# Obtaining Credentials for Cloudera Director

To get started with Cloudera Director and Microsoft Azure, you create an [Active Directory (AD) application and service principal](https://azure.microsoft.com/en-us/documentation/articles/active-directory-application-objects/) and obtain the required Azure credentials for Director. The service principal is tied to the AD application, and Cloudera Director uses the service principal credentials to create and delete resources on Microsoft Azure.

Follow these general steps to obtain the required credentials:

1. Create the AD application and make sure that it has the contributor role in your Azure subscription, which allows you to create and delete resources.
2. Create the service principal. This is typically created by a system administrator or security administrator in your organization. This person must have administrator privileges for your Microsoft Azure subscription.
3. Obtain the following Azure credentials for Cloudera Director:
   * Subscription ID - You can get the subscription ID in the Azure
   * Tenant ID
   * Client ID
   * Client Secret

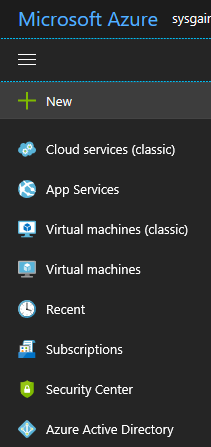
You can create the AD application and service principal, get the tenant ID, client ID, and client secret, and assign the contributor role to the newly-created AD application by using Azure portal.

# Required permissions

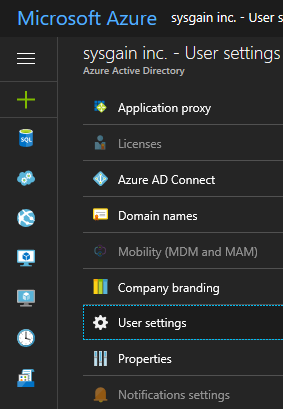
To complete this topic, you must have sufficient permissions to register an application with your Azure AD tenant, and assign the application to a role in your Azure subscription. Let's make sure you have the right permissions to perform those steps.

## Check Azure Active Directory permissions

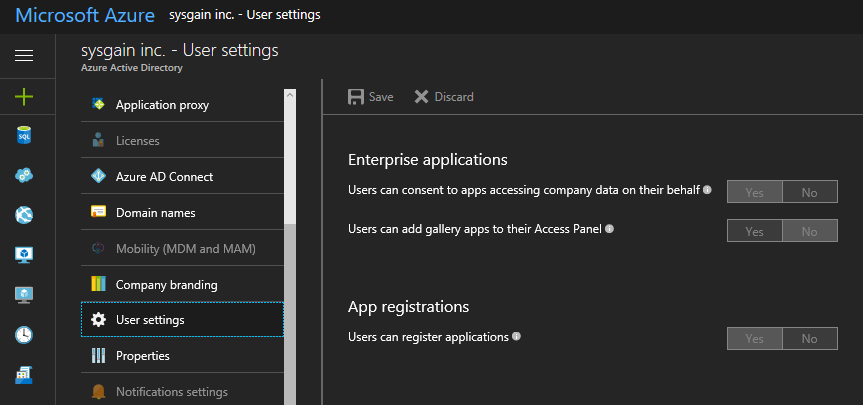
1. Log in to your Azure Account through the [Azure portal](https://portal.azure.com/).
2. Select **Azure Active Directory**.



1. In Azure Active Directory, select **User settings**.



1. Check the **App registrations** setting. If set to **Yes**, non-admin users can register AD apps. This setting means any user in the Azure AD tenant can register an app.

