

Microsoft Intune

# Blocking access from untrusted locations

1. Open a browser window (not InPrivate) in Microsoft Edge to <https://portal.azure.com>.
2. Log in with your global admin credentials: **admin@M365x723661.onmicrosoft.com**, and tenant password: sochania@1122
3. Browse to <https://www.whatismyip.com/>.
4. 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.

| Steps |
| --- |
|  |
| **Configuring location-based conditional 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@M365x723661.onmicrosoft.com**. 31. Click Sign out. |
| **Access resources from untrusted location**   1. Browse to <https://myapps.microsoft.com>. 2. Click **Use another account**. 3. Sign in as [**meganb@M365x723661.onmicrosoft.com**](mailto:meganb@M365x723661.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 [meganb@M365x723661.onmicrosoft.com](mailto:meganb@M365x723661.onmicrosoft.com). 3. Click **Sign out**. |
| **Adding trusted locations**   1. Browse to <https://portal.azure.com>. 2. Log in with your global admin credentials: **admin@M365x723661.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@M365x723661.onmicrosoft.com**. 5. Click **Sign out**. |
| **Access resources from a trusted location**   1. Browse to <https://myapps.microsoft.com>. 2. Sign in as [**meganb@M365x723661.onmicrosoft.com**](mailto:meganb@M365x723661.onmicrosoft.com)with the tenant password. 3. Click on the **Expensify** tile. Note that access is now successful. |

# Requiring device enrollment for mobile application access

| Steps |
| --- |
| **Configuring device-based conditional access**   1. Browse to <https://portal.azure.com>. 2. Log in with your global admin credentials: **admin@M365x723661.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**. |

# Requiring multi-factor authentication for applications

1. Ensure that you have access to a mobile device to be used for multi-factor authentication.
2. Open a browser window (not InPrivate) in Microsoft Edge to <https://portal.azure.com>.
3. Log in with your global admin credentials:  [**admin@M365x723661.onmicrosoft.com**](mailto:admin@%3ctenant%3e.onmicrosoft.com)using thetenant password from your demo card on [demos.microsoft.com](https://demos.microsoft.com/).

| Steps |
| --- |
|  |
| **Configuring application-based conditional access**   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@M365x723661.onmicrosoft.com](mailto:admin@%3ctenant%3e.onmicrosoft.com). 25. Click **Sign** **out**. |
| **Application access using MFA**   1. Browse to <https://myapps.microsoft.com>. 2. Click **Use another account**. 3. Sign in as **meganb@M365x723661.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. |