SECURED RETAIL
NETWORKS, INC

Managed Wireless Services

The Ideal Wireless Solution for Your Business

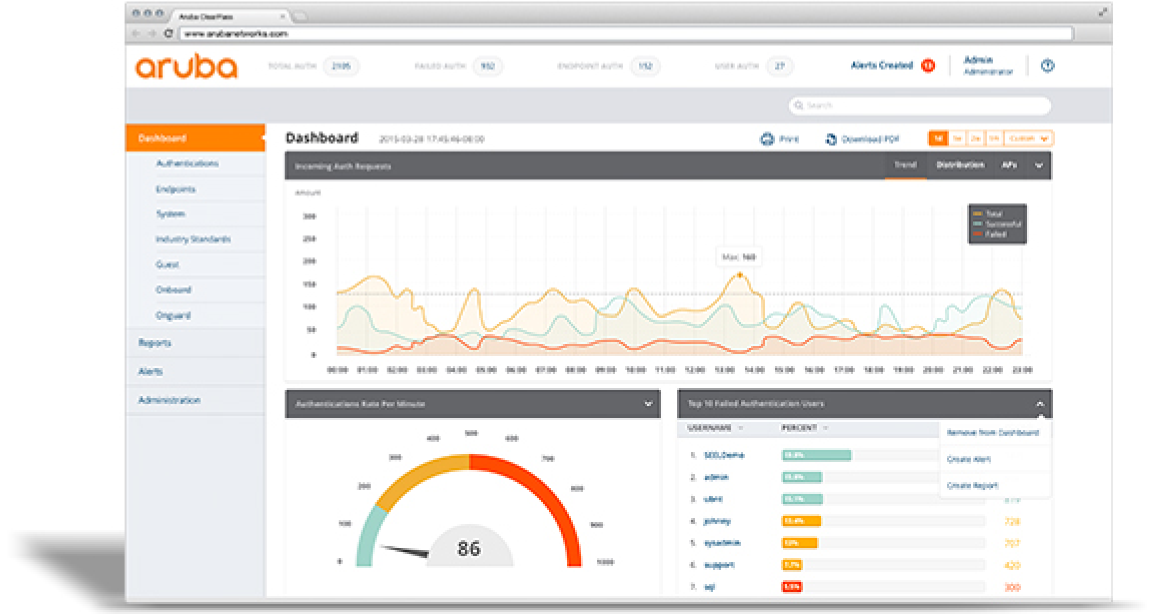
Secured Retail Networks provides Managed Wireless (802.11) services that deliver high-speed wireless connectivity to devices such as laptops, tablets, smartphones and IoT devices. We offer a variety of wireless service offerings to meet an extensive range of customer needs, ranging from private wireless LANs to public guest and vendor access connectivity. SRN manages multiple access points at both large corporate environments and small branch facilities. We provide a secure and compliant wireless network to customers utilizing cloud- or on premise-based global management, authentication and reporting systems.

On Premise Managed Wireless – In Depth

Private Wireless LAN (WLAN)

Local or dedicated controller management solution options will vary based on the underlying hardware platform selected by the customer. Our Wireless Local Area Network (WLAN) service enables customer locations to utilize wireless for back-office use by authorized personnel and hand-held devices for accessing corporate resources on the LAN. WLAN access is segregated from private LAN traffic, such as Point of Sale traffic, via creation of separate Virtual LANs (VLAN) to adhere to PCI DSS requirements. WLAN services support use of local on-board wireless as well as dedicated access points (APs) to provide complete wireless coverage throughout the customers' locations.

Wireless Networks: SRN configures wireless access points with service set identifiers (SSIDs), often referred to as a network name, which uniquely names a WLAN. This name allows wireless enabled devices to connect to the desired network when multiple independent networks operate in the same physical area. Multiple SSIDs are supported by the service to segment wireless device access capabilities to specific WLANs.



Authentication: SRN configures wireless devices to communicate with optional customer-provided radius servers (802.1x), enabling access controls and denying unauthorized authentication credentials. Additionally, SRN can configure a static Wireless Protected Access II (WPA2) key that is used to authenticate end users. If WPA2 is used, SRN will rotate that key in accordance with customer policies.

Rogue Wireless Detection/Wireless Intrusion Detection: Included in our WLAN service to meet PCI DSS or security best practice requirements. Rogue Wireless Detection entails monitoring the radio spectrum for the presence of unauthorized APs. Upon detecting the presence of an unauthorized AP, an alert is triggered and sent to the SRN team for analysis and action.

