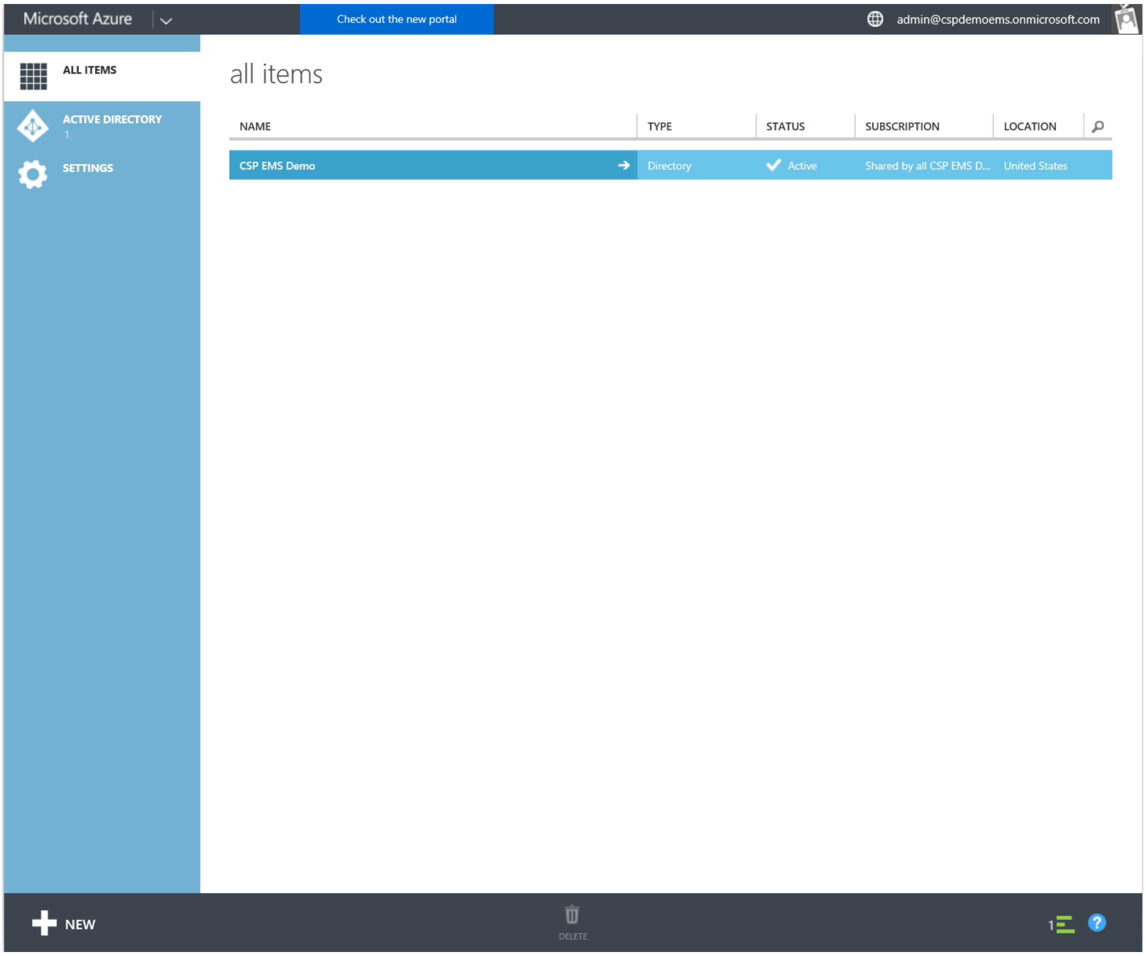
Configuring Azure access control to Azure Saas applications

