

RUCKUS® IoT Suite



BENEFITS

REUSE OF EXISTING INFRASTRUCTURE

Reduce infrastructure spend and connect Wi-Fi and non-Wi-Fi IoT endpoints with a single multi-standard wireless access network.

MULTI-LAYERED PROTECTION

Security between each IoT Suite component protects data in transit and guards against physical attacks.

STANDARDS-BASED SECURITY

AES over-the-air encryption, SSL-secured MQTT traffic and HTTPS REST API communication protect the IoT access network.

SIMPLIFIED DEVICE ONBOARDING

Connect Wi-Fi and non-Wi-Fi IoT endpoints quickly with the RUCKUS® IoT Controller.

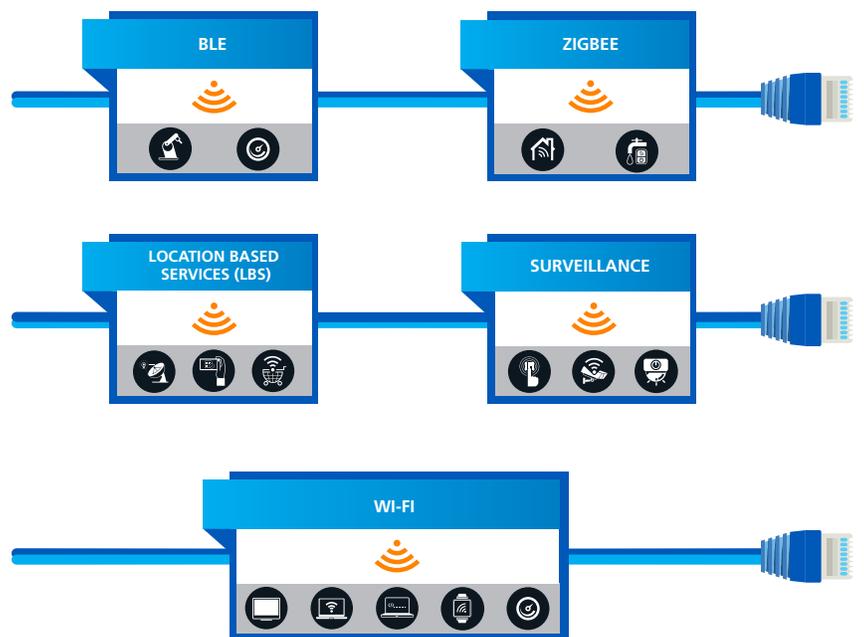
EXPEDITED DEPLOYMENT

Connect an IoT module to existing IoT-ready APs to quickly upgrade the WLAN to support BLE, Zigbee 3.0, iBeacon and Eddystone-based IoT endpoints.

Organizations seeking to deploy IoT solutions face a complex, fragmented ecosystem of standards, devices and services that often slows or stalls enterprise IoT deployments.

To encourage adoption, enterprise IoT solution vendors develop vertically-integrated, proprietary infrastructure silos that often address only a single problem but that do not readily integrate with other silos—and offer limited opportunity for infrastructure reuse. The net result is that even successful IoT deployments require redundant network infrastructure, additional security apparatus and extensive integration services.

The RUCKUS IoT Suite is a collection of network hardware and software infrastructure components that enable organizations to build a secure IoT access network that addresses these issues. The RUCKUS IoT Suite consolidates multiple physical-layer IoT networks into a single network—enabling organizations to more quickly realize benefits from IoT investments.

