Configure conditional access

Note:

You are not required to complete the processes, tasks, activities, or steps presented in this example. The various samples provided are for illustrative purposes only and it's likely that if you try this out you will encounter issues in your system.

Conditional access is a feature that enables you to define the conditions under which a user can connect to your Azure subscription and access services. Conditional access provides an additional layer of security that can be used in combination with authentication to strengthen the security access to your network.

Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action. As an example, if a Data Engineer wishes to access services in Azure Synapse Analytics, they may be requested by the conditional access policy to perform an additional step of multi-factor authentication (MFA) to complete the authentication to get onto the service

Conditional access policies use signals as a basis to determine if conditional access should first be applied. Common signals include:

- User or group membership names
- IP address information
- Device platforms or type
- Application access requests
- Real-time and calculated risk detection
- Microsoft Cloud App Security (MCAS)

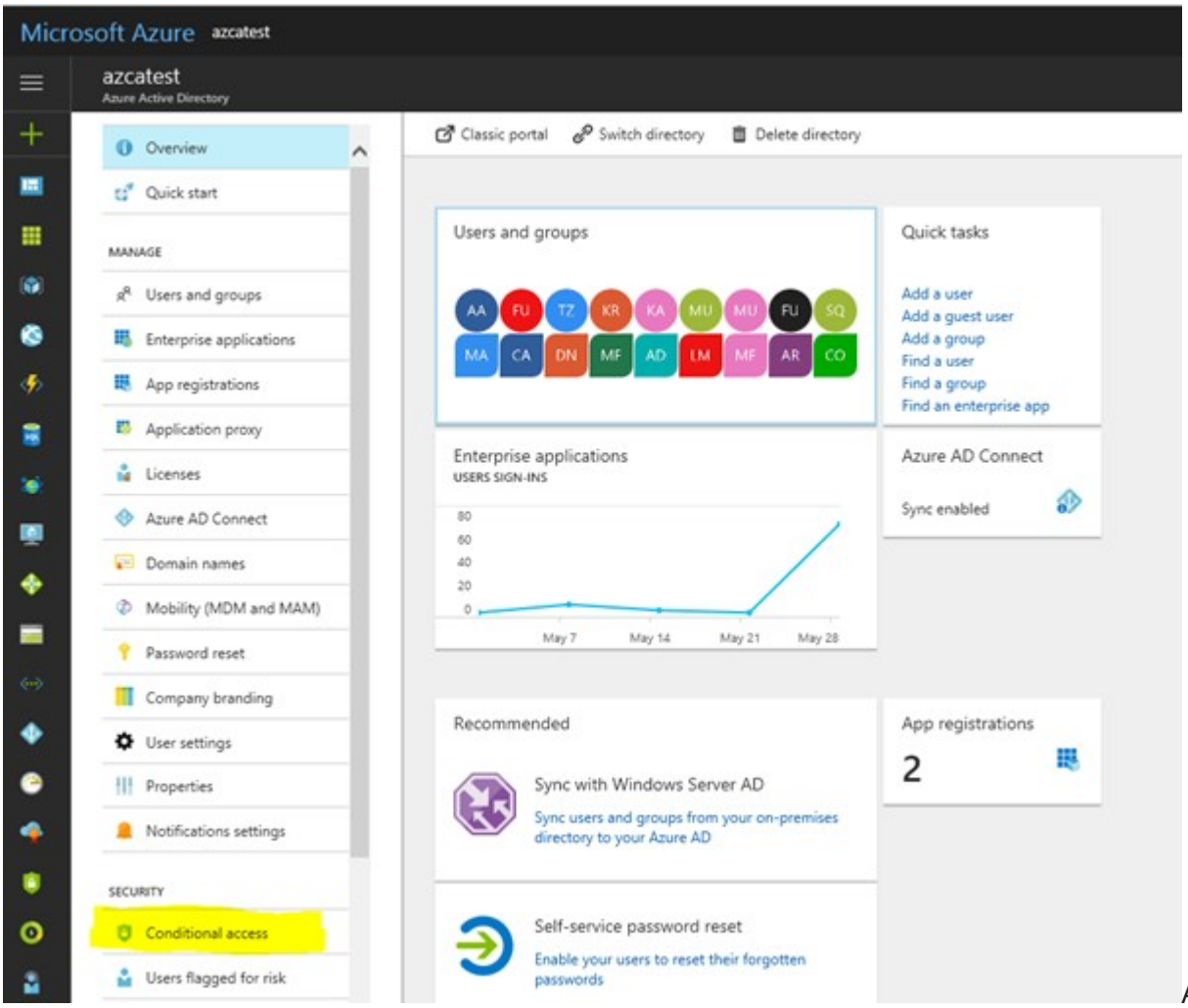
Based on these signals, you can then choose to block access. The alternative is you can grant access, and at the same time request that the user perform an additional action including:

- Perform Multi-Factor authentication
- Use a specific device to connect

Given the amount of data that could potentially be stored, Azure Synapse Analytics dedicated SQL pools supports conditional access to provide protection for your data. It does require that Azure Synapse Analytics is configured to support Azure Active Directory, and that if you chose multi-factor authentication, that the tool you are using support it.

To configure conditional access, you can perform the following steps:

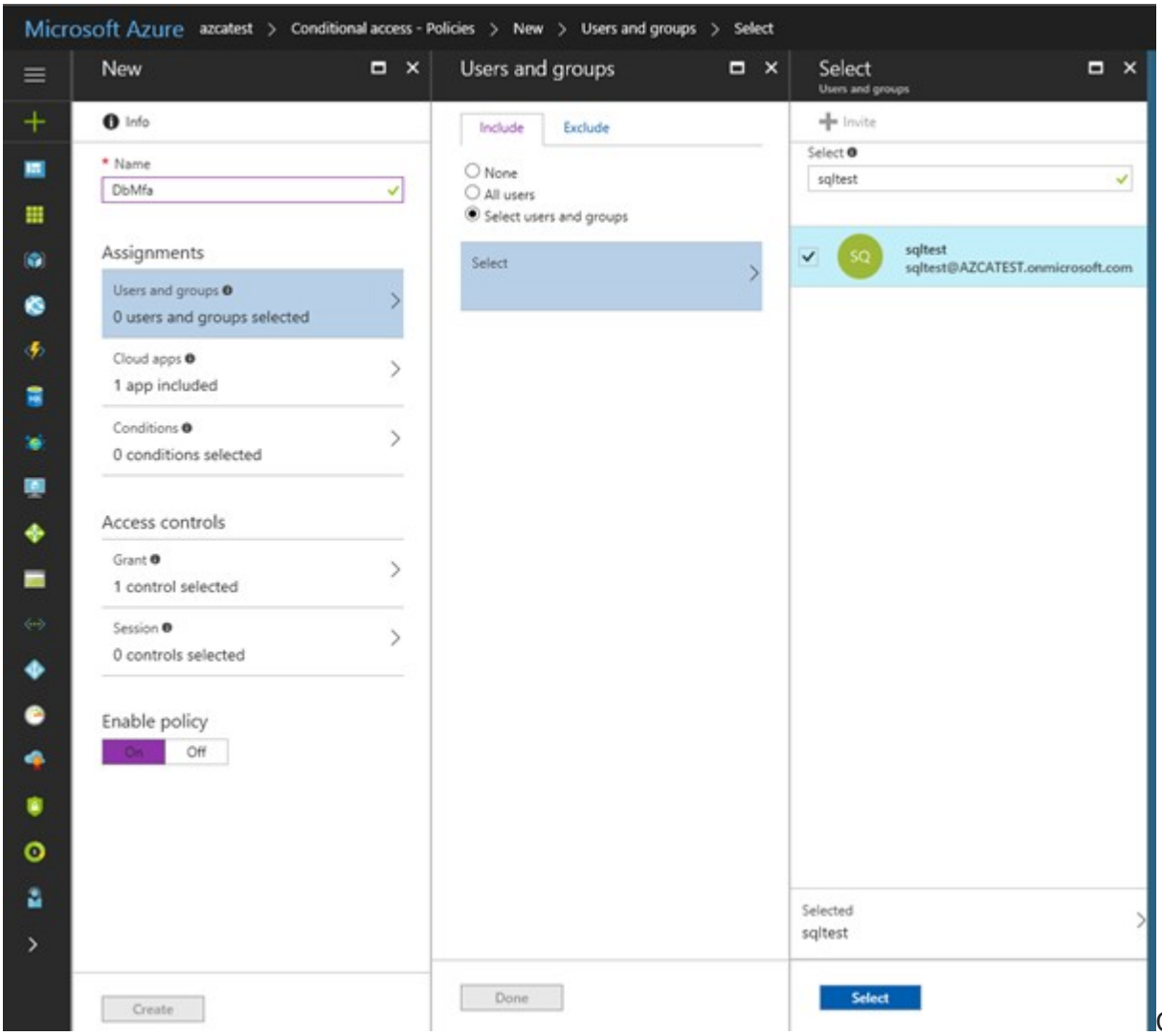
1. Sign in to the Azure portal, select **Azure Active Directory**, and then select **Conditional Access**.



Accessing conditional access in the Azure portal.

