

# Understanding Microsoft Cloud Identities

Robert Crane

<http://about.me/ciaops>



# Agenda

- Identity options
- What is Azure AD?
- Enabling Azure AD using Office 365
- Configuring Azure AD Single Sign On Portal
- Configuring Azure AD Branding
- Configuring Azure AD Cloud User Password Reset Portal
- Conclusions

Identity options

# Identity Options Comparison

## 1. MS Online Identities

### Appropriate for

- Smaller orgs without AD on-premise

### Pros

- No servers required on-premise

### Cons

- No SSO
- No 2FA
- 2 sets of credentials to manage with differing password policies
- IDs mastered in the cloud

## 2. MS Online Identities + Azure AD Connect

### Appropriate for

- Medium/Large orgs with AD on-premise

### Pros

- Users and groups mastered on-premise
- Enables co-existence scenarios

### Cons

- No SSO
- No 2FA
- 2 sets of credentials to manage with differing password policies
- Server deployment required

## 3. Federated IDs + Azure AD Connect

### Appropriate for

- Larger enterprise orgs with AD on-premise

### Pros

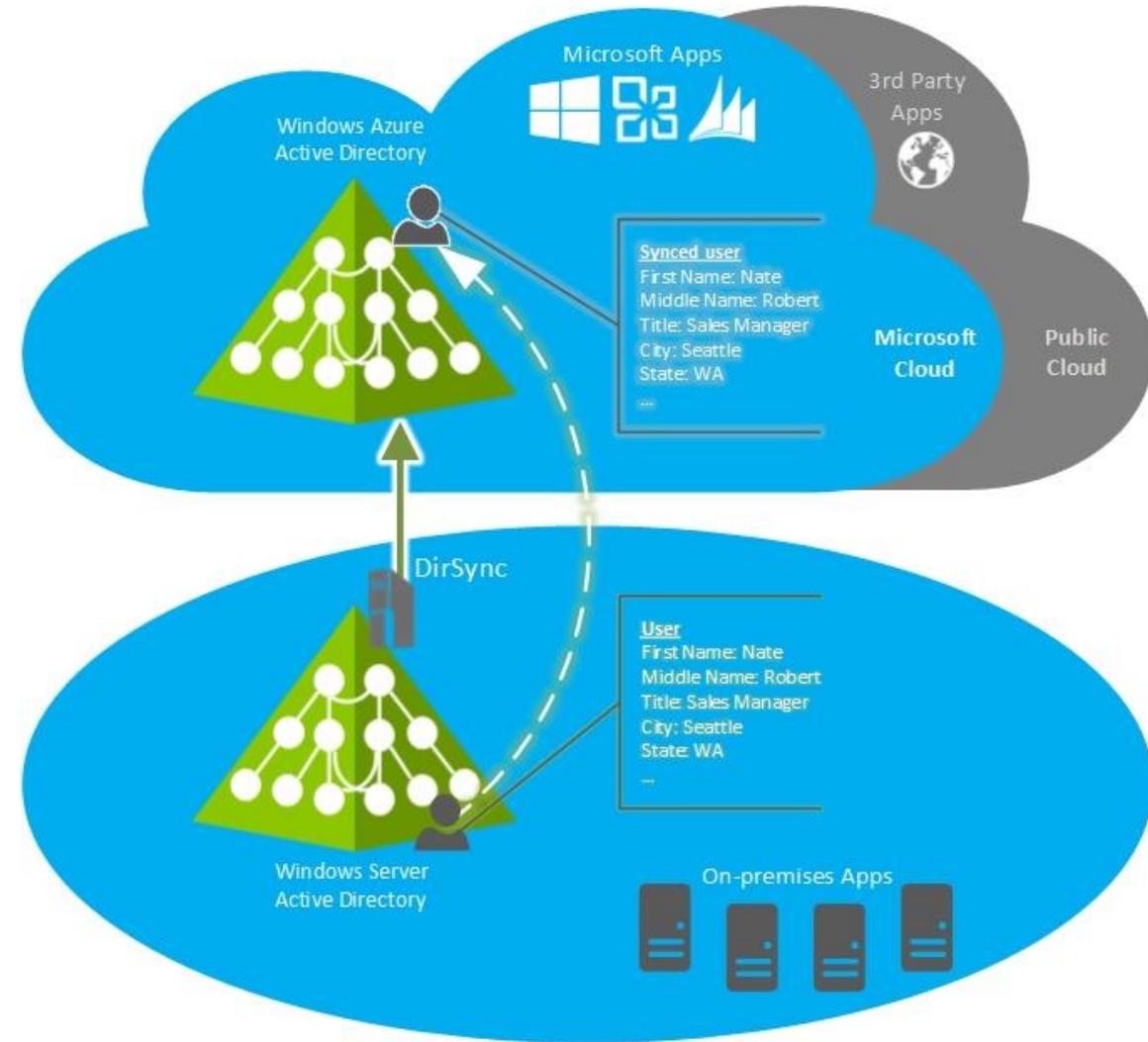
- SSO with corporate cred
- IDs mastered on-premise
- Password policy controlled on-premise
- 2FA solutions possible
- Enables co-existence scenarios