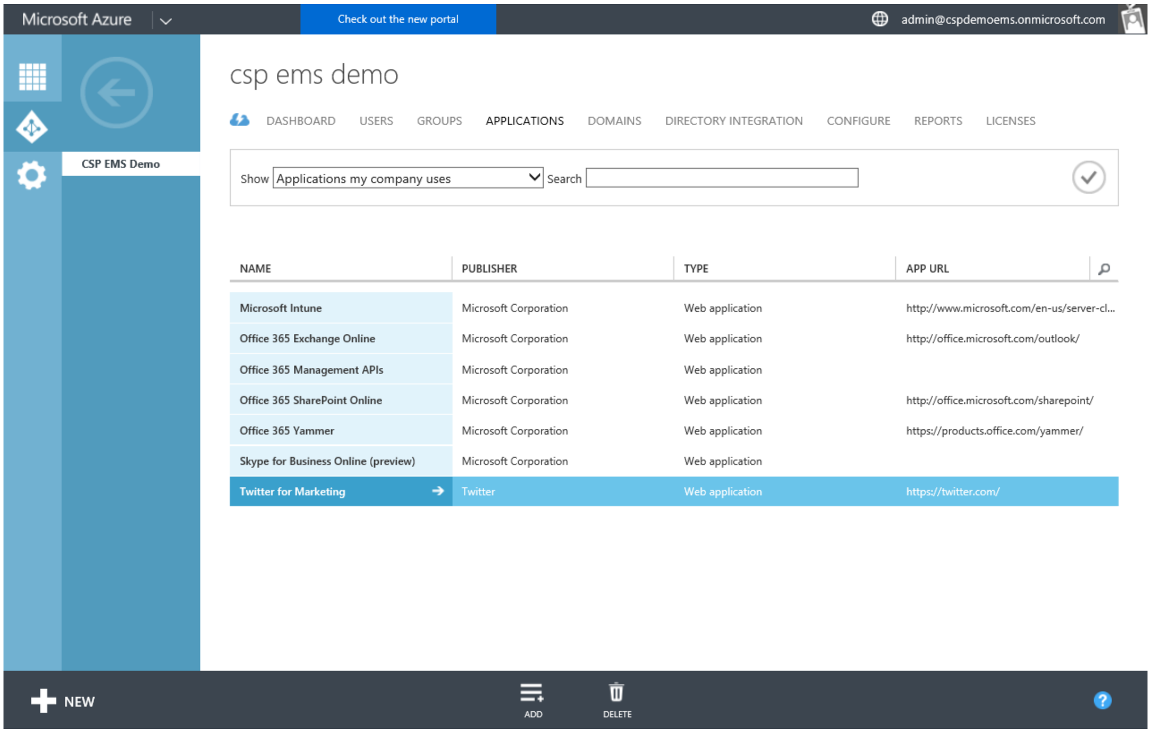
In this **example**, the following instructions will add Azure access control to the SaaS application **Twitter for Marketing**.

1. Sign in to the Azure Management Portal as a co-administrator for your tenant. Select your AAD tenant.



NAME	TYPE	STATUS	SUBSCRIPTION	LOCATION
CSP EMS Demo	Directory	✓ Active	Shared by all CSP EMS D...	United States

