

Microsoft Intune

Core Product Guide

Updated: October 21st, 2018

Contents

[Demo Overview: Intune– Core 3](#_Toc526164643)

[Scenarios and Features 3](#_Toc526164644)

[Intended Audience 4](#_Toc526164645)

[Length 4](#_Toc526164646)

[Demo Prerequisites 4](#_Toc526164647)

[One-Time Demo Environment Setup 4](#_Toc526164648)

[Blocking access from untrusted locations 5](#_Toc526164649)

[Pre-Demo Steps 5](#_Toc526164650)

[Demo Reset Steps 9](#_Toc526164651)

[Requiring device enrollment for mobile application access 9](#_Toc526164652)

[Pre-Demo Steps 9](#_Toc526164653)

[Demo Reset Steps 13](#_Toc526164654)

[Requiring multi-factor authentication for applications 14](#_Toc526164655)

[Pre-Demo Steps 14](#_Toc526164656)

[Demo Reset Steps 16](#_Toc526164657)

[Appendix 1: Configure your Demo Environment 17](#_Toc526164658)

[Install Access Panel browser extension 17](#_Toc526164659)

[Configuring SaaS app for scenario Blocking access from untrusted locations 17](#_Toc526164660)

[Configuring SaaS app for scenario Requiring multi-factor authentication for applications 18](#_Toc526164661)

[Create Exchange Online Conditional Access Policy 19](#_Toc526164662)

[Configure Apple Push Notification Service Certificate for scenario Requiring device enrollment for mobile application access 20](#_Toc526164663)

[Create an Apple ID (if necessary) 20](#_Toc526164664)

[Configure Intune Admin Settings for iOS Device Management 20](#_Toc526164665)

[Appendix 2: Configure Your Demo Devices 22](#_Toc526164666)

[Requiring device enrollment for mobile application access 22](#_Toc526164667)

[Requirements: 22](#_Toc526164668)

[Set up Steps: 22](#_Toc526164669)

# Demo Overview: Intune Core Functionality

Now more than ever, people are connected. With smartphones, tablets, laptops, and PCs, people have an increasing number of options for getting and staying connected at any time. Users expect the freedom to access their corporate email and documents from anywhere on any device – and they expect the experience to be seamless and modern. IT, on the other hand, needs to make sure that corporate data is secure while enabling users to stay productive in today’s mobile-first world, where the threat landscape is increasingly complex and sophisticated.

Conditional access provides the control and protection you need to keep your corporate data secure, while giving your people an experience that allows them to do their best work from any device. With Enterprise Mobility + Security, you can define policies that provide contextual controls at the user, location, device, and app levels. You can allow or block access or challenge users with Multi-Factor Authentication, device enrollment, or password change. Plus, our machine learning-based identity protection, which leverages billions of signals daily, can detect suspicious behavior and apply risk-based conditional access that protects your applications and critical company data in real time.

With conditional access by Enterprise Mobility + Security, you get the control you need to ensure your corporate data is secure, while your people roam freely between apps and devices, accessing your data in the cloud and on premises.

**Increase productivity and reduce helpdesk costs with self-service and single sign-on experiences**

Employees are more productive when they have a single username and password to remember and a consistent experience from every device. They also save time when they can perform self-service tasks like resetting a forgotten password, or requesting access to an application, without waiting for assistance from the helpdesk.

**Manage and control access to corporate resources**

Microsoft identity and access management solutions help IT protect access to applications and resources across the corporate datacenter and into the cloud, enabling additional levels of validation such as multi-factor authentication and conditional access policies. Monitoring suspicious activity through advanced security reporting, auditing and alerting helps mitigate potential security issues.

## Scenarios and Features

The Intune Core demo guide will cover the following technical scenarios listed below. Please note some scenarios are available as PowerPoint click through demos only as these require a lot of setup to perform live using a demo environment.

|  |  |  |
| --- | --- | --- |
| Scenario & Value Prop | Technical Scenario | Demo Resources/Links |
| **Blocking access from untrusted locations** | Configuring location-based conditional access | [Demo Script](#_Blocking_access_from) |
| Access resources from an untrusted location |
| Adding trusted locations |
| Access resources from a trusted location |
| **Requiring device enrollment for mobile application access** | Configuring device-based conditional access | [Demo Script](#_Requiring_device_enrollment) |
| Enrolling device for access |
| **Requiring multi-factor authentication for applications** | Configuring application-based conditional access | [Demo Script](#_Requiring_multi-factor_authenticati) |
| Application access using MFA |

This guide covers the **Microsoft Intune Core** scenarios. The other scenarios are in other demos guides that can be downloaded from <https://demos.microsoft.com>.