### Cons

- High availability server deployments required

# Directory Sync

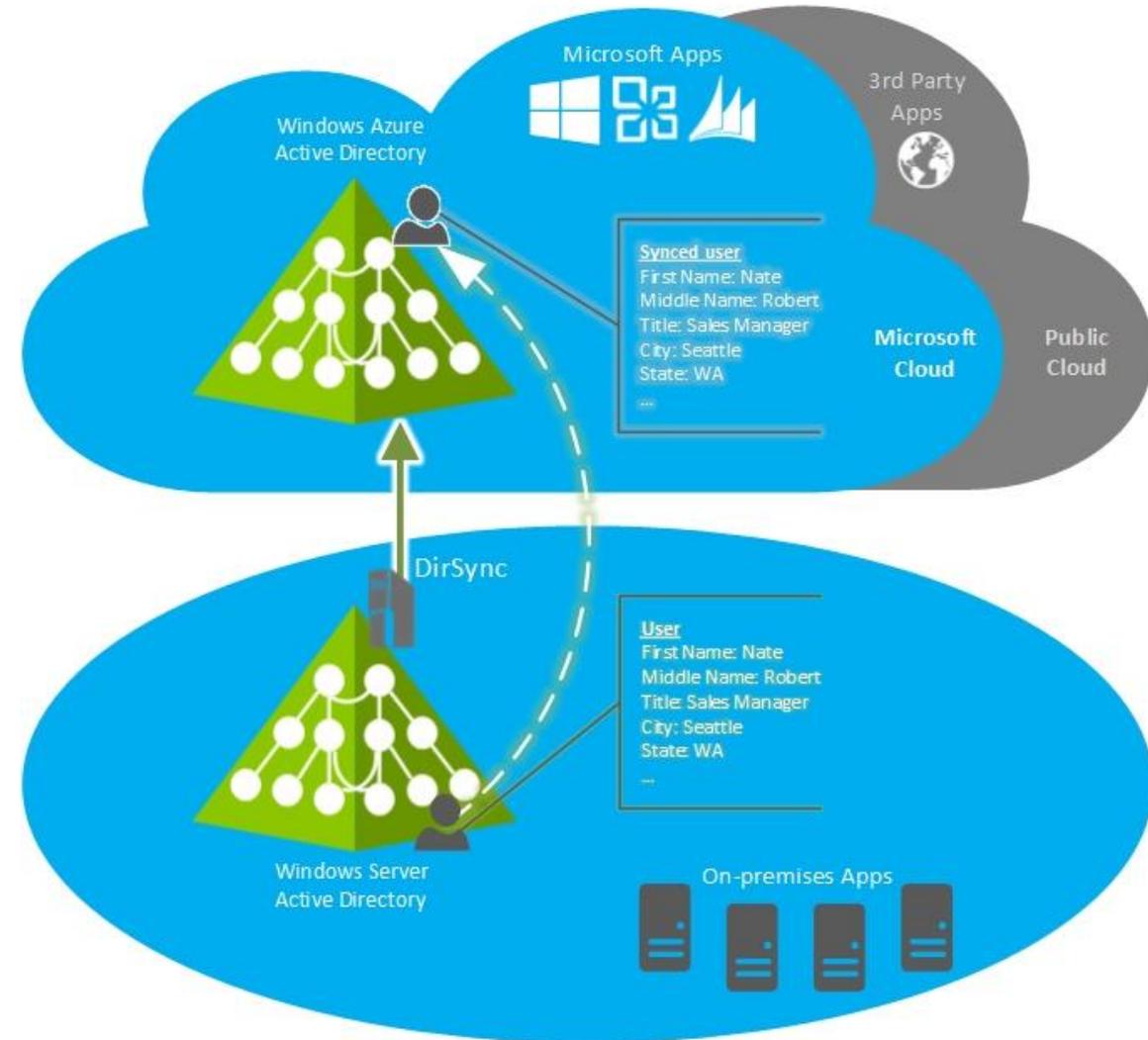
- Synchronizes users, groups, and contacts to Windows Azure AD.
- Users will have a **different password** in Windows Azure AD than they have for the on-premises AD.



