|  |  |
| --- | --- |
|  | Microsoft Enterprise Mobility |
|  | Hero Demo Guide |
|  | Updated: April, 2016 |

This document is provided “as-is”. Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

© 2016 Microsoft. All rights reserved.

Table of Contents

[EMS Demo Requirements and Scenarios 5](#_Toc448995746)

[Demo Pre-Requisites 5](#_Toc448995747)

[Scenario 1: Manage Mobile Productivity 5](#_Toc448995748)

[Scenario 2: Deploy and Manage All of Your Applications Using Enterprise Mobility 5](#_Toc448995749)

[Scenario 3: Comprehensive Protection of Your Corporate Data with EMS 6](#_Toc448995750)

[Demo 1: Manage Mobile Productivity 7](#_Toc448995751)

[Pre-Demo Checklist 7](#_Toc448995752)

[Demo Sequence 7](#_Toc448995753)

[Opening 7](#_Toc448995754)

[Managing Office Mobile Apps without Device Enrollment 8](#_Toc448995755)

[Conditional Access and Device Enrollment 8](#_Toc448995756)

[Mobile Application Management 10](#_Toc448995757)

[Demo Reset Instructions 12](#_Toc448995758)

[Demo 2: Deploy and Manage All of Your Apps with EMS 13](#_Toc448995759)

[Pre-Demo Checklist 13](#_Toc448995760)

[Demo Sequence 13](#_Toc448995761)

[Add SaaS Apps: Salesforce 13](#_Toc448995762)

[Add an App and Configure SSO: Twitter 14](#_Toc448995763)

[Use MyApps to Access Applications 15](#_Toc448995764)

[Self-Service on MyApps Portal 16](#_Toc448995765)

[Access to Windows-based Apps 16](#_Toc448995766)

[Close 17](#_Toc448995767)

[Demo Reset 17](#_Toc448995768)

[Demo 3: Comprehensive Protection of Corporate Data with EMS 18](#_Toc448995769)

[Pre-Demo Checklist 18](#_Toc448995770)

[Demo Sequence 18](#_Toc448995771)

[Use MyApps to Access Applications 18](#_Toc448995772)

[Review Azure Security Reports 19](#_Toc448995773)

[Microsoft Advanced Threat Analytics 21](#_Toc448995774)

[Introducing Microsoft Cloud App Security 23](#_Toc448995775)

[Demo Reset 28](#_Toc448995776)

[Appendix 1: Configure your Demo Tenant 28](#_Toc448995777)

[Add Your Authentication Phone and Email (for MFA verification) to Hero User 28](#_Toc448995778)

[Grant EMS License to Global Admin user 29](#_Toc448995779)

[Configuring Tenant for iOS Devices 29](#_Toc448995780)

[Create an Apple ID for Your Demo Tenant (if necessary) 29](#_Toc448995781)

[Configure Intune Admin Settings for iOS Device Management 30](#_Toc448995782)

[Apply Contoso Branding to Intune Company Portal 32](#_Toc448995783)

[Create an App Policy for MAM without Enrollment 32](#_Toc448995784)

[Add SaaS Applications to AAD 33](#_Toc448995785)

[Configure Salesforce SSO Integration 34](#_Toc448995786)

[Configure Twitter Integration 40](#_Toc448995787)

[Appendix 2: Installing/Configuring Azure RemoteApp (ARA) 42](#_Toc448995788)

[Installing Azure RemoteApp 42](#_Toc448995789)

[Configuring Azure RemoteApp 43](#_Toc448995790)

[Appendix 3: Configure Your Demo Devices 44](#_Toc448995791)

[Mobile Device Requirements 44](#_Toc448995792)

[Device Setup Steps 44](#_Toc448995793)

[Set Up Device #1 (iOS or Android) 44](#_Toc448995794)

[Set Up Device #2 (iOS or Android) 45](#_Toc448995795)

# 

# EMS Demo Requirements and Scenarios

This demo guide contains 3 key scenarios – each demonstrating different value propositions of the Enterprise Mobility Suite. Each scenario can be performed independently. Prior to running through these demo scenarios, please ensure the one-time demo environment and device requirements are met.

## Demo Pre-Requisites

* Follow the steps documented in the [EMS Demos – Getting Started Guide](http://emsassetspub.blob.core.windows.net/demoassets/EMS%20Demos%20Getting%20Started%20Guide.pptx) to create your free, personal, 90-day Office 365 demo tenant with EMS add-on.
* Preform one-time manual setup steps against your demo environment as detailed in Appendix 1[.](#_Appendix_1:_Configure_2)
* If you’d like to include the Desktop Virtualization scenario to your demos, perform installation/configuration of Azure RemoteApp (ARA) as detailed in [Appendix 2](#_Appendix_2:_Installing/Configuring).
* Prepare your demo devices as detailed in [Appendix](#_Appendix_3:_Configure) 3.
* Prior to each demo, perform the pre-demo checklist steps listed at the beginning of each demo scenario.
* After each demo, perform post-demo reset steps to ensure you’re able perform the demo again in the future.

## Scenario 1: Manage Mobile Productivity

One of the first challenges in the mobile-first, cloud-first world is to deliver secure email to employees’ on-the-go. This scenario, demonstrates how EMS provides employees with secure and seamless access to corporate email and documents using familiar productivity experiences with Office mobile apps such as Outlook, Word, Excel, PowerPoint, and OneDrive. EMS also helps to protect corporate data on the device itself and beyond with multi-layer protection, all without impacting personal data.

**Features**

* Familiar productivity experience with Office mobile apps
* Managing access to email and documents with conditional access
* Enable secure access for corporate email, SharePoint and One Drive
* Comprehensive protection of corporate data at 4 layers: identity, device, application, and data
* Flexible architecture

**Services**

* Active Directory Premium
* Microsoft Intune
* Azure Rights Management

## Scenario 2: Deploy and Manage All of Your Applications Using Enterprise Mobility

Demonstrate the flexibility to deploy and manage apps that employees need to be productive. Using this scenario, you can show how Enterprise Mobility supports SaaS apps, native apps and Windows apps on a variety of devices. You can deep dive into Azure Active Directory, Intune and Azure RemoteApp app management to show how Enterprise Mobility solutions offer security and management for your apps.

**Features**

* One common identity across on-prem and cloud
* Single sign-on to cloud and on-premises apps with multi-factor authentication
* Cloud App Discovery
* Cross-platform Company Portal
* Mobile Application Management
* Enable users to access Windows apps and data from any device and any location

**Services**

* Active Directory Premium
* Microsoft Intune
* Azure Rights Management

## Scenario 3: Comprehensive Protection of Your Corporate Data with EMS

Demonstrate how Enterprise Mobility Suite (EMS) provides the most comprehensive protection of corporate data across 4 layers: identity, device, application, and data. This demo will cover how different components of EMS help to keep the corporate data protected.

**Features**

* One Identity across on-prem & cloud
* Access to resources, apps and files
* Additional security to sensitive apps (MFA)
* Self-service and automation for password and groups
* Mobile application management
* File level protection - virtually all types on any device platform
* Protect on-premises identity
* Stop external threats from stealing corporate information

**Services**

* Active Directory Premium
* Microsoft Intune
* Azure Rights Management
* Microsoft Advanced Threat Analytics

# Demo 1: Manage Mobile Productivity

One of the first challenges in the mobile-first, cloud-first world is to deliver secure email to employees on-the-go. This scenario demonstrates how EMS provides employees with secure and seamless access to corporate email and documents using familiar productivity experiences with Office mobile apps such as Outlook, Word, Excel, PowerPoint, and OneDrive. EMS also helps to protect corporate data on the device itself and beyond with multi-layer protection, all without impacting personal data.

## Pre-Demo Checklist

Follow these steps prior to each demo presentation to ensure a smooth and speedy demo experience:

1. Prepare your mobile devices (iOS or Android) as outlined in **Appendix 2**. If you only have one device available, consider presenting the following demos via a custom PowerPoint slideshow:
   * Managing Office Mobile Apps without Device Enrollment
   * Device Enrollment for Conditional Access
2. Launch the native **Notes** app on your device and jot down the login credentials of your demo persona (so you can quickly access it during the demo and minimize typos).
   * Demo persona’s corporate account : **garthf@<tenant>.onmicrosoft.com** and password: **pass@word1**
   * Demo persona’s personal email account: <your demo Live ID user account info>
   * Copy the demo persona’s corporate account email and keep it in device’s clipboard.
3. MFA authentication requires a valid phone number. Ensure your demo persona’s Azure AD account has your mobile phone number set up as verification number.
4. <If presenting demo remotely via Skype> Launch a iOS screen sharing utility (such as **AirServer** or **Reflector 2**) on your Windows PC and mirror your device onto the PC’s screen.
5. Launch a new browser session on a browser that supports Silverlight (IE or Firefox) and navigate to the demo tenant’s **Intune management portal**, at <https://manage.microsoft.com>. Login with your demo tenant’s Global Admin user ([admin@<tenant>.onmicrosoft.com](mailto:admin@%3ctenant%3e.onmicrosoft.com) and pass@word1), then minimize the browser.

## Demo Sequence

| **Speaker Script** | **Click Steps** |
| --- | --- |
| Opening I think you would agree with me that one of the main things your employees want on their mobile devices is access to their corporate email and documents. And they expect to do it in fast and easy way without the need of going through multiple complex steps or calling the help desk. IT on the other hand wants to keep the corporate data secure wherever it is.  Let me show how you can solve both of these problems with Office 365 and EMS. |  |
| Managing Office Mobile Apps without Device Enrollment A new capability of Microsoft Intune allows Mobile Application Management (MAM) without requiring the device to be enrolled for IT management. In short “**Intune MAM without enrollment**”. This is particularly useful for BYO scenarios where end users don’t want to or can’t enroll their devices for IT management. This capability is also useful in cases where a device is already enrolled in another MDM solution.  An increasing number of Office mobile apps support MAM without enrollment for both iOS and Android platforms.  This new capability is an addition to the existing Intune MAM capabilities that require enrollment into Intune mobile device management (MDM).  Here, I’m accessing a Word document from SharePoint. This document is considered corporate data. As such, I’m disallowed from saving it outside of corporate locations.  I’m also not allowed to copy/paste the contents of this document to non-corporate locations.  Although this device is not enrolled with my organizations, the application policies set by my organization block me from taking my data outside of my organization – thereby protecting my corporate data. | Perform these steps on mobile device #1 (iOS or Android)   * + 1. On your mobile device, launch **Word** app.     2. Ensure you’re logged in to the Word app as your demo persona (e.g. GarthF@<tenant>.onmicrosoft.com).     3. Go to **Open** > **SharePoint** > **Documents** > Northwind Proposal.     4. In the Word menu, tap **File** > **Duplicate**.      * + 1. Choose <device> (**iPad** or **Android**, as applicable).     2. Note the prompt that disallows saving to non-corporate locations due to policy set by Administrator. |
| Conditional Access and Device Enrollment When employees add their corporate Office 365 account in the Outlook app, they expect to get access to all of their email, but with EMS you can enable conditional access which ensures that employees access corporate email only from managed and compliant devices.  The first thing I see as I type in my corporate email alias is my company’s logo: a branding I’m familiar with. With the power of Azure AD, this form already recognized me as a user of my corporation; and the customized branding ensures me I’m signing in to a trusted location so I can type in my password without concern.  As you can see here, they are blocked and are informed that in order to get access they need to first enroll their device to Intune.  Next they need to install the Intune company app which has already been done to save time.  Employees then need to login with their corporate Azure AD identity (same credentials one employees would use to access email), and go through the standard iOS enrollment process that includes applying a management profile and certificates for secure communication between the device and Microsoft Intune.  There are few things are happening behind scenes here. First, Intune gets device information without collecting personal data since this is a personal device. Next, Intune also registers this device with Azure AD, so now both Intune and Azure AD know that this device belongs to this employee which useful for few other scenarios when the employees wants to access corporate resource from this device. Intune also starts to deploy and enforce device settings like password requirements, resource access profiles such as WiFi and VPN, certificates, and applications.  Once the enrollment is completed, employees need to ensure that their device is compliant with the corporate policies. This is a great solution since employees get access to email with just few simple steps but IT is also happy because the corporate data is accessed only from managed devices. | Perform these steps on mobile device #1 (iOS or Android)   * + 1. On your device, launch **Outlook** app.     2. Tap **Get Started**, then dismiss app initialization/welcome messages, if necessary.     3. **Add an Account** > **Office 365** account as follows:        1. Email: [**garthf@<tenant>.onmicrosoft.com**](mailto:garthf@%3ctenant%3e.onmicrosoft.com)(paste it in)        2. Password: **pass@word1**   then tap **Sign in**.   * + 1. Note the Conditional Access policy message that blocks access to email:      * + 1. Tap **Enroll**.     2. Tap **OPEN** to launch Microsoft Intune Company Portal app.     3. Tap **Sign in**, then sign in to Intune Company Portal as: [garthf@<tenant>.onmicrosoft.com](mailto:garthf@%3ctenant%3e.onmicrosoft.com) (paste it in) pass@word1 (type it in).     4. On Company Access Setup page, type **Begin**.     5. On Device Enrollment page, tap **Enroll**. You will be directed to the built-in iOS **Settings** app.     6. On Install Profile page, tap **Install**.     7. Enter device passcode (*promoted only if device currently has a passcode*).     8. Tap **Install**.     9. On Warning page, tap **Install**.     10. On Remote Management dialog, tap **Trust**.     11. On Profile Installed page, tap **Done**. You’ll be re-directed back to the Intune Company Portal app.     12. On Company Access Setup page, tap **Continue**.     13. Tap **Done** to complete Company Access Setup.     14. You should now see the **Intune Company Portal** home page, similar to the screen shot below.      * + 1. Press the device’s **home button**. You will see a Passcode Requirement dialog where you must change passcode within 60 minutes.     2. Tap **Continue**, then set a new device passcode. If your device has a passcode currently, you’ll be prompted to type that in first.   **Tip**: For a complex, 4-character passcode, use **1111** so it’s easy to remember.   * + 1. Re-launch the built-in **Mail** app.   1. Note the **Inbox** is now populated with GarthF’s emails from Exchange server. |
| Mobile Application Management Since the device is managed and compliant, employees now have access to the corporate email. They just need to re-enter their Azure AD credentials, and the access to email will be granted. Behind the scenes, when employees login, Office 365 checks with Azure AD to see, if the device is managed and compliant which in this case it is. Because of that, Office 365 enables the access to email. Since the device is now managed, Employees can also access internal company apps as well as public apps from the Intune Company Portal. For the next part of my demo I actually need to install few of these applications, **but to save time I am going to switch to another iPad for same user that already has these apps installed.**  As Brad Anderson showed at Ignite, Intune is uniquely able to manage and enforce app restrictions for Outlook and Office mobile apps on iOS and Android. This provides best in class and consistent user experience for email, productivity and collaboration while protecting corporate data. Employees are productive with real Office, not Office like proprietary apps with limited functionality and confusing user interface. When employees launch Outlook they need to enter their PIN since it was configured in Intune by IT. In this example, this email has useful information that they want to keep for a project. If they try to copy it and paste to app, it doesn’t work since this is a personal app. But, if they try to paste into Microsoft Word app, it works since this is a managed app. This provides a consistent user experience for employees and helps to keep corporate data within the managed app ecosystem. | * 1. Perform these steps on iOS **device #2** (one that’s already been enrolled and configured with Managed Apps.)      1. Launch **Outlook** app (which is now configured with 2 email accounts: one corporate mailbox and one personal).      2. In GarthF’s corporate inbox, scroll down and tap on an email from Alex Darrow (subject **Northwind Proposal**).   **Tip**: You may open any email in the user’s corporate inbox with a **Word** document attachment.   * + 1. Tap on the attachment file name to preview contents.     2. On a text paragraph, **tap and hold,** then **Copy**.      * + 1. Tap **Close** to dismiss document preview.     2. Tap the **Reply** icon.     3. In the reply message body (whitespace) tap and hold for a second to reveal **Paste** option, then tap **Paste**.      * + 1. Discard the email message (by tapping the **X** icon, then confirming **Delete draft**).     2. Press the home button, then launch the built-in iOS **Notes** app.     3. Create a new note and attempt to paste (**tap+hold** on whitespace.) Note the **Paste option is not available**.      * + 1. **Double-press the home button**, then return to **Outlook** app.     2. Back in the Northwind Proposal email, tap **Open in Word** link under the included email attachment. The Word app will launch.     3. Dismiss any introduction video, tips and guides that may be prompted by the Word app until the attachment document (Northwind Traders Proposal) opens in the app.     4. Tap the **File** menu icon in Word app, then **Duplicate**.     5. Tap **Dropbox**.     6. Tap **Duplicate**.     7. At alert box with message: “**Your administrator doesn’t allow saving to personal locations**.” tap **OK**.     8. Tap **Save** again.     9. Tap **OneDrive for Business**, then **Save**.     10. Close the **Northwind Traders Proposal** document by tapping the close icon (🡨). |

