All About Azure AD

Robert Crane

http://about.me/ciaops

# Agenda

- What is Azure?
- What is Single Sign on (SSO)?
- What is WAAD?
- Accessing your free WAAD using Office 365
- Configuring your Azure SSO portal
- Conclusions

What is Azure?

Your on demand datacenter

Cloud Computing

Packaged Software	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

You manage (Packaged Software: all)

Infrastructure: You manage Applications, Data, Runtime, Middleware, O/S; Managed by vendor Virtualization, Servers, Storage, Networking

Platform: You manage Applications, Data; Managed by vendor Runtime, Middleware, O/S, Virtualization, Servers, Storage, Networking

Software: Managed by vendor all

Platform Services

Security & Management
- Portal
- Active Directory
- Multi-Factor Authentication
- Automation
- Key Vault
- Store / Marketplace
- VM Image Gallery & VM Depot

Compute
- Cloud Services
- Service Fabric
- Batch
- Remote App

Web and Mobile
- Web Apps
- API Apps
- API Management
- Mobile Apps
- Logic Apps
- Notification Hubs

Developer Services
- Visual Studio
- Azure SDK
- Team Project
- Application Insights

Hybrid Operations
- Azure AD Connect Health
- AD Privileged Identity Management
- Backup
- Operational Insights
- Import/Export
- Site Recovery
- StorSimple

Integration
- Storage Queues
- Biztalk Services
- Hybrid Connections
- Service Bus

Analytics & IoT
- HDInsight
- Machine Learning
- Data Factory
- Event Hubs
- Stream Analytics
- Mobile Engagement

Data
- SQL Database
- SQL Data Warehouse
- Redis Cache
- Search
- DocumentDB
- Tables

Media & CDN
- Media Services
- Content Delivery Network (CDN)

Infrastructure Services

Compute
- Virtual Machines
- Containers

Storage
- BLOB Storage
- Azure Files
- Premium Storage

Networking
- Virtual Network
- Load Balancer
- DNS
- Express Route
- Traffic Manager
- VPN Gateway
- Application Gateway

Datacenter Infrastructure (24 Regions, 19 Online)

Common Questions

- Can Azure AD replace my on premises domain controller?

- Can I join PC's directly to Azure AD?

- Can Azure AD to manage mobile devices?

- Can Azure AD to manage local devices like printers?

- Can I use MFA?

- Can you protect documents with Azure AD?

Identity Options Comparison

1. MS Online IDs	2. MS Online IDs + DirSync	3. Federated IDs + DirSync
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	**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	**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

Online Identity

Cloud identity model
http://portal.office.com
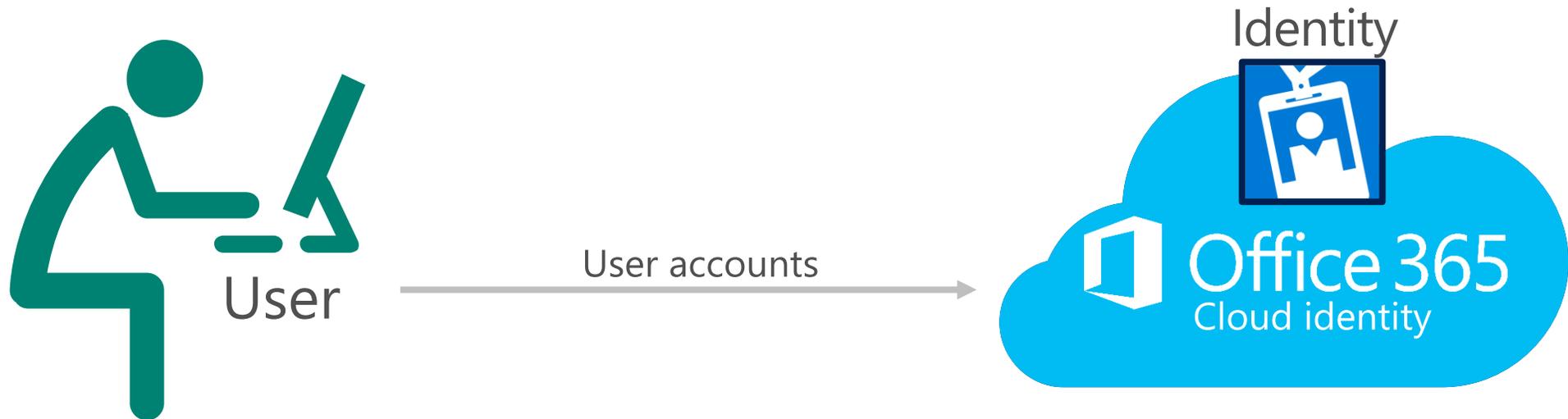
Office 365

Office 365 admin center

Search users, admin tasks an

- Active Users
- Deleted Users
- Partner Relationships

COMPANY PROFILE

IMPORT

CONTACTS

SHARED MAILBOXES

MEETING ROOMS

GROUPS

DOMAINS

PUBLIC WEBSITE

BILLING

EXTERNAL SHARING

MOBILE MANAGEMENT

SERVICE SETTINGS

REPORTS

SERVICE HEALTH

SUPPORT

DASHBOARD | ACTIVE USERS

CIAOPS (Test) (Edit)

