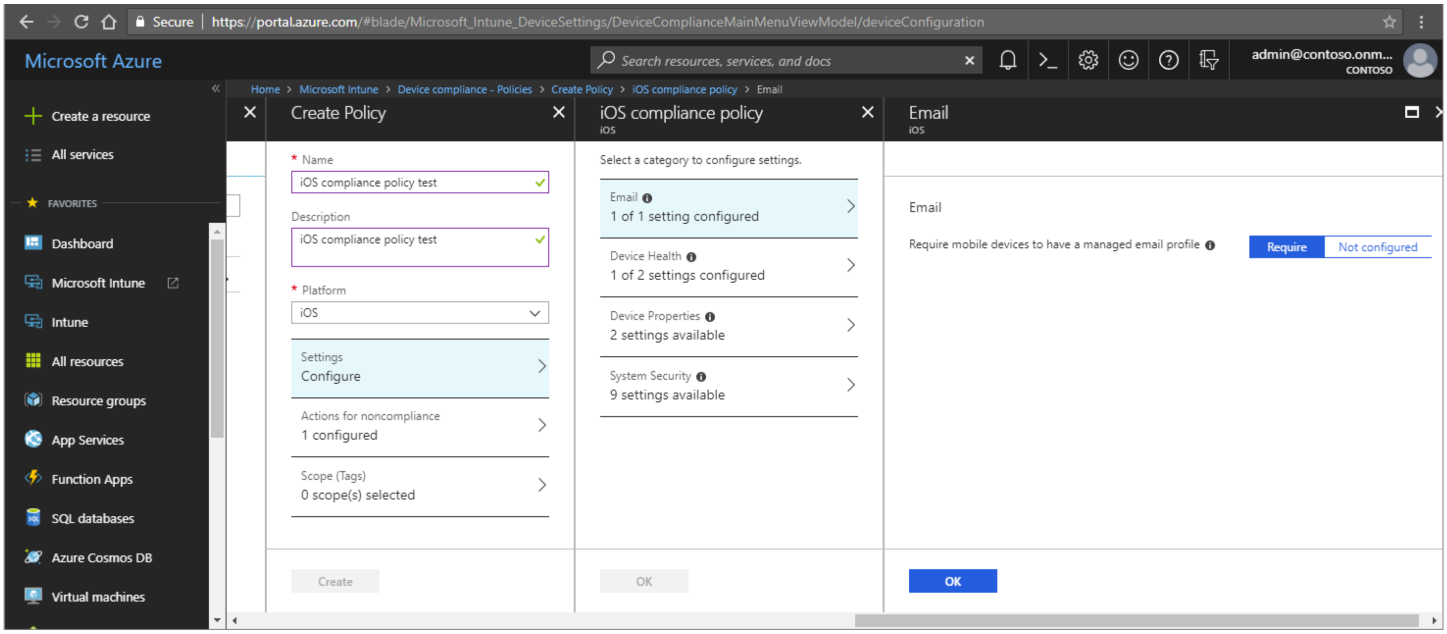
Example: Protect Exchange Online email

Protect Exchange Online email on managed devices

Create the iOS device compliance policy

1. In Intune, select **Device compliance** > **Policies** > **Create Policy**.
2. In **Name**, enter **iOS compliance policy test**.
3. In **Description**, enter **iOS compliance policy test**.
4. Under **Platform**, select **iOS**.
5. Select **Settings** > **Email**.
    a. Next to **Require mobile devices to have a managed email profile**, select **Require**.
    b. Select **OK**.



Secure | https://portal.azure.com/#blade/Microsoft_Intune_DeviceSettings/DeviceComplianceMainMenuViewModel/deviceConfiguration

Home > Microsoft Intune > Device compliance - Policies > Create Policy > iOS compliance policy > Email

Create Policy

* Name: iOS compliance policy test

Description: iOS compliance policy test

* Platform: iOS

Settings: Configure

Actions for noncompliance: 1 configured

Scope (Tags): 0 scope(s) selected

iOS compliance policy (iOS)

Select a category to configure settings.

