**ArcGIS Enterprise: CORS Implementation**

Prepared by Noe Diaz

Document Release: Version 0.1

April 15, 2024

Revision History

The table that follows summarizes the revision history of this document.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Release | Summary of Revisions | Date | Author(s) | Approver |
| Draft 0.1 | Draft content created | 03/22/2024 | Noe Diaz | N/A |
| Draft 0.2 | Technical edit and formatting | 04/15/2024 | Noe Diaz | N/A |
| Draft 0.3 | Updated draft |  |  | N/A |
| Draft 0.4 | Technical edits from peer review |  |  | N/A |
| Draft 0.5 | Content edits |  |  | N/A |
| Draft 0.6 | Content corrections |  |  | N/A |
| Draft 0.7 | Quality assurance review |  |  | N/A |
| Final 1.0 | Accepted edits and baselined the document |  |  | N/A |

Contents

[Section 1 – Introduction 1](#_Toc181017612)

[1.1 Purpose 1](#_Toc181017613)

[1.2 Document Conventions 1](#_Toc181017614)

[Section 2 – About This Guide 2](#_Toc181017615)

[Section 3 – What is CORs? 3](#_Toc181017616)

[3.1 CORS Example Allowlist 4](#_Toc181017617)

[3.1.1 Do ArcGIS Web Applications built in Portal require an allowlist? 5](#_Toc181017618)

[3.2 Sample Allowlist 6](#_Toc181017619)

[3.3 Trusted SERVERS’ vs CORS 7](#_Toc181017620)

[3.3.1 Enterprise Reporter Tool 7](#_Toc181017621)

[Section 4 – Allow PowerBI Connections 9](#_Toc181017622)

[4.1 Sign into Power BI for US Government 9](#_Toc181017623)

[4.1.1 Add Power BI URLs to your Allowlist 9](#_Toc181017624)

[4.1.2 Authentication 10](#_Toc181017625)

[4.1.3 GCC Allow List URLs 10](#_Toc181017626)

[4.1.4 Getting an access token from Microsoft Entra ID 11](#_Toc181017627)

[4.1.5 General Site Usage 11](#_Toc181017628)

[4.1.6 Connect Government and Global Azure Cloud 13](#_Toc181017629)

[4.1.7 Power BI Visuals 14](#_Toc181017630)

[4.1.8 Cross-Cloud B2B 15](#_Toc181017631)

[Appendix A – References A-1](#_Toc181017632)

# Introduction

## Purpose

This installation guide provides the information necessary to configure and understand CORS on the ArcGIS Enterprise System.

## Document Conventions

Table 1‑1 describes the conventions used in this documentation.

Table 1‑1: Document Conventions

| Convention | Meaning |
| --- | --- |
| **🛈** | Indicates a note that supplements the information in the current section or about the procedure. |
| ! | Indicates an important note related to the current section or procedure. |
|  | Indicates that a section or procedure needs to be repeated. |
| Text > Text > Text | The arrow symbol (>) is used for navigation paths (e.g., **Start** > **Programs** > **Adlib** > **Express** > **Express Server**). All navigation paths in this document assume that Windows is set to display Classic View. |

# About This Guide

The content in this installation guide contains references to the software manufacturer’s online help documentation specific to ArcGIS Enterprise CORS Implementation. These help topics are noted, where applicable, and the links to the specific topics are in alphabetical order in Appendix A.

# What is CORs?

CORS is enabled by default on your ArcGIS Enterprise, however the wording is very tricking, because although its on by default, it’s not actually doing anything until you add an allowlist. So keep that in mind, when looking at your enterprise settings.

If you are wondering if your currently utilizing resources in your portal that require cross-origin resource sharing. So were we, there isn’t anything that really tells you if anyone is reaching our domain from cross domain resource sharing. Best bet is to keep an eye on the server logs and see if you see any errors or communicate with your portal users and engineer team. Certainly! Cross-Origin Resource Sharing (CORS) is a mechanism that allows resources on a web page to be requested from another domain outside the domain from which the first resource was served. CORS is a crucial aspect of modern web development, especially when dealing with APIs or fetching resources from different domains.

Let's consider a hypothetical scenario in portal, where you have a web application hosted on `www.mygisapp.com`. This application needs to fetch data from an API hosted on a different domain, let's say `api.gis.com`.

