Important!

Action Required for Wireless Network Services API (aka UWS) Security Enhancement

Dear Wireless Network Services API (aka UWS) Customer,

Please read this important communication about possible changes to your applications and services that use Verizon's Wireless Network Services API, also known as UWS.

Wireless Network Services API Security Enhancement

Verizon is constantly working to maintain safe and secure access to all of our products and services. To enhance the security of our Wireless Network Services API, starting on **May 2, 2018**, we will require HTTPS protocol to retrieve the API WSDLs, initiate API sessions, and make all API calls. The WSDLs will no longer be available via HTTP and no API calls using HTTP requests will be accepted after this date.

Required Change

If your Wireless Network Services application was built using the WSDLs from our Software Development Kit (SDK), you do not need to make any changes. The WSDLs in the SDK have always specified only HTTPS connections.

If your application retrieves the API WSDLs from our servers dynamically, you must review your code to make sure that it uses HTTPS protocol to get the WSDLs and to send requests to the API. Note that the <soap: address location> value in all WSDLs will always be an HTTPS endpoint after this change.

Recommended Change

If your application has been retrieving the API WSDLs dynamically and your code review shows that you need to make changes to ensure the use of HTTPS, we recommend that you change your UWS account password when you put your code changes into production. Verizon recommends that all customers change their passwords at least once every 90 days, and switching from HTTP to HTTPS protocol is a good time to do it.

If you have any questions about this change, please contact your Verizon account representative or email us at IoTdeveloper@Verizon.com.

Thank you,

The Verizon IoT Team