**Lab – 25: Create an Account Lockout in the MFA service.**

**Objective:** The objective of this lab is –

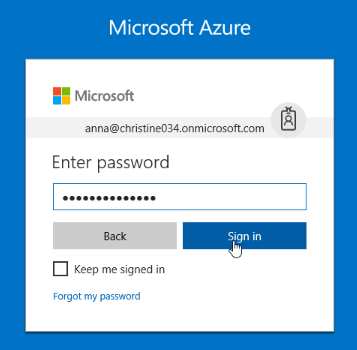
* To create an Account Lockout in the Multi-Factor Authentication service.

You can use temporarily lock accounts if there are too many denied authentication attempts in a row for your organization. In this lab, we are going to create an account lockout.

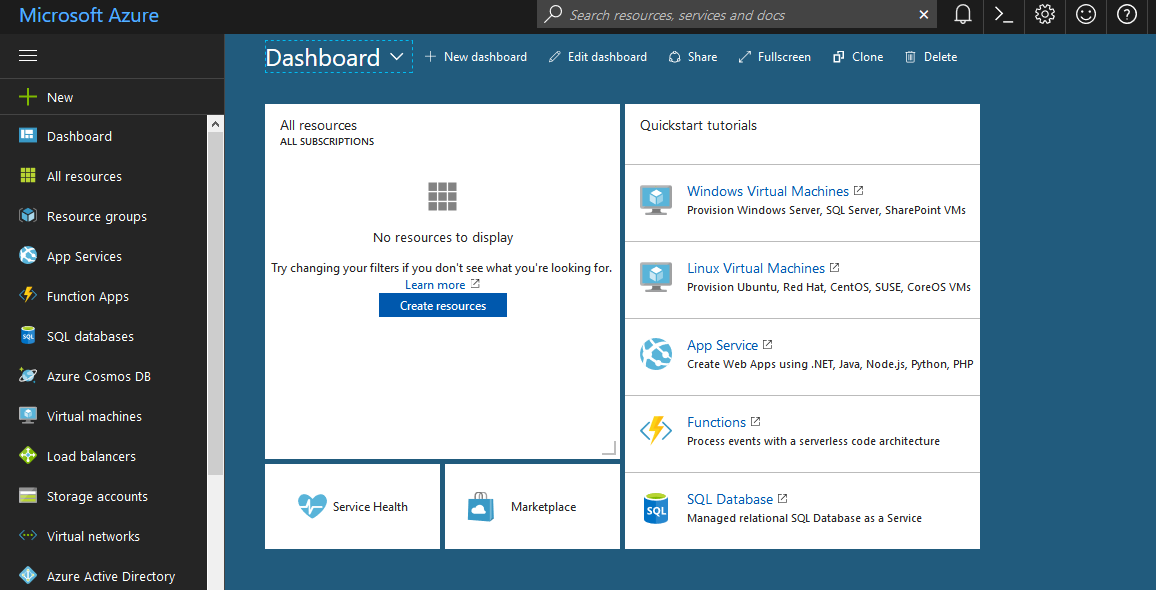
**Prerequisite:** EMS Enterprise Mobility + Security E5.

**Steps:**

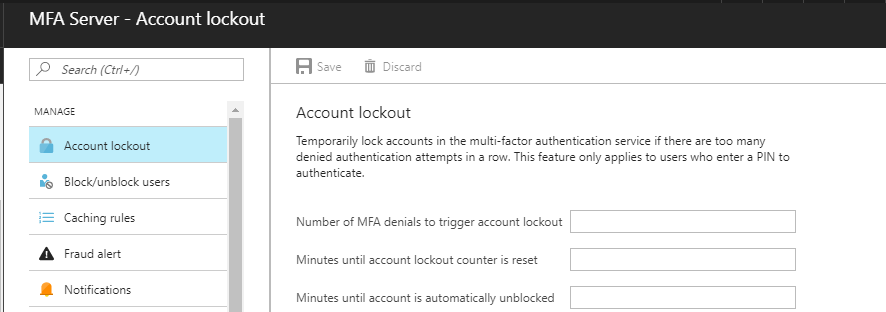
1. Sign in to your Azure Portal, by using the link - **https://portal.azure.com/**. Enter your credentials and click Sign In.



1. Microsoft Azure AD Dashboard will open.

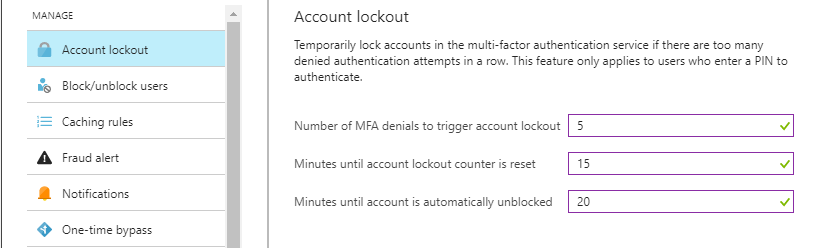


1. Navigate to **Azure Active Directory** > **MFA Server** > **Account Lockout**. This feature allows you to temporarily lock accounts in the multi-factor authentication service if there are too many denied authentication attempts in a row. This feature only applies to users who enter a PIN to authenticate.



1. Enter number of MFA denials to trigger account lockout, here type 5.
2. Enter minutes until account lockout counter is reset, here type 15.
3. And, enter minutes until account is automatically unblocked, here type 20.

Note: You can enter the values according to your requirement.



1. Then, click **Save** from the toolbar.



1. A notification message will pop-up of successfully updated settings.
2. So, in this way you can create an Account Lockout in the Multi-Factor Authentication service.