Email: 1 of 1 setting configured

Device Health: 1 of 2 settings configured

Device Properties: 2 settings available

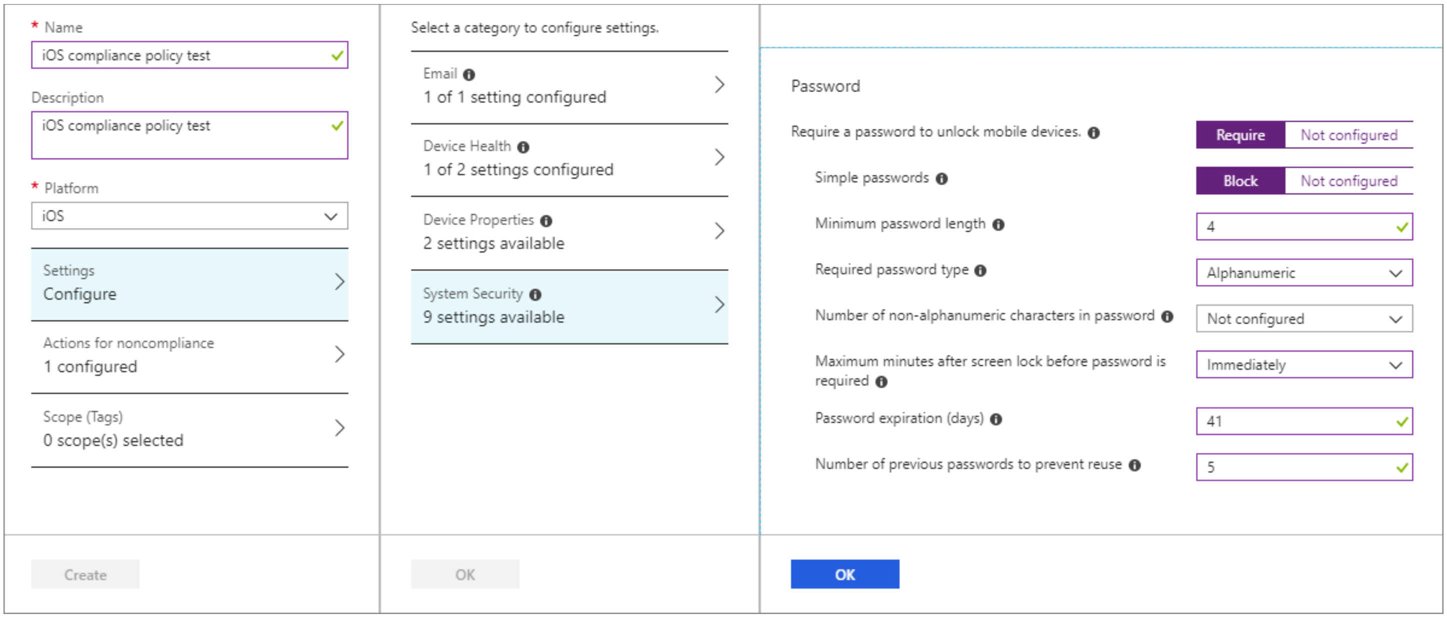
System Security: 9 settings available

Email (iOS)

Require mobile devices to have a managed email profile: Require | Not configured

6. Select **Device Health**. Next to **Jailbroken devices**, select **Block**, and then select **OK**.
7. Select **System Security** and enter **Password** settings. For this tutorial, select the following recommended settings:
    - For **Require a password to unlock mobile devices**, select **Require**.
    - For **Simple passwords**, select **Block**.
    - For **Minimum password length**, enter **4**.
    - For **Required password type**, choose **Alphanumeric**.
    - For **Maximum minutes after screen lock before password is required**, choose **Immediately**.
    - For **Password expiration (days)**, enter **41**.