## Intended Audience

IT Pros, Business Decision Makers

## Length

30 minutes

## Demo Prerequisites

1. A Microsoft 365 demo environment equipped with Microsoft 365 Enterprise Demo Content, available through demos.microsoft.com portal.
2. An iOS mobile device (iPhone or iPad) running iOS 9 or higher.
   1. Android devices are supported as well. For detailed instruction on using Android devices with Intune, please [review this article](https://docs.microsoft.com/en-us/intune/enduser/using-your-android-device-with-intune).
3. A Windows PC or Virtual Machine running the latest version of Windows 10.

## One-Time Demo Environment Setup

Your demo tenant is pre-provisioned with plenty of content and settings that you can leverage as-is. However, some settings need to be manually configured by you. Please ensure the following activities are performed against your tenant prior to your first demo:

1. If you plan to use custom demo personas for your demo, ensure the user accounts are appropriately licensed for EMS and Office 365. You may use the Office Admin Portal (<https://portal.office.com> then click **Admin** tile) to review and modify the tenant subscription and user licensing status.
2. Perform one-time manual setup steps against your **demo environment** as detailed in [**Appendix 1**](#_Appendix_1:_Configure).
3. Prepare your demo **mobile device** as detailed in [**Appendix 2**](#_Requiring_multi-factor_authenticati_1).

Review, and if necessary, execute the scenario-specific pre-demo setup steps specified at the beginning section of each demo.

# Blocking access from untrusted locations

## Pre-Demo Steps

1. Ensure that the set-up steps in [Appendix 1](#_Conditional_access_for) have been completed.
2. Open a browser window (not InPrivate) in Microsoft Edge to <https://portal.azure.com>.
3. Log in with your global admin credentials: **admin@<tenant>.onmicrosoft.com**, and tenant password.
4. Browse to <https://www.whatismyip.com/>.
5. Make a note of the IP address displayed.

**Note:** Azure Multi-Factor Authentication only supports IPv4 addresses. If your ISP is only allocating IPv6 addresses, you will not be able to add the address to the trusted IPs.