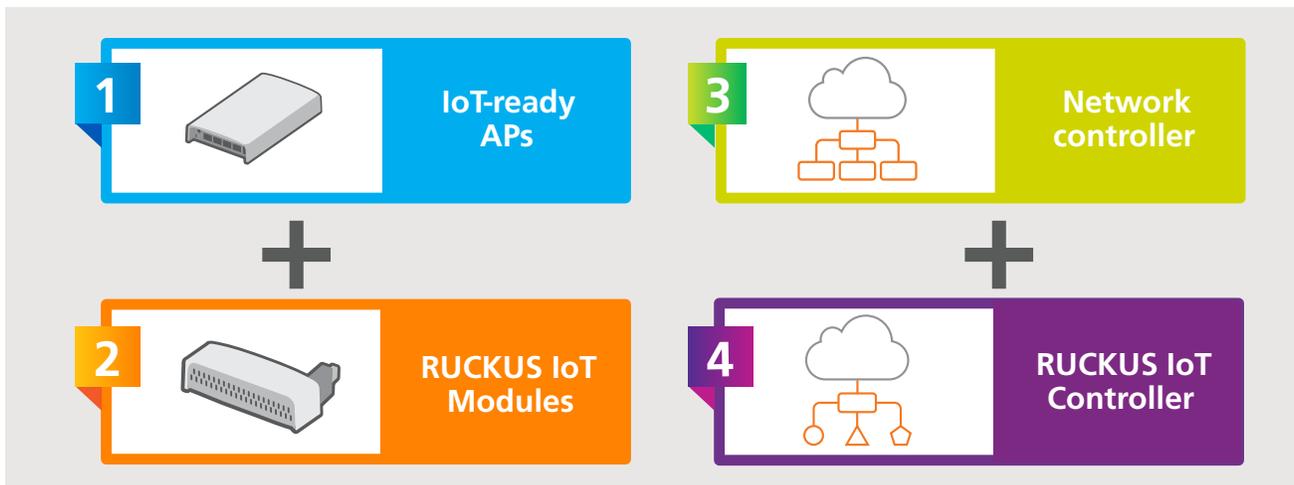
Siloed IoT deployment

RUCKUS IoT Suite

The RUCKUS IoT Suite is a collection of network hardware and software infrastructure components used to create a converged, multi-standard IoT access network.

- **RUCKUS IoT-ready access points (APs)**—Built-in IoT radios to establish multi-standard wireless access for Wi-Fi and non-Wi-Fi IoT endpoints.
- **RUCKUS IoT modules**—Radio or radio-and-sensor devices that connect to a RUCKUS IoT-ready AP to enable endpoint connectivity based on standards such as Bluetooth Low Energy (BLE) and Zigbee.
- **RUCKUS SmartZone™ controller**—A network controller that provides a management interface for the WLAN.
- **RUCKUS IoT controller**—A virtual controller, deployed in tandem with a RUCKUS SmartZone OS-based controller, that performs connectivity, device and security management functions for non-Wi-Fi devices, as well as facilitates disparate endpoint management coordination and APIs for northbound integration with analytics software and IoT cloud services.

RUCKUS IoT Suite



RUCKUS IoT Module

Wi-Fi 6 access points support integrated IoT radios that do not require any additional hardware. Simultaneous Zigbee and BLE operations are possible with RUCKUS access points. The RUCKUS IoT module (I100) is a pluggable module that connects to a RUCKUS IoT-ready access point, typically Wi-Fi 5 and earlier model access points. The I100 provides IoT endpoint connectivity using Bluetooth Low Energy (BLE) and Zigbee. I100 serves as a single connectivity point between disparate IoT devices using different protocols and a RUCKUS IoT-ready AP.

RUCKUS patented technologies coordinate frequency spectrum usage by automating channel selection so different radio-frequency standards can co-habitat intelligently and perform optimally. RUCKUS coordinates channel selection so Wi-Fi and Zigbee do not compete for the same channels.



RUCKUS IoT Controller

The RUCKUS IoT Controller is a virtual controller that integrates with the SmartZone controller to perform connectivity, device and security management functions for non-Wi-Fi devices. It enables enterprise-grade management of IoT devices and simplifies the addition of new services to the IoT solution.

