Microsoft-Mobilität und -Sicherheit für Enterprise-Architekten

Was IT-Architekten über die Mobilität in Microsoft-Cloud-Diensten und -Plattformen wissen müssen

Dieses Thema ist 1 von 4 in einer Reihe. 1 2 3 4

Bereitstellen von Produktivität und Zusammenarbeit von beliebigen Orten aus bei gleichzeitigem Schutz von Daten und Anwendungen

Microsoft bietet Unterstützung für mobile Produktivität auf breiter Front, die Unterstützung für Anwendungen und umfassende Funktionen zum Steuern des Zugriffs auf die Bestände Ihrer Organisation beinhaltet.

Mobile Apps von Microsoft für Unternehmen

Microsoft stellt eine Reihe von mobilen Apps auf Unternehmensniveau zur Steigerung der Produktivität her. Die empfohlenen Anwendungen finden Sie auf Seite 2.

Mit einem Office 365 Business-Abonnement erhalten Sie mobile Apps, um an Ihrem bevorzugten Gerät mehr erledigen zu können. Dabei sind Ihre Daten stets geschützt. Zusätzliche Sicherheit bei der Verwendung dieser mobilen Anwendungen bietet Ihnen die mobile Anwendungsverwaltung mit Intune.

Skype for Business, Yammer, OneNote und weitere Business-Apps sind ebenfalls verfügbar. Rufen Sie die vollständige Liste der Apps ab, und erfahren Sie alles zur Installation auf Ihren Geräten.

Dynamics CRM enthält darüber hinaus Apps für Smartphones und Tablets.

Cloud-App-Sicherheit für SaaS-Apps

Microsoft Cloud App Security ist ein umfassender Dienst, der vertiefte Sichtbarkeit, umfassende Steuerungsmöglichkeiten und verbesserten Schutz für Ihre Cloudanwendungen bietet.

App-Ermittlung	Identifizieren Sie alle Cloudanwendungen in Ihrem Netzwerk – von allen Geräten – und werten Sie Risikobewertungen und die fortlaufende Risikobeurteilung und -analyse aus. Erfordert keine Agents.
Datenkontrolle	Genehmigen Sie Apps. Legen Sie fein abgestufte Kontrollen und Richtlinien für Datenfreigabe und DLP fest.
Threat Protection	Identifizieren Sie riskante Nutzungsmuster, Sicherheitsvorfälle, und erkennen Sie anormales Benutzerverwalten, um Bedrohungen zu vermeiden.

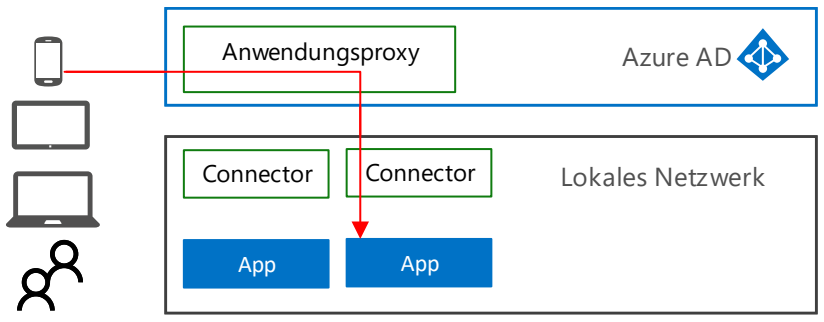
Entwickeln eigener mobiler Apps

Verwenden Sie das Feature "Mobile Apps" von Azure App Service, um fesselnde iOS-, Android- und Windows-Apps oder plattformübergreifende Xamarin- oder Cordova-Apps (Phonegap) für Ihre Kunden und Ihr Unternehmen zu entwickeln.

- Pushübertragung mit Kundensegmentierung Einmaliges
- Anmelden für Unternehmen mit Active Directory
- Automatische Skalierung zur Unterstützung von Millionen von Geräten
- Möglichkeit zur Offline-Arbeit mit Apps und Synchronisierung
- Social-Integration mit Facebook, Twitter, Google

Mobiler Zugriff auf lokale Anwendungen

Mit dem Microsoft Azure Active Directory-Anwendungsproxy können Sie Anwendungen, wie etwa webbasierte Apps, innerhalb Ihres privaten Netzwerks veröffentlichen und Benutzern außerhalb Ihres Netzwerks sicheren Zugriff bieten. Sie können lokale Anwendungen mit den gleichen Anforderungen wie andere cloudbasierte Anwendungen mit MFA, Geräteanforderungen und anderen Anforderungen für den bedingten Zugriff schützen.



Verwalten des Zugriffs auf cloudbasierte Anwendungen und Daten von mobilen Geräten

Microsoft bietet eine Reihe von Funktionen, die Sie zum Steuern des Zugriffs auf Anwendungen und Daten von mobilen Geräten verwenden können.

Office 365

Grundfunktionen für Office 365-Anwendungen

Mehrstufige Authentifizierung für Office 365-Anwendungen.

Einfache Steuerelemente für den Zugriff auf Exchange Online und SharePoint Online.

Einfache Funktionen zur mobilen Geräteverwaltung (MDM).

Enterprise Mobility + Security (EMS)

Azure AD Premium

Steuern des Zugriffs auf Anwendungen auf der Grundlage von Benutzerkonten und Gruppen

Mehrstufige Authentifizierung mit benutzer-, standort- und gerätebasierten Regeln für SaaS-Anwendungen in Ihrer Umgebung.

Erweiterter Schutz mit risikobezogener adaptiver Zugriffssteuerung.

Einmaliges Anmelden an allen SaaS-Apps in Ihrer Umgebung.

Microsoft Intune

Steuerelemente zum Verwalten von mobilen Anwendungen, Geräten und PCs

Richtlinien für mobile Anwendungen (MAM) für mobile Geräte.

Gerätebezogene Verwaltung, Konfigurationskompatibilität und bedingter Zugriff.

Bereitstellung und Verwaltung von Apps auf mobilen Geräten und PCs.

Azure Information Protection

Richtlinien für Verschlüsselung, Klassifizierung, Bezeichnung, Identität und Autorisierung werden auf E-Mails und Dateien angewendet

Vormals "Azure Rights Management (RMS)".Schützen Sie Zieldatasets mit RMS-Richtlinien.

Alle Dateitypen werden unterstützt.Der Schutz von Dateien bleibt aktiv, unabhängig vom Speicherort der Dateien.

