

Acquiring Azure AD credentials for blob storage

Microsoft recommends transitioning away from Shared Key authorization for Azure Storage in favor of using Azure AD. This cheat sheet describes how to create credentials in Azure AD for use with WCSM.

The process is a two-stage process. In the first stage create a service principal and register it with the AD. Please note this service principal represents/acts on behalf of the WCSM platform. In the second stage allow service principal through a role assignment process, to access the storage account.

Service Principal Creation and App registration

Step 1: Search for “Microsoft Entra ID” and click on it.

Step 2: Under “Manage” on the side menu click on “App registrations”

Step 3: Click on “+ New registration” in the top menu

Step 4: Enter a name, e.g. “WCSMApp” (or any other name of your choosing). And choose “Accounts in this organizational directory only (xxx Azure Directory only – single tenant)”. And then press “Register”

Home > Wasabi Azure Directory | App registrations >

Register an application

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

WCSMApp

Supported account types
Who can use this application or access this API?

- Accounts in this organizational directory only (Wasabi Azure Directory only - Single tenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - 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

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

register

Step 5: You will see details about the newly registered app here, including, “Application (client) ID”, Directory (tenant) ID here. **Note down the “Application (client) ID” and Directory (tenant) ID”** (you can come back to it later as well).

Home > Wasabi Azure Directory | App registrations >

WCSMApp

Search [] Delete Endpoints Preview features

Overview Quickstart Integration assistant Manage Support + Troubleshooting

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name : WCSMApp	Client credentials : Add a certificate or secret
Application (client) ID : 904e1[]	Redirect URIs : Add a Redirect URI
Object ID : 41055[]	Application ID URI : Add an Application ID URI
Directory (tenant) ID : aa9[]	Managed application in I. : WCSMApp
Supported account types : My organization only	

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

[Get Started](#) Documentation

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)



Call APIs

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

[View API permissions](#)



Sign in users in 5 minutes

Use our SDKs to sign in users and call APIs in a few steps. Use the quickstarts to start a web app, mobile app, SPA, or daemon app.

[View all quickstart guides](#)



Configure for your organization

Assign users and groups, apply conditional access policies, configure single sign-on, and more in Enterprise applications.

[Go to Enterprise applications](#)

Step 6: Click on “Client Credentials: “Add a certificate or secret”

Step 7: Click on “+ New client secret”. Enter description and press “Add”.

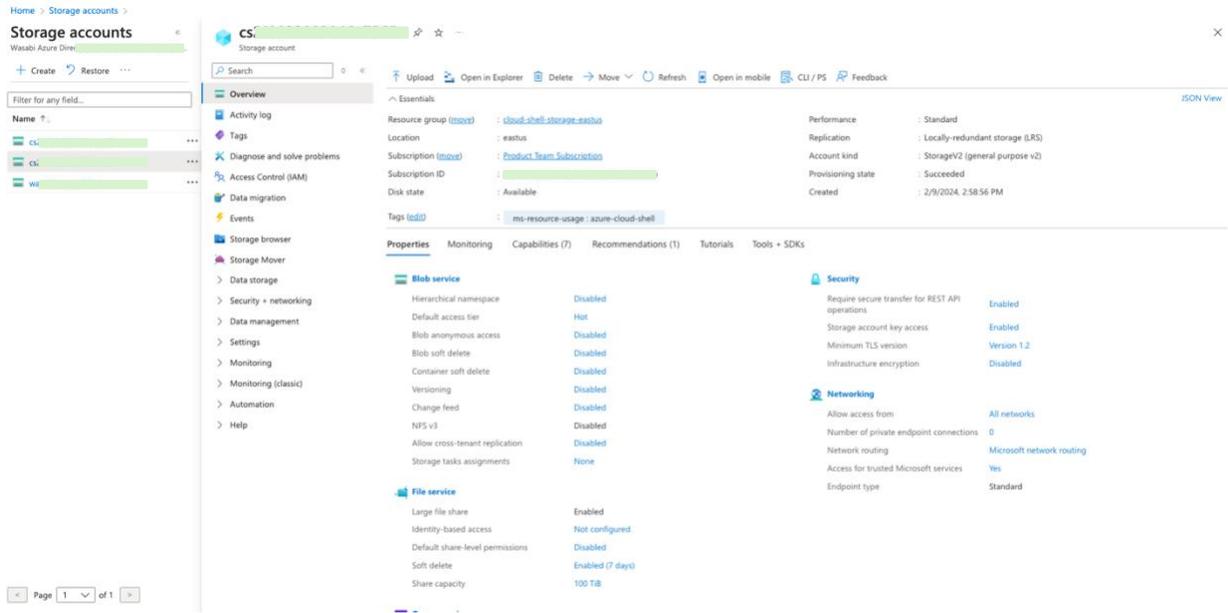
Step 8: Note down the “Value” and “secret ID” values. (The value is only visible once). If you miss noting it down, you can come back to create new client secret.

At this point you have all the information that is required for WCSM. Use the “Tenant ID” and “Client ID” from Step 5 AND “Secret ID” and “Value” from Step 7 to specify the source bucket “Credentials” in WCSM.

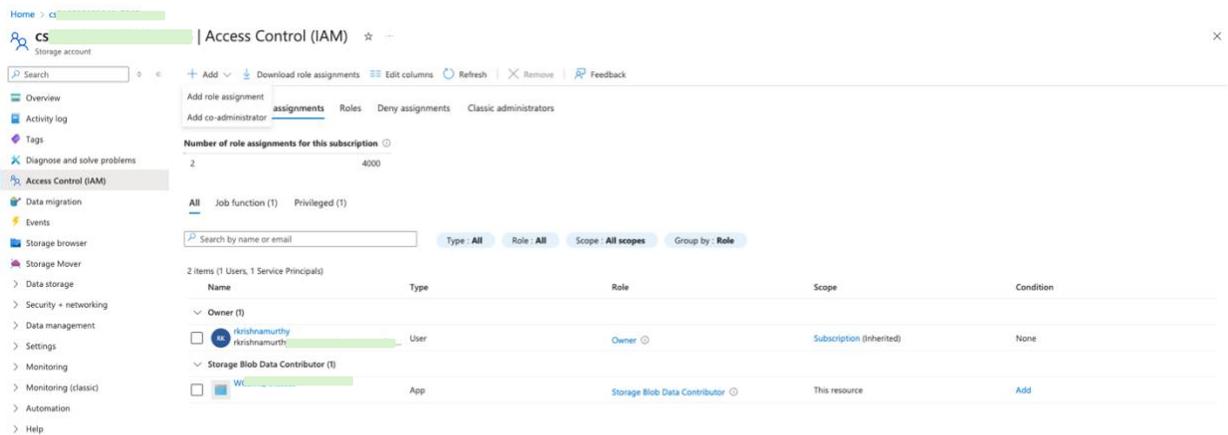
Storage account role assignment to the Service Principal

This step is required to allow the Service Principal created to access the storage account containing the blob storage.

Step 1: Go to your “Storage accounts” and click on the storage account containing source data.



Step 2: Click on “Access Control (IAM)” tab on the left and click on “Role assignments” and then press “Add” and choose “Add role assignment”



Step 3: Search for and select “Storage Blob Data Reader”. Search for and select “Storage Blob Data Contributor”. And press next.

Step 4: Press “+Select member” and search for and select “WCSMApp” (or the name you had used for “App registration” process in Step 4). And press “Next”