## Demo Reset Instructions

Follow these steps to reset the demo at the conclusion of each presentation:

**Device #1:**

1. Un-enroll the device from Intune **Comp Portal**.
2. Delete the Exchange mailbox that was added during the demo:
   1. Go to the built-in device **Settings** app.
   2. Tap **Mail, Contacts, Calendars** then **Exchange**.
   3. Tap **Delete** Account, then **Delete from my iPhone/iPad**.
3. Close any open documents in Word app (by tapping back arrow icon: 🡨).

**Device #2:**

1. Browse to GarthF’s OneDrive Pro for Business web site (https://<tenant>-my.sharepoint.com/, logged in as GarthF) then delete the **Northwind Proposal** document from the root.
2. Go through steps of Setup Device #2 in the appendix so the same device is ready for your next demo. You may skip the steps where the configurations from prior run are already there (e.g. Dropbox setup, personal inbox setup, etc.)

# Demo 2: Deploy and Manage All of Your Apps with EMS

## Pre-Demo Checklist

Follow these steps prior to each demo presentation to ensure a smooth and speedy demo experience:

1. Launch a new browser session in **IE or Edge** and navigate to the MyApps portal, at <https://myapps.microsoft.com>. Login with your demo Hero user ([garthf@<tenant>.onmicrosoft.com](mailto:garthf@%3ctenant%3e.onmicrosoft.com) and pass@word1). Minimize the browser.
2. Launch a separate, **InPrivate** browser session (IE or Edge) and navigate to the demo tenant’s Azure management portal, at <https://manage.windowsazure.com>. Login with your demo tenant’s Global Admin user (admin@<tenant>.onmicrosoft.com and pass@word1).
3. In the Azure Management Portal, ensure the user GarthF has a **Authentication Phone** **number** supplied and configured with a mobile phone number that you possess. This is required for multi-factor authentication demo. See Appendix 1 for details.
4. Launch the Azure RemoteApp desktop client on your PC and connect to your tenant’s RemoteApp collection as the user GarthF. Minimize the ReportApp client.
   * If you have not done so yet, please refer to [Appendix 2](#_Appendix_2:_Installing/Configuring) in order to install and configure Azure RemoteApp.

## Demo Sequence

| **Speaker Script** | **Click Steps** |
| --- | --- |
| Let me show you how to ensure your users have access to the applications they need to be productive.  The first solution I’ll show you leverages the power of Azure Active Directory to enable access to Software as a Service, and web-based applications. |  |
| Add SaaS Apps: Salesforce You probably recognize that I’m starting in the Azure Portal. Navigate to applications for your active directory. You’ll see the list of applications that have been added  Adding a SaaS app is very straightforward. There are 3 types of applications that can be added   * Application my organization is developing – a custom application that your company has created, that can be integrated with Azure AD to provide secure sign in and authorization for their services. * Application from the gallery – add an application from a list of SaaS apps that are pre-integrated with Azure AD and many of them offer deep integration like provisioning of users using federation. * Publish an application to be available from outside your network – enables you to make your internal web-based applications available externally   We’ll start by adding an application from the gallery - There are over 2400 SaaS applications listed, such as Twitter, Dropbox, or Workday – these applications are pre-integrated and can be easily configured for single sign on.  If the SaaS application is not on the list, it can be added as a custom application  I’ll add Salesforce  When the application is added, the quick start page is displayed, showing our next steps  There are just 3 steps and you can have this SaaS app available  The first step is to Configure single sign-on  Windows Azure AD Single Sign-on – this option enables users to authenticate to Salesforce with their account in Azure AD using federation  Configure App URL – the sign on URL is the custom URL for your domain on Salesforce  Finally configure single sign-on on Salesforce, by downloading the certificate you will need to upload at Salesforce when you configure that side of the federation, and verifying proper configuration and clicking complete  The second step is to Configure user provisioning. Add your Salesforce admin credentials to enable automatic user provisioning. This enables user provisioning and deprovisioning based on changes made in Azure Active Directory. (optional)  The third step is to assign users and or groups you want to access SaaS app.  When these steps are completed the SaaS application will be available in MyApps. | 1. Bring up the browser session with Microsoft Azure Management Portal (**Global Admin** user). 2. In the ACTIVE DIRECTORY workspace, click **Contoso <TenantName>**. 3. Click the **APPLICATIONS** tab. 4. Click **Add**. 5. In the **What do you want to do?** window, review the options that are available.  * Application my organization is developing * Application from the gallery * Publish an application to be available from outside your network  1. Click **Add an application from the gallery**. 2. Review the applications that are available in the application gallery. 3. Click **Custom**, and review the benefits. 4. Click **FEATURED APPLICATIONS**, type **Salesforce** in the search box and click **Search**. 5. Click **Salesforce**, and in the **DISPLAY NAME** text field type **Salesforce-Demo**, and then click **Complete**. 6. Review the items on the **Quick Start** page.  * Configure single-sign on * Configure account provisioning * Assign accounts |
| Add an App and Configure SSO: Twitter Many organizations rely upon software as a service (SaaS) applications such as Office 365, Box, and Salesforce for end user productivity but IT has typically had to create and update user accounts for each SaaS app, Users had to remember their credentials for each, which gets messy fast.  Azure AD enables integration to many of today’s popular SaaS applications (e.g., Box, Twitter, and so on). It provides identity and access management, and delivers an access panel for users, in which they can discover what application access they have and single sign-on to access their applications.  I’ll demonstrate this two ways, starting with password single sign-on to the Twitter app.  Configuring password-based single sign-on enables Azure to automatically sign users in to third-party SaaS applications by using the SaaS application’s user account information. When you enable this feature, Azure AD collects and securely stores the SaaS app’s user account information and the related password.  Azure AD can support password-based single sign-on for any cloud-based app that has an HTML-based sign-in page. By using a custom browser plugin, Azure AD automates the sign in process by securely retrieving application credentials, such as the username and the password, from the directory, and entering these credentials in to the application’s sign in page on behalf of the user.  Here you see that no users have access to this app.  Likewise, you see that no groups have access to this app. I will give the Sales & Marketing group access to the Twitter app, and everyone in the group will share the same set of app credentials.  The last step is to copy the single sign-on URL to the clipboard. This is the URL that I will share with members of the Sales & Marketing team. | **Note**: Ensure you have a demo Twitter account (and login info available) prior to performing this section.   1. Bring up the browser session with Microsoft Azure Management Portal (**Global Admin** user). 2. In the ACTIVE DIRECTORY workspace, click **Contoso <TenantName>**. 3. Click the **APPLICATIONS** tab. 4. Click **ADD**. 5. Click **Add an application from the gallery**. 6. In the **Search** box, type **twitter** and press **Enter**. 7. Click **Twitter**. 8. In the **DISPLAY NAME** box, type **Twitter-Demo**. 9. Click **OK**. 10. Click **Configure single sign-on**. 11. Select **Password Single Sign-On**, then https://manage.windowsazure.com/Content/Images/button-complete.png(**Complete**). 12. In the **SHOW** list, click **All Users**, and click **OK**. 13. Click **Assign accounts**. 14. Select **Show** **Groups** then https://manage.windowsazure.com/Content/Images/button-complete.png(OK). 15. Click **sg-Sales & Marketing** to highlight 16. Click **ASSIGN** button (at the bottom of the screen). 17. Select the **I want to enter Enterprise Twitter credentials to be shared among all group members** check box. 18. In the **User Name** box, type the user name for the Twitter account. 19. In the **Password** box, type the Twitter account’s password. 20. Click **OK**. 21. Highlight **sg-Sales & Marketing**. 22. Click **EDIT ACCOUNT**. 23. Click **Cancel**. 24. Click **DASHBOARD**. 25. In the **SINGLE SIGN-ON URL** box, click **Copy to Clipboard**. |
| Use MyApps to Access Applications In your Enterprise, you may have Mac users such as graphic designers. You’ll want to ensure all platforms can be equally productive.  MyApps is accessible using iOS, Android, Mac, and Windows to view available applications.  I’ll log in to MyApps using my corporate credentials, and I can see all the applications available to me.  Applications can be easily launched (office 365, Corporate Twitter). Using single sign-on I am redirected directly to the page.  Notice there are SaaS apps, custom apps, and on-premises apps, displayed.  I also have the ability to perform self-service on my account that really empowers me to get my work done. I can add myself to groups, to add applications. I can reset, and change my own password. Self-service is a very effective cost cutting method by reducing help desk calls.  By joining the Contoso Bug Bashers security group, I was automatically granted access to the BrowserStack application. | **Important:** Use GarthF’s browser session (in IE or Edge) for this portion of the demo.   1. Bring up the browser session with the **My Apps Portal** (logged in as GarthF). 2. In the **applications** page, click **Office 365 SharePoint Online**. Note the login-free SSO experience in new brower tab. 3. Go back to the Access Panel Apps browser tab. 4. Click **Salesforce.** 5. Authorize the login on your phone (multi-factor authentication) by accepting the call on your mobile phone and responding to the authentication request. 6. Note the login-free SSO experience to Salesforce in a new browser tab. 7. Go back to the Access Panel Apps browser tab. 8. Click **groups**. 9. Change **My groups** drop-drown to **All**. 10. Scroll down the page, then click on **ssg-Contoso Bug Bashers**. 11. Click **Join group**. 12. In the pop-up window, click **Request**. (You will be auto-approved.) 13. Click **applications** to go back to the applications page. 14. Refresh the page. Note the inclusion of a new application on the page: **BrowserStack**. |
| Self-Service on MyApps Portal I also have the ability to perform self-service on my account that really empowers me to get my work done. I can add myself to groups, to add applications. I can reset, and change my own password. Self-service is a very effective cost cutting method by reducing help desk calls.  Password reset ties back to password write-back. When changes are made to Azure AD, those changes are sync’ed with Active Directory. | **Important:** Use GarthF’s browser session (in IE or Edge) for this portion of the demo.   1. Bring up the browser session with the **My Apps Portal** (logged in as GarthF). 2. Click **profile**. 3. Click **Register for Password Reset**. 4. Review the options for alternate verification options:    1. Authentication Phone    2. Authentication Email 5. Click **Cancel**. 6. Click **Change password**. 7. Review the password change form, then click **cancel**. |
| Access to Windows-based Apps Next question is how do I enable access to Windows-based applications across all the devices in my enterprise?  The next solution I’ll show you is **Azure RemoteApp** that enable organizations to provide windows-based applications for employees to work across devices, from anywhere. As you saw in Brad’s keynote, he accessed Dynamics using an iPad. This windows-based application could be accessed from many different mobile devices.  Let me show you the client experience using Microsoft Remote Desktop app here on my iPad.  I have signed in using my corporate credentials, and the list of applications published to me is displayed. Using the RD Client I can see all of the applications I have available in a single location.  Different kinds of apps can be published: line of business applications productivity apps, or Windows-based apps. (Launch Excel)  I want to show you the power of this service, running an application in Azure, accessing corporate resources securely on-premises.  I selected a file I have been working with. This file is securely accessed from the cloud, and contains some sensitive data like credit card information. I’m still able to work on it without storing it on my local device. This way, even if this device is lost or comprised, the data remains protected.  Notice I can use Excel as if the application were local, the functionality is exactly the same. I can use the slicers to manage the data that is displayed.  This Remote Desktop client experience is available on iOS, Android, Mac and Windows. | **Note:** Perform these steps on your Windows PC.   * + 1. Launch the **Azure RemoteApp** program on your demo device.     2. If necessary, log in with your demo persona credentials.     3. Review the list of available applications.     4. Review the available applications under Work Resources.     5. Launch **Excel**.     6. Review functionality within Excel.        1. Go to **File > Open > OneDrive – Contoso <Tenant>**        2. Select **Contoso Purchasing Data – Q1.xlsx** to open it.        3. **Enable Editing** once the document opens.        4. Click anywhere on the table area (e.g. cell A1).        5. In the ribbon bar, go to **INSERT**, **SLICER**, then check **Card Type** and **OK**.        6. Click **MasterCard** on the Card Type slicers to filter the table data. |
| Close As you’ve seen today, Azure Active Directory and Azure RemoteApp enables users to be productive anywhere on a variety of devices. Everything I’ve shown you is available today and delivered by Azure.  Thank you. |  |