Active Directory synchronization: Set up | Learn more
Change the password expiration policy for your users: Change now
Set Multi-factor authentication requirements: Set up | Learn more

Select a view: [All users ▾]

	Display name	User name ▲	Status
☐	TEST_TEST_SPOProvHeartbeat_E3_15...	admin@a830edad9050849NDA3148....	In cloud
☐	Gordon Jackson	gordon.jackson@ciaops365.com.au	In cloud
☐	Lewis Collins	lewis.collins@ciaops365.com.au	In cloud
☐	Martin Shaw	martin.shaw@ciaops365.com.au	In cloud
☐	Michael Smith	michael.smith@ciaops365.com.au	In cloud
☐	Robert Crane	robert.crane@ciaops365.com.au	In cloud
☐	user0TestUser	user0@a830edad9050849NDA3148....	In cloud

Select users to:
- **Edit user details**
- **Delete users**
- **Reset user password**

♥ Feedback

Lewis Collins

Details
Roles
Settings
Licenses
Email address
Mailbox permissions
More

Name

First name

Lewis

Last name

Collins

* Display name

Lewis Collins

* User name

lewis.collins @ ciaops365.com.au

Additional details ▲

Job title:

Department

Office

Office phone

Save   Cancel

Synchronised Identity

Office 365 Identity Models

Office 365 — Cloud identity

Office 365 — Synchronized identity

Office 365 — Federated identity

On-premises directory

On-premises directory

Zero on-premises servers

Directory sync with password sync

Federation | Directory sync

On-premises identity

On-premises identity
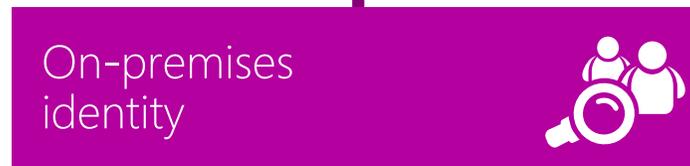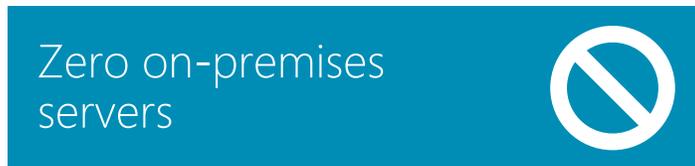
Between zero and three additional on-premises servers depending on the number of users
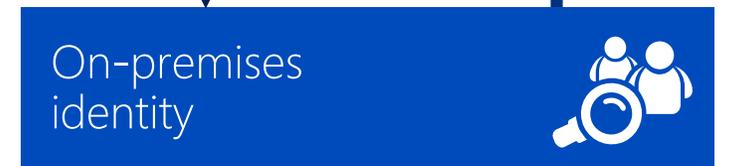
Between two and eight on-premises servers and networking configuration depending on the sign-in availability requirements

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.
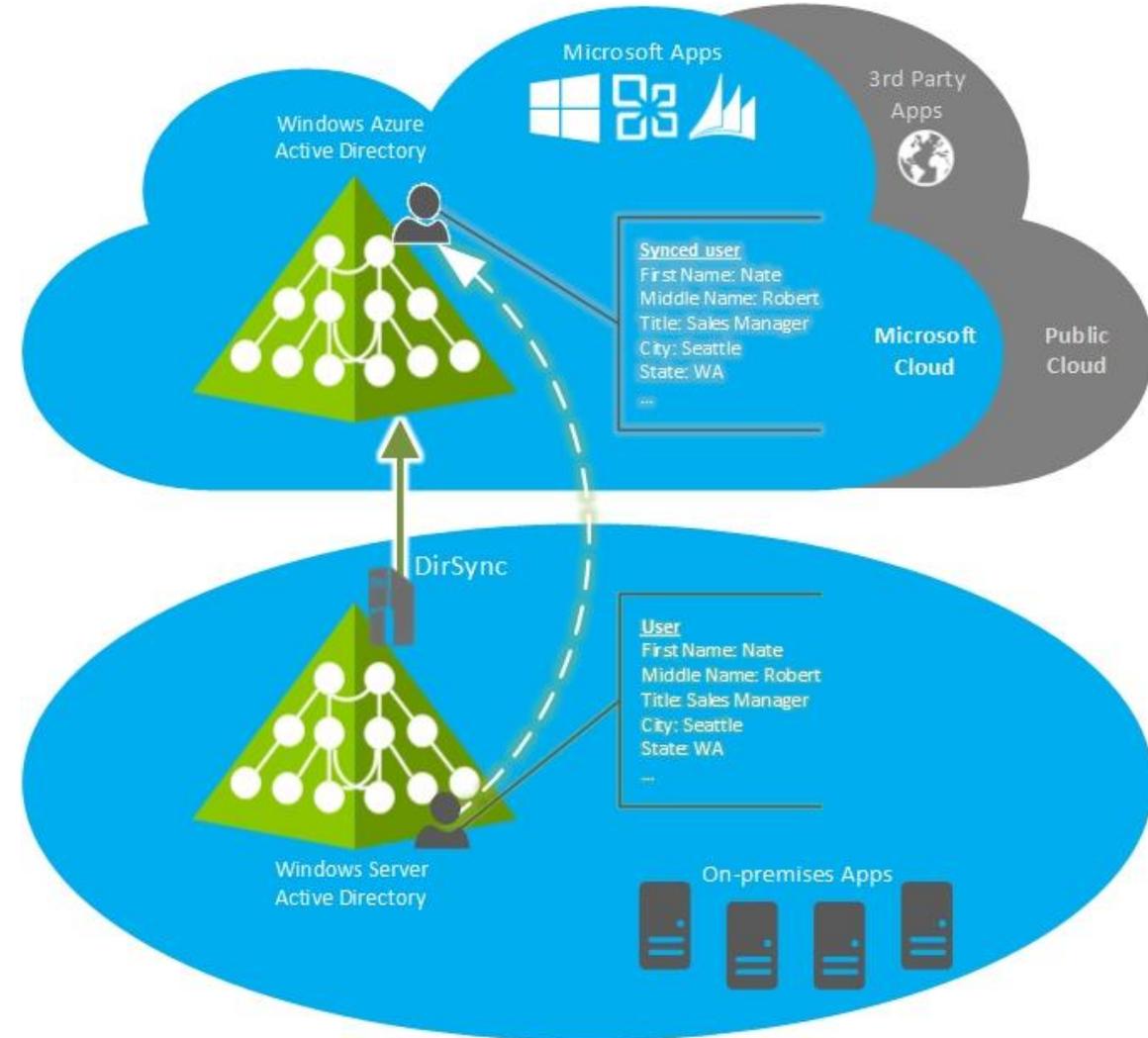
DEPRECATED

