Microsoft Azure

Unlock the power of the cloud with enterprise-level identity services for all your cloud apps.

AZURE ACTIVE DIRECTORY

Use Azure Active Directory (Azure AD) at global scale to centrally manage employee access and provide single sign-on to Microsoft services such as Azure, Office 365, Dynamics CRM, Windows Intune, and thousands of non-Microsoft cloud apps.

MULTI-FACTOR AUTHENTICATION

Use Multi-Factor Authentication to protect access to sensitive company information and to help protect your organization from malicious attacks.

Choose what you need: Azure AD Free or Premium

Azure Active Directory Free

Manage user accounts, synchronize with on-premises directories, and get single sign-on across Azure, Office 365, and thousands of popular SaaS applications, such as Salesforce, Workday, Concur, DocuSign, Google Apps, Box, ServiceNow, Dropbox, and more.

Azure Active Directory Premium

Get all that Free has to offer plus the identity management capabilities described below.

SELF-SERVICE PASSWORD RESET

Reduce helpdesk calls. Give users the ability to reset their password in the cloud or on-premises when sync is enabled.

SELF-SERVICE GROUP MANAGEMENT

Enable group owners to approve requests and maintain group memberships.

GROUP-BASED APPLICATION ACCESS

Use groups to assign user access in bulk to SaaS applications. Create groups solely in the cloud or leverage existing groups from your on-premises Active Directory.

ADVANCED SECURITY REPORTS

Monitor and protect access to your cloud applications with logs that show anomalies and reports that flag inconsistent access patterns. Advanced reports help you improve access security and respond to potential threats.

COMPANY BRANDING

Add your company logo and color scheme to your organization's Sign In and Access Panel pages. Add localized versions of the logo for specific languages and locales. Wherever you see the fictional company name **CONTOSO** is where you can apply your company logo.

MULTI-FACTOR AUTHENTICATION

Help prevent unauthorized access to on-premises and cloud applications by providing an additional layer of authentication. You also get a license to deploy a Multi-Factor Authentication server for additional security of on-premises applications, such as remote access VPNs and web applications, as well as cloud applications using Active Directory Federation Services.

MICROSOFT IDENTITY MANAGER

Do you have a variety of on-premises directories and databases that you want to sync directly to Azure AD? Premium comes with Identity Manager servers and user licenses to support any combination of hybrid identity solutions.

Like it? Get it.

© 2014 Microsoft Corporation. All rights reserved.
Created by the Azure poster team
Email: AzurePoster@microsoft.com
Part no. 098-117678

Cloud Identity and Access Management

Microsoft

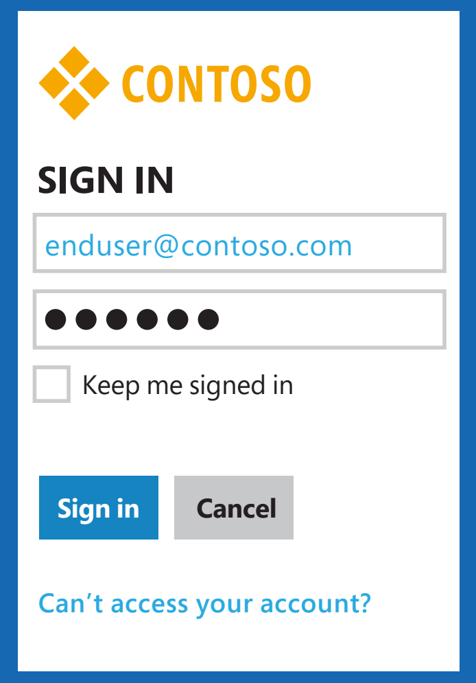
EMPOWER YOUR USERS

Enable users to work from any location using any device. Give them always-on access to all their work resources using a single set of credentials protected with Multi-Factor Authentication. After a user has signed in, they get single sign-on access to their apps and data.