- For **Number of previous passwords to prevent reuse**, enter **5**.



* Name: iOS compliance policy test ✓

Description: iOS compliance policy test ✓

* Platform: iOS

Settings
Configure

Actions for noncompliance
1 configured

Scope (Tags)
0 scope(s) selected

Select a category to configure settings.

Email
1 of 1 setting configured

Device Health
1 of 2 settings configured

Device Properties
2 settings available

System Security
9 settings available

Password

Require a password to unlock mobile devices.	[✓ Require] Not configured
Simple passwords	[✓ Block] Not configured
Minimum password length	4 ✓
Required password type	Alphanumeric
Number of non-alphanumeric characters in password	Not configured
Maximum minutes after screen lock before password is required	Immediately
Password expiration (days)	41 ✓
Number of previous passwords to prevent reuse	5 ✓

8. Select **OK**, and then select **OK** again.
9. Select **Create**.

Create the conditional access policy

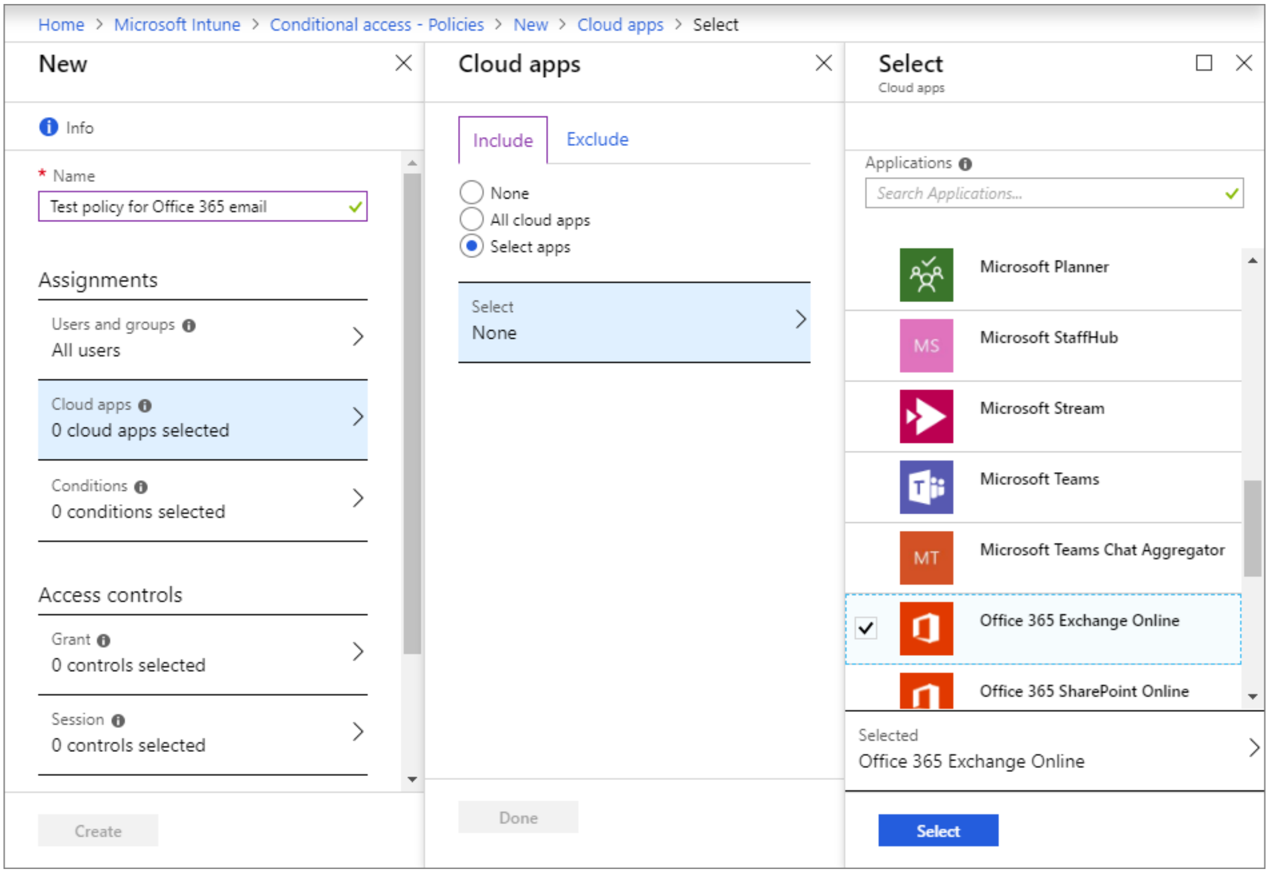
1. In Intune, select **Conditional access** > **Policies** > **New policy**.
2. In **Name**, enter **Test policy for Office 365 email**.
3. Under **Assignments**, select **Users and groups**. On the **Include** tab, select **All users**, and then select **Done**.
4. Under **Assignments**, select **Cloud apps**. Because we want to protect Office 365 Exchange Online email, we'll select it by following these steps:

