

LAB 4: Security considerations in Exchange and SharePoint Online.

Mobile Device Management

Contents

Introduction to LAB 4	2
Exercise 1: Send encrypted emails	2
Sending encrypted emails by a user	3
Create mail flow rule to encrypt email messages	5
Exercise 2: Configure Office 365 ATP	6
Safe attachments.....	7
Safe links - tbd	9
Exercise 3: Mobile device management	9
Configure conditional access to require approved client app	9
Configure conditional access to require approved client app and a managed device	18
Create app protection policies	21
Create device configuration profile.....	24
Enroll a client device to access the corporate email.....	26
Test the MAM and MDM policies	27
Retire the device (delete the company data).....	29

Introduction to LAB 4

In this first LAB, you will test how Office 365 Message Encryption works, create and test Advanced Threat Protection policies and finally, you will explore the Mobile device management solution – Microsoft Intune.

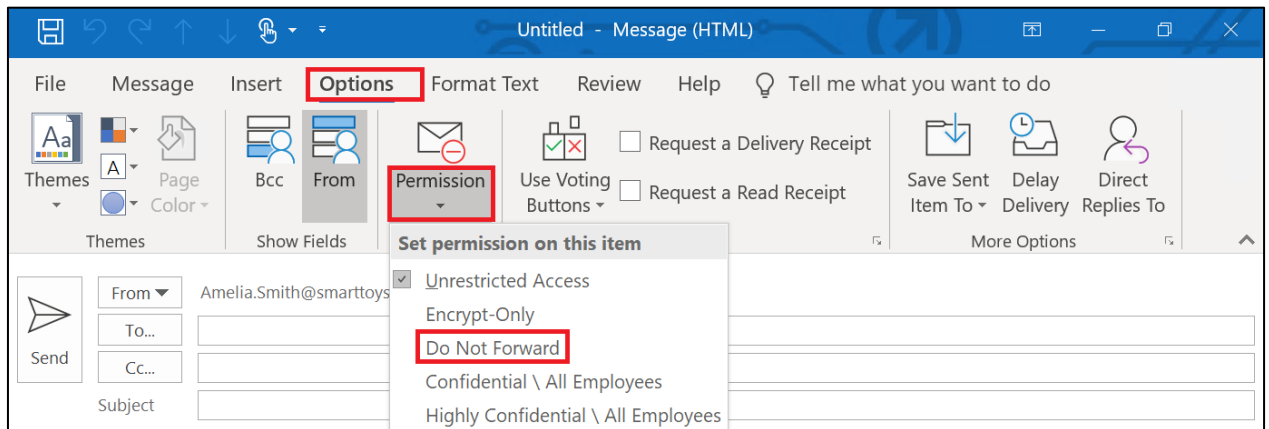
Exercise 1: Send encrypted emails

As you know, there are multiple ways to send encrypted messages in Office 365. What we will use now is OME (Office 365 Message Encryption) with the combination of “Do Not Forward” Azure RMS template.

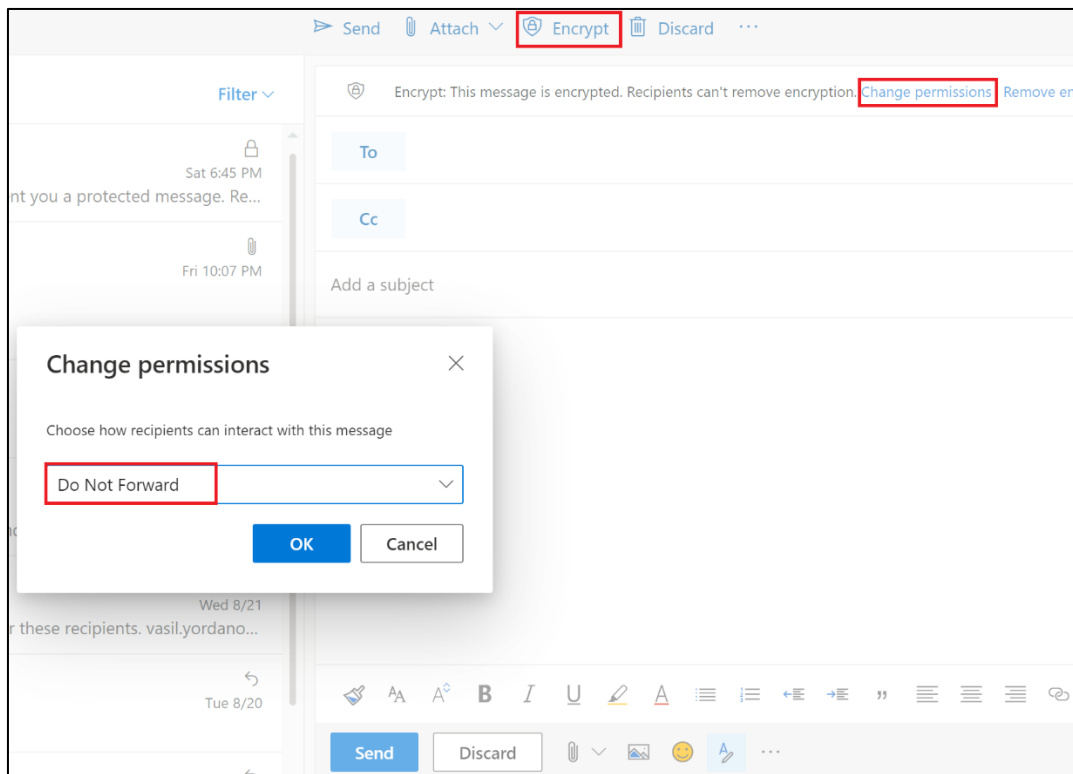
Sending encrypted emails by a user

OME should be enabled by default in your tenant. Also, there are several Azure RMS predefined templates which a user can apply to his/her outgoing emails. To send an encrypted email, follow these steps:

1. Open either **Outlook** or **Outlook for the web** and go to New email (Or New message)
2. If using Outlook, go to Options -> Permission and select Do Not Forward

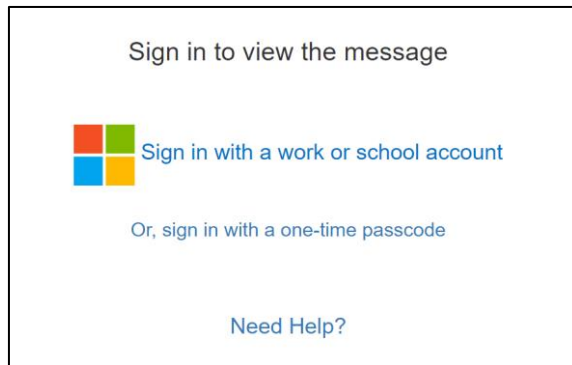


If using Outlook for the web, go to Encrypt -> Change permissions and select Do Not Forward



3. This is it! You have now sent not only encrypted email, but this email cannot be forwarded. Now go and try to open it. You should receive a link “Read the message” and the email should automatically be decrypted. If it is internal, you do not need to do anything, you will just see a sign that it is encrypted. If it is external, depending on to what domain you have sent it, you can either authenticate with your email address (for example, Gmail, Yahoo, Hotmail, Outlook) or sign in with a one-time passcode

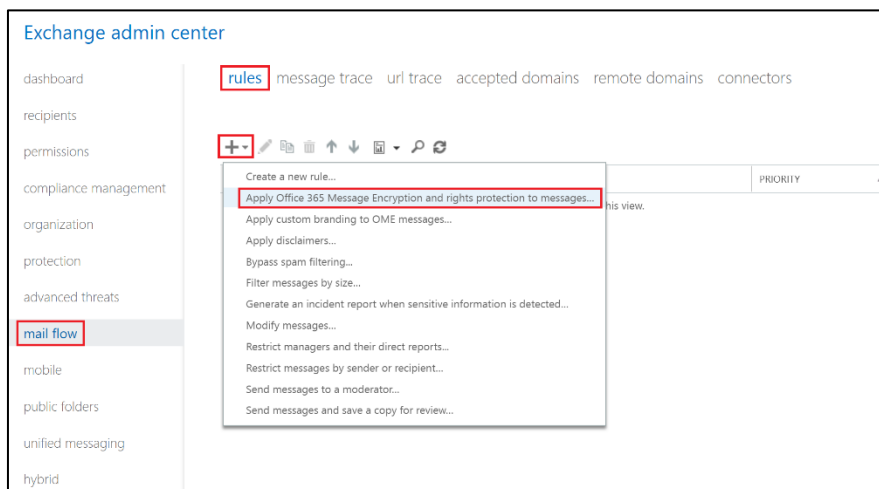
Note: If it is sent to a domain, which does not have an option to directly authenticate, you have the “one-time passcode” option, but you also have an option to create a Microsoft ID with this email address. This concept is explained and “noted” in the previous lab guide (**Exercise 3: Microsoft Teams -> Add external user as a member (guest) -> 5. Login with the external user**)



Create mail flow rule to encrypt email messages

In addition to a user's decision to send an encrypted email or not, an Office 365/Exchange Online administrator can create a mail flow rule(s) to enforce encryption of the outgoing emails. In this example, we will create a rule which will encrypt (and apply the Do Not Forward RMS template) all emails sent from a particular user.

1. With your global admin (or Exchange Online admin) go to EAC. To do this, go to <https://portal.office.com> -> Admin -> Exchange
2. Navigate to mail flow -> rules, click on the + sign and select Apply Office 365 Message Encryption and right protection to messages...



3. Choose a name of your rule, select the user who will be in scope (whose emails will be encrypted) and select the Do Not Forward template. Then click Save

The screenshot shows the 'new rule' interface in Google Chrome. The browser address bar displays the URL: `outlook.office365.com/ecp/RulesEditor/NewTransportRule.aspx?ActivityCorrelationID=da3ad620-249e-2431-d9ab-2d50566...`. The page title is 'new rule'. The 'Name:' field contains 'Encrypt mails from Amelia'. The '*Apply this rule if...' section has a dropdown menu set to 'The sender is...' and a text box containing 'Amelia Smith'. Below this is an 'add condition' button. The '*Do the following...' section has a dropdown menu set to 'Apply Office 365 Message Encryption' and an 'add action' button. The 'Except if...' section has an 'add exception' button. A 'select RMS template' dialog box is open, showing a list of templates: 'Confidential \ All Employees', 'Confidential \ All Employees', 'Highly Confidential \ All Employees', 'Encrypt', and 'Do Not Forward'. The 'Do Not Forward' template is selected. The 'select one...' button is visible. At the bottom right, there are 'Save' and 'Cancel' buttons. The 'Properties of this rule:' section at the bottom left has a checkbox for 'Audit this rule with severity level:' which is checked, and a dropdown menu set to 'Not specified'.

4. This is it! Now all the emails, sent from this user will be automatically encrypted and applied the Do Not Forward template regardless of the destination email. You can experiment with different domains/recipients and how they will read the protected email

Exercise 2: Configure Office 365 ATP

Office 365 ATP (Advanced Thread Protection) gives two additional functionalities to EOP (Exchange Online Protection):

