AM/AMM Product Bulletin – Device Configuration for AM/AMM 2.17.3

Recommended Changes for MGOS and ALEOS Devices to Comply with Security Changes in AM/AMM 2.17.3

AM/AMM 2.17.2 and 2.17.3 introduce a series of changes that improve the overall security of the AirLink solution. As part of these changes, we are restricting access between AirLink routers and gateways and the AM/AMM management system to require secure connections. This will restrict insecure communication, and after the upgrade to AM/AMM 2.17.3, it is possible that devices will not be able to communicate with the management system and will need to be manually reconfigured.

We recommend that you review the security bulletin *Security Improvements and Operational Impacts in AM/AMM 2.17.2.1 and 2.17.3* that we published in July 2022.

This product bulletin provides directions for the changes that should be made to your configuration prior to the AM/AMM being upgraded to 2.17.3. We have provided separate instructions for both MGOS and ALEOS devices.

For customers that need support with firewall configurations, we have published a reference article on the Source that we would recommend.

MGOS Devices (AirLink MG90)

All MGOS-based devices should be configured to use the management tunnel when connecting to an AM/AMM management system. Using the management tunnel ensures that the connection between the device and the management system is secured.

The settings described below are typically configured by default. We understand that some customers have made changes to disable them in the past. If you have made changes to these settings, we recommend that you return them to the default values to ensure the settings are correctly configured:

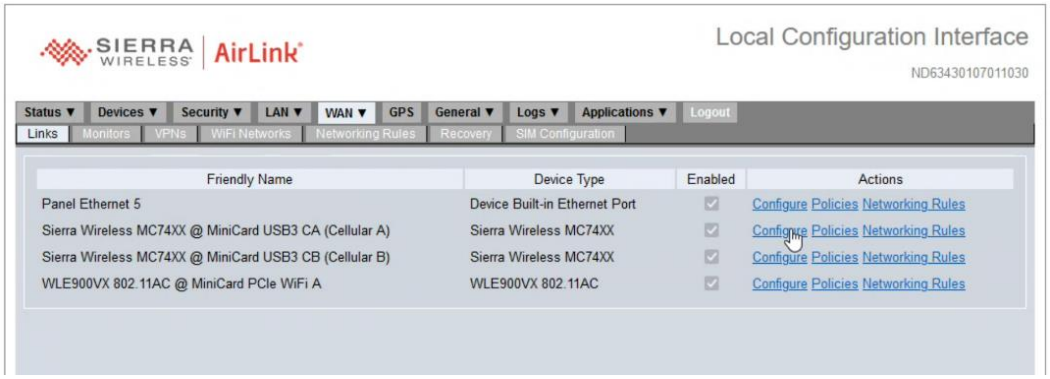

Figure 1: In the LCI - WAN --> Links – Click "Configure" to ensure each cellular radio is configured to use the Management Tunnel. If you use Ethernet or Wi-Fi as WAN, you may need to make similar changes to those interfaces.