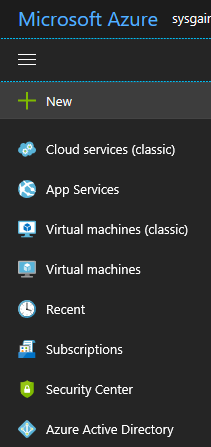


# Check Azure subscription permissions

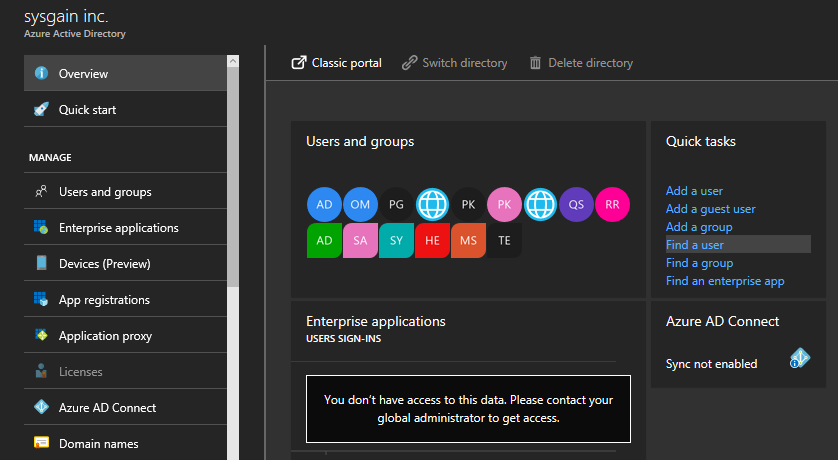
In your Azure subscription, your account must have Microsoft.Authorization/\*/Write access to assign an AD app to a role. This action is granted through the [Owner](https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-built-in-roles#owner) role or [User Access Administrator](https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-built-in-roles#user-access-administrator) role. If your account is assigned to the **Contributor** role, you do not have adequate permission. You will receive an error when attempting to assign the service principal to a role.

## To check your subscription permissions:

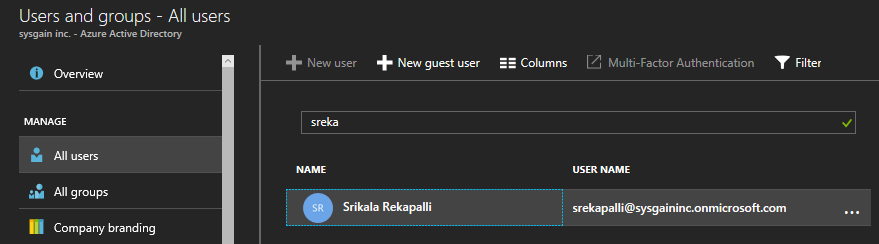
1. Select **Azure Active Directory** from the left pane.



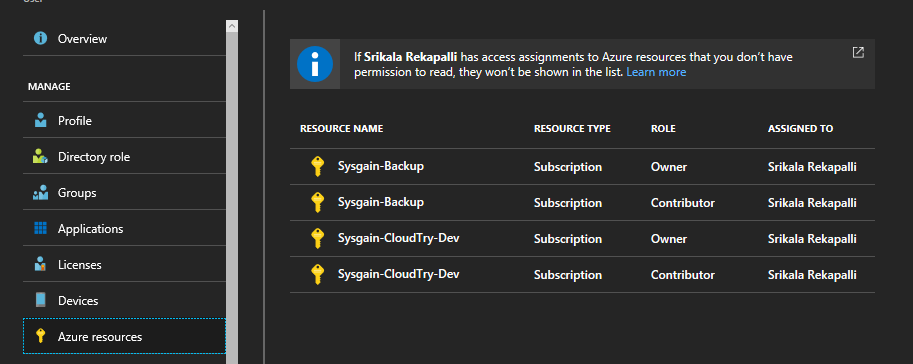
1. Find your Azure AD account. Select **Overview** and **Find a user** from Quick tasks.



1. Search for your account, and select it when you find it.

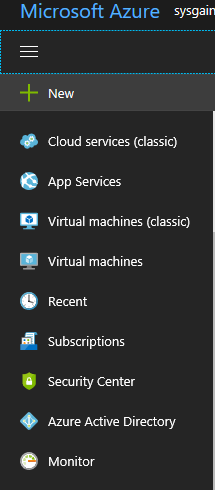


1. Select **Azure resources**.
2. View your assigned roles, and determine if you have adequate permissions to assign an AD app to a role. In the following image, the user is assigned to the Owner role for two subscriptions, which means that user has adequate permissions.