Here's how you can determine if your application is utilizing resources that require CORS:

1. Inspect Network Requests: You can use browser developer tools to inspect network requests. When your application makes a request to an external domain, check if the request is successful or if there are any CORS-related errors in the console.

2. Check Response Headers: If your application is making cross-origin requests, the server should include specific CORS-related headers in its responses. These headers include `Access-Control-Allow-Origin`, `Access-Control-Allow-Methods`, `Access-Control-Allow-Headers`, etc. You can inspect the response headers in the network tab of your browser's developer tools to see if these headers are present.

3. Testing CORS Behavior: You can deliberately make a cross-origin request from your application to see how it behaves. For example, if your application is trying to fetch data from `api.gis.com`, but `api.gis.com` does not have CORS enabled or configured properly, your application may encounter CORS-related errors.

Here's a simplified JavaScript example of making a cross-origin request:

```javascript

1. fetch('https://api.gis.com/data')
2. .then(response => {
3. **if** (!response.ok) {
4. **throw** **new** Error('Network response was not ok');
5. }
6. **return** response.json();
7. })
8. .then(data => console.log(data))
9. .**catch**(error => console.error('Error fetching data:', error));

```

If `api.gis.com` allows requests from `www.mygisapp.com`, it should include the appropriate CORS headers in its responses. Otherwise, the browser will block the request, and you'll see CORS-related errors in the console.

By inspecting network requests, checking response headers, and testing CORS behavior, you can determine whether your application is utilizing resources that require CORS.

## CORS Example Allowlist

A CORS URL whitelist is a list of domains that are allowed to make cross-origin requests to a particular server. This whitelist helps control access to resources and protects against unauthorized requests from other domains. Here's an example of a CORS URL whitelist:

https://www.example.com

https://api.example.com

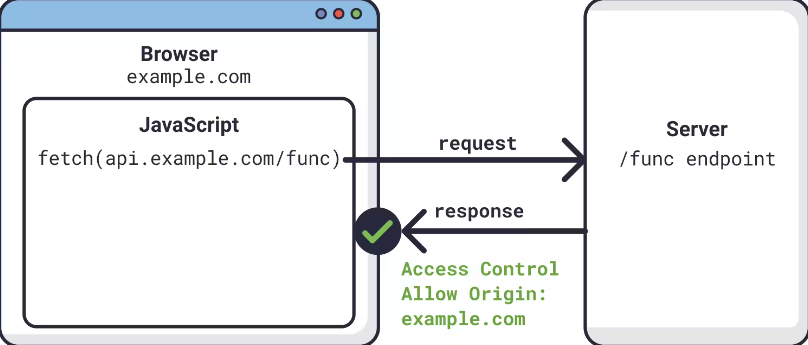
https://subdomain.example.com

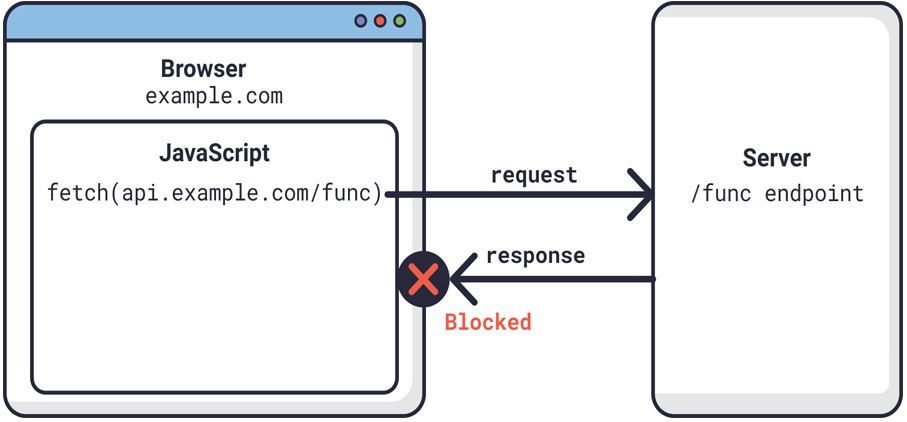
1. `https://www.example.com` is a domain representing the main website.

2. `https://api.example.com` is a domain representing an API endpoint hosted on a subdomain.

3. `https://subdomain.example.com` is a domain representing a specific subdomain of the main website.

These URLs specify the domains that are allowed to make cross-origin requests to the server. Any requests originating from these domains will be permitted by the server, while requests from other domains will be blocked by default (unless specifically allowed).