## Demo Reset

1. Go back to the Azure Management Portal browser session and delete any SSO Applications you added during the demo (i.e. Twitter-demo, Salesforce-demo). Do NOT delete the apps that you had configured previously, before the demo.
2. Go back to the MyApps portal (as GarthF) and **leave group** for sso-Contoso Bug Bashers.
3. Ensure the Excel file you opened in the Azure RemoteApp session is closed. Do **NOT** save changes to the files.

# Demo 3: Comprehensive Protection of Corporate Data with EMS

## Pre-Demo Checklist

Follow these steps prior to each demo presentation to ensure a smooth and speedy demo experience:

1. Launch a new browser session in **IE or Edge** and navigate to the MyApps portal, at <https://myapps.microsoft.com>. Login with your demo Hero user ([garthf@<tenant>.onmicrosoft.com](mailto:garthf@%3ctenant%3e.onmicrosoft.com) and pass@word1). Minimize the browser.
2. Launch a separate, **InPrivate** browser session (IE) and navigate to the demo tenant’s Azure management portal, at <https://manage.windowsazure.com>. Login with your demo tenant’s Global Admin user (admin@<tenant>.onmicrosoft.com and pass@word1).
3. In the same browser session, open a new browser tab, then log in to the Intune management portal at <https://manage.microsoft.com> (as Global Admin).
4. In the Azure Management Portal, ensure the user GarthF has a **Authentication Phone** **number** supplied and configured with a mobile phone number that you possess. This is required for multi-factor authentication demo. See Appendix 1 for details.
5. In the same browser session, open a new browser tab, then log in to the staged Cloud App Security demo site as follows:
   * Browse to <https://acme.console-demo.adallom.com/>
   * Login as: admin@<tenant name>.onmicrosoft.com with password: Pass@word1

## Demo Sequence

| **Speaker Script** | **Click Steps** |
| --- | --- |
| I will demonstrate how Enterprise Mobility Suite (EMS) provides the most comprehensive protection of corporate data across 4 layers: identity, device, application, and data. This demo will cover how different components of EMS help to keep the corporate data protected. |  |
| Use MyApps to Access Applications In your Enterprise, you may have Mac users such as graphic designers. You’ll want to ensure all platforms can be equally productive.  MyApps is accessible using iOS, Android, Mac, and Windows to view available applications.  I’ll log in to MyApps using my corporate credentials, and I can see all the applications available to me.  Applications can be easily launched (office 365, Corporate Twitter). Using single sign-on I am redirected directly to the page.  Notice there are SaaS apps, custom apps, and on-premises apps, displayed.  I also have the ability to perform self-service on my account that really empowers me to get my work done. I can add myself to groups, to add applications. I can reset, and change my own password. Self-service is a very effective cost cutting method by reducing help desk calls.  By joining the Contoso Bug Bashers security group, I was automatically granted access to the BrowserStack application. | **Important:** Use GarthF’s browser session (in IE or Edge) for this portion of the demo.   1. Bring up the browser session with the **My Apps Portal** (logged in as GarthF). 2. In the **applications** page, click **Office 365 SharePoint Online**. Note the login-free SSO experience in new brower tab. 3. Go back to the Access Panel Apps browser tab. 4. Click **Salesforce.** 5. Authorize the login on your phone (multi-factor authentication) by accepting the call on your mobile phone and responding to the authentication request. 6. Note the login-free SSO experience to Salesforce in a new browser tab. 7. Go back to the Access Panel Apps browser tab. 8. Click **groups**. 9. Change **My groups** drop-drown to **All**. 10. Scroll down the page, then click on **ssg-Contoso Bug Bashers**. 11. Click **Join group**. 12. In the pop-up window, click **Request**. (You will be auto-approved.) 13. Click **applications** to go back to the applications page. 14. Refresh the page. Note the inclusion of a new application on the page: **BrowserStack**. |
| Review Azure Security Reports You can use Azure AD Premium’s access and usage reports to learn the integrity and security of your organization’s directory. With this information, you can better determine where possible security risks might exist so that you can adequately plan to mitigate those risks. There are four categories I will show you today: anomalous activity, activity logs, integrated applications, and premium reports.  You can use Azure AD Premium’s access and usage reports to learn the integrity and security of your organization’s directory. With this information, you can better determine where possible security risks might exist so that you can adequately plan to mitigate those risks. There are four categories I will show you today: anomalous activity, activity logs, integrated applications, and premium reports.  **Anomalous activity reports**  This report indicates users who have successfully signed in to your directory while assigned a client IP address that has been recognized by Microsoft as an anonymous proxy IP address. People often use these proxies if they want to hide their computer’s IP address, and they might be used for malicious intent—sometimes hackers use these proxies. Results from this report will show the number of times a user successfully signed in to your directory from that address and the proxy’s IP address.  **Sign ins after multiple failures** report indicates users who have successfully signed in after multiple consecutive failed sign-in attempts. Possible causes include users had forgotten their passwords, or users are victims of successful password-guessing brute force attacks. Results from this report will show you the number of consecutive failed sign-in attempts made prior to the successful sign-in and a timestamp associated with the first successful sign-in.  **Sign ins from multiple geographies** report includes successful sign-in activities from a user where two sign ins appeared to originate from different regions and the time between the sign ins makes it impossible for the user to have travelled between those regions. Possible causes include users sharing their passwords, users using remote desktop connections to launch a web browser for sign in, or a hacker signing in to a user’s account from a different country. Results from this report will show you the successful sign-in events, together with the time between the sign ins, the regions where the sign ins appeared to originate from, and the estimated travel time between those regions.  **Activity Logs reports**  This audit report shows records of all audited events within the last 24 hours, last 7 days, or last 30 days. Categories include:   * Credential updates * Device management * Directory synchronization * Domain management * Group management * Partner administration * Policy management (MFA) * Role changes * User account changes * User licensing * User, group, and contact management   **Integrated Applications reports**  This report provides a history of attempts to provision accounts to external applications.  Use this report to monitor errors that occur during the synchronization of accounts from SaaS applications to Azure AD.  **Premium reports**  This report includes sign-in attempts that have been executed from IP addresses where suspicious activity has been noted. Suspicious activity includes many failed sign-in attempts from the same IP address over a short period of time and other activity that was deemed suspicious. This might indicate that a hacker has been trying to sign in from this IP address. Results from this report will show you sign-in attempts that were originated from an IP address where suspicious activity was noted, together with the timestamp associated with the sign in. | **Note:** Use Global Administrator’s browser session for this portion of the demo.   1. Bring up the browser session with Microsoft Azure Management Portal (**Global Admin** user). 2. In the ACTIVE DIRECTORY workspace, click **Contoso <TenantName>**. 3. Click the **REPORTS** tab. 4. Click **Sign ins from unknown sources**. 5. Click **Sign ins after multiple failures**. 6. Click **CONFIGURE**. 7. In the **NUMBER OF CONSECUTIVE FAILED SIGN INS CONSIDERED ANOMALOUS** box, type **5**. 8. Click **SAVE**. 9. Click **Sign ins from multiple geographies**. 10. Click **Users**. 11. Click **Aarif Sherzai** to highlight, then point to the buttons at the bottom of the page:      1. Click **MANAGE MULTI-FACTOR AUTH**. 2. Place checkmark next to Aarif Sherzai’s display name. 3. Under **quick steps**, click **Enable**. 4. Review **About enabling multi-factor auth**, then click **Cancel**. 5. Go back to the Active Directory browser tab, if necessary, then click **Audit report**. 6. Click **Account provisioning activity**. 7. Click **Sign ins from IP addresses with suspicious activity**. 8. Click **Password reset activity**. 9. Click **Password reset registration activity**. 10. Click **Self-service groups activity**. 11. Click **Application usage**.      1. Click **Sign ins from IP addresses with suspicious activity**. |
| Microsoft Advanced Threat Analytics Microsoft Advanced Threat Analytics or ATA, is an on-premises product, that helps IT protect their enterprise from advanced targeted attacks by automatically analyzing, learning and identifying normal and abnormal entity behavior. Entity can be a user, a device or simply a resource in the network.  Using deep packet inspection technology, ATA analyzes all Active Directory traffic. It can also collect relevant events from SIEM or Windows Event logs.  The constant reporting of traditional security tools and sifting through them to locate the important and relevant alerts can get overwhelming. Instead, ATA provides an easy to consume, simple to drill down, social media feed-like report helping IT to focus on what is important fast. Presenting this quantity of data as a timeline gives you the power of perspective, and insight into who’s accessing what, when they’re accessing it, and how they’re accessing that data.  **Event Timeline**  Here’s an event indicating suspicion of identity theft based on abnormal behavior of a user. ATA provided an alert as this user activity deviated from this user’s normal behavior.  With ATA, these alerts happen once suspicious activities are contextually aggregated to its own behavior, as well as to the other entities in its interaction path. So multiple events were used and correlated to detect it. Four in this case. ATA also compared this user’s behavior to all the other users in his interaction map, in order to avoid any reduce false positive or negative alerts.  Let’s take a look at the list of abnormal devices that contributed to this alert.  The user, a full time employee, suddenly logs on to an external vendor terminal server, raising suspicion. It is even more suspicious that the user did so outside of their normal working hours. This is another behavioral aspect that ATA tracks. | **Note:** The ATA demo suggested here will be performed using a static web site with limited functionality. For fully functional ATA demo, please connect to <https://atademo> in the Microsoft CorpNet or use the ATA Center demo virtual machine.   1. Browse to the static ATA demo site, located at <https://atademoui.azurewebsites.net/>. 2. Scroll down the page to 11:54 PM “**Suspicion of Identity Theft based on Abnormal Behavior**”. 3. Point mouse to the bulleted list of 4 suspected behaviors.      1. Click on **6 Abnormal computers**. 2. Hover mouse over **EXTVENDOR-TS** (last item on the Abnormal Computers list). |
| **Suspicious Activity Profile**  We begin the investigation process by clicking on the External Vendor Terminal Server, taking us to the profile view.  We then get to see the attack timeline from the Terminal Server’s perspective, by clicking on the Suspicious activities tab.  As with many attacks, this one begins with a reconnaissance phase where we see the attacker attempting to guess usernames.  Ultimately, the attacker(s) succeeded and guessed three different accounts, one of them being the User’s account.  In the next phase of the attack, we will clearly see the attacker attempting a brute force attack including them guessing the user’s password.  Once the Users account was compromised, we can see the user behaving abnormally. With the list of alerts prior to this, we have sufficient evidence to conclude that this user’s credentials are now compromises. Eventually we see the attacker attempting to elevate their privilege to a domain administrator account, possibly their ultimate goal.  In this instance the attack was detected by ATA with the help of data provided by a third party SIEM solution which was configured to forward Windows security events to ATA – in this case a SIEM solution. The third-party software was already collecting these events, so no additional configuration was required there beyond the event forwarding itself.  All of ATA’s detection algorithms are self-learning, allowing it to detect suspicious activities from the first minute it’s deployed, without the need to configure or tweak rules, baselines, or thresholds; you simply plug it in and off it goes.  Also you can configure ATA to send an event to your SIEM system for each suspicious activity with a link to the specific event on the attack timeline.  In summary, ATA uses machine learning in its deterministic and detection engine to establish an understanding of the normal patterns of behavior for both users and entities, and it’s that unique capability that allows us to provide timely and accurate alerts across a huge variety of attack vectors. | 1. Click on the **EXTVENDOR-TS** label to go to the terminal profile view page. 2. Click the **Suspicious Activities** tab. 3. Scroll down the bottom of the timeline, then up slightly to **Reconnaissance Using Account Enumeration**. 4. Scroll up to **Brute Force Attack Using LDAP Simple Bind.** 5. Under **Attacked Accounts**, click on the picture of **Michael Dubinsky** to view his User Profile Page. 6. Click **Suspicious activities** tab. 7. Click **Back** (browser navigation) to return to Timeline. 8. Scroll up to **Suspicion of Identity Theft based on Abnormal Behavior.** 9. Scroll up to **Identity Theft Using Pass-the-Ticket Attack**. 10. Scroll up to **Remote Execution Attempt Detected**. |
| Introducing Microsoft Cloud App Security As an IT professional to Executive Officer of any business, ask yourselves these questions when referencing Cloud Applications: Do you know how many cloud apps your users may be using? Do you know if customers Personally Identifiable Information (PII) are located on these apps? Do you know if these apps are secure or not?  Now to introduce you to Microsoft’s Cloud App Security. This newly added feature does not just apply to Microsoft specific cloud applications but also public and line of business applications as well. The vision behind Cloud App Security is to empower businesses of all sizes with:   * Visibility: the ability to Discover & Investigate * Protection: the ability to Control & Respond   We'll look at how you can gain deeper visibility, stronger controls and enhanced security for your cloud apps with this new feature.  **General Dashboard**   * The Dashboard provides an overview of your cloud security status. * The service provides a wide set of capabilities for securing cloud applications, allowing companies to discover, investigate, control and protect their data in the cloud. * **Discovery Dashboard** * Moving on to the discovery dashboard. * The Discovery Dashboard provides a detailed overview of all cloud applications being used in the organization. It identifies all users and IP addresses accessing the application. It also conducts a risk assessment and automated risk score for each app. * Since the data is collected via logs, through firewalls and proxies, there is no need to deploy additional agents. These tasks can also be automated. * As you can see the company has 500+ apps and 12 are specifically risky. If you scroll down, you can also see top services used and top risky services. You can also see if the apps being used are sanctioned or unsanctioned. * **Discovered Apps**   To drill down, let’s click on discovered apps:  Here you see all of the discovered apps in the organization. You can see all sanctioned (approved by my organization) and unsanctioned apps. You can easily filter based on the name, activity time frame or the risk score associated with the application. You can also filter by a category: for instance collaboration apps.  You can also drill down on a specific app. For this, let’s click on Office 365. With a simple drill down here is the risk assessment and risk score for Office 365. Cloud App Security not only discovers more than 13,000 cloud applications in use but it also provides an automated risk score by evaluating each discovered service against more than 60 parameters.  Here you can see all of the different parameters used for the risk evaluation. You can dive into more details for a specific parameter to get a breakdown on the score. You can also interact with this risk assessment by reporting new data or requesting score update.  **App Overview Charts**  Discovering which apps are in use across your organization is just the first step in making sure your sensitive corporate data is protected. Cloud App Security also provides powerful reporting and analytics capabilities for you to gain the complete context of your cloud usage: such as the breakdown of usage, app activity or we can delve into specific users or IPs.  **File Log**  Once you sanction an app, you can gain granular visibility into that app. You also have the ability to see all activities across all apps and can easily apply filters to this log.  You know that employees can make a simple mistake and make a file link viewable by the public. This type of mistake can turn into a costly security incident.  Thanks to Cloud App Security you can now see and govern all files in the cloud, with a very powerful and easy to use query engine. It also provides all the information that you need to perform a detailed investigation by showing you who the owner(s) and collaborator(s)are of the file. It can also show you the folder hierarchy, inspects the content and provides easy mitigation options.  For example, you can sort by access level and find all public files. Here you see all files and folders viewable to the public.  **File-Level Investigation**  Let’s review 2 different scenarios regarding file-level violations, to an existing policy that is currently in place. Within these scenarios, the following topics about policies will be covered 1) allow you to authorize legitimate files and 2) how to take action against suspicious/costly file violations.  For this, you will go to the Control menu at the top navigation bar and click on policies:  Within Cloud App Security, There is a very wide set of policies available to configure. You can either use out of the box policies or build and customize your own.  Let’s filter the policies to find the file level policies.  The file-level policy you will be looking at is the PCI compliance policy. The purpose of this policy is to identify files containing customer credit card numbers that are publicly shared and also providing options for investigation and remediation.  Let’s click on this policy, to see if there are any files violating this policy.  Now that you are viewing the results of our investigation for the PCI Compliance policy, you can see that there are 2 files currently violating this policy.  **Scenario 1**: Investigating & Remediating a Violation  For the 1st scenario, let’s investigate the Payment schedule and details.xlsx file. To dive deeper into this file, all you need to do is click on the file to expand its description bar.  By expanding the file details, you can see the owner of the file, the collaborators, when it was created and when it was modified.  You can also view the violation matches, which can provide a little more detail for your investigation. Upon opening the matches window, you can see that it produces a match for credit card information.  You can also see file hierarchy by clicking on view hierarchy in details.  It seems like this file is located under one of the customer information folders and it is available in a public link, which seems suspicious. Based on the information found while investigating, you can now take action.  By clicking on the more information icon, you can view all of the options available in order to remediate this violation.  To prepare for the next scenario, exit the hierarchy window.  **Scenario 2:** Authorizing Legitimate Files  For the 2nd scenario, you will investigate the Test\_file\_for\_DLP\_test.docx file. To start off, let’s expand the file description bar.  Now let’s view the results in the matches window. As you can see none of the results look real.  To further investigate, you want to view the file hierarchy, which will show you where this file resides. Viewing the hierarchy of this file, you can see that this file resides in a folder named “Test Files”.  ( For the purpose of this demo, you will be shown how to authorize this file but DO NOT click the check mark.)  Now you have determined that this is a test file. Since this file isn’t violating this policy you can take further action and authorize this file, which will remove it from the Unauthorized Violations filter.  **Alerts**  Visibility and controls are not enough if not coupled with a powerful detection engine that can provide insights and alerts.  The alerts center gathers alert of a wide variety of categories, including threat detection, privileged accounts and compliance violations.  Let’s see how Cloud App Security helps you detect anomalies and prevent threats.  To do this you will go to the “Alerts” menu. The alerts center gathers all the red flags identified by Cloud App Security including anomaly and threat detection compliance violations and privileged accounts.  Let’s look into the general anomaly detection alert:  Cloud App Security advanced machine learning heuristics learns how each user interacts with each SaaS app and through behavioral analysis, assesses the risk in each transaction.  Here you can see a user who is an administrator performing suspicious activities such as logging in from a new anonymous location and two countries simultaneously within an hour with several failed login attempts. you can take look at the details of the activity and take action to mitigate any threats right away.  This concludes this demonstration. As you have seen, Microsoft Cloud App Security is a comprehensive solution for gaining deeper visibility, stronger controls and enhanced security for your cloud apps. I would like to emphasize - We not only support Microsoft cloud apps. We are committed to help you secure third party cloud apps as well.  For more information regarding Cloud App Security,  Please visit: [www.cloudappsecurity.com](http://www.cloudappsecurity.com/) | **Note:** To get a better understanding of Cloud App Security you will be using a static website (staged environment) with full functionality. This is a shared environment accessible to others who are also interested in Cloud App Security. So please use this site to only **VIEW** and **EXPLORE ONLY. DO NOT MAKE ANY EDITS** **TO THIS ENVIRONMENT.**  **To get access to a canned environment:**   1. Create a [Cloud App Security](https://portal.microsoftonline.com/Signup/MainSignUp15.aspx?OfferId=757c4c34-d589-46e4-9579-120bba5c92ed) tenant. Note that the activation link requires an Office365 sandbox environment where the license can be provisioned. Copy the link to a browser where you are logged in as admin in the Office365 demo tenant 2. Provision the "Cloud app security" license for one of the users by going to <https://portal.office.com>, "Admin"->"Active users" ->"Assigned license" and choose "Microsoft Cloud App Security". 3. After creation go to: <https://portal.cloudappsecurity.com> and login to the tenant 4. Go to General settings -> Organization details -> Managed domains and add your domain to the list   Ensure Pre Demo step 5 is complete and display the Cloud App Security browser session.   1. On the Top Navigation Bar, click **Discover**. 2. Click **Discovery Dashboard**. 3. On the Cloud Discovery Navigation Bar, click **512 Discovered App**. 4. Scroll down until you see the **Categories** section in the **Left Navigation Bar**. 5. Under **Categories**, click **Collaboration** to filter only **Collaboration** apps. 6. Scroll up to the top of the page. 7. Under the **Score** column, click Office 365’s score, **10**.   **Note**: Do not click on the Office 365 label itself (this will take you to a different page, described later).   1. Scroll down to parameter labeled **HTTP Security Headers** and hover over it. 2. Scroll up to the top of the page. 3. Under the **Score** column, click on Office 365’s score, **10**, to minimize the app details. 4. Under the **Name** column, click **Office 365**. 5. On the **Top Navigation Bar**, click **Investigate**. 6. Click **Files**. 7. On the **Filtering Bar**, click on the **Access Level** drop down menu. 8. Select **Public** (not **Public Internet**). 9. On the **Top Navigation Bar**, click **Control**. 10. Click **Policies**. 11. On the **Filter Bar**, click on the **Type** drop down menu. 12. Click **File Policy**. 13. Click outside of the drop down menu to minimize it. 14. Click on the **PCI Compliance**. 15. Click on the **Payment schedule and details.xlsx** file. 16. Under the **Violation Count** column for the **Payment schedule and details.xlsx** file, click **Matches**. 17. Click **Close**. 18. Below the file name, click on **View Hierarchy**. 19. Click **Done** to exit. 20. On the far right side, click on the **more information icon** (3 vertically stacked dots) for the **Payment schedule and details.xlsx** file. 21. Click the **more information icon** again to close drop down menu. 22. Click **Test\_file\_for\_DLP\_test.docx file**. 23. Under the **Violation Count** column for the **Test\_file\_for\_DLP\_test.docx file**, click **Matches**. 24. Click **Close**. 25. Below the file name, click **View Hierarchy**. 26. Click **Done** to exit.   **Note**: The following step is just to show you how to authorize a legitimate file. **DO NOT CLICK THE CHECK MARK**.   1. To the left of the **more information icon**, locate the **check mark** but do not click it. 2. On the **Top Navigation Bar**, click **Alerts**. 3. Scroll down to the first **General Anomaly Detection** alert. 4. Click **General Anomaly Detection**.   **Note**: If you click on any alert in the **Activity Log**, you can view a detailed report of that specific alert. |  |
|  |  |

## Demo Reset

1. Go back to the MyApps portal (as GarthF) and **leave group** for **sso-Contoso Bug Bashers**.

# Appendix 1: Configure your Demo Tenant

These steps need to be performed only once per demo tenant, and are required prior to performing demos or configuring devices for demoing.

## Add Your Authentication Phone and Email (for MFA verification) to Hero User

**Note**: You may already have performed these steps for Azure AD demo configuration.

1. Open a new browser session in **InPrivate mode** (<CTRL>+Shift+P).
2. Log in to your demo tenant’s Azure admin portal <https://manage.windowsazure.com/> as **Global Admin**,  
   [admin@<TENANT>.onmicrosoft.com](mailto:admin@%3cTENANT%3e.onmicrosoft.com) (corporate account) and password: pass@word1
3. In the list of ALL ITEMS, locate and click on your tenant’s **directory** name, labeled as **Contoso <TENANT>**.
4. Click **USERS** to view list of all directory users.
5. Locate and click on Garth Fort ([garthf@<tenant>.onmicrosoft.com](mailto:garthf@%3ctenant%3e.onmicrosoft.com)) in the directory.
6. In the WORK INFO page, scroll down to Authentication Contact Info, then fill in the following info:
   1. **Authentication Phone**: (provide your actual, real world mobile phone number)
   2. **Authentication Email**: (provide your actual, real world email address)
7. Click **Save**.

## Grant EMS License to Global Admin user

**Note**: Your demo tenant has free EMS licenses for up to 100 users. Most of the users in the demo AD are already assigned a license.