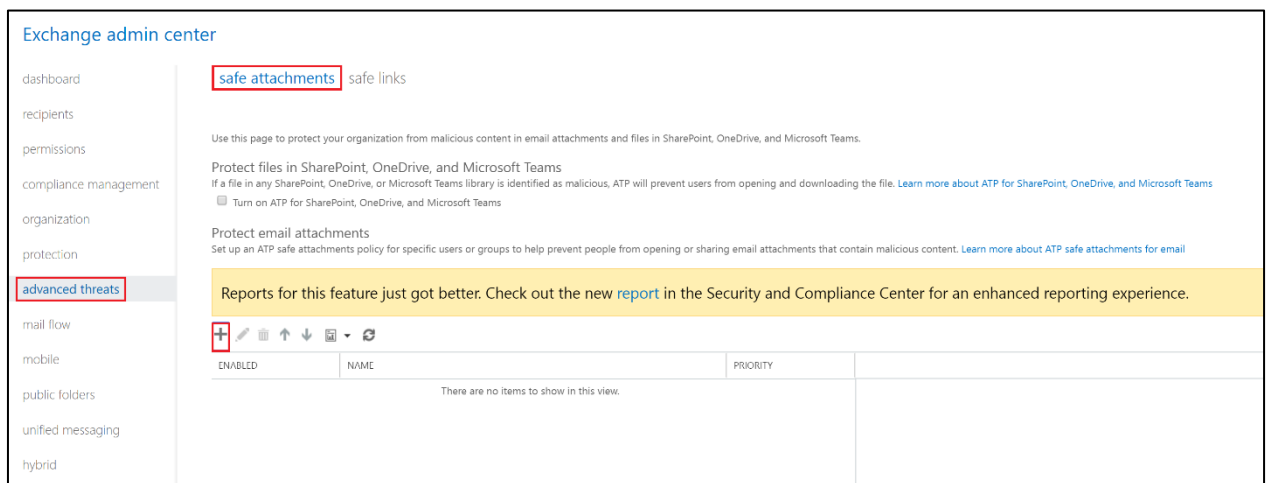
- Safe attachments

- Safe links

Although it can be enabled also for SharePoint Online, OneDrive and Microsoft Teams, we will demonstrate it now only in Exchange Online.

Safe attachments

1. Login to EAC (<https://portal.pffice.com> -> Admin -> Exchange) with a global admin (or Exchange admin) account
2. Navigate to advanced threats -> safe attachments and click on the + sign



3. Create a new safe attachments policy, click Save and confirm the warning message. For the settings of the policy, use the following:
 - Select Dynamic Delivery as attachment delivery method
 - Check the Enable redirect option and specify an email address for blocked attachments or in case of errors
 - On the **Applied To** section, select The recipient domain is and choose the custom domain that you have previously added to Office 365

Safe attachments policy - Google Chrome

outlook.office365.com/ecp/SafeAttachment/NewSafeAttachmentPolicy.aspx?ActivityCorrelationID=74cd08ee-1c48-...

new safe attachments policy

replace blocked attachments with selected images, sounds, or video messages

☒ Dynamic Delivery - Deliver the message without attachments immediately and reattach once scan is complete.

Redirect attachment on detection
Send the blocked, monitored, or replaced attachment to an email address.

☒ Enable redirect
Send the attachment to the following email address
vasil.yordanov@softunisaas.onmicrosoft.com

☒ Apply the above selection if malware scanning for attachments times out or error occurs.

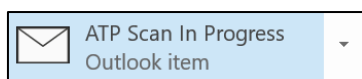
Applied To
Specify the users, groups, or domains for whom this policy applies by creating recipient based rules:

*if...
The recipient domain is smarttoys.ml
add condition

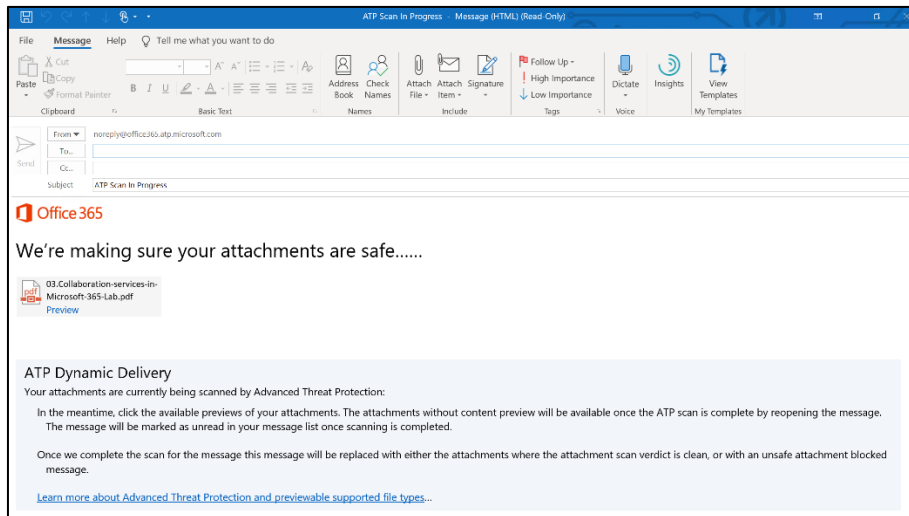
Except if...
add exception

Save Cancel

4. Your safe attachments policy is ready, and you can test it. Send an email (from external email system) containing attachment and wait in the destination user's inbox. If you are fast enough, you can see the message in the moment when it is in the mailbox, but the attachment is not yet fully checked. The attachment will look like this:



If you click on the attachment in this moment, you will see something like this:



5. After a while, the attachment should be fully scanned and tested and “inserted” into the email. Now, you can not only read the message, but use the attachment

Safe links - tbd

Exercise 3: Mobile device management

In this exercise, you will explore some interesting MAM (Mobile Application Management) and MDM (Mobile Device Management) functionalities and protection mechanisms. You will also use **Conditional access** to require that:

- a. A user needs “approved” client application (like Microsoft Outlook) to access Exchange Online (this is the MAM part)
- b. A user needs to enroll his/her device in Intune so the device becomes managed by the organization (this is the MDM part)

