



Designing Identity Solutions with Azure Active Directory



Hands-on lab

This lab is intended for IT Professionals who need to design and manage Azure Active Directory solutions. In this lab you will learn how to use Azure AD Connect to integrate Azure AD with your on-premises AD, use Azure AD to authenticate with SaaS services and discover which SaaS services are being used.

Produced by HynesITe, Inc
Version 1.0
10/2/2015



This document supports a preliminary release of a software product that may be changed substantially prior to final commercial release. This document is provided for informational purposes only and Microsoft makes no warranties, either express or implied, in this document. Information in this document, including URL and other Internet Web site references, is subject to change without notice. The entire risk of the use or the results from the use of this document remains with the user. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Copyright 2014 © Microsoft Corporation. All rights reserved.

Microsoft Active Directory, Azure Active Directory, Azure, Hyper-V, Windows, and Windows Server 2012 are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Contents

Contents.....	3
Designing Identity Solutions with Azure Active Directory	4
Before You Begin.....	5
Azure Subscriptions	5
Create a Free Trial Account	5
Configure an Azure Pass	6
Hosted Workstations.....	7
Use of Own System.....	7
GitHub repository for Lab Files.....	7
Required Software	7
Optional Software.....	7
Access the Lab Environment	9
Introduction and Scenario	10
Installing and Configuring Azure AD Connect.....	11
Create a DirSync Account in Azure AD	11
Install Azure AD Connect.....	12
Confirm Azure AD Connect Synchronization.....	13
Confirm Initial Synchronization	13
Test Delta Synchronization.....	14
Establishing Single Sign-On with a 3 rd Party Provider and Azure AD.....	16
Adding 3 rd Party providers to the Azure AD directory	16
Test 3 rd Party Single Sign-On	17
Cloud App Discovery.....	19
Enable Azure AD Premium Trial	19
Enable Azure AD Cloud App Discovery.....	19
Configure Cloud App Discovery & Generate Data	20
Generate Cloud App Activity	21
Explore the Cloud App Discovery report.....	21

Designing Identity Solutions with Azure Active Directory

Your Active Directory is one of your most valuable assets when it comes to IT services you provide to your users. Are you leveraging it to its utmost potential? With your users signing up for 3rd party cloud-based SaaS services, what sort of control and visibility do you have to ensure you can help them accessing their data in a secure fashion? Learn how you can securely sync select user Identities with Azure Active Directory in order to replace one-off logons by 3rd party providers in a secure and scalable fashion once you design an updated identity solution with Azure AD.

In this lab you will learn how to install and configure the Azure AD Connect tool, as well as using your Azure AD service to enable Single Sign-on with 3rd party providers. Finally, you will learn how to use Cloud App Discovery to identify which 3rd party SaaS solutions are being used.

Before You Begin

In this lab you will create Azure AD Connect synchronization, Single Sign-On for 3rd Party applications and Cloud App Discovery. This lab is self-contained, but there dependencies between the tasks and exercises. Due to the nature of the lab environment, please ensure that you have enough time to complete the lab in a single sitting. The directory synchronization will be broken when the lab environment is shut down.

Additionally, because you are working with directory services, rather than Azure resources, these objects are not encapsulated as parts of Resource Groups. As a result, there is no cleanup script to undo the directory work you have done. Consequently, you may want to ensure that you use a trial account, rather than your own personal account.

To as great extent as possible, the lab instructions assume the use the Azure Preview Portal, which is located at <https://portal.azure.com>. Some tasks are only available through the Azure Portal. There will be some need to switch back and forth between the two portals. Most of what you will be doing could also be done using the full portal. However, for the sake of consistency and clarity, lab instructions have only been written using the Preview Portal whenever possible. The full portal is located at <https://manage.windowsazure.com>.

For more information on the preview portal, please see <http://channel9.msdn.com/Blogs/Windows-Azure/Azure-Preview-portal> for a brief demonstration or <http://azure.microsoft.com/en-us/documentation/preview-portal/> to read the current documentation for the preview portal.

Azure Subscriptions

This IT Camp lab requires a valid Azure subscription. While you may use an existing subscription such as a subscription associated MSDN account or existing corporate account, it is strongly recommended to use a an Azure Free Trial account or an Azure Pass. By using a Free Trial or an Azure Pass, you will avoid any charges against your MSDN or corporate subscription that would result from doing the exercises in this camp.