1. Close the <https://www.whatismyip.com/> browser tab.

| Talk Track | Steps |
| --- | --- |
| Today’s mobile workers access corporate information from many locations outside of the corporate network, such as home, customer sites, and coffee shops.  Contoso uses a third-party SaaS application called Expensify to track travel and expense reporting for their mobile workforce. Contoso IT wants to ensure additional security while accessing this app. |  |
| **Configuring location-based conditional access**  Let’s look at applying a conditional access policy to the enterprise application Expensify.  The application is already configured in our Azure Active Directory for single sign-on. Let’s add a new conditional access policy to this application.  First we need to create a group of Trusted IPs to be used for the Conditional Access Policy.  Here we can specify our corporate network ranges. They are added using CIDR notation.  The policy can be set to apply to specific users or groups, so you can have fine grained control over which users are subject to which conditions and controls.  We are going to apply this policy to the Sales and Marketing group.  To set a location-based policy we need to add a location condition.  We want this policy to trigger for all locations except those that we specify as trusted locations. To achieve this, we add Any Location to be included in the policy and then add the list of trusted IP ranges to exclude. These are the networks that we trust and control.  Selecting All trusted locations includes the list of Trusted IPs we added earlier.  Now that the appropriate conditions to trigger the policy have been configured we need to select the controls that the policy will apply. In this example, we will select to block access. | 1. In the left-hand navigation, click **Azure Active Directory**. 2. Under **Security**, click **Conditional access**. 3. In the **Manage** section, click **Named locations**. 4. Click **Configure MFA trusted IPs**. 5. In the **trusted ips** text box enter the following IP addresses: 192.168.1.0/24 192.168.2.0/24 192.168.3.0/24      1. Click **Save**. 2. Click **Close**. 3. Close the Multi-factor authentication browser tab. 4. Click **X** to close the **Conditional access – Named locations** blade. 5. Click **Enterprise applications**, and then click **All applications**. 6. In the Enterprise application list, click **Expensify**. 7. Under **Security**, click **Conditional access**. 8. Click **+ New policy**. 9. In the Name field type **Expensify location policy**. 10. In the **Assignments** section, click **Users and groups**. 11. Click **Select users and groups**, and then click **Users and groups**. 12. Click **Select**. 13. In the search box, type **sg** and press **Enter**. 14. Click on **sg-Sales and Marketing**. 15. Click **Select**. 16. Click **Done**. 17. In the **Assignments** section, click **Conditions**. 18. On the **Conditions** blade, Click **Locations**. 19. Set Configure to **Yes**. 20. Under **Include**, ensure that **Any location** is selected. 21. Click **Exclude**. 22. Check **All trusted locations**. 23. At the bottom of the **Locations** blade, click **Done**. 24. At the bottom of the **Conditions** blade, click **Done**. 25. In the **Access controls** section, click **Grant**. 26. Select **Block access**. 27. Click **Select**. 28. Set Enable policy to **On**. 29. Click **Create**. 30. In the top right corner of the portal, click **admin@<tenant>.onmicrosoft.com**. 31. Click Sign out. |
| **Access resources from untrusted location**  Logging in to the MyApps portal as a member of Sales and Marketing group, we can see the Expensify applications as one of the available applications.  If I try and launch the application now, as I am coming in from a different network than those listed in the trusted IPs list, access to the application is blocked. | 1. Browse to <https://myapps.microsoft.com>. 2. Click **Use another account**. 3. Sign in as **isaiahl@<tenant>.onmicrosoft.com** with the tenant password. 4. Click on the **Expensify** tile. 5. On the **You cannot access this right now** message, click **More details**.   Note the message notifying you are unable to access the content right now and it was triggered by conditional access.     1. Close the Sign in to your account tab. 2. In the top right corner of the portal, click [isaiahl@<tenant>.onmicrosoft.com](mailto:isaiahl@%3ctenant%3e.onmicrosoft.com). 3. Click **Sign out**. |
| **Adding trusted locations**  If this network is a trusted location, we could add the current IP address range to the trusted IP list.  Going in to the location-based policy, we can add this specific IP address to the list of trusted IPs.  I’ll add my current external IP address as if it was a trusted IP address range. | 1. Browse to <https://portal.azure.com>. 2. Log in with your global admin credentials: **admin@<tenant>.onmicrosoft.com** 3. In the left-hand navigation, click **Azure Active Directory**. 4. Under **Security**, click **Conditional access**. 5. In the **Manage** section, click **Named locations**. 6. Click **Configure MFA trusted IPs**. 7. In the **trusted ips** text box add the IP addresses noted earlier with /32 appended.  For example: 24.20.119.40/32      1. Click **Save**. 2. Click **Close**. 3. Close the **Multi-factor authentication** browser tab. 4. In the top right corner of the portal, click **admin@<tenant>.onmicrosoft.com**. 5. Click **Sign out**. |
| **Access resources from a trusted location**  Now when I access Expensify, it recognizes my IP address as within one of the trusted IP address ranges and allows me access to the application. | 1. Browse to <https://myapps.microsoft.com>. 2. Sign in as **isaiahl@<tenant>.onmicrosoft.com** with the tenant password. 3. Click on the **Expensify** tile. Note that access is now successful. |
| Using location-based conditional access policies can enable protection of corporate data by restricting where the data can be accessed from. It could be that this is highly sensitive information that should only be accessed when on the corporate premises, such as medical data which should only be accessed when the medical staff are on hospital premises.  Another example would be requiring Multi-Factor Authentication when an employee is accessing corporate data from home or an internet hotspot, but allowing them access without MFA if on the corporate network or connected via VPN. |  |

## Demo Reset Steps

Perform these steps after each demo presentation to ensure re-usability of this demo environment:

1. Browse to <https://portal.azure.com>.
2. Log in with your global admin credentials: [**admin@<tenant>.onmicrosoft.com**](mailto:admin@%3ctenant%3e.onmicrosoft.com)using thetenant password from your demo card on [demos.microsoft.com](https://demos.microsoft.com/).
3. In the left-hand navigation, click **Azure Active Directory**.
4. Under **Security**, click **Conditional access**.
5. In the **Manage** section, click **Named locations**.
6. Click **Configure MFA trusted IPs**.
7. Remove all IP addresses from the Trusted IPs list.
8. Click **Save**.
9. Click **Close**.
10. Close the **Multi-factor authentication** browser tab.
11. Close the **Named locations** blade.
12. Click **Policies**.
13. Click **Expensify location policy**.
14. On the **Expensify location policy** blade, click **Delete**.
15. Click **Yes**.

# Requiring device enrollment for mobile application access

## Pre-Demo Steps

1. Ensure that the set-up steps in [Appendix 1](#_Appendix_1:_Configure) have been completed.
2. See the [Appendix 2](#_Requiring_multi-factor_authenticati_1) for detailed device setup instructions.