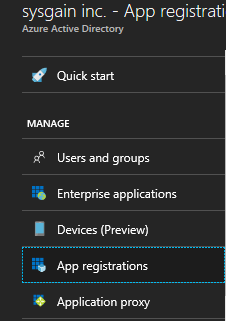


# Create an Azure Active Directory application

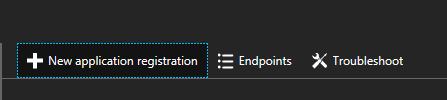
1. Log in to your Azure Account through the [Azure portal](https://portal.azure.com/).
2. Select **Azure Active Directory**.



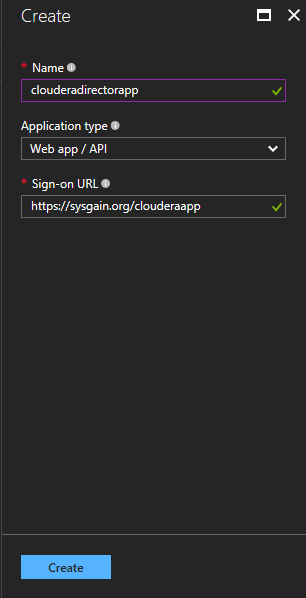
1. Select **App registrations**



1. Select **New application registration**



1. Provide a name and URL for the application. Select either **Web app / API** or **Native** for the type of application you want to create. After setting the values, select **Create**.

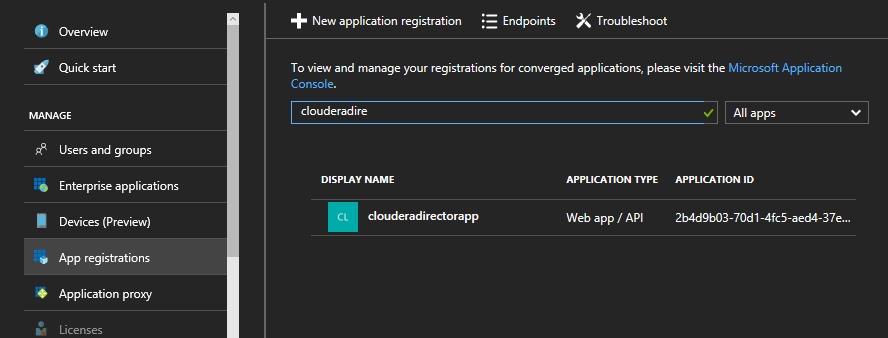


1. You have created your application.

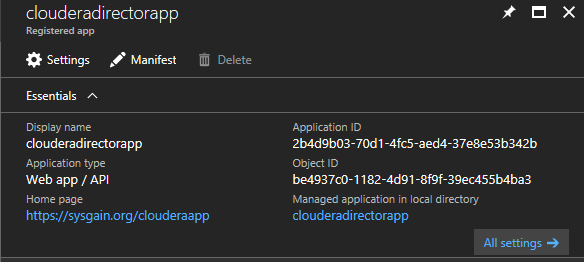
### Get application ID and authentication key

When programmatically logging in, you need the ID for your application and an authentication key. To get those values, use the following steps:

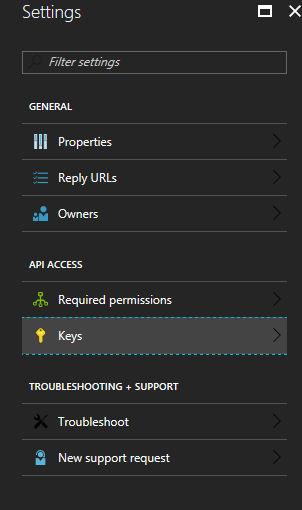
1. From **App registrations** in Azure Active Directory, select your application



