

Prerequisites

-
-
-
-
-
-
-
-
-

[eqmp7 mmm t bo f j bj bapbq m](#)

Note that upon completion of the manual setup I did circle back and investigated this method. It appears to be a wizard driven interface for the manual steps and could simplify the process however at the time of writing there is a disclaimer that prevents our use of this method in this scenario.

Note: An application registered here can't be used as a service principal. [Learn how to register a service principal](#)

Creating an App Reg



App registrations

App registrations

[+ New registration](#) [Endpoints](#) [Troubleshooting](#) [Refresh](#) [Download](#) [Preview features](#) | [Got feedback?](#)

Microsoft Azure Search resources, services, and docs (G+)

[Home](#) >

Register an application

* Name

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

NTTEEmbeddedDemo

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Sierra Systems Dev AD 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.

Select a platform

e.g. <https://example.com/auth>

Search (Ctrl+/)

DeleteEndpointsPreview features

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

Essentials

Display name
NTTEmbedDemo

Application (client) ID
dcd55b4a-163b-4683-a05b-35b233886ec3

Object ID
a9862e95-279c-4a90-b2c4-f1243f3d853c

Directory (tenant) ID
337a945d-ac66-4f8c-b739-e23a06080308

Client credentials
0 certificate, 1 secret

Redirect URIs
Add a Redirect URI

Application ID URI
Add an Application ID URI

Managed application in local directory
NTTEmbedDemo

Add a client secret



Description

Demo Embedded Content II

Expires

Recommended: 6 months



Search (Ctrl+/)

Got feedback?

- Overview
- Quickstart
- Integration assistant
- Manage
 - Branding & properties
 - Authentication
 - Certificates & secrets
 - Token configuration
 - API permissions
 - Expose an API
 - App roles
 - Owners
 - Roles and administrators

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) Client secrets (1) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
Demo Embedded Content II	12/3/2022	JoJ8Q~CRQY6MGWhQ0m~bx9z0qnu...	112bb9b4-f5dc-4483-a26f-901cfcdaca...

G 6 . 3 e . j u6w n r edfw d g

Security Group



Azure Active Directory



[Home](#) >



Sierra Systems Dev

Azure Active Directory

<<



Overview



Preview features



Diagnose and solve problems

Manage



Users



Groups



External Identities



Roles and administrators



Administrative units



Enterprise applications



Devices



New Group ...



Got feedback?

Group type * ⓘ

Security

Group name * ⓘ

PBIEmbeddedDemo

Group description ⓘ

A very top secret club

Membership type * ⓘ

Assigned

Owners

No owners selected

Members

No members selected



TMathews@sierrasyste...
SIERRA SYSTEMS DEV AD (SIERR...



Add members



Search ⓘ

NTTE



NTTEEmbedDemo

dcd55b4a-163b-4683-a05b-35b233886ec3

Power BI Config

Tenant settings

Admin portal

Developer settings

- **Embed content in apps**

The screenshot displays the Power BI Admin portal interface. On the left is a navigation sidebar with options: Home, Create, Data hub, Goals, Apps, Shared with me, Learn, Workspaces, and My workspace. The main content area is titled 'Admin portal' and contains a list of settings categories. 'Tenant settings' is highlighted with a red box. Below it, a list of options includes Usage metrics, Users, Premium Per User, Audit logs, Capacity settings, Refresh summary, Embed Codes, Organizational visuals, Azure connections, Workspaces, Custom branding, Protection metrics, and Featured content. To the right of the 'Tenant settings' list, the 'Developer settings' section is visible, also highlighted with a red box. Within 'Developer settings', the option 'Embed content in apps' is highlighted with a red box. Below this option, a toggle switch is shown in the 'Enabled' position, also highlighted with a red box. The text 'Enabled for the entire organization' is displayed below the toggle. Further down, the 'Apply to:' section shows three radio button options: 'The entire organization' (selected), 'Specific security groups', and 'Except specific security groups'. At the bottom right of the settings area are 'Apply' and 'Cancel' buttons.