Your instructor may be able to provide you with a code that will allow you to redeem an Azure Pass. Or, you may use a CLEAN and UNUSED Azure Trial account - details on how to set up both a Free Trial account and configure an Azure Pass subscriptions are provided below.

Create a Free Trial Account

To create a new Azure trail account perform the following steps.

1. Navigate to www.live.com and click **Sign up now**.
2. Follow the on-screen instructions to create a new Microsoft Account.
3. Navigate to www.azure.com and click **Free Trial**.
4. Follow the on-screen instructions to activate a new Windows Azure Trial.
5. Navigate to Manage.windowsazure.com and sign in.
6. In Microsoft Azure portal, in the upper left, click your user name, and then click **View my bill**.

7. Click your current trial subscription, and then click **Edit subscription details**.
8. Type a name you will recognize in SUBSCRIPTION NAME, such as ITCamps, and then click the **Done** icon.

Configure an Azure Pass

Your instructor may be able to provide you with a pre-provisioned Microsoft Account that already has an Azure Pass subscription associated with it. Alternatively, your instructor may be able to provide you with an Azure promotional code.

To activate the promotional code and create a new Azure Pass account perform the following steps.

1. If you are not using the lab virtual machine to activate your Azure Pass promotional code, ensure you open an InPrivate browser session before performing these steps.
 - ❖ It is critically important that you do not accidentally associate the promotional code with any account that has previously been associated with or linked to an Azure subscription. Use an InPrivate browser session to ensure that no credentials are unintentionally forwarded during the process to activate and redeem the promotional code. If you fail to activate the code because you logged in with the wrong account, you will render the code useless and will not be able to use it again.
2. Navigate to www.live.com and click **Sign up now**.
3. Follow the on-screen instructions to create a new Microsoft Account.
 - ★ Please ensure, you create an outlook.com, live.com or Hotmail.com account. Do not use accounts that have country code suffixes, such as .dk, ca, uk, etc. in their names.
4. Navigate to <http://www.microsoftazurepass.com> and follow the onscreen instructions to redeem the promotional code.
 - ★ Once you have submitted the promotional code, it will take a few minutes for the account to become activated. Only one promo code can be redeemed per the life of the Microsoft ID.
5. Follow the on-screen instructions to activate a new Windows Azure Trial.
6. Navigate to Manage.windowsazure.com and sign in.
7. In Microsoft Azure portal, in the upper left, click your user name, and then click **View my bill**.
8. Click your current trial subscription, and then click **Edit subscription details**.
9. Type a name you will recognize in SUBSCRIPTION NAME, such as ITCamps, and then click the **Done** icon.

Hosted Workstations

Labs in this camp are written to be completed on a pre-configured workstation. This lab, in particular, requires a specific environment that has a domain controller and other servers. A hosted virtual machine environment is provided for this purpose. Your instructor will provide a link to this environment.

If you are using the hosted workstation environment, use **Administrator** as the username and **Passw0rd!** as the password.

Use of Own System

You may complete lab instructions using your own workstation (either Windows 10 or Windows 8.1) and infrastructure, provided that you set up a domain controller, and admin workstation, a server to perform directory synchronization, and so on. As well, on the admin workstation, you need to ensure you have downloaded the files required for the lab from GitHub and have the following software installed.

GitHub repository for Lab Files

If you are not using the hosted virtual machine and are using your own workstation, any custom files the lab instruction call out can be found in a GitHub repository. The repository is located here:

<https://github.com/AZITCAMP/Labfiles>.

Required Software

10. Microsoft Azure PowerShell - <http://go.microsoft.com/?linkid=9811175&clcid=0x409> (also installs the Web Platform Installer)
11. Visual Studio Code - <https://code.visualstudio.com/>
12. GitHub Desktop for Windows - <https://desktop.github.com/>
13. Windows Credential Store for Git (if VSCode won't authenticate with GitHub) - <http://gitcredentialstore.codeplex.com/>
14. Iometer - <http://sourceforge.net/projects/iometer/>

Optional Software

Any additional software that you require will be called out in the lab. The following software may be useful when working with Azure in general.

15. Remote Server Administration Tools - <http://support.microsoft.com/kb/2693643> (Windows 8.1)
or <http://www.microsoft.com/en-ca/download/details.aspx?id=45520> (Windows 10)
16. AzCopy - <http://aka.ms/downloadazcopy>
17. Azure Storage Explorer - <http://azurestorageexplorer.codeplex.com/downloads/get/891668>
18. Microsoft Azure Cross-platform Command Line Tools (installed using the Web Platform Installer)
19. Visual Studio Community 2015 with Microsoft Azure SDK - 2.7.1 (installed using the Web Platform Installer)

- 20. Msysgit - <http://msysgit.github.io>
- 21. PuTTY and PuTTYgen - www.putty.org
- 22. Microsoft Online Services Sign-In Assistant for IT Professionals RTW -
<http://go.microsoft.com/fwlink/?LinkID=286152>
- 23. Azure Active Directory Module for Windows PowerShell (64-bit version) -
<http://go.microsoft.com/fwlink/p/?linkid=236297>

Please note that these lab exercises require a minimum version of 0.9.8 of the Microsoft Azure module for PowerShell. To determine the module version installed on your system, open a Windows PowerShell prompt, type the following commands, and then press ENTER.

```
↪ import-module Azure
↪ get-module Azure).version
```

```
PS C:\> import-module azure
PS C:\> (get-module Azure).Version
```

Major	Minor	Build	Revision
0	9	8	-1

Access the Lab Environment

For this lab you will be accessing a hosted environment that contains all the VMs and resources you require. Your instructor will provide a link to the hosted lab environment.

You should be able to connect with any recent web browser, including Microsoft Edge. Once you have connected to the lab environment, take a few minutes to familiarize yourself with Launchpad.

For this course there are four VMs that you will work in. If you look at the Machines tab on the right side of the lab environment you will find a listing of all the VMs. To switch to another VM, just click on the appropriate name in the Machines list. Below you will find a listing of the VMs for this course.

Virtual Machine	Role
AZRCamp-Admin	Windows 10. A member of the Contoso.com domain. Used for Azure management.
AZRCamp-Edge	A Stand-alone Windows Server 2012 R2 Server. Routing and Remote Access has been installed and it is acting as the default gateway for all outbound traffic.
AZRCamp-DC	Windows Server 2012 R2 domain controller and DNS server.
AZRCamp-Sync	Directory Sync for use in other Labs.

The password for all logons in these VMs is "Passw0rd!".

- ★ You can type this in to the VM manually, or use the **Commands→Paste→Paste Password** sequence from the Launchpad.

Introduction and Scenario

Contoso, Inc. has been using Azure primarily to provide Infrastructure as a Service and Platform as a Service services. It has not been leveraging any security and identity services, such as Azure Active Directory, that are also available in Azure.

One of the management challenges that Contoso is facing is caused by its increasing reliance on applications that are built, hosted, and maintained by 3rd-party vendors, commonly known as Software as a Service (SaaS) applications. For example, Contoso recently migrated from an on-premises customer relationship management (CRM) solution to a cloud-based solution. This is just one example among many SaaS applications that Contoso is increasingly reliant on.

These SaaS applications have provided significant benefits to Contoso in the form of reduced costs and greater agility in managing public relations through social media. However, there has been a management cost. Managing account passwords for sanctioned SaaS applications is proving difficult. Additionally, there is an increasing and unauthorized use of consumer SaaS applications. The extent of this use is unknown at the present time.

Management has asked you to explore how Azure AD might benefit the organization by providing single sign capabilities for SaaS applications. Additionally, you have a mandate to explore how Cloud App Discovery, which is part of Azure Active Directory Premium, can assist Contoso in discovering consumer cloud applications that are currently in use and that can be potentially integrated with Azure AD single sign on.


Installing and Configuring Azure AD Connect

Azure Active Directory (Azure AD) provides the heart of your authentication and identity services in Azure, just as Active Directory (AD) does for your on-premises infrastructure. Azure AD Connect allows you to quickly and easily leverage your existing AD investment by synchronizing users and groups from your on-premises AD to Azure AD.

In this lab you will download and install Azure AD Connect, configure it with the default configuration—which includes password synchronization—and test and verify synchronization.

Create a DirSync Account in Azure AD

Azure AD Connect requires an Azure AD account with the Global Admin role to enable the synchronization. You should not use the default Global Admin account, i.e. the Microsoft ID you used to create the Azure subscription. In this task you will create a Global Admin account to be used for Azure AD Connect directory synchronization.

 Begin this task logged in to **AZRCamp-Admin**, logged in as **Contoso\Administrator** with a password of **Passw0rd!**.

24. Open the Azure Preview Portal (<https://portal.azure.com>), and log on to your Azure subscription.

25. In the home page, click on **Azure Portal**.

 This will open the legacy Azure portal. At this time Azure AD can only be managed in this portal.

26. In the navigation bar of the Azure portal, scroll down until “Active Directory” appears.

27. Click **ACTIVE DIRECTORY**.


28. In the Active Directory pane, click **Default Directory**.

29. Click the **USERS** link.

30. Click **ADD USER**.

31. In the “Tell us about this user” screen, in the USER NAME box, type **DirSync**.

32. Record the entire username that will be created.

 You will need this information in later tasks. It should be in the format of
`<user>@<yoursubscription>.onmicrosoft.com`.

33. Click **Next** (the right arrow in the lower right corner of the page).

34. Complete the “user profile” screen with the following information, then click **Next**.

First Name: Directory

Last Name: Sync

Display Name: DirSync



Role: Global Admin

Alternate Email Address: <Use an email address you can access>

35. In the "Get temporary password" page, click **create**.
36. Record the password, and then click **Complete** (the check mark).
37. Open a new InPrivate window in the web browser.
38. Log on the Azure Preview Portal using the DirSync account and temporary password you just created.
39. When prompted to update your password, create and confirm a new password of "Passw0rd!"
40. Click **Update password and sign in**.
 - ✦ You have now configured an account that will be used for directory synchronization.
41. Log out of the Azure Preview Portal that is running in the InPrivate window.

Install Azure AD Connect

In this task you will download the Azure AD Connect tool from the Azure Preview Portal, and then you will do an express installation of the tool on a dedicated synchronization server. The default installation will automatically do an initial directory synchronization.

- ✦ Begin this task logged in to **AZRCamp-Admin**, logged in as **Contoso\Administrator** with a password of **Passw0rd!**.
1. If required, open the Azure Preview Portal (<https://portal.azure.com>), and log on to your Azure subscription.
 2. In the home page, click on **Azure Portal**.
 - ✦ This will open the legacy Azure portal. At this time Azure AD can only be managed in this portal.
 3. In the navigation bar of the Azure portal scroll down until "Active Directory" appears.
 4. Click **ACTIVE DIRECTORY**.
 5. In the Active Directory pane, click **Default Directory**.
 6. Click on the **Quick Start** link to the left of the Users link.
 7. In the "GET STARTED" section of the Default Directory page, click **Download Azure AD Connect**.
 - ✦ This will open up a download page in a new tab of your web browser.
 8. Click **Download**, and wait for the download to complete.
 9. Click **View downloads**.
 10. In the Downloads pane, click **Open folder**.
 - ✦ The File Explorer icon in the taskbar should flash.
 11. Click on the icon and confirm that AzureADConnect.msi is in the Downloads folder.


12. Copy and paste AzureADConnect.msi to **C:**.
 - ✦ This will make it easier to find in later steps.
13. If prompted to provide administrator permission, click **Continue**.
 - ✎ Perform the following steps logged in to **AZRCamp-Sync**, logged in as **Contoso\Administrator** with a password of **Passw0rd!**.
14. Open File Explorer and navigate to **\\Admin\c\$**.
15. Copy the AzureADConnect.msi file to **C:**.
16. Once copied, double-click **AzureADConnect.msi**.
17. When prompted with a security warning, click **Run**.
18. The Microsoft Azure Active Directory Connect wizard will start.
 - ✦ It may open behind the current active window.
19. Minimize the File Explorer window.
20. In the Welcome to Azure AD Connect page, agree to the license terms and privacy notice, and then click **Continue**.
21. In the Express Settings page, review what the wizard will do, and then click **Use express settings**.
22. On the Connect to Azure AD page, enter the username and password of the DirSync account you created in the previous task, then click **Next**.
23. On the Connect to AD DS page, enter the following credentials, then click **Next**.
Username: **Contoso\Administrator**
Password: **Passw0rd!**
24. Review the information on the "Ready to configure" page.
25. Confirm that there is a check in the box to start synchronization, and then click **Install**.
26. It may take up to 5 minutes for configuration to complete. When it does, review the information on the page, and then click **Exit**.

Confirm Azure AD Connect Synchronization

In this task you will verify that the Azure AD Connect directory synchronization has occurred, and then you will force a manual delta synchronization to confirm that future changes will also synchronize.


