

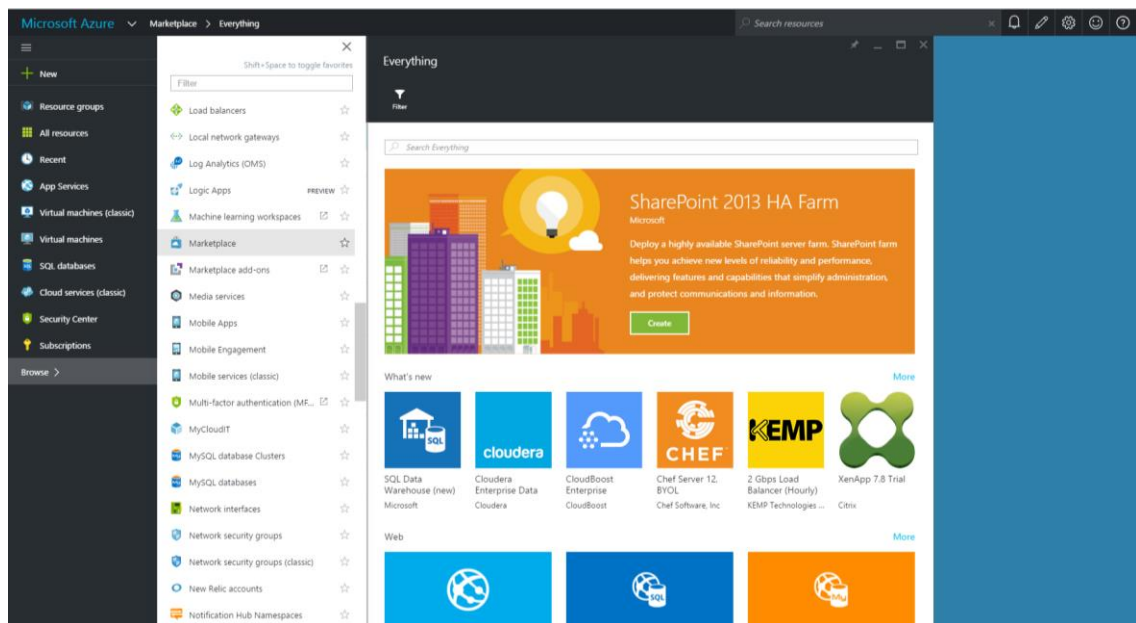
# Configuring the Cloud App Discovery Service

Cloud App Discovery is a Premium feature of Azure Active Directory that enables organizations to discover cloud (SaaS) applications that are used by the employees within the organization.

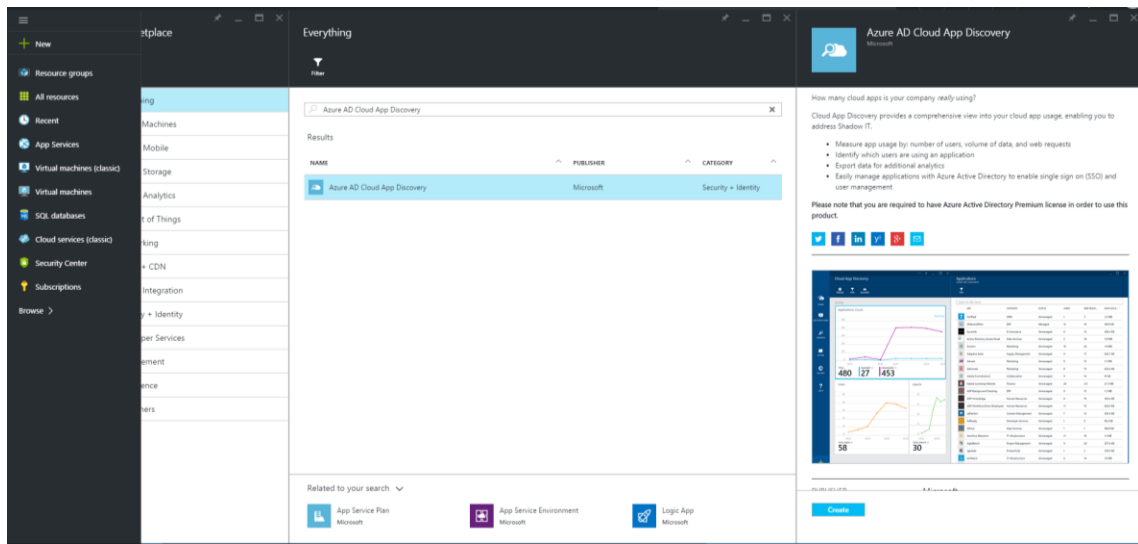
There are number of elements to the Cloud App Discovery service that needs to be agreed upon with the end customer, which will enable visibility of the business and consumer cloud apps in use within the organizations environment. These include the following settings:

- Manage Agent
  - User Consent Option
  - Deep inspection
  - Automatic Updates
- Data Collection
- Store Data
- Manage Access
- Notifications

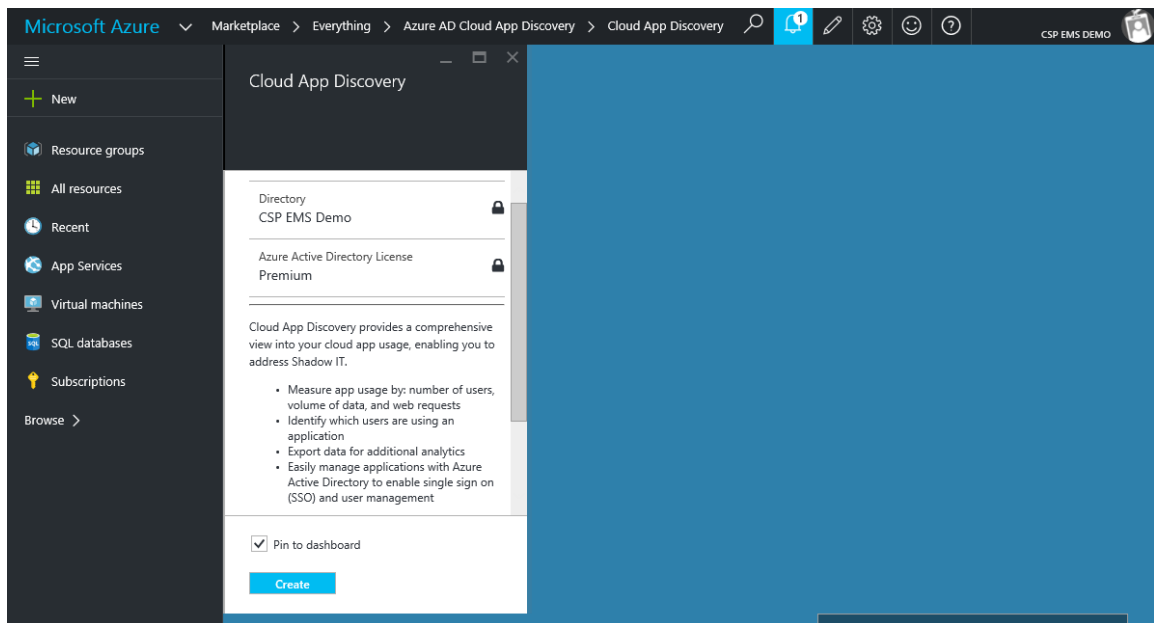
1. In the Azure Administration Portal (<https://portal.azure.com>), browse for and select **Marketplace**.



