

Using the MobileFirst Server to authenticate external resources

Overview

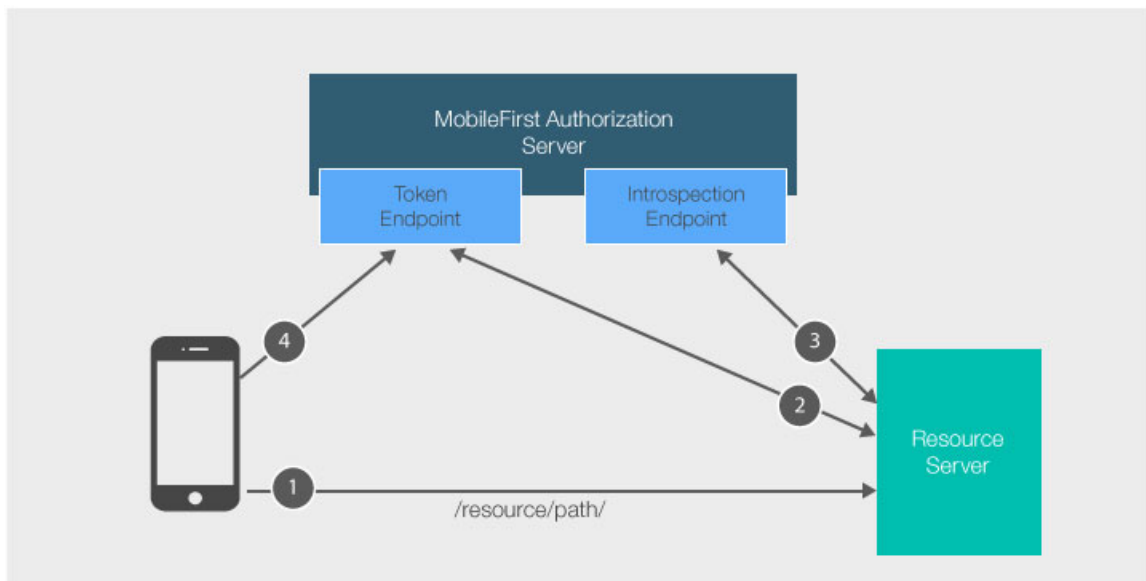
Protected resources can run on the MobileFirst Server (such as **Adapters**), or on **external servers**. You can protect resources on external servers by using the validation modules that are provided with MobileFirst Foundation.

In this tutorial, you learn how to protect an external **resource server** by implementing a **filter** that validates a MobileFirst **access token**. You can implement such protection either entirely with custom code, or by using one of the MobileFirst Foundation helper libraries that encapsulate part of the flow.

Prerequisite:

- Understanding of the MobileFirst Foundation security framework (../).

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. 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 the MobileFirst Client SD is used.

Confidential Client

Because the introspection endpoint is an internal resource protected by the scope `authorization.introspect`, the resource server needs 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 is 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**.

MobileFirst Operations Console

Analytics ConsoleHello, admin

Dashboard

mfp runtime

Applications (1)

New

Adapters (2)

New

UserLogin

ResourceAdapter

Runtime Settings

Error Log

Devices

Download Center

Home > mfp > Runtime Settings

Runtime Settings

The confidential client was saved successfully.

Runtime Properties

Keystore

Confidential Clients

Confidential Clients

By using IBM MobileFirst™ Platform Foundation, you can let a confidential (or non-mobile) client connect to mobile services in a secure way. For example, you can grant a back-end service access to the push service.

New

Client ID	Display Name	Client Secret	Allowed Scope	Actions
test	Test Client	*****	**	<div></div> <div></div>
admin	admin	*****	push.* mfp.admin.plugins	<div></div> <div></div>
push	push	*****	authorization introspect	<div></div> <div></div>
JTV	MyExternalServer	*****	authorization introspect	<div></div> <div></div>

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 by using the provided **Trust Association Interceptor**, or any other Java-based filter using the provided **Java Token Validator**:

Last modified on

IBM

Legal notices	Social	Site
(file:///home/travis/build/MFPSamples/DevCenter/ibm/legal-notices/)	Facebook	RSS feed
Privacy	(https://www.facebook.com/ibmmobiledev)	(file:///home/travis/build/MFPSamples/DevCenter/ibm/legal-notices/)
(http://www.ibm.com/privacy/us/en/)	Twitter	Open issue
Terms of use	(https://twitter.com/ibmmobiledev)	(https://github.com/MobileFirst-Platform-Developer-Center/DevCenter/issues/new)
(file:///home/travis/build/MFPSamples/DevCenter/ibm/legal-notices/terms-of-use/)	YouTube	Contribute
Third party notice	(https://www.youtube.com/channel/UCz1A4Kznci2Qusu97Q)	(https://github.com/MobileFirst-Platform-Developer-Center/DevCenter/blob/master/contributing.m
(file:///home/travis/build/MFPSamples/DevCenter/ibm/legal-notices/third-party-notice/)	GitHub	Report abuse
	(https://github.com/MobileFirst-Platform-Developer-Center)	(https://www.ibm.com/developerworks/commu