**DEPRECATED**

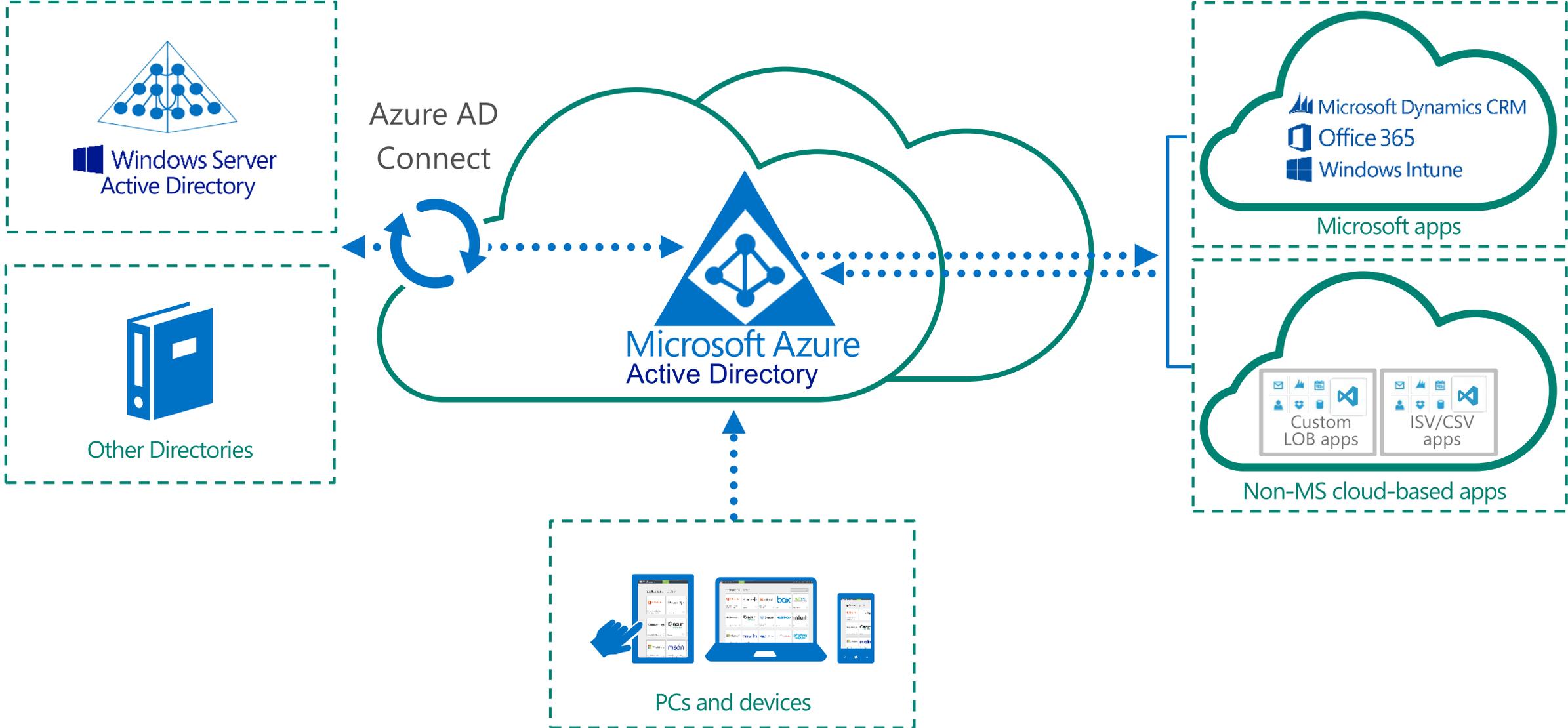
# Azure AD sync tool

- Formerly known as **Dirsync**, this tool has been updated to allow for the synchronization of local Active Directory passwords to Azure Active Directory.
- Also synchronizes users, groups and contacts.
- This new feature will allow for same user sign in with Microsoft cloud services such as Office 365 powered by Azure Active Directory since the username and the password from local AD will be synced up to Azure AD.



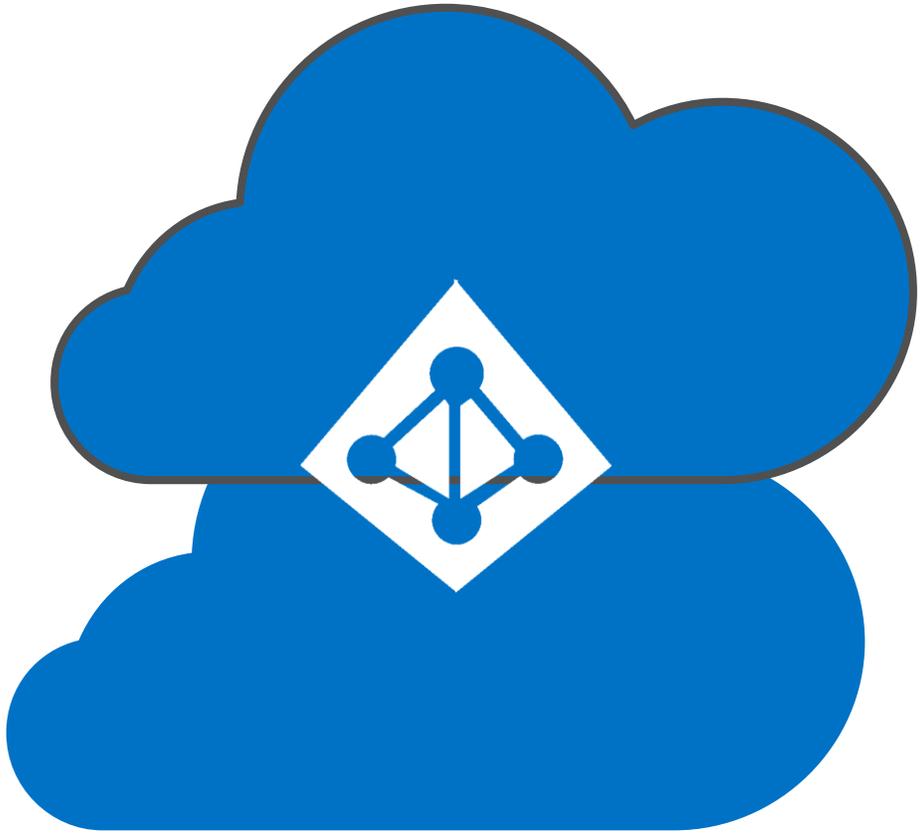
**DEPRECATED**

# Azure AD as the control point



What is Azure AD?

# What is Azure Active Directory?



A comprehensive identity and access management cloud solution.

It combines directory services, advanced identity governance, application access management and a rich standards-based platform for developers.

