# Module 11: Securing Azure Web Applications

# Lab: Integrating Azure Active Directory with the Events Administration Portal

### Scenario

Even though the Contoso Events web application is public, the Administration application should be locked down to users only from your domain. You have decided to use Azure AD and ASP.NET identity to provide this functionality. In this lab, you will create a new ASP.NET project by using the ASP.NET identity framework and integrate the project with Azure AD. The website will then use your organization accounts for signing in.

### Objectives

After you complete this lab, you will be able to:

* Create an Azure AD Directory
* Secure an Existing ASP.NET Web Application using Azure AD

### Lab Setup

* *Estimated Time*: 90 minutes

Before starting this lab, you must complete the lab in Module 2. For the lab in this module, you will use the available host machine. Also, you must complete the following steps:

1. On the host computer, click **Start**, type **Remote**, and then click **Remote Desktop Connection**.
2. In Remote Desktop Connection, provide the name of your virtual machine in the **Computer** box by using the following format:
   * **[Your VM IP Address]:[*Your VM RDP Port*]**

* **Note:** The name and port for your virtual machine might be saved in the Computer drop-down list. If this is the case, use this value instead of typing it in manually. If you are unsure about your virtual machine’s RDP port, use either of the Azure portals to find your virtual machine’s endpoints. The endpoint with the name **Remote Desktop** is the correct port for RDP. This port is randomized to protect your virtual machine from unauthorized access.

1. In Remote Desktop Connection, click **Connect**. Wait until the RDP client accesses the virtual machine.
2. If necessary, sign in by using the following credentials:
   * User name: **Student**
   * Password: **AzurePa$$w0rd**
3. Verify that you received the credentials to sign in to the Azure portal from your training provider. You will use these credentials and the Azure account throughout the labs in this course.

## Exercise 1: Creating an Azure AD Directory

#### Task 1: Sign in to the Azure Portal

1. Sign in to the Azure Portal (https://portal.azure.com).
2. If this is your first time logging in to the Azure portal, you will see a dialog with a tour of the portal. Click Get Started.

#### Task 2: Creating an Azure Active Directory Instance

1. View the **Directory + subscription** blade.
2. Observe and record the value of the **Current Directory**
3. Create an **Azure Active Directory** with the following details:
   * Organization Name: Contoso Events
   * Initial domain name:
   * Country or region: region closest to your location.

* **Note**: Wait for Azure to finish creating the Azure Active Directory instance prior to moving forward with the lab.

1. Access your newly created **Azure Active Directory**.

#### Task 3: Switch Back to Your Primary Directory

1. View the **Directory + subscription** blade.
2. Return to your default directory within your Azure subscription.

#### Task 4: Populate the Directory With An Example User

**Note**: If you created your Azure subscription using an organizational identity. You will likely not have access to create new users in your directory. You can safely skip this task and use your own identity in the remaining exercises.

1. In the navigation pane on the left side of the Azure Portal, click **All services**.
2. In the **All services** blade that displays, click **Azure Active Directory**.
3. In the **Azure Active Directory** blade, locate the **Manage** section on the left-side of the blade and click the **Users** link.
4. In the **Users - All users** pane, observe that your currently logged in account was automatically added to the directory as an administrator.
5. Click the **New user** button at the top of the pane.
6. In the **User** blade, perform the following actions:
   1. In the **Name** field, enter the value **Example Person**.
   2. In the **User name** field, enter the value **exampleperson@[your domain]**. Make sure you use the domain for your default Azure Active Directory instance. For example, if your default domain was contoso.onmicrosoft.com, the value for this field would be exampleperson@contoso.onmicrosoft.com. Record this username as you will need it to login to your application later in this lab.
   3. Ensure the checkbox for the **Show Password** option is selected.
   4. Copy the value of the **Password** field. You will need this temporary password to login to your application later in this lab.
   5. Click the **Create** button to create the new user and temporary password.

## Exercise 2: Securing an Existing ASP.NET Web Application

#### Task 1: Deploying the Contoso Events Solution using ARM

1. Create a **Template Deployment** with the following details.
   * Custom Deployment: **Allfiles (F):\Mod11\Labfiles\Starter\azuredeploy.json**
   * New Resource Group: MOD11AZAD
2. Wait for the creation task to complete before moving on with this lab.

#### Task 2: Enabling Azure AD Integration with Azure App Service

1. Access the newly created **Web App** with the prefix **webm**.
2. Browse and Observe the web app to confirm it loads successfuly.
3. Access the **Authentication / Authorization** blade within settings and update the following settings:
   * App Service Authentication: On
   * Action to take when request is not authenticated: Log in with Azure Active Directory
4. Update the settings for **Azure Active Directory** within Authentication Providers with the following items:
   * Management Mode: Express
   * Management Mode(2): Create New AD App
   * Create App: contosoevents[Your Name Here]
   * Grant Common Data Services Permissions: On

#### Task 3: Validate Azure AD Security

1. Browse the **Web App** once again.
2. When prompted, login using the account in your *default directory*.
3. On the left-side of the blade, locate and click the **Overview** link.

**Note**: You will now see a prompt asking if you authorize the **contosoevents[Your Name Here]** application in Azure Active Directory to have specific permissions on your behalf.

1. Observe that the web application has remain unchanged but it is now secure.

## Exercise 3: Cleanup Subscription

#### Task 1: Open Cloud Shell

1. At the top of the portal, click the **Cloud Shell** icon to open a new shell instance.
2. In the **Cloud Shell** command prompt at the bottom of the portal, type in the following command and press **Enter** to list all resource groups in the subscription:

* az group list

1. Type in the following command and press **Enter** to view a list of possible CLI commands to *delete a Resource Group*:

* az group delete --help

#### Task 2: Delete Resource Group

1. Type in the following command and press **Enter** to delete the **MOD10MNUL** *Resource Group*:

* az group delete --name MOD11AZAD --no-wait --yes

1. Close the **Cloud Shell** prompt at the bottom of the portal.

#### Task 3: Close Active Applications

1. Close the currently running web browser application.
2. Close the currently running **Visual Studio** application.

**Review**: In this exercise, you "cleaned up your subscription" by removing the **Resource Groups** used in this lab.

©2016 Microsoft Corporation. All rights reserved. The text in this document is available under the [Creative Commons Attribution 3.0 License](https://creativecommons.org/licenses/by/3.0/legalcode), additional terms may apply. All other content contained in this document (including, without limitation, trademarks, logos, images, etc.) are ***not*** included within the Creative Commons license grant. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred. Microsoft makes no warranties, express or implied, with respect to the information provided here.