a. On the **Include** tab, choose **Select apps**.

b. Choose **Select**.

c. In the applications list, select **Office 365 Exchange Online**, and then choose **Select**.

d. Select **Done**.



Home > Microsoft Intune > Conditional access - Policies > New > Cloud apps > Select

New

Info

* Name: Test policy for Office 365 email ✓

Assignments

Users and groups: All users

Cloud apps: 0 cloud apps selected

Conditions: 0 conditions selected

Access controls

Grant: 0 controls selected

Session: 0 controls selected

Create

Cloud apps

Include | Exclude

○ None
○ All cloud apps
● Select apps

Select: None

Done

Select
Cloud apps

Applications: Search Applications... ✓

- Microsoft Planner
- Microsoft StaffHub
- Microsoft Stream
- Microsoft Teams
- Microsoft Teams Chat Aggregator
- ☑ Office 365 Exchange Online
- Office 365 SharePoint Online

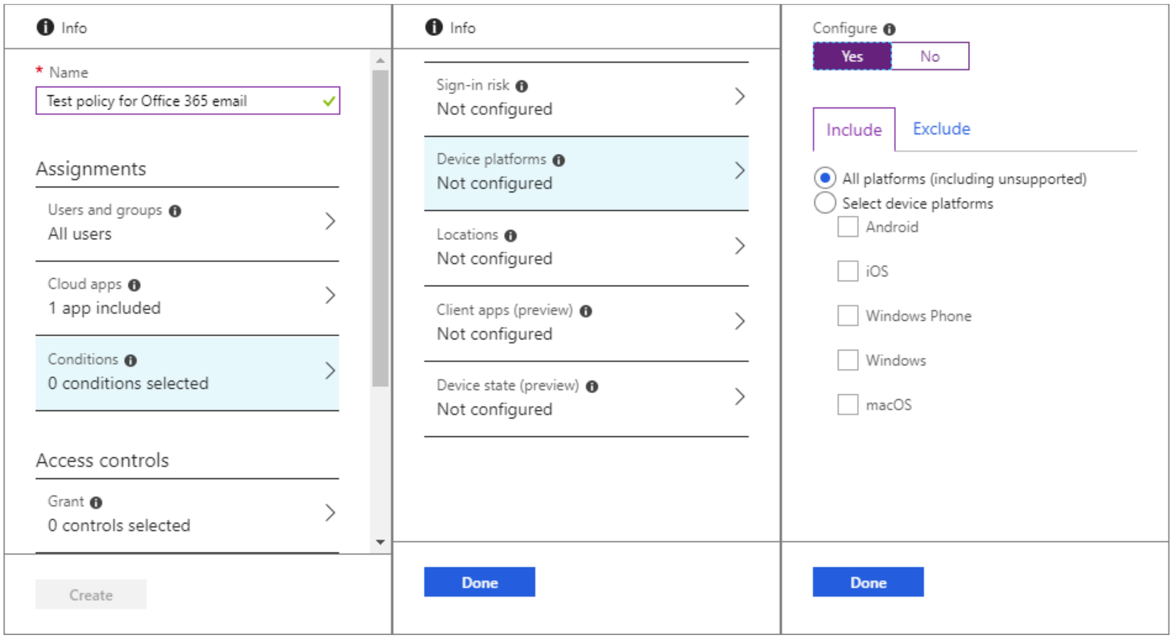
