Using the MobileFirst Server to authenticate external resources

fork and edit tutorial (https://github.ibm.com/MFPSamples/DevCenter/tree/master/tutorials/en/foundation/8.0/authentication-and-security/protecting-external-resources/index.md) | report issue (https://github.ibm.com/MFPSamples/DevCenter/issues/new)

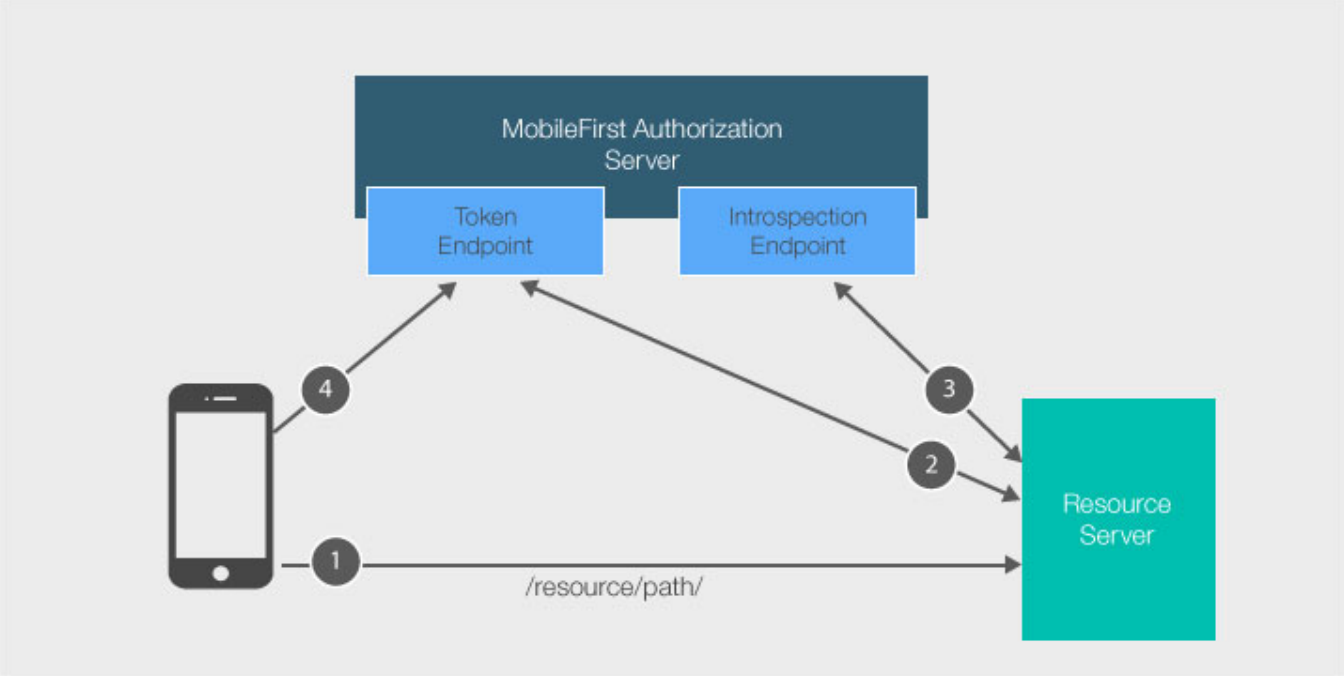
Overview

Protected resources can run on the MobileFirst Server (such as **Adapters**), or on **external servers**. Resources on external servers can be protected by using the validation modules that are provided with MobileFirst.

This tutorial covers how an external **resource server** can be protected by implementing a **filter** that validates a MobileFirst **access token**.

This can either be done entirely with custom code, or using one of MobileFirst Foundation's helper libraries that encapsulate part of the flow.

Flow



The MobileFirst Server has a component called the **introspection endpoint** which is capable of validating and extracting data from a MobileFirst **access token**. This introspection endpoint is available via a REST API.

1. An application with the MobileFirst Foundation client SDK makes a resource request call (or any HTTP request) to a protected resource with or without the `Authorization` header (**client access token**).
2. In order to communicate with the introspection endpoint, the **filter** on the resource server needs to obtain a separate token for itself (see the **confidential client** section).
3. The **filter** on the resource server extracts the **client access token** from step 1, and sends it to the introspection endpoint for validation.
4. If the MobileFirst Authorization Server determined that the token is invalid (or doesn't exist), the

resource server redirects the client to obtain a new token for the required scope. This part happens internally when using the MobileFirst Client SDK.