CORPORATE OFFICE

HOME OFFICE

ON THE GO



CONTOSO

SIGN IN

enduser@contoso.com

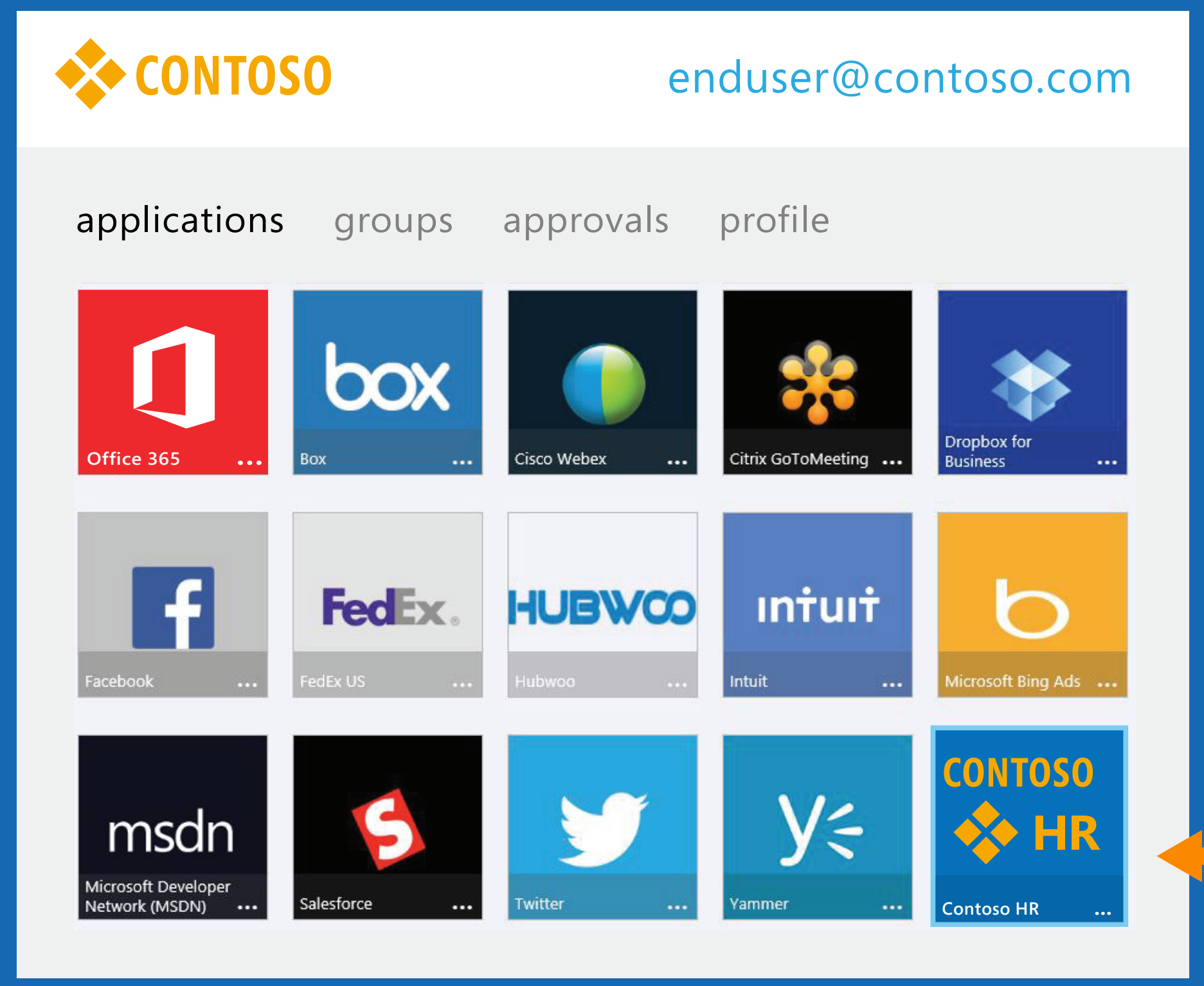
●●●●●●

□ Keep me signed in

Sign in | Cancel

Can't access your account?

