✓ 200 XP ▶

Vault authentication with managed identities for Azure resources

4 minutes

Azure Key Vault uses **Azure Active Directory** to authenticate users and applications that try to access a vault. To grant our web application access to the vault, we first need to register our app with Azure Active Directory. Registering creates an identity for the app. Once the app has an identity, we can assign vault permissions to it.

Apps and users authenticate to Key Vault using an Azure Active Directory authentication token. Getting a token from Azure Active Directory requires a secret or certificate, because anyone with a token could use the application identity to access all of the secrets in the vault.

Our application secrets are secure in the vault, but we still need to keep a secret or certificate outside of the vault in order to access them! This problem is called the *bootstrapping problem*, and Azure has a solution for it.

Managed identities for Azure resources

Managed identities for Azure resources is an Azure feature that your app can use to access Key Vault and other Azure services without having to manage even a single secret outside of the vault. Using a managed identity is a simple and secure way to take advantage of Key Vault from your web app.

When you enable managed identity on your web app, Azure activates a separate token-granting REST service specifically for use by your app. Your app will request tokens from this service instead of directly from Azure Active Directory. Your app needs to use a secret to access this service, but that secret is injected into your app's environment variables by App Service when it starts up. You don't need to manage or store this secret value anywhere, and nothing outside of your app can access this secret or the managed identity token service endpoint.

Managed identities for Azure resources also registers your app in Azure Active Directory for you, and will delete the registration if you delete the web app or disable its managed identity.

Managed identities are available in all editions of Azure Active Directory, including the Free edition included with an Azure subscription. Using it in App Service has no extra cost and requires no configuration, and it can be enabled or disabled on an app at any time.

Enabling a managed identity for a web app requires only a single Azure CLI command with no configuration. We'll do it later on when we set up an App Service app and deploy to Azure. Before that, though, we're going to apply our knowledge of managed identities to write the code for our app.

Check your knowledge

1. How does using managed identities for Azure resources change the way an app authenticates to Azure Key Vault?

○ The app uses a certificate to authenticate instead of a secret.

○ Each user of the app must enter a password.

● The app gets tokens from a token service instead of Azure Active Directory. ✓

When you enable managed identity on your web app, Azure activates a separate token-granting REST service specifically for use by your app. Your app will request tokens from this service instead of Azure Active Directory.

○ Managed identities are automatically recognized by Azure Key Vault and authenticated automatically.

2. Which one of these statements describes a primary benefit of using managed identities for Azure resources to authenticate an app to Key Vault?

○ Using managed identities improves application performance.

● Using managed identities eliminates the need to handle secrets during configuration. ✓

Your app authenticates to a managed identities token service with a secret injected into its environment variables at runtime. This eliminates the need to store secrets during configuration.

○ Managed identities can automatically grant Azure Key Vault permissions.

Next unit: Exercise - Access secrets stored in Azure Key Vault

Continue >