Important Security Information

10 steps to help secure your IoT/M2M applications

Securing your device

1 Change the default password of your device/router.

2 Use the latest version of firmware from your hardware manufacturer.

3 Consider securing your device with a firewall.

4 Ensure that your devices are not tampered with.

Securing your SIM

5 Bar/block any services that you don't need using SIMPro – for example SMS or roaming.*

6 Consider IMEI locking services to ensure that your SIM is associated with the appropriate device.**

Manage and monitor your services

7 Actively manage user profiles for your SIMPro account.

8 Closely monitor usage by setting up SIMPro alerts and ensure that you review your bill every month.

Overlay private APN services

9 Consider encrypted Virtual Private Network (VPN) solutions, static IPs and direct interconnects .

10 Consider outbound IP whitelisting to ensure that data traffic can only be sent to defined end points.

*Some networks may not be able to bar specific services.

**IMEI locking is not available on all networks.

Wireless Logic Fixed Public IP service

Assigning a 'Fixed Public IP' address to a SIM will make the device, into which the SIM is inserted, directly accessible from the Internet. Wireless Logic do not provide inbound traffic filtering as part of this service.

Customers should ensure that they take relevant precautions to minimise this security risk.

Following these steps does not guarantee security for your applications, but they will minimise your risk.

If you notice any suspicious activity, or would like to discuss any of our services, please contact us.
Email **salesadmin@wirelesslogic.com** or call **0330 056 3300**

wirelesslogic.com