1. Go to **LICENSES** page, then click **ASSIGN** button (at bottom of the page).
2. Review the **ASSIGNMENT STATUS** column. Most of the users should already be **Enabled**.
3. Locate the global admin user ([admin@<tenant>.onmicrosoft.com](mailto:admin@%3ctenant%3e.onmicrosoft.com)).
4. Ensure the **admin** user is **Enabled**. If not, add to **ASSIGN** then click **Complete** (checkmark icon).
5. Repeat steps 10-11 for any other users/custom demo personas that you may have added that require an EMS license.

## Configuring Tenant for iOS Devices

**Estimated Setup Time: 15 minutes**

These steps need only be performed once per tenant. **Perform these steps using a desktop/laptop device (Windows 8.1 or higher)** (not an iOS device) using Internet Explorer or Firefox browser.

Before you can manage iOS mobile devices with Intune, you need an **Apple Push Notification service (APNs) certificate**. This certificate allows Intune to manage iOS devices and establish an accredited and encrypted IP connection with the mobile device management authority services. One Apple ID can be used for multiple demo tenants/demo iOS devices. **Skip to step #5** if you already have an Apple ID from a previous demo tenant setup.

**Note**: no such setup/certificates are required for Android device enrollment. However, you will need a Google Play account for downloading apps to your Android device.

### Create an Apple ID for Your Demo Tenant (if necessary)

1. Navigate to the following URL <https://appleid.apple.com/> and click **Create an Apple ID**.
2. Fill in the My Apple ID form as required:
   1. First Name: **Demo**
   2. Last Name: **Admin**
   3. Apple ID: [**admin@<tenant>.onmicrosoft.com**](mailto:admin@%3ctenant%3e.onmicrosoft.com) (replace <tenant> with appropriate value)

*The following values are provided as example only. Feel free to put in your own values that you can remember later*.

* 1. Password: **Contoso1** (do **not** use pass@word1 as it does not satisfy complex password requirement)
  2. Choose the 3 security questions from the drop-downs
  3. Security question answer 1: **Contoso 1**
  4. Security question answer 2: **Contoso 2**
  5. Security question answer 3: **Contoso 3**
  6. Date of Birth: **January 1, 1980**
  7. Mailing Address: (**your business address**)
  8. Uncheck Email preference options.
  9. Type in the captcha text as you see on the screen.

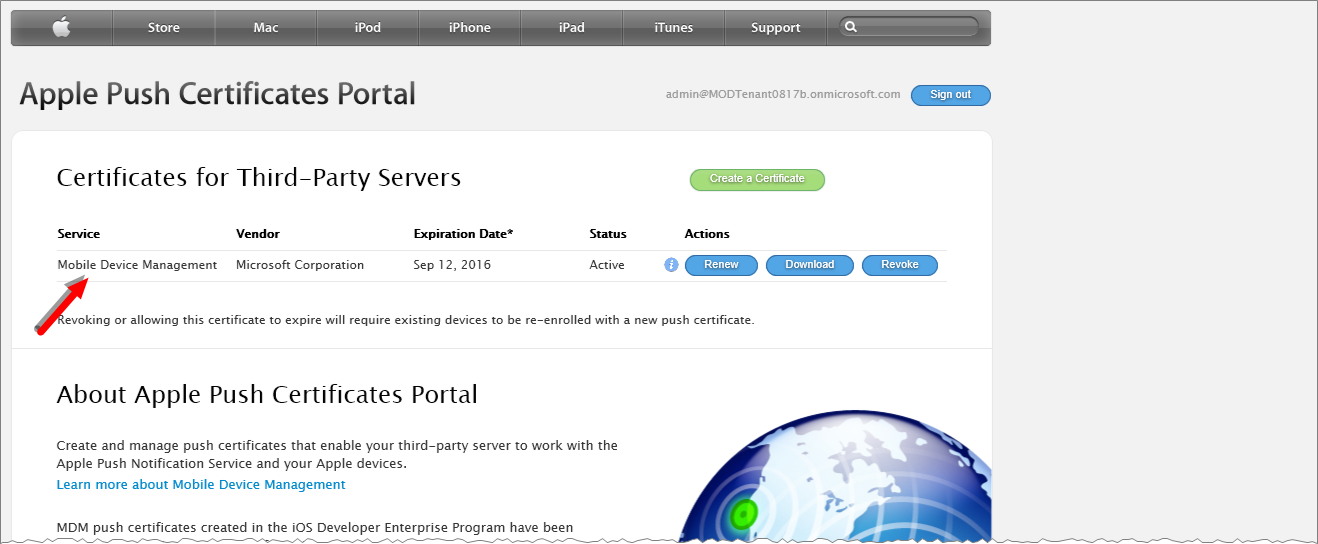
1. Click **Create Apple ID**.
2. To verify your email address:
   1. Browse to <https://outlook.office365.com/>.
   2. Log in with your Domain Admin credentials (same account you used for Apple ID above).
   3. Locate the email from Apple with subject **Verify your Apple ID**, then click **Verify now >** link in the body of the email.
   4. Log in with the user name and password you set up earlier for your Apple ID.

### Configure Intune Admin Settings for iOS Device Management

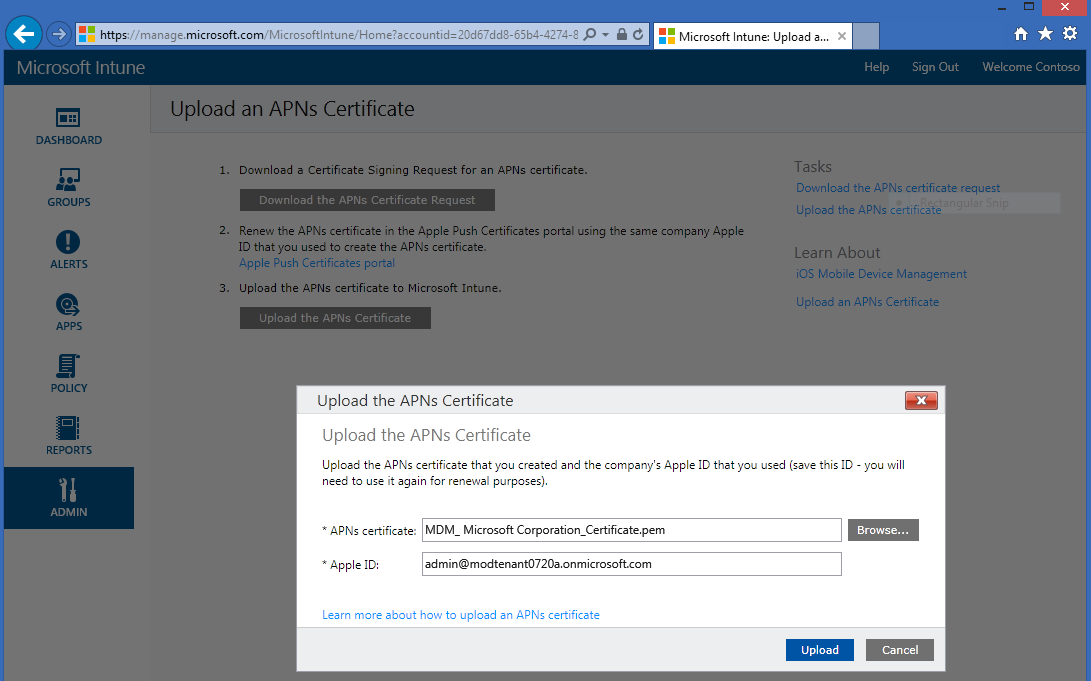
1. In the same browser session, navigate to the Intune management console site, at <https://manage.microsoft.com>. If you closed the previous browser session and are prompted for login, provide your demo tenant’s global admin’s credentials.
2. In the left navigation pane, click **ADMIN** (icon at the bottom).
3. Under **Administration** links, click **Mobile Device Management**.
4. In the Mobile Device Management page, under iOS section, click **Enable the iOS and Mac OS X platform**.
5. In the **Upload an APNs Certificate** page, click button **Download the APNs Certificate Request** (step 1).
6. In the Save As pop-up window, provide a file name by typing it (e.g. “MyDemoCSRFile”). Take a note of the local folder location you’re about to save the file to, then click **Save**.
7. Back on the Intune Admin page, click the link **Apple Push Certificates portal** (step 2). You will be taken to **Apple Push Certificates Portal** web site.

Note: If you closed the previous browser session and are prompted for login, provide the Apple ID credentials you set up earlier in step #2. **Note**: the password is not pass@word1 here!

1. Click **Create a Certificate**.
2. Accept Terms of Use by checking appropriate box and clicking **Accept**.
3. In the **Create a New Push Certificate** page, click **Browse…** under Vendor-Signed Certificate Signing Request.
4. Point to the .CSR file you saved to your local computer earlier (in step 6 above) and click **Open**.
5. Click **Upload**.
   * If you see a prompt to download a .json file, ignore it.
   * If you are not re-directed to a new page after 30 seconds, click **Cancel**, which will take you to **Apple Push Certificates Portal** page.



1. Click **Download** to download the mobile Device Management certificate. Save the file to a local folder on your PC with .pem file extension.
2. Return to the **Intune Administration** > **Upload an APNs Certificate** page.
3. Click **Upload the APNs Certificate** button.
4. Point to the APNs certificate you downloaded earlier (.pem file), type in the demo admin’s Apple ID, and click **Upload**.
5. In the Apple ID field, type in the Apple ID email address used to register the certificate, then click **Upload**.



1. You will see a confirmation page stating iOS is ready for enrollment.

Your demo tenant is now ready to accept iOS devices for enrollment!

## Apply Contoso Branding to Intune Company Portal

**Estimated Setup Time: 3 minutes**

1. Download Contoso company logo locally to your PC from <http://emsassetspub.blob.core.windows.net/demoassets/Logo.png>.
2. Log in to the **Microsoft Intune** management console, if necessary (<https://manage.microsoft.com>) as your demo tenant’s Global Administrator.
3. Go to **ADMIN** > **Company Portal** page.
4. Fill in the form as follows:
   1. IT department contact name: **IT Admin**
   2. IT department phone number: **800-555-1234**
   3. Support website URL: https://<tenant>.sharepoint.com/sites/contoso/Employee/ITWeb
   4. Website name: **IT Web**
   5. Customization: **Include company logo** to **ON**
   6. Select a logo to use on top of the selected color scheme (second option), click **Browse…**
   7. Point to the Contoso log you downloaded locally in step #1 above, then **Open**.
   8. Set Show the company name next to your company logo to **unchecked**.
5. Click **Save**. [**Note**: there is no save confirmation!]

## Create an App Policy for MAM without Enrollment

**Estimated Setup Time: 4 minutes**

If you wish to demo Intune’s Mobile Application Management without device enrollment, you will need to define a policy for your demo tenant using the new Azure portal:

1. Log in to the new Azure portal (<https://portal.azure.com>) as the Global Administrator user of your tenant ([admin@<tenant>.onmicrosoft.com](mailto:admin@%3ctenant%3e.onmicrosoft.com) and appropriate password).
2. In the left navigation, click **Browse** > **Intune**.
3. In the **Settings** blade, click **App Policies**
4. Click **Add a policy**, then complete the policy details as follows:
   1. Policy name: **MAM without enrollment**
   2. Platform: **iOS**
   3. Apps: (select all apps available by clicking checkmark next to each: Word, Excel, PowerPoint, OneDrive). Click **Select** to save selection.
   4. Settings: (leave default/recommended values). Click **OK** to save settings.
   5. Click **Create**.
5. In the **App policy** blade, click on the policy label just created to reveal policy settings blade.
6. Click **User groups** > **Add user group**
7. Select **sg-Sales and Marketing**, then click **Select**.
8. Repeat steps 4 – 7 above for **Android platform**.  
   **Please note**: the Apps available for Android platform may be fewer than for iOS.

Next, you’ll need to ensure another Intune conditional access policy does not conflict with this policy (i.e. ensure another policy that requires device enrollment for access to a corporate resource like SharePoint does not require device enrollment:

1. Using Internet Explorer or FireFox browser, log in to the Intune management portal (<https://manage.microsoft.com>) as a Global Administrator user of your demo tenant.
2. Go to **POLICY** > **Conditional Access** > **SharePoint Online Policy**
3. Ensure the **Enable conditional access policy** checkbox is **UNCHECKED**. If not, modify form values as follows:
   1. **Select** Device platforms: All platforms
   2. **Select** Targeted Groups: All users
   3. **UNCHECK** Enable conditional access policy
   4. Click **Save**.

## Add SaaS Applications to AAD

These steps need to be performed only once per demo tenant, and are required prior to performing demos.

**Estimated Setup Time: 5 minutes**

1. Open a new browser session in **InPrivate mode** (<CTRL>+Shift+P).
2. Log in to your demo tenant’s Azure admin portal <https://manage.windowsazure.com/> as **Global Admin**,  
   [admin@<TENANT>.onmicrosoft.com](mailto:admin@%3cTENANT%3e.onmicrosoft.com) (corporate account) and password: pass@word1
3. In the list of ALL ITEMS, locate and click on your tenant’s **directory** name, labeled as **Contoso <TENANT>**.
4. Go to **APPLICATIONS**.
5. Click **ADD**, then **Add an application from the gallery**.
6. Choose  **Salesforce** then click **complete** (checkmark icon).
7. Go back to APPLICATIONS tab and **repeat steps 5-6** to add the following SaaS applications.