Unterstützung für lokale Dienste sowie für Office 365.

September 2016

Microsoft

Microsoft-Mobilität und -Sicherheit für Enterprise-Architekten

Was IT-Architekten über die Mobilität in Microsoft-Cloud-Diensten und -Plattformen wissen müssen

Empfohlene Apps für Mobilgeräte

Microsoft Office-Apps

Überprüfen, bearbeiten, analysieren und präsentieren Sie mit einer konsistenten und vertrauten Benutzeroberfläche, die für die Verwendung auf Ihrem mobilen Gerät optimiert ist. Die Kernfunktionen zur Bearbeitung sind für Endverbraucher auf Geräten mit Bildschirmgrößen unterhalb 10,1" kostenlos.

[Zusätzliche Features auf Ihrem iPad* und iPhone mit Office 365]

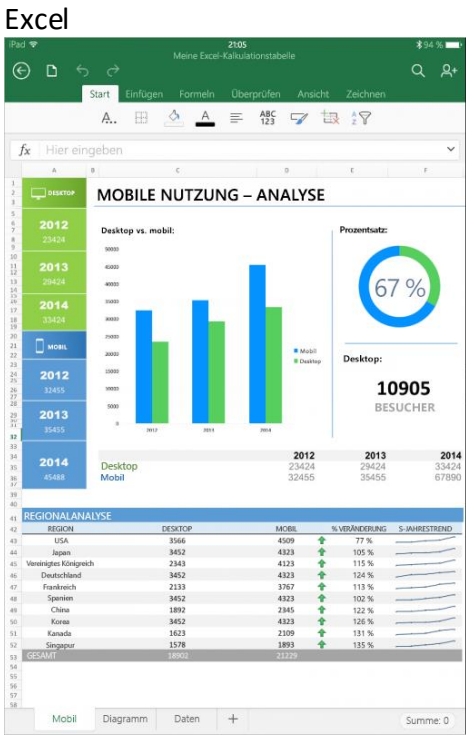
[Zusätzliche Features auf Ihrem Android-Tablet und -Smartphone mit Office 365]

[Zusätzliche Features auf Ihrem Windows Phone und Windows-Tablet mit Office 365]

[Erweiterte Verwaltung von Informationsrechten in den mobilen Apps von Word, Excel und PowerPoint]

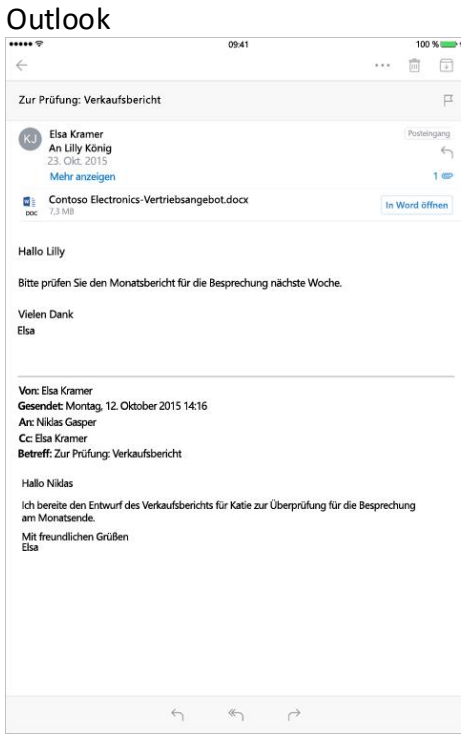
[Azure RMS-Anforderungen: Anwendungen]

Excel



PowerPoint

Outlook



Word

OneNote

Tippen Sie, schreiben Sie mit der Hand, zeichnen Sie, und schneiden Sie Sachen im Web aus, um Ihre Gedanken in Ihrem Notizbuch festzuhalten. Verwenden Sie die flexible Zeichnungsfläche von OneNote, um Inhalte beliebig zu platzieren. Sie können sogar handschriftliche Notizen oder Seiten direkt in OneNote scannen und sie dann durchsuchbar machen.

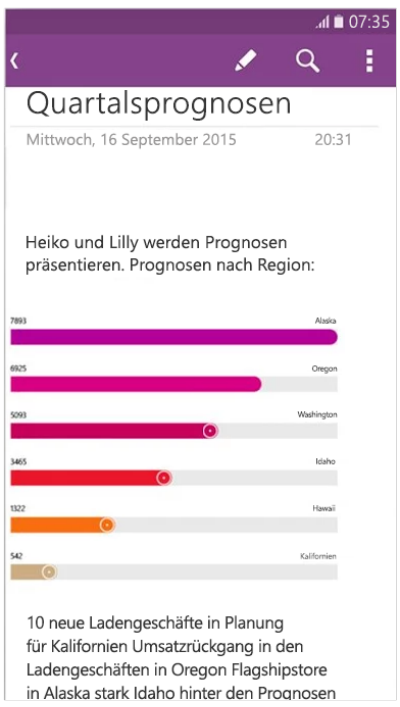
https://www.onenote.com/

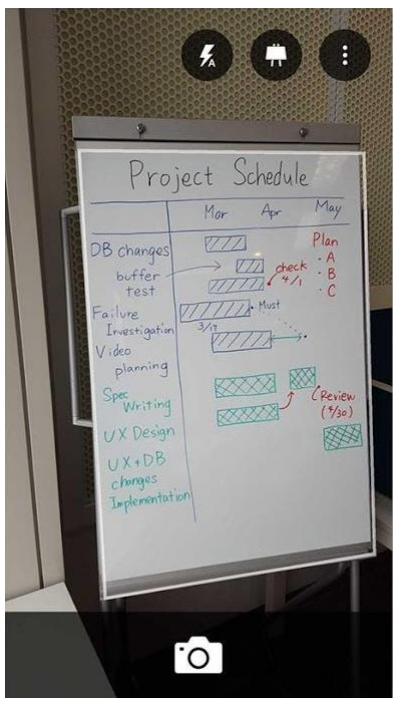
[OneNote auf einem Smartphone oder mobilen Gerät installieren]