ACCESS PANEL



CONTOSO enduser@contoso.com

applications groups approvals profile

Office 365 · Box · Cisco Webex · Citrix GoToMeeting · Dropbox for Business

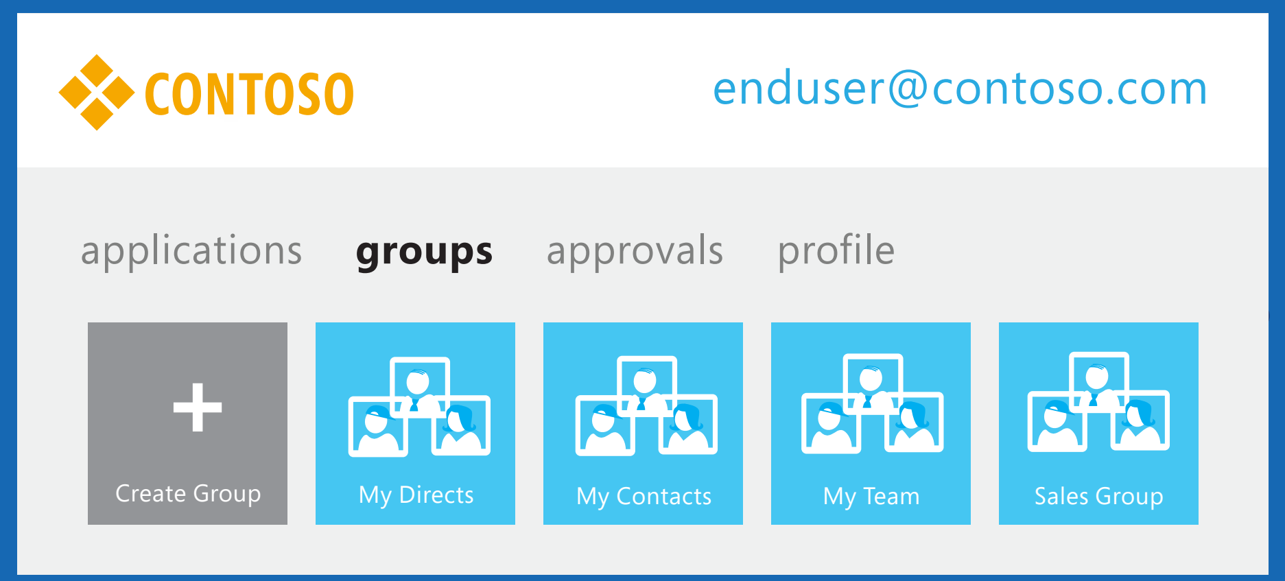
Facebook · FedEx US · Hubwoo · Intuit · Microsoft Bing Ads

Microsoft Developer Network (MSDN) · Salesforce · Twitter · Yammer · Contoso HR

SELF-SERVICE CAPABILITIES

Minimize support costs and keep users up and running by configuring self-service experiences. With web-based tools such as Access Panel and Password Reset, give users a personalized, company-branded portal to access SaaS applications.