Versions:

- Free
- Basic
- Premium

# Azure Active Directory versions



## Versions:

- Free
  - Manage user accounts, synchronise with on-premises directories, get single sign on across Azure, Office 365, and thousands of popular SaaS applications.
- Basic
  - Get all the capabilities that Azure Active Directory Free has to offer, plus group-based access management, self-service password reset for cloud applications, Azure Active Directory application proxy (to publish on-premises web applications using Azure Active Directory), customizable environment for launching enterprise and consumer cloud applications, and an enterprise-level SLA of 99.9 percent uptime.
- Premium
  - Get all of the capabilities that the Azure Active Directory Free and Basic editions have to offer, plus additional feature-rich enterprise-level identity management capabilities such as branding, group based application access, multi factor authentication, Microsoft Identity Manager (MIM)

# Azure Active Directory editions feature comparison + Office 365 IAM features

		Azure Active Directory Free	Azure Active Directory Basic	Azure Active Directory Premium	Office 365 IAM features
Common Features	Directory as a Service	500,000 Object Limit	No Object Limit	No Object Limit	No Object limit for Office 365 user accounts
	User/Group Management (add/update/delete)	Yes	Yes	Yes	Yes
	SSO to pre-integrated SAAS Applications /Custom Apps	10 apps per user	10 apps per user	No Limit	10 apps per user
	User-Based access management/provisioning	Yes	Yes	Yes	Yes
	Self-Service Password Change for cloud users	Yes	Yes	Yes	Yes
	Identity Synchronization Tool (Windows Server Active Directory integration, Multi Forest)	Yes	Yes	Yes	Yes
	Security Reports	3 Basic Reports	3 Basic Reports	Advanced Security Reports	3 Basic Reports
	Cloud App Discovery*	Yes(Basic)	Yes(Basic)	Yes(Advanced)**	Yes(Basic)
Premium + Basic Features	Group-based access management/provisioning		Yes	Yes	
	Self-Service Password Reset for cloud users		Yes	Yes	
	Company Branding (Logon Pages/Access Panel customization)		Yes	Yes	
	SLA		Yes	Yes	Yes
Premium Features	Identity Synchronization Tool advanced write-back capabilities * (FY15 Roadmap)			Yes	
	Self-Service Group Management			Yes	
	Self-Service Password Reset/Change with on-premises write-back			Yes	
	Advanced Usage Reporting			Yes	
	Multi-Factor Authentication (Cloud and On-premises (MFA Server))			Yes	Limited Cloud only features for accessing Office 365
	Azure Active Directory Application proxy*			Yes	
	MIM CAL + MIM Server			Yes	
	Administrative Delegation* (FY15 Roadmap)			Yes	

\*Features in Preview (Sept 2014) or in the roadmap

\*\* Advanced functionality on Cloud App Discovery is in the roadmap for FY15 H2

10 Apps per user : Every user can have a different set of Apps, up to ten. MS Online apps (e.g. O365) are counted among these 10.

# Enabling Azure access in Office 365

# Access to free Azure AD via Office 365

ADMIN

- Exchange
- Lync
- SharePoint
- Azure AD 

## Sign up

Access to Azure Active Directory

[Learn more](#)



## Windows Azure

rcrane@ciaops365.com.au

1 About you

FIRST NAME	LAST NAME	COUNTRY/REGION
<input type="text" value="Robert"/>	<input type="text" value="Crane"/>	<input type="text" value="Australia"/>
CONTACT EMAIL	COMPANY NAME	WORK PHONE
<input type="text"/>	<input type="text" value="- Optional -"/>	<input type="text" value="499 123 456"/>

2 Mobile verification

Send text message  Call me

## Windows Azure

rcrane@ciaops365.com.au SIGN OUT

HOME PRICING DOCUMENTATION DOWNLOADS COMMUNITY SUPPORT ACCOUNT

subscriptions store profile preview features

### Portal

## Summary for Access to Azure Active Directory

OVERVIEW

**i** You can start using Azure services while we setup the billing for this subscription. [Click here to refresh.](#)

CURRENT BILLING PERIOD  
1/23/2015 - 2/22/2015

[Contact Microsoft Support](#)

ACCOUNT ADMINISTRATOR  
rcrane@ciaops365.com.au

SUBSCRIPTION ID  
14d079b2-a27e-47b2-943b-44b84be0bd8b

ORDER ID  
d725f4ec-6afb-4256-b0bd-8826a0b6a49

STATUS  
Pending

## Microsoft Azure

ALL ITEMS

ACTIVE DIRECTORY 1

SETTINGS

# all items

NAME
CIAOPS TEST

## Microsoft Azure

←

# ciaops test

USERS GROUPS APPLICATIONS



CIAOPS TEST

You

Azure AD Web Single Sign On  
Portal

# Add an application

Microsoft Azure

lewis.collins@ciaops365.com | CIAOPS |

applications

profile



Office 365 Exchange Online ...



Office 365 SharePoint Online ...



Citrix GoToMeeting ...



Dropbox for Business ...



Microsoft Account (Windows Live) ...



Microsoft OneDrive ...

Showing 7 of 7

<http://myapps.microsoft.com>

# Add an application

Microsoft Azure | admin@ciaops365.com

ciaops

USERS | GROUPS | **APPLICATIONS** | DOMAINS | DIRECTORY INTEGRATION | CONFIGURE | REPORTS | LICENSES

NAME	PUBLISHER	TYPE	APP URL
Citrix GoToMeeting →	Citrix	Web application	http://www.gotomeeting.com/
Dropbox for Business	Dropbox	Web application	http://www.dropbox.com/
Microsoft Account (Windows Live)	Microsoft Corporation	Web application	http://www.live.com/
Microsoft App Discovery	Microsoft Corporation	Web application	http://appdiscovery.azure.com/
Microsoft OneDrive	Microsoft Corporation	Web application	http://www.onedrive.com/
Office 365 Exchange Online	Microsoft Corporation	Web application	http://office.microsoft.com/outlook/
Office 365 SharePoint Online	Microsoft Corporation	Web application	http://office.microsoft.com/sharepoint/

+ NEW    ADD    DELETE    ?

