M2M / Smart Meter / Specialty Networks

Cloudessa RADIUS – a cloud service that provides a managed RADIUS/802.1X access solution – makes it easy to deploy and administer RADIUS services on behalf of your customers. If you deliver cloud and managed WiFi solutions, manage the migration of apps to the cloud, or provide other managed IT services to your enterprise customers, Cloudessa RADIUS will let you expand your service offerings, strengthen your customer connections, and drive additional sources of recurring revenue – without having to install or maintain your own hardware or software.

Services based on Cloudessa RADIUS provide the following compelling benefits to customers:

- **Authenticate IP-enabled devices to the network** – Cloudessa RADIUS ensures that only authorized devices can join the network. It authenticates devices against a back-end database that contains device authentication information, such as one based on SQL or LDAP.
- **Record the usage of such devices to a log file** – Cloudessa RADIUS generates RADIUS accounting records that log when a device connects or disconnects, allowing administrators to understand network usage and uptime, and diagnose and fix problems.

Most M2M / IP enabled devices are authenticated onto the cellular data network by the carriers RADIUS server infrastructure. The carrier RADIUS server authenticates the device onto the network by validating its credentials against a listing of authorized devices maintained a data stores on their network.

New RADIUS as-a-Service Options

Cloudessa RADIUS offers an exciting new option for utilities, hospitals and other end-user organizations, to gain a higher level of access control, and for device manufactures to offer a managed authentication service for their customers, all without having to deploy or manage any on-premises servers.

With Cloudessa RADIUS, authentication requests are forwarded via Proxy RADIUS from the Carrier RADIUS server to the Cloudessa RADIUS server. Cloudessa RADIUS, a hosted, multi-tenant RADIUS server then authenticates the access request against the appropriate tenant RADIUS instance, against a data store directly updated and maintained by the end-user customer.

Under this deployment scenario, end user organizations gain added control over which devices are permitted on the network, and benefit from RADIUS usage logs, which can be used to validate service charges.

Device manufactures can work with Cloudessa, and offer their customers a managed authentication service, so the end user organization can get the control and insight of Cloudessa RADIUS, but on a managed service basis.

The benefits of this solution also apply in other deployment scenarios where there are cellular data access aggregators involved who aggregate device connections across multiple carrier networks, and scenarios where devices are capable of connecting to the network via either a WiFi (leveraging an WiFi roaming network) or Cellular connection.

Cloudessa
RADIUS-as-a-Service℠

Cellular Data Aggregators and WiFi Roaming Consortiums

Both Cellular data aggregators and WiFi roaming consortiums all also use RADIUS for authentication. Similar to the above carrier scenario, the data aggregator or the roaming consortium would Proxy RADIUS the authentication request to the Cloudessa RADIUS server, which would then authenticate the device against the access list maintained by the end-user customer, and create an appropriate log of the network access.

For more information about the use of Cloudessa RADIUS within an M2M network, or to speak with one of our technical professionals about your deployment requirements, please contact *sales@cloudessa.com*.