ACCESS PANEL > GROUPS



CONTOSO enduser@contoso.com

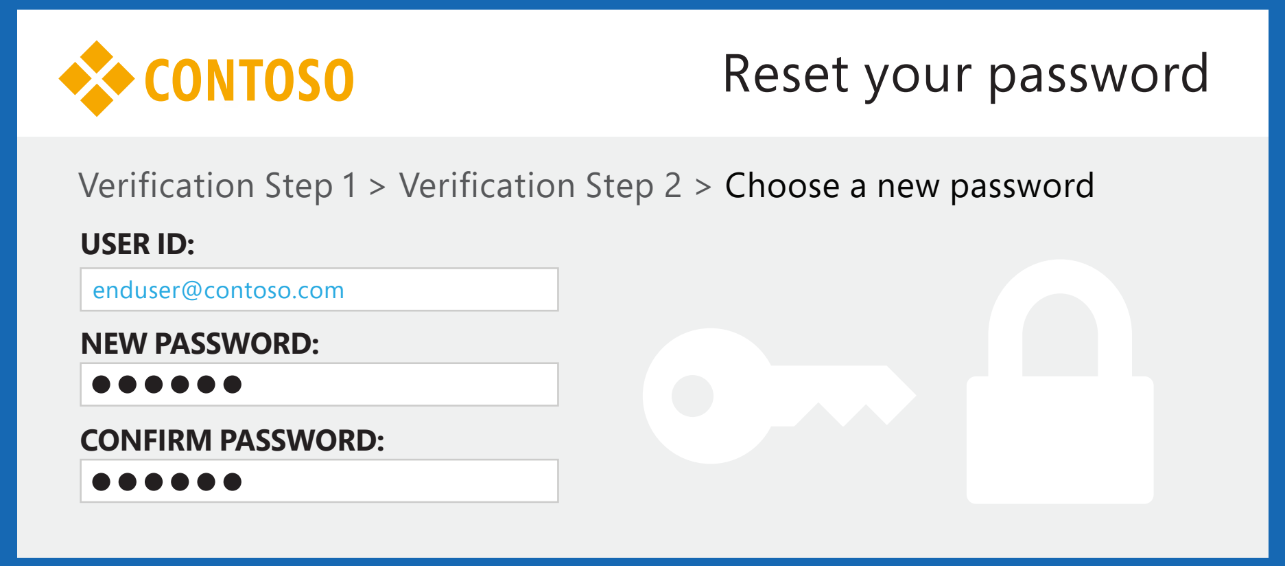
applications groups approvals profile

Create Group · My Directs · My Contacts · My Team · Sales Group

USERS CREATE AND MANAGE THEIR OWN GROUPS

Empower users to create their own groups, assign members to groups they own, approve join requests, and more.

PASSWORD RESET



CONTOSO Reset your password

Verification Step 1 > Verification Step 2 > Choose a new password

USER ID:
enduser@contoso.com

NEW PASSWORD:
●●●●●●

CONFIRM PASSWORD:
●●●●●●

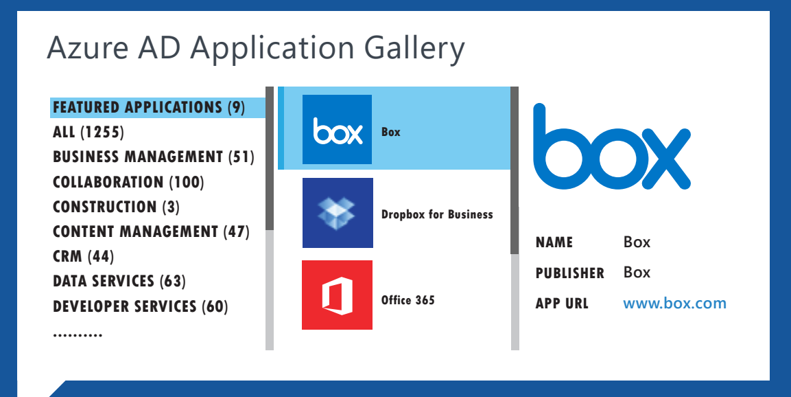
USERS CHANGE AND RESET THEIR OWN PASSWORDS

Give all users in your directory the capability to change and reset their passwords--whether they are in the cloud or on-premises.

CLOUD

MANAGE YOUR SAAS APPLICATIONS

Add and manage SaaS applications in the public cloud by using the Azure AD Application Gallery. Users can then quickly sign in to your Microsoft and third-party SaaS apps from the Access Panel. Set up user provisioning to automatically sync users to your app and back.



Azure AD Application Gallery

FEATURED APPLICATIONS (9)
ALL (1255)
BUSINESS MANAGEMENT (51)
COLLABORATION (100)
CONSTRUCTION (3)
CONTENT MANAGEMENT (47)
CRM (44)
DATA SERVICES (63)
DEVELOPER SERVICES (60)
....