It's important to note that the URLs in the whitelist should include the protocol (`https://`) and should match the exact origin from which requests are expected to originate. Wildcards can also be used to allow requests from multiple subdomains, but they should be used cautiously as they can potentially open up security vulnerabilities if not properly configured.

### Do ArcGIS Web Applications built in Portal require an allowlist?

In the context of CORS (Cross-Origin Resource Sharing), a "web application" refers to any software application that is accessed and interacted with via a web browser over the internet. This includes applications built using various web technologies such as HTML, CSS, JavaScript, and possibly backend technologies like APIs.

In this case, the web applications such as a Dashboard or Experience Builder are indeed examples of web applications. They are accessed through a web browser and likely utilize web technologies to present data, visualize maps, and provide interactive experiences to users.

When it comes to CORS, it's particularly relevant if these web applications are making requests to servers outside of their own domain. For instance, if your Dashboard needs to fetch data from an API hosted on a different domain (e.g., `api.data.com`), or if the Experience Builder needs to access map tiles from a map service hosted elsewhere (e.g., `maps.globe.com`), then CORS considerations come into play.

The domains hosting these APIs or services would need to have CORS properly configured to allow requests from the domains where your web applications are hosted (`gis.geo.gov.com` in this case). Without proper CORS configuration, the browser may block these cross-origin requests, potentially leading to functionality issues within your web applications.

Therefore, when discussing CORS in the context of your Enterprise and its web applications, it's important to consider any cross-origin requests these applications may be making and ensure that CORS is configured appropriately on the relevant servers to allow these requests. This will ensure that your web applications can access the necessary resources and function as intended.

## Sample Allowlist

Keep in mind that, in typical circumstances, putting arcgis.com would cover anything in that domain, however depending on your environment, its better to put the full URL.

Portal Sample CORS List

https://login.microsoftonline.com

https://analysis.usgovcloudapi.net/powerbi/api

https://pbidedicated.usgovcloudapi.net

https://api.powerbigov.us

https://app.powerbigov.us

https://survey123.arcgis.com

https://azure.us

https://visualstudio.us

https://gov.content.powerapps.us

https://basemaps.arcgis.com

https://cdn.arcgis.com

https://geocode.arcgis.com

https://route.arcgis.com

https://services.arcgis.com

https://traffic.arcgis.com

https://www.arcgis.com

Server Sample CORS List

https://login.microsoftonline.com, https://usdos.sharepoint.com, https://app.powerbigov.us, https://analysis.usgovcloudapi.net/powerbi/api, https://pbidedicated.usgovcloudapi.net, https://api.powerbigov.us, https://gatewayadminportal-gov.azure.us, https://visualstudio.us, https://gov.content.powerapps.us, https://www.arcgis.com, https://survey123.arcgis.com, https://basemaps.arcgis.com, https://cdn.arcgis.com, https://geocode.arcgis.com, https://route.arcgis.com, https://services.arcgis.com, https://traffic.arcgis.com

## Trusted SERVERS’ vs CORS

In the context of ArcGIS Enterprise Portal Admin, "Trusted Servers" and "Access Control Allow Origin" serve different purposes related to security, particularly regarding access to resources from external sources.

Trusted Servers: This feature allows you to specify which servers are trusted by your ArcGIS Enterprise deployment. When a server is marked as trusted, it means that requests originating from that server are considered safe and are allowed to access resources within your ArcGIS Enterprise environment without encountering security restrictions. This can be particularly useful for integrating with other servers or services that need to interact with your ArcGIS Enterprise deployment. By designating certain servers as trusted, you can streamline workflows and ensure that authorized access is maintained.

Access Control Allow Origin (CORS): CORS is a security feature implemented by web browsers that restricts web pages from making requests to resources on another domain outside the domain from which the original web page was served. This restriction is in place to prevent cross-origin attacks, which can potentially compromise the security of web applications. However, there are legitimate scenarios where you may need to make cross-origin requests, such as when integrating different web services or accessing resources from multiple domains. In such cases, you can configure the CORS settings to specify which origins are allowed to make cross-origin requests to your ArcGIS Enterprise resources. This allows you to control and restrict access to your resources while still enabling legitimate cross-origin interactions.

In summary, while both "Trusted Servers" and "Access Control Allow Origin" are security features aimed at controlling access to resources within ArcGIS Enterprise, they serve different purposes. Trusted Servers are used to designate specific servers as trusted sources of requests, while Access Control Allow Origin (CORS) is used to control which origins are allowed to make cross-origin requests to ArcGIS Enterprise resources.

### Enterprise Reporter Tool

The first tool that will give you a sense of your architecture. You can find this tool on GitHub from Danny Krouk. A common challenge in administering an ArcGIS Enterprise system is the need document and/or otherwise communicate its design and configuration.

Typically, this is done by someone creating one or more diagrams. These diagrams sometimes have errors and/or omissions. And, they easily lose their relevance as the system changes. The underlying challenge is that the documentation of the system is not generated by the system itself, it reflects the understanding of one person at one moment in time.

GIS Enterprise Reporter is designed to help address this challenge by automating the creation of documentation artifacts. Point the tool at your ArcGIS Enterprise, with administrative credentials, and it will generate documentation that includes:

1. A logical diagram
2. Listings of administrative/configuration settings (from the REST admin API's)
3. Listings of machine resources and installed software (for the machines running the software in the ArcGIS Enterprise system)
4. ArcGIS Server service inventories (inclusive of workspaces and datasets)
5. Portal content inventory
6. Portal users and groups inventory
7. Information about TLS/SSL certificates (including certificate expirations, required trust chains, etc.)

The documentation is output in Microsoft Excel format, making it easy to share, analyze, and mark-up.

# Allow PowerBI Connections

To use the Power BI service on your ArcGIS Enterprise, you must allow connections to required endpoints on the internet. These destinations have to be reachable to enable communication between your own network, Power BI, and other dependent services.

## Sign into Power BI for US Government

The URLs for connecting to Power BI differ for government users and commercial users. To sign in to the correct Power BI version, use one of the following URLs:

* **Commercial version**: [https://app.powerbi.com](https://app.powerbi.com/)
* **GCC**: [https://app.powerbigov.us](https://app.powerbigov.us/)
* **GCC High**: [https://app.high.powerbigov.us](https://app.high.powerbigov.us/)
* **DoD**: [https://app.mil.powerbigov.us](https://app.mil.powerbigov.us/)

The following table lists the required endpoints to add to your allowlist to enable connection to the Power BI service for general site usage. These endpoints are unique to the US government cloud. The Power BI service requires only Transmission Control Protocol (TCP) port 443 to be opened for the listed endpoints.

The endpoints for getting data, dashboard and report integration, Power BI visuals, and other optional services aren’t unique to the US government cloud.

To add these URLs to your allowlist also, see [Add Power BI URLs to your allowlist](https://learn.microsoft.com/en-us/power-bi/admin/power-bi-allow-list-urls).

This section will describe which, when, and where we should run our tools/scripts and in what order. Read the instructions on how to use the tool or script with CfA ArcGIS Enterprise KBAs Documentation.

### Add Power BI URLs to your Allowlist

The Power BI service requires internet connectivity. The endpoints listed in the following tables should be reachable for customers who use the Power BI service.

To use the Power BI service, you must be able to connect to the endpoints marked **required** in the tables in this article, and to any endpoints marked **required** on the linked sites. If the link to an external site refers to a specific section, you only need to review the endpoints in that section.

You can also add endpoints that are marked **optional** to allowlists for specific functionality to work.

The Power BI service requires only TCP Port 443 to be opened for the listed endpoints.

Wildcards (\*) represent all levels under the root domain. N/A is used when information isn't available. The **Destination(s)** column lists domain names and links to external sites, which contain further endpoint information.

### Authentication

Power BI depends on the required endpoints in the Microsoft 365 authentication and identity sections. To use Power BI, you must be able to connect to the endpoints in the following linked site.

| **Purpose** | **Destination** | **Port** |
| --- | --- | --- |
| **Required:** Authentication and identity | See the documentation for [Microsoft 365 Common and Office Online URLs](https://learn.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges#microsoft-365-common-and-office-online) | N/A |

### GCC Allow List URLs

Authentication, identity, and administration for Power BI depend on connectivity to Microsoft 365 services. You also have to connect to Microsoft 365 to view audit logs. To identify the endpoints for these services, see "Microsoft 365 integration" in the following table:

| **Purpose** | **Destination** |
| --- | --- |
| Back-end APIs | **GCC**: https://api.powerbigov.us **GCC High**: api.high.powerbigov.us **DoD**: api.mil.powerbigov.us |
| Back-end APIs | **GCC**:https://analysis.usgovcloudapi.net/powerbi/api/.default **GCC High**: \*.high.analysis.usgovcloudapi.net **DoD**: \*.mil.analysis.usgovcloudapi.net |
| Back-end APIs | **All**: https://pbidedicated.usgovcloudapi.net |
| Content Delivery Network (CDN) | **GCC**: https://gov.content.powerapps.us **GCC High**: high.content.powerapps.us **DoD**: mil.content.powerapps.us |
| Microsoft 365 integration | **GCC**: [Worldwide endpoints](https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges) **GCC High**: [US Government GCC High endpoints](https://learn.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-u-s-government-gcc-high-endpoints) **DoD**: [US Government DOD endpoints](https://learn.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-u-s-government-dod-endpoints) |
| Portal | **GCC**: <https://app.powerbigov.us/>  **GCC High**: \*.high.powerbigov.us **DoD**: \*.mil.powerbigov.us |
| Manage gateways, connections and data policies (preview) | **GCC**: https://gatewayadminportal-gov.azure.us **GCC High**: gatewayadminportal-high.azure.us **DoD**: gatewayadminportal-mil.azure.us |
| Service telemetry | **All**: https://dc.services.visualstudio.us |
| Informational messages (optional) | **All**: arc.msn.com |

### Getting an access token from Microsoft Entra ID

Within your application, you need to get an access token, from Microsoft Entra ID, before you can make calls to the Power BI REST API. For more information, see [Authenticate users and get a Microsoft Entra access token for your Power BI app](https://learn.microsoft.com/en-us/power-bi/developer/embedded/generate-embed-token). Since there are different national/regional cloud affiliations, there are distinct URLs to get an access token for your application.

Government Community Cloud (GCC) - https://login.microsoftonline.com

### General Site Usage

For the general use of Power BI, you must be able to connect to the endpoints and linked sites in the following table.

| **Purpose** | **Destination** | **Port** |
| --- | --- | --- |
| **Required:** Backend APIs | api.powerbi.com | TCP 443 |
| **Required:** Backend APIs | \*.analysis.windows.net | TCP 443 |
| **Required:** Backend APIs | \*.pbidedicated.windows.net | TCP 443 |
| **Required:** Content Delivery Network (CDN) | content.powerapps.com | TCP 443 |
| **Required:** Datamart SQL | One of the following:   datamart.fabric.microsoft.com   datamart.pbidedicated.windows.net | 1433 |
| **Required:** Microsoft 365 integration | See the documentation for [Microsoft 365 Common and Office Online URLs](https://learn.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges#microsoft-365-common-and-office-online) | N/A |
| **Required:** Portal | \*.powerbi.com | TCP 443 |
| **Required:** Manage gateways, connections and data policies (preview) | gatewayadminportal.azure.com | TCP 443 |
| **Required:** Service telemetry | dc.services.visualstudio.com | TCP 443 |
| **Optional:** Informational messages | arc.msn.com | TCP 443 |
| **Optional:** NPS surveys | nps.onyx.azure.net | TCP 443 |

### Connect Government and Global Azure Cloud

Power BI depends on certain endpoints to support your dashboards and reports. You must be able to connect to the endpoints and linked sites in the following table.

| **Purpose** | **Destination** | **Port** |
| --- | --- | --- |
| **Required:** Excel integration | See the documentation for [Microsoft 365 Common and Office Online URLs](https://learn.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges#microsoft-365-common-and-office-online) | N/A |

Azure is distributed across multiple clouds. By default, you can enable firewall rules to open a connection to a cloud-specific instance, but cross-cloud networking is different. To communicate between services in the public cloud and services in the Government Community Cloud, you have to configure specific firewall rules. For example, if you want to access public cloud instances of an SQL database from your government cloud deployment of Power BI, you need a firewall rule in the SQL database. Configure specific firewall rules for SQL databases to allow connections to the Azure Government Cloud for the following datacenters:

* USGov Iowa
* USGov Virginia
* USGov Texas
* USGov Arizona
* US DoD East
* US DoD Central

To get the US government cloud IP ranges, download the [Azure IP Ranges and Service Tags – US Government Cloud](https://www.microsoft.com/download/details.aspx?id=57063) file. Ranges are listed for both Power BI and Power Query.

For more information about Microsoft Azure Government cloud services, see [Azure Government documentation](https://learn.microsoft.com/en-us/azure/azure-government/).

To set up firewalls for SQL databases, see [Create and manage IP firewall rules](https://learn.microsoft.com/en-us/azure/sql-database/sql-database-firewall-configure#create-and-manage-ip-firewall-rules)

### Power BI Visuals

Power BI depends on certain endpoints to view and access Power BI visuals. You must be able to connect to the endpoints and linked sites in the following table.

| **Purpose** | **Destination** | **Port** |
| --- | --- | --- |
| **Required:** Import a custom visual from the Marketplace interface or from a file | \*.powerbi.com \*.osi.office.net \*.msecnd.net store.office.com store-images.s-microsoft.com visuals.azureedge.net | TCP 443 |
| **Optional:** Azure Maps | https://atlas.microsoft.com https://us.atlas.microsoft.com https://eu.atlas.microsoft.com | N/A |
| **Optional:** Bing Maps | bing.com platform.bing.com r.bing.com \*.virtualearth.net | TCP 443 |
| **Optional:** Esri Maps | \*.esri.com \*.arcgis.com | TCP 443 |
| **Optional:** PowerApps | See the [Required services section](https://learn.microsoft.com/en-us/powerapps/maker/canvas-apps/limits-and-config#required-services) from the PowerApps system requirements site | N/A |
| **Optional:** Visio | See the documentation for [Microsoft 365 Common and Office Online URLs](https://learn.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges#microsoft-365-common-and-office-online), as well as [SharePoint Online and OneDrive for work or school](https://learn.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges#sharepoint-online-and-onedrive-for-business) | N/A |

### Cross-Cloud B2B

You can use Power BI's B2B capabilities across Microsoft Azure clouds by configuring Microsoft cloud settings for B2B collaboration. Read [Microsoft cloud settings](https://learn.microsoft.com/en-us/azure/active-directory/external-identities/cross-tenant-access-overview#microsoft-cloud-settings) to learn how to establish mutual B2B collaboration between the Microsoft Azure global cloud and Microsoft Azure Government.

There are some limitations to the B2B experience that you should be aware of:

* Guest users may already have a Power BI license that was assigned to them through their own organization. But “Bring your own license” doesn’t work across different Microsoft Azure clouds. A new license has to be assigned to these guest users by the provider tenant.
* New external users can be invited to the organization through Power BI sharing, permissions, and subscription experiences.
* On the Home page, the **From external orgs** tab won't list content shared from other clouds.

###### References

**GIS Bibliography**

A comprehensive index of journal articles, conference proceedings, books, and reports related to GIS, including references and full-text materials. gis.library.esri.com

**ArGIS Documentation and Tutorials**

In-depth information, tutorials, and documentation for ArcGIS Products.

ArcGIS Online: arcgis.com

ArcGIS Desktop: desktop.arcgis.com

ArcGIS Enterprise: enterprise.arcgis.com

**Esri Community**

Join the online community of GIS users and experts: community.esri.com

**Esri Videos**

View an extensive collection of videos by Esri leaders, event keynote speakers, and product experts. youtube.com/user/esritv

**GIS Dictionary**

This browser defines and describes thousands of GIS terms. support.esri.com/other-resources/gis-dictionary

PowerBI for US government customers: <https://learn.microsoft.com/en-us/power-bi/enterprise/service-govus-overview>

Add Power BI URLs to your allowlist: <https://learn.microsoft.com/en-us/power-bi/enterprise/power-bi-allow-list-urls>

Embed Power BI content into your application for national/regional clouds: [Embed content in your Power BI embedded analytics application for government and national/regional clouds - Power BI | Microsoft Learn](https://learn.microsoft.com/en-us/power-bi/developer/embedded/embed-sample-for-customers-national-clouds)

Utilizing PowerBI REST API for GCC: [Utilizing Power BI REST API for Government Cloud (GCC) - Analytic Archives](https://analyticarchives.com/utilizing-power-bi-rest-api-for-government-cloud-gcc/)

Using the PowerBI REST APIs: [Power BI REST APIs for embedded analytics and automation - Power BI REST API | Microsoft Learn](https://learn.microsoft.com/en-us/rest/api/power-bi/)

Register your Application to make REST API Calls: [Get started with Power BI Embedded - Power BI | Microsoft Learn](https://learn.microsoft.com/en-us/power-bi/developer/embedded/register-app?tabs=customers)