**Note**: Most of the apps are optional (goal is to make a busy app dashboard later in the demo). Salesforce, BrowserStack and Twitter are **required** as some demo scenarios specifically depend on them.

* 1.  BrowserStack (required for self-service group demo)
  2.  Twitter (required for password rollover demo)
  3.  Evernote (optional)
  4.  Concur (optional)
  5.  LinkedIn (optional)

1. Configure BrowserStack application:
   1. Click BrowserStack from the list of applications.
   2. In the Quick Access page (), click **Assign accounts**.
   3. In the SHOW Groups STARTING WITH text box, type “ssg” then click search (checkmark icon [Complete](https://manage.windowsazure.com/MOD46935.onmicrosoft.com)).
   4. Highlight **ssg-Contoso Bug Bashers**, then click **ASSIGN**.
   5. Click checkmark icon to **Complete**.
2. [Optional] Repeat step 8 for the following apps: Evernote, LinkedIn, Concur and **ASSIGN** to **All Employees** group.

## Configure Salesforce SSO Integration

**Estimated Setup Time: 30 minutes**

You can use Salesforce as an example to demonstrate secure, single sign-on integration with a third-party SaaS application. For this demo to succeed, you’ll need to create a new Salesforce account for your demo tenant and configure the SSO.

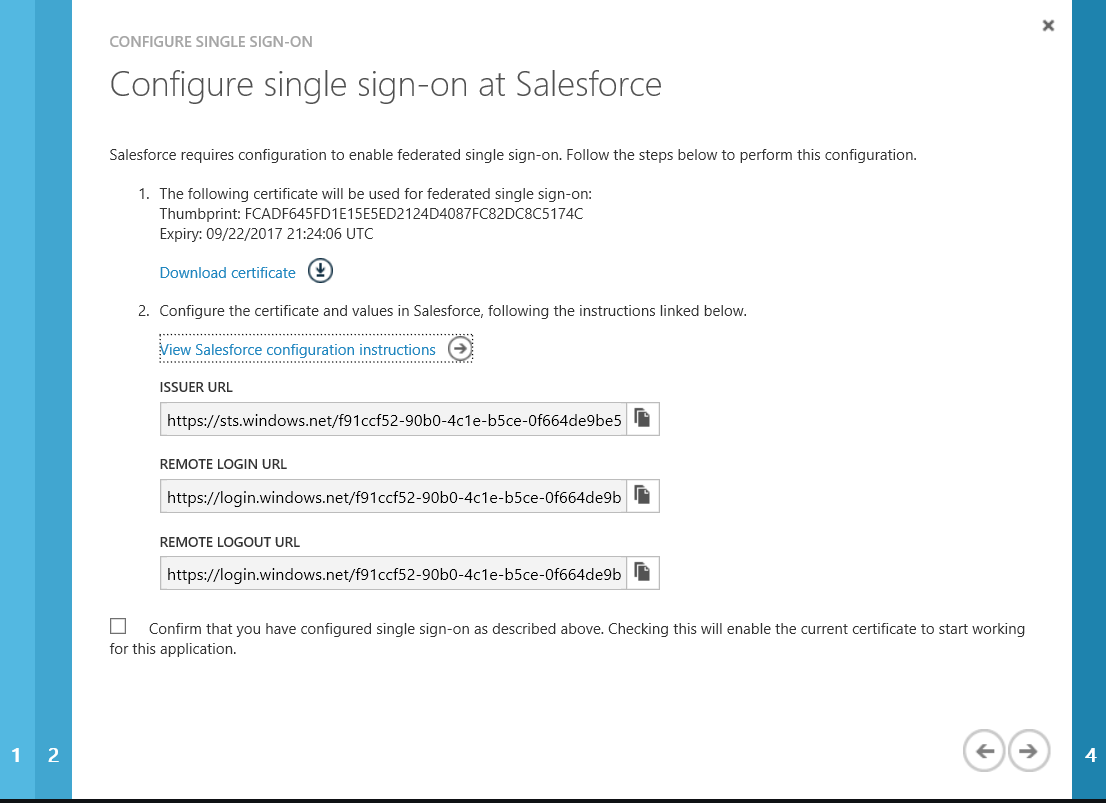
**Sign up for a Salesforce Developer Account:**

You can sign up for a free Salesforce Developer Environment account through the Salesforce website, as detailed below.

1. In a new browser tab, navigate to <https://developer.salesforce.com/signup>.
2. Fill up the form as follows:
   1. First Name: Contoso
   2. Last Name: Admin
   3. Dropdown option: **Developer**
   4. Email: admin@<tenant>.onmicrosoft.com
   5. Company: Contoso
   6. Country/Postal Code: (as appropriate)
   7. Username: admin@<tenant>.onmicrosoft.com
3. Check Master Subscription Agreement checkbox, then click **Sign me up**.
4. When promoted to check email to confirm account:
   1. Launch a new, **InPrivate** browser session.
   2. Sign in to <https://outlook.office365.com> as admin@<tenant>.onmicrosoft.com and pass@word1.
   3. Locate the email from Salesforce and click on the link provided. You’ll be taken to Salesforce web site.
5. Provide a new password: pass@word1
6. Pick a security question and answer it.
7. Click **Save**. You’ll be taken to the Salesforce Home page. Keep this page open.

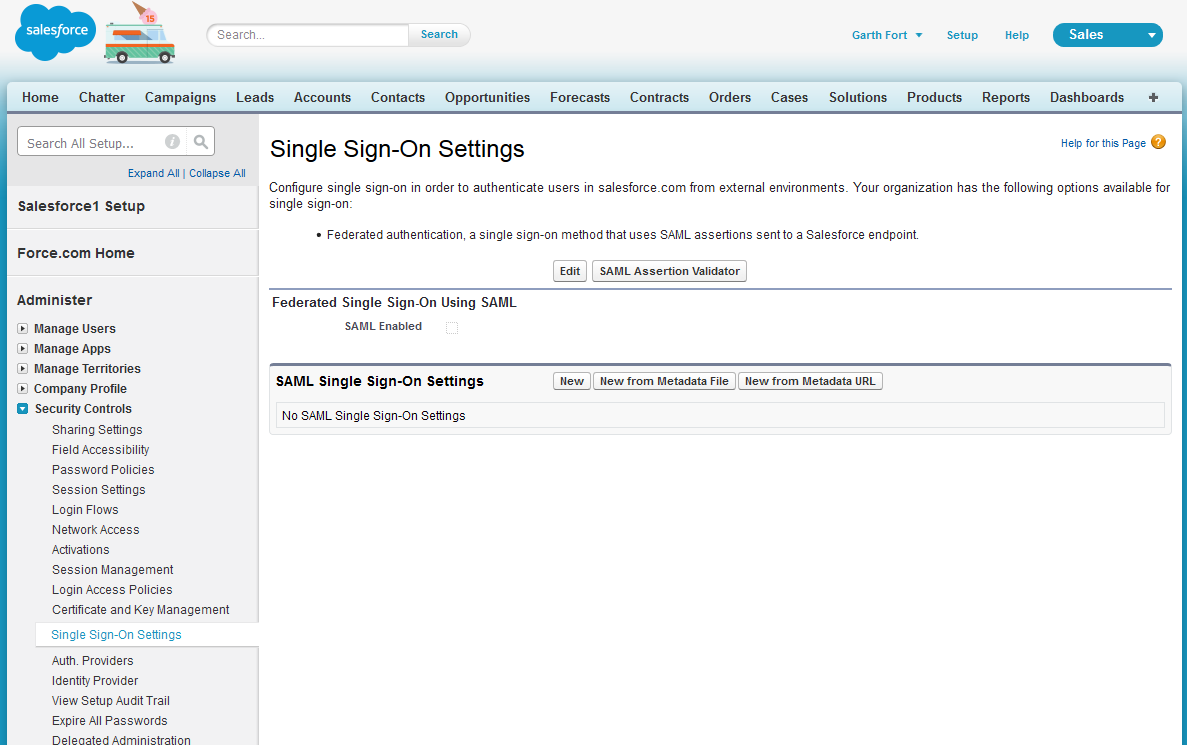
**Configure Azure to Salesforce Single Sign-On:**

1. In a **new browser session**, log in to the Azure Management Portal (<https://manage.windowsazure.com>) as your tenant’s Global Admin user ([admin@<tenant>.onmicrosoft.com](mailto:admin@%3ctenant%3e.onmicrosoft.com)).
2. Go to your demo Active Directory, **APPLICATIONS**, then click **Salesforce**.
3. Click **Configure single sign-on**.
4. Select **Microsoft Azure AD Single Sign-On**, then **next** icon (🡪).
5. For SIGN ON URL, type **https://<tenant>-dev-ed.my.salesforce.com** (**Important**: replace <tenant> with your appropriate value), then click **next**.
6. On the **Configure single sign-on at Salesforce** page, to download your certificate, click **Download certificate**, and then save the certificate file locally on your computer.

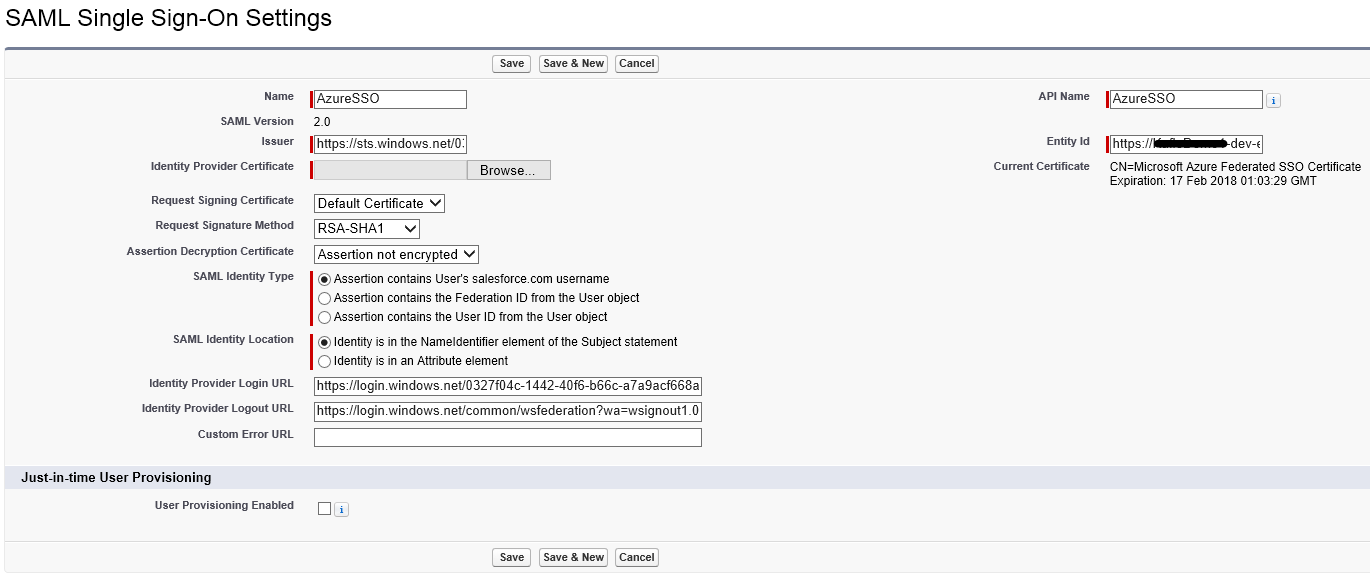


**Important**: Keep this page/dialog window open as you’ll need to copy values into Salesforce later.

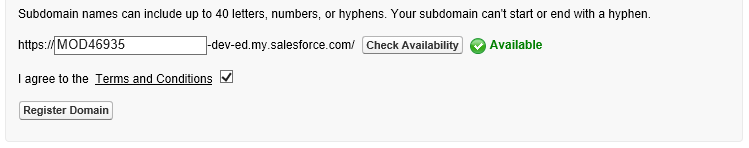
1. Switch to the browser session with **Salesforce**.
2. In the left navigation, under **Administer**, expand **Security Controls**, then click **Single Sign-On Settings**.