Monitoring and Support: SRN proactively monitors the availability and health of Wireless Access Points, and provides alerts when outages and/or health issues are determined. Upon trouble ticket creation, SRN network operations troubleshoots Wireless outages and/or health issues to determine cause and restore service. For in warranty wireless equipment, SRN ships preconfigured replacement device via overnight shipping to remedy the outage.

Field Maintenance: A field maintenance technician is dispatched to replace faulty device and/or troubleshoot with SRN certified engineers, so no technical expertise from the customer is required on-site.

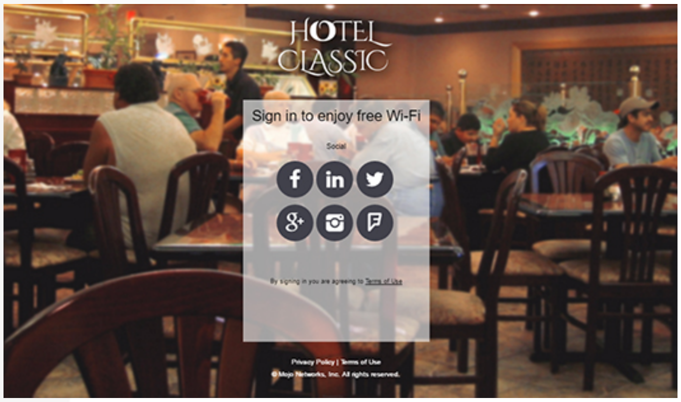
Bandwidth Shaping: SRN provides the ability to rate limit throughput by SSID to prevent Wireless networks from consuming bandwidth that is needed for non-Wireless or business critical applications.

Software Updates / Vulnerability Patching: Included in SRN's managed solution is regular software patching to keep devices current and stay ahead of zero-day attacks as well as ensure our customers are benefitting from the last improvements in software. We also track vulnerabilities and work directly with the hardware/software vendors to apply workarounds and/or patches as soon as they become available and have been tested in our lab.

Change Management: Using our PCI compliant and security best practice change management process, we test all configuration changes in a non-production environment. All changes are submitted for customer approval and stakeholders notified. SRN then manages the process during customer approved change process to update thousands of access points and associated systems.

Guest WLAN

SRN can enable customers with a public wireless zone for guests and devices to publicly connect to the Internet. Hotspot access is segregated from private LAN traffic, such as business systems, via creation of separate virtual LANs (VLAN) and security zone to adhere to PCI DSS and security best practice requirements.

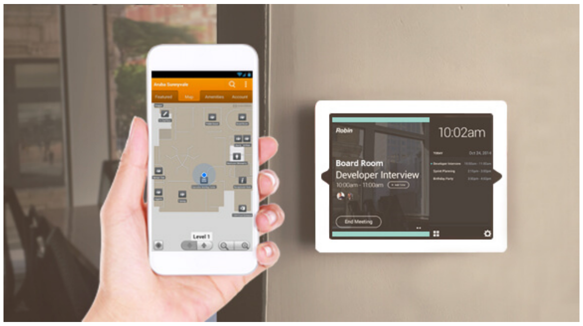


Sign in to enjoy free Wi-Fi

By signing in you are agreeing to Terms of Use

© Mojo Networks, Inc. All rights reserved.

Vendor WLAN



With the explosion in Internet of Things (IoT) devices that support building automation and the overall digitization of the workplace that is enabled by wireless, SRN will create and manage a separate VLAN and security zone to adhere to PCI DSS and security best practice requirements.

SLA Driven Support

SRN configured alerts will proactively open a trouble ticket within the SRN ticketing system for availability and security incidents. For all other problems, level 2 and level 3 help desk support are available 8x5 PST with an after-hours callback option for priority 1 incidents.

Certified Professionals

Our design and support engineers carry numerous certifications in wireless networking and security. These accreditations include vendor agnostic certifications as well as specific certifications in HP Aruba and associated management platforms as well as Fortinet and Mojo Networks (formerly Airtight networks). We require all our engineers to stay current on the latest technologies and threats that exploit wireless network vulnerabilities.

aruba NETWORKS CERTIFIED ACMP MOBILITY PROFESSIONAL

aruba NETWORKS CERTIFIED ACMX MOBILITY EXPERT

aruba NETWORKS CERTIFIED ACSP SOLUTIONS PROFESSIONAL

aruba NETWORKS CERTIFIED ACCA CLEARPASS ASSOCIATE

aruba NETWORKS CERTIFIED ACCX CLEARPASS EXPERT

aruba MOBILE FIRST EXPERT

FORTINET Network Security Expert 8

mojo Networks

Give us a call today at 949.390.6700, and we'll discuss with you what we can do to help your business reach its apex of communications.