

Web API

va-poc-web-api | 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
- Manifest

Support + Troubleshooting

Application ID URI:

Scopes defined by this API

Define custom scopes to restrict access to data and functionality protected by 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 type. [Go to App roles.](#)

+ Add a scope

Scopes	Who can con
https://va-poc-web-api/Files.Read	Admins and u
https://va-poc-web-api/File.Read	Admins and u

Authorized client applications

Authorizing a client application indicates that this API trusts the application on this API.

Web API java code using spring boot:

```
@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."; }

    @GetMapping("/user")
```

```

@EnableWebSecurity
@EnableGlobalMethodSecurity(prePostEnabled = true)
public class AADOAuth2ResourceServerExposeAPISecurityConfig extends WebSecurityConfigurerAdapter {
    @Override
    protected void configure(HttpSecurity http) throws Exception {
        http.authorizeRequests((requests) -> requests.anyRequest().authenticated()) HttpSecurity
            .oauth2ResourceServer() OAuth2ResourceServerConfigurer<HttpSecurity>
            .jwt() OAuth2ResourceServerConfigurer<H>JwtConfigurer
            .jwtAuthenticationConverter(new AADJwtBearerTokenAuthenticationConverter());
    }
}

```

Application.properties:

```

# 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=a9c8d331-bdbf-458c-b861-b1878c73eeb1
# Specifies your App Registration's secret key:
azure.activedirectory.client-secret=03~ndMNaj6M_DYNW-U~8t0.hJjv_LkHwG.
#demo-web-api azure.activedirectory.client-secret=4FKZ2L5.Lw2I~n---2Hu5M2Zh2F
# 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

```

Client/web app:

* Name

The user-facing display name for this application (this can be changed later).

va-poc-client-api

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (rbc only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

Add a client secret

Description

Expires

In 1 year

In 2 years

Never

Add

va-poc-client-api | API permissions

Search (Ctrl+F) Refresh 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
Manifest

Support + Troubleshooting
Troubleshooting
New support request

Successfully granted admin consent for the requested permissions.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for rbc

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (2)				
Directory.Read.All	Delegated	Read directory data	Yes	✓ Granted for rbc
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for rbc
va-poc-web-api (2)				
File.Read	Delegated	Read user	No	✓ Granted for rbc
Files.Read	Delegated	Read user	No	✓ Granted for rbc

To view and manage permissions and user consent, try [Enterprise applications](#).

Generated Token using Client -api information:

client id : 4533b917-a939-46b1-ada3-d18e7c400b0a
secret : iMJPiHqn~6-uP_.J3-EMehw93.qjhBkh0z
redirect uri: http://localhost:8080/login/oauth2/code/
auth url: https://login.microsoftonline.com/4533b917-a939-46b1-ada3-d18e7c400b0a/oauth2/v2.0/authorize
token url: https://login.microsoftonline.com/4533b917-a939-46b1-ada3-d18e7c400b0a/oauth2/v2.0/token
scope: https://va-poc-web-api/File.Read