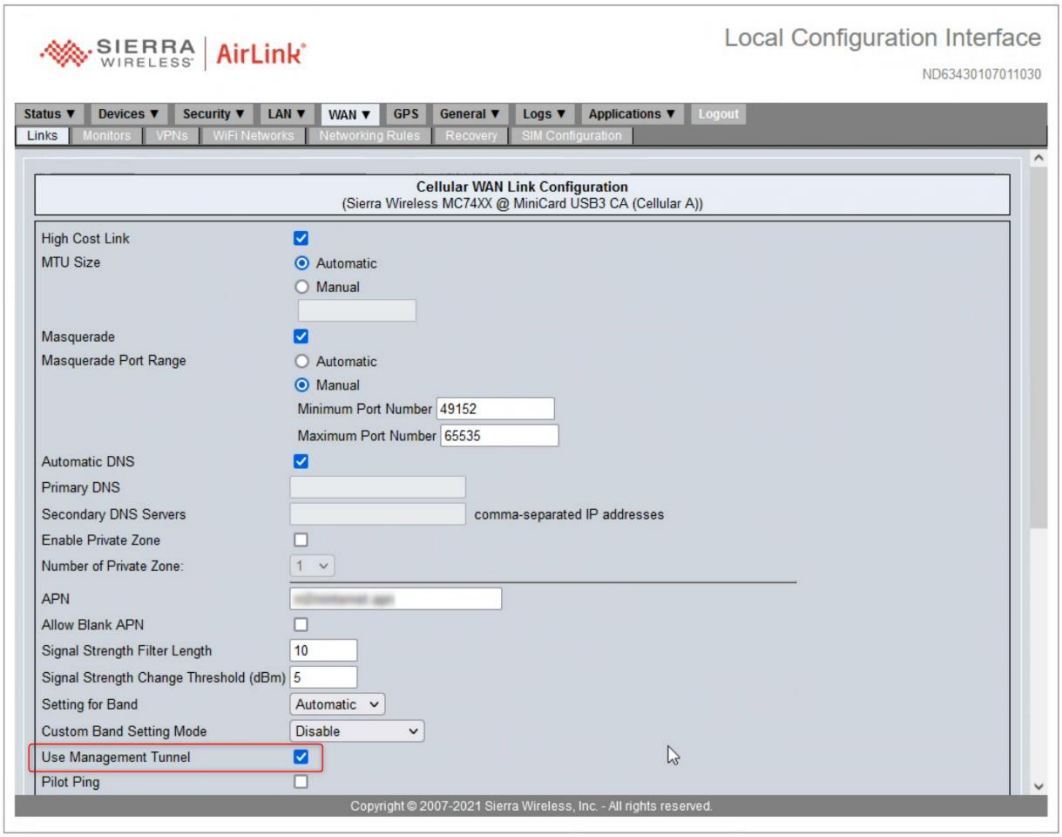

Figure 2: For each cellular radio, ensure the "Use Management Tunnel" box is selected.

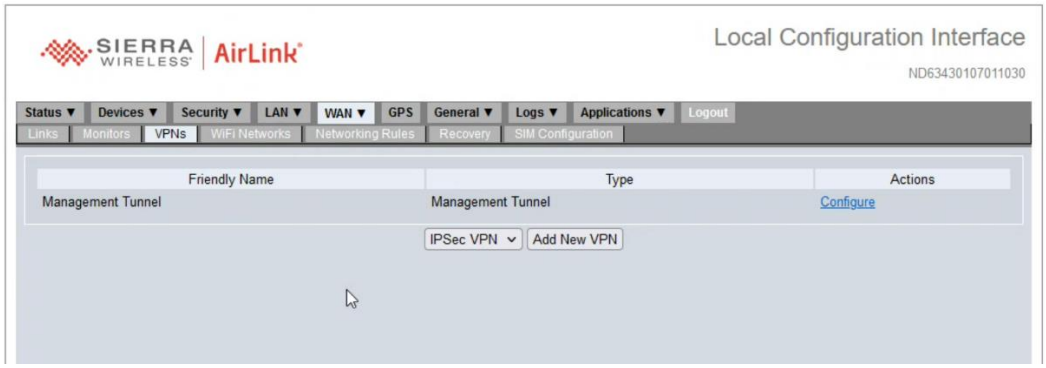

Figure 3: In the LCI - WAN --> VPNs – There should be a default "Management Tunnel" entry. Click "Configure" to ensure the Management Tunnel is correctly configured.

In the WAN/VPNs section of the LCI, click "Configure" and ensure that all the check boxes are selected.

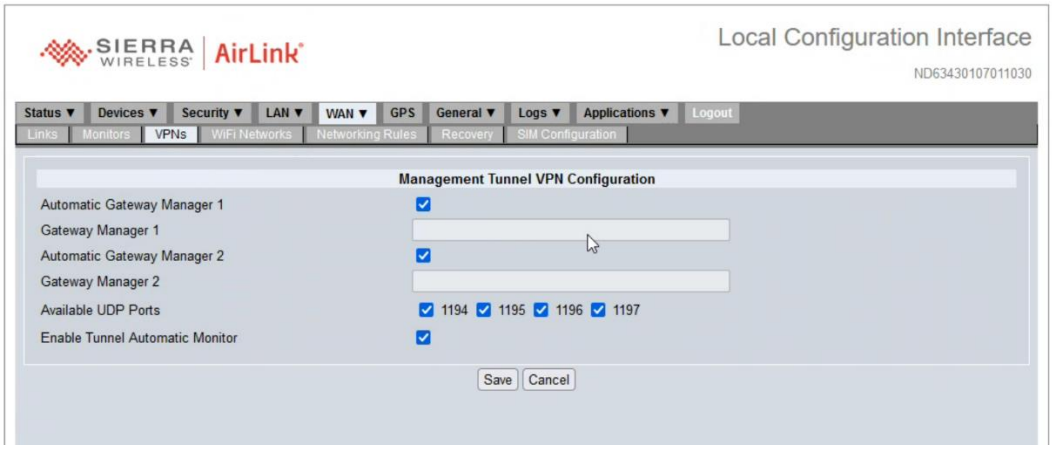

Figure 4: Ensure that all check boxes are selected.