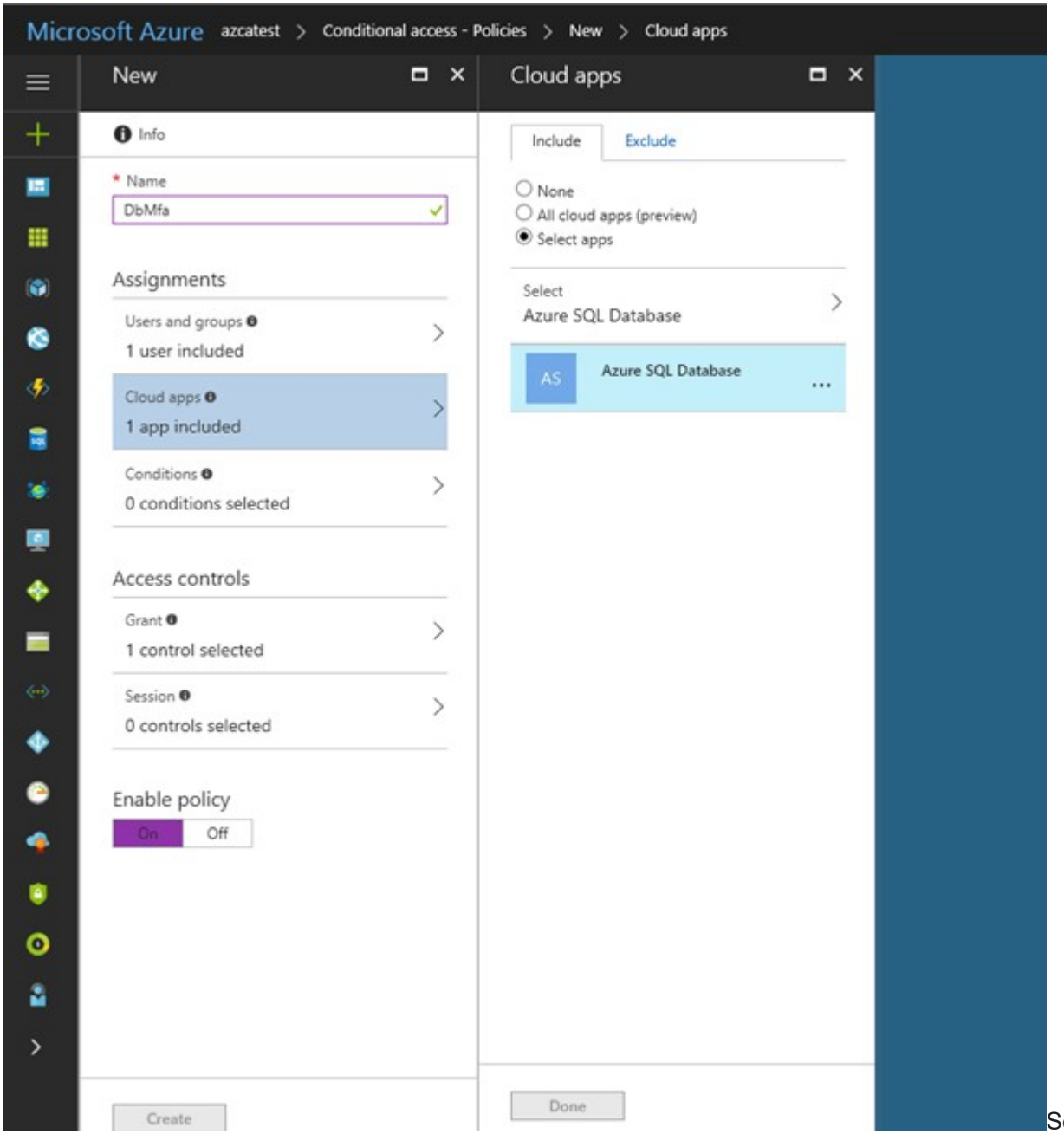
2. In the **Conditional Access-Policies** blade, click **New policy**, provide a name, and then click **Configure rules**.

3. Under **Assignments**, select **Users and groups**, check **Select users and groups**, and then select the user or group for Conditional Access. Click **Select**, and then click **Done** to accept your selection.



Creating a conditional access policy in the Azure portal.

4. Select **Cloud apps**, click **Select apps**. You see all apps available for Conditional Access. Select **Azure SQL Database**, at the bottom click **Select**, and then click **Done**.