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.
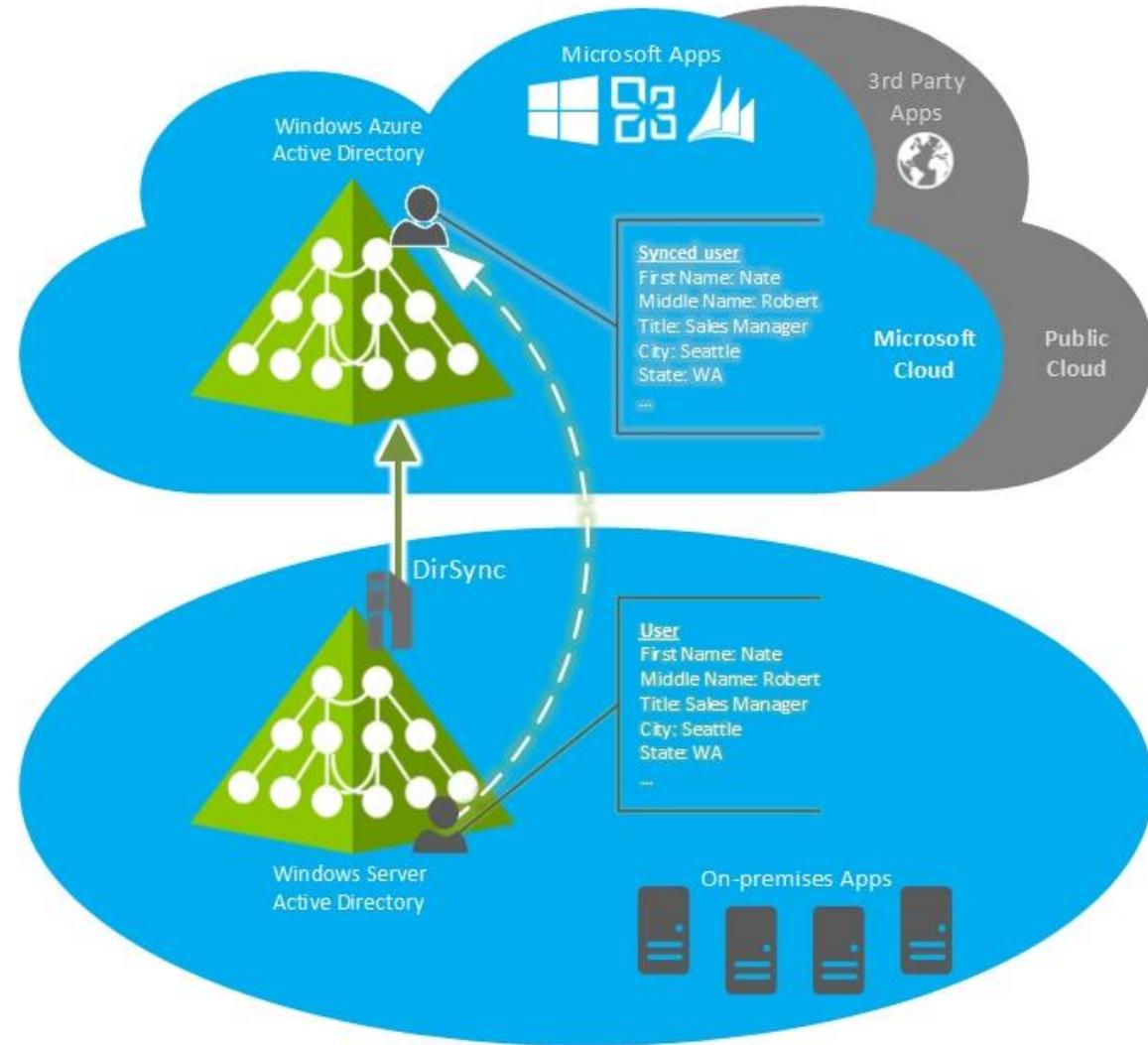
DEPRECATED