Please ensure that your firewall is configured to allow for UDP traffic from the device to the management system over this protocol and port combination (UDP 1194-1197).

ALEOS Devices

All ALEOS devices should be configured to use the management tunnel when connecting to an AM/AMM management system. Using the management tunnel ensures that the connection between the device and the management system is secured. We recommend that you make the following configuration changes in ACEmanager to ensure these settings are correctly configured:

Ensure the server URL is set to use HTTPS instead of HTTP. Historically, some customers have configured their gateways to check in using MSCI on port 8082 (e.g. http://ammxxx.domain.com:8082/msci). These should be updated to use a secure channel (e.g. https://ammxxx.domain.com:8083/msci).

Set *AMM Management Tunnel* to "Enable" in the MSCI section of the ACEmanager interface. The default value for the AMM Management Tunnel Port can be set as the default (UDP 1190), or use any of the

ports in the range of 1190-1193. Please ensure that your firewall is configured to allow for UDP traffic from the device to the management system over this protocol and port combination.

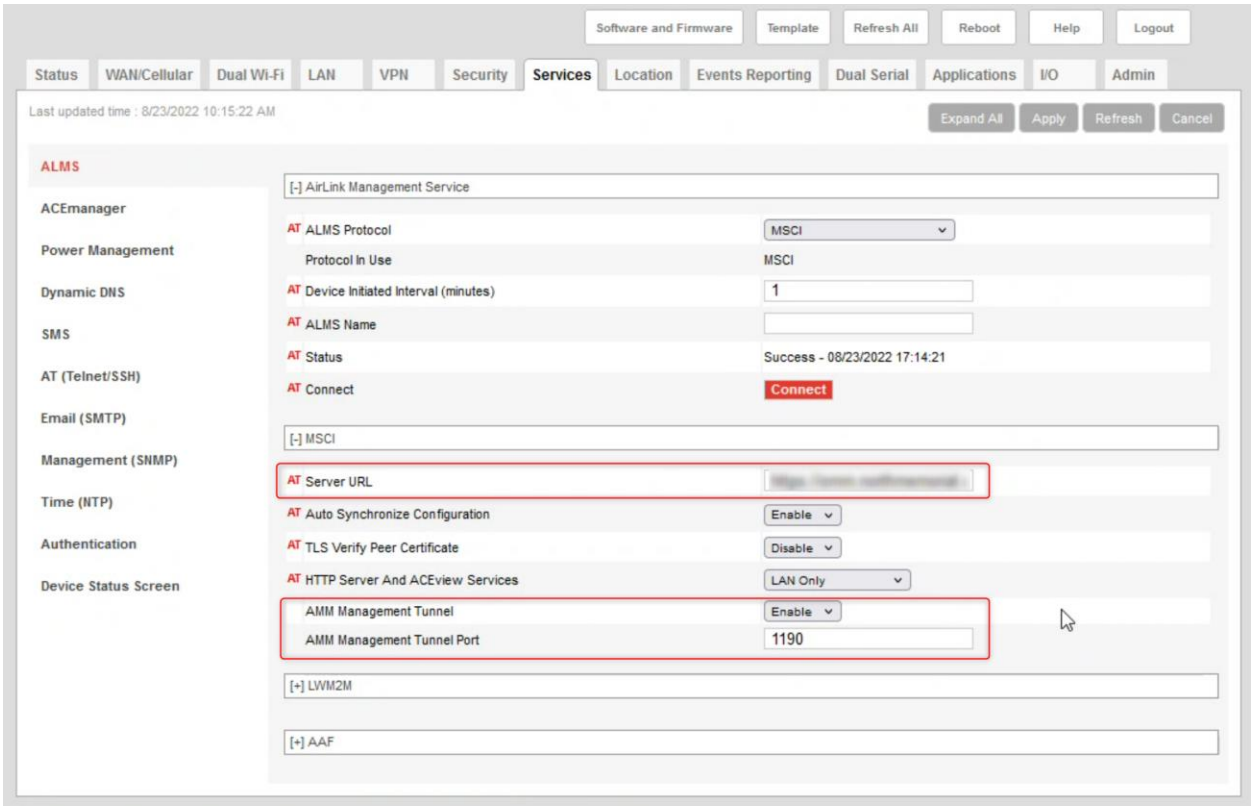

Figure 5: Ensure the three highlighted fields are configured correctly.

Please review your configurations and ensure your devices are correctly configured to protect your system prior to any upgrade to AM/AMM 2.17.3.