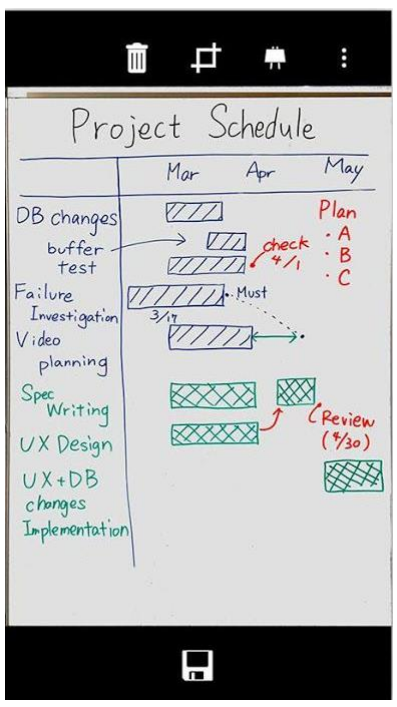
Office Lens

Office Lens beschneidet und verbessert Bilder von Whiteboards und Dokumenten und macht sie lesbar. Mithilfe von Office Lens können Sie Bilder in PDF-, Word- und PowerPoint-Dateien umwandeln oder sie sogar in OneNote oder auf OneDrive speichern.

[Office Lens ist auf iPhone und Android verfügbar]







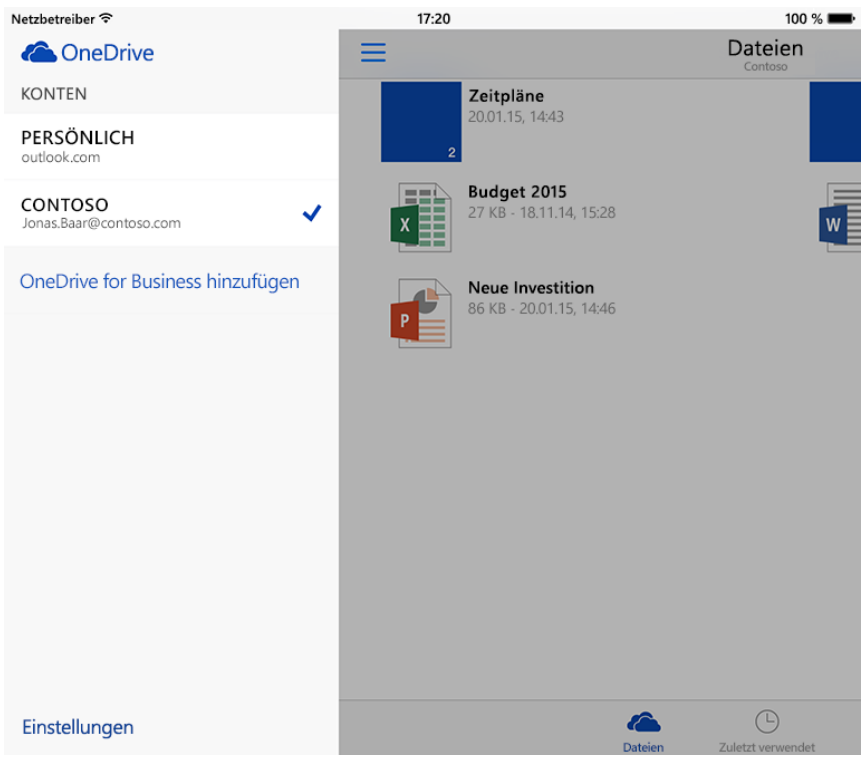
Fortsetzung auf der nächsten Seite

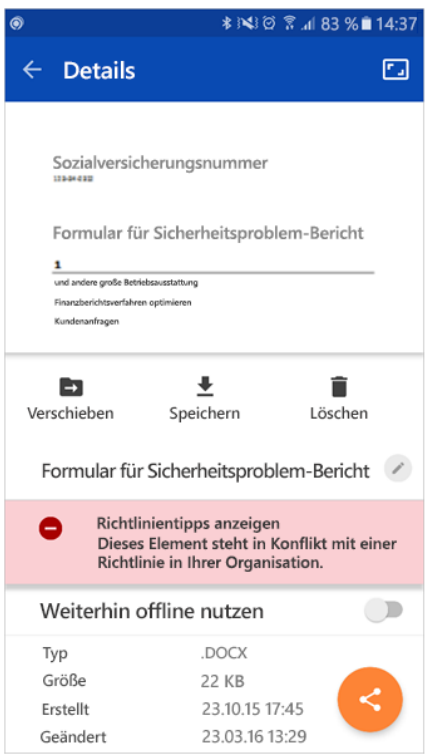
Mobile OneDrive-App

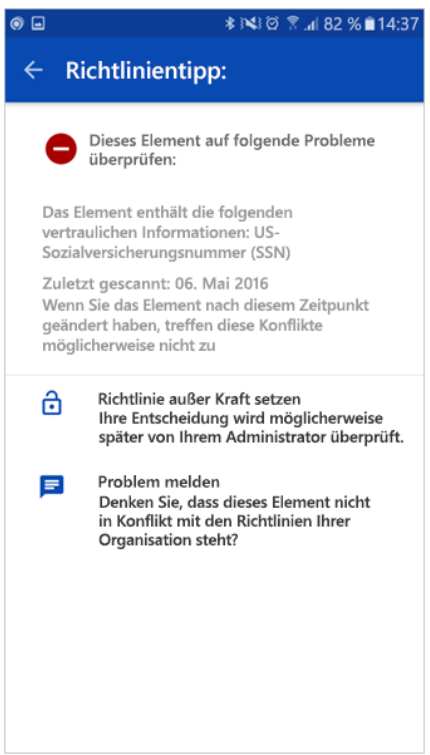
Verwenden Sie die gleiche App für Ihr Arbeits- und Ihr Privatkonto. Weitere Konten können hinzugefügt werden.

[OneDrive for Business auf Ihrem Smartphone oder Tablet einrichten]

Konfigurieren Sie [Tipps für Richtlinien zur Verhinderung von Datenverlust für mobile OneDrive-Apps]. In OneDrive for Business gespeicherte Dokumente werden nach vertraulichen Informationen durchsucht und im Vergleich mit den in Office 365 konfigurierten Unternehmensrichtlinien beurteilt. In den Office 365-Plänen E3 und E5 enthalten.







