

Authenticate requests to Azure Cognitive Services

11/22/2019 • 8 minutes to read •  +1

In this article

[Prerequisites](#)

[Authentication headers](#)

[Authenticate with a single-service subscription key](#)

[Authenticate with a multi-service subscription key](#)

[Authenticate with an authentication token](#)

[Authenticate with Azure Active Directory](#)

[Authorize access to managed identities](#)

[See also](#)

Each request to an Azure Cognitive Service must include an authentication header. This header passes along a subscription key or access token, which is used to validate your subscription for a service or group of services. In this article, you'll learn about three ways to authenticate a request and the requirements for each.

- Authenticate with a [single-service](#) or [multi-service](#) subscription key
- Authenticate with a [token](#)
- Authenticate with [Azure Active Directory \(AAD\)](#)

Prerequisites

Before you make a request, you need an Azure account and an Azure Cognitive Services subscription. If you already have an account, go ahead and skip to the next section. If you don't have an account, we have a guide to get you set up in minutes: [Create a Cognitive Services account for Azure](#).

You can get your subscription key from the [Azure portal](#) after [creating your account](#).

Authentication headers

Let's quickly review the authentication headers available for use with Azure Cognitive Services.

Header	Description
--------	-------------


Header	Description
Ocp-Apim-Subscription-Key	Use this header to authenticate with a subscription key for a specific service or a multi-service subscription key.
Ocp-Apim-Subscription-Region	This header is only required when using a multi-service subscription key with the Translator service . Use this header to specify the subscription region.
Authorization	Use this header if you are using an authentication token. The steps to perform a token exchange are detailed in the following sections. The value provided follows this format: Bearer <TOKEN>.

Authenticate with a single-service subscription key


The first option is to authenticate a request with a subscription key for a specific service, like Translator. The keys are available in the Azure portal for each resource that you've created. To use a subscription key to authenticate a request, it must be passed along as the `Ocp-Apim-Subscription-Key` header.

These sample requests demonstrates how to use the `Ocp-Apim-Subscription-Key` header. Keep in mind, when using this sample you'll need to include a valid subscription key.

This is a sample call to the Bing Web Search API:

cURL	 Copy
<pre>curl -X GET 'https://api.cognitive.microsoft.com/bing/v7.0/search? q=Welsch%20Pembroke%20Corgis' \ -H 'Ocp-Apim-Subscription-Key: YOUR_SUBSCRIPTION_KEY' json_pp</pre>	

This is a sample call to the Translator service:

cURL	 Copy
<pre>curl -X POST 'https://api.cognitive.microsofttranslator.com/translate?api- version=3.0&from=en&to=de' \ -H 'Ocp-Apim-Subscription-Key: YOUR_SUBSCRIPTION_KEY' \ -H 'Content-Type: application/json' \ --data-raw ' [{ "text": "How much for the cup of coffee?" }]' json_pp</pre>	

The following video demonstrates using a Cognitive Services key.

Authenticate with a multi-service subscription key

⚠ Warning

At this time, these services **don't** support multi-service keys: QnA Maker, Speech Services, Custom Vision, and Anomaly Detector.

This option also uses a subscription key to authenticate requests. The main difference is that a subscription key is not tied to a specific service, rather, a single key can be used to authenticate requests for multiple Cognitive Services. See [Cognitive Services pricing](#) for information about regional availability, supported features, and pricing.

The subscription key is provided in each request as the `Ocp-Apim-Subscription-Key` header.



Supported regions

When using the multi-service subscription key to make a request to `api.cognitive.microsoft.com`, you must include the region in the URL. For example: `westus.api.cognitive.microsoft.com`.


When using multi-service subscription key with the Translator service, you must specify the subscription region with the `Ocp-Apim-Subscription-Region` header.

Multi-service authentication is supported in these regions:


- australiaeast
- brazilsouth
- canadacentral
- centralindia
- eastasia
- eastus
- japaneast
- northeurope
- southcentralus
- southeastasia
- uksouth
- westcentralus
- westeurope
- westus
- westus2

Sample requests

This is a sample call to the Bing Web Search API:

cURL	 Copy
<pre>curl -X GET 'https://YOUR- REGION.api.cognitive.microsoft.com/bing/v7.0/search? q=Welsch%20Pembroke%20Corgis' \ -H 'Ocp-Apim-Subscription-Key: YOUR_SUBSCRIPTION_KEY' json_pp</pre>	

This is a sample call to the Translator service:

cURL	 Copy
<pre>curl -X POST 'https://api.cognitive.microsofttranslator.com/translate?api- version=3.0&from=en&to=de' \ -H 'Ocp-Apim-Subscription-Key: YOUR_SUBSCRIPTION_KEY' \ -H 'Ocp-Apim-Subscription-Region: YOUR_SUBSCRIPTION_REGION' \ -H 'Content-Type: application/json' \ --data-raw ' [{ "text": "How much for the cup of coffee?" }]' json_pp</pre>	

Authenticate with an authentication token

Some Azure Cognitive Services accept, and in some cases require, an authentication token. Currently, these services support authentication tokens:

- Text Translation API
- Speech Services: Speech-to-text REST API
- Speech Services: Text-to-speech REST API

Note

QnA Maker also uses the Authorization header, but requires an endpoint key. For more information, see [QnA Maker: Get answer from knowledge base](#).