Configure conditional access to require approved client app

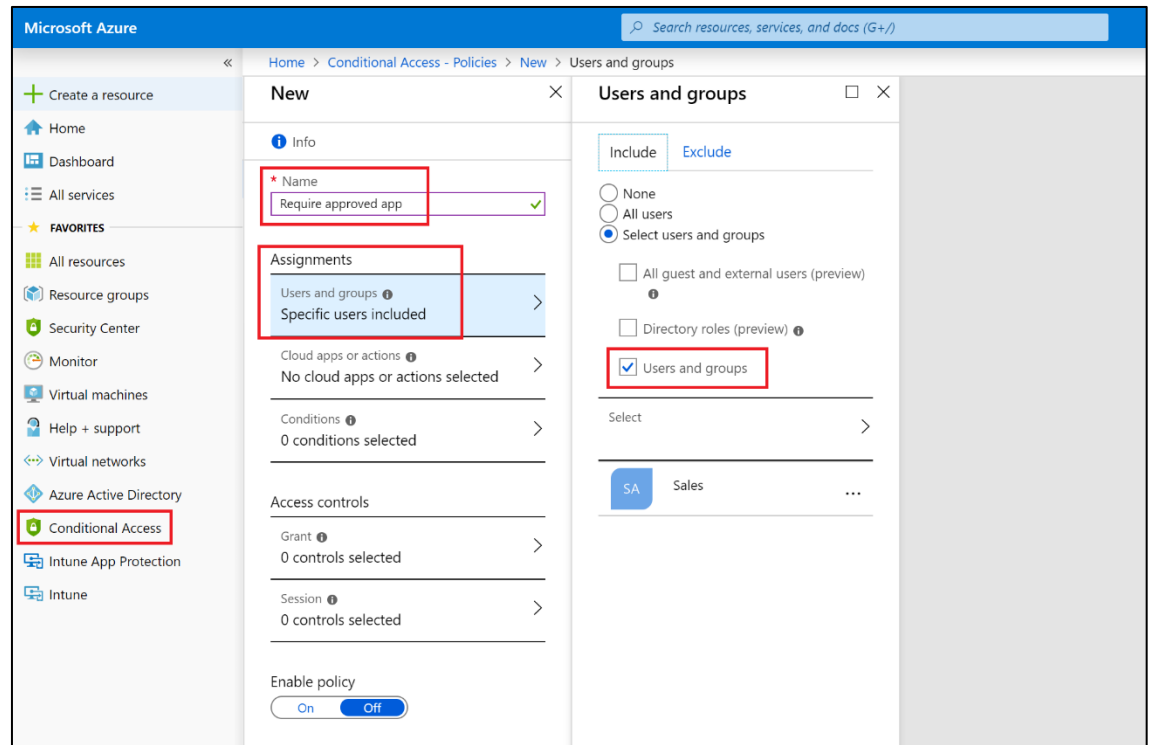
In this scenario, when a user tries to configure any email client to connect with the company email (which is Exchange Online), the system will say “Ok, but you will need an **Outlook** client to access your mailbox”.

We will create 3 policies. The first two will require approved client app (Microsoft Outlook) and the third one will block legacy apps, for security reasons. The difference between the first and the second will only be one “detail” under Conditions – one policy will be for Modern authentication clients and the other one will be for Exchange ActiveSync clients. Microsoft recommends creating two different policies for these client types.

I. **Policy 1: Require approved app**

To configure this policy, follow the steps below:

1. Go to the azure portal and login with your Office 365 global admin account:
<https://portal.azure.com>
2. Go to Conditional access section (you can first go to All services, find it there and then make it “favorite” to appear later on the left side menu or simply use the search field)
3. Create new policy using the following settings:
 - a. **Name:** Require approved app
 - b. **Users and groups:** select a user or group, which you want to be in the scope of policy. Recommendation is to put a group here (Office 365 group)



c. **Cloud apps or actions:** Office 365 Exchange Online

Home > Conditional Access - Policies > New > Cloud apps or actions

New

Info

* Name
Require approved app ✓

Assignments

Users and groups ⓘ
Specific users included >

Cloud apps or actions ⓘ
1 app included >

Conditions ⓘ
0 conditions selected >

Access controls

Grant ⓘ
0 controls selected >

Session ⓘ
0 controls selected >

Enable policy
On Off


Cloud apps or actions


Select what this policy applies to
Cloud apps User actions

Include Exclude

☐ None
☐ All cloud apps
☒ Select apps

Select
Office 365 Exchange Online >

 Office 365 Exchange Onli... ..

 Selecting Office 365 Exchange Online will also affect apps such as OneDrive and Teams.

d. **Conditions** -> **Device platforms**: Android and iOS

Home > Conditional Access - Policies > New > Conditions > Device platforms

New

Info

* Name
Require approved app ✓

Assignments

Users and groups
Specific users included

Cloud apps or actions
1 app included

Conditions
1 condition selected

Access controls

Grant
0 controls selected

Session
0 controls selected

Enable policy
On Off

Conditions

Info

Sign-in risk
Not configured

Device platforms
2 included

Locations
Not configured

Client apps (preview)
Not configured

Device state (preview)
Not configured

Device platforms

Apply policy to selected device platforms.
[Learn more](#)

Configure
Yes No

Include Exclude

Any device

Select device platforms

Android

iOS

Windows Phone

Windows

macOS

e. **Conditions -> Client apps (preview): Modern authentication clients**

Home > Conditional Access - Policies > New > Conditions > Client apps (preview)

New

Info

* Name
Require approved app ✓

Assignments

Users and groups
Specific users included

Cloud apps or actions
1 app included

Conditions
2 conditions selected

Access controls

Grant
0 controls selected

Session
0 controls selected

Enable policy
On Off

Conditions

Info

Sign-in risk
Not configured

Device platforms
2 included

Locations
Not configured

Client apps (preview)
1 included

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

- f. **Grant:** Require approved client app. At the bottom, select Require all the selected controls (although it doesn't matter at this point)

Home > Conditional Access - Policies > New > Grant

New ×

Grant □ ×

Info

* Name
Require approved app ✓

Assignments

Users and groups ⓘ
Specific users included >

Cloud apps or actions ⓘ
1 app included >

Conditions ⓘ
2 conditions selected >

Access controls

Grant ⓘ
1 control selected >

Session ⓘ
0 controls selected >

Enable policy
On Off

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](#)

☐ Require app protection policy (preview) ⓘ
[See list of policy protected client apps](#)

For multiple controls

☒ Require all the selected controls

☐ Require one of the selected controls

- g. **Enable policy:** On
Click Create at the bottom

Home > Conditional Access - Policies > New

New

Info

* Name
Require approved app ✓

Assignments

Users and groups ⓘ
Specific users included >

Cloud apps or actions ⓘ
1 app included >

Conditions ⓘ
2 conditions selected >

Access controls

Grant ⓘ
1 control selected >

Session ⓘ
0 controls selected >

Enable policy

☒ On ☐ Off

Create

II. Policy 2: Require approved app [ActiveSync]

Using the same logic and steps as the first one, create another policy. The only two different things should be:

- **Name:** Require approved app [ActiveSync]
- **Conditions -> Clients apps (preview):** Exchange ActiveSync clients (this is step “e” from **Policy 1**)