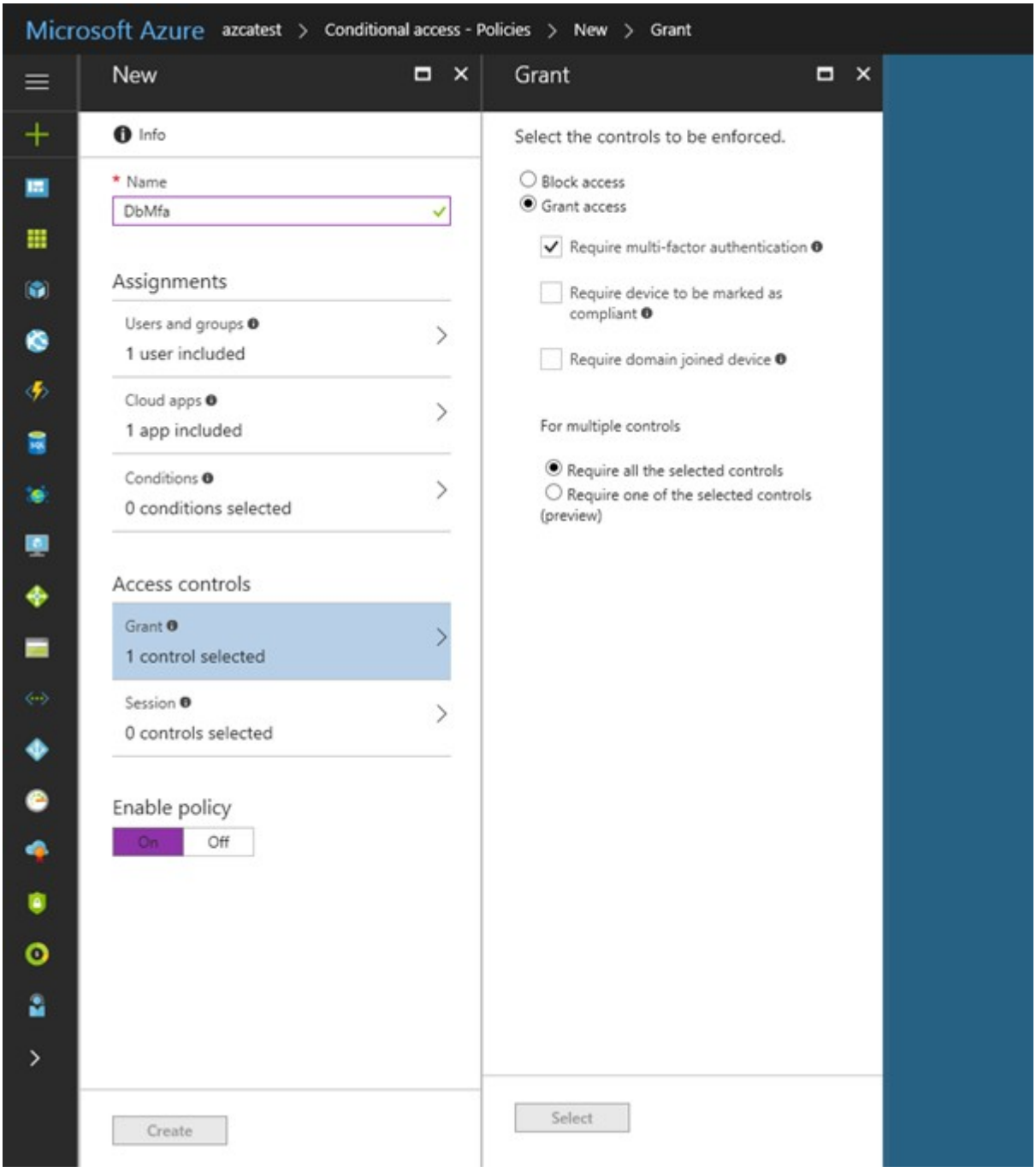


Selecting your service in a conditional access policy in the Azure portal.

5. If you can't find **Azure SQL Database** listed in the following third screenshot, complete the following steps:

- Connect to your database in Azure SQL Database by using SSMS with an Azure AD admin account.
- Execute CREATE USER [user@yourtenant.com] FROM EXTERNAL PROVIDER.

6. Select **Access controls**, select **Grant**, and then check the policy you want to apply. For this example, we select **Require multi-factor authentication**.


Microsoft Azure
azcatest > Conditional access - Policies > New > Grant
New
Info
* Name
DbMfa
Assignments
Users and groups
1 user included
Cloud apps
1 app included
Conditions
0 conditions selected
Access controls
Grant
1 control selected
Session
0 controls selected
Enable policy
On
Off
Create
Grant
Select the controls to be enforced.
Block access
Grant access
Require multi-factor authentication
Require device to be marked as compliant
Require domain joined device
For multiple controls
Require all the selected controls
Require one of the selected controls (preview)
Select