# Add an application

Microsoft Azure | admin@ciaops365.com

ciaops

USERS | GROUPS | APPLICATIONS | DOMAINS | DIRECTORY INTEGRATION | CONFIGURE | REPORTS | LICENSES

NAME	PUBLISHER	TYPE	APP URL
Citrix GoToMeeting	Citrix	Web application	http://www.gotomeeting.com/
Dropbox for Business	Dropbox	Web application	http://www.dropbox.com/
Microsoft Account (Windows Live)	Microsoft Corporation	Web application	http://www.live.com/
Microsoft App Discovery	Microsoft Corporation	Web application	http://appdiscovery.azure.com/
Microsoft OneDrive	Microsoft Corporation	Web application	http://www.onedrive.com/
Office 365 Exchange Online	Microsoft Corporation	Web application	http://office.microsoft.com/outlook/
Office 365 SharePoint Online	Microsoft Corporation	Web application	http://office.microsoft.com/sharepoint/

+ NEW    ≡+ ADD    🗑️ DELETE    ?



# Add an application

What do you want to do?

➔ Add an application my organization is developing

➔ Add an application from the gallery



# Add an application

APPLICATION GALLERY

Add an application for my organization to use

evernote



x



FEATURED APPLICATIONS (14)

CUSTOM

[ALL \(2455\)](#)

BUSINESS MANAGEMENT (88)

COLLABORATION (278)

CONSTRUCTION (3)

CONTENT MANAGEMENT (84)

CRM (108)

DATA SERVICES (108)

DEVELOPER SERVICES (85)

E-COMMERCE (68)

EDUCATION (69)

ERP (37)

FINANCE (218)

HEALTH (46)

HUMAN RESOURCES (183)

IT INFRASTRUCTURE (116)

MAIL (20)

MARKETING (170)



Evernote



NAME Evernote

PUBLISHER Evernote Corporation

APPLICATION URL <http://www.evernote.com/>

Use Windows Azure AD to enable user access to Evernote.

Requires an existing Evernote subscription.



# Add an application

 DASHBOARD [USERS](#)



Your app has been added!

Enable your app to integrate with Windows Azure AD

Skip Quick Start the next time I visit

## 1 Enable single sign-on with Windows Azure AD

Configure single sign-on access to this application.

Configure single sign-on



Single sign-on is enabled for existing application accounts

## 2 Assign users to Evernote

Specify which user accounts in Windows Azure AD can access this application.

Assign users



# Add an application

evernote

 DASHBOARD **USERS**

DISPLAY NAME	USER NAME	JOB TITLE	DEPARTMENT	ACCESS	METHOD	
Alexandra Zammit	thaz@ciaops365.com			No	Unassigned	
Barry Jones	barry.jones@kumoallianc...			No	Unassigned	
Chris Green	chris@ciaops365e1.onmi...	IT Manager	Information Technology	No	Unassigned	
CIAOPS Presenter	presenter@ciaops365e1....			No	Unassigned	
Demo	SMO-Demo@kumoallian...			No	Unassigned	
director@ciaops.com	director@ciaops.com			No	Unassigned	
Gordon Jackson	gordon.jackson@kumoal...			No	Unassigned	
James Hill	james.hill@ciaops365e1....			No	Unassigned	
Kevin Fyfe	thkf@ciaops365.com			No	Unassigned	
Lewis Collins	lewis.collins@ciaops365...			No	Unassigned	
Martin Shaw	martin.shaw@ciaops365e...			No	Unassigned	
Pepper Potts	pepper.potts@ciaops365...			No	Unassigned	



ASSIGN  EDIT ACCOUNT  REMOVE 

# Add an application

## Assign Users

This action will allow the selected user to authenticate to the Evernote application from within the Access Panel. Users can enter and update their Evernote credentials using the Access Panel at any time.

I want to enter Evernote credentials on behalf of the user

User Name

Password



Kevin Fyfe	thkf@ciaops365.com	No	Unassigned
Lewis Collins	lewis.collins@ciaops365....	Yes	Direct
Martin Shaw	martin.shaw@ciaops365e...	No	Unassigned

✓ Successfully enabled access for the selected users.

OK



# Add an application



Sign in with your work or school account

Keep me signed in

Sign in

[Can't access your account?](#)

<http://myapps.microsoft.com>

# Add an application

Microsoft Azure

lewis.collins@ciaops365.com | CIAOPS |

applications

profile



Office 365 Exchange Online ...



Office 365 SharePoint Online ...



Citrix GoToMeeting ...



Dropbox for Business ...



Evernote ...



Microsoft Account (Windows Live) ...



Microsoft OneDrive ...

Showing 7 of 7

<http://myapps.microsoft.com>

# Add an application

The screenshot shows the Evernote web interface in a browser window. The address bar displays the URL <https://www.evernote.com/Home.action#st=p&n=2b37e5ae-4a6e-40e6-97af-cd3002171>. The browser tabs include "Access Panel Applications" and "Evernote Web". The Evernote header features a green bar with "Get Premium for Free" on the left and "Go Premium" and the user name "Robert Crane" on the right. Below the header, the "EVERNOTE" logo is on the left, followed by a search bar and a "+ New Note" button. The main interface is divided into three sections: a left sidebar, a central list of notes, and a right-hand editor.