Require approved app [ActiveSync]

Info Delete

* Name
Require approved app [ActiveSync] ✓

Assignments

Users and groups
Specific users included

Cloud apps or actions
1 app included

Conditions
2 conditions selected

Access controls

Grant
1 control selected

Session
0 controls selected

Enable policy
On Off

Conditions

Info

Sign-in risk
Not configured

Device platforms
2 included

Locations
Not configured

Client apps (preview)
1 included

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

☐ Apply policy only to supported platforms

☐ Other clients

Exchange ActiveSync currently does not support all other conditions

III. Policy 3: Block legacy apps

Create the third policy. Most of the settings of this policy are the same as the first two. The different settings are:

- **Name:** Block legacy apps
- **Conditions -> Client apps (preview):** Other clients

Home > Conditional Access - Policies > Block legacy apps > Conditions > Client apps (preview)

Block legacy apps

Info Delete

Name

Block legacy apps

Assignments

Users and groups

Specific users included

Cloud apps or actions

1 app included

Conditions

2 conditions selected

Access controls

Grant

Block access

Session

0 controls selected

Enable policy

On Off

Conditions

Info

Sign-in risk

Not configured

Device platforms

2 included

Locations

Not configured

Client apps (preview)

1 included

Device state (preview)

Not configured

Client apps (preview)

Close

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

- **Grant: Block access**

Home > Conditional Access - Policies > Block legacy apps > Grant

Block legacy apps

Info Delete

Name

Block legacy apps

Assignments

Users and groups

Specific users included

Cloud apps or actions

1 app included

Conditions

2 conditions selected

Access controls

Grant

Block access

Session

0 controls selected

Enable policy

On Off

Grant

Close

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

Require app protection policy (preview)

See list of approved client apps

See list of policy protected client apps

For multiple controls

Require all the selected controls

Require one of the selected controls

All policies are now configured. What is the final effect of them?

Answer: You can create such policies if you want to force the users to use an approved client application (in this situation Microsoft Outlook for Android/iOS) if they want to use a corporate resource (in this case Exchange Online)

Configure conditional access to require approved client app and a managed device

In the previous section we have configured policies which will force a user to install Microsoft Outlook. Why? Because later, we can configure App protection policies and protect what the user can do inside Microsoft Outlook – this is one way how we can increase the protection of the corporate resources. This is known as MAM (Mobile Application Management) and is a very good solution for BYOD (bring your own device) scenarios.

Now, we will go one step further – we will not only force the user to install Microsoft Outlook as an approved app, but to make his/her device managed by the company. Why? Because this way the administrators can have greater control over the **hardware** – for example, they can restrict the phone camera. Or, if the user loses his/her device, the admins can wipe it (or only delete the company data) remotely. This is known as MDM (Mobile Device Management) and is often used for company owned devices.

What we will do now is to modify the policies from the “Configure conditional access to require approved client app” section. This modification will transform the MAM only scenario (controlling only how the user uses the application) to MAM + MDM (controlling the application usage and the whole phone as a device).

Note: At the end, we will test the MAM + MDM by enrolling a mobile phone. If you do not have a spare phone which has to be fully controlled by Intune, you can test only the MAM scenario.

I. Modify Policy 1: Require approved app

- Go again to Conditional access and click on the first policy that you have created – Require approved app. You need to modify two things:
 - Name:** Require approved app and device is registered
 - Grant:** Check the Require device to be marked as compliant checkbox so now you have two selections there

The screenshot displays the configuration page for a Conditional Access policy named "Require approved app and device is registered".

Left Pane (Policy Details):

- Name:** Require approved app and device is registered
- Assignments:**
 - Users and groups:** Specific users included
 - Cloud apps or actions:** 1 app included
 - Conditions:** 2 conditions selected
- Access controls:**
 - Grant:** 2 controls selected (highlighted with a red box)
- Session:** 0 controls selected
- Enable policy:** On (selected)

Right Pane (Grant):

Select the controls to be enforced.

- ☐ Block access
- ☒ Grant access

Require multi-factor authentication

☒ Require device to be marked as compliant (highlighted with a red box)

☐ Require Hybrid Azure AD joined device

☒ Require approved client app [See list of approved client apps](#) (highlighted with a red box)

☐ Require app protection policy (preview) [See list of policy protected client apps](#)

For multiple controls

- ☒ Require all the selected controls (highlighted with a red box)
- ☐ Require one of the selected controls

Don't lock yourself out! Make sure that your device is compliant.

Note that the Require all the selected controls option at the bottom should be selected

II. Modify Policy 2: Require approved app [ActiveSync]

Again, there are two things to be modified here:

- **Name:** Require approved app [ActiveSync] and device is registered
- **Grant:** Check the Require device to be marked as compliant checkbox so now you have two selections there

Require approved app [ActiveSync] and device is registered

Info Delete

Name
Require approved app [ActiveSync] and device is registered

Assignments

Users and groups
Specific users included

Cloud apps or actions
1 app included

Conditions
2 conditions selected

Access controls

Grant
2 controls selected

Session
0 controls selected

Enable policy
On Off

Grant

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](#)

☐ Require app protection policy (preview)
[See list of policy protected client apps](#)

For multiple controls

☒ Require all the selected controls

☐ Require one of the selected controls

Warning: Don't lock yourself out! Make sure that your device is compliant.

Note that the Require all the selected controls option at the bottom should be selected

That is all, the “blocking” policy doesn’t need to be modified. What we have achieved now?