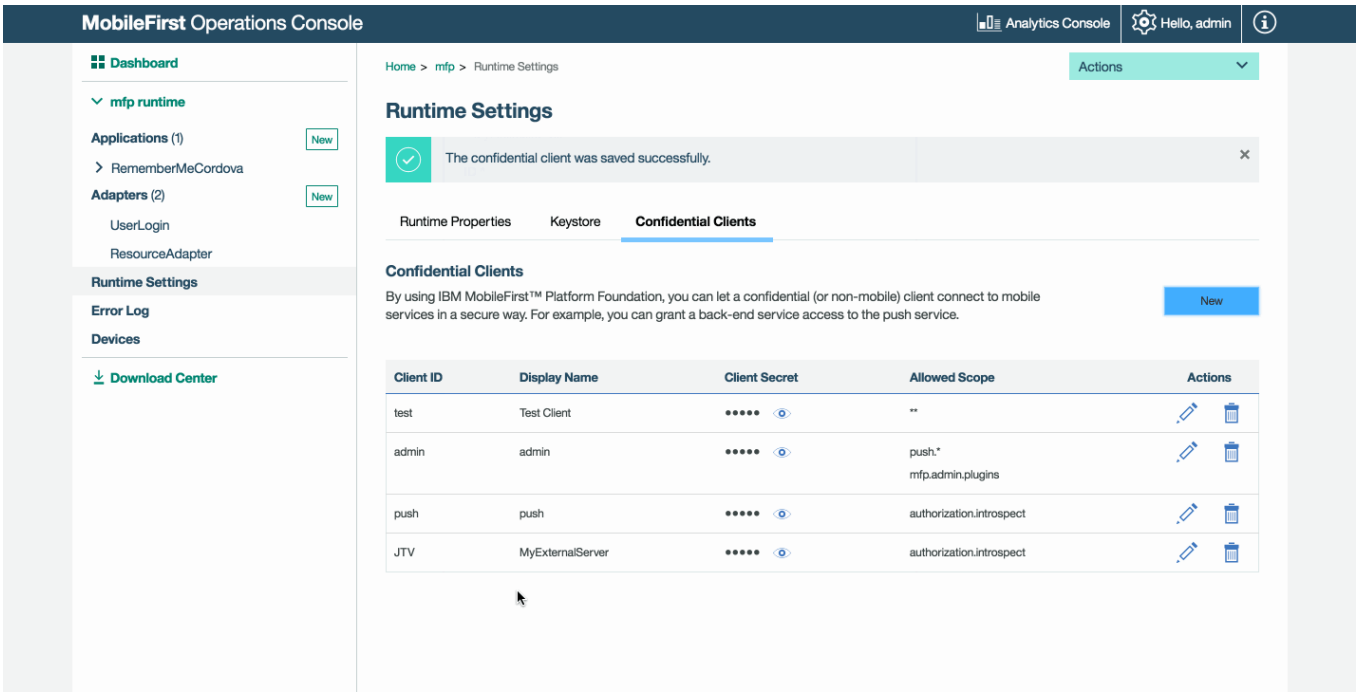
Confidential Client

Since the introspection endpoint is an internal resource protected by the scope `authorization.introspect`, the resource server will need to obtain a separate token in order to send any data to it. If you attempt to make a request to the introspection endpoint without an authorization header, a 401 response will be returned.

For the external resource server to be able to request a token for the `authorization.introspect` scope, the server needs to be registered as a **confidential client** via the MobileFirst Operations Console.

> Learn more in the Confidential Clients (../confidential-clients/) tutorial.

In the MobileFirst Operations Console, under **Settings → Confidential Clients**, add a new entry. Choose a **client ID** and **API secret** value. Make sure to set `authorization.introspect` as the **Allowed Scope**.



Implementations

This flow can be implemented manually by making HTTP requests directly to the various REST APIs (see documentation).
MobileFirst Foundation also provides libraries to help you achieve this on **WebSphere** servers using the provided **Trust Association Interceptor**, or any other Java-based filter using the provided **Java Token Validator**: