

# Microsoft Azure Cloud Integration Guide

Microsoft Azure is a comprehensive cloud computing platform that provides a wide range of services, including virtual machines, databases, AI tools, and storage, enabling organizations to build, deploy, and manage applications across global data centers. It supports hybrid and multi-cloud environments, offering scalability, security, and advanced analytics to help businesses accelerate innovation and optimize operations.

## Deployment Type

This integration supports **on-premises**, **private cloud**, and **vendor cloud** deployments through **port 443**.

If you already know that your environment supports these deployments, continue to the next step. If you are unsure, please check your organization's compatibility before continuing.

## Required Information and Setup

To integrate GreyMatter with Microsoft Azure Cloud, collect the following details:

- Token Base URL
  - Default: <https://login.microsoftonline.com>
- Base URL
  - Default: <https://management.azure.com>
- API Version
- Tenant
  - Directory (tenant) ID in the overview section of the app registration
- Client ID:
  - application (Client) ID in the overview section of the app registration
- Client Secret

See instructions below to gather the required information.

## Register the Application for API Access

1. Log in to the Azure Portal with an account that has Owner, Contributor, or User Access Administrator permissions.
2. Click **App registrations** in the Azure Active Directory menu.
3. Click **New Registration**.
4. Fill out the required fields:
  - Name (e.g. ResourceGraphAPIApp)
  - Supported account types: Accounts in this organization directory only (by default) unless you want multi-tenant access.
  - Redirect URI: Leave empty for server-to-server communication (not required for Resource Graph API)
5. Click **Register** to create the app.

# Microsoft Azure Cloud Integration Guide

## Configure API Permissions for Registered App

1. In the left navigation menu of the App Registrations Overview page, select **API Permissions**.
2. Click **Add a permission**.
3. Select **Microsoft APIs**.
4. Choose **Azure Service Management**.
5. Select **Application permissions**.
6. Check the box for **user\_impersonation**.
7. Click **Grant admin consent for <your organization>**.
8. Click **Yes** to confirm.

## Create a Client Secret

1. In the left navigation menu, select **Certificates & secrets**.
2. Click **New client secret** under Client secrets.
3. Enter a **description** (e.g. "ResourceGraphAPISecret").
4. Select an **expiration period** (e.g. 1 year, 2 years).
5. Click **Add**.
6. Copy the **Value** immediately and paste somewhere secure. It will not be visible again.

## Assign Required Permissions to the Subscription

1. Search for and select **Subscriptions** in the Azure Portal.
2. Select the subscription you want app to access.
3. In the subscription menu, select **Access Control (IAM)**.
4. Click **Add role assignment**.
5. Select the **Reader role**.
6. Under Assign access to, select **Azure AD user, group, or service principal**.
7. Search for and select your **app registration name**.
8. Click **Save**.

## Permissions and Functionality

### Permissions

GreyMatter Capability	Action(s)	Required Permission
Asset Inventory	Fetch Cloud Assets	Role: <ul style="list-style-type: none"> <li>• Reader</li> </ul> Actions: <ul style="list-style-type: none"> <li>• Microsoft.ResourceGraph/resources/read</li> <li>• Microsoft.Resources/subscriptions/resources/read</li> </ul>

### Asset Inventory

# Microsoft Azure Cloud Integration Guide

Asset Inventory provides a comprehensive overview of your digital environment by integrating directly with Microsoft Azure Cloud, providing real-time insights into all available Resources within the Azure Cloud instance for a given tenant ID, their status, and potential risks.

**Disclaimer:** All customer data is classified and handled as 'Confidential' (as outlined in our Data Classification & Handling Policy). Customer data is restricted to authorized personnel only based on their business need. ReliaQuest uses least privilege and role-based access controls via Active Directory to provision and manage access. Please see our Access Control Policy for more information. ReliaQuest employees are also required to sign confidentiality agreements as part of their employment.