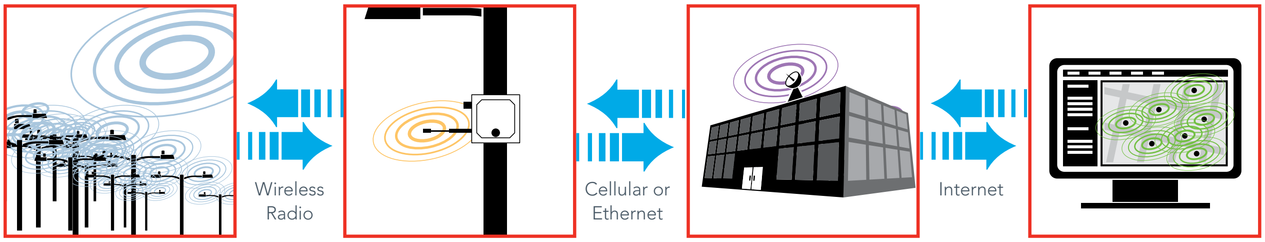
ROAM – Evolution in Cyber Security

Overview

Introduced in 2006, the ROAM® system was an innovative offering, for municipal, multi-site and large institutional customers, designed to monitor and control outdoor lighting fixtures, minimize maintenance costs, and optimize energy use leveraging wireless technology. The ROAM solution has now gone through a major architectural upgrade to enhance system security and enable the product to meet the requirements of recent security legislation such as California's IoT Security law (SB-327). The updated architecture includes a new ROAM ER900 gateway and many enhancements to our ROAM cloud capabilities to provide a more secure environment designed to protect against evolving cyber-attacks.



ROAM Nodes

ROAM Gateway

Cloud or Locally Hosted ROAM Network Operations Center (NOC)

ROAM Customer Portal

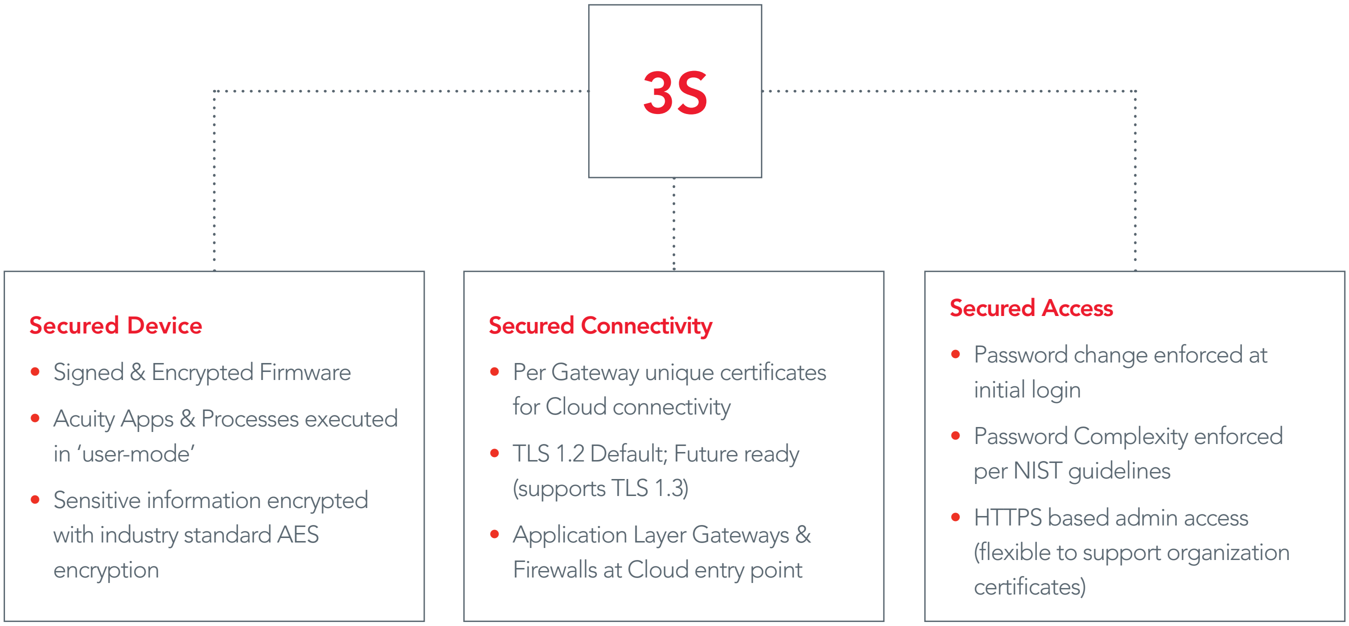
Note: For details around migration of existing ER700 ROAM Gateways, please refer to Acuity Brands announcement here.