| Talk Track | Steps |
| --- | --- |
| **Opening**  One of the main capabilities employees want on their mobile devices is access to their corporate email and documents. And they expect to do it in a 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. |  |
| **Configuring device-based conditional access**  How difficult is this to configure for the IT Admin? Typically, this is a challenging project that often requires email gateways, servers in the perimeter network, lots of configuration, and custom scripts.  Due to our cloud architecture, we significantly reduced the complexity, and made it very easy to configure.  There are only two things the IT needs to do to enable conditional access.  First, we define a compliance policy in Intune Admin Console which verifies if the device is healthy or not. As you can see, there are multiple settings that can be checked on the devices running Windows, Windows Phone, iOS, and Android.  Second, we enable the conditional access policy. In this example, it is enabled for Exchange Online. The appropriate restrictions and targeted groups are configured. Now employees in these groups need to have their devices enrolled and healthy to access the email. Note that you can separately block access from mobile client applications and via the browser.  You can protect access to Exchange Online email from Outlook and other apps that use modern authentication. | 1. Browse to <https://portal.azure.com>. 2. Log in with your global admin credentials: **admin@<tenant>.onmicrosoft.com** 3. In the left-hand navigation, **All services**. 4. In the filter text box, type **Intune**, and click **Intune** in the search results (not Intune App Protection) 5. Under **Manage**, click **Device compliance**. 6. Under **Manage**, click **Policies**. 7. Click **Contoso MDM Compliance Policy for iOS** and click **Properties.** 8. Click **Settings** and click each of the categories to review the configuration:  * Email * Device Health * Device Properties * System Security  1. Click **X** on each open blade until back at the Microsoft Intune overview blade. 2. Under **Manage**, cllick **Conditional Access**. 3. Click **Exchange Online Policy**. 4. In the **Assignments** section, click on **Cloud Apps** to show **Office 365 Exchange Online** is selected. 5. On the **Exchange Online Policy** blade, in the **Access controls** section, click **Grant** to show the requirement for compliant device. 6. On the **Exchange Online Policy** blade, in the **Assignments** section, click **Users and groups** to show the selected groups. 7. Click **X** on **Users and groups** to close the blade. 8. On the Exchange Online Policy blade, click **On** for **Enable policy**, and then click **Save**. |
| **Enrolling device for access**  When employees add their corporate Office 365 account in the Outlook app, they expect to get access to all their email, but with EMS you can enable conditional access which ensures that employees access corporate email only from managed and compliant devices.  As you can see here, they are blocked and are informed that to get access they need to first enroll their device to Intune.  Enrollment is performed via the Intune Company Portal app. The app is already installed on this device, so the user can launch straight in to the enrollment process.  Employees need to login with their corporate Azure AD identity, 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 happening behind the 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 – and that’s useful in scenarios where the employees want to access corporate resources from this device. Intune also starts to deploy and enforce device settings like password requirements, resource access profiles such as Wi-Fi and VPN, certificates, and applications.  Once the enrollment is completed, employees need to ensure their device is compliant with the corporate policies. This is a great solution, as employees get access to email with just a few simple steps, and IT stays happy because the corporate data is accessed only from managed devices. | 1. On your iOS device, launch the **Outlook** app. 2. Tap **Get Started**, then dismiss app initialization/welcome messages, if necessary. 3. If prompted for notifications tap **No Thanks**.      1. Enter the email address: [IsaiahL@<tenant>.onmicrosoft.com](mailto:IsaiahL@%3ctenant%3e.onmicrosoft.com) and tap **Add Account**.   Note: If you select the email address and copy it to the clipboard it will enable you to paste it in later in the demo, rather than typing it each time.   1. Enter your tenant password and tap **Sign in**.   Note the Conditional Access policy message that requires your device to be enrolled to be managed before you are able to access email.     1. Tap **Enroll now**. 2. Tap **OPEN** to launch Microsoft Intune Company Portal app. 3. Log in to Intune Company Portal as: IsaiahL@<tenant>.onmicrosoft.com, and tap **Sign in**. 4. On Set up <company> access page, tap **Begin**. 5. On the What can <company> see page, tap **Continue**. 6. On What‘s next? page, tap **Continue**. You will be directed to the built-in iOS Settings app. Complete the enrollment steps:    1. If you’re prompted, tap **Allow** to open Settings.    2. On Install Profile page, tap **Install**.    3. Enter device passcode (*prompted only if device currently has a passcode*).    4. Tap **Install**.    5. On Warning page, tap **Install**.    6. On Remote Management dialog, tap **Trust**.    7. On Profile Installed page, tap **Done**.    8. Tap **Open** to open the page in the Intune Company Portal app.   **Note**: Install the apps you are prompted to install. Agree to Apple Media Services Terms and Conditions if prompted.   * 1. On the Set up Company access page, tap **Continue**.   2. On the Profile installed page, tap **Done** to complete Company Access Setup.   3. Tap **Done** to complete Company Access Setup.   4. Review the **Intune Company Portal** home page.  1. Press the device’s **home button**. If your device does not have a PIN, you’ll see a Passcode Requirement dialog where you must set one within 60 minutes. 2. Tap **Outlook** to return to app. 3. Tap the back arrow to return to theAdd Account page. 4. Tap **Sign In with Office 365**, and complete sign in for [IsaiahL@<tenant>.onmicrosoft.com](mailto:IsaiahL@%3ctenant%3e.onmicrosoft.com). 5. Click **OK** to restart the app. 6. Tap **Outlook** to return to app. 7. Set a new device passcode to access your organization’s data.   **Tip**: For a 4-character passcode, use something like **111@** so it’s easy to remember.   1. Note the **Inbox** is now populated with Isaiah’s emails. |

