

Microsoft Mobility and Security for Enterprise Architects

What IT architects need to know about mobility with Microsoft cloud services and platforms

This topic is 1 of 4 in a series 1 2 3 4

Enable productivity and collaboration from anywhere while protecting data and applications

Microsoft provides broad support for mobile productivity with support for applications and rich features for controlling access to your organization's assets.

Microsoft mobile apps for business

Microsoft produces a number of [business class mobile apps](#) for productivity. See page two for featured applications.

With an Office 365 for business subscription, you get mobile apps that help you get more done from your favorite device while keeping your data secured. Use Intune Mobile Application Management to apply additional security when using these mobile applications.



Skype for Business, Yammer, OneNote, and more apps for business are also available. Get the full list of apps and [learn how to set them up on your devices](#).

Dynamics CRM also includes [apps for phones and tablets](#).

Developing your own mobile apps

Use the [Mobile Apps feature of Azure App Service](#) to build engaging iOS, Android, and Windows apps or cross-platform Xamarin or Cordova (Phonegap) apps for your customers and business.

- Broadcast push with customer segmentation
- Enterprise single sign-on with Active Directory
- Autoscale to support millions of devices
- Apps can work offline and sync
- Social integration with Facebook, Twitter, Google



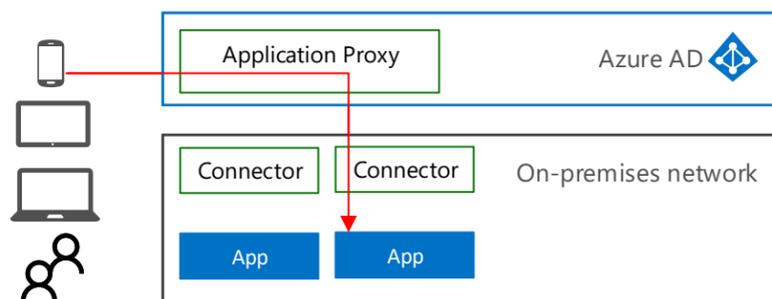
Cloud App Security for SaaS apps

[Microsoft Cloud App Security](#) is a comprehensive service that provides deeper visibility, comprehensive controls, and improved protection for your cloud applications.

- App discovery** Identify all cloud applications in your network—from all devices—and evaluate risk scoring and ongoing risk assessment and analytics. No agents required.
- Data control** Approve apps. Set granular controls and policies for data sharing and DLP.
- Threat protection** Identify high-risk usage, security incidents, and detect abnormal user behavior to prevent threats.

Mobile access to on-prem applications

Microsoft [Azure Active Directory Application Proxy](#) lets you publish applications, such as web-based apps inside your private network and provides secure access to users outside your network. You can protect on-premises applications with the same requirements as other cloud-based applications with MFA, device requirements, and other conditional access requirements.



Managing access to cloud-based applications and data from mobile devices

Microsoft provides a range of capabilities you can use to control access to applications and data from mobile devices.

Enterprise Mobility + Security (EMS)

Office 365

Basic capabilities for Office 365 applications

Multi-factor authentication for Office 365 applications.

Basic controls for access to Exchange Online and SharePoint Online.

Basic Mobile Device Management (MDM) capabilities.

Azure AD Premium

Control access to applications based on user accounts and groups

Multi-factor authentication with user, location, and device-based rules for SaaS applications in your environment.

Advanced protection with risk-based adaptive access control.

Single sign-on to all SaaS applications in your environment.

Microsoft Intune

Controls for managing mobile applications, devices, and PCs

Mobile application policies (MAM) for mobile devices.

Device-based management, configuration compliance, and conditional access.

Deploy apps and manage apps to mobile devices and PCs.

Azure Information Protection

Encryption, classification, labeling, identity, and authorization policies applied to email and files

Previously "Azure Rights Management (RMS)."

Protect targeted data sets with RMS policies. All file types are supported.

Protection stays with files no matter where they go.

Support for on-premises services, as well as Office 365.

Microsoft Mobility and Security for Enterprise Architects

What IT architects need to know about mobility with Microsoft cloud services and platforms

This topic is 2 of 4 in a series 1 2 3 4

Featured apps for mobile devices

Microsoft Office apps

Review, edit, analyze and present with a consistent and familiar user interface optimized for use on your mobile device. Core editing is free for consumers on devices with screen sizes smaller than 10.1".

[Extra features on your iPad* and iPhone with Office 365](#)

[Extra features on your Android tablet and phone with Office 365](#)

[Extra features on your Windows phone and Windows tablet with Office 365](#)

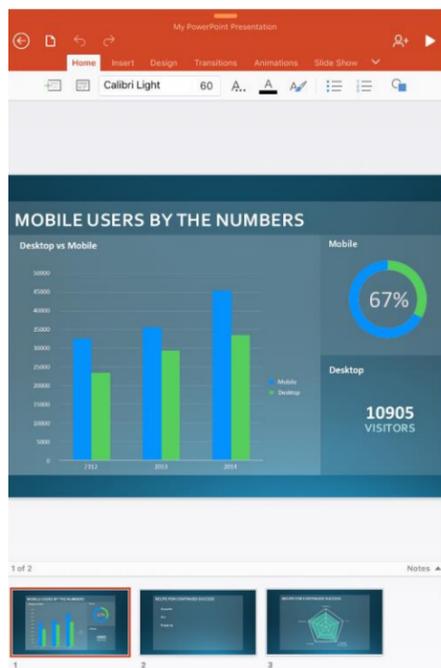
[Enhancing information rights management in Word, Excel and PowerPoint mobile apps](#)

[Azure RMS requirements: Applications](#)

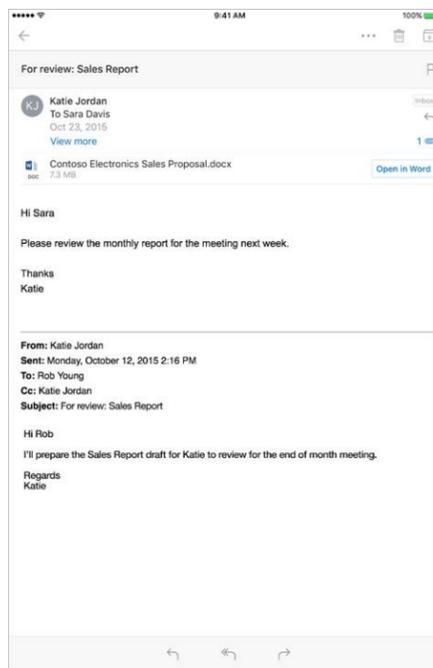
Excel



PowerPoint



Outlook



Word

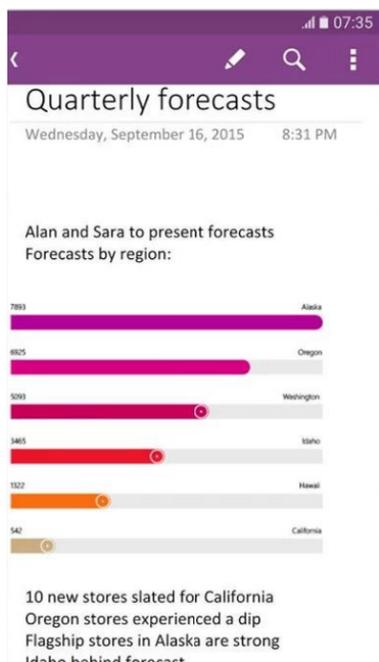
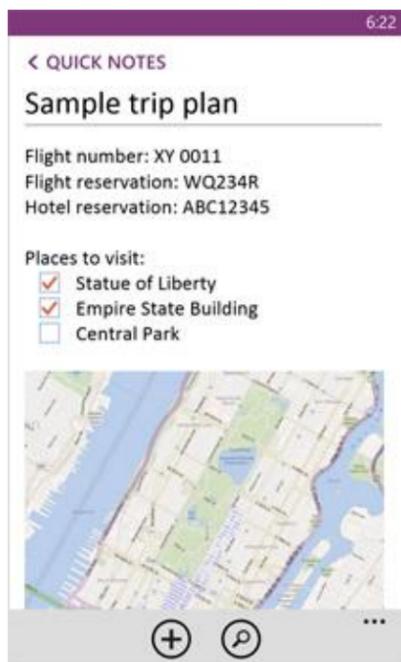


OneNote

Type, hand write, draw, and clip things from the web to get down your thoughts into your notebook. Use OneNote's flexible canvas to place content anywhere you want. You can even scan hand written notes or pages straight into OneNote then make them searchable.

<https://www.onenote.com/>

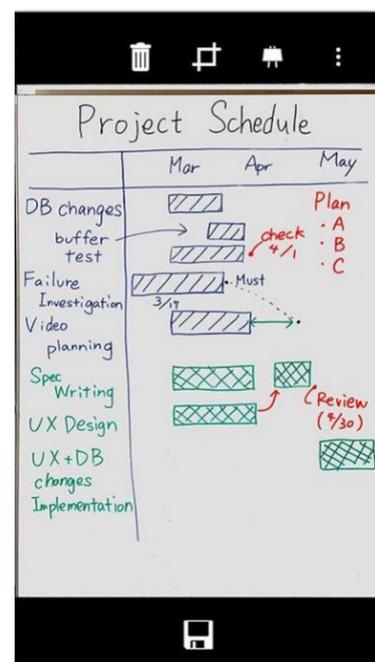
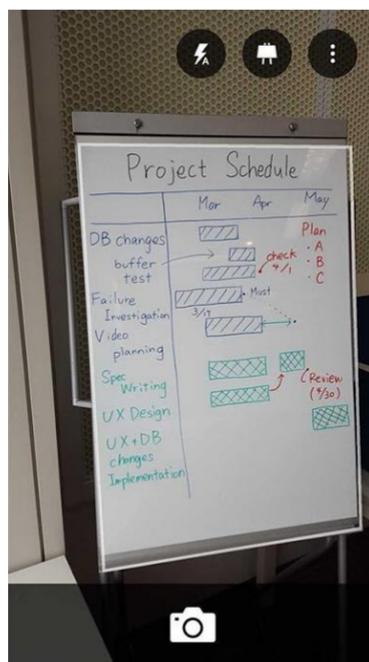
[Install OneNote on a mobile phone or device](#)



Office Lens

Office Lens trims, enhances, and makes pictures of whiteboards and docs readable. You can use Office Lens to convert images to PDF, Word and PowerPoint files, and you can even save images to OneNote or OneDrive.

[Office Lens comes to iPhone and Android](#)

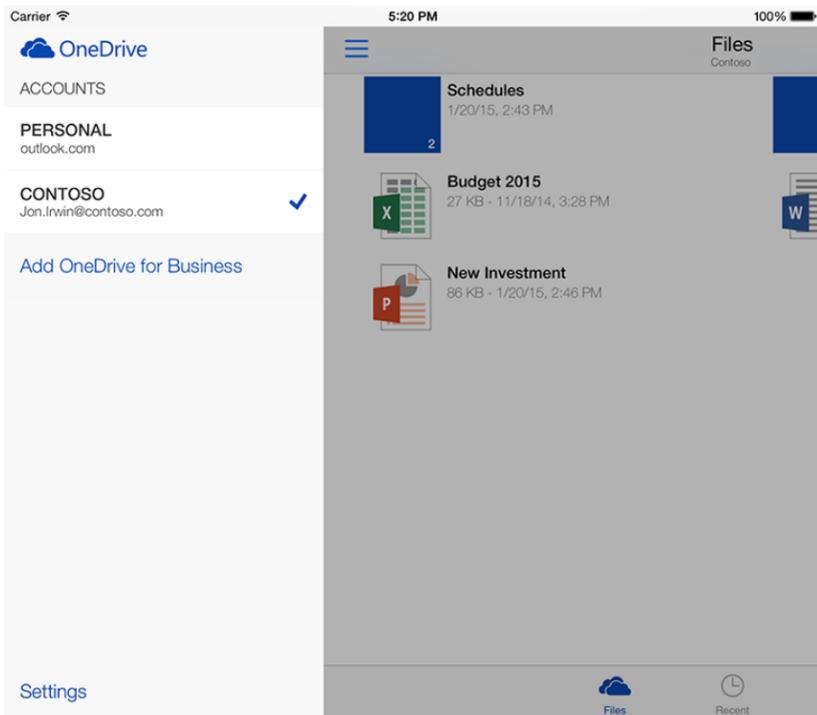


Continued on next page

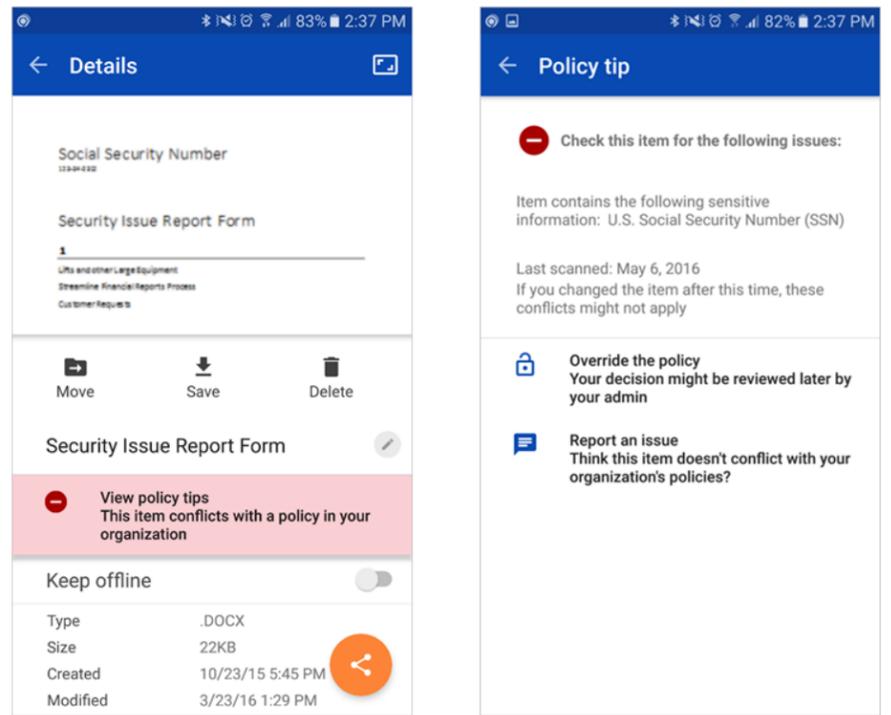
OneDrive mobile app

Use the same app for your business and personal accounts. Add additional accounts.

[Set up OneDrive for Business on your phone or tablet](#)



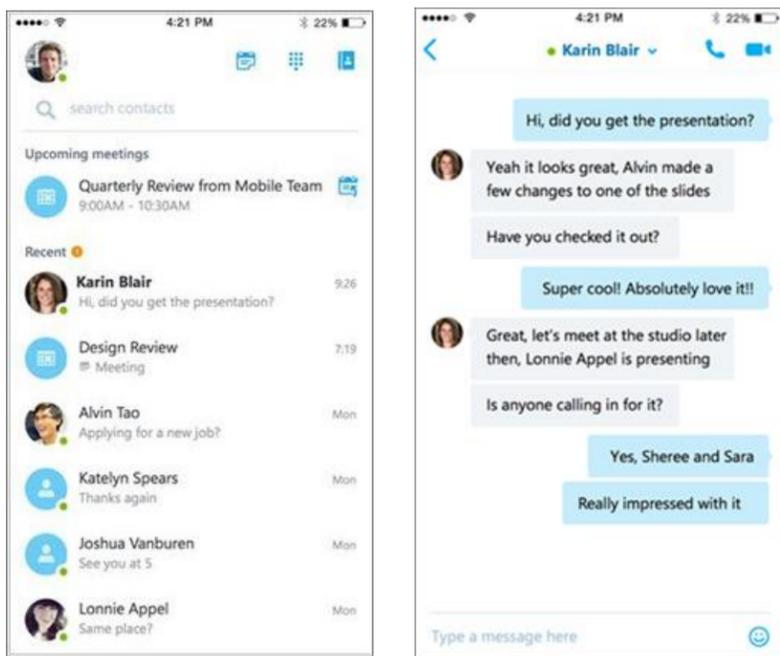
Configure [Data Loss Prevention Policy Tips for OneDrive mobile apps](#). Documents stored in OneDrive for Business are scanned for sensitive information and evaluated against company policies configured in Office 365. Included with Office 365 E3 and E5 plans.



Skype for Business mobile app

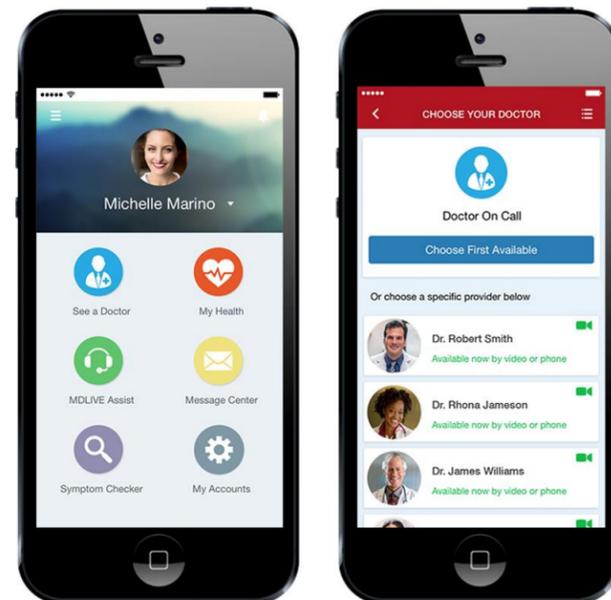
Connect with your team anywhere using clients across Windows, Mac, iOS, and Android™, or bring remote participants into meeting spaces of all sizes with Skype for Business.

[Download Skype for Business across all your devices](#)



Add Skype for Business inside your mobile apps

The [Skype for Business App SDK Preview](#) is now available for download. This new SDK enables developers to seamlessly integrate instant messaging, audio and video experiences into their custom iOS and Android applications.



Office Delve for Android

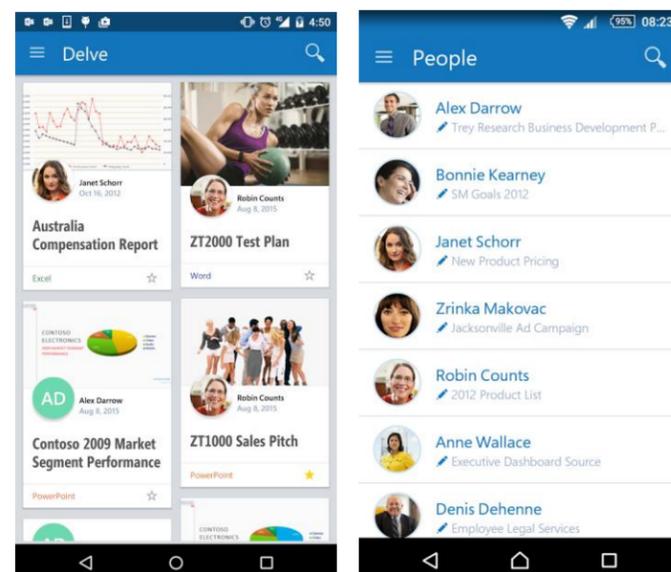
[Use Delve](#) to see what you and your colleagues are working on across Office 365. Based on who you work with and how you work together, Delve suggests documents that are relevant to you.

Key features:

- Discover new information
- Find documents through people
- Get back to documents you're working on

In Delve you'll only see content that has been shared with you. This means that your colleagues won't see your private documents, and you won't see theirs.

IMPORTANT: You can only use this app if your organization uses Office 365 and Delve.



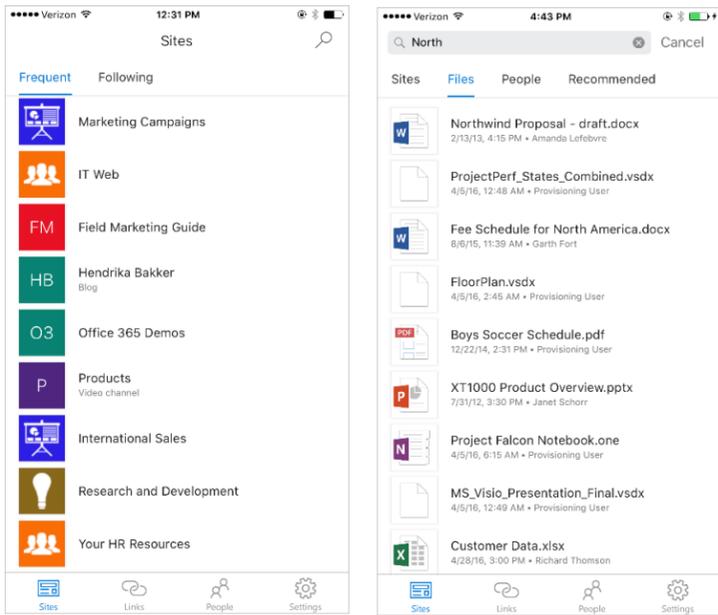
[Continued on next page](#)

SharePoint mobile app

Navigate SharePoint sites, view links to sites your organization has marked as important, view people profiles and search for people, sites and documents.

[Getting started with the SharePoint mobile app](#) Available from the Apple App Store starting June 2016. Android and Windows versions will follow.