Synchronized Identity Model

Identity Copy

Office 365
Synchronized identity

Password hashes

User accounts

AAD Sync or Connect

On-premises directory

Identity

Sign-on

User
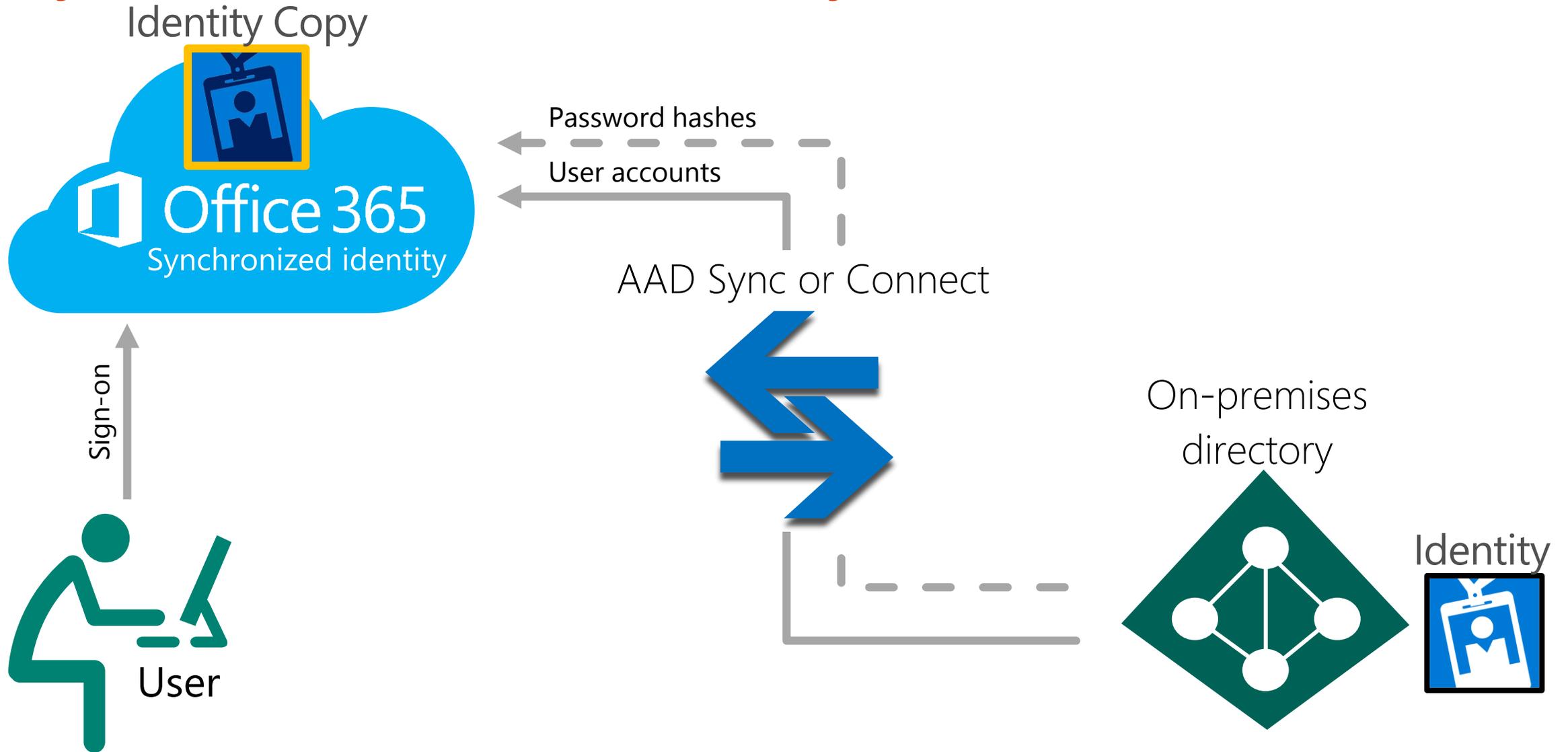
Federated Identity

Federated identity model
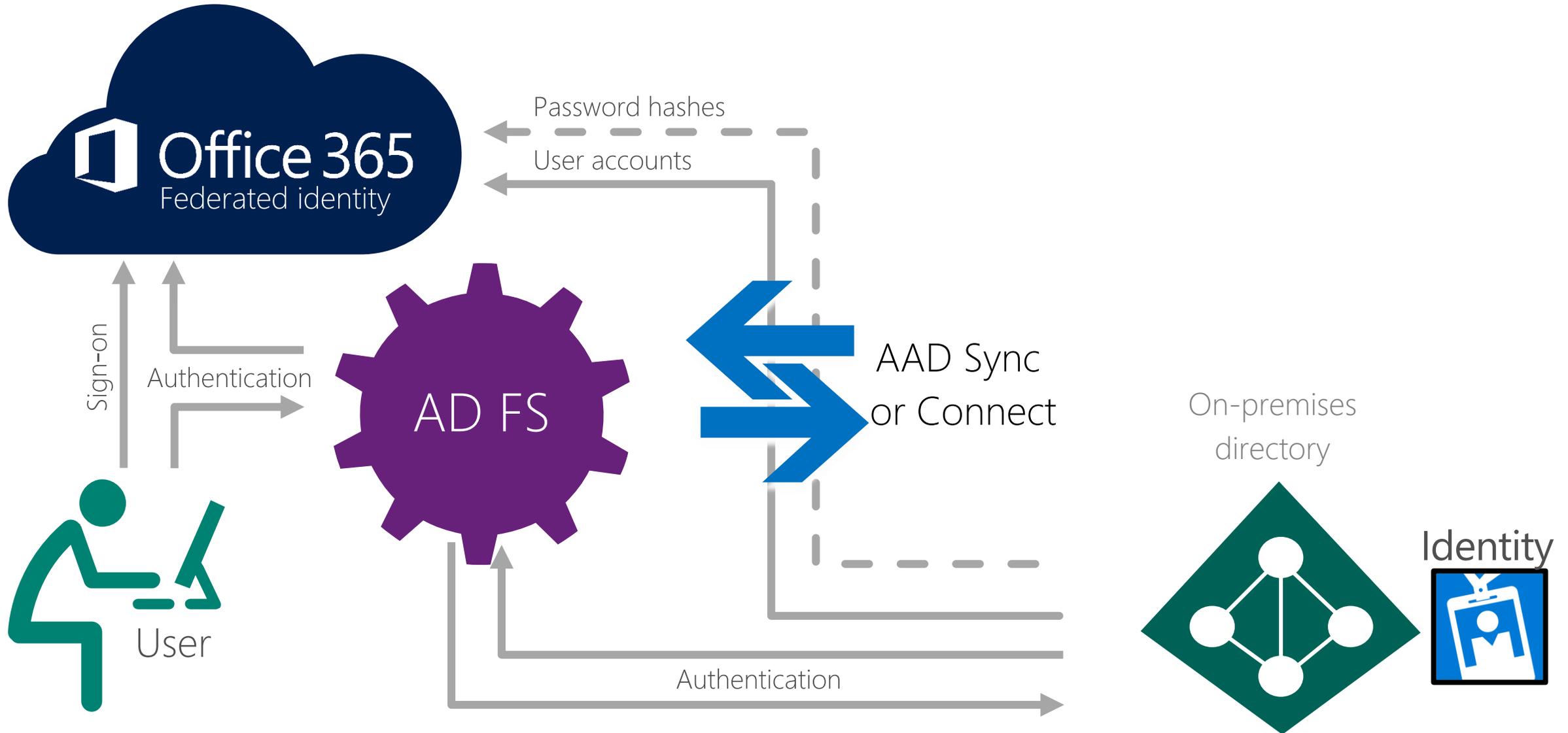
Password Sync Backup for Federated Sign-In

This new backup option for Office 365 customers using federated sign-in provides the option to manually switch your domain in a short amount of time during outages such as on- premises power loss, internet connection interruption and any other on-premises outage.