## Demo Reset Steps

Perform these steps after each demo presentation to ensure re-usability of this demo environment:

1. Disable Conditional access policies:
   * Browse to <https://portal.azure.com>
   * Sign in as the tenant’s Global Admin account.
   * Navigate to **Azure Active Directory >** **Conditional Access** > **Exchange Online Policy**.
   * Set **Enable policy** to **Off**.
   * Click **Save**.
2. Un-enroll the iOS device. Perform a factory reset and repeat setup steps as detailed in [Appendix 2](#_Requiring_device_enrollment_2).

# Requiring multi-factor authentication for applications

## Pre-Demo Steps

1. Ensure that the set-up steps in [Appendix 1](#_Appendix_1:_Configure) have been completed.
2. Ensure that you have access to a mobile device to be used for multi-factor authentication.
3. Open a browser window (not InPrivate) in Microsoft Edge to <https://portal.azure.com>.
4. Log in with your global admin credentials: [**admin@<tenant>.onmicrosoft.com**](mailto:admin@%3ctenant%3e.onmicrosoft.com)using thetenant password from your demo card on [demos.microsoft.com](https://demos.microsoft.com/).

| Talk Track | Steps |
| --- | --- |
| Azure Active Directory Conditional Access for SaaS apps and Azure AD connected apps lets you configure conditional access based on group, location, and application sensitivity.  With conditional access based on application sensitivity, you can set multi-factor authentication (MFA) access rules per application. MFA per application provides the ability to block access for users who are not on a trusted network. You can apply MFA rules to all users that are assigned to the application, or only for users within specified security groups. Users may be excluded from the MFA requirement if they are accessing the application from an IP address that is inside the organization’s network. |  |
| **Configuring application-based conditional access**  Let’s walk through configuring Azure Active Directory Conditional Access to require multi-factor authentication for a group of applications.  A new conditional access policy is created to which we can assign users and groups, the applications, any additional conditions (such as location or device platform), and the control to be applied (such as requiring MFA or blocking access).  The group of users to be prompted for MFA can be specified here. You could have a group of trusted users excluded from this policy and allow them access without MFA, while including sensitive accounts to require MFA.  The applications to which this policy is to be applied are now specified. This enables you to configure a single policy and apply it to all apps of a similar risk profile. In this instance, the policy we are configuring is for HBI apps, so you would add all the apps with high business impact data to this policy.  Next, we need to configure the control to be applied through this policy. In this example, we’ll only require multi-factor authentication.  Let’s sign out of the administrator experience and see what the end user experience is like. | 1. In the left-hand navigation, click **Azure Active Directory**. 2. Under **Security**, click **Conditional access**. 3. Click **+ New policy**. 4. In the **Name** field type **High Business Impact MFA policy**. 5. In the **Assignments** section, click **Users and groups**. 6. Click **Select users and groups**, and then click **Users and groups**. 7. Click **Select**. 8. In the search box, type **sg** and press **Enter**. 9. Click on **sg-Sales and Marketing**. 10. Click **Select**. 11. Click **Done**. 12. In the **Assignments** section, click **Cloud apps**. 13. Click **Select Apps**. 14. Click **Select**. 15. In the Applications text box, type **Woodgrove** and click **Woodgrove Expense Manager**. 16. Click **Select**. 17. Click **Done**. 18. In the **Access controls** section, click **Grant**. 19. Ensure **Grant access** is selected. 20. Check **Require multi-factor authentication**. 21. Click **Select**. 22. Set Enable policy to **On**. 23. Click **Create**. 24. In the top right corner of the portal, click [admin@<tenant>.onmicrosoft.com](mailto:admin@%3ctenant%3e.onmicrosoft.com). 25. Click **Sign** **out**. |
| **Application access using MFA**  End users access enterprise applications published in Azure through the MyApps portal.  Here you can see the Woodgrove application that we applied the policy to.  If I click on the application, it requires multi-factor authentication for access. As this is the first prompt for MFA, I can walk through the set-up experience now.  The authentication code can be sent to a mobile device by text message or through a voice call. There is also an app for the major device platforms to provide the MFA authentication.  Now I’ve received the code via text message, I can enter it and verify my sign in.  This now allows me through to the application.  Let’s see the experience for an end user on subsequent application accesses.  When I click the Docusign tile now, it prompts me straight away for the code and sends the text message to my mobile device. | 1. Browse to <https://myapps.microsoft.com>. 2. Click **Use another account**. 3. Sign in as **isaiahl@<tenant>.onmicrosoft.com**. 4. Click on the **Woodgrove Expense Manager** tile. 5. If this is your first time performing this demo, you’ll have to configure MFA. On the **More information required** window, click **Next** to begin configuration of MFA.    1. In the **Additional Security Verification** page    * Authentication Phone is selected.    * Select your country or region pick the appropriate country or region for your cellphone.    * Type your cellphone number in the text box next to the country code.    * Method select **Send me a code by text message**    1. Click **Next**.    2. When prompted, type the verification code received on your cellphone, then click **Verify**.    3. At the **Verification successful** prompt, click **Done**. 6. Respond to the MFA verification by entering code sent by text message, then click **Verify**. 7. Close all browser windows. |