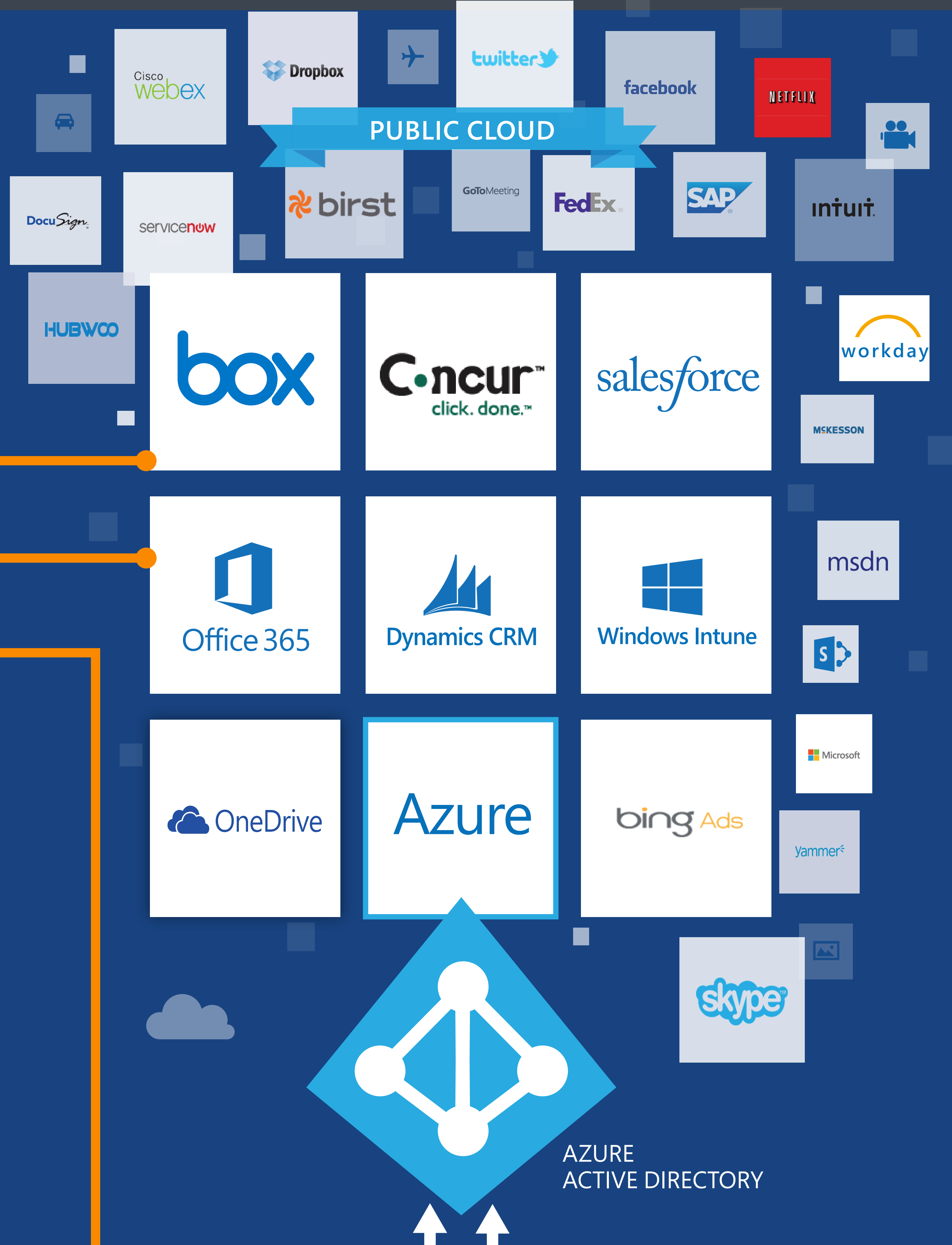
Box
Dropbox for Business
Office 365

NAME	Box
PUBLISHER	Box
APP URL	www.box.com

NON-MICROSOFT APPS

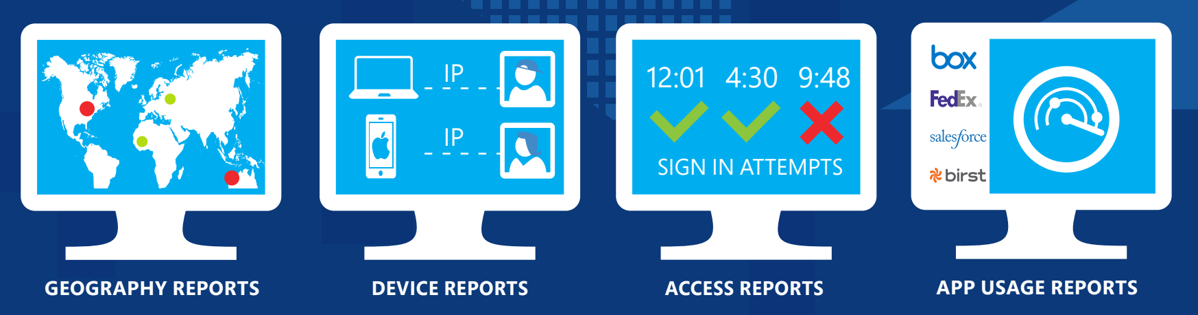
MICROSOFT APPS + SERVICES

APPS YOU BUILD



AZURE ACTIVE DIRECTORY

PREVENT MALICIOUS ATTACKS

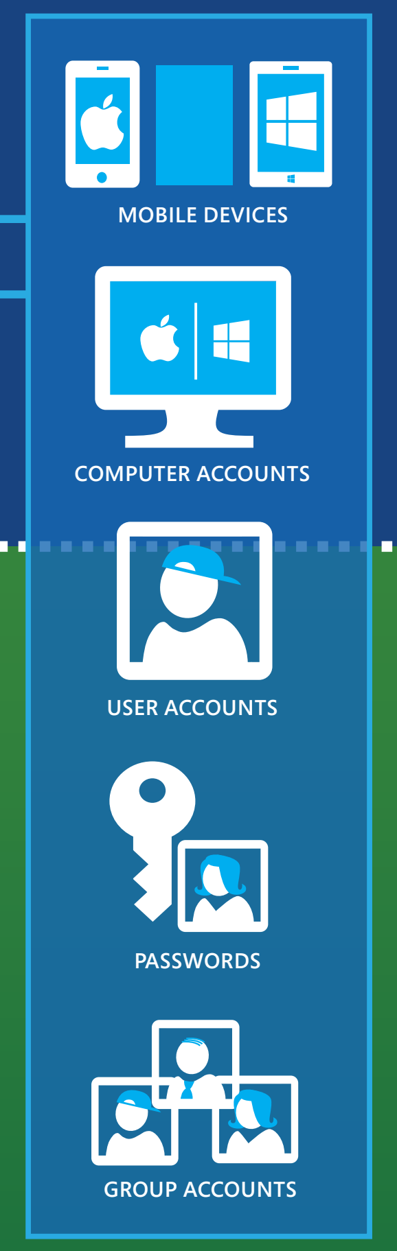


Monitor access and anomaly reports to help secure your Azure AD directory. Get visibility into security risks so that you can mitigate them.