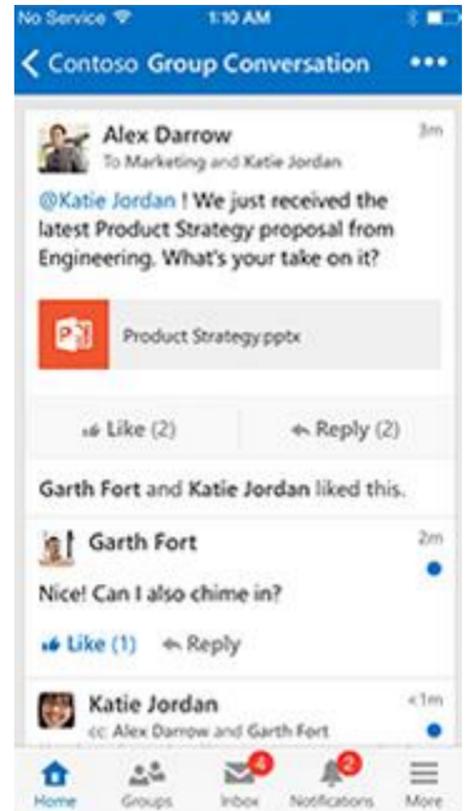
Also: [Use a mobile device to work with SharePoint Online sites](#)



Yammer mobile app

Stay on top of conversations, post updates, and collaborate with your team no matter where in the world you are.

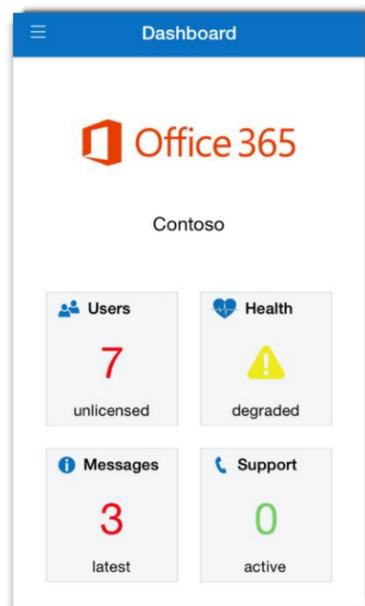
[Download the Yammer app](#)



Office 365 Admin app

Manage Office 365 from anywhere. The Office 365 Admin app allows you to receive notifications, add users, reset passwords, create support requests, and more, when you're on the go.

[Learn about and download the app](#)



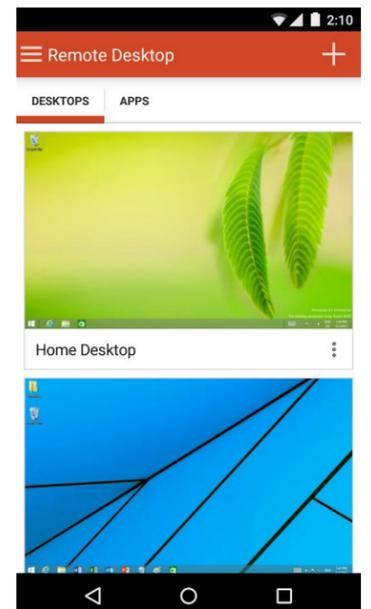
Microsoft Remote Desktop

With the Microsoft Remote Desktop app, you can connect to a remote PC and your work resources from almost anywhere.

[Google Play \(Android\)](#)

[Apple Store](#)

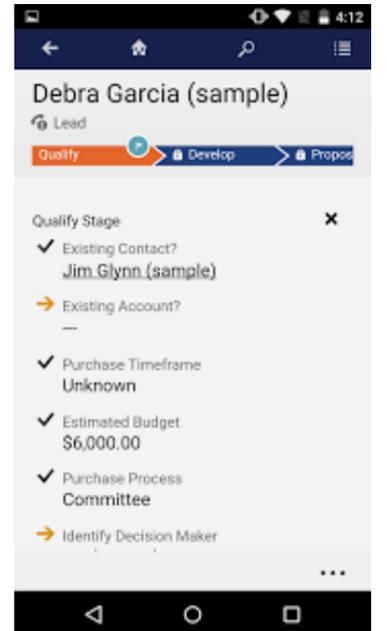
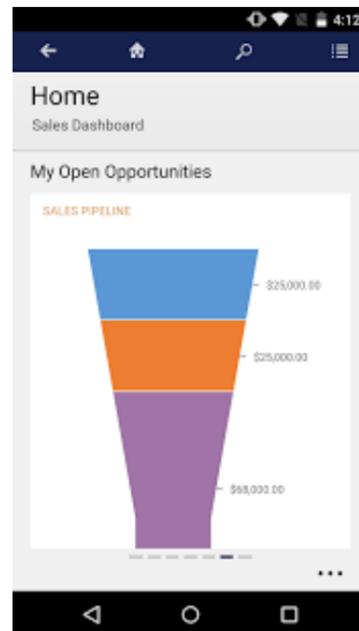
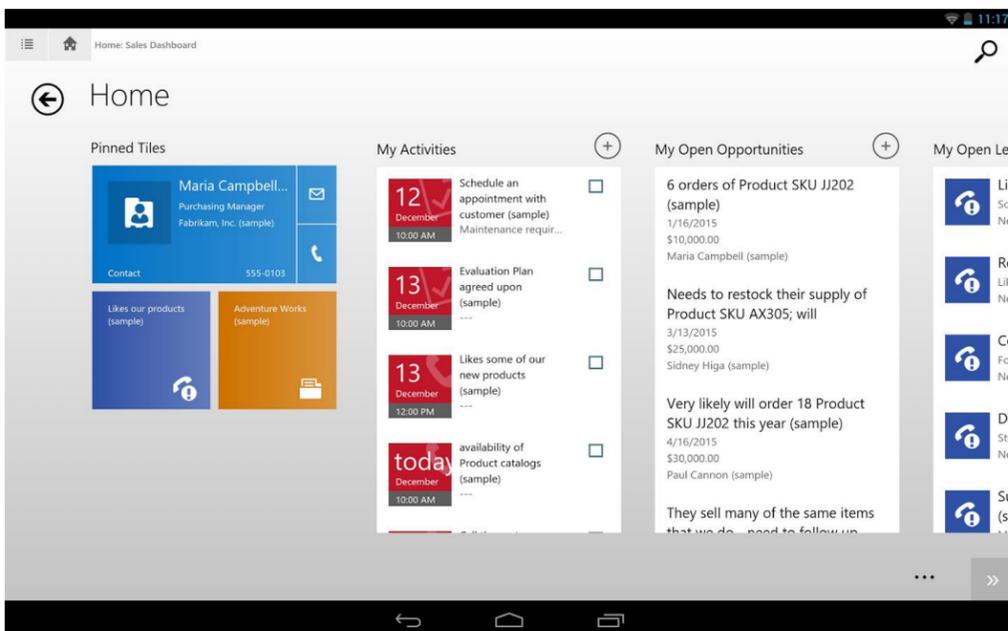
[Microsoft Store](#)



