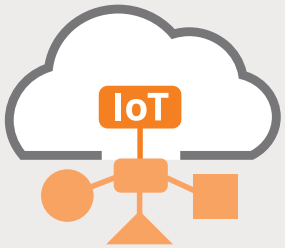
RUCKUS IoT SUITE

DATA SHEET



BENEFITS

REUSE EXISTING INFRASTRUCTURE

Reduce infrastructure spend and connect Wi-Fi and non-Wi-Fi IoT endpoints with a single multi-standards 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 protects the IoT access network.

SIMPLIFY DEVICE ONBOARDING

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

EXPEDITE DEPLOYMENT

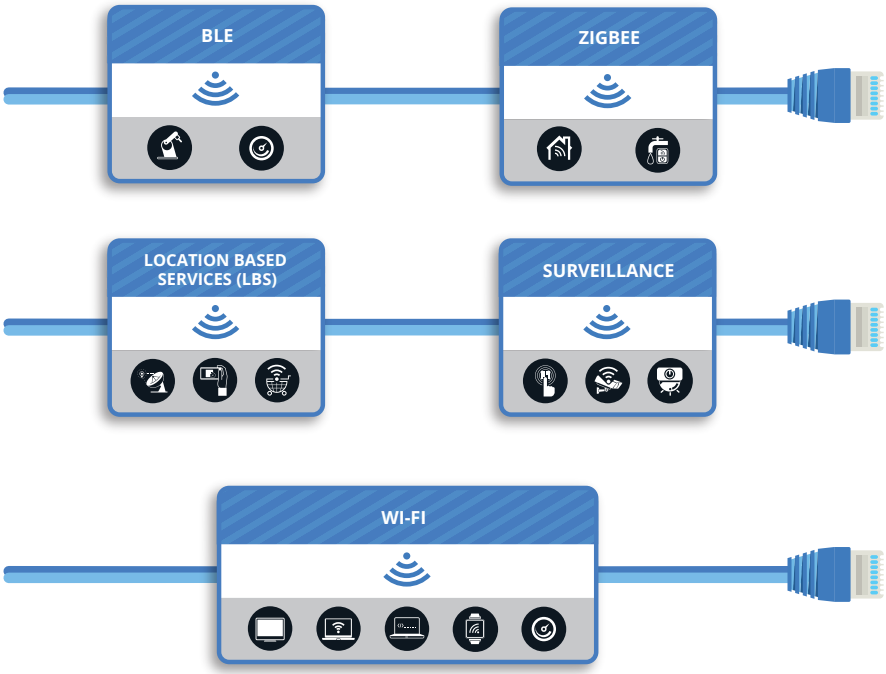
Connect an IoT Module to an existing IoT-ready APs to quickly upgrade the WLAN to support BLE, Zigbee 3.0, iBeacon and Eddystone based IoT endpoints.