Answer: When a client, which is in the scope of the policies, requires email access, he/she will be forced to:

1. Install and use approved client app (Microsoft Outlook)
2. Enroll the device and make it managed by the company

So far so good – we will require Outlook and a managed device. What we need to configure now is:

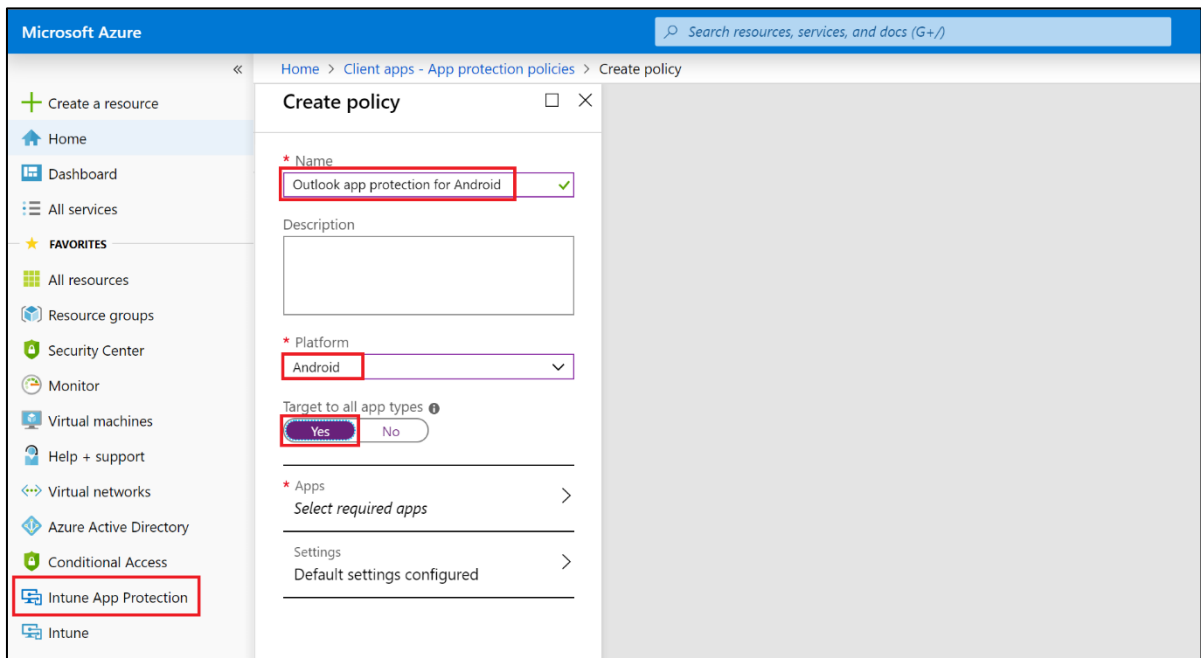
1. What the user will be allowed/denied to do in his/her Outlook
2. Restrictions that we can apply on a device level

These will be covered in the next two sections.

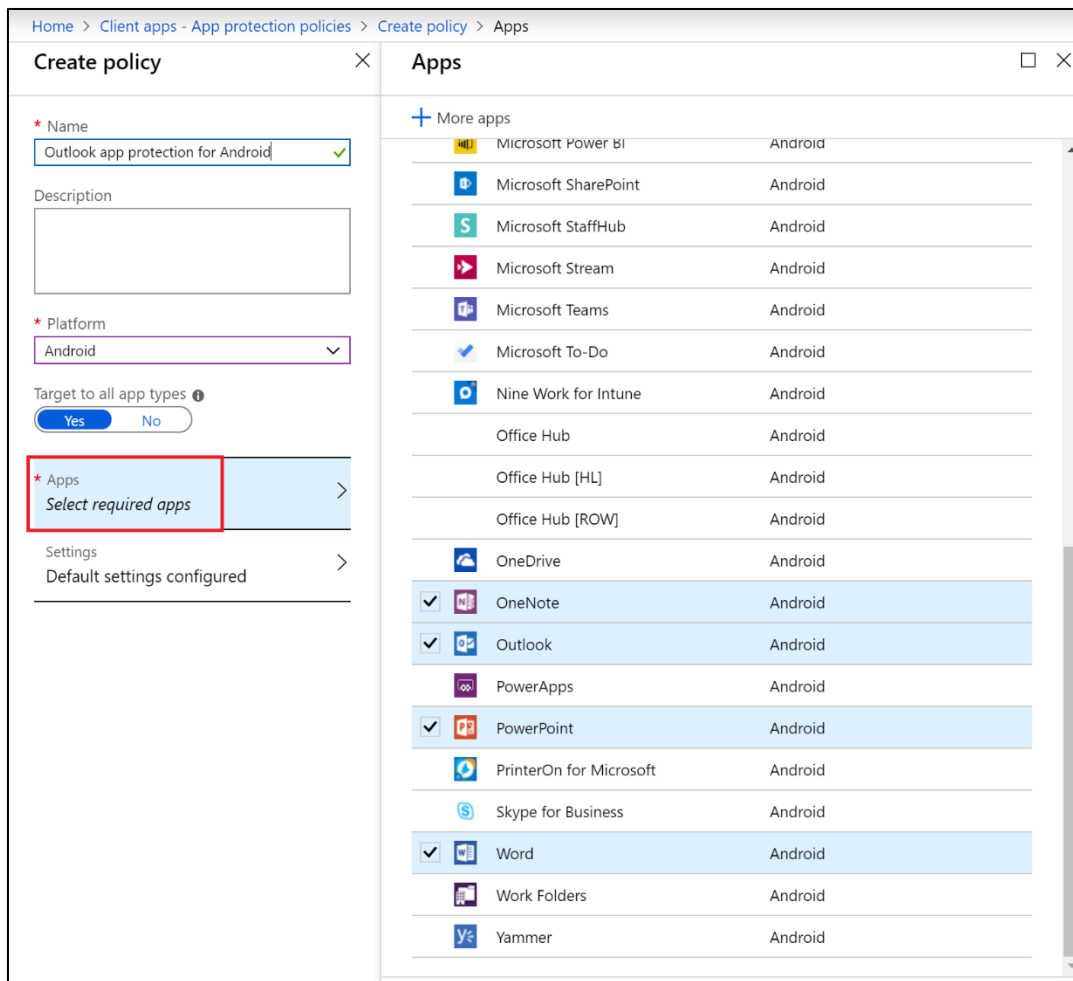
Create app protection policies

I. Create app protection policy for Android

1. Go to Intune App Protection section (this is MAM)
2. Go to App protection policies and click on Create policy
3. Name it Outlook app protection for Android, select Android as a **Platform** and click on Yes for **Target to all app types**