- **Allow service principals to use Power BI APIs**

Developer settings

- ▶ Embed content in apps
Enabled for the entire organization

- ◀ Allow service principals to use Power BI APIs
Unapplied changes

Web apps registered in Azure Active Directory (Azure AD) will use an assigned service principal to access Power BI APIs without a signed in user. To allow an app to use service principal authentication its service principal must be included in an allowed security group. [Learn more](#)

☒ Enabled

⚠ Service principals can use APIs to access tenant-level features controlled by Power BI service admins and enabled for the entire organization or for security groups they're included in. You can control access of service principals by creating dedicated security groups for them and using these groups in any Power BI tenant level-settings. [Learn more](#)

Apply to:

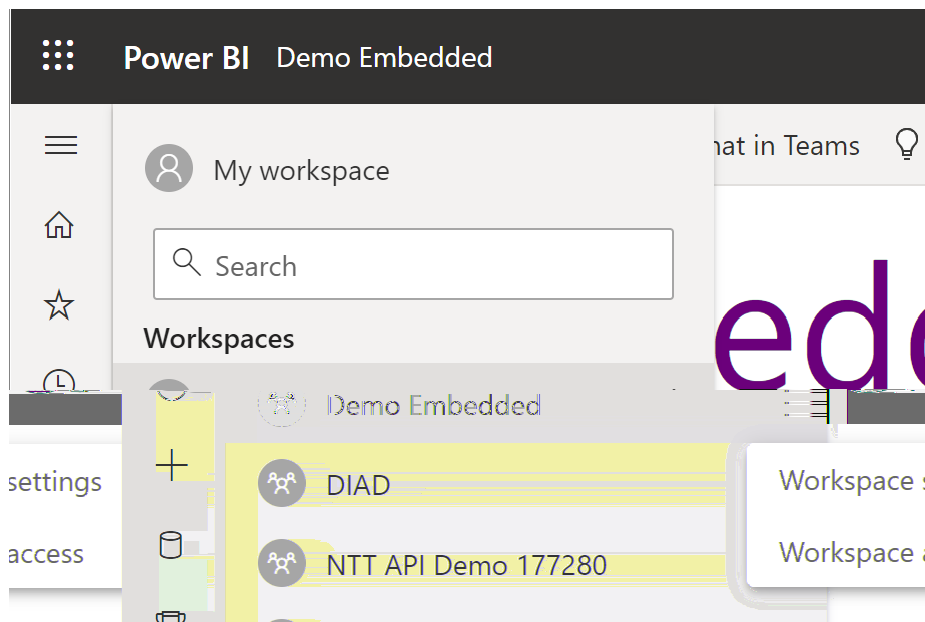
- ☐ The entire organization
- ☒ Specific security groups (Recommended)

Enter security groups

☐ Except specific security groups

Apply

Cancel



Access

NTT Embedded

NTT Embedded Demo AppID: dcd55b4a-163b-4683-a05b-35b233886ec3

Add admins, members, or contributors. [Learn more](#)

NTTEm

Member

Add

Search

NAME	PERMISSION
NTTEmbedDemo (Service Principal) ⓘ	Member
Trevor Mathews ⓘ	Admin

Setup Completion

-
-
-
-
-

Client ID



Our Example

^ Essentials	
Display name	Client credentials
NTTEmbedDemo	0 certificate, 1 secret
Application (client) ID	Redirect URIs
dcd55b4a-163b-4683-a05b-35b233886ec3	Add a Redirect URI
Object ID	Application ID URI
a9862e95-279c-4a90-b2c4-f1243f3d853c	Add an Application ID URI
Directory (tenant) ID	Managed application in local directory
337a945d-ac66-4f8c-b739-e23a06080308	NTTEmbedDemo
Supported account types	
My organization only	

Workspace ID



powerbi.com/groups/**97341742-1a52-416b-a331-e6c2c78e7a4e**/reports/

Admin portal

- Tenant settings
- Usage metrics
- Users
- Premium Per User
- Audit logs
- Capacity settings
 - Refresh summary
- Embed Codes
- Organizational visuals
- Azure connections
- Workspaces**
- Custom branding
- Protection metrics
- Featured content

Workspaces

View personal and group workspaces that exist in your organization. To change users' ability to create workspaces, see [Tenant settings](#).