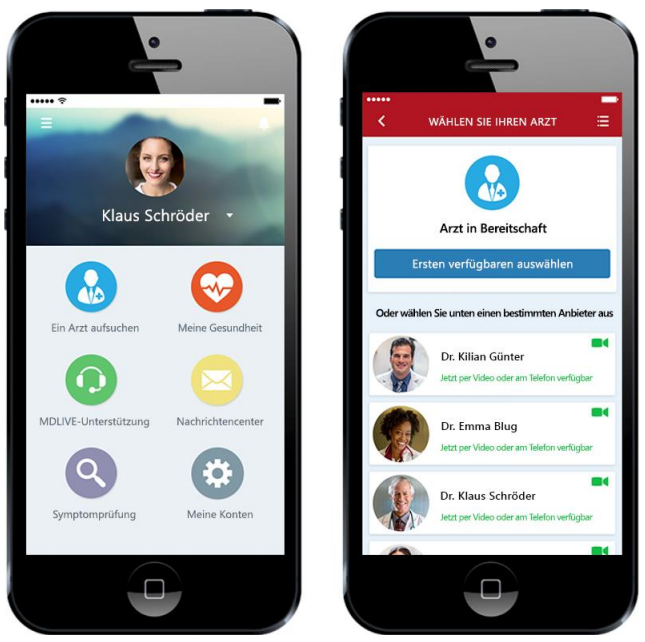
Mobile Skype for Business-App

Stellen Sie mit Skype for Business überall Verbindungen mit Ihrem Team her, und verwenden Sie Clients unter Windows, Mac, iOS und Android™, oder bringen Sie Remoteteilnehmer in Besprechungsräume jeder Größe.

[Skype for Business für alle Ihre Geräte herunterladen]

Fügen Sie Skype for Business Ihren mobilen Apps hinzu

Die [Skype for Business App-SDK-Vorschau] steht jetzt zum Download bereit. Mit diesem neuen SDK können Entwickler Chat, sowie Audio- und Video-Benutzererfahrungen nahtlos in ihre maßgeschneiderten iOS- und Android-Anwendungen integrieren.



Office Delve für Android

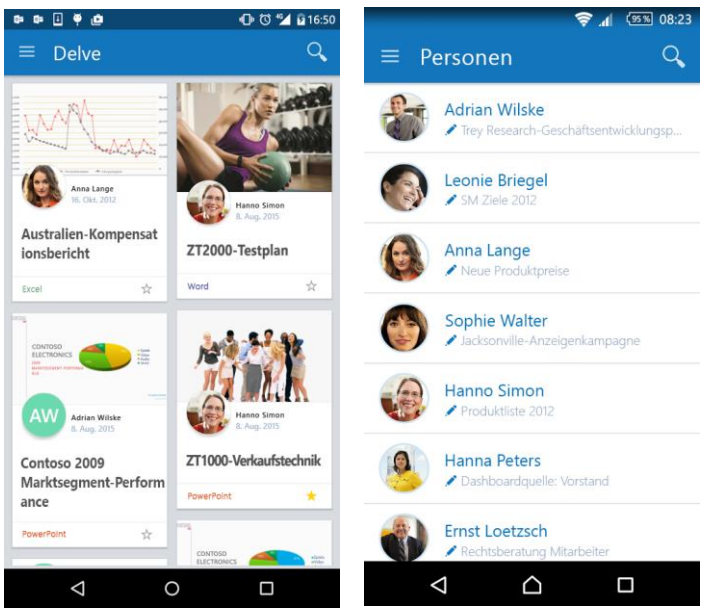
[Verwenden Sie Delve], um zu sehen, woran Sie und Ihre Kollegen innerhalb von Office 365 arbeiten. Basierend auf den Personen, mit denen Sie zusammenarbeiten und der Art der Zusammenarbeit schlägt Delve Ihnen Dokumente vor, die für Sie relevant sind.

Wichtige Leistungsmerkmale:

- Entdecken neuer Informationen
- Suchen von Dokumenten anhand von Personen
- Rückkehr zu Dokumenten, an denen Sie arbeiten

In Delve sehen Sie nur Inhalte, die für Sie freigegeben wurden. Dies bedeutet, dass Ihre Kollegen Ihre privaten Dokumente nicht sehen und Sie nicht ihre.

WICHTIG: Sie können diese App nur verwenden, wenn Ihre Organisation Office 365 und Delve einsetzt.



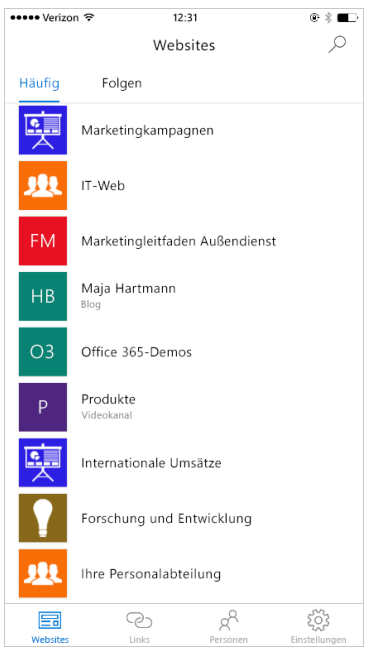
Fortsetzung auf der nächsten Seite

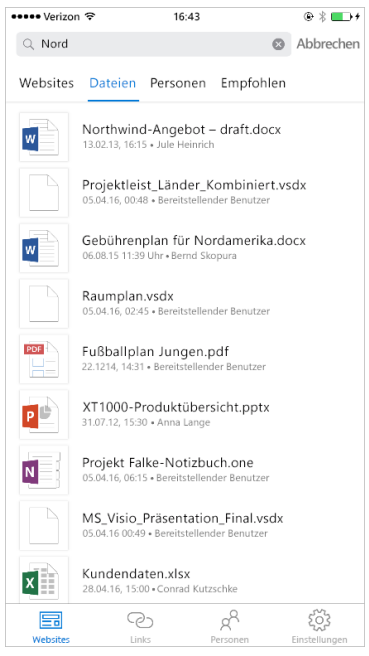
Mobile SharePoint-App

Navigieren Sie auf SharePoint-Websites, zeigen Sie Links zu Websites an, die Ihre Organisation als wichtig gekennzeichnet hat, sehen Sie Personenprofile ein, und suchen Sie nach Personen, Websites und Dokumenten.

Erste Schritte mit der mobilen SharePoint-App Ab dem Juni 2016 im Apple App Store verfügbar. Android- und Windows-Versionen folgen.