Dynamics CRM for phones and tablets

Keep track of your contacts, leads, and activities on the go with the [Microsoft Dynamics CRM for phones and Microsoft Dynamics CRM for tablets apps](#). You get the same intuitive experience on both your phone and tablet.

[Dynamics CRM Developers: Build Your Own Mobile Apps for Windows, iOS, and Android](#)



Microsoft Mobility and Security for Enterprise Architects

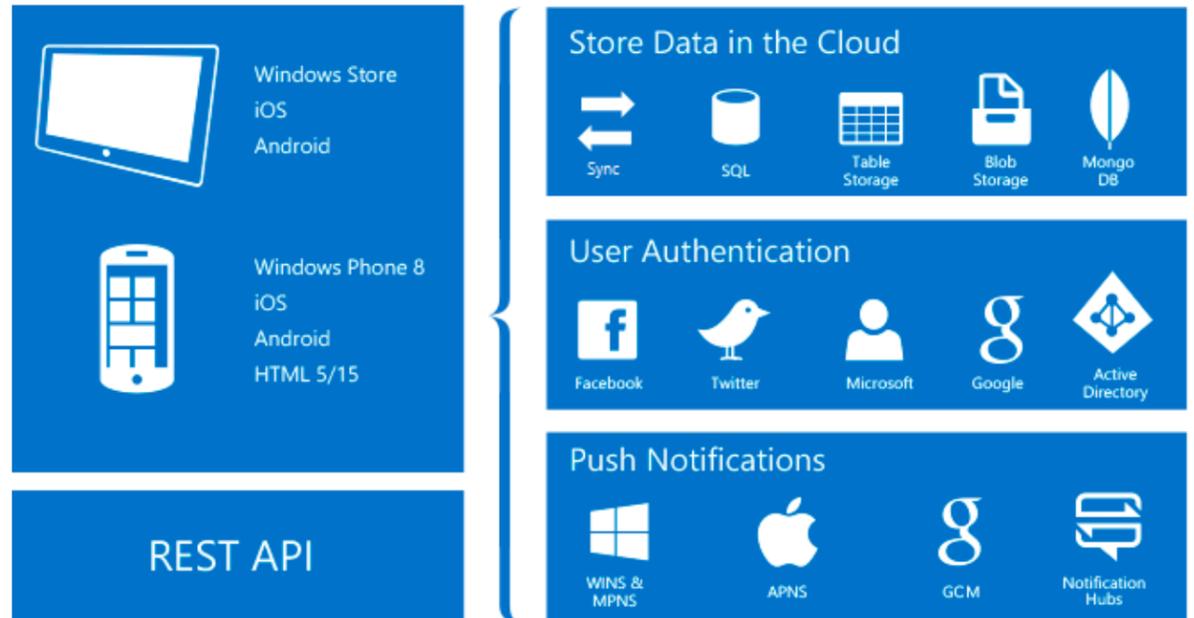
What IT architects need to know about mobility with Microsoft cloud services and platforms

This topic is 3 of 4 in a series 1 2 3 4

Mobile app development

With the Mobile Apps feature of Azure App Service, you can rapidly build engaging cross-platform and native apps for iOS, Android, Windows, or Mac; store app data in the cloud or on-premises; authenticate users; send push notifications; or add your custom backend logic in C# or Node.js.

Azure App Service is a fully managed Platform as a Service (PaaS) offering for professional developers that brings a rich set of capabilities to web, mobile and integration scenarios. Mobile Apps in Azure App Service offer a highly scalable, globally available mobile application development platform for Enterprise Developers and System Integrators.



Build native and cross platform apps

Build native iOS, Android, and Windows apps or cross-platform Xamarin or Cordova (Phonegap) apps. Take advantage of App Service using native SDKs.

Connect to your enterprise systems

With Mobile Apps you can add corporate sign on in minutes, and connect to your enterprise on-premises or cloud resources.

