Token-Based Authentication

The Token-Based Authentication

A *Token* can be used to authenticate a user or a device in place of a signature. This allows the creation of applications that do not need access to the passwords of the users and devices which are required for signature generation. Tokens provide a layer of simplicity, but must obey the following restrictions:

1. Token-based authentication is enabled for user and device requests only. Owner requests must use signatures.
2. Token-based authentication is enabled under secure (https) connections only.

A *Token* can be created or renewed using GenerateToken, RenewToken and VerifyCredentials APIs. It can then be passed as a parameter to requests instead of the signature.

When no longer needed, *Token* can be deleted and cleared using DeleteToken.

In order to use a token-based authentication, requests should specify the authentication mode by setting the value of the parameter “apsws. authMode” to “token”. In addition, the token should be passed with the parameter "apsdb.authToken", and the user with the parameter "apsws.id".

Example

```
http://sandbox.apstrata.com/apsdb/rest/[authenticationkey]/VerifyCredentials?apsws.time=[timestamp]&apsws.id=[userIdentifier]&apsdb.authToken=[token]&apsws.authMode=token
```