## Demo Reset Steps

Perform these steps after each demo presentation to ensure re-usability of this demo environment:

1. Browse to <https://portal.azure.com>
2. Log in with your global admin credentials: [**admin@<tenant>.onmicrosoft.com**](mailto:admin@%3ctenant%3e.onmicrosoft.com)**,** using thetenant password from your demo card on [demos.microsoft.com](https://demos.microsoft.com/).
3. In the left-hand navigation, click **Azure Active Directory**.
4. Under **Security**, click **Conditional access**.
5. Click **High Business Impact MFA policy**.
6. Click **Delete**.
7. Click **Yes**.
8. Close all browser windows.

# Appendix 1: Configure your Demo Environment

**Note:** These activities need to be performed only once per demo tenant. You may have performed some or all of these steps against your environment in preparation for another demo, in which case you may skip these steps.

These demo scenarios require a Microsoft Enterprise Mobility + Security (EMS) demo environment provisioned through demos.microsoft.com portal.

## Install Access Panel browser extension

To demonstrate password-based single sign-on experience, you’ll need to install/enable Access Panel extension for your browser on your demo PC.

**Estimated Setup Time: 2 minutes**

1. In Microsoft Edge (not InPrivate), navigate to <https://www.microsoft.com/store/apps/9pc9sckkzk84>.
2. On the **My Apps Secure Sign-in Extension**, click **Get**.
3. In the Store app window, click **Install**.
4. When the install has been completed, close the Store app.
5. In the Microsoft Edge notification “You have a new extension”, click **Turn it on**.

Note: if the notification does not appear shortly, click **Launch** then click **Turn it on.**

## Configuring SaaS app for scenario Blocking access from untrusted locations

**Estimated Setup Time: 15 minutes**

You’ll signup for a (free) Expensify account, then configure it for password-based SSO with your demo tenant. If you already have an Expensify demo account, you can skip to step #9.

1. In a browser, navigate to <http://www.expensify.com>.
2. In the email address field enter: **admin@<tenant>.onmicrosoft.com**
3. Click **SIGN UP FOR FREE**.
4. Open a browser tab to <https://outlook.office.com>.
5. Sign in using your demo tenant global admin credentials: [**admin@<tenant>.onmicrosoft.com**](mailto:admin@%3ctenant%3e.onmicrosoft.com), using thetenant password from your demo card on [demos.microsoft.com](https://demos.microsoft.com/).
6. Locate the email from Expensify, then click **Validate Account**.

**Tip**: Look in your **Other** inbox if you don’t see the Expensify email in the Focused inbox.

1. In the password and confirm password fields, provide a password (e.g. **Pass@word1**)

**Note**: Expensify requires at least one capital letter, one symbol and one digit.

1. Click **Set Expensify Password**.
2. Open a browser tab to <https://portal.azure.com>.
3. Sign in using your demo tenant global admin credentials: [**admin@<tenant>.onmicrosoft.com**](mailto:admin@%3ctenant%3e.onmicrosoft.com), using thetenant password from your demo card on [demos.microsoft.com](https://demos.microsoft.com/).
4. In the left-hand navigation, click **Azure Active Directory**.
5. Under **Manage**, click **Enterprise applications**.
6. Click **+ New application**.
7. In the “Add from the gallery” search box, type **Expensify**.
8. In the search results, click **Expensify.**
9. Click **Add**.
10. On the **Expensify – Quick Start** blade, click **Users and groups**.
11. Click **+ Add user**.
12. Click **Users and groups**.
13. In the search field, type **sg** and press **Enter**.
14. Click on **sg-Sales and Marketing**.
15. Click **Select**.
16. Click **Assign**.
17. Click **Single sign-on**.
18. On the **Select a single sign-on method** blade, select **Password-based**.
19. Click **Save**.
20. Click **Users and groups**.
21. Check the box for **sg-Sales and Marketing**.
22. Click **Update credentials**.
23. In the **Email Address** field, type **admin@<tenant>.onmicrosoft.com**.
24. In the **Password** field, type the password you Expensify demo account (e.g. **Pass@word1**).
25. Click **Save**.
26. Close all browser tabs.