INTEGRATE YOUR LOB AND SAAS APPS

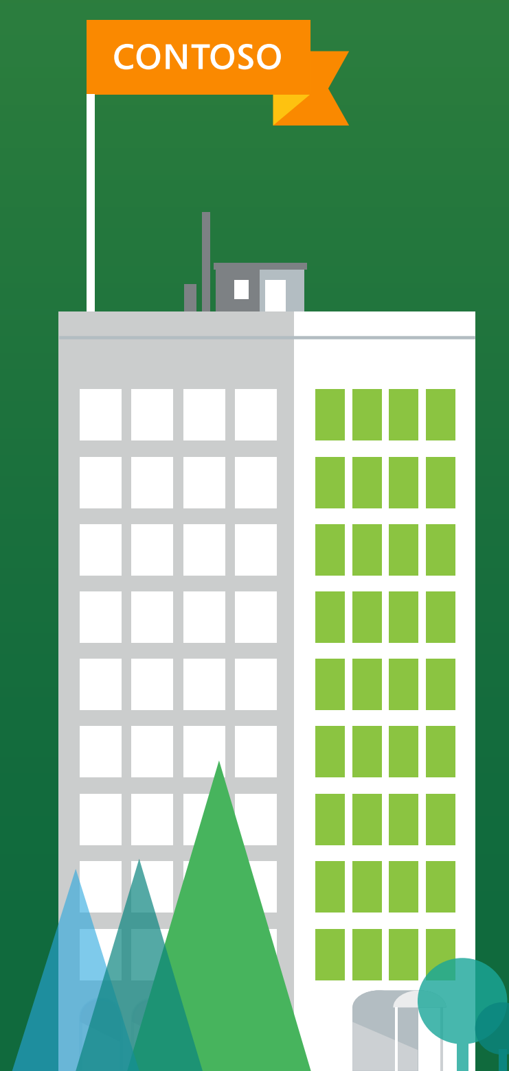
Build line-of-business (LOB) or SaaS applications using standard development tools and integrate your applications with Azure AD for use in one organization (single tenant) or many organizations (multi-tenant). Integrated applications leverage Azure AD for single sign-on, identity and access management, querying the directory, and more.

