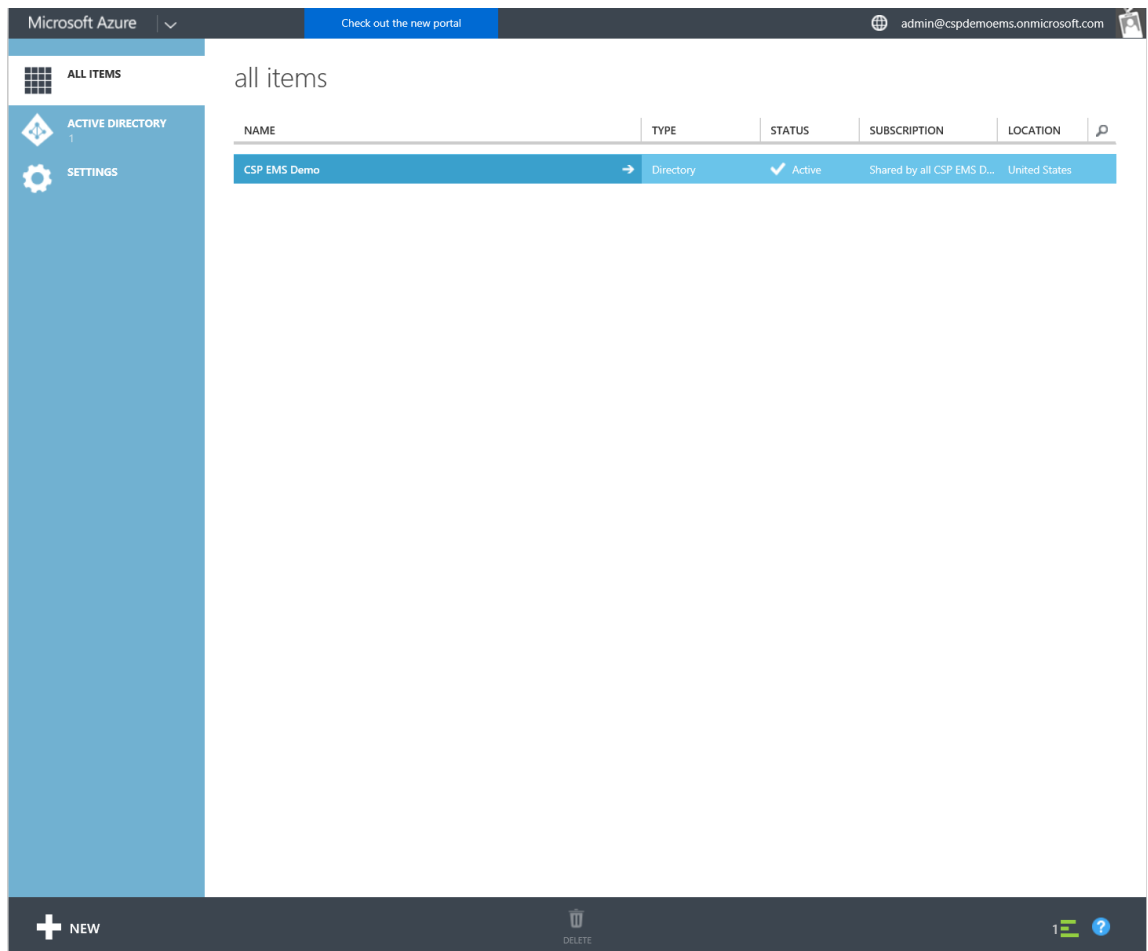


# Configuring Azure access control to Azure SaaS applications

In this **example**, the following instructions will add Azure access control to the SaaS application **Twitter for Marketing**.

1. Sign in to the [Azure Management Portal](#) as a co-administrator for your tenant. Select your AAD tenant.



2. Select the **Applications** tab, then select the SaaS application **Twitter for Marketing**.

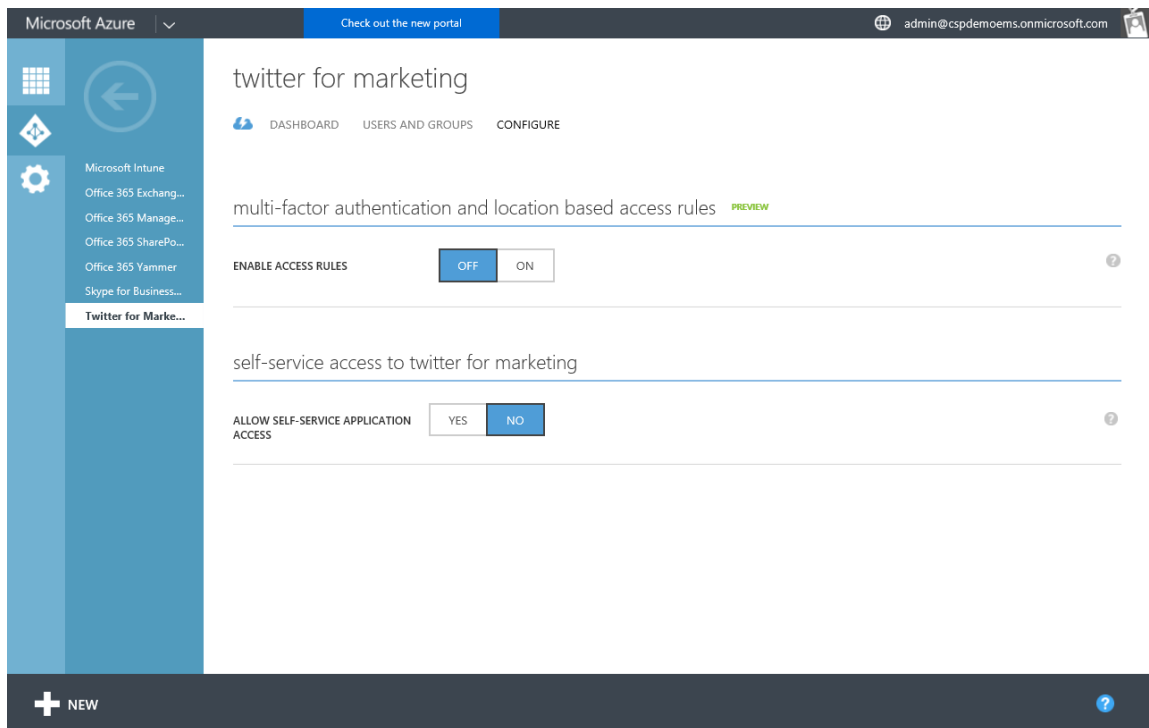
The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure', a dropdown arrow, a 'Check out the new portal' button, and a user profile icon with the email 'admin@cspdemoems.onmicrosoft.com'. The left sidebar contains a grid icon, a back arrow, and a 'CSP EMS Demo' section with a gear icon. The main content area is titled 'csp ems demo' and features a navigation menu with 'DASHBOARD', 'USERS', 'GROUPS', 'APPLICATIONS' (selected), 'DOMAINS', 'DIRECTORY INTEGRATION', 'CONFIGURE', 'REPORTS', and 'LICENSES'. Below the menu is a search bar with a dropdown set to 'Applications my company uses' and a search input field. A table lists applications with columns: NAME, PUBLISHER, TYPE, and APP URL. The 'Twitter for Marketing' application is highlighted in blue.