Außerdem: Verwenden von mobilen Geräten zum Arbeiten mit SharePoint Online-Websites





Mobile Yammer-App

Bleiben Sie bei Unterhaltungen auf dem Laufenden, veröffentlichen Sie Updates, und arbeiten Sie mit Ihrem Team zusammen, ganz gleich, an welchem Ort der Welt Sie sich aufhalten.

Die Yammer-App herunterladen

Office 365 Admin-App

Verwalten Sie Office 365 von jedem beliebigen Ort aus. Die Office 365 Admin-App ermöglicht Ihnen den Empfang von Benachrichtigungen, das Hinzufügen von Benutzern, das Zurücksetzen von Kennwörtern, das Erstellen von Supportanfragen und mehr von unterwegs.

Weitere Informationen und Download der App

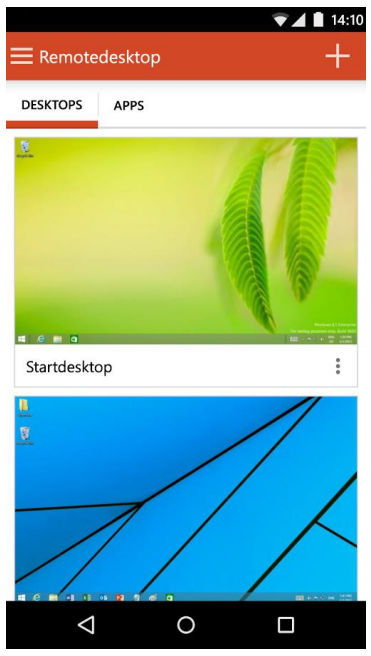
Microsoft-Remotedesktop

Mit der Microsoft-Remotedesktop-App können Sie sich von praktisch überall aus mit einem Remote-PC und Ihren Arbeitsressourcen verbinden.

Google Play (Android)

Apple Store

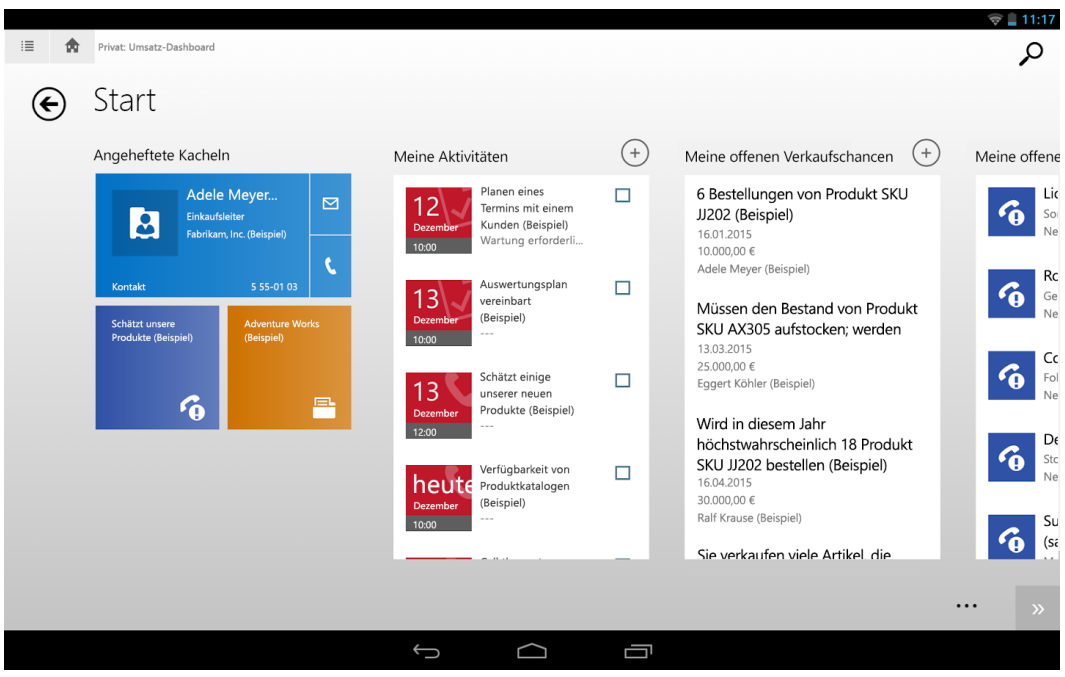
Microsoft Store

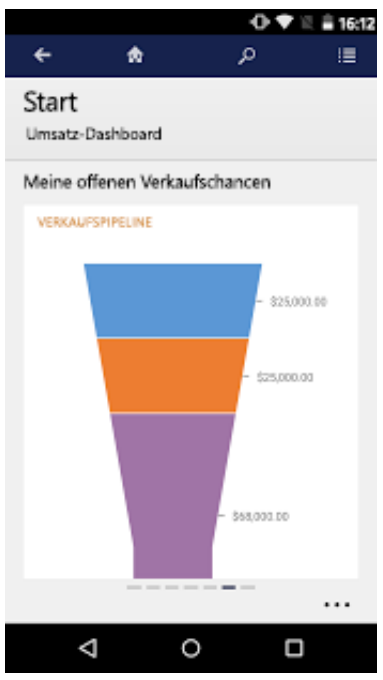


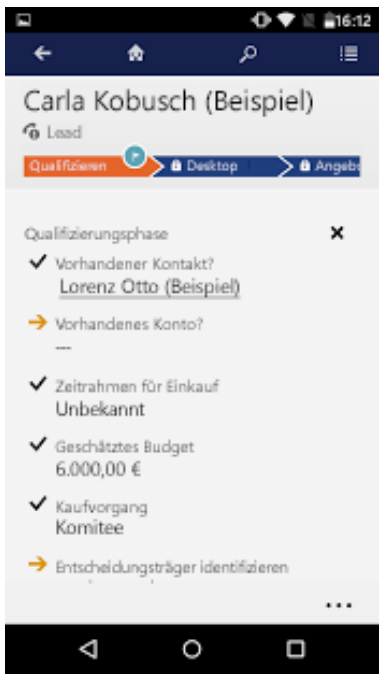
Dynamics CRM für Smartphones und Tablets

Bleiben Sie unterwegs mit den Microsoft Dynamics CRM für Smartphones- und Microsoft Dynamics CRM für Tablets-Apps über Ihre Kontakte, Leads und Aktivitäten auf dem Laufenden. Smartphone und Tablet bieten Ihnen die gleiche intuitive Benutzererfahrung.