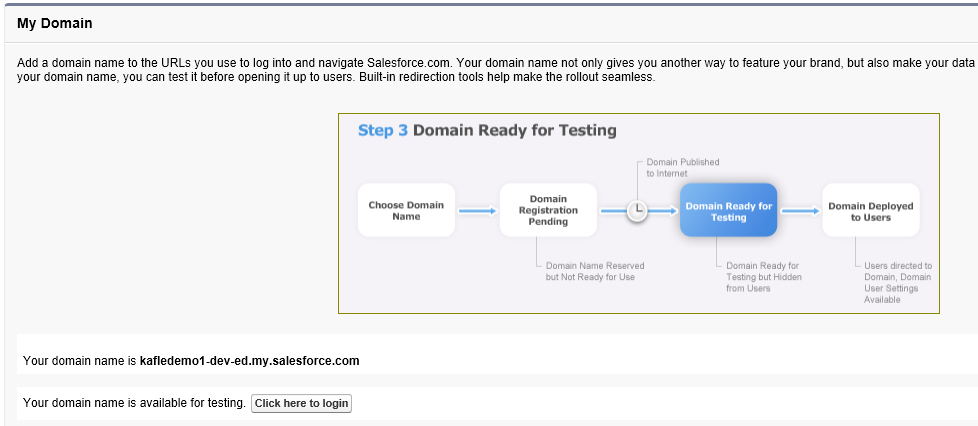
1. Under **Single Sign-On Settings**, click **Edit**.
2. Select **SAML Enabled**, and then click **Save**.
3. Under **SAML Single Sign-On Settings**, click **New**.
4. Fill in the SAML Single Sign-On Settings form as follows (also see screen shot on next page for example):
5. Name: **AzureSSO**
6. Issuer: [**Copy+Paste the** **ISSUER URL** value from the Azure configuration dialog]
7. Entity ID: **https://<tenant>-dev-ed.my.salesforce.com** (replace <tenant> with appropriate value)
8. Identity Provider Certificate: [Click **Browse** and point to the certificate file you downloaded earlier from Azure].
9. SAML Identity Type: default selection (Assertion contains User's salesforce.com username).
10. SAML Identity Location: default selection (Identity is in the NameIdentifier element of the Subject statement).
11. Identity Provider Login URL: [**Copy+Paste the Remote Login URL** value from the Azure configuration dialog].
12. Identity Provider Logout URL: [**Copy+Paste the Remote Logout URL** value from the Azure configuration dialog].
13. Leave all other fields with their default values.
14. Click **Save** to apply your SAML single sign-on settings.

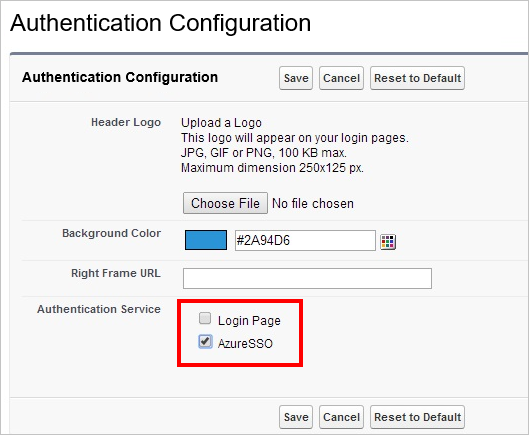


1. On the left navigation pane in Salesforce, expand **Domain Management**, then click **My Domain**.
2. Under My Domain, type your tenant name (e.g. MOD46935) in the Subdomain text box, as shown:



1. Click **Check Availability** to verify, check **Terms and Conditions**, then click **Register Domain**.
2. **Wait 10 minutes** while your custom domain name is being published. Refresh until you see the graphic status on the page move to **Step 3 Domain Ready for Testing**.



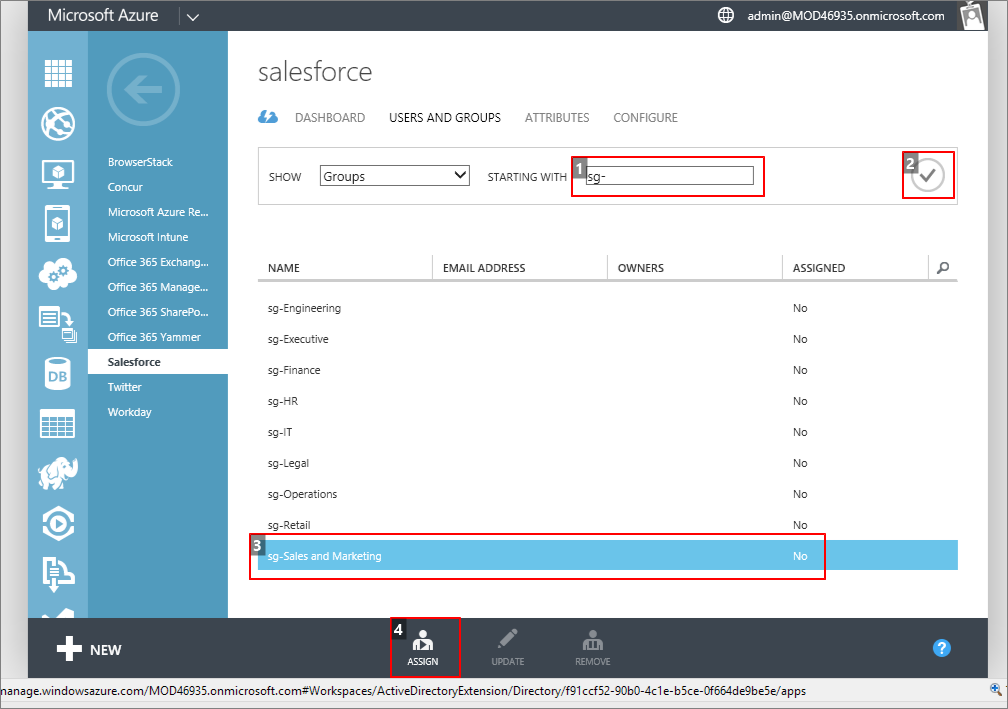
1. Click button labeled **Click here to login**.
2. If necessary, login with your Salesforce administrator user ID ([admin@<tenant>.onmicrosoft.com](mailto:admin@%3ctenant%3e.onmicrosoft.com)) and pass@word1.
3. When prompted to register your mobile phone, click **I Don’t Want to Register My Phone**.
4. Back in the My Domain page, click **Deploy to Users**. Click **OK** to dismiss warning prompt.
5. Under **Authentication Configuration**, click **Edit.**
6. Fill in the Authentication Configuration form as follows, then **Save**.
   1. Header Logo: (click Browse…, then upload logo from file located at <http://emsassetspub.blob.core.windows.net/demoassets/Logo-250.png>)
   2. Authentication Service: **AzureSSO** (uncheck other options).  
      
7. Go back to **Security Controls > Single Sign-On Settings > AzureSSO**, then click **Edit**.
8. Under **Service Provider Initiated Request Binging**, select **HTTP Redirect**, then **Save**.
9. Switch to the browser tab/session with **Azure AD SSO configuration** page.
10. Check the box for **Confirm that you have configured single sign-on**, then click **next** (🡪).
11. Click **Complete** icon [Complete](https://manage.windowsazure.com/MOD46935.onmicrosoft.com).

**Configure User Provisioning for Salesforce:**

1. In the Azure Management Portal page, click **Configure account provisioning**.
2. Fill in Salesforce Admin user name: [admin@<tenant>.onmicrosoft.com](mailto:admin@%3ctenant%3e.onmicrosoft.com) and password (pass@word1).
3. Switch to the browser window/tab with **Salesforce**.
4. Click **Contoso Admin** (user menu at top of the page), then **My Settings**.
5. In the left navigation, expand **Personal**, then click **Reset my Security Token**.
6. Click **Reset Security Token** button. A security token will be sent to the current user (Admin) via email.
7. Switch to the browser window/tab with Admin’s email, then locate the new email from Salesforce.
8. **Copy the Security Token** from the body of the email (e.g. Jaw9XnUhe0PxN1flSE6P5GVwF).
9. Return to the Azure Management Portal page.
10. Paste the security token under **User Security Token** field, then click next (🡪).
11. Click **Start Test** to verify SSO integration.
12. Once confirmed, click next (🡪) twice.
13. Check the **Start automatic provisioning now option**, then click Complete icon [Complete](https://manage.windowsazure.com/MOD46935.onmicrosoft.com).

**Configure User Provisioning for Salesforce:**

1. Under **Assign users to Salesforce**, click **Assign accounts**.
2. In the USERS AND GROUPS page, choose **SHOW Groups** (dropdown), under STARTING WITH type “**sg-**“, then click **checkmark**.



1. Highlight **sg-Sales and Marketing**, then click **ASSIGN**.
2. Select Salesforce Profile to **Chatter Free User**, then click **Complete**.

**Configure Salesforce Access Rule to Require MFA:**

1. Under **Assign users to Salesforce**, click **Assign accounts**.
2. In the Salesforce application page, click **CONFIGURE**.
3. Scroll down to **multi-factor authentication and location based access rules** and configure the following values:
   1. ENABLE ACCESS RULES: **ON**
   2. APPLY TO: **ALL USERS** (default)
   3. RULES: **Require multi-factor authentication** (default)
4. Click **Save**.

## Configure Twitter Integration

**Estimated Setup Time: 10 minutes**

You will be using the Twitter app to demonstrate password roll-over feature in Azure AD.

**Sign up for a Demo Twitter Account:**

You will need to sign up for a new Twitter account just for this demo tenant, at [twitter.com](http://www.twitter.com).

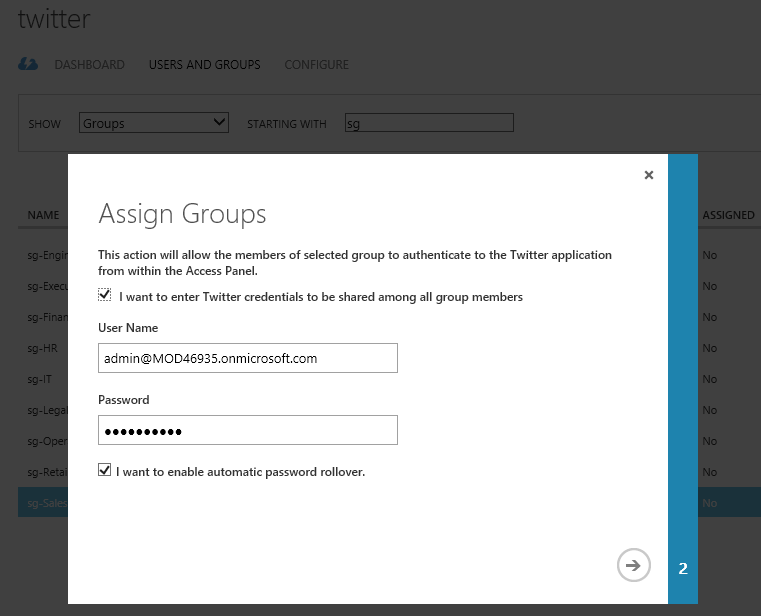
1. In a new InPrivate browser session, navigate to <https://twitter.com/signup>.
2. Fill up the form as follows:
   1. Full Name: **Contoso Demo**
   2. Email address: **admin@<tenant>.onmicrosoft.com**
   3. Password: **pass@word1**
   4. Username: **Contoso<tenant>**, e.g. ContosoMOD45654  
      **Important**: This will be the Twitter handle, hence needs to be unique!
3. Click **Sign Up**.
4. On the **Enter your phone** page, provide your mobile phone number, then click **Continue**.
5. Click **Let’s go**.
6. In the **What are you interested in?** page, check **Business,** then click **Continue**.
7. In the **Suggestions just for you** page, check to **unselect all** items, then click **Continue**.
8. Click **Upload your photo** > **Upload photo**.
9. In the **File name** field, paste the Contoso logo URL: <https://spdoclibrary.blob.core.windows.net/documents/Contoso-200x200.png>, then click **Open**.
10. Click **Apply** to apply the logo as display image for the new Twitter account.
11. Click **Continue**.
12. In the **Find people you know p**age, click **Skip this step**.

**Confirm email address for Twitter account:**

1. In a new browser tab, navigate to <https://outlook.office365.com> and login as [admin@<TENANT>.onmicrosoft.com](mailto:admin@%3cTENANT%3e.onmicrosoft.com).
2. Locate the email from Twitter, then click **Confirm now** link on the email body.

**Configure Single Sign-On**

1. In a new browser tab (same browser session), navigate to Azure Management Portal, <https://manage.windowsazure.com>. You will be logged in as your demo tenant’s global admin.
2. Go to the demo tenant’s Active Directory, **APPLICATIONS** page, then click **Twitter**.
3. Click **Configure single sign-on**.
4. Select **Password Single Sign-On**, then click **Complete**.
5. Click **Assign Accounts**.
6. Highlight **sg-Sales and Marketing**, then click **ASSIGN**.
7. In the Assign Groups dialog, check **I want to enter Twitter credentials** to be shared among all group members.
8. Type in the Twitter user name and password you set up earlier.



1. Check **I want to enable automatic password rollover**, then click **next** (🡪).
2. In the Configure Password Rollover page, leave the default value (4 weeks) then click **Complete**.

# Appendix 2: Installing/Configuring Azure RemoteApp (ARA)

**Important Notes:**

* If you want to perform Desktop Virtualization demo using Azure RemoteApp (ARA), you’ll need to manually deploy an app collection to your Azure tenant.
* If your demo tenant was provisioned prior to March 18 2016, a RemoteApp collection may have been provisioned already.
* The free trial of a RemoteApp collection is free, but has the following limitations:
  + Expires 30 days from the date of provisioning.
  + Limit of 2 free RemoteApp collections per Subscription ID.
* If your RemoteApp collection free trial period has expired, you have the option to continue your subscription but will be charged.
  + Please refer to the [Azure RemoteApp Pricing Plans](https://www.microsoft.com/en-us/server-cloud/products/azure-remoteapp/Purchasing.aspx) for more details.