NAME	PUBLISHER	TYPE	APP URL
Microsoft Intune	Microsoft Corporation	Web application	http://www.microsoft.com/en-us/server-cl...
Office 365 Exchange Online	Microsoft Corporation	Web application	http://office.microsoft.com/outlook/
Office 365 Management APIs	Microsoft Corporation	Web application	
Office 365 SharePoint Online	Microsoft Corporation	Web application	http://office.microsoft.com/sharepoint/
Office 365 Yammer	Microsoft Corporation	Web application	https://products.office.com/yammer/
Skype for Business Online (preview)	Microsoft Corporation	Web application	
Twitter for Marketing	Twitter	Web application	https://twitter.com/

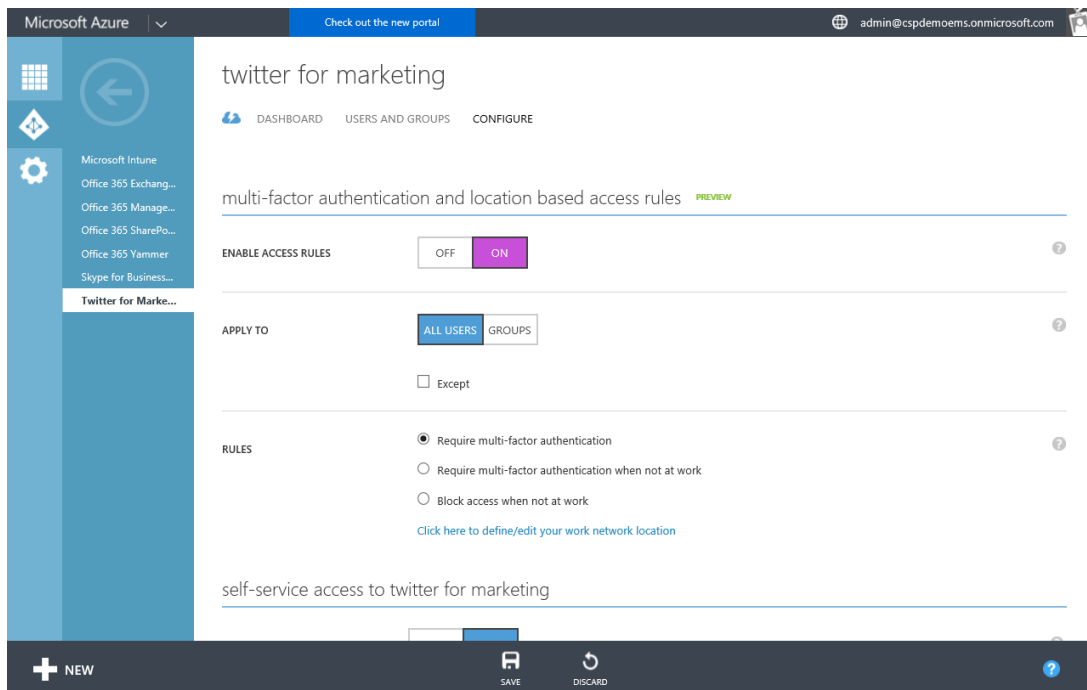
3. Select **Configure**.

The screenshot shows the 'Configure' page for the 'twitter for marketing' application in the Microsoft Azure portal. The top navigation bar is the same as the previous screenshot. The left sidebar shows a list of applications, with 'Twitter for Marke...' selected. The main content area is titled 'twitter for marketing' and has a navigation menu with 'DASHBOARD', 'USERS AND GROUPS', and 'CONFIGURE' (selected). A large message box states 'Your app has been added!' and 'Enable your app to integrate with Microsoft Azure AD', with a checkbox for 'Skip Quick Start the next time I visit'. Below this, there are two numbered steps: 1. 'Enable single sign-on with Microsoft Azure AD' with a 'Configure single sign-on' button and a status indicator 'Single sign-on is enabled for existing application accounts'. 2. 'Assign users to Twitter for Marketing' with an 'Assign accounts' button.

4. Select **ON** to **Enable access rules**.



5. Leave **Apply to** set to **All Users**, and leave **Rules** configured as **Require Multi-Factor Authentication**.



**6. Select **Save**.**

This process can be repeated for any other SaaS applications that are to be integrated with Azure AD.

This Azure access control will add the requirement that all end users assigned to the SaaS application are required to be registered for MFA before access is granted to the application.