

Web api:

Delete Endpoints Preview features

^ Essentials

Display name : demo-web-app Supported account types : My organization only

Application (client) ID : 241cff78-cbb9-44bf-bd58-13e18bf55170 Redirect URIs : Add a Redirect URI

Directory (tenant) ID : 4533b917-a939-46b1-ada3-d18e7c400b0a Application ID URI : api://241cff78-cbb9-44bf-bd58-13e18bf55170

Object ID : 643a2332-d3cf-444f-91ca-554b286ba29a Managed application in L... : demo-web-app

demo-web-app | Expose an API

Search (Ctrl+/) Got feedback?

Overview Quickstart Integration assistant

Manage

Branding Authentication Certificates & secrets Token configuration API permissions Expose an API App roles Owners Roles and administrators | Preview

Application ID URI: api://241cff78-cbb9-44bf-bd58-13e18bf55170

Scopes defined by this API

Define custom scopes to restrict access to data and functionality protected by the API. An application API can request that a user or admin consent to one or more of these.

Adding a scope here creates only delegated permissions. If you are looking to create application-only type. [Go to App roles.](#)

+ Add a scope

Scopes	Who can consent	Admin con:
api://241cff78-cbb9-44bf-bd58-13e18bf55170/File.Re...	Admins and users	Read User f
api://241cff78-cbb9-44bf-bd58-13e18bf55170/Files.R...	Admins and users	Read user fi

Authorized client applications

Java Spring boot Code for Web API:

Application.proerties

```
# Specifies your Active Directory ID:
azure.activedirectory.tenant-id=4533b917-a939-46b1-ada3-d18e7c400b0a
# Specifies your App Registration's Application ID:
azure.activedirectory.client-id=241cff78-cbb9-44bf-bd58-13e18bf55170
# Specifies your App Registration's secret key:
azure.activedirectory.client-secret=4FKZ2L5.Lw2I~n--2Hu5M2Zh2RBX4W60-
# Specifies the list of Active Directory groups to use for authorization:
#azure.activedirectory.user-group.allowed-groups=group1

#azure.activedirectory.authorization-clients.graph.scopes=https://graph.microsoft.com
server.port=8080
```

```
@EnableWebSecurity
@EnableGlobalMethodSecurity(prePostEnabled = true)
public class AAD0Auth2ResourceServerExposeAPISecurityConfig extends WebSecurityConfigurerAdapter {
    @Override
    protected void configure(HttpSecurity http) throws Exception {
        http.authorizeRequests((requests) -> requests.anyRequest().authenticated())
            .oauth2ResourceServer()
            .jwt()
            .jwtAuthenticationConverter(new AADJwtBearerTokenAuthenticationConverter());
    }
}
```

```
@RestController
public class HelloController {

    @GetMapping("/files")
    @ResponseBody
    @PreAuthorize("hasAuthority('Files.Read')")
    public String files() { return "File read success."; }

    @GetMapping("/file")
    @ResponseBody
    @PreAuthorize("hasAuthority('SCOPE_File.Read')")
    public String file() { return "File read success."; }
}
```

Client api:

demo-client-app

Search (Ctrl+/) << Delete Endpoints Preview features

Overview	Essentials	Supported account types : My organization only
Quickstart	Display name : demo-client-app	Redirect URIs : 1 web, 0 spa, 0 public client
Integration assistant	Application (client) ID : f71fda0a-a8c7-4789-b78f-4be0ab598aa2	Application ID URI : Add an Application ID URI
Manage	Directory (tenant) ID : 4533b917-a939-46b1-ada3-d18e7c400b0a	Managed application in L... : demo-client-app
	Object ID : 72636232-d2ca-492e-97b3-66cbdef87a21	

Passing generated to to Web api:

GET localhost:8080/files Send

Params Authorization **Headers (9)** Body Pre-request Script Tests Settings

Headers 8 hidden

	KEY	VALUE	DESCRIPTION	...	Bulk Edit	Pres...
<input checked="" type="checkbox"/>	Auth	Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6I...				
	Key	Value	Description			

Body Cookies (1) Headers (12) Test Results Status: 401 Unauthorized Time: 181 ms Size: 416 B Save Respon...

GET localhost:8080/file

Params Authorization **Headers (9)** Body Pre-request Script Tests Settings

Headers 8 hidden

	KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/>	Auth	Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6I...	
	Key	Value	Description

Body Cookies (1) Headers (11) Test Results Status: 401 Unauthorized Time: 13 ms Si

Error detail:

```
XBhZGRyTjoiOTkuMjM0LjIyMjY4MCI5Im5hbWU0i01JU2XN0IFVzZXIiLCJvaWQiOiI3ZjExMDI0NS00YzgxLTRhYTUtOGUxNi11YWRlYjZlNGZkZmEiLCJyaCI6IjAuQVgwQUY3a3pSVG1wc1VhdG
UjFLiIsInNjcCI6IkZpbGUUUmVhZCBGaWx1cy5SZWFKIiwic3ViIjoicVJVVU8wcVfyZwzaG9RRVdKdG9LcnN3RFFMVVJRcm1LQXJxcERVczFyOCIsInRpZCI6IjQ1MzNiOTE3LWE5MzktNDZiMS
joidGVzZdFVzZXJAYXp1cmVkaXJlY3Rvcn1wb2Mub25taWYyZm91Y29tIiwidXBuIjoicVZlZdFVzZXJAYXp1cmVkaXJlY3Rvcn1wb2Mub25taWYyZm91Y29tIiwidXRpIjoiaU1hdUdHY0
DCJlYSkJN4iV06tCF8t6MMoumDTh9MVRqVCHLToA91XQAPjh80vLHGupdvU1HGv81S3EKmEILA0Cfwmc6MMxg6w3fUkpAc1VQ1ny-mRMANBkXWBS62sNCFyFHa_CDz51XM06xz-_MbwSh4SDkuDj
x7vGPJU4A9_ZhRW-mgHs4gt0hTYA9qP7HC_w9Xfloyj-pinIXC-MJfcZeJBiH0DBqMcap_gvsjwZe2-pgZLz_Jy51A3Z76ZCbC1DVXZStH8Pa2xnEeNRCUNb8hANnsb9dP-VTTJWR1ILeX8sQ"
User-Agent: "PostmanRuntime/7.26.10"
Accept: "*/*"
Cache-Control: "no-cache"
Postman-Token: "e25d484b-f72b-46ba-8a9f-8d56871b3bd7"
Host: "localhost:8080"
Accept-Encoding: "gzip, deflate, br"
Connection: "keep-alive"
Cookie: "JSESSIONID=2320A292849600BC2579580991FC3BAF"
Response Headers
WWW-Authenticate: "Bearer"
X-Content-Type-Options: "nosniff"
X-XSS-Protection: "1; mode=block"
Cache-Control: "no-cache, no-store, max-age=0, must-revalidate"
Pragma: "no-cache"
Expires: "0"
X-Frame-Options: "DENY"
Content-Length: "0"
Date: "Wed, 31 Mar 2021 14:37:51 GMT"
Keep-Alive: "timeout=60"
```