Office 365
Federated identity

Backup Password Hash Sync

User accounts

AAD Sync

ADFS

On-premises directory
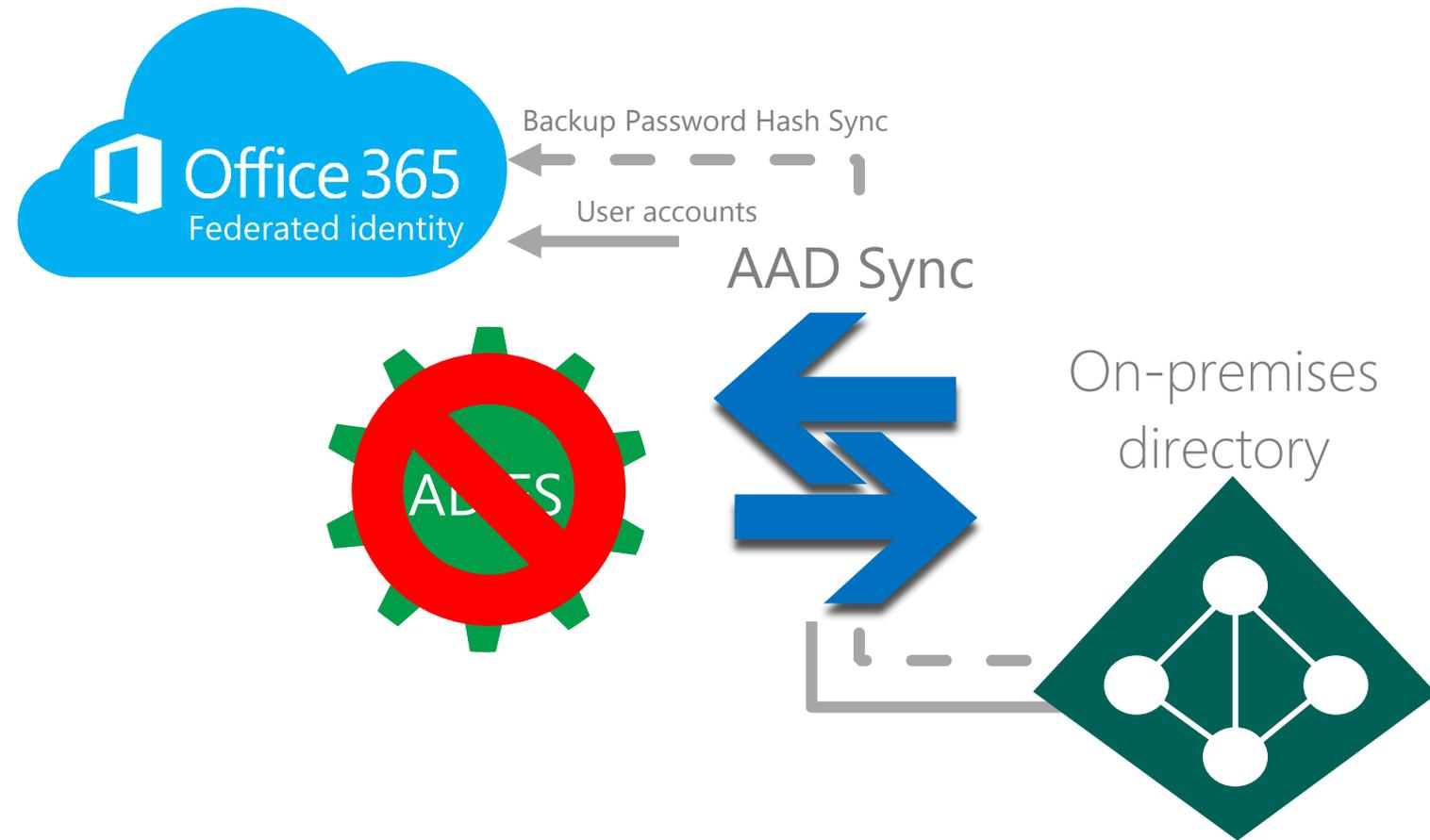
Azure AD as the control point