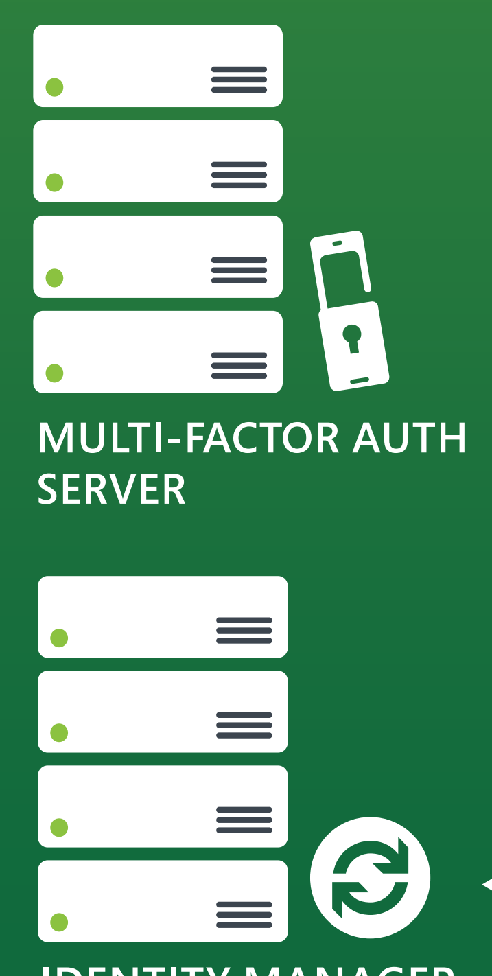
Publish your app to the Azure AD Application Gallery. An administrator then adds it to the Access Panel for use by any user or group that has been assigned access.