**Left Sidebar:**

- Shortcuts:** Drag notes, notebooks or tags here for quick access.
- Notebooks:**
  - All Notes (875)
  - ifttt linkedin (648)
  - ifttt twitter directorcia (196)
  - Robert Crane (31)
  - Trash (193)
- Tags:**
  - ifttt (844)
  - linkedin (648)
  - office365 (1)
  - sharepoint
  - twitter (196)

**Central List of Notes:**

- All Notes**
- New CIAOPS Blog post: Introduction to Lookup Colum...**  
Yesterday <http://ift.tt/1LGsGGc> via LinkedIn
- New CIAOPS Blog post: Need to Know podcast–Episod...**  
2 days ago <http://ift.tt/1Ez0IQ5> via LinkedIn
- New CIAOPS Blog post: OneDrive for Business now av...**  
6 days ago <http://ift.tt/1wC2yBp> via LinkedIn
- New CIAOPS Blog post: Connect SharePoint to MS Acc...**  
6 days ago <http://ift.tt/1zZxrHf> via LinkedIn
- New CIAOPS Blog post: Globalization of SMB–Webinar ...**  
Last week <http://ift.tt/15LTXFR> via LinkedIn
- New CIAOPS Blog post: Need to Know podcast–Episod...**  
Last week <http://ift.tt/1wwE1xA> via LinkedIn
- New CIAOPS Blog post: Australian Office 365 tenant rel...**  
Last week <http://ift.tt/1Bjuoaw> via LinkedIn

**Right-Hand Editor:**

ifttt linkedin | iftt | linkedin | + | SHARE | INFO | TOOLS | X

Created: Feb 03, 2015 | Modified: Feb 03, 2015

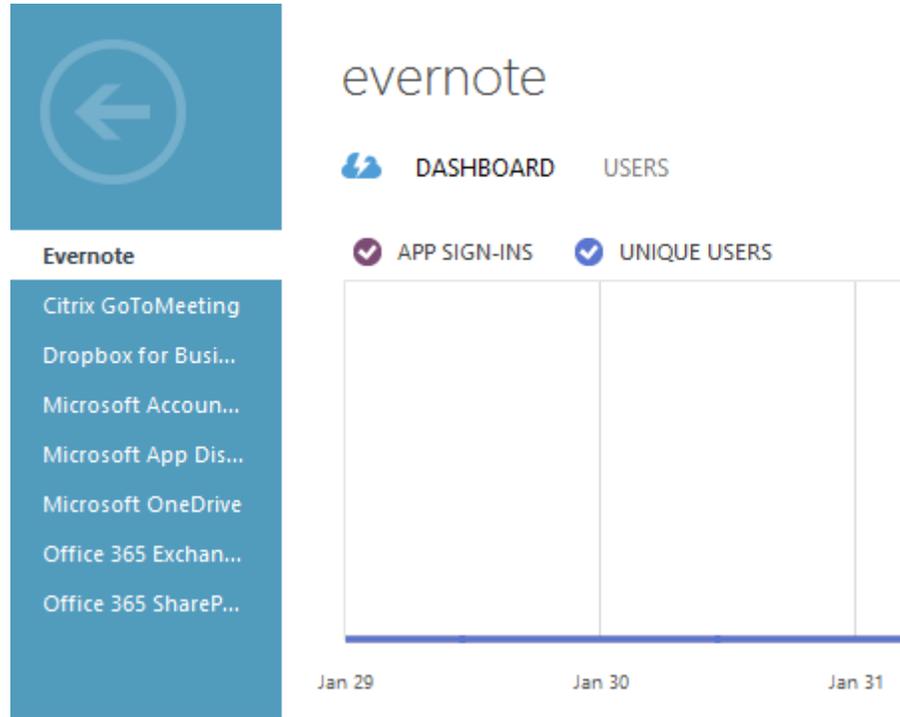
New CIAOPS Blog post: Introduction to Lookup Columns in SharePoint - <http://ift.tt/1LGsGGc>

<http://ift.tt/1LGsGGc>

via LinkedIn

View Options ▲ | 1-8 of 879 notes

# Monitor an application



# Preintegrated SaaS apps in the application gallery



Microsoft Bing Ads  
By Microsoft Corporation



Microsoft Developer Network (MSDN)  
By Microsoft Corporation



Microsoft OneDrive  
By Microsoft Corporation



Office 365 Exchange Online  
By Microsoft Corporation



Dynamics CRM  
By Microsoft Corporation



Microsoft Account (Windows Live)  
By Microsoft Corporation



Skype  
By Microsoft Corporation



Yammer  
By Microsoft Corporation



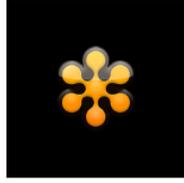
ServiceNow  
By ServiceNow



Box  
By Box



Salesforce  
By Salesforce.com



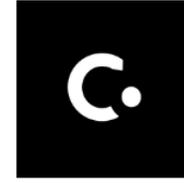
Citrix GoToMeeting  
By Citrix



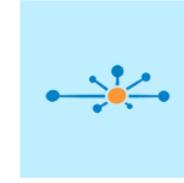
NASDAQ Online  
By The NASDAQ OMX Group, Inc.



SAP BusinessObjects BI OnDemand  
By SAP



Concur  
By Concur



Concur TripIt  
By TripIt.