Confirm Initial Synchronization

- ✎ Begin this task logged in to **AZRCamp-Admin**, logged in as **Contoso\Administrator** with a password of **Passw0rd!**.
1. If required, open the Azure Preview Portal (<https://portal.azure.com>), and log on to your Azure subscription.


2. In the home page, click on **Azure Portal**.
 This will open the legacy Azure portal. At this time Azure AD can only be managed in this portal.
3. In the navigation bar of the Azure portal, scroll down until "Active Directory" appears.
4. Click **ACTIVE DIRECTORY**.
5. In the Active Directory pane, click **Default Directory**.
6. In the "default directory" page, click **USERS**.
7. The first user listed should be "Admin" and be sourced from Local Active Directory, as seen below.

DISPLAY NAME	USER NAME	SOURCED FROM
Admin	Admin@taytaynzoutlookco.onmicrosoft.com	Local Active Directory
DirSync	DirSync@taytaynzoutlookco.onmicrosoft.com	Microsoft Azure Active Directory
On-Premises Directory Synchronization Service Account	Sync_SYNC_a74c7c5ca083@taytaynzoutlookco.onmicroso...	Local Active Directory
Taylor Finley	taytaynz@outlook.co.nz	Microsoft account

Test Delta Synchronization

1. Minimize your web browser.
2. Use the Search bar to find and open "Active Directory Users and Computers"
3. Create a new user account in the Users container with the following details.
 - First Name: Test
 - Last Name: User
 - Full Name: Test User
 - User logon name: TestUser
 - User logon name (pre-Windows 2000): TestUser
 - Password: Passw0rd!
 - User must change password at next logon: No
-  Begin this task logged in to **AZRCamp-Sync**, logged in as **Contoso\Administrator** with a password of **Passw0rd!**.
4. Use the shortcut on the desktop to open the **Windows Azure Active Directory Module for Windows PowerShell**.
5. Type the following command and press **Enter**.

```
Cd 'C:\Program Files\Microsoft Azure AD Sync\Bin'
```
6. Type the following command and press **Enter**. This will manually trigger a delta directory synchronization.

```
.\DirectorySyncClientCmd.exe delta
```
-  Begin this task logged in to **AZRCamp-Admin**, logged in as **Contoso\Administrator** with a password of **Passw0rd!**.

7. Refresh the "USERS" page of the Azure default directory. Test User should now appear in the Azure default directory.

✦ You have just confirmed that ongoing synchronization is successful.

Establishing Single Sign-On with a 3rd Party Provider and Azure AD

Azure is not the only Software as a Service (SaaS) provider that organizations use. Azure AD allows you to create a single sign-on solution that can securely store the credentials for these third party providers, as well as act as a broker to use these authentication mechanisms for your own web apps.

In this exercise you will configure Azure AD to store the credentials for a third party SaaS provider, and then you will test the single sign-on capabilities provided by the Azure AD sign in page.

Adding 3rd Party providers to the Azure AD directory

In this task you will add a 3rd-party provider to your Azure AD and configure it with predefined credentials.

- ✎ Begin this task logged in to **AZRCamp-Admin**, logged in as **Contoso\Administrator** with a password of **Passw0rd!**.
1. If not already there, open the Azure Preview Portal, and open the default directory Azure AD page.
 2. Click **APPLICATIONS**.
 3. Click **ADD**.
 4. On the "What do you want to do?" page, click **Add an application from the gallery**.
 5. On the "Add an application for my organization to use" page, click **Social** in the left column, then click **Facebook**.
 - ✎ If you have an account for a different application that is in the gallery, you may use that application instead.
 6. Click **Complete** (the check in the lower right corner).
 7. On the facebook (or whichever application you are using) page, click **Configure single sign-on**.

The screenshot shows the 'Your app has been added!' page for Facebook in the Azure AD portal. The page is divided into two main sections:

- 1 Enable single sign-on with Microsoft Azure AD**: This section includes the text 'Configure single sign-on access to this application.' and a green button labeled 'Configure single sign-on'. To the right of the button is a checkbox labeled 'Single sign-on is enabled for existing application accounts' which is checked.
- 2 Assign users to Facebook**: This section includes the text 'Specify which accounts in Microsoft Azure AD can access this application.' and a green button labeled 'Assign accounts'.

At the bottom right of the page, there is a small 'Active' status indicator.