4. Click on Apps (Select required apps) and select Excel, OneNote, Outlook, PowerPoint and Word



5. Go to Settings. Here you have 4 sections: Data protection, Access requirements, Conditional launch and Scope (Tags). Configure only the Data protection section and leave the defaults for the others (but have a look at them). Pay attention to the highlighted entries and here is what they mean:
- **Number 1:** If you have an email with attached word document, you can only open it with Microsoft Word and not with other application
 - **Number 2:** You will not be able to download attached files to a local storage (nor to OneDrive or SharePoint) on your phone
 - **Number 3:** If you try to copy a text between an email for example, and an “external” application (like SMS, Keep Notes, Docs, etc.) you will receive a message “Your organization’s data cannot be pasted here”

Data protection

Outlook app protection Android

Save Discard

Data Transfer

Backup Org data to Android backup services ⓘ

Allow
Block

Send Org data to other apps ⓘ

Policy managed apps

Select apps to exempt

Select

Receive data from other apps ⓘ

All apps

Save copies of Org data ⓘ

Allow
Block

Allow user to save copies to selected services ⓘ

0 selected

Restrict cut, copy and paste between other apps ⓘ

Policy managed apps

Cut and copy character limit for any app

0

Screen capture and Google Assistant ⓘ

Enable
Disable

Encryption

Encrypt Org data ⓘ

Require
Not required

Encrypt Org data on enrolled devices ⓘ

Require
Not required

Functionality

Sync app with native contacts app ⓘ

Enable
Disable

Printing Org data ⓘ

Enable
Disable

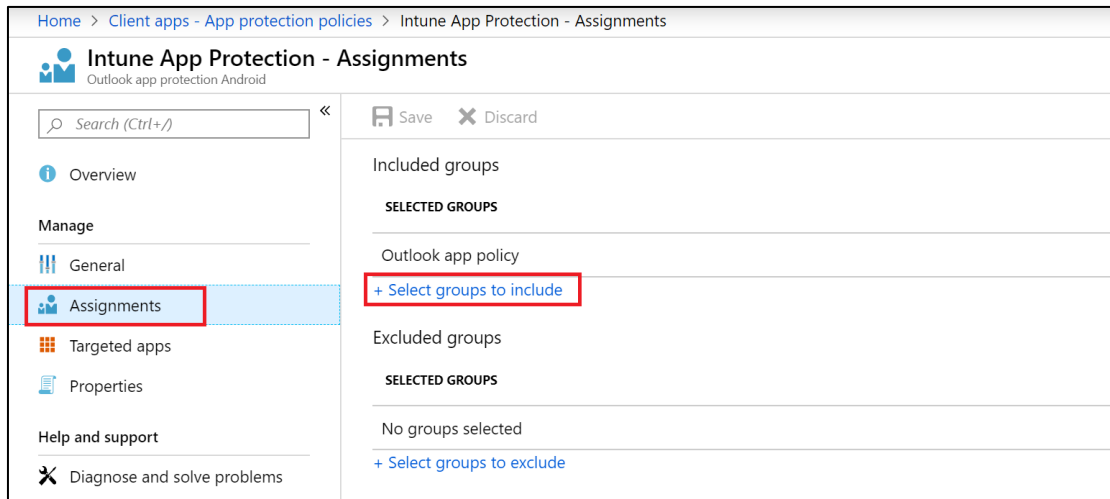
Restrict web content transfer with other apps ⓘ

Any app

Unmanaged Browser ID ⓘ

Unmanaged Browser Name ⓘ

- Click on Create to create the policy
- After the policy has been created, you need to apply it. This means that you have to open it, go to Assignments and associate it to a group. Note that you are allowed to use here only Security groups. If you do not have one, go to the Office 365 admin portal, create a security group and put members (Use the same user(s) that you use for all the policies and tests)



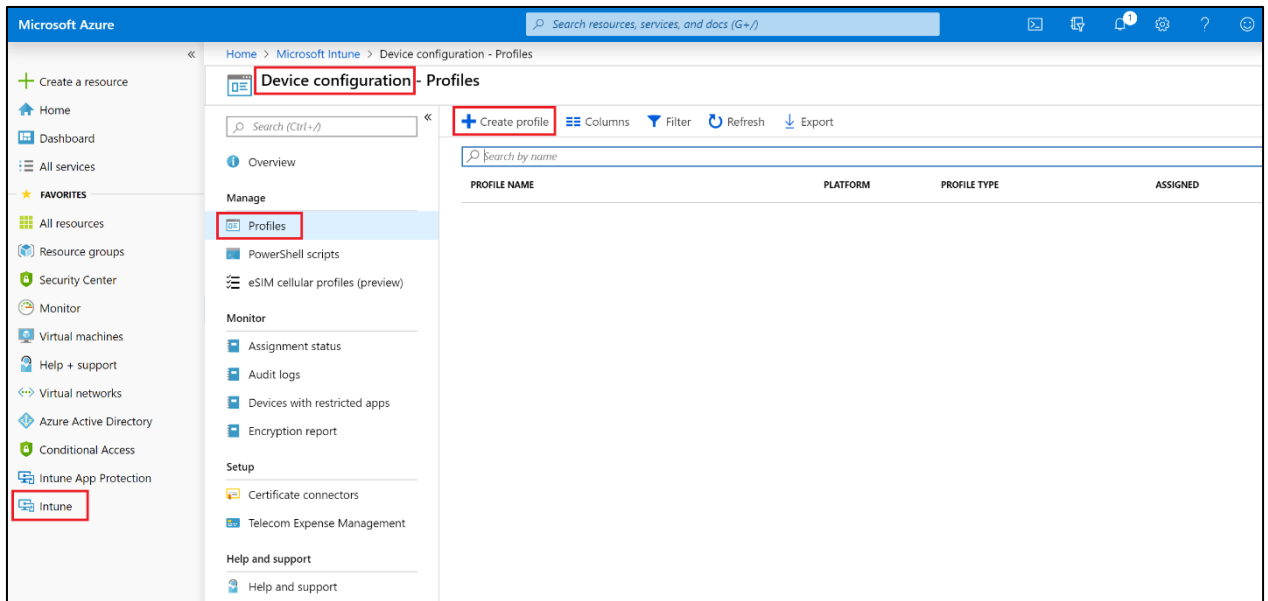
II. Create app protection policy for iOS