Build offline-ready apps with data sync

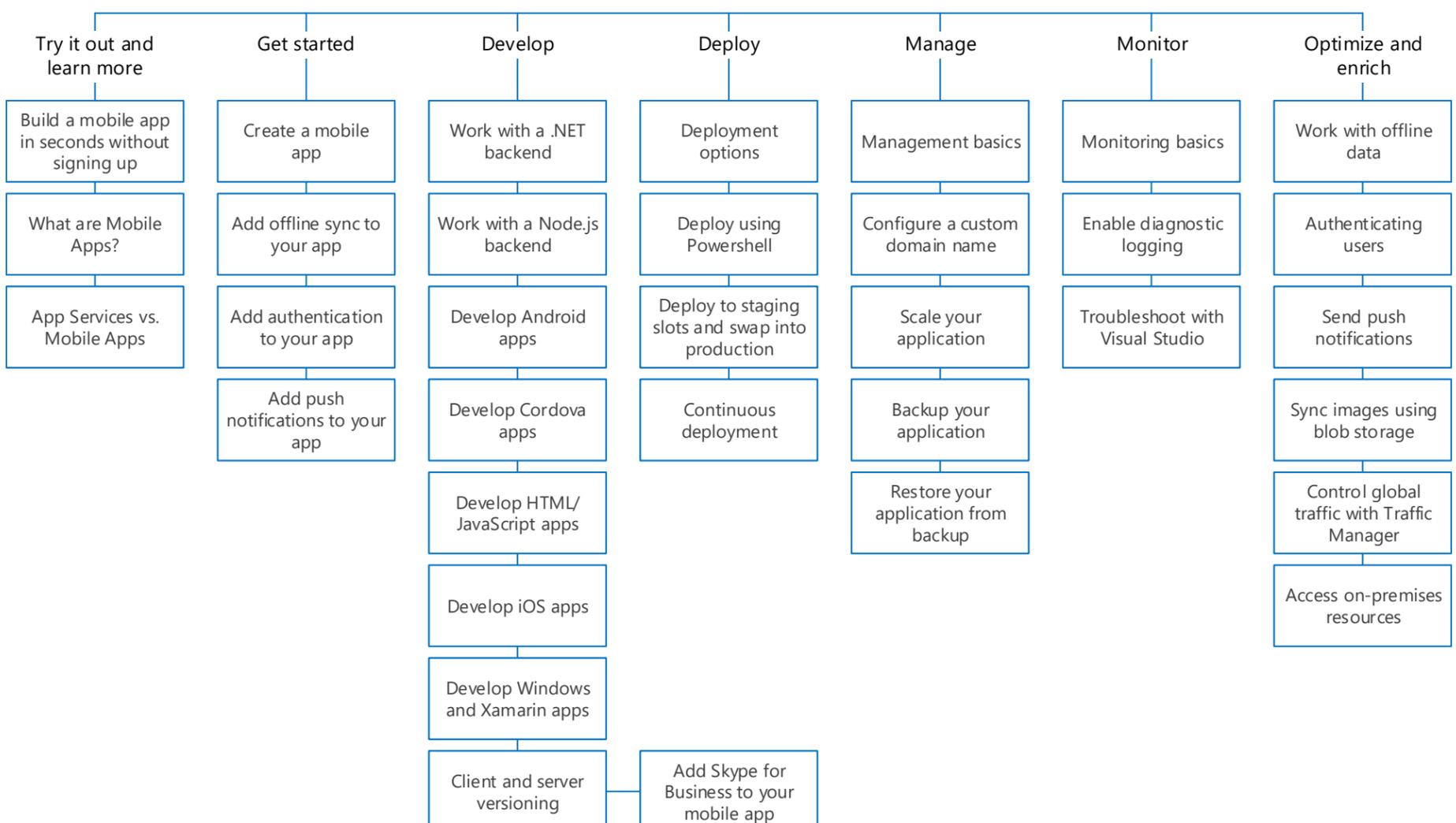
Make your mobile workforce productive by building apps that work offline and use Mobile Apps to sync data in the background when connectivity is present with any of your enterprise data sources or SaaS APIs.

Push Notifications to millions in seconds

Engage your users and customers with instant push notifications on any device, personalized to their needs, sent when the time is right.

App Service Mobile Apps capabilities and documentation

Click on each box for more information



Microsoft Mobility and Security for Enterprise Architects

What IT architects need to know about mobility with Microsoft cloud services and platforms

This topic is 4 of 4 in a series



Controlling access to applications and protecting data on mobile devices

Access control capabilities by product

For more information, see [Controlling Access to Office 365 and Protecting Content on Devices](#)



Microsoft Intune

BYOD (not enrolled)

Exchange Online — Configure basic password policies for Outlook Web Access (OWA).
SharePoint Online — Configure basic policies for external access to SharePoint sites.

Single sign-on to all SaaS applications in your environment.
Multi-factor authentication (MFA) — Enable per user.
Conditional access policies — Configure per application. Policies can vary between applications. Common policies are listed below.

Multi-factor authentication and location based access rules:

- Apply rules to all users or specific groups
- Require multi-factor authentication
- Require multi-factor authentication when not at work
- Block access when not at work

Applications that can be configured for conditional access using Azure AD Premium include:

- Microsoft Power BI
- Exchange Online
- SharePoint Online
- Yammer
- Outlook Groups
- Skype for Business
- Other SaaS apps in your environment that are configured for Azure AD single sign-on

Send a wipe request.