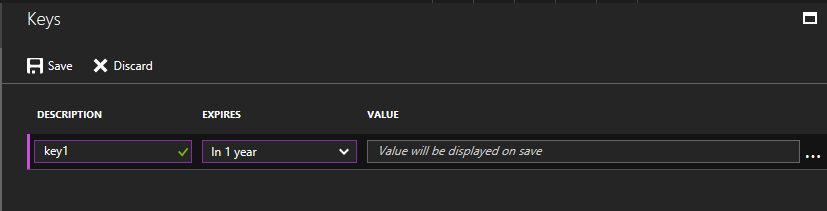
1. Copy the **Application ID** and store it in your application code. This application ID also refers as the client id.



1. To generate an authentication key, select **Keys**.



1. Provide a description of the key, and a duration for the key. When done, select **Save**.

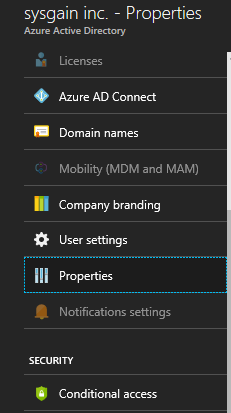


1. After saving the key, the value of the key is displayed. Copy this value because you are not able to retrieve the key later. You provide the key value with the application ID to log in as the application. Store the key value where your application can retrieve it.

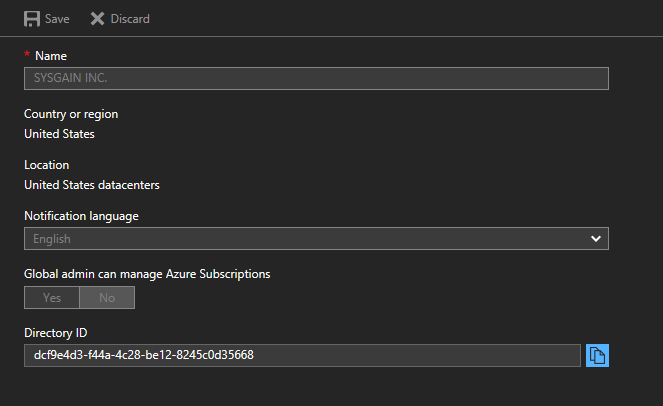
## Get tenant ID

When programmatically logging in, you need to pass the tenant ID with your authentication request.

1. To get the tenant ID, select **Properties** for your Azure AD tenant.



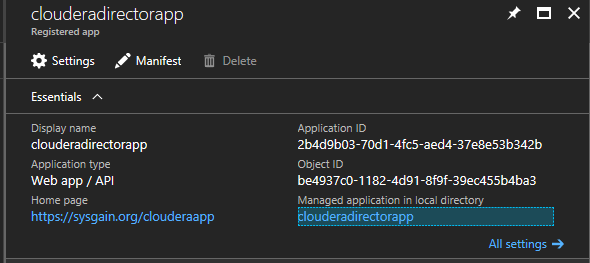
1. Copy the **Directory ID**. This value is your tenant ID.



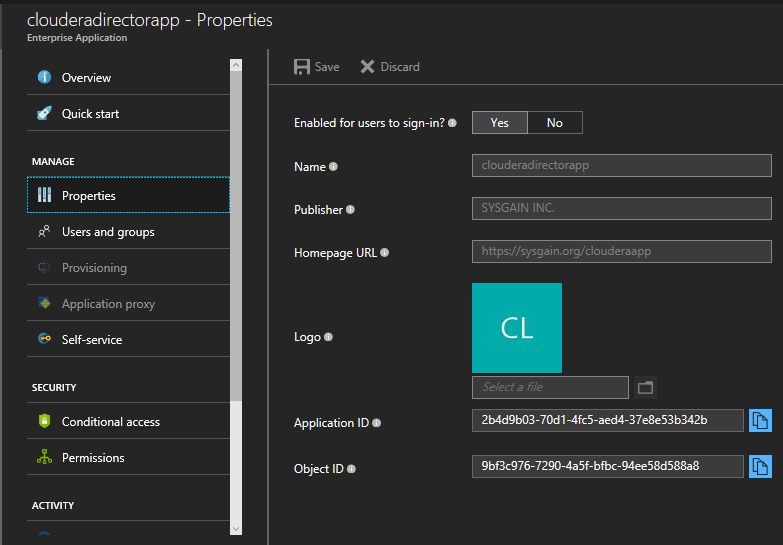
## Get Object ID:

Get AAD object ID of the service principal. This service principal will be given permissions on the root folder of the Data Lake Store account.

1. Go to your application and click on your application name as shown below.



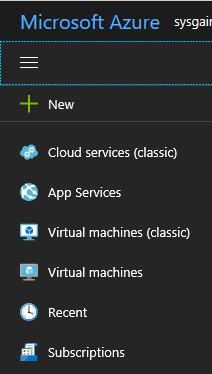
1. Click on properties to get the object ID.
2. Copy the Object ID.



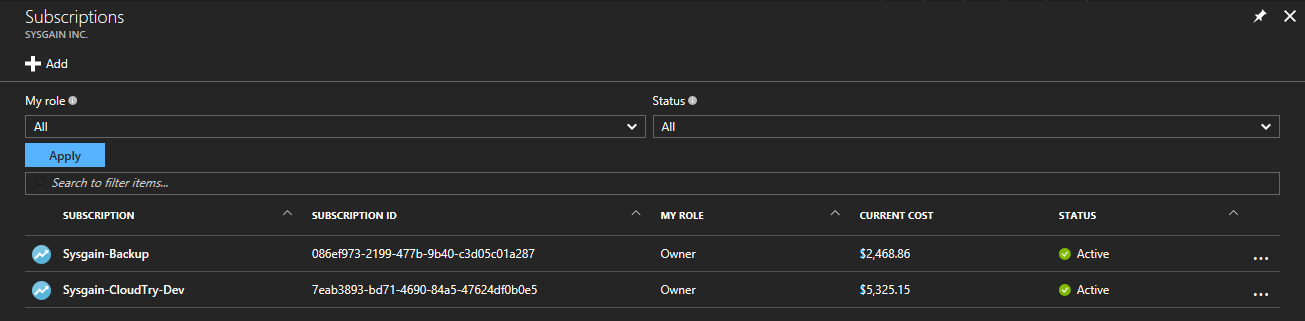
## Assign application to role

To access resources in your subscription, you must assign the application to a role. Make sure that it has the contributor role in your Azure subscription, which allows you to create and delete resources.

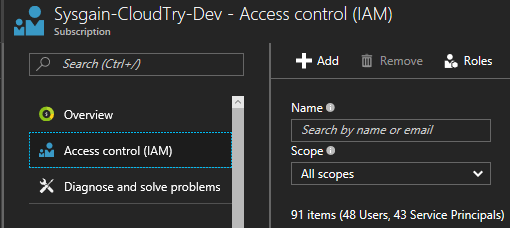
1. Navigate to the level of scope you wish to assign the application to. For example, to assign a role at the subscription scope, select **Subscriptions**. You could instead select a resource group or resource.



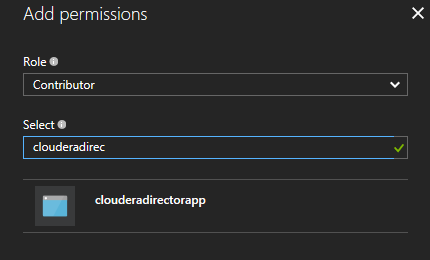
1. Select the particular subscription (resource group or resource) to assign the application to.



1. Select **Access Control (IAM)**.
2. Select **Add**.



1. Select Contributor role to assign to the application.



1. Search for your application, and select it.
2. Select **Save** to finish assigning the role. You see your application in the list of users assigned to a role for that scope.

