

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.

5. 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
- trusted ips ([learn more](#))
- ☐ Skip multi-factor authentication for requests from federated users on my intranet
- Skip multi-factor authentication for requests from following range of IP address subnets
- 192.168.1.0/24

192.168.2.0/24

192.168.3.0/24
6. Click **Save**.
 7. Click **Close**.
 8. Close the Multi-factor authentication browser tab.
 9. Click **X** to close the **Conditional access – Named locations** blade.
 10. Click **Enterprise applications**, and then click **All applications**.
 11. In the Enterprise application list, click **Expensify**.

Steps

12. Under **Security**, click **Conditional access**.
13. Click **+ New policy**.
14. In the Name field type **Expensify location policy**.
15. In the **Assignments** section, click **Users and groups**.
16. Click **Select users and groups**, and then click **Users and groups**.
17. Click **Select**.
18. In the search box, type **sg** and press **Enter**.
19. Click on **sg-Sales and Marketing**.
20. Click **Select**.
21. Click **Done**.
22. In the **Assignments** section, click **Conditions**.
23. On the **Conditions** blade, Click **Locations**.
24. Set Configure to **Yes**.
25. Under **Include**, ensure that **Any location** is selected.
26. Click **Exclude**.
27. Check **All trusted locations**.
28. At the bottom of the **Locations** blade, click **Done**.
29. At the bottom of the **Conditions** blade, click **Done**.
30. In the **Access controls** section, click **Grant**.
31. Select **Block access**.
32. Click **Select**.
33. Set Enable policy to **On**.
34. Click **Create**.
35. In the top right corner of the portal, click **admin@M365x723661.onmicrosoft.com**.
36. Click Sign out.

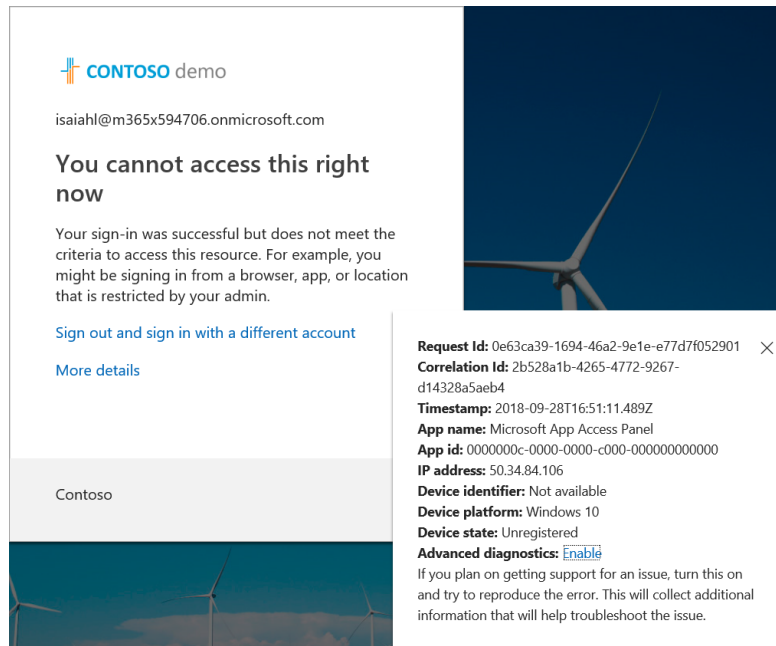
Access resources from untrusted location

1. Browse to <https://myapps.microsoft.com>.
2. Click **Use another account**.
3. Sign in as meganb@M365x723661.onmicrosoft.com with the tenant password.

Steps

- Click on the **Expensify** tile.
- 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.



The screenshot shows a message from 'CONTOSO demo' with the email 'isaiah1@m365x594706.onmicrosoft.com'. The message title is 'You cannot access this right now'. The body text states: 'Your sign-in was successful but does not meet the criteria to access this resource. For example, you might be signing in from a browser, app, or location that is restricted by your admin.' Below the message are links for 'Sign out and sign in with a different account' and 'More details'. To the right, a details pane is open showing the following information:

- Request Id:** 0e63ca39-1694-46a2-9e1e-e77d7f052901
- Correlation Id:** 2b528a1b-4265-4772-9267-d14328a5aeb4
- Timestamp:** 2018-09-28T16:51:11.489Z
- App name:** Microsoft App Access Panel
- App id:** 0000000c-0000-0000-c000-000000000000
- IP address:** 50.34.84.106
- Device identifier:** Not available
- Device platform:** Windows 10
- Device state:** Unregistered
- Advanced diagnostics:** [Enable](#)

Below the details pane, there is a note: 'If you plan on getting support for an issue, turn this on and try to reproduce the error. This will collect additional information that will help troubleshoot the issue.'

- Close the Sign in to your account tab.
- In the top right corner of the portal, click meganb@M365x723661.onmicrosoft.com.
- Click **Sign out**.

Adding trusted locations

- Browse to <https://portal.azure.com>.
- Log in with your global admin credentials: **admin@M365x723661.onmicrosoft.com**
- In the left-hand navigation, click **Azure Active Directory**.
- Under **Security**, click **Conditional access**.
- In the **Manage** section, click **Named locations**.
- Click **Configure MFA trusted IPs**.
- In the **trusted ips** text box add the IP addresses noted earlier with /32 appended.
For example: 24.20.119.40/32

Steps

trusted ips ([learn more](#))

☐ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

192.168.1.0/24
192.168.2.0/24
192.168.3.0/24
24.20.119.40/32

8. Click **Save**.
9. Click **Close**.
10. Close the **Multi-factor authentication** browser tab.
11. In the top right corner of the portal, click **admin@M365x723661.onmicrosoft.com**.
12. Click **Sign out**.

Access resources from a trusted location

13. Browse to <https://myapps.microsoft.com>.
14. Sign in as meganb@M365x723661.onmicrosoft.com with the tenant password.
15. 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:

Steps

- Email
- Device Health
- Device Properties
- System Security

- Click **X** on each open blade until back at the Microsoft Intune overview blade.
- Under **Manage**, click **Conditional Access**.
- Click **Exchange Online Policy**.
- In the **Assignments** section, click on **Cloud Apps** to show **Office 365 Exchange Online** is selected.
- On the **Exchange Online Policy** blade, in the **Access controls** section, click **Grant** to show the requirement for compliant device.
- On the **Exchange Online Policy** blade, in the **Assignments** section, click **Users and groups** to show the selected groups.
- Click **X** on **Users and groups** to close the blade.
- On the Exchange Online Policy blade, click **On** for **Enable policy**, and then click **Save**.

Requiring multi-factor authentication for applications

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

Steps

Configuring application-based conditional access

- In the left-hand navigation, click **Azure Active Directory**.
- Under **Security**, click **Conditional access**.
- Click **+ New policy**.
- In the **Name** field type **High Business Impact MFA policy**.
- In the **Assignments** section, click **Users and groups**.
- Click **Select users and groups**, and then click **Users and groups**.
- Click **Select**.

Steps

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.
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.
 - a. 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.

Steps

- Method select **Send me a code by text message**
 - b. Click **Next**.
 - c. When prompted, type the verification code received on your cellphone, then click **Verify**.
 - d. 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.