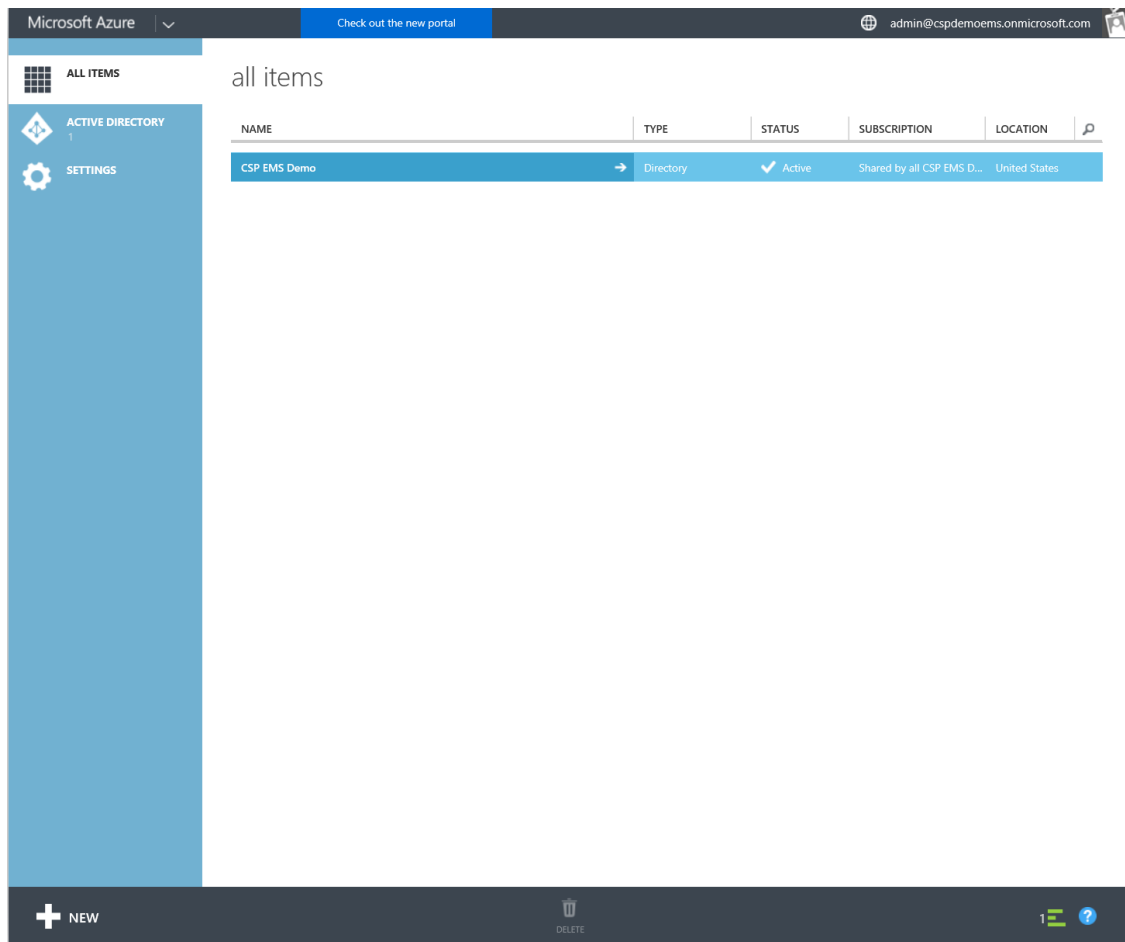


Configuring Multi-Factor Authentication Service Settings

1. Sign in to the [Azure Management Portal](#) and select your Azure Active Directory (AAD) tenant.



2. Select the **Users** tab.

3. At the bottom of the page, select **Manage Multi-Factor Auth.**

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a dropdown arrow, a link to 'Check out the new portal', and the user's email address 'admin@cspdemoems.onmicrosoft.com'. The left sidebar contains a grid icon, a back arrow, and a gear icon. The main content area is titled 'csp ems demo' and features a navigation menu with options: DASHBOARD, USERS, GROUPS, APPLICATIONS, DOMAINS, DIRECTORY INTEGRATION, CONFIGURE, REPORTS, and LICENSES. Below the navigation menu is a table with three columns: DISPLAY NAME, USER NAME, and SOURCED FROM. The table lists five users: 'CSP EMS Demo', 'User Four', 'User One', 'User Three', and 'User Two'. The 'CSP EMS Demo' user is highlighted. At the bottom of the page, there is a dark blue bar with a '+ NEW' button, an 'ADD USER' button, a 'MANAGE MULTI-FACTOR AUTH' button, and a help icon.

DISPLAY NAME	USER NAME	SOURCED FROM
CSP EMS Demo	admin@cspdemoems.onmicrosoft.com	Microsoft Azure Active Directory
User Four	UserFour@cspdemoems.onmicrosoft.com	Microsoft Azure Active Directory
User One	UserOne@cspdemoems.onmicrosoft.com	Microsoft Azure Active Directory
User Three	UserThree@cspdemoems.onmicrosoft.com	Microsoft Azure Active Directory
User Two	UserTwo@cspdemoems.onmicrosoft.com	Microsoft Azure Active Directory

4. The Multi-Factor Authentication portal will be presented. Select the **Service Settings** tab.

Microsoft Azure

admin@cspdemoems.onmicrosoft.com | ?

multi-factor authentication

users service settings

app passwords [\(learn more\)](#)

☒ Allow users to create app passwords to sign in to non-browser apps

☐ Do not allow users to create app passwords to sign in to non-browser apps

trusted ips [\(learn more\)](#)

☐ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

192.168.1.0/27

192.168.1.0/27

192.168.1.0/27

verification options [\(learn more\)](#) **PREVIEW**

Methods available to users:

☒ Call to phone

☒ Text message to phone

☒ Notification through mobile app

☒ Verification code from mobile app

remember multi-factor authentication [\(learn more\)](#) **PREVIEW**

☐ Allow users to remember multi-factor authentication on devices they trust

Days before a device must re-authenticate (1-60):

save

Manage advanced settings and view reports [Go to the portal](#)

5. Configure the **MFA Service Settings** as needed, and select **Save**.