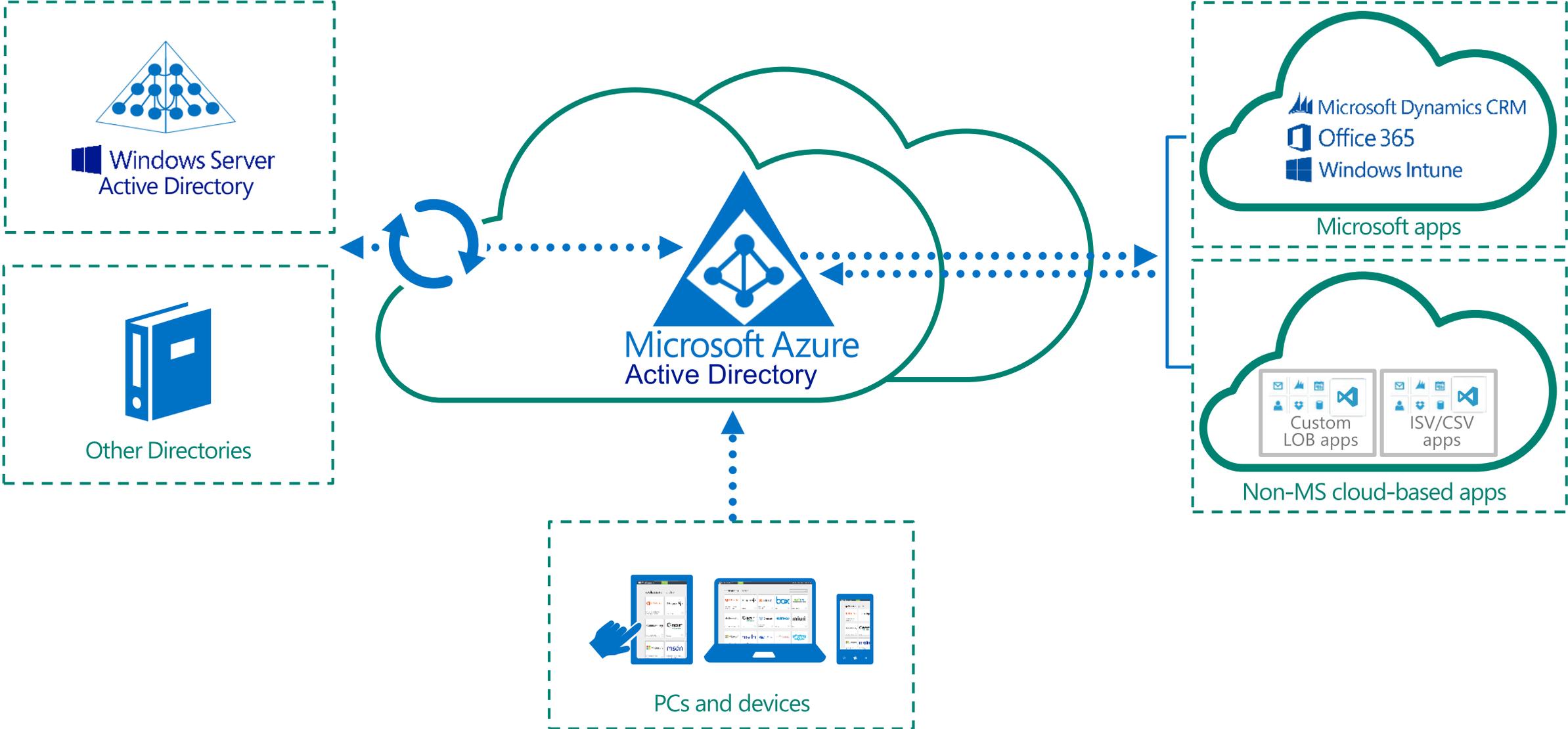
What is Azure Active Directory?
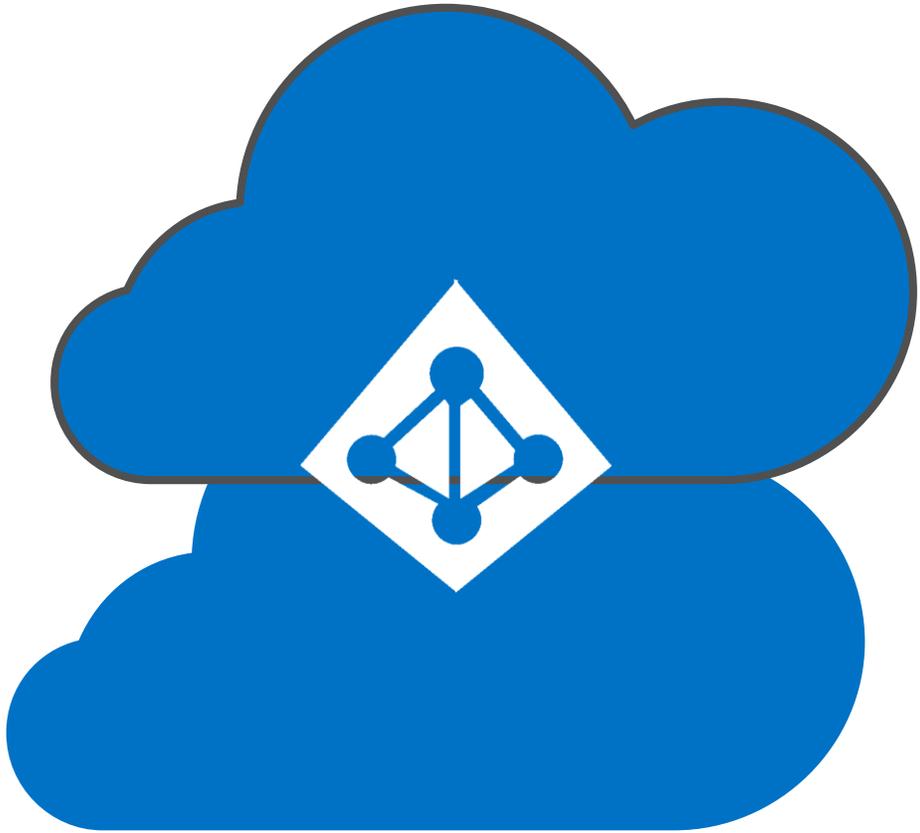
A comprehensive identity and access management cloud solution.