Dynamics CRM-Entwickler: Erstellen Sie eigene mobile Apps für Windows, iOS und Android







Microsoft

Microsoft-Mobilität und -Sicherheit für Enterprise-Architekten

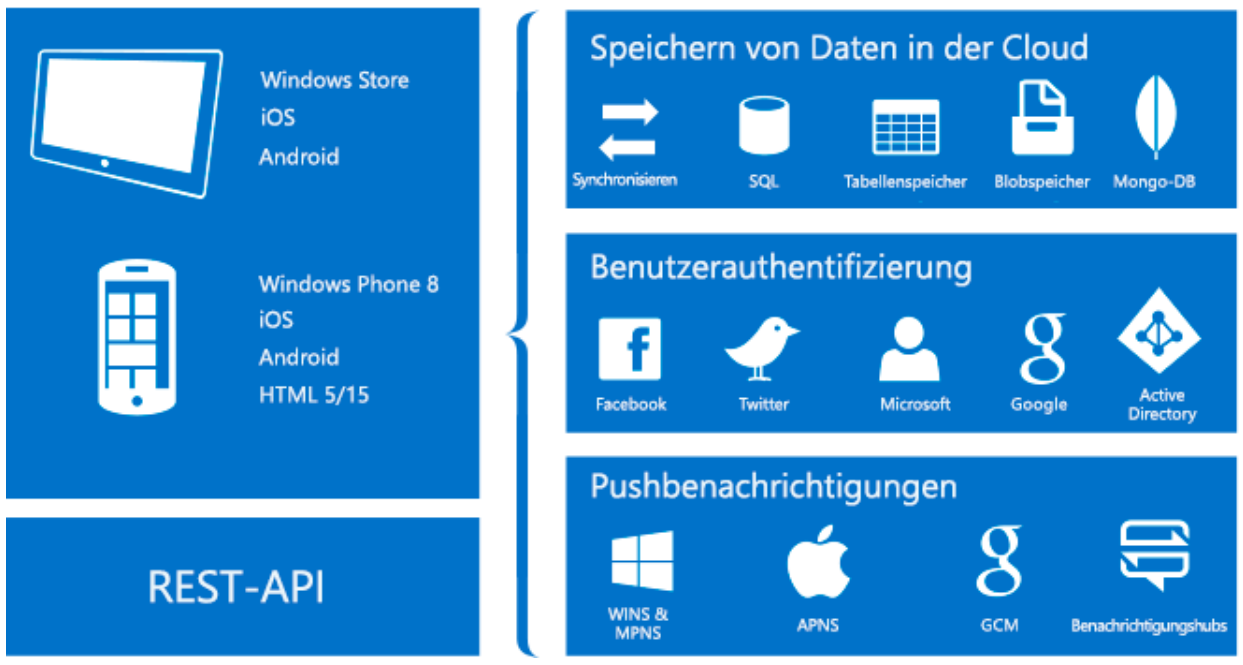
Was IT-Architekten über die Mobilität in Microsoft-Cloud-Diensten und -Plattformen wissen müssen

Dieses Thema ist 3 von 4 in einer Reihe. 1 2 **3** 4

Entwicklung von mobilen Apps

Mit dem Feature Mobile Apps von Azure App Service können Sie schnell fesselnde plattformübergreifende und native Apps für iOS, Android, Windows oder Mac erstellen, App-Daten in der Cloud oder lokal speichern, Benutzer authentifizieren, Pushbenachrichtigungen senden oder eigene, benutzerdefinierte Back-End-Logik in C# oder Node.js hinzufügen.

Azure App Service ist ein vollständig verwaltetes PaaS-Angebot (Platform as a Service) für professionelle Entwickler, das eine umfangreiche Sammlung von Funktionen für Web-, mobile und Integrationsszenarien mitbringt. Mobile Apps in Azure App Service bieten eine hochgradig skalierbare, global verfügbare Plattform für die Entwicklung von mobilen Anwendungen für Enterprise-Entwickler und Systemintegratoren.



Erstellen von nativen und plattformübergreifenden Apps

Erstellen Sie native iOS-, Android- und Windows-Apps oder plattformübergreifende Xamarin- oder Cordova-Apps (Phonegap). Nutzen Sie App Service mithilfe von nativen SDKs.

Stellen Sie Verbindungen mit den Systemen Ihres Unternehmens her

Mit Mobile Apps können Sie die Firmenanmeldung innerhalb von Minuten hinzufügen und Verbindungen mit den lokalen oder Cloudressourcen Ihres Unternehmens herstellen.

Erstellen von offlinefähigen Apps mit Datensynchronisierung

Machen Sie Ihre mobile Belegschaft produktiv, indem Sie Apps erstellen, die offline funktionieren und Daten mithilfe von Mobile Apps im Hintergrund mit beliebigen Unternehmensdatenquellen oder SaaS-APIs synchronisieren, wenn Verbindungen verfügbar sind.

Pushbenachrichtigungen an Millionen in Sekunden

Fesseln Sie Ihre Benutzer und Kunden mit sofortigen Pushbenachrichtigungen auf beliebigen Geräten, die ihren Anforderungen gemäß gestaltet sind und zur richtigen Zeit gesendet werden.

App Service Mobile Apps – Funktionen und Dokumentation

Durch Klicken auf die einzelnen Felder erhalten Sie weitere Informationen

- **Ausprobieren und mehr erfahren**
  - Erstellen einer mobilen App in Sekunden ohne Registrierung
  - Was sind Mobile Apps?
  - App Services im Vergleich mit Mobile Apps
- **Erste Schritte**
  - Erstellen einer mobilen App
  - Hinzufügen von Offlinesynchronisierung zu Ihrer App
  - Hinzufügen von Authentifizierung zu Ihrer App
  - Hinzufügen von Pushbenachrichtigungen zu Ihrer App
- **Entwickeln**
  - Arbeiten mit einem .NET-Back-End
  - Arbeiten mit einem Node.js-Back-End
  - Entwickeln von Android-Apps
  - Entwickeln von Cordova-Apps
  - Entwickeln von HTML/JavaScript-Apps
  - Entwickeln von iOS-Apps
  - Entwickeln von Windows- und Xamarin-Apps
  - Versionsverwaltung für Clients und Server
- **Bereitstellen**
  - Bereitstellungsoptionen
  - Bereitstellen mithilfe von Powershell
  - Bereitstellen in Stagingslots und Wechseln zur Produktionsumgebung
  - Continuous Deployment
  - Hinzufügen von Skype for Business zu Ihrer mobilen App
- **Verwalten**
  - Managementgrundlagen
  - Konfigurieren eines benutzerdefinierten Domänennamens
  - Skalieren der Anwendung
  - Sichern der Anwendung
  - Wiederherstellen der Anwendung aus einer Sicherung
- **Überwachen**
  - Überwachungsgrundlagen
  - Aktivieren von Diagnoseprotokollierung
  - Behandeln von Problemen mit Visual Studio
- **Optimieren und Erweitern**
  - Arbeiten mit Offlinedaten
  - Authentifizieren von Benutzern
  - Senden von Pushbenachrichtigungen
  - Synchronisieren von Images mithilfe von Blobspeicher
  - Steuerung des globalen Datenverkehrs mit Traffic Manager
  - Zugriff auf lokale Ressourcen