Warning


The services that support authentication tokens may change over time, please check the API reference for a service before using this authentication method.

Both single service and multi-service subscription keys can be exchanged for authentication tokens. Authentication tokens are valid for 10 minutes.

Authentication tokens are included in a request as the Authorization header. The token value provided must be preceded by Bearer, for example: Bearer YOUR_AUTH_TOKEN.

Sample requests

Use this URL to exchange a subscription key for an authentication token: `https://YOUR-REGION.api.cognitive.microsoft.com/sts/v1.0/issueToken`.


cURL	 Copy
<pre>curl -v -X POST \ "https://YOUR-REGION.api.cognitive.microsoft.com/sts/v1.0/issueToken" \ -H "Content-type: application/x-www-form-urlencoded" \ -H "Content-length: 0" \ -H "Ocp-Apim-Subscription-Key: YOUR_SUBSCRIPTION_KEY"</pre>	

These multi-service regions support token exchange:

- australiaeast
- brazilsouth
- canadacentral
- centralindia

- eastasia
- eastus
- japaneast
- northeurope
- southcentralus
- southeastasia
- uksouth
- westcentralus
- westeurope
- westus
- westus2

After you get an authentication token, you'll need to pass it in each request as the Authorization header. This is a sample call to the Translator service:

cURL	 Copy
<pre>curl -X POST 'https://api.cognitive.microsofttranslator.com/translate?api-version=3.0&from=en&to=de' \ -H 'Authorization: Bearer YOUR_AUTH_TOKEN' \ -H 'Content-Type: application/json' \ --data-raw ' [{ "text": "How much for the cup of coffee?" }]' json_pp</pre>	

Authenticate with Azure Active Directory

Important

1. Currently, **only** the Computer Vision API, Face API, Text Analytics API, Immersive Reader, Form Recognizer, Anomaly Detector, and all Bing services except Bing Custom Search support authentication using Azure Active Directory (AAD).
2. AAD authentication needs to be always used together with custom subdomain name of your Azure resource. **Regional endpoints** does not support AAD authentication.

In the previous sections, we showed you how to authenticate against Azure Cognitive Services using either a single-service or multi-service subscription key. While these keys provide a quick and easy path to start development, they fall short in more complex scenarios that require role-based access controls. Let's take a look at what's required to authenticate using Azure Active Directory (AAD).

In the following sections, you'll use either the Azure Cloud Shell environment or the Azure CLI to create a subdomain, assign roles, and obtain a bearer token to call the Azure Cognitive Services. If you get stuck, links are provided in each section with all available options for each command in Azure Cloud Shell/Azure CLI.

Create a resource with a custom subdomain

The first step is to create a custom subdomain. If you want to use an existing Cognitive Services resource which does not have custom subdomain name, follow the instructions in [Cognitive Services Custom Subdomains](#) to enable custom subdomain for your resource.

1. Start by opening the Azure Cloud Shell. Then [select a subscription](#):

PowerShell	Copy	Try It
<pre>Set-AzContext -SubscriptionName <SubscriptionName></pre>		

2. Next, [create a Cognitive Services resource](#) with a custom subdomain. The subdomain name needs to be globally unique and cannot include special characters, such as: ".", "!", ",", ".".

PowerShell	Copy	Try It
<pre>\$account = New-AzCognitiveServicesAccount -ResourceGroupName <RESOURCE_GROUP_NAME> -name <ACCOUNT_NAME> -Type <ACCOUNT_TYPE> - SkuName <SUBSCRIPTION_TYPE> -Location <REGION> -CustomSubdomainName <UNIQUE_SUBDOMAIN></pre>		

3. If successful, the **Endpoint** should show the subdomain name unique to your resource.

Assign a role to a service principal

Now that you have a custom subdomain associated with your resource, you're going to need to assign a role to a service principal.

Note

Keep in mind that AAD role assignments may take up to five minutes to propagate.

1. First, let's register an [AAD application](#).

PowerShell

 Copy Try It

```
$SecureStringPassword = ConvertTo-SecureString -String <YOUR_PASSWORD>
-AsPlainText -Force

$app = New-AzADApplication -DisplayName <APP_DISPLAY_NAME> -
IdentifierUri <APP_URIS> -Password $SecureStringPassword
```

You're going to need the **ApplicationId** in the next step.

2. Next, you need to [create a service principal](#) for the AAD application.

PowerShell

 Copy Try It

```
New-AzADServicePrincipal -ApplicationId <APPLICATION_ID>
```

Note

If you register an application in the Azure portal, this step is completed for you.