Security Architecture

A recent survey[1] by SonicWall Capture Labs Threat research team found that malware attacks against Internet of Things (IoT) devices in July 2020 rose 50% compared to the prior year. The trend demands commitment from vendors to secure their connected devices. In keeping with Acuity Brands' commitment to security, we have redesigned the ROAM gateway, the ROAM system architecture and its integrations with other related components, such as the cloud services and data storage. With security in mind, we implemented the Triple-S (3S) approach during the design and development phases of our ROAM update. The Triple-S approach helps to separate the security architecture into three different domains and implement industry standard controls accordingly for each domain.

The 3-S approach include:

1. Secure the device
2. Secured the connectivity
3. Secure the access



3S

Secured Device

- Signed & Encrypted Firmware
- Acuity Apps & Processes executed in 'user-mode'
- Sensitive information encrypted with industry standard AES encryption

Secured Connectivity

- Per Gateway unique certificates for Cloud connectivity
- TLS 1.2 Default; Future ready (supports TLS 1.3)
- Application Layer Gateways & Firewalls at Cloud entry point

Secured Access

- Password change enforced at initial login
- Password Complexity enforced per NIST guidelines
- HTTPS based admin access (flexible to support organization certificates)

Secure the Device

In order to secure the ROAM ER900 gateway to thwart most common attack vectors, we leveraged industry standard practices to protect the device- chipset, firmware, and interfaces. Similarly, we have protected the software image by signing and encrypting the firmware to prevent malicious actors from uploading modified images to the gateways.

Secure the Connectivity

ROAM gateways are integrated to the Acuity cloud for monitoring and remote management purposes. To provide security for this integration, the link between the ROAM ER900 Gateways and Acuity cloud uses industry standard TLS 1.2 protocol specifications (by default). Each gateway uses unique certificates to protect against the threat of common attacks such as BORE (Break Once, Run Everywhere).

Secure the Access

Occasionally, the appropriate support teams may need to access the gateway to monitor usage or system information. Enforced change of password at initial login, password complexity baseline, and support for encrypted HTTPS protocol are examples of a few of the controls implemented at the access layer. The gateways also restrict inbound access only to permissible ports.

Acuity Product Security Improvement Promise

Acuity Brands is fully committed to developing and maintaining secure products and has a robust Product Security Program in place. Our products and services are audited periodically by third parties for validation of security controls. Through the security governance model, we incorporate core security principles and best practices in the product development lifecycle. Our security governance policies include standards-based policies, industry best practices and guidelines.

Acuity Brands has a mature Product Security Incident Response Team (PSIRT) which is a member of the Forum of Incident Response and Security Teams (FIRST). Our PSIRT works with appropriate internal and external resources for coordinating stakeholder interests regarding security concerns that potentially affect Acuity Brands products and services. For more information, contact the Acuity Brands cybersecurity team at:

www.AcuityBrands.com/PSIRT

[1] https://www.sonicwall.com/news/sonicwalls-mid-year-cyber-threat-report/

© 2020 Acuity Brands Lighting, Inc. All rights reserved. | AC_555196_0920