Selected: Office 365 Exchange Online

Select

5. Under **Assignments**, select **Conditions** > **Device platforms**.

. Under **Configure**, select **Yes**.

   a. On the **Include** tab, select **All platforms (including unsupported)**, and then select **Done**.
   b. Select **Done** again.



Info

* Name: Test policy for Office 365 email ✓

Assignments

Users and groups: All users

Cloud apps: 1 app included

Conditions: 0 conditions selected

Access controls

Grant: 0 controls selected

Create

Info

Sign-in risk: Not configured

Device platforms: Not configured

Locations: Not configured

Client apps (preview): Not configured

Device state (preview): Not configured

Done

Configure: [✓ Yes] No

Include | Exclude

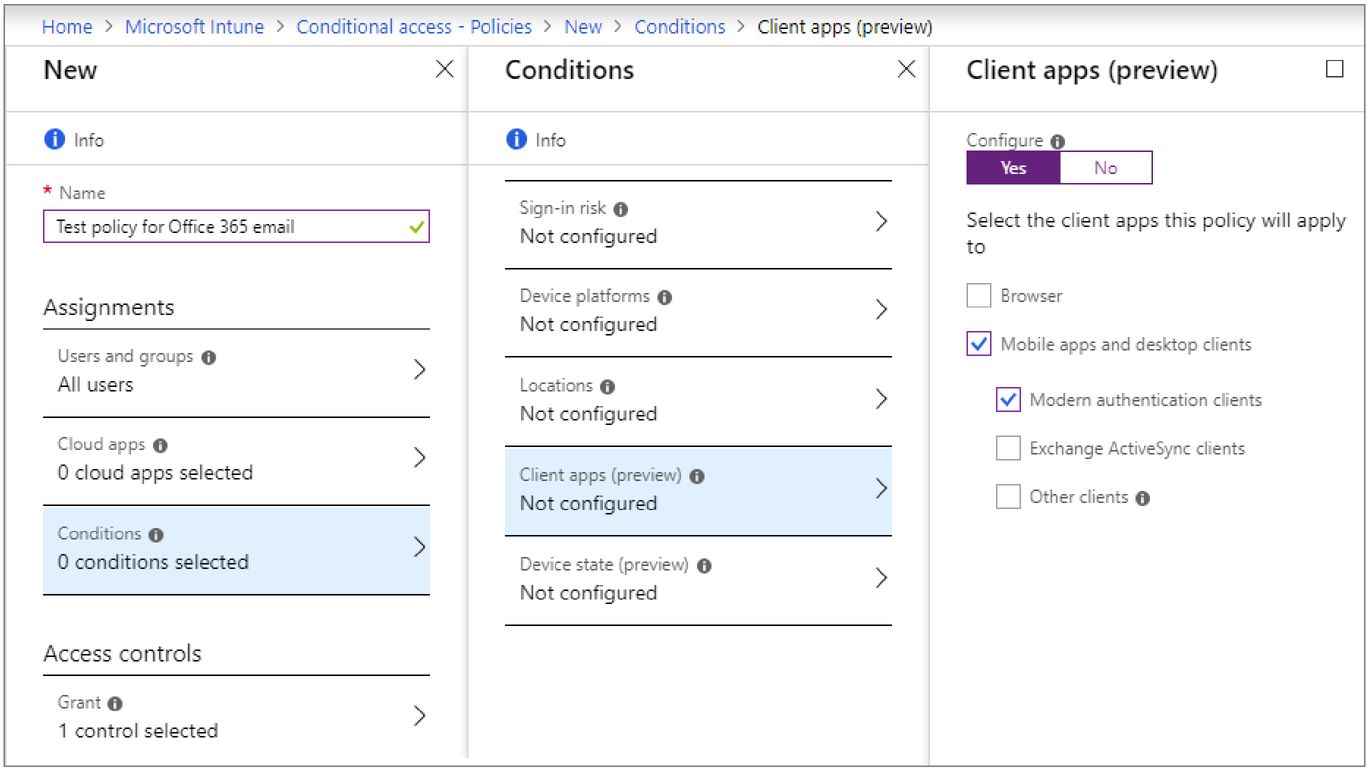
● All platforms (including unsupported)
○ Select device platforms
□ Android
□ iOS
□ Windows Phone
□ Windows
□ macOS

