**Why AD is used?**

* Azure Active Directory is an Identity and Access Management system.
* It is used to grant access to your employees to specific products and services in your network
* The service gives administrators the freedom to choose which information will stay in the cloud, who can manage or use the information, what services or applications can access the information and which end users can have access
* Creating user in active directory select the group like admin, employee, HR
* Then select role like admin, global admin, user

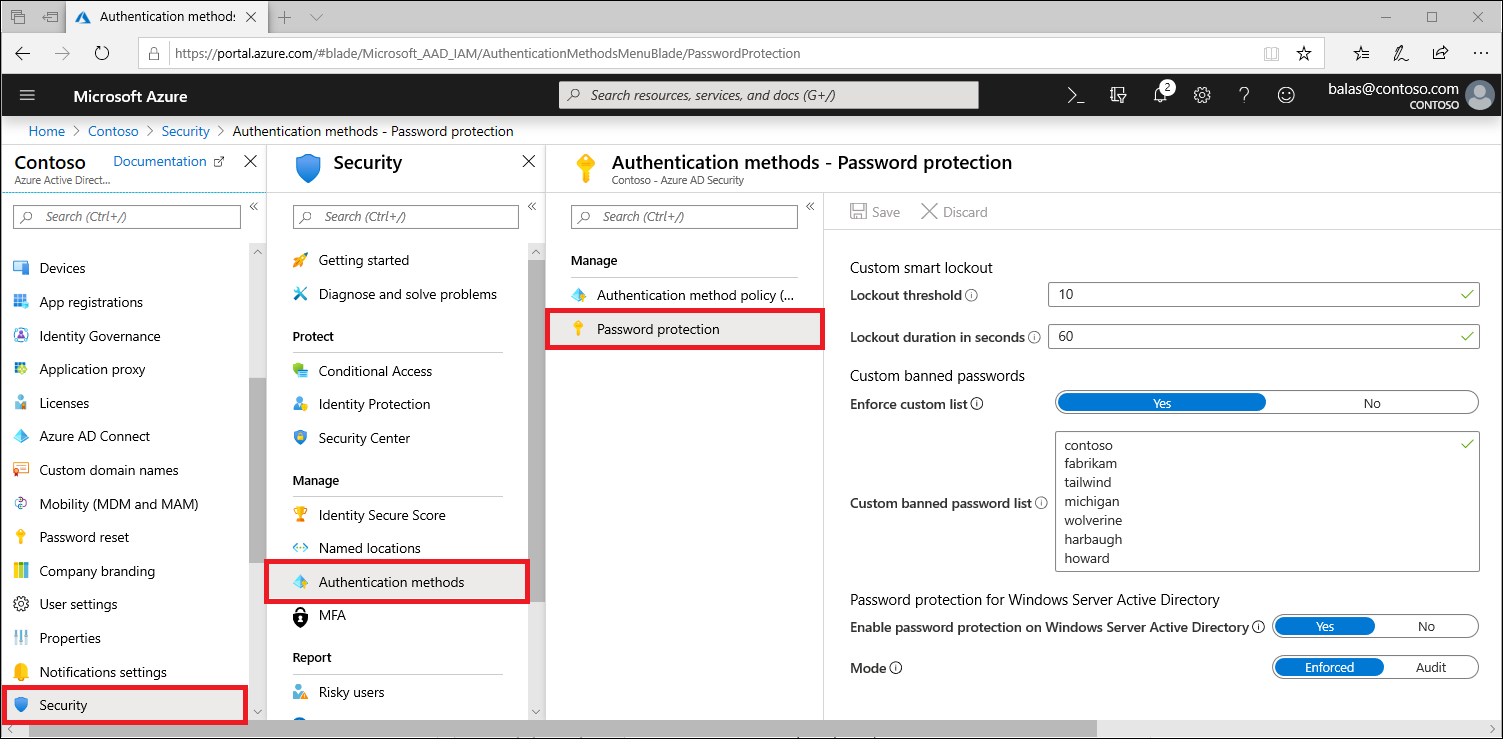
**What happens when you exhaust the maximum failed attempts for authenticating yourself via Azure AD?**

To check or modify the smart lockout values for your organization, use the following steps:

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. Search for and select *Azure Active Directory*. Select **Authentication methods** > **Password protection**.
3. Set the **Lockout threshold**, based on how many-failed sign-ins are allowed on an account before its first lockout. The default is 10.
4. Set the **Lockout duration in seconds**, to the length in seconds of each lockout. The default is 60 seconds (one minute).

 Note

If the first sign-in after a lockout also fails, the account locks out again. If an account locks repeatedly, the lockout duration increases.



## How to determine if the Smart lockout feature is working or not

When the smart lockout threshold is triggered, you will get the following message while the account is locked:

**Your account is temporarily locked to prevent unauthorized use. Try again later, and if you still have trouble, contact your admin**

### What is the difference between Service Bus Queues and Storage Queues?