

**Implement Security Through a Pipeline using Azure DevOps (AZ-2001)**

**Course Number:** MOC-AZ-2001
**Duration:** 1 day

**Overview**

This Microsoft Applied skills training, Implement Security Through a Pipeline using Azure DevOps (AZ-2001), helps attendees prepare for the corresponding exam and teaches them how to configure and secure Azure Pipelines, validate permissions, configure a project and repository structure, extend a pipeline, configure pipelines to use variables and parameters securely, and manage identity for projects, pipelines, and agents.

**Prerequisites**

All attendees must have:

* An Azure Subscription.
* Basic knowledge of Azure DevOps
* Basic knowledge of security concepts like identities and permissions
* Experience using the Azure portal to create resources like Azure Key Vault and set permissions

**Materials**

All Microsoft training students receive Microsoft official courseware.

For all Microsoft Official Courses taught in their entirety that have a corresponding certification exam, an exam voucher is included for each participant.

**Software Needed on Each Student PC**

Attendees will not need to install any software on their computers for this class. The class will be conducted in a remote environment that Accelebrate will provide; students will only need a local computer with a web browser and a stable Internet connection. Any recent version of Microsoft Edge, Mozilla Firefox, or Google Chrome will be fine.

**Objectives**

* Understand the importance of configuring a secure project and repository structure to support pipelines in Azure DevOps
* Understand the importance of pipeline security and how to secure pipeline resources using Azure DevOps
* Validate user permissions, pipeline permissions, approval and branch checks, and audit and manage permissions
* Create nested templates, rewrite the main deployment pipeline, configure the pipeline and the application to use tokenization, remove plain text secrets, restrict agent logging, and identify and conditionally remove script tasks
* Secure access to packages, credential secrets, secrets for services, and Azure Key Vault.
* Ensure that parameters and variables retain their type, identify and restrict insecure use of parameters and variables, move parameters into a YAML file that protects their type, limit variables set at queue time, and validate that mandatory variables are present and set correctly

**Outline**

* Configure a Project and Repository Structure to Support Secure Pipelines
* Configure Secure Access to Pipeline Resources
* Manage Identity for Projects, Pipelines, and Agents
* Configure and Validate Permissions
* Extend a Pipeline to use Multiple Templates
* Configure Secure Access to Azure Repos from Pipelines
* Configure pipelines to Securely use Variables and Parameters