8. On the "How would you like users to sign on to Facebook?" page, select "Password Single Sign-On", and then click **Complete**.
9. Click **Assign Accounts**.
10. Click on the line for "Test User", and then click **ASSIGN**.
11. Put a check in the box "I want to enter Facebook credentials on behalf of the user".
 - ✦ If you choose not to enter credentials, the user will be given the opportunity to provide the credentials when they first attempt to access the SaaS application from the Azure AD sign-in page.
12. Enter a facebook login email address and password that you know, and then click **Complete**.
 - ✦ It will be securely stored as part of Azure AD.
 - 💡 Tip: Type the password in Notepad to ensure it is correct, and then past it to the Azure screen. If you make a mistake, single sign on will fail.
13. Click **DASHBOARD**.



14. From the "quick glance" section of the application's dashboard, copy the Single Sign-On URL.

Test 3rd Party Single Sign-On

In this task you will install the access agent on a client machine and test that the Azure Single Sign-On is passing the credentials to the 3rd Party application.

1. Open an Internet Explorer inPrivate browsing window and paste in the url you just copied into the address bar.
 - 💡 If prompted for credentials, use the Test User user name and password.
2. When prompted to install some software first, click **Install Now**.
3. In the download bar at the bottom of your browser click **Run**.
4. In the Welcome to the Access Panel Extension Setup Wizard, click **Next**.
5. Click **Install**.
6. In the User Account Control dialog box, click **Yes**.

7. Click **Finish**.
8. In the Set up Internet Explorer 11 box, choose to use the recommended settings, and then click **OK**.
9. In the add-in box at the bottom of Internet Explorer 11, click **Enable**.
10. Close Internet Explorer.
 - ◆ Internet Explorer needs to be restarted for the Access Control add-in to function properly.
11. Use the Search bar to open Internet Explorer.
12. Type <https://myapps.microsoft.com> into the address bar and then press **Enter**.
13. Notice that an Azure logon page appears. Log on using the Test User username and password.
14. Click on the **Facebook** tile.
15. Watch as you are automatically logged on to Facebook.
 - ◆ If you are prompted for a password, double-check that you entered the correct password when configuring this in Azure.
16. Log off of Facebook and close Internet Explorer.

Cloud App Discovery

Azure Cloud App Discovery (a feature of the Azure AD Premium services) allows you to track what SaaS applications are being accessed by your staff. The Cloud App Discovery agent, once deployed to a user, can evaluate the web and application traffic and report back to Azure which SaaS applications are being used.

The Cloud App Discovery can then compare and analyze that data and generate reports to help you better understand which known (or registered) apps are being used, as well as which unregistered apps are being used. With this report you can take appropriate action to meet your needs, whether that is to register the apps for single sign-on in Azure AD or find ways to block access.

In this exercise you will enable the Azure AD Premium Trial, enable the Azure AD Cloud App Discovery feature, take an inventory and explore the Cloud App Discovery reports.

Enable Azure AD Premium Trial

In this task you will enable the Azure AD Premium functionality in a trial state, and assign an initial Azure AD Premium license to your Global Admin account.

1. Open the default directory quick start page, if it isn't already open.
2. In the Get Azure AD Premium section, click **Try it now**.
3. Click **TRY AZURE ACTIVE DIRECTORY PREMIUM NOW**.
4. Review the Azure AD Premium trial terms, then click **Complete**.
5. Click on the link to refresh the status of the Azure AD Premium license until the license appears in the portal.
6. Click **Assign**.
7. Choose your current logged on user and Test User, then click **Complete**.

Enable Azure AD Cloud App Discovery

In this task you will enable the Azure Cloud App Discovery feature for your subscription.

1. Open the Azure Preview Portal and log on with your Azure administration account.
 - ★ If you were logged on to the Preview Portal while you activated Azure AD Premium, then you will need to log out of the Preview Portal and log back on. Until you do that, Azure will not recognize that you have an Azure AD Premium license.
2. Click **New**, then click **Security + Identity**.
3. In the Security + Identity blade, click **Marketplace**.



4. Click **Azure AD Cloud App Discovery**.
5. On the Azure AD Cloud App Discovery blade, click **Create**.
6. On the Cloud App Discovery blade, click **Create**.

Configure Cloud App Discovery & Generate Data


In this task you will configure the Cloud App Discovery to search for all known (by Azure) SaaS Cloud Apps. You will then download, install, and test the Cloud App Discovery agent.