## Installing Azure RemoteApp

1. Open a new browser session in **InPrivate mode** (<CTRL>+Shift+P).
2. Navigate to the **Azure Management Portal**, <https://manage.windowsazure.com/>
3. Log in using your demo tenants **Global Admin** credentials, i.e. [admin@<TENANT>.onmicrosoft.com](mailto:admin@%3cTENANT%3e.onmicrosoft.com).

NOTE: (IMPORTANT INFORMATION for Step 8)

Upon logging in your default view should be in the **ALL ITEMS** window, if not, please navigate to the all items window. In the **ALL ITEMS** window, please take note of the **REGION** your **Azure Active Directory (AAD)** is located in. This can be found under the **LOCATION** column, the far right column (next to the search bar)

1. Using the Navigation Bar, located on the left hand side, locate and click on the **REMOTEAPP** tab.
2. Locate and click on the **CREATE A REMOTEAPP COLLECTION** button
   1. Performing this action will enable your free 30-day trial, which limits you to 2 RemoteApp collections per subscription.
3. Type desired **NAME** (Name can only contain letters and numbers, no spaces)
4. Choose a **REGION:**

NOTE:

In order to minimize cost, select the region closest to the location of your storage. If you do not currently have a storage, base your choice of REGION using your AAD location (storage location should also be based off of your AAD location as well). This is referencing the note from Step 3.

1. Leave **PLAN** type as default setting: Basic
2. Select **TEMPLATE IMAGE:** **Office 365 ProPlus**
3. Click **CREATE REMOTEAPP COLLECTION** when done

NOTE:

Once you click **CREATE REMOTEAPP COLLECTION**, this will start the actual creation of your ARA. This process can take up to 2 hours.

1. Continue to the next section, Configuring Azure RemoteApp, to finalize ARA.

## Configuring Azure RemoteApp

1. Upon completing the creation of your ARA, you should already be in the **REMOTEAPP** tab. If not, navigate to the **REMOTEAPP** tab.
2. You should see your named ARA in the RemoteApp tab
3. Click on your **ARA**
4. In the **Top Menu Bar**, click on the **Publishing** tab

NOTE:

The publishing tab is where you select or deselect applications you wish to have available in ARA.

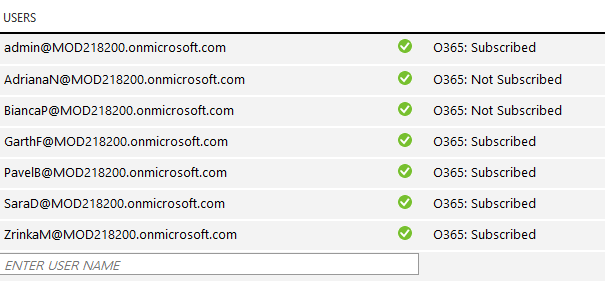
\*\*\*There is the option to add third party applications but that will not be covered in this guide.

1. Verify all Office 365 items in this tab has a green check mark and is labelled as **PUBLISHED** under the **STATUS** column.
2. Upon verifying your published applications, navigate to the **USER ACCESS** tab located on the **Top Menu Bar**.

NOTE:

By default, your [admin@<TENANT>.onmicrosoft.com](mailto:admin@%3cTENANT%3e.onmicrosoft.com) account will be the only account located in the user access tab.

1. To add new users to your subscription, type the user’s email address, [xxxxxx@<TENANT>.onmicrosoft.com](mailto:xxxxxx@%3cTENANT%3e.onmicrosoft.com), into the text box labelled **ENTER USER NAME** (located right below your administrator account). Once you type the user’s email address into the text box, ARA will search for that user in AAD then add him/her to the subscription. Repeat this step for additional users.
   1. For demo purposes, here is a list of user credentials you can use:



Once finished adding users, click **SAVE**.

# Appendix 3: Configure Your Demo Devices

Currently, the demo configuration and documentation has been tested against iOS devices only. We are working on incorporating other devices (Android and Windows Phone) as well.

## Mobile Device Requirements

* iOS (iPad or iPhone) running latest version of iOS; or Android device (phone or tablet) running OS v4.4.2 or higher.
  + Ideally, **two** such devices to be able to perform Conditional Access and Mobile Application Management demos back-to-back without setup time in between.
* Ensure devices are free of Office mobile apps (delete if they exist). If feasible, perform factory reset of the device.
* Ensure you have an Apple ID (if using iOS device) or Google Play account (for Android device) as you’ll be prompted for credentials during the setup. If you need to setup a new Apple ID, refer to the Create Apple ID section under Appendix 1.

## Device Setup Steps

**Estimated Setup Time: 30-45 minutes**

### Set Up Device #1 (iOS or Android)

The following demos will be presented on Device #1: **MAM without Enrollment** and **Conditional Access** policy.

1. Go to the App Store (for iOS) or Google Play Store (for Android) and **download/install** the following apps:
   1. Microsoft Intune Company Portal
   2. Microsoft Outlook
   3. Microsoft Word
2. Launch **Word** application. Dismiss any app initialization/startup messages/prompts.
3. In Word, sign in as your demo persona (e.g. [GarthF@<tenant>.onmicrosoft.com](mailto:GarthF@%3ctenant%3e.onmicrosoft.com) and password).
4. Tap **Open** > **SharePoint**.
5. You’ll see a prompt to set a PIN for the app (since you’re about to access company data). Set a 4-digit numeric PIN (e.g. 1111).
6. Tap on the label of SharePoint instance of your tenant (e.g. **Contoso <TenantName>**) then open a Word document from SharePoint (e.g. **DemoDocs** folder > **Northwind Proposal**.docx )
7. If necessary, **sign in again** as your demo persona (e.g. [GarthF@<tenant>.onmicrosoft.com](mailto:GarthF@%3ctenant%3e.onmicrosoft.com) and password).
8. Attempt to make an offline copy (a.k.a. Save As or Duplicate) of the file as follows:
   1. Tap **File** > **Duplicate**
   2. Choose location to duplicate: **<local device>** (e.g. iPad)
   3. Tap **Duplicate**.
9. If you see a prompt saying “Your administrator doesn’t allow saving to personal locations.” then your MAM Without Enrollment policies are working!
10. Tap **OK**, then **Cancel** to dismiss Save As attempt.
11. Tap back arrow (🡨) to close the Word document, then close Word app on your device.

### Set Up Device #2 (iOS or Android)

You will perform the majority of mobile demos, including the Mobile Application Management demo, on this device.

1. Go to the App Store (for iOS) or Google Play Store (for Android) and search for **Microsoft** **Intune**.
2. Download/install the app **Microsoft Intune Company Portal**.
3. Launch the installed app.
4. Sign in to Intune Company Portal with the following account: [garthf@<tenant>.onmicrosoft.com](mailto:garthf@%3ctenant%3e.onmicrosoft.com) and pass@word1

**TIP**: copy the account email address in your device’s buffer so you can paste it easily later, instead of typing it each time!

1. On Device Enrollment dialog, tap **Enroll**. You will be re-directed to device settings app.
2. On Install Profile, tap **Install**.
3. Enter device passcode (prompted if device currently has a passcode).
4. On Install Profile, tap **Install**.
5. On Warning, tap **Install**.
6. On Remote Management, tap **Trust**.
7. On Profile Installed, tap **Done**. You’ll be directed back to the Company Portal app.
8. On Device Enrolled confirmation, tap **OK**.
9. On Compliance Details, wait for compliance confirmation (“This device is no longer out of compliance” message) tap **OK**.
10. If your device does not have a passcode, you’ll see a prompt to set a passcode within 60 minutes. Tap **Continue**, then set a 4-digit passcode (e.g. 1111)

**Important**: Note your new passcode. You’ll need this passcode to unlock your device each time from now!

1. Back in Intune Company Portal app, tap **Company Apps**.
2. Tap on each of the following apps then **Install** (note: for each app, you’ll see App Installation confirmation pop-up message after 10-20 seconds. Tap **Install** to confirm).
   1. Outlook (required for demo flow)
   2. Word (required for demo flow)
   3. Managed Browser (required for demo flow)
   4. My Apps (optional but recommended)
   5. PowerPoint (optional but recommended)
   6. Excel (optional but recommended)
   7. RMS Sharing App (optional but recommended)
   8. OneDrive for Business (optional but recommended)

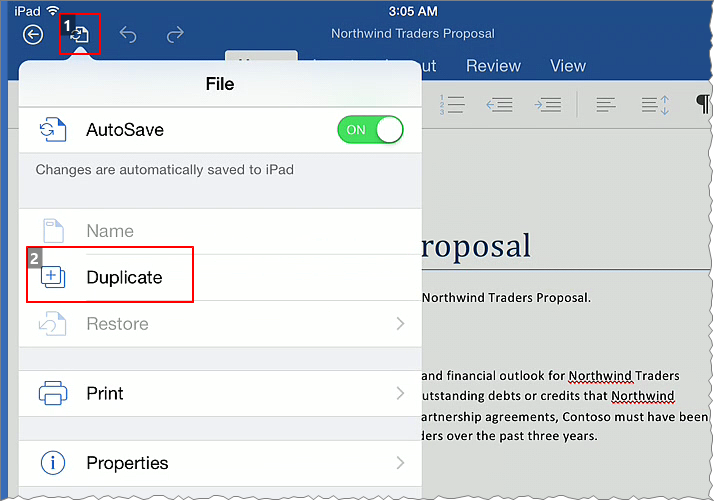
**Note**: Depending on your internet speed, it may take 10-30 minutes for these apps to finish installing to your device! We recommend you start by installing Outlook first as it requires further setup.

#### Setup Outlook/Emails/Dropbox:

1. When **Outlook** app has finished installing, tap on its icon to launch it.
2. If prompted to set up a numeric pin, tap an easy to remember 4-digit number, e.g. **1111**.
3. In Add an Account page, tap **Office 365**.
4. In the Office 365 login page, paste Garth Fort’s corporate email address ([**garthf@<tenant>.onmicrosoft.com**](mailto:garthf@%3ctenant%3e.onmicrosoft.com)).
5. Type in GarthF’s password (**pass@word1**) then tap **Sign in**.
6. **Dismiss** the Outlook app tips.
7. Tap **Settings** at the bottom of the screen, then **+ Add Account.**
8. Tap **Outlook.com**.
9. In the Outlook.com Sign in page, type your demo Live ID user email address (e.g. **MyDemoUser@outlook.com**) and **select/copy the email address** in clipboard memory (for use later).
10. Type the Live ID password then tap **Sign in**.
11. Let this app access your info? Tap **Yes**.
12. Tap **Settings** at the bottom of the screen, then **+ Add Account.**
13. Tap **Files** > **Dropbox**.
14. In the Dropbox sign in page, paste your demo Live ID email address (e.g. **MyDemoUser@outlook.com**), type password, then tap **Sign in**.
15. At the prompt “Let this app access your account info” tap **Yes**.

#### Setup/Configure Word

1. In Garth’s corporate inbox, scroll down and tap on an email from Alex Darrow (subject **Northwind Proposal**).
2. Tap **Open in Word** for the included email attachment. The Word app will launch.
3. Since this is the first time you’re launching Word app on this device, you’ll see several welcome messages and tips. Dismiss all such messages.
4. When prompted to sign in to Office 365, provide **GarthF**’s credentials, and continue.
5. When the attachment document finally opens, tap the **File** menu icon in Word app, then **Duplicate**.



1. Tap **Add a Place.**
2. Tap **Dropbox**.
3. In the Dropbox login page, paste Garth Fort’s personal email address ([garth.fort@hotmail.com](mailto:garth.fort@hotmail.com)), and type his password (Contoso1) then tap **Sign in and Link**.
4. Tap **Dropbox – Personal** to select it, then tap **Save**.

If you see an alert box with message: “Your administrator doesn’t allow saving to personal locations.” then your MAM smoke test is successful

1. Dismiss/cancel the pop-up dialog boxes in Word.
2. Close the Northwind Traders Proposal document by tapping the exit icon, .

#### Setup Azure RemoteApp Access

1. Install the **Microsoft Remote Desktop** app from the iOS App store:
   1. Launch the **App Store** app on your device.
   2. Search for the app **Remote Desktop** (see app icon below as hint), then **install** it.  
      
   3. If promoted, provide your Apple ID credentials for authentication to the App Store.
2. Launch the app on your device (the app will be labeled as **RD Client**.)
3. Within the Microsoft Remote Desktop app, tap the **+** button (top-right corner), then **Add Azure RemoteApp**, and **Continue**.
4. In the Sign In page, provide your demo persona’s corporate login credentials: [garthf@<tenant>.onmicrosoft.com](mailto:garthf@%3ctenant%3e.onmicrosoft.com), then continue.
5. You will see the Microsoft Remote Desktop apps page, similar to below:



1. Tap **Excel** icon to launch. You may be prompted with a login screen again. Provide your demo persona’s email address and password.
2. In the RemoteApp session of Excel, you’ll be prompted to **Activate Office**. Once again, provide your demo persona’s email address, work account, and password.
3. In the First things first pop-up, choose **Use recommended settings**, then click **Accept**.
4. If you see no files listed under Open, Recent Workbooks, follow these steps:
   1. Click Open Other Workbooks, One Drive – Contoso <Tenant>, then Browse.
   2. Open the file **Contoso Purchasing Data - 2014.xlsx** from Garth Fort’s OneDrive for Business.
5. Close the Excel application window.