DIRECTORY OBJECTS

ON-PREMISES





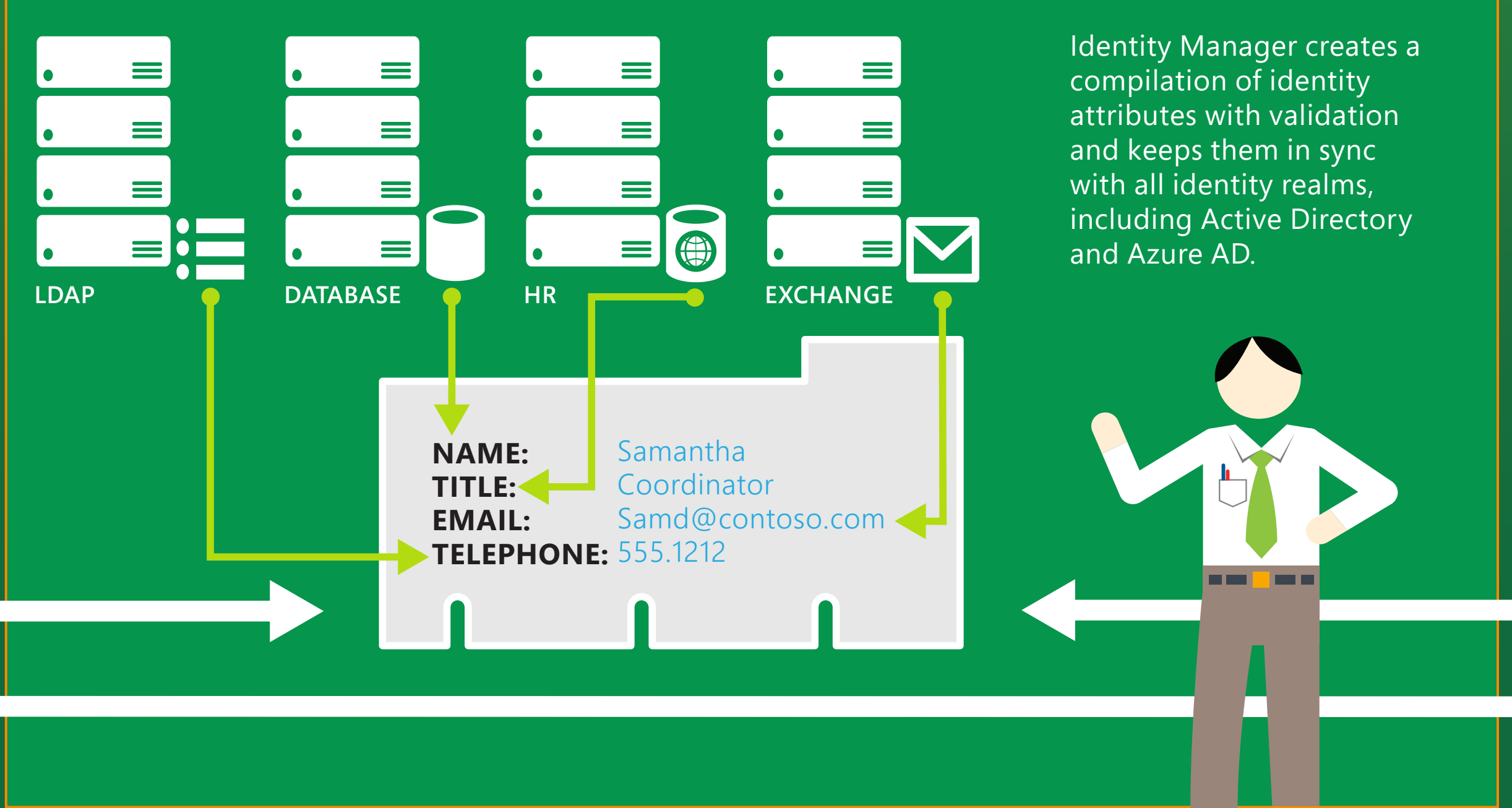
MULTI-FACTOR AUTH SERVER

IDENTITY MANAGER SERVER

HYBRID IDENTITY SOLUTIONS

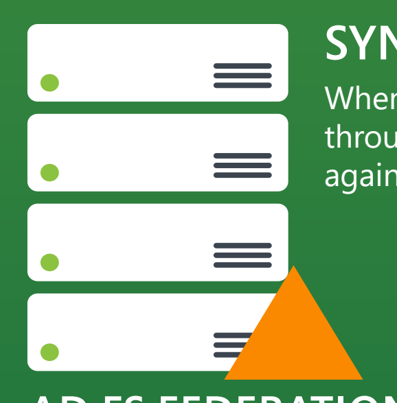
Provide users with a common identity across on-premises and cloud-based services, leveraging Windows Server Active Directory and Azure AD capabilities.

SYNC FROM ANY DIRECTORY OR DATABASE TO THE CLOUD AND BACK



NAME: Samantha
TITLE: Coordinator
EMAIL: Samd@contoso.com
TELEPHONE: 555.1212

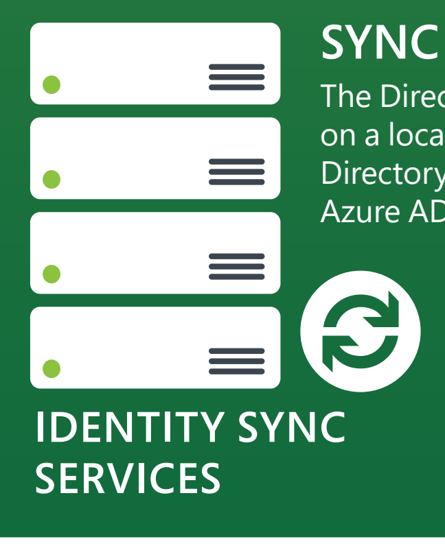
Identity Manager creates a compilation of identity attributes with validation and keeps them in sync with all identity realms, including Active Directory and Azure AD.



AD FS FEDERATION SERVER

SYNC AND FEDERATION TOGETHER

When used together, user attributes are synchronized using DirSync. Authentication is passed back through a federation server, such as Active Directory Federation Services (AD FS), and completed against your on-premises Active Directory.



IDENTITY SYNC SERVICES

SYNC USERS, GROUPS, DEVICES, PASSWORDS, AND MORE

The Directory Sync tool and Azure AD sync are both identity sync services that can be installed on a local server to sync directory objects between directories. Password Sync, a feature of the Directory Sync tool, synchronizes user passwords from your on-premises Active Directory to Azure AD.

WINDOWS SERVER ACTIVE DIRECTORY