Done

6. Under **Assignments**, select **Conditions** > **Client apps**.

. Under **Configure**, select **Yes**.

   a. For this tutorial, select **Mobile apps and desktop clients** and **Modern authentication clients** (which refers to apps like Outlook for iOS and Outlook for Android). Clear all other check boxes.
   b. Select **Done**, and then select **Done** again.



Home > Microsoft Intune > Conditional access - Policies > New > Conditions > Client apps (preview)

New

Info

* Name: Test policy for Office 365 email ✓

Assignments

- Users and groups: All users
- Cloud apps: 0 cloud apps selected
- Conditions: 0 conditions selected

Access controls

- Grant: 1 control selected

Conditions

Info

- Sign-in risk: Not configured
- Device platforms: Not configured
- Locations: Not configured
- Client apps (preview): Not configured
- Device state (preview): Not configured

Client apps (preview)

Configure: **Yes** | No

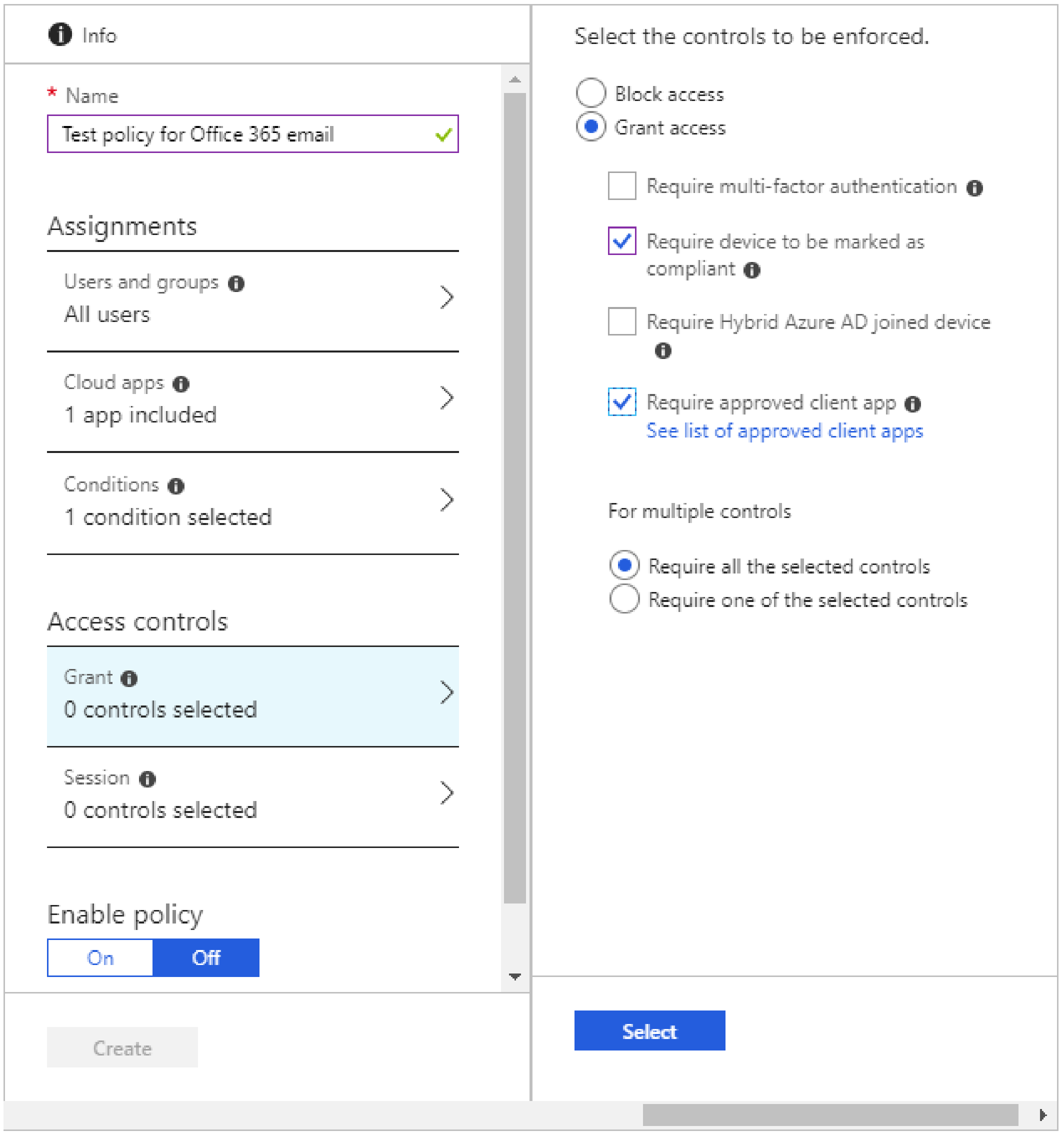
Select the client apps this policy will apply to

- □ Browser
- ☑ Mobile apps and desktop clients
  - ☑ Modern authentication clients
  - □ Exchange ActiveSync clients
  - □ Other clients

7. Under **Access controls**, select **Grant**.

. On the **Grant** pane, select **Grant access**.

   a. Select **Require device to be marked as compliant**.
   b. Select **Require approved client app**.
   c. Under **For multiple controls**, select **Require all the selected controls**. This setting ensures that both requirements you selected are enforced when a device tries to access email.
