Service Authentication

M2M Service Authentication

After ARDC has set up your Handle service account you will be issued with a unique App Id (Application Identifier) and Shared Secret.

Example:

- App Id: 9b310b815997d2d3123456565f253b0e75e970f7
- Shared Secret: 5f4abcdeaa

Authentication with the Handle M2M service can then be carried out with either a combination of:

- your App ID and shared secret, OR
- your App ID and a registered IP address

The **Handle service authentication process** functions in the following way:

1. Upon receiving a request the Handle service will check that the provided App ID is valid. *If invalid the request will fail with an appropriate response.*
2. The service will then check to see if a Shared Secret has been provided in the request and if it matches the shared secret assigned to the provided App ID. If matched the request is authorised.
3. If the Shared Secret check fails, the Service will then then check to see if the IP address of the machine making the request is registered against the provided App ID. If registered the request is authorised. *If the IP address is not registered the request will fail with an appropriate response.*

Shared Secrets

Shared Secrets were introduced in the Handle service as an alternate and preferred method of authenticating against the M2M service where a user's IP address was unpredictable (e.g. cloud based virtual machines). The shared secret is a unique string which is automatically assigned by the Handle service upon account creation, and is only known by ARDC Handle Service Administrators and the account owner.

When authenticating using a Shared Secret, the secret can be passed in one of two ways.

1. The first and preferred way is to **include the secret in the HTTPS request header**. In order to do this the Shared Secret shall be appended to the App ID separated by a colon and then base64 encoded.
    - *PHP example:*
        - Authorization: Basic '.base64_encode($app_id.":".$shared_secret) ; OR

          $str = base64_encode($app_id.":".$shared_secret);
        - Authorization: Basic '.$str

2. The second way is to **pass your appID & shared secret in the body of the POST request.**

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<request name="mint">
    <properties>
        <property name="appId" value="exampleAppID"/>
        <property name="sharedSecret" value="exampleSharedSecret"/>
        <property name="identifier" value="ExampleUser"/>
        <property name="authDomain" value="ExampleAuthDomain"/>
    </properties>
</request>
```

« Handle Client Registration   Handle Service Policy Statement »