Refresh Export Details Edit Access Capacity

Name	Description	Type	State
TemplateAppTest		Workspace	Active
		Workspace	Orphaned

Our Example

app.powerbi.com/groups/f538985c-629f-4137-8eed-e6ab1a68b569/reports/377c25db-a32e-4e3f-af20-b0d5fce5e4fc/ReportSection


c 0565 3/6c .04 5bba b3 . 35 36

Report ID



/reports/**de0db6db-232f-4807-b5b5-1abe1d71da76**/ReportSection

Our Example

 app.powerbi.com/groups/f538985c-629f-4137-8eed-e6ab1a68b569/reports/377c25db-a32e-4e3f-af20-b0d5fce5e4fc/ReportSection

044 / a 0/b b0c c/ a c b b c

Client secret



Our Example

Home > App registrations > NTTEmbedDemo

NTTEmbedDemo | Certificates & secrets

✕

Search (Ctrl+ /)

«

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) Client secrets (1) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
Demo Embedded Content II	12/3/2022	JoJ8Q~CRQY6MGWhQ0m~bx9z0qnu...	112bb9b4-f5dc-4483-a26f-901cfdbca...

G 5 . 3 e . j u6w n r edfw d g

Tenant ID

✓

✕

✕

✓

Our Example

^ Essentials

Display name

[NTTEmbedDemo](#)

Application (client) ID

dcd55b4a-163b-4683-a05b-35b233886ec3

Object ID

a9862e95-279c-4a90-b2c4-f1243f3d853c

Directory (tenant) ID

337a945d-ac66-4f8c-b739-e23a06080308

Supported account types

[My organization only](#)

Client credentials

[0 certificate, 1 secret](#)

Redirect URIs

[Add a Redirect URI](#)

Application ID URI

[Add an Application ID URI](#)

Managed application in local directory

[NTTEmbedDemo](#)