DocuSign  
By DocuSign Inc.



Red Hat OpenShift  
By Red Hat, Inc.



Egnyte  
By Egnyte, Inc.



Evernote  
By Evernote Corporation



MarcomCentral  
By PTI Marketing Technologies



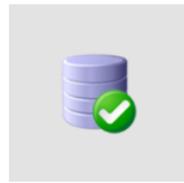
McKesson InterQual Online Learning  
By McKesson



Oracle SRM  
By Oracle Corporation



Oracle Taleo  
By Oracle Corporation



ClearDB  
By SuccessBricks, Inc.



SuccessFactors  
By SuccessFactors, Inc. A SAP Company



American Express OPEN Small Business  
By American Express Company.



IBM Kenexa  
By IBM Corp



IBM SmartCloud for Social Business  
By IBM Corp



Workday  
By Workday



Blogger  
By Google



Google  
By Google



Google App Engine  
By Google



DreamBox Learning  
By DreamBox Learning, Inc.



Dropbox for Business  
By Dropbox



Facebook  
By Facebook



AT&T Business Direct  
By AT&T



Twitter  
By Twitter



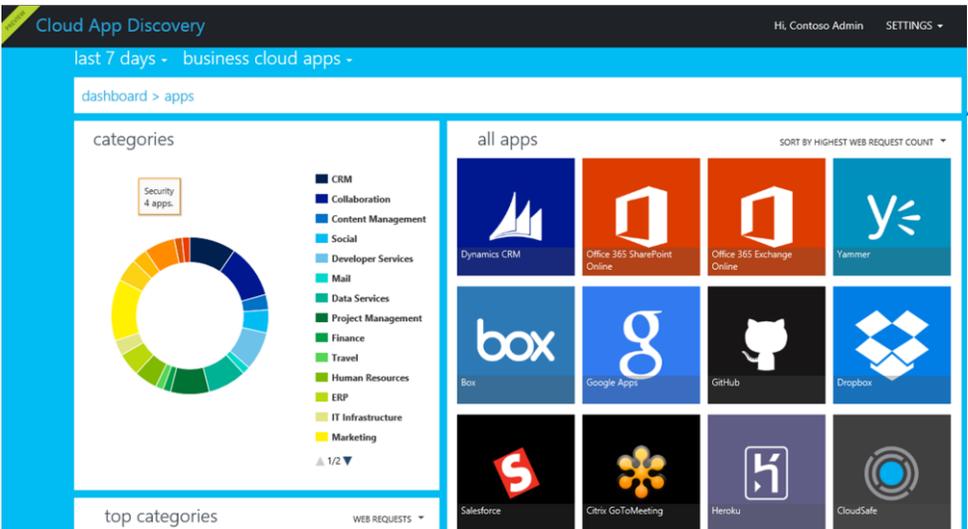
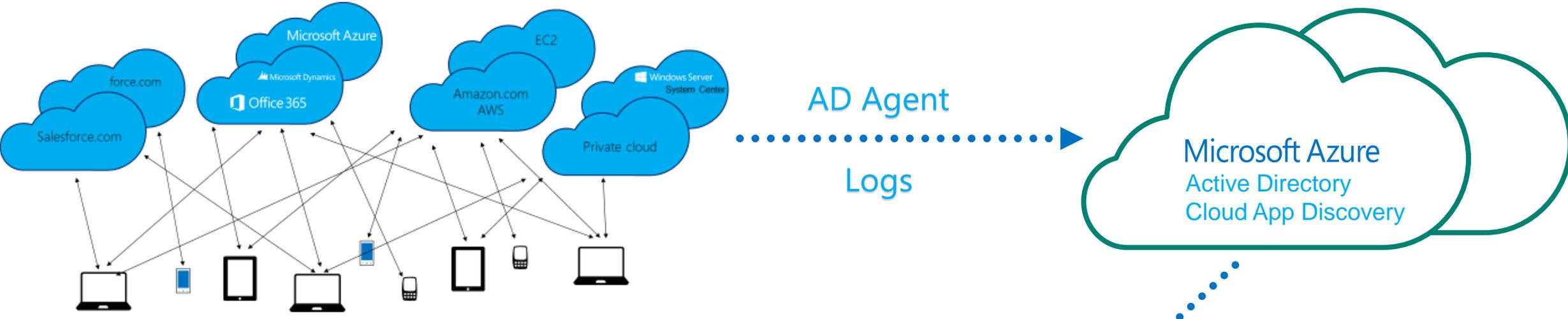
Amazon Web Services (AWS)  
By Amazon



Netflix  
By Netflix, Inc.

# Cloud app discovery

A world of devices and SaaS Applications



# Azure AD Branding

# Branding

The screenshot shows the Microsoft Azure portal interface for a directory named 'ciaops (test)'. The top navigation bar includes 'Microsoft Azure' and the user profile 'robert.crane@ciaops365.com.au'. The left-hand navigation pane shows a grid icon, a back arrow, and a gear icon labeled 'CIAOPS (Test)'. The main content area has a sub-menu with 'USERS', 'GROUPS', 'APPLICATIONS', 'DOMAINS', 'DIRECTORY INTEGRATION', 'CONFIGURE', 'REPORTS', and 'LICENSES'. A red arrow points to the 'CONFIGURE' menu item. Below this, the 'directory properties' section is visible, with a text input field for 'NAME' containing 'CIAOPS (Test)'. The 'SIGN IN AND ACCESS PANEL PAGE APPEARANCE' section contains a green button labeled 'Customize Branding', which is also highlighted by a red arrow. Below this, the 'user password reset policy' section has two toggle controls: 'USERS ENABLED FOR PASSWORD RESET' (set to 'YES') and 'RESTRICT ACCESS TO PASSWORD RESET' (set to 'NO'). The bottom of the page features a dark blue bar with a '+ NEW' button and a help icon.