Microsoft-Mobilität und -Sicherheit für Enterprise-Architekten

Was IT-Architekten über die Mobilität in Microsoft-Cloud-Diensten und -Plattformen wissen müssen

Steuern des Zugriffs auf Anwendungen und Schutz von Daten auf mobilen Geräten

Funktionen für die Zugriffssteuerung nach Produkt

Weitere Informationen finden Sie unter Steuern des Zugriffs auf Office 365 und Schutz von Inhalten auf Geräten

	Office 365	Azure AD Premium	Microsoft Intune
BYOD (nicht registriert)	Exchange Online – Konfigurieren von grundlegenden Kennwortrichtlinien für Outlook Web Access (OWA). SharePoint Online – Konfigurieren von grundlegenden Richtlinien für den externen Zugriff auf SharePoint-Websites.	Einmaliges Anmelden an allen SaaS-Apps in Ihrer Umgebung. Mehrstufige Authentifizierung (MFA) – Aktivierung auf Benutzerbasis. Richtlinien für den bedingten Zugriff – Konfiguration auf Anwendungsbasis. Die Richtlinien können sich je nach Anwendung unterscheiden. Häufig verwendete Richtlinien sind unten aufgelistet. **Mehrstufige Authentifizierung und standortbezogene Zugriffsregeln**: • Anwenden von Regeln auf alle Benutzer oder spezifische Gruppen • Mehrstufige Authentifizierung vorschreiben • Mehrstufige Authentifizierung bei Nutzung fern vom Arbeitsplatz vorschreiben • Blockieren des Zugriffs bei Abwesenheit am Arbeitsplatz Zu den Anwendungen, die mithilfe von Azure AD Premium für den bedingten Zugriff konfiguriert werden können, gehören: • Microsoft Power BI • Exchange Online • SharePoint Online • Yammer Online • Outlook Groups • Skype for Business • Andere SaaS-Apps in Ihrer Umgebung, die für Einmaliges Anmelden bei Azure AD konfiguriert sind	Senden einer Zurücksetzungsanforderung. Konfigurieren von Richtlinien zur mobilen Anwendungsverwaltung (MAM) nach Plattform (ohne Geräteregistrierung): • iOS • Android Auswählen, auf welche Anwendungen eine Richtlinie angewendet werden soll, anschließend Konfigurieren der Richtlinienregeln. Beispieleinstellungen für iOS: • Verhindern von Sicherungen mithilfe von iTunes und iCloud • Zulassen der Übertragung von Daten durch die App an andere Apps • Zulassen des Empfangs von Daten von anderen Apps durch die App • Verhindern von "Speichern unter" Einschränken von Ausschneiden, Kopieren und Einfügen mit anderen Apps • Einschränken der Anzeige von Webinhalten im verwalteten Browser • Verschlüsseln von App-Daten • Deaktivieren der Synchronisierung von Kontakten • Vorschreiben einer PIN für den Zugriff (mit zusätzlichen Einstellungen) • Vorschreiben von Firmenanmeldeinformationen für den Zugriff • Blockieren der Ausführung von verwalteten Apps auf Geräten mit entfernten Nutzungsbeschränkungen • Erneute Überprüfung der Zugriffsanforderungen (Timeout und Offlinekarenzzeit) • Offlineintervall (Tage) vor dem Löschen der App-Daten Diese Einstellungen betreffen auch Geräte im Firmenbesitz.

Registrierte Geräte	Registrieren von Geräten und Konfigurieren von grundlegenden Zugriffskontrollen:
	• Anforderungen für Kennwörter, Anmeldeversuche, Timeoutsperren und Fehler bei der Gerätezurücksetzung nach dem Anmelden
	• Verschlüsselung vorschreiben
	• Ausschließen von Geräten mit entfernten Nutzungsbeschränkungen
	• Melden von Verstößen
	
	Zusätzliche Sicherheitsrichtlinien:
	• Verschlüsselte Sicherung vorschreiben
	• Cloud-Sicherung blockieren
	• Dokumentsynchronisierung blockieren
	• Screenshots blockieren
	• Videokonferenzen auf Gerät blockieren
	• Senden von Diagnosedaten von Geräten aus blockieren
	• Zugriff auf App Store blockieren
	• Kennwort beim Zugriff auf App Store anfordern
	• Verbindung mit Wechselmedien blockieren
	• Bluetooth-Verbindung blockieren
		Gerätebezogene Regeln für den bedingten Zugriff bauen auf Intune-Kompatibilitätsrichtlinien auf und gelten für registrierte Geräte. Sie können auf den gleichen Satz Anwendungen angewendet werden, der oben aufgelistet ist.
		Gerätebezogene Zugriffsregeln (Vorschau):
		• Alle Geräte müssen kompatibel sein.
		• Nur die ausgewählten Geräte müssen kompatibel sein, anderen Geräten wird der Zugriff erlaubt
		  ○ Android
		  ○ iOS
		  ○ Windows Mobile
		  ○ Windows
		• Durchsetzen der Anwendung:
		  ○ Für Browser- und native Anwendungen
		  ○ Nur für native Anwendungen
			Verwalten von mehr Geräteplattformen und Typen:Android, iOS, Mac OS X, Windows Phones und Windows Desktopcomputer. Zugriff von nicht unterstützten Geräten blockieren.
			
			Bereitstellen von Apps, einschließlich Branchenanwendungen.
			