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

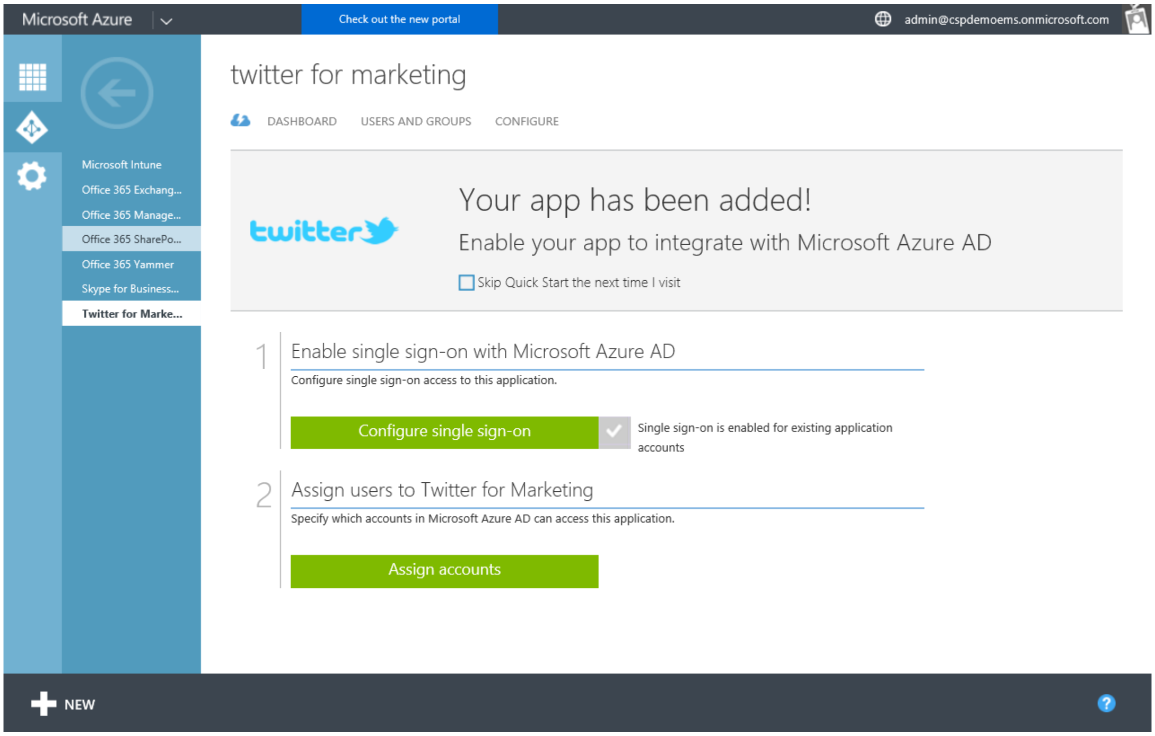


csp ems demo

Show Applications my company uses Search

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.**



twitter for marketing

Your app has been added!

Enable your app to integrate with Microsoft Azure AD

□ Skip Quick Start the next time I visit

1 Enable single sign-on with Microsoft Azure AD

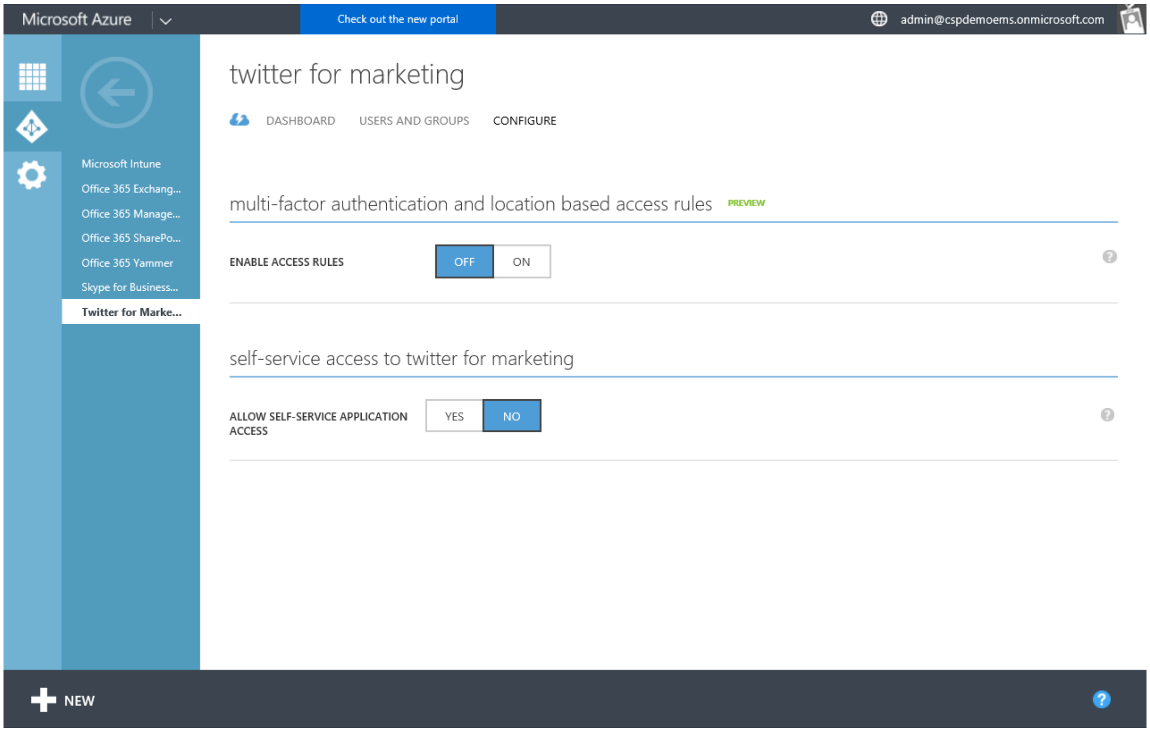
Configure single sign-on access to this application.

