MSB micro SYSTEMS
ILLUMINATING NETWORK SOLUTIONS

CASEstudy

August 2017 ©MSB Micro

THE CHALLENGE

A nationally represented life insurance company posed an interesting problem for the mobile connectivity requirements of different areas of their business.

On the one hand, there were employees of the company requiring access to systems, facilities and data stored at the company's centralised data centre. Whilst off-site these requirements could range from simple access to email, access to tariff and pricing tools, through to access to client history and medical reports, amongst other requirements.

Secondly, there were a large number of external users (not company employees, but outside brokers, etc.) that required similar remote access to information in order to perform their functions.

Naturally, because of the confidentiality of this type of information, security was of prime concern to the company. Access to the company systems needed to be strictly controlled and secure.

An added requirement was the need to differentiate between the various types of users as well as to be able to measure and account for their individual data usage whilst using the remote access facilities. This information would be used to charge different divisions within the organisation as well as bill the outside brokers for the data that was used.

INDUSTRY:

Life Insurance (National)

The information provided, as an added challenge, needed to be made available as close as possible to real-time.

THE SOLUTION

Working in conjunction with their preferred Network Service Provider, two APNs (Access Point Names) were deployed using technologies such as 3G and LTE as the carrier medium. One APN would cater for company staff members and the other would allow connectivity for the brokers.

In order to satisfy the security component when connecting remotely, MSB Micro Systems designed and provided a solution that required the users to login to the APN using their Active Directory credentials even when off-site. This was found to be less confusing and facilitated ease of connectivity for staff members. The MSB-supplied RADIUS solution acted as a 'proxy server' sending authentication requests to the company's Active Directory implementation and would only allow connectivity if all was reported as correct. This gave the company central control over the more than 5,000 SIM cards that were in use by various staff members and brokers. With staff turnover being a factor in the industry, it was also easier to keep tabs on who was allowed access and who wasn't. By installing a MSB Micro value-added feature called Volume Tracking with Quotas (VTQ) the company was able to set monthly data volume quotas for individual users. Customer defined thresholds setup in the RADMIN portal facilitated early warning emails to be sent to administrator/s so that preventative action could be taken thus avoiding possible cost overruns or abuse.

The same feature, VTQ, also allowed for individual SIM cards to be assigned to one of the customer defined user groups set up in the RADMIN portal, e.g. Division, Cost Centre, Branch, Region, etc. This, in turn, allowed for full reporting of connectivity and data usage by user group.

The RADMIN portal also provided for a host of additional management information and statistics such as connection times and duration in near real-time. The Network Service Provider provides the RADIUS server with updated statistics and information at 30 minute intervals.

"In order to satisfy the security component when connecting remotely, MSB Micro Systems designed and provided a solution that required the users to login to the APN using their Active Directory credentials even when off-site."