   d. Choose **Select**.



Info

* Name

Test policy for Office 365 email ✓

Assignments

Users and groups
All users

Cloud apps
1 app included

Conditions
1 condition selected

Access controls

Grant
0 controls selected

Session
0 controls selected

Enable policy

On | **Off**

Create

Select the controls to be enforced.

○ Block access
● Grant access

□ Require multi-factor authentication

☑ Require device to be marked as compliant

□ Require Hybrid Azure AD joined device

☑ Require approved client app
See list of approved client apps

For multiple controls

● Require all the selected controls
○ Require one of the selected controls

Select

8. Under **Enable policy**, select **On**.
9. Select **Create**.

Try it out

With the policies you've created, any iOS device that attempts to sign in to Office 365 email will need to enroll in Intune and use the Outlook mobile app for iOS. To test this scenario on an iOS device, try signing in to Exchange Online using credentials for a user in your test tenant. You'll be prompted to enroll the device and install the Outlook mobile app.

1. To test on an iPhone, go to **Settings** > **Passwords & Accounts** > **Add Account** > **Exchange**.
2. Enter the email address for a user in your test tenant, and then press **Next**.
3. Press **Sign In**.
4. Enter the test user's password, and press **Sign in**.

5. A message appears that says your device must be managed to access the resource, along with an option to enroll.