3. The last step is to [assign the "Cognitive Services User" role](#) to the service principal (scoped to the resource). By assigning a role, you're granting service principal access to this resource. You can grant the same service principal access to multiple resources in your subscription.

Note

The ObjectId of the service principal is used, not the ObjectId for the application. The ACCOUNT_ID will be the Azure resource Id of the Cognitive Services account you created. You can find Azure resource Id from "properties" of the resource in Azure portal.

Azure CLI



 Copy Try It

```
New-AzRoleAssignment -ObjectId <SERVICE_PRINCIPAL_OBJECTID> -Scope
<ACCOUNT_ID> -RoleDefinitionName "Cognitive Services User"
```

Sample request

In this sample, a password is used to authenticate the service principal. The token provided is then used to call the Computer Vision API.







1. Get your **TenantId**:

PowerShell	 Copy	 Try It
<pre>\$context=Get-AzContext \$context.Tenant.Id</pre>		



2. Get a token:

ⓘ Note

If you're using Azure Cloud Shell, the `SecureClientSecret` class isn't available.

PowerShell	Azure Cloud Shell						
<table border="1"><tr><td>PowerShell</td><td> Copy</td><td> Try It</td></tr><tr><td colspan="3"><pre>\$authContext = New-Object "Microsoft.IdentityModel.Clients.ActiveDirectory.AuthenticationCont ext" -ArgumentList "https://login.windows.net/<TENANT_ID>" \$secureSecretObject = New-Object "Microsoft.IdentityModel.Clients.ActiveDirectory.SecureClientSecret " -ArgumentList \$SecureStringPassword \$clientCredential = New-Object "Microsoft.IdentityModel.Clients.ActiveDirectory.ClientCredential" -ArgumentList \$app.ApplicationId, \$secureSecretObject \$token=\$authContext.AcquireTokenAsync("https://cognitiveservices.az ure.com/", \$clientCredential).Result \$token</pre></td></tr></table>		PowerShell	 Copy	 Try It	<pre>\$authContext = New-Object "Microsoft.IdentityModel.Clients.ActiveDirectory.AuthenticationCont ext" -ArgumentList "https://login.windows.net/<TENANT_ID>" \$secureSecretObject = New-Object "Microsoft.IdentityModel.Clients.ActiveDirectory.SecureClientSecret " -ArgumentList \$SecureStringPassword \$clientCredential = New-Object "Microsoft.IdentityModel.Clients.ActiveDirectory.ClientCredential" -ArgumentList \$app.ApplicationId, \$secureSecretObject \$token=\$authContext.AcquireTokenAsync("https://cognitiveservices.az ure.com/", \$clientCredential).Result \$token</pre>		
PowerShell	 Copy	 Try It					
<pre>\$authContext = New-Object "Microsoft.IdentityModel.Clients.ActiveDirectory.AuthenticationCont ext" -ArgumentList "https://login.windows.net/<TENANT_ID>" \$secureSecretObject = New-Object "Microsoft.IdentityModel.Clients.ActiveDirectory.SecureClientSecret " -ArgumentList \$SecureStringPassword \$clientCredential = New-Object "Microsoft.IdentityModel.Clients.ActiveDirectory.ClientCredential" -ArgumentList \$app.ApplicationId, \$secureSecretObject \$token=\$authContext.AcquireTokenAsync("https://cognitiveservices.az ure.com/", \$clientCredential).Result \$token</pre>							

3. Call the Computer Vision API:

PowerShell	 Copy	 Try It
<pre>\$url = \$account.Endpoint+"vision/v1.0/models" \$result = Invoke-RestMethod -Uri \$url -Method Get -Headers @{"Authorization"=\$token.CreateAuthorizationHeader()} -Verbose \$result ConvertTo-Json</pre>		

Alternatively, the service principal can be authenticated with a certificate. Besides service principal, user principal is also supported by having permissions delegated through another AAD application. In this case, instead of passwords or certificates, users would be prompted for two-factor authentication when acquiring token.

Authorize access to managed identities

Cognitive Services support Azure Active Directory (Azure AD) authentication with [managed identities for Azure resources](#). Managed identities for Azure resources can authorize access to Cognitive Services resources using Azure AD credentials from applications running in Azure virtual machines (VMs), function apps, virtual machine scale sets, and other services. By using managed identities for Azure resources together with Azure AD authentication, you can avoid storing credentials with your applications that run in the cloud.

Enable managed identities on a VM

Before you can use managed identities for Azure resources to authorize access to Cognitive Services resources from your VM, you must enable managed identities for Azure resources on the VM. To learn how to enable managed identities for Azure Resources, see:

- [Azure portal](#)
- [Azure PowerShell](#)
- [Azure CLI](#)
- [Azure Resource Manager template](#)
- [Azure Resource Manager client libraries](#)

For more information about managed identities, see [Managed identities for Azure resources](#).

See also

- [What is Cognitive Services?](#)
- [Cognitive Services pricing](#)
- [Custom subdomains](#)

Is this page helpful?

 Yes  No
