StrategyBlocks

StrategyBlocks : Integrating with Microsoft Azure Active Directory

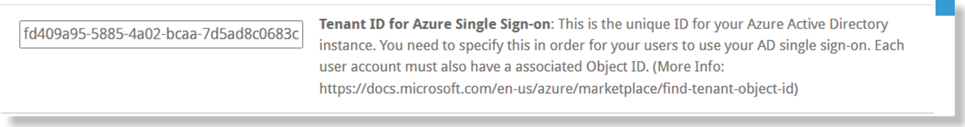
StrategyBlocks and Azure Active Directory

StrategyBlocks now offers deeper integration to Microsoft Azure Active Directory (AAD) extending past the current Single Sign-on (SSO) capability. This integration will provide you the ability to leverage AAD in three primary ways.

- AAD administrators can create users and add them to one or more groups in AAD. These groups can then be synchronized to SB roles (administrator, author, user) and SB security groups in the SB user administration console. New users must be added to a role group and will automatically be made active in SB if available empty seats exist.

- Integration will also allow some user information to be modified, this will include their name *NB: only if they are not in multiple company models*, email address (achieved by creating a new user for the email account and then transferring the membership to the new user), role and security groups.

1

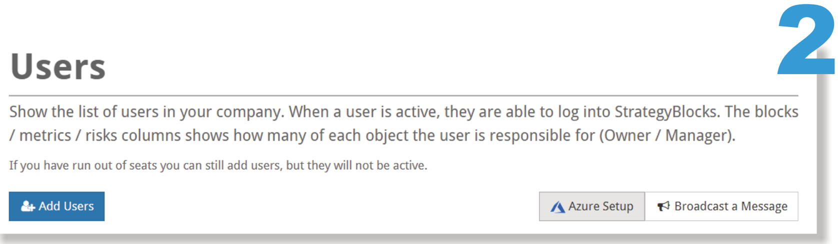


fd409a95-5885-4a02-bcaa-7d5ad8c0683c

Tenant ID for Azure Single Sign-on: This is the unique ID for your Azure Active Directory instance. You need to specify this in order for your users to use your AD single sign-on. Each user account must also have a associated Object ID. (More Info: https://docs.microsoft.com/en-us/azure/marketplace/find-tenant-object-id)

- When a user is removed from AAD, that user account will be deleted in SB only if they do not own any assets (blocks, metrics, risks, dashboards, exports, bookmarks etc), if they do own any asset(s) the account will be made inactive automatically.

2



Users

Show the list of users in your company. When a user is active, they are able to log into StrategyBlocks. The blocks / metrics / risks columns shows how many of each object the user is responsible for (Owner / Manager).

If you have run out of seats you can still add users, but they will not be active.

Setup Steps

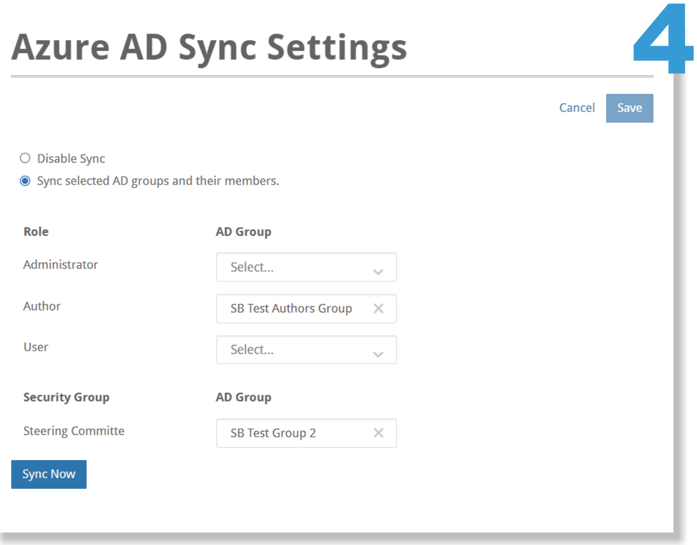
1. In the StrategyBlocks capabilities page **[Company Settings > Capabilities]** add the organizations AD tenant ID. This enables the Azure login button, directing users to login with their network credentials.

2. In the StrategyBlocks users page, click the **Azure** button **[Company Settings > Users > Azure Setup]** and then click **Grant Permission** button. You are only required to do this once per Tenant ID even if you apply it to more than one model *NB: This operation would be ideally carried out by someone who has administration status for both SB and AAD.*

3. In AAD create a new security group to represent your StrategyBlocks users, or you can use an existing group. *NB: making a new one is preferable to maintain consistency*.

4. In the StrategyBlocks Azure AD Sync Settings page [**Company Settings > Users > Azure Setup]**, select the **Sync selected AD groups and their members** option and then select the mapping to the group you created at step 3.

4



Azure AD Sync Settings

○ Disable Sync
● Sync selected AD groups and their members.

Role	AD Group
Administrator	Select...
Author	SB Test Authors Group
User	Select...

Security Group	AD Group
Steering Committe	SB Test Group 2

5. Press **Save** and **Sync Now.**