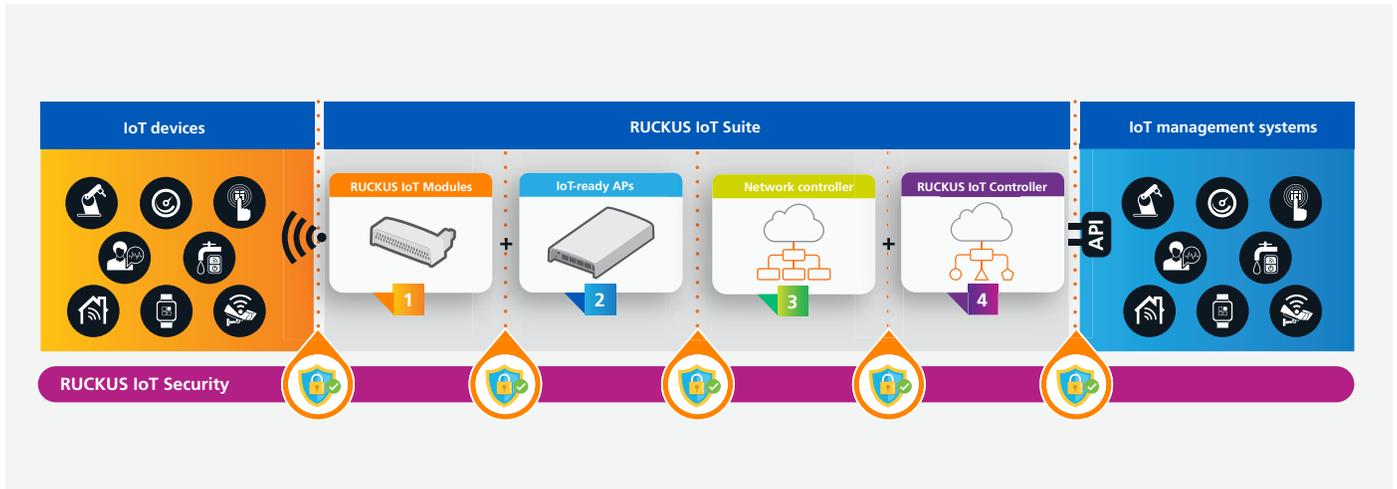
RUCKUS IoT Controller enables a rules engine for inter-IoT device policy management. It offers open APIs that can be leveraged by third-party IoT management systems for integration with analytics software and IoT cloud services.

Security

Security concerns top the list of factors that contribute to IoT solution deployment delays. The RUCKUS IoT Suite addresses such concerns through a multi-layered approach, including:

- **Digital certificates**—Secure certificates make trusted platforms of IoT-ready APs and IoT controllers.
- **Traffic isolation**—IT and OT endpoint traffic is separated using Virtual LAN (VLAN).
- **Physical security**—A lockable enclosure secures IoT modules to IoT-ready APs.
- **Encryption**—Radio-level or application-level encryption protects data in transit for non-IP IoT endpoints; MQTT-over-SSL secures data in transit between IoT-ready APs and the IoT controller; and authenticated HTTPS and secure session management protects northbound REST calls.

The multi-layered RUCKUS security approach protects data in transit and guards against physical intrusion through data traffic encryption between the access point and the IoT devices, security mounts between the IoT module and the access point and encrypted SSL traffic, and HTTPs protection between the AP through the IoT controller to any external management system.



Use cases and the RUCKUS IoT Suite ecosystem

Integrations with industry-leading operational technology (OT) and customer technology (CT) solution providers enable organizations to use the RUCKUS IoT Controller to establish cross-solution policy rules while easily allowing for the use of third-party analytics tools and services to increase IoT investment benefits.

The RUCKUS IoT Suite serves as the access network between IoT devices and their respective IoT management systems. By leveraging and extending the existing network infrastructure with multi-radio standards support and multi-layered IoT security, the RUCKUS IoT Suite can address a variety of IoT requirements.

RUCKUS IoT Controller

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

Visit our website or contact your local CommScope representative for more information.

© 2021 CommScope, Inc. All rights reserved.

Unless otherwise noted, all trademarks identified by ® or ™ are registered trademarks or trade names, respectively, of CommScope, Inc. This document is for planning purposes only and is not intended to modify or supplement any specifications or warranties relating to CommScope products or services. CommScope is committed to the highest standards of business integrity and environmental sustainability with a number of CommScope's facilities across the globe certified in accordance with international standards, including ISO 9001, TL 9000, and ISO 14001. Further information regarding CommScope's commitment can be found at www.commscope.com/About-Us/Corporate-Responsibility-and-Sustainability.

PA-1144292-EN (06/21)