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

Microsoft Azure
Active Directory

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 he 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.

Access to free Azure AD via Office 365

Add an application

Add an application

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

Add an application for my organization to use

evernote

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

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

Add an application

evernote

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

Add an application

Add an application

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
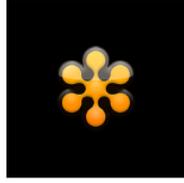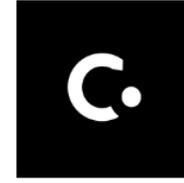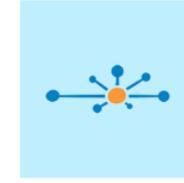
MarcomCentral By PTI Marketing Technologies	**McKesson InterQual Online Learning** By McKesson
Oracle SRM By Oracle Corporation	**Oracle Taleo** By Oracle Corporation
ClearDB By SuccessBricks, Inc.	**SuccessFactors** By SuccessFactors, Inc. A SAP Company
American Expresss OPEN Small Business By American 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


AD Agent

Logs

Microsoft Azure
Active Directory
Cloud App Discovery
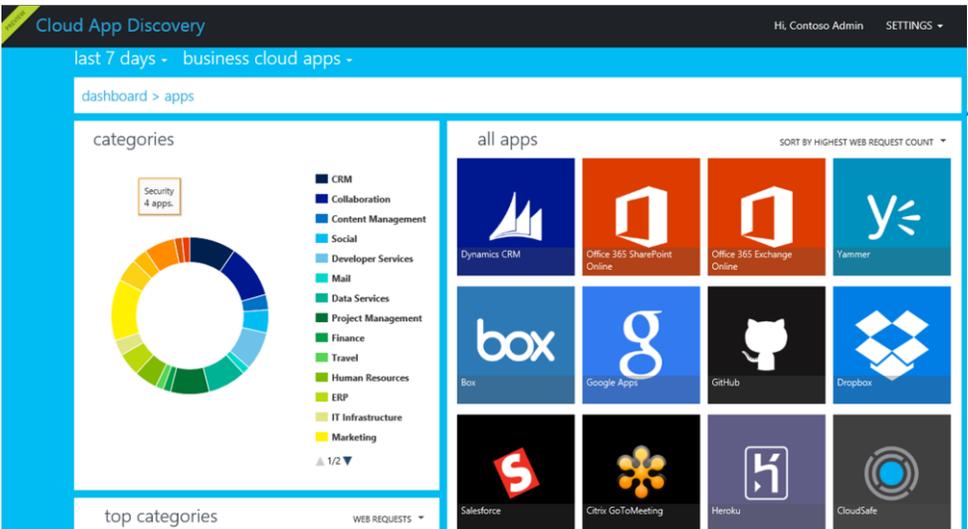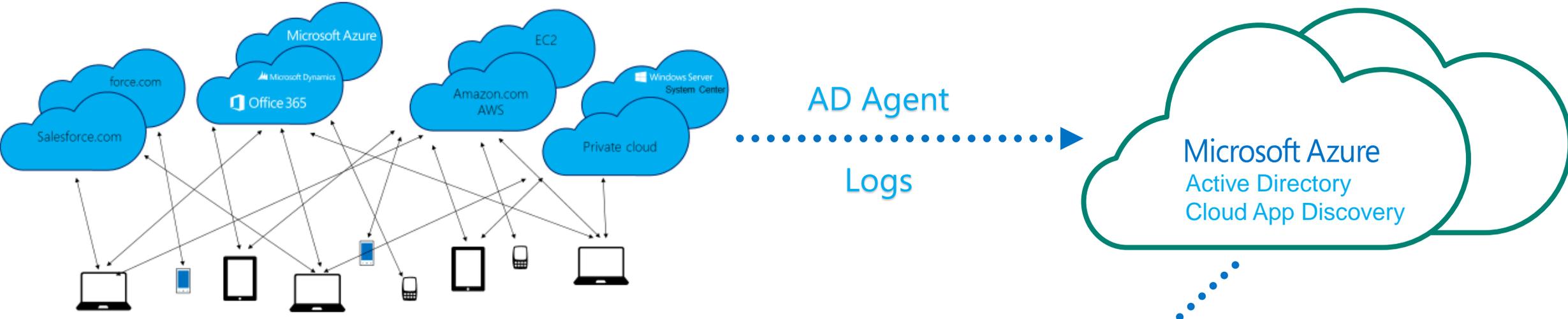
Your Directory on the cloud

Connect and Sync on-premises directories with Azure.

2400+ Preintegrated popular SaaS apps.

Windows Server
Active Directory
+
Other Directories

Microsoft Azure
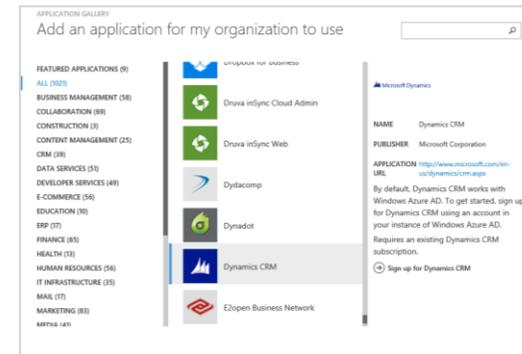
SaaS apps

Centrally managed identities and access

Comprehensive identity and access management console.

Centralized access administration for preintegrated SaaS apps and other cloud-based apps.

Secure business processes with advanced access management capabilities.

Your cloud apps are ready when you are.

Connect to Azure AD

https://www.youtube.com/watch?v=qpPYmGV5GjM

Mobile Device Management

Conditional Access

Device Management
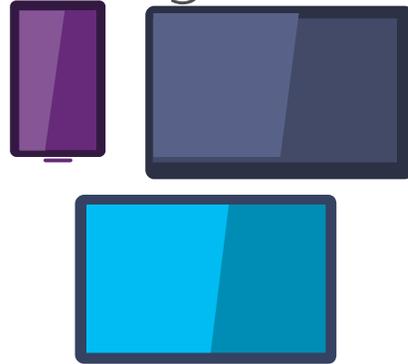
Selective Wipe
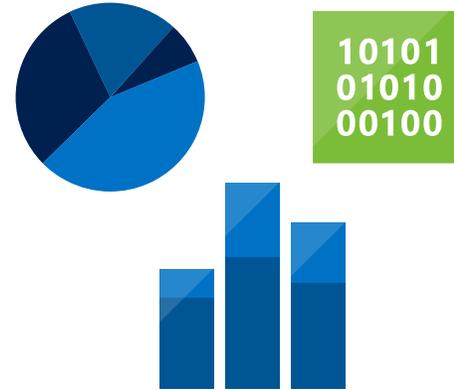
Advanced Application Management

10101
01010
00100

OneDrive

LoB app
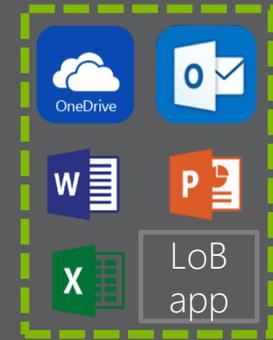
Built-in

Microsoft Intune

Recent additions

B2B Sharing

- http://blog.ciaops.com/2015/11/using-azure-ad-b2b-sharing-with.html

Azure AD Domain Services

- https://azure.microsoft.com/en-us/services/active-directory-ds/

References

What is Azure Active Directory
- http://azure.microsoft.com/en-us/documentation/articles/active-directory-whatis/

Azure Active Directory Editions
- https://msdn.microsoft.com/en-us/library/azure/dn532272.aspx

MSDN Channel 9 Azure videos
- http://channel9.msdn.com/Series/Windows-Azure-Active-Directory

Windows 10 and Azure AD
- http://blogs.windows.com/business/2015/05/15/windows-10-and-azure-active-directory-embracing-the-cloud/

Thank You

Questions / Feedback?

@directorcia
http://about.me/ciaops