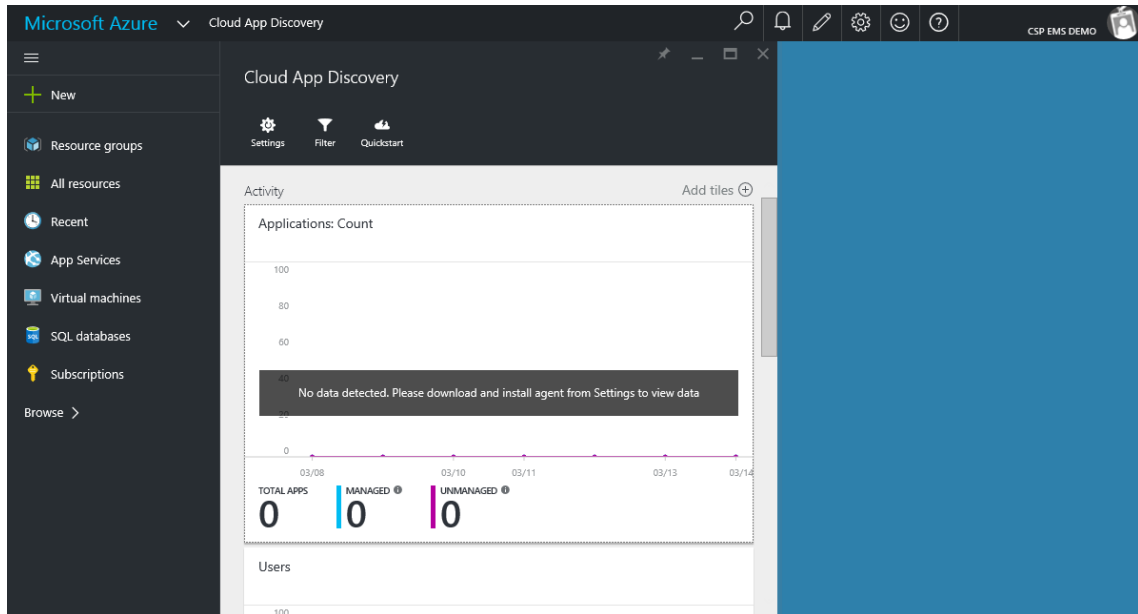
2. Search for and select **Azure AD Cloud App Discovery**. Click **Create**.



3. Verify the Azure AD and Licensing, and click **Create**.



4. A pinned link will be created for Azure AD Cloud App Discovery on the portal dashboard. Click this link, then click **Settings**.



5. Click **Manage Agent** in the Settings pane, and select the **User Consent Option**. Enter the agreed upon end customer settings and select **Update**.

Microsoft Azure Cloud App Discovery > Settings > Manage Agent > User Consent

Settings Cloud App Discovery

Manage Agent Settings

Download Save Discard

Search settings

GENERAL

Manage Agent >

Data Collection >

Store Data >

Manage Access >

Notifications >

Download the agent and deploy to devices managed by your organization to discover cloud apps in use.

User consent option Please select a consent option >

Deep Inspection

on off

I acknowledge that the agent will inspect encrypted traffic in order to gather HTTP information to improve the accuracy of the reporting. [Learn more](#)

Automatic Updates

on off

General

Supported on

☒ No notification or consent required

Web traffic monitoring will begin immediately and without notifying user.

☐ Require notification

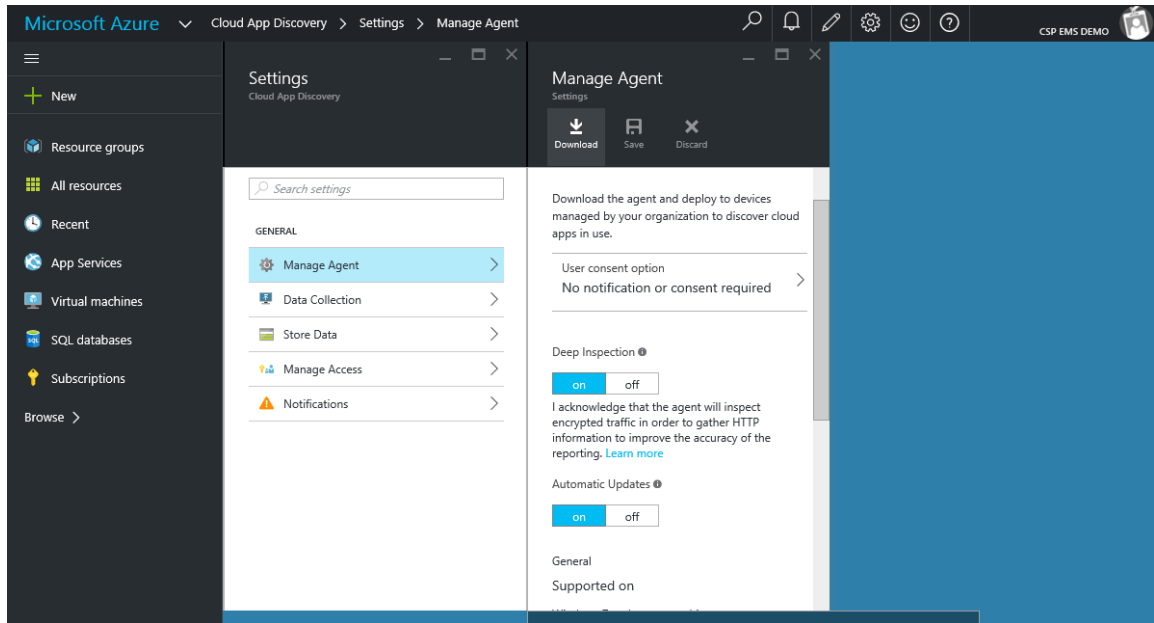
Upon login, the user will be notified that web traffic is monitored. The agent will only start collecting web traffic after the user acknowledges the notification.