Use the same steps to create app protection policy, this time choosing iOS as a **Platform**

Create device configuration profile

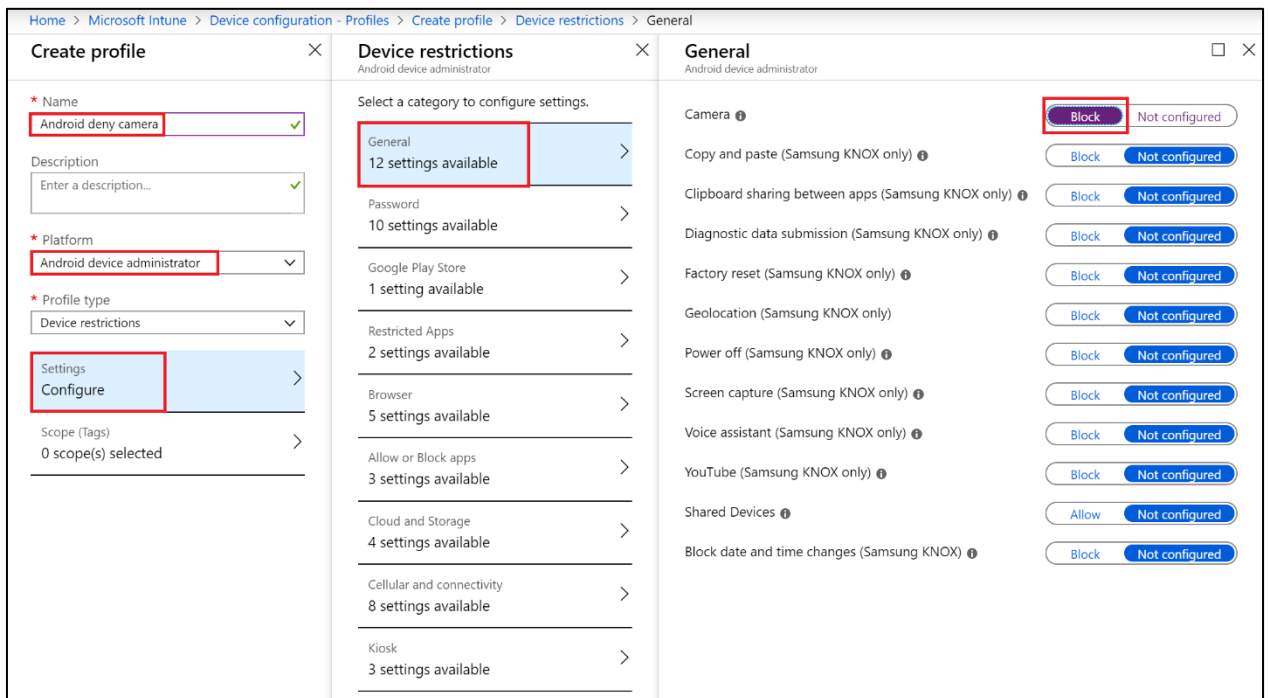
Now that we have the applications protected, we want to protect also the whole device. This is the MDM part. To do this, we need to create “Device configuration profiles”. In this example, we will create one profile, for Android, which will only block the camera access. Although the settings for iOS are not exactly the same (since the OS is different), they are similar, so you can test easily with an iPhone too.

1. Go to Intune -> Device configuration -> Profiles and click on Create profile



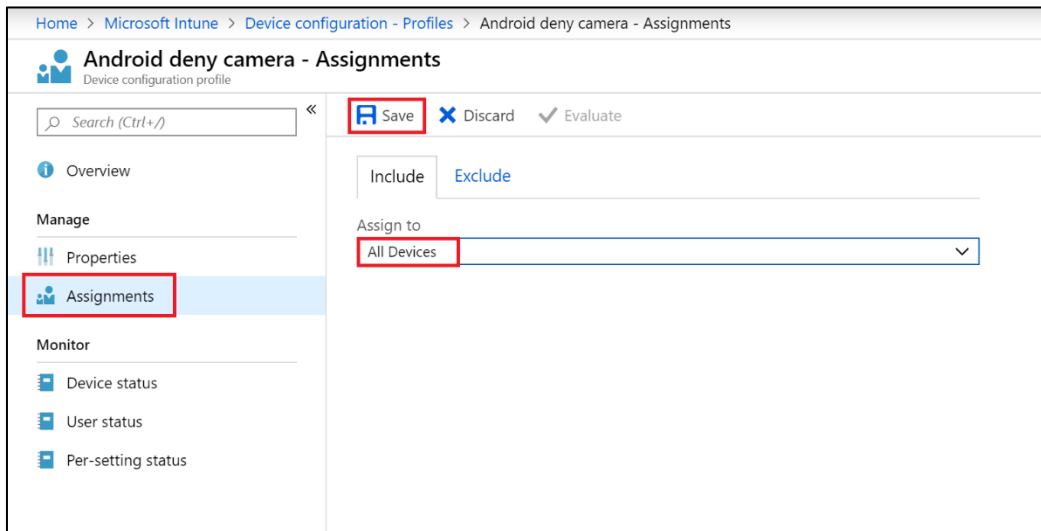
2. Make the following settings to your profile:

- **Name:** Android deny camera
- **Platform:** Android device administrator
- Go to Configure -> General and click on Block for **Camera**



Confirm your settings and click Create

- When the profile is created, go to Assignments and assign it to All devices. Then click Save



Enroll a client device to access the corporate email

If you have a spare mobile phone, which you can use for tests, you can enroll it in your Intune instance. Again, the example here and the created device configuration profile is for Android, but you can easily make it for iPhone, too.

You can watch [this video](#) to see the end-to-end enrollment process with the settings configured above. Several things to note about the process, which you will see in the video:

1. The user tries to login to her email using the native (Gmail) app
2. The user denies allowing Gmail to act as device admin
3. After the setup, the only message that the user can see inside Gmail says that she has to install Outlook in order to access her mailbox (This is because of the Require approved client app option)
4. Then she goes and installs Outlook. During the setup, she receives a message that the sign-in was successful, but she needs to **enroll** her device.