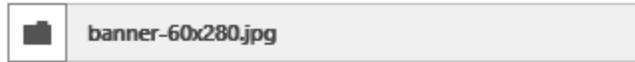
# Branding

## CUSTOMIZE DEFAULT BRANDING ✕

Manage how company logos, text, and colors should appear on your organization's Sign In and Access Panel pages. You can also apply unique branding settings for different languages.

[Learn more](#)

### BANNER LOGO (60 PIXELS BY 280 PIXELS) ?



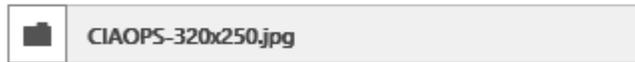
### TILE LOGO (200 PIXELS BY 200 PIXELS) ?



### SIGN IN PAGE TEXT ?

A text input field with a light gray border and a vertical scrollbar on the right side. The text "CIAOPS Sign in" is entered into the field.

### SIGN IN PAGE ILLUSTRATION ?



### SIGN IN PAGE BACKGROUND COLOR ?

A text input field with a light gray border and a small "✕" icon on the right side. The text "#FFFFFF" is entered into the field.

# Branding



Sign in with your work or school account

Keep me signed in

Sign in

Cancel

[Can't access your account?](#)

Azure AD Cloud User Password  
Reset Portal

# Password reset portal

ciaops test

 [USERS](#) [GROUPS](#) [APPLICATIONS](#) [DOMAINS](#) [DIRECTORY INTEGRATION](#) [CONFIGURE](#) [REPORTS](#) [LICENSES](#)

directory properties

---

NAME

CIAOPS TEST

SIGN IN AND ACCESS PANEL PAGE  
APPEARANCE

[Customize Branding](#)

user password reset policy

---

USERS ENABLED FOR PASSWORD RESET

YES

NO

# Password reset portal

user password reset policy

---

USERS ENABLED FOR PASSWORD RESET

YES  NO



RESTRICT ACCESS TO PASSWORD RESET

YES  NO PREVIEW

Before users can reset their passwords, they must first have at least one authentication method defined. [Edit users in 'CIAOPS TEST' now.](#)

AUTHENTICATION METHODS AVAILABLE TO USERS

- Office Phone
- Mobile Phone
- Alternate Email Address
- Security Questions PREVIEW

NUMBER OF AUTHENTICATION METHODS REQUIRED

1

NUMBER OF QUESTIONS REQUIRED TO REGISTER

5

# My apps portal



Sign in with your work or school account

Keep me signed in

Sign in

[Can't access your account?](#)

<http://myapps.microsoft.com>

# My apps portal

Your administrator has required you to verify your contact info. You can use this to reset your password if you ever lose access to your account.

[verify now](#)

# My Apps portal

don't lose access to your account!

To make sure you can reset your password, we need to collect some info so we can verify who you are. We won't use this to spam you - just to keep your account more secure.

-  Authentication Phone is not configured. [Set it up now](#)
-  Authentication Email is not configured. [Set it up now](#)
-  Security Questions are not configured. [Set them up now](#)

finish

cancel

# Password reset



Sign in with your work or school account

Keep me signed in

[Can't access your account?](#)



# Password reset



## Reset your password

### User verification

To reset your password, begin by entering your user ID and the characters in the picture or audio below.

\* User ID:

 ✕

Example: user@contoso.onmicrosoft.com or user@contoso.com



Enter the characters in the picture or the words in the audio.

Next

Cancel

# Password reset



## Reset your password

**verification step 1** > choose a new password

---

Please choose the contact method we should use for verification:

- Email my alternate email
- Text my mobile phone
- Call my mobile phone
- Answer my security questions

You will receive an email containing a verification code at your alternate email address (di\*\*\*\*\*@hotmail.com).

Email

[Cancel](#)

# Password reset



## Reset your password

verification step 1 ✓ > **choose a new password**

---

\* Enter new password:

Password strength

\* Confirm new password:

Finish

Cancel

A strong password is required. Strong passwords are 8 to 16 characters and must combine uppercase and lowercase letters, numbers, and symbols. They cannot contain your username.

# Password reset



Reset your password

✓ Your password has been reset

# References

## **What is Azure Active Directory**

- <http://azure.microsoft.com/en-us/documentation/articles/active-directory-what-is/>

## **Azure Active Directory Editions**

- <https://msdn.microsoft.com/en-us/library/azure/dn532272.aspx>

## **Azure AD Editions**

- <https://azure.microsoft.com/en-us/documentation/articles/active-directory-editions/>

## **Azure AD features and capabilities**

- <http://www.microsoft.com/en-au/server-cloud/products/azure-active-directory/features.aspx>

## **MSDN Channel 9 Azure videos**

- <http://channel9.msdn.com/Series/Windows-Azure-Active-Directory>

## **Add company branding to your Sign In and Access Panel pages**

- <https://msdn.microsoft.com/en-us/library/azure/dn532270.aspx?f=255&MSPPError=-2147217396>

# QUESTIONS / FEEDBACK?



director@ciaops.com



@directorcia