☐ Require user consent

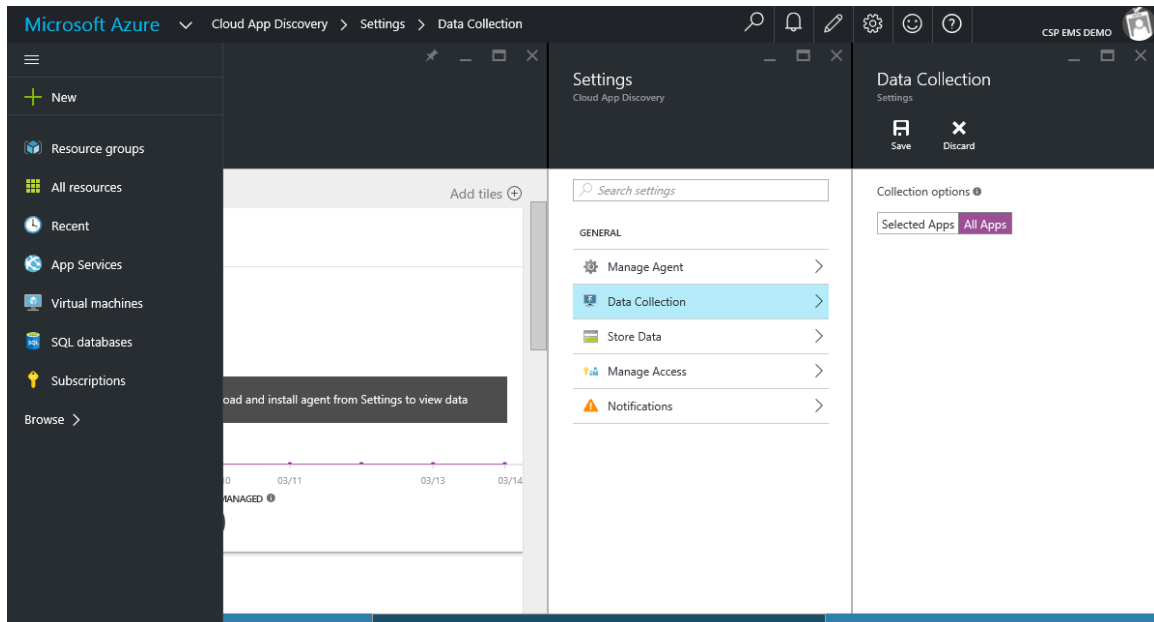
Upon login, the user will be asked to approve data collection. The agent will only start collecting web traffic if the user selects 'Approve'.

Update Reset

6. Select the **Download** link, this will download a compressed file containing the Cloud App Discovery agent installer and the associated Azure AD tenant certificate.



7. Select Data Collection from the settings list, and select the option for Data Collection agreed upon with the end user. Click Save. Note: in this example, All Apps will be captured.



8. Select **Store Data** from the Settings pane, and configure the options for **Manage Access** and **Notifications** and agreed upon with the end customer.