✓ Single sign-on is enabled for existing application accounts

2 Assign users to Twitter for Marketing

Specify which accounts in Microsoft Azure AD can access this application.

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



twitter for marketing

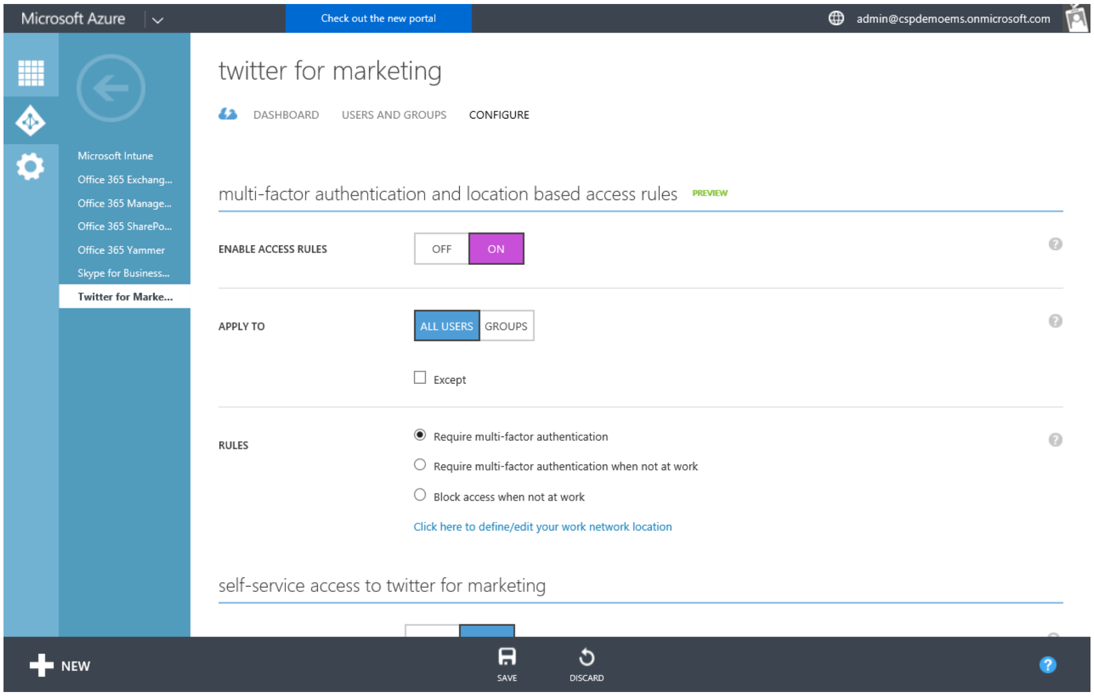
multi-factor authentication and location based access rules

ENABLE ACCESS RULES [✓ OFF] ON

self-service access to twitter for marketing

ALLOW SELF-SERVICE APPLICATION ACCESS YES [✓ NO]

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



twitter for marketing

multi-factor authentication and location based access rules

ENABLE ACCESS RULES OFF [✓ ON]

APPLY TO [✓ ALL USERS] GROUPS

□ Except

RULES

● Require multi-factor authentication

○ Require multi-factor authentication when not at work

○ Block access when not at work

Click here to define/edit your work network location

self-service access to twitter for marketing

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.