zwiększaniu poczucia bezpieczeństwa gości i wywierają na nich pozytywne wrażenie.

Inteligentne miasta

Miasta mogą z większą łatwością wdrażać rozwiązania służące podnoszeniu jakości życia mieszkańców od wskazywania miejsc do parkowania po usprawnianie organizacji wywozu śmieci. Miasta mogą monitorować poziom zanieczyszczeń wody i powietrza w ramach działań prozdrowotnych.

Inteligentne kampusy

Inteligentne kampusy wyposażone w IoT mogą sprawić, że szkoły i uniwersytety staną się miejscami bezpieczniejszymi i lepiej zorganizowanymi dzięki użyciu aplikacji do wskazywania drogi, śledzenia zasobów, integracji transportu i roweru publicznego oraz obsługi parkowania. Połączone z Internetem kamery ochrony, inteligentne sterowanie oświetleniem i inteligentne zamki sprawiają, że wszyscy będą się czuli na kampusie bezpieczniej.

Właściciele budynków

Właściciele i operatorzy budynków mogą za pomocą aplikacji IoT tworzyć nowe usługi inteligentnego domu i inteligentnego biura, które będą przyciągały nowych mieszkańców i lokatorów oraz podniosą konkurencyjność ich nieruchomości. Udogodnienia takie jak inteligentne sterowanie oświetleniem, klimatyzacja i połączona z Internetem ochrona nie tylko obniżają koszty eksploatacji, ale także podnoszą poziom bezpieczeństwa budynku, co przekłada się na wzrost wartości nieruchomości i czynszów.

Kontroler IoT RUCKUS

HARDWARE REQUIREMENTS

- Four vCPU cores
- RAM: 32GB
- HDD:1TB recommended

PLATFORM SUPPORT

- ESXi (6.5 and above)
- KVM (1:2.5+dfsg-5ubuntu 10.42 and later)
- VM workstation player (12 and above)
- VirtualBox (5.1 and above)

ACCESS POINT SUPPORT

INDOOR:

- [R550](#)
- [H550](#)
- [R750](#)
- [R730](#)
- [R720](#)
- [R710](#)
- [R650](#)
- [R610](#)
- [R510](#)
- [H510](#)
- [M510](#)
- [C110](#)

OUTDOOR:

- [T350](#)
- [T750](#)
- [T610](#)
- [T310](#)
- [E510](#)

SMARTZONE OS SUPPORT

- SmartZone and Virtual SmartZone 5.2 and above

SCALE

- One virtual instance supports up to 500 access points

DEFAULT PORTS

- TCP/8883 (MQTT SSL), TCP/443 (HTTPS), TCP/22 (SSH), TCP/123 (NTP), UDP/123 (NTP)

PROTOCOL SUPPORT

IoT protocol	<ul style="list-style-type: none">• Zigbee 3.0• BLE• iBeacon• Eddystone
---------------------	--

MANAGEMENT

- RESTful APIs, SDK for ecosystem integration
- Management GUI
- Rules engine, IoT insights
- LoRaWAN, Z-Wave

RUCKUS IoT

I100

Protocol	<ul style="list-style-type: none">• Zigbee 3.0, BLE
Device capacity	<ul style="list-style-type: none">• 32 (Zigbee)• Eight (BLE connected and concurrent)• Several hundred (BLE beacons)
Interfaces	<ul style="list-style-type: none">• USB 2.0, Type A
Output power	<ul style="list-style-type: none">• 20dBm (max)
Power consumption	<ul style="list-style-type: none">• 500mW (max)
Current draw	<ul style="list-style-type: none">• -100mA on 5V (max)
Mechanical	<ul style="list-style-type: none">• Dimensions: 47.83 x 18 x 8.25mm• Max weight: 85 grams
Temperature	<ul style="list-style-type: none">• -40°C to 70°C
Certifications	<ul style="list-style-type: none">• FCC and ETSI/CE—complete list available on request

When ordering PoE injectors or power supplies, you must specify the destination region by indicating -US, -EU, -AU, -BR, -CN, -IN, -JP, -KR, -SA, -UK, or -UN instead of -XX.

For access points, -Z2 applies to the following countries: Algeria, Egypt, Israel, Morocco, Tunisia, and Vietnam.

Warranty: Sold with a limited one-year warranty.



commscope.com

Więcej informacji można znaleźć na naszej stronie internetowej lub uzyskać od lokalnego przedstawiciela CommScope.

© 2021 CommScope, Inc. Wszelkie prawa zastrzeżone.

O ile nie jest zaznaczone inaczej, wszystkie znaki towarowe opatrzone symbolem ® lub ™ są zastrzeżonymi znakami towarowymi lub znakami towarowymi CommScope, Inc. Niniejszy dokument przeznaczony jest tylko do planowania i nie oznacza modyfikacji ani uzupełnienia żadnych charakterystyk lub gwarancji dotyczących produktów lub usług CommScope. CommScope przestrzega najwyższych standardów etyki biznesowej i oszczędności zasobów naturalnych, czego dowodem jest przyznanie wielu zakładom CommScope na całym świecie certyfikatów zgodności z międzynarodowymi normami, w tym ISO 9001, TL 9000 i ISO 14001. Więcej informacji o aktywności prospołecznej CommScope można przeczytać na stronie www.commscope.com/About-Us/Corporate-Responsibility-and-Sustainability.