## Configuring SaaS app for scenario Requiring multi-factor authentication for applications

You’ll configure SSO to a custom application called Woodgrove Expense Reporting.

**Estimated Setup Time: 10 minutes**

1. Open a browser tab to [https://portal.azure.com](https://portal.azure.com/).
2. Sign in using your demo tenant global admin credentials: [**admin@<tenant>.onmicrosoft.com**](mailto:admin@%3ctenant%3e.onmicrosoft.com), using thetenant password from your demo card on [demos.microsoft.com](https://demos.microsoft.com/).
3. In the left-hand navigation, click **Azure Active Directory**, and then click **Enterprise applications**.
4. Click **+** **New application** at the top of the page.
5. Click **Non-gallery application**.
6. In the **Name** field, type **Woodgrove Expense Manager**, then click **Add**.
7. Under **Manage**, click **Single sign-on**.
8. On the **Select a single sign-on method**, select **Password-based**.
9. In the **Sign-on URL** textbox, copy/paste this URL:  
   <https://woodgroveexpensemanager.azurewebsites.net>
10. Click **Save**.
11. When the changes have successfully saved, click **Configure Woodgrove Expense Manager Password Single Sign-on Settings**.
12. In the **Configure sign-on** blade, select **Manually detect sign-in fields** option.
13. Click **Capture sign-in fields** link. A new browser tab will open the sign in page for the Expense Reporting app.

**Note:** this must be done in a regular Edge browser session. The Access Panel browser extension is not available in InPrivate browser sessions.

1. Fill in the sign in form as follows:

Email: [achimm@woodgrove.com](mailto:achimm@woodgrove.com)

Password: **pass@word1**

1. Click **Sign in**.
2. In the browser message box “Save Captured login details?” click **OK**. The browser tab with Expense Reporting App will close automatically in a few seconds.
3. Back in the **Configure sign-on** blade, check **Ok, I was able to sign-in to the app successfully**.
4. Click **OK** at the bottom of the blade to save.
5. On the **Woodgrove Expense Manager** blade, under **Manage**, click **Users and groups**.
6. Click **+** **Add user**.
7. Click **Users and groups**.
8. Type **sg**, then select **sg-Sales and Marketing** security group.
9. Click **Select** at the bottom of the blade.
10. Click **Assign Credentials**.
11. Set **Assign credentials to be shared among all group members** to **Yes**.
12. Fill in the credentials form as follows:
    * Account Name: [achimm@woodgrove.com](mailto:achimm@woodgrove.com)
    * Password: **pass@word1**
13. Click **OK**.
14. Click **Assign**.
15. **OPTIONAL**: Upload a logo for this application:
    * In a new browser tab, navigate to <http://emsassetspub.blob.core.windows.net/demoassets/WoodgroveBank.png>
    * Save the image to a suitable location.
    * Return to the Azure Portal browser tab.
    * Under **Manage**, click **Properties**.
    * Under **Logo**, click Select a file.
    * Select the logo file downloaded, then click **Open**.
    * Click **Save**.
16. Close the browser window.

## Create Exchange Online Conditional Access Policy

**Estimated Setup Time: 5 minutes**

1. If necessary, log in to the **Azure Portal** (<https://portal.azure.com>) as your demo tenant’s Global Administrator.
2. In the left navigation bar, click **Azure Active Directory**.
3. In the **Security** section, click **Conditional access**.
4. If **Exchange Online Policy** does not exist, click **+ New Policy** and configure it as follows:
   * Name: **Exchange Online Policy**
   * Users and Groups: **sg-Sales and Marketing**
   * Cloud apps: **Office 365 Exchange Online**
   * Grant: **Require device to be marked as compliant**
   * Enable policy: **Off**
5. Click **Create**.

## Configure Apple Push Notification Service Certificate for scenario Requiring device enrollment for mobile application access

**Estimated Setup Time: 15 minutes**

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.

### Create an Apple ID (if necessary)

You may use your existing Apple ID, if you have one, and skip this section.