Visual Studio Project Example

```
<appSettings>
  <add key="webpages:Version" value="3.0.0.0" />
  <add key="webpages:Enabled" value="false" />
  <add key="UnobtrusiveJavaScriptEnabled" value="true" />

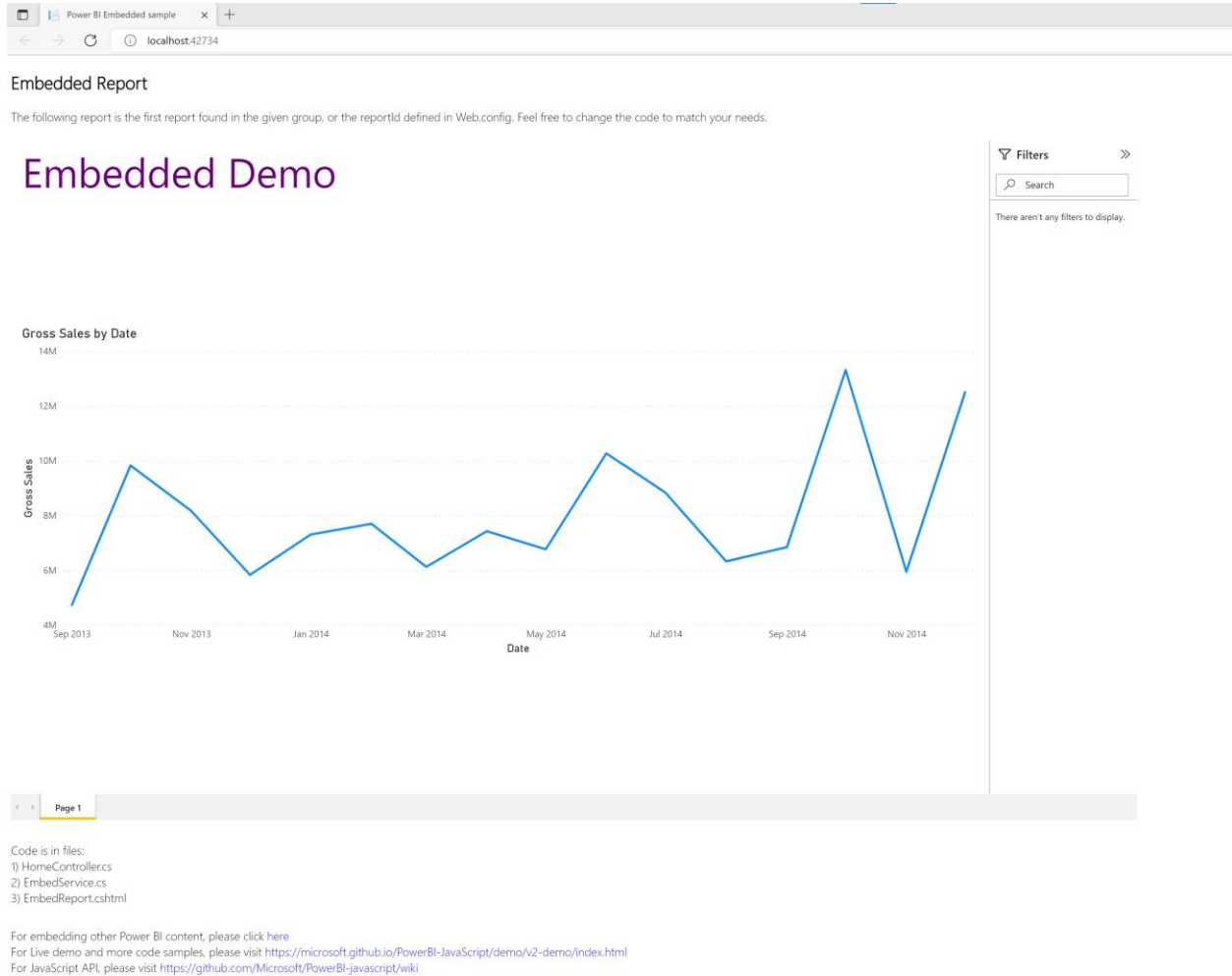
  <!-- Two possible Autentication method:
    - For authentication with master user credential choose MasterUser as AuthenticationType.
    - For authentication with app secret choose ServicePrincipal as AuthenticationType.
    More details here: https://docs.microsoft.com/en-us/power-bi/developer/embed-service-principal
  -->
  <add key="authenticationType" value="ServicePrincipal" />
  <!-- Common configuration properties for both authentication types -->
  <add key="applicationId" value="dcd55b4a-163b-4683-a05b-35b233886ec3" />
  <add key="workspaceId" value="f538985c-629f-4137-8eed-e6ab1a68b569" />
  <add key="reportId" value="377c25db-a32e-4e3f-af20-b0d5fce5e4fc" />

  <!-- Fill Tenant ID in authorityUrl-->
  <add key="authorityUrl" value="https://login.microsoftonline.com/organizations/" />
  <add key="scope" value="https://analysis.windows.net/powerbi/api/.default" />
  <add key="urlPowerBiServiceApiRoot" value="https://api.powerbi.com/" />

  <!-- Note: Do NOT leave your credentials on code. Save them in secure place like Key Vault. -->
  <add key="pbiUsername" value="" />
  <add key="pbiPassword" value="" />

  <!-- Note: Do NOT leave your app secret on code. Save it in secure place like Key Vault. -->
  <add key="applicationSecret" value="JoJ8Q~CRQY6MGWhQ0m~bx9z0qnu0RNhgizE4gcYj" />
  <add key="tenant" value="337a945d-ac66-4f8c-b739-e23a06080308" />
</appSettings>
```

Execution



Configured project code



Web.config