Cloud and Managed Authentication Services

RUCKUS AND CLOUDESSA PROVIDE SECURE FLEXIBLE ACCESS AUTHENTICATION OPTIONS

Cloud and Managed Authentication Services

Early Wi-Fi installations were often viewed as overlay, limited purpose networks with small coverage areas. Now, with more and more devices supporting Wi-Fi connectivity and end-users demanding full mobility, Wi-Fi networks are mission critical and increasingly the only network access option in schools, hotels, stores and other businesses.

WLAN deployments and upgrades must deliver comprehensive, robust performance with full coverage across the entire location while ensuring robust end-user access security — even when there are limited on-site IT resources.

Ruckus Wireless WLANs with ZoneDirector controllers deliver best in class wireless performance even in the most challenging environments, which is a critical foundation for any wireless service. Ruckus also offers a number of innovations to help large and small organizations deploy a secure wireless LAN. Ruckus Dynamic PSK (DPSK) can provide simple encryption key administration to increase encryption strength over common WPA-PSK deployments. This is particularly valuable to organizations that are not ready for a full RADIUS based 802.1X deployment, or don’t have the resources to deploy and maintain such a network. DPSK is a perfect balance between the right level of security for your organization with the right level of convenience for your IT resources and end users alike.

Cloudessa augments the Ruckus built-in authentication functionality with a cloud based managed RADIUS/AAA platform that supports both robust, enterprise-class WPA2 / 802.1X for securing the access of users who will be accessing enterprise LAN applications, and flexible Captive Portal browser based logins for hotspots and, guest, customer, and visitor access.

Cloudessa securely authenticates and controls network access for all users and devices without the cost and complexity of an on-premises RADIUS deployment.
Cloud and Managed Authentication Services

The service can either be deployed and managed by end user organizations, or delivered as a managed service by Ruckus value-added resellers.

Either way, services based on Cloudessa RADIUS provide the following customer benefits:

- **Strong Wi-Fi security** — Cloudessa RADIUS fully supports industry-standard Wi-Fi security protocols, including 802.1X, WPA2-Enterprise, and Captive Portal browser based logins.

- **Simplified network management** — The Cloudessa platform enables user authentication against virtually any enterprise (AD, SQL, SAML) or cloud / social network user store (Google Apps, Facebook, Twitter, and other OAuth user stores)

- **Single Authentication Solution for all Remote Access** — Cloudessa provides a centralized access security platform for all Wi-Fi, VPN, and Firewall user authentication;

- **Enhanced network capabilities**, such as guest access or customer engagement / captive portal platform;

- **Reduced security infrastructure spend** — Whether you run Cloudessa RADIUS in the public cloud or on a virtual machine, it will dramatically cut your hardware, administrative and licensing expenses versus a traditional on-site RADIUS appliance.

This diagram illustrates how a multi-location organization such as a retail chain, school district or enterprise can leverage the Cloudessa RADIUS service to authenticate and authorize Wi-Fi users and devices via WPA2-Enterprise and 802.1X.

**FIGURE 1: Wi-Fi with WPA2 / 802.1x Security**

---

**Page 2**
Cloud and Managed Authentication Services

1. End users connect to their local Wi-Fi network via an 802.1X client; credential security during the exchange is protected by the use of EAP-TTLS or EAP-PEAP.

2. The Ruckus ZoneFlex access point (or other network gateway) communicates with Cloudessa RADIUS in the public cloud to determine whether the user is authorized to connect and, if so, how to configure the connection.

3. Cloudessa RADIUS authenticates the Wi-Fi user against the enterprise’s existing user name and password database — for example, Active Directory, LDAP, SQL or a SAML server- located in the enterprise data center; authentication against the Google Apps cloud-based user store, and social network sites such as Facebook, Twitter, and LinkedIn and a native database are also supported.

4. If Cloudessa RADIUS determines the user is authorized to connect, it passes the authorization parameters back to either the ZoneFlex AP or ZoneDirector controller to configure the appropriate level of access rights for the user.

5. Once authenticated onto the network with appropriate access level, Wi-Fi user’s data security is protected by WPA2-Enterprise.

For Ruckus Partners that include Cloudessa RADIUS as part of their managed service offerings, Cloudessa creates new business opportunities with:

- Small businesses who have not yet adopted RADIUS based Wi-Fi security because the cost or complexity has been prohibitively high. With Cloudessa RADIUS, customers pay only for the users that access the network, and incur no hardware or software maintenance costs.

- Larger enterprises and government agencies who are migrating applications and infrastructure to the cloud; these organizations, who often already use on-premises RADIUS servers, are likely to be receptive to the cost savings and simplified management afforded by Cloudessa’s cloud-hosted RADIUS services.

- Guest, hotspot and co-working space operators who need a flexible and scalable RADIUS authentication capability that easily integrates with their Captive Portal platform.

Cloudessa provides a broad range of options for authenticating users, against virtually any existing enterprise, cloud, social network, or custom user store. A key advantage of Cloudessa RADIUS is that it can be deployed either as a public cloud service running in the AWS EC2 Cloud, either by the end-customer or by a managed services partner or as a Virtual Appliance. Ruckus Partners also have the opportunity to offer Cloudessa RADIUS as a “White-Label” managed service to end-customers.

Cloudessa RADIUS augments the built-in capabilities of Ruckus SmartCell and ZoneFlex access points and ZoneDirector Controller, enabling users to quickly and easily deploy advanced RADIUS based WPA 2 / 802.1X and Captive Portal access security, without the hassle or cost of on-premises servers.

For more information, please visit www.cloudessa.com/ruckus