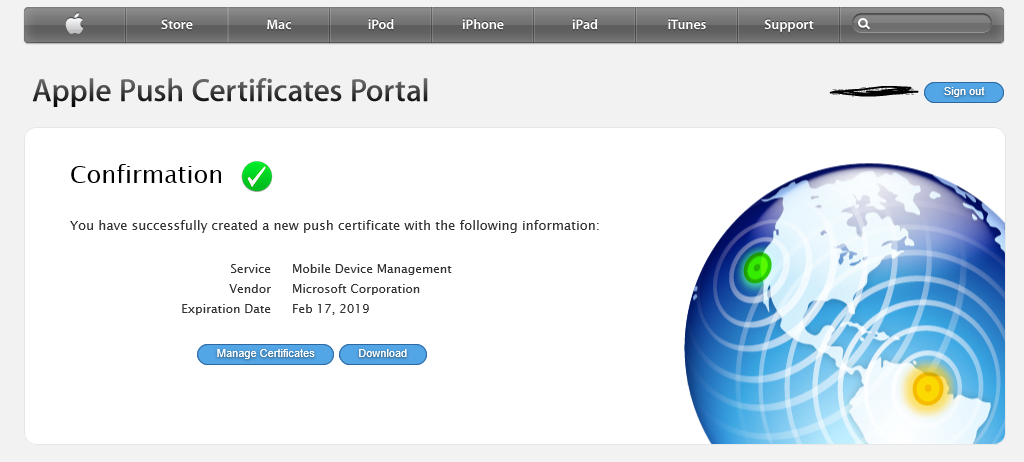
1. Navigate to the following URL <https://appleid.apple.com/> and click **Create your Apple ID**.
2. Fill in the My Apple ID form as required. Sample values provided below – feel free to use your own values.
   * First Name: **Demo**
   * Last Name: **Admin**
   * Country: (fill in as appropriate)
   * Birthday: (fill in as appropriate)
   * Email: **admin@<tenant>.onmicrosoft.com** (replace <tenant> with appropriate value)
   * Password (example): **Contoso1**
   * Choose the 3 security questions from the drop-downs and answer them as appropriate.
   * Uncheck Email preference options
   * Type in the captcha text as you see on the screen
3. Click **Continue**.
4. 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 make a note of the verification code in the email.
   4. Return to the Apple ID page and enter the verification code from the email.

### Configure Intune Admin Settings for iOS Device Management

1. Navigate to the Azure Portal: <https://portal.azure.com>, and login using your demo tenant’s Global Administrator.
2. In the left navigation pane, click **All services**.
3. In the filter text box, type **Intune** and click **Intune** in the search results (not Intune App Protection).
4. Under **Manage**, click **Device enrollment**.
5. Under **Manage**, click **Apple enrollment**.
6. Under **Prerequisites**, click **Apple MDM Push Certificate**.
7. In the list of **Steps**, click **I agree**.
8. In the list of **Steps**, click **Download your CSR**, and save the Intune certificate.
9. In the list of **Steps**, click **Create your MDM push Certificate**. The **Apple Push Certificates Portal** will be displayed in a new browser tab.

**Note:** If you closed the previous browser session and are prompted for login, provide the Apple ID credentials you configured earlier.

1. On the **Apple Push Certificates Portal** page, click **Create a Certificate**.
2. To accept the Terms of Use click the check box and then click **Accept**.
3. On the **Create a New Push Certificate** page, under **Vendor-Signed Certificate Signing Request**, click **Browse**.
4. Point to the .CSR file you saved to your local computer earlier (in step 8 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. On the **Confirmation** page, click **Download** to download the Mobile Device Management certificate. Save the file to a local folder on your PC with .pem file extension (example MDM\_MicrosoftCorporation\_Certificate.pem).
2. Return to **Azure Portal** > **Configure MDM Push Certificate** page.
3. In the **Apple ID** text box, enter the Apple ID (email address) used to sign in to the Apple Push Certificates Portal.
4. Under **Apple MDM push certificate**, click the browse icon, browse to the certificate you downloaded earlier (.pem file), and click **Open**.
5. Click **Upload**.
6. Close all the open browser tabs.

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

# Appendix 2: Configure Your Demo Devices

## Requiring device enrollment for mobile application access

The demo configuration and documentation has been written for and tested against iOS devices. Android devices are supported as well but demo steps have not been specifically provided. For detailed instruction on using Android devices with Intune, please [review this article](https://docs.microsoft.com/en-us/intune/enduser/using-your-android-device-with-intune).

**Estimated Setup Time: 5 minutes**

### Requirements:

iOS (iPad or iPhone) running iOS 9 or above.

### Set up Steps:

1. If feasible, perform a factory reset of the device first.
2. Ensure device does not have **Microsoft** **Outlook** or the **Microsoft Intune** **Company Portal** apps installed. Delete if already installed.
3. Go to the iOS App Store and install **Microsoft** **Outlook** and the **Microsoft Intune** **Company Portal** apps.

**Note:** You can use any Apple ID to sign in to the App Store, or you can use the one created in [Appendix 1](#_Create_an_Apple).