			Konfigurieren einer feiner abgestuften Zugriffssteuerung auf Unternehmensressourcen durch Konfiguration von Richtlinien.
			
			Richtlinientypen:
			• **Konfiguration** – Verwalten von Sicherheitseinstellungen und Funktionen auf Geräten.
			• **Gerätekompatibilität** – Definieren von Regeln und Einstellungen, denen ein Gerät entsprechen muss.
			• **Bedingter Zugriff** – Sicherer Zugriff auf E-Mail und andere Dienste nach von Ihnen festgelegten Bedingungen.
			
			Richtlinien werden normalerweise kombiniert angewendet. Definieren Sie beispielsweise Kompatibilitätsrichtlinien und anschließend Richtlinien für den bedingten Zugriff, die Kompatibilität voraussetzen. Richtlinien für den bedingten
			
			Zugriff werden nach Anwendung definiert:
			• Dynamics CRM Online
			• Exchange Online
			• SharePoint Online und OneDrive for Business
			• Skype for Business Online

Fortsetzung auf der nächsten Seite

Unterstützte Funktionen für mobile Plattformen und Anwendungen

Microsoft verbessert die Unterstützung für mobile Plattformen und Anwendungen fortlaufend. Informationen zu verfügbaren Updates finden Sie in der offiziellen Produktdokumentation.

					Für diese Funktionen ist eine Geräteregistrierung erforderlich		
	Grundlegende Zugriffsrichtlinien in Office 365 für Exchange Online und SharePoint Online	Office 365 MFA	Azure AD Premium MFA. Durch das Benutzerkonto aktiviert. Standortbezogene Regeln für MFA werden mithilfe einer SaaS-App angewendet	Intune MAM-Richtlinien für mobile Apps	Grundlegende Office 365-MDM-Steuerelemente	Gerätebezogene Azure AD Premium-Zugriffsregeln. Mithilfe einer SaaS-App konfiguriert	Intune-Richtlinien für Gerätemanagement und bedingten Zugriff
Android	✓	✓	✓	✓	✓	✓	✓
iOS	✓	✓	✓	✓	✓	✓	✓
Mac OS X	✓	✓	✓				✓*
Windows Phone	✓	✓	✓		✓	✓	✓
Windows Desktop	✓	✓	✓		✓	✓	✓
Andere Plattformen	✓	✓	✓				
Einschränkungen		Gilt nur für Office 365-Anwendungen	Wenn MFA für einen Benutzer nicht aktiviert ist, werden die anwendungsbezogenen MFA-Richtlinien nicht auf den Benutzer angewendet und wirken sich nicht auf seinen Zugriff aus.	Nicht unterstützte Plattformen erfahren keine Einschränkung.	Nicht unterstützte Plattformen erfahren keine Einschränkung.		Nicht unterstützte Plattformen können gesperrt werden * Mac OS X wird hinsichtlich Geräterichtlinien, jedoch nicht im Hinblick auf bedingten Zugriff unterstützt.
Anwendungen	Exchange Online SharePoint Online	Exchange Online SharePoint Online Outlook Groups OneDrive for Business Skype for Business Online Clientanwendungen	Microsoft Power BI Exchange Online SharePoint Online Yammer Outlook Groups Skype for Business Online Andere SaaS-Apps in Ihrer Umgebung, die für Einmaliges Anmelden bei Azure AD konfiguriert sindLokale Anwendungen, die von Ihnen mithilfe des Azure AD-Anwendungsproxys veröffentlicht werden	Microsoft Dynamics CRM Outlook Groups Verwaltete Browser Skype for Business Excel Outlook PowerPoint Word OneNote Remotedesktop Microsoft SharePoint OneDrive Yammer	Der Anwendungssupport unterscheidet sich je nach Plattform Unterstützte Geräte und Anwendungen	Microsoft Power BI Exchange Online SharePoint Online Yammer Outlook Groups Skype for Business Online Andere SaaS-Apps in Ihrer Umgebung, die für Einmaliges Anmelden bei Azure AD konfiguriert sindLokale Anwendungen, die von Ihnen mithilfe des Azure AD-Anwendungsproxys veröffentlicht werden	Dynamics CRM Online Exchange Online Exchange lokal SharePoint Online und OneDrive for Business Skype for Business Online

Testen von Funktionen zur Zugriffsverwaltung in einer Laborumgebung

Sie können alle diese Funktionen in einer Laborumgebung testen und beurteilen. Durch Klicken auf die einzelnen Felder gelangen Sie zum betreffenden Testlaborhandbuch. Alle Testlaborhandbücher anzeigen.

Verwenden Sie diese Testlaborhandbücher, um Funktionen in einer schlanken Umgebung zu testen und zu beurteilen.

1. **Office 365 Dev/Test-Umgebung**
   Einrichten eines Office 365 E5-Testabonnements
2. **Office 365- und EMS-Dev/Test-Umgebung**
   Hinzufügen eines EMS-Testabonnements (Enterprise Mobility Suite)
3. **MAM-Richtlinien für Ihre Office 365- und EMS-Dev/Test-Umgebung**
   Erstellen von MAM-Richtlinien für iOS- und Android-Geräte
4. **Registrieren und Verwalten von iOS- und Android-Geräten mit Intune**
   Remoteregistrierung und -verwaltung dieser Geräte

Verwenden Sie diese Testlaborhandbücher, um Funktionen mit einer Simulation der Identitätssynchronisierung im Unternehmen zu testen und zu beurteilen.

1. **Standardkonfigurations-Testumgebung**
   Erstellen eines vereinfachten Intranets, das eine Azure-Infrastruktur mit einem Domänencontroller ausführt
2. **Office 365 Dev/Test-Umgebung**Einrichten eines Office 365 E5-Testabonnements
3. **Verzeichnissynchronisierung für Ihre Office 365 Dev/Test-Umgebung**
   Ausführen von Azure AD Connect für die Verzeichnissynchronisierung
4. **Office 365- und EMS-Dev/Test-Umgebung**
   Hinzufügen eines EMS-Testabonnements (Enterprise Mobility Suite)
5. **MAM-Richtlinien für Ihre Office 365- und EMS-Dev/Test-Umgebung**
   Erstellen von MAM-Richtlinien für iOS- und Android-Geräte
6. **Registrieren und Verwalten von iOS- und Android-Geräten mit Intune**
   Remoteregistrierung und -verwaltung dieser Geräte