1. Once the Cloud App Discover object is created, click **Settings**.
2. On the Settings blade, click **Manage Agent**.
3. On the Manage Agent blade, click **Please select a consent option**.
4. On the User Consent blade, put a check in the box next to **No notification or consent required**.
5. Click **Update**.
6. On the Settings blade, click **Data Collection**.
7. Set the Collection options to **All Apps**.
8. Click **Save**, then close the Data Collection blade.
9. On the Manage Agent blade, click **Download**.
10. When it finishes downloading, click **Open**.
11. Copy and paste the two files in the directory to C:\. If prompted for permission, click **Continue**.
12. Double-click **EndpointAgentSetup.exe**.

13. In the Cloud App Discovery-Endpoint Agent setup, click **Install**.
14. Click **Yes** to allow changes to be made.
15. When the installation is complete, click **Close**.

Generate Cloud App Activity

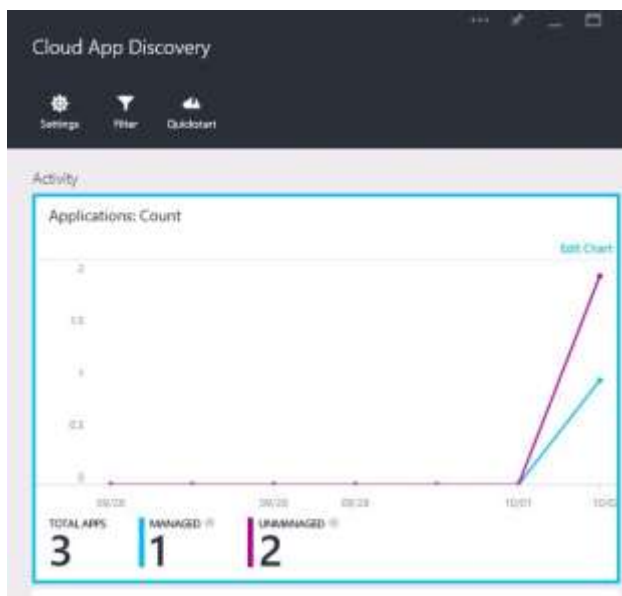
In this task you will generate some traffic to various cloud services to generate traffic for the Cloud App Discovery service to report on.

1. Click **Start**, then click **Github**. (You can access any other cloud services you are subscribed to if you so choose.)
2. If you have a Github account, log on using that account. Leave Github running.
3. Use the Start menu again to open **Groove Music**.
4. Leave these applications running.
 It may take up to 15 minutes for the data to appear in the Azure Preview Portal.
5. If you are concerned that data is not appearing in the Azure Preview Portal, confirm that the Microsoft Cloud App Discovery Endpoint Agent service is running on the computer.

Explore the Cloud App Discovery report

In this task you will view the Cloud App Discovery reports, and register an app for management with Azure AD.


1. Once the data starts being passed to Azure, the Cloud App Discovery charts will start to appear similar to below.



2. In the Activity chart, click **Edit Chart**.

3. In the Edit Chart blade, you will find a drop down list that will allow you to view the activity in one of three ways, by application count, web requests or volume. Choose a view other than "Count" and click **Update**.
4. You'll notice that the data is still categorized by managed and unmanaged, but the summary values reflect the data being displayed.
5. Click on the main area of the chart itself. This will open a table with more detail about the underlying data. You'll note that Windows Azure itself is reporting as an app.

APP	CATEGORY	STATUS	USERS	WEB RE...	DATA VOLUME	FILES UP...	FILES D...	LAST ACCESSED (UTC)
 Windows Azure	Developer Services	Managed	1	38	2.4 MB	0	0	10/02/15
 GitHub	Developer Services	Unmanaged	1	15	42.3 KB	0	0	10/02/15
 GlobalSign	Security	Unmanaged	1	1	2.3 KB	0	0	10/02/15

6. You should also notice that every app has a status of either Managed or Unmanaged.
7. Click on the listing for one of the unmanaged apps.
8. This opens a more detailed set of reports for that app, but may also suggest that you manage the app with Azure AD. Click on **Manage <xxx> with Azure AD** (<xxx> is the name of the app you chose).
9. If it is a supported app, the Azure Portal opens directly to the homepage of your Azure AD service, specifically to the page to add SaaS applications.
 If you choose to manage this service you would configure it from [here](#).
10. Close the Azure Portal and Azure Preview Portal