Configure mobile application management (MAM) policies per platform (without enrolling devices):

- iOS
- Android

Choose which applications to apply a policy to and then configure policy rules. Example settings for iOS:

- Prevent iTunes, iCloud backups
- Allow app to transfer data to other apps
- Allow app to receive data from other apps
- Prevent "Save As"
- Restrict cut, copy, and paste with other apps
- Restrict web content to display in the Managed Browser
- Encrypt app data
- Disable contacts sync
- Require PIN for access (with additional settings)
- Require corporate credentials for access
- Block managed apps from running on jailbroken or rooted devices
- Recheck the access requirements (timeout and offline grace period)
- Offline interval (days) before app data is wiped

These settings also apply to Company Owned Devices.

Enrolled devices

Enroll devices and configure basic access controls:

- Requirements for passwords, login attempts, lock timeout, and wipe after sign-in failures
- Require encryption
- Prevent jail broken or rooted devices
- Report violations

Additional security policies:

- Require encrypted backup
- Block cloud backup
- Block document synchronization
- Block screen capture
- Block video conferences on device
- Block sending diagnostic data from devices
- Block access to application store
- Require password when accessing application store
- Block connection with removable storage
- Block Bluetooth connection

Device based conditional access rules rely on Intune compliance policies and apply to enrolled devices. These can be applied to the same set of applications listed above.

Device based access rules (Preview):

- All devices must be compliant
- Only selected devices must be compliant, other devices will be allowed access
 - Android
 - iOS
 - Windows Mobile
 - Windows
- Application enforcement:
 - For browser and native applications
 - For only native applications

Manage more device platforms and types: Android, iOS, Mac OS X, Windows phones and desktops. Block access from unsupported devices.

Deploy apps, including LOB apps.

Configure finer-grain control of access to corporate resources by configuring policies.

Types of policies:

- **Configuration** — manage security settings and features on devices.
- **Device compliance** — Define rules and settings that a device must comply with.
- **Conditional access** — Secure access to email and other services, depending on conditions that you specify.

Policies are typically used in combination. For example, define compliance policies and then define conditional access policies that require compliance.

Conditional access policies are defined by application:

- Dynamics CRM Online
- Exchange Online
- SharePoint Online & OneDrive for Business
- Skype for Business Online

Continued on next page

Capability support for mobile platforms and applications

Microsoft continues to enhance support for mobile platforms and applications. Check the official product documentation for updates.

	These capabilities require device enrollment						
	Office 365 basic access policies for Exchange Online and SharePoint Online	Office 365 MFA	Azure AD Premium MFA. Enabled by user account. Location-based rules for MFA apply per SaaS app	Intune MAM policies for mobile apps	Office 365 MDM basic controls	Azure AD Premium device-based access rules. Configured per SaaS app	Intune device management and conditional access policies
Android	✓	✓	✓	✓	✓	✓	✓
iOS	✓	✓	✓	✓	✓	✓	✓
Mac OS X	✓	✓	✓				✓*
Windows Phone	✓	✓	✓		✓	✓	✓
Windows desktop	✓	✓	✓		✓	✓	✓
Other platforms	✓	✓	✓				
Restrictions		Only applies to Office 365 applications	If MFA is not enabled for a user, the application-based MFA policies don't apply to the user and their access is not affected.	Unsupported platforms are unrestricted.	Unsupported platforms are unrestricted.		Unsupported platforms can be blocked * Mac OS X is supported for device policies but not for conditional access.
Applications	Exchange Online SharePoint Online	Exchange Online SharePoint Online Outlook Groups OneDrive for Business Skype for Business Online Client applications	Microsoft Power BI Exchange Online SharePoint Online Yammer Outlook Groups Skype for Business Online Other SaaS apps in your environment that are configured for Azure AD single sign-on On-premises applications you publish using Azure AD Application Proxy	Microsoft Dynamics CRM Outlook Groups Managed Browser Skype for Business Excel Outlook PowerPoint Word OneNote Remote Desktop Microsoft SharePoint OneDrive Yammer	Application support varies by platform Supported devices and applications	Microsoft Power BI Exchange Online SharePoint Online Yammer Outlook Groups Skype for Business Online Other SaaS apps in your environment that are configured for Azure AD single sign-on On-premises applications you publish using Azure AD Application Proxy	Dynamics CRM Online Exchange Online Exchange On-premises SharePoint Online & OneDrive for Business Skype for Business Online

Testing access management capabilities in a lab environment

You can evaluate and test all of these features in a test lab environment. Click on each box to link to the test lab guide. [See all test lab guides.](#)



To evaluate and test capabilities in a lightweight environment, use these Test Lab Guides.

1 [Office 365 dev/test environment](#)

Setup an Office 365 E5 trial subscription

2 [Office 365 and EMS dev/test environment](#)

Add an Enterprise Mobility suite (EMS) trial subscription

3 [MAM policies for your Office 365 and EMS dev/test environment](#)

Create MAM policies for iOS and Android devices

4 [Enroll and manage iOS and Android devices with Intune](#)

Enroll and manage these devices remotely

To evaluate and test capabilities with simulation of enterprise identity synchronization, use these Test Lab Guides.

1 [Base configuration test environment](#)

Create a simplified intranet running Azure in a infrastructure with a domain controller

2 [Office 365 dev/test environment](#)

Setup an Office 365 E5 trial subscription

3 [DirSync for your Office 365 dev/test environment](#)

Run Azure AD Connect for directory synchronization

4 [Office 365 and EMS dev/test environment](#)

Add an Enterprise Mobility suite (EMS) trial subscription

5 [MAM policies for your Office 365 and EMS dev/test environment](#)

Create MAM policies for iOS and Android devices

6 [Enroll and manage iOS and Android devices with Intune](#)

Enroll and manage these devices remotely