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

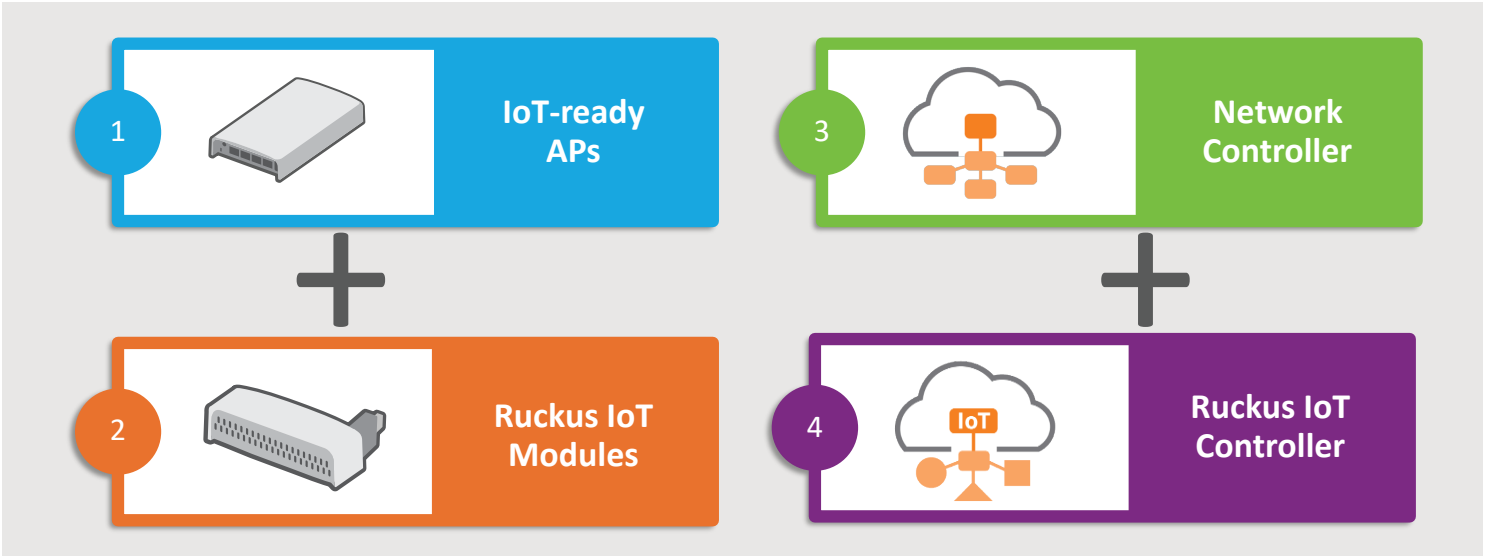


RUCKUS IoT SUITE

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)—Accommodate Ruckus IoT Modules to establish multi-standards 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 facilitate disparate endpoint management coordination and APIs for northbound integration with analytics software and IoT cloud services.

RUCKUS IOT SUITE



RUCKUS IoT MODULE

The Ruckus IoT Module (I100) is a pluggable module that connects to a Ruckus IoT-ready access point. 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.

The I100 IoT Module along with Ruckus patented technologies coordinates 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.

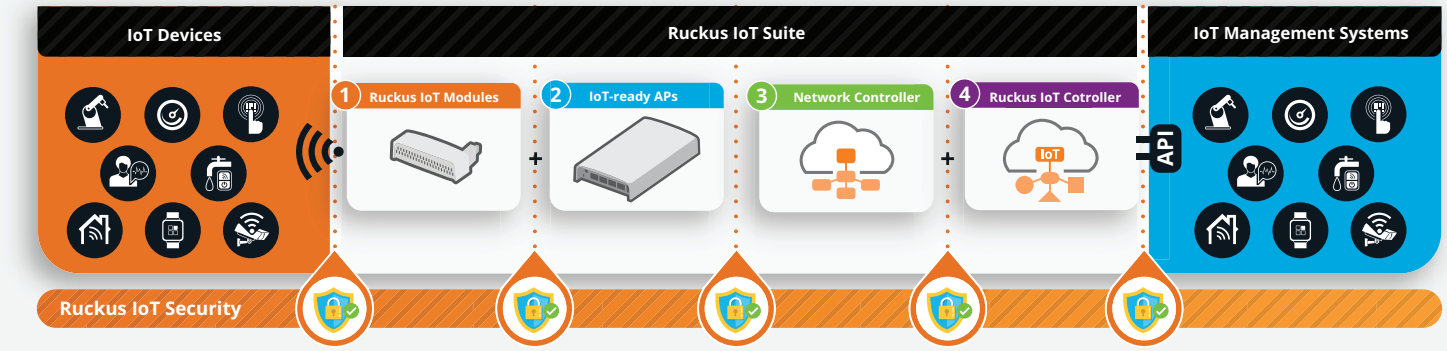
Ruckus IoT Controller enables a rules engine for inter-IoT device policy management. It offers open APIs that can be leveraged by third-party IoT managements systems for integration with analytics software and IoT cloud services.

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; and 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.

Ruckus' multi-layered 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.

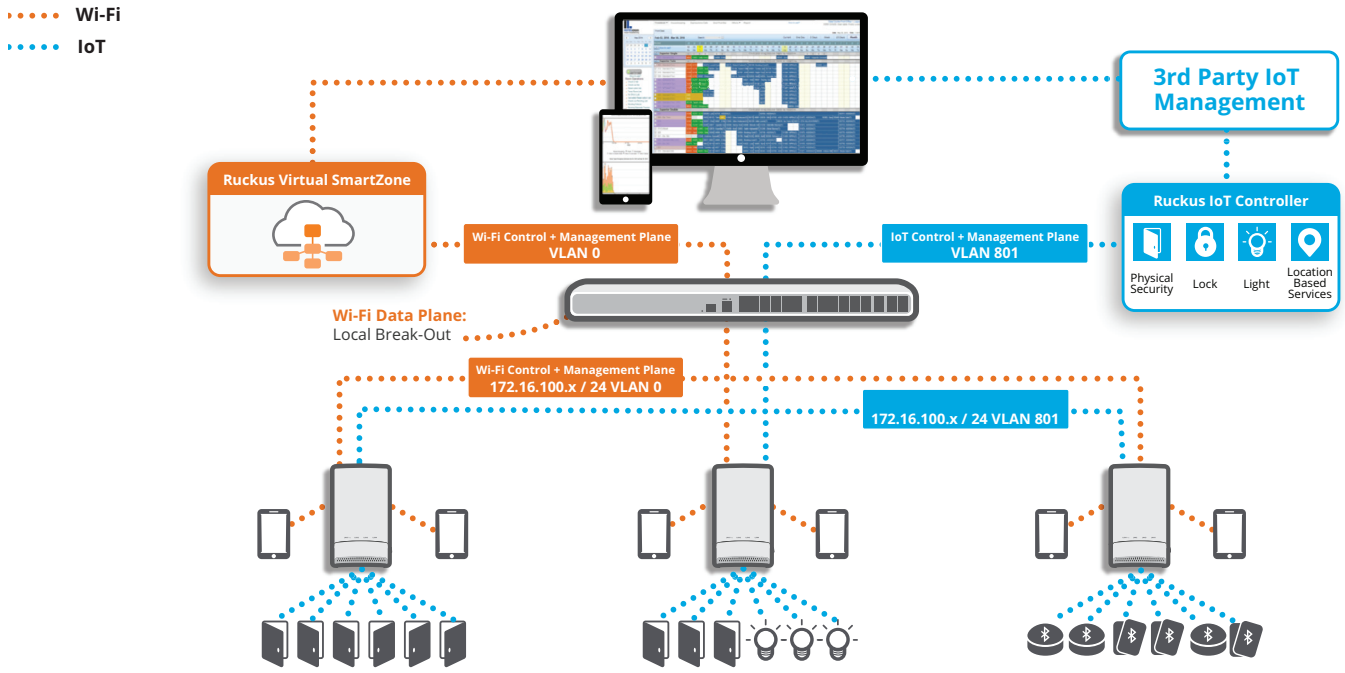


USE CASES AND THE RUCKUS IoT SUITE ECOSYSTEM

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 3rd 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.

AN IoT DEPLOYMENT



DEPLOYMENT EXAMPLES

Hospitality

Hotels can more easily enhance security and convenience for guests through remote key card management and offering smart-home amenities to improve guest satisfaction. Additionally, lock audit trails, canceling or changing key card room access and alerting staff in cases of a forced room entry all build a safer and better guest experience.

Smart Cities

Cities can more easily implement a range of citizen-centric quality-of-life solutions ranging from parking location assistance to more efficient trash collection. Cities can monitor air, water and pollution quality to improve public health.

Smart Campuses

IoT-enabled Smart Campuses make colleges and universities safer and more efficient, through wayfinding, connected transit and bike shares, and smart parking applications. Connected CCTV, smart lighting and smart locks make everyone on campus safer.

Building Owners

Building owners and operators are using IoT applications to create new smart-home and smart-office experiences that attract new residents and tenants and help their properties compete. Amenities like smart lighting, environmental controls, and connected security make buildings safer, increasing property values and rents, while reducing operational costs.

RUCKUS IoT CONTROLLER

HARDWARE REQUIREMENTS

- 2 vCPU cores (min 2.7GHz Intel Xeon / i7)
- RAM: 2GB
- HDD:8GB minimum (100GB to support maximum number of APs and IoT endpoints)

PLATFORM SUPPORT

- ESXi (5.5 and above)
- VM Workstation Player (12 and above)
- VirtualBox (5.1 and above)

ACCESS POINT SUPPORT

- R720
- R710
- R610
- R510
- H510
- T610
- T310
- E510

SMARTZONE OS SUPPORT

- SmartZone and Virtual SmartZone 3.6.1.2

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	• Zigbee 3.0 • BLE • iBeacon • Eddystone

MANAGEMENT

- RESTful APIs for ecosystem integration
- Management GUI

RUCKUS IoT MODULES

I100	
Protocol	• Zigbee 3.0, BLE, iBeacon, Eddystone (software configurable)
Device Capacity	• 25 (Zigbee) • 12 (BLE)
Interfaces	• USB 2.0, Type A
Memory	• RAM: 256KB • Flash: 1MB
Output Power	• 16.5dBm (max)
Power Consumption	• 500mW (max)
Current Draw	• –100mA on 5V (max)
Mechanical	• Dimensions: 47.83 x 18 x 8.25mm • Max weight: 85 grams
Temperature	• -40 to 70°C
Certifications	• FCC and ETSI

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.

RUCKUS™ an ARRIS company

350 West Java Dr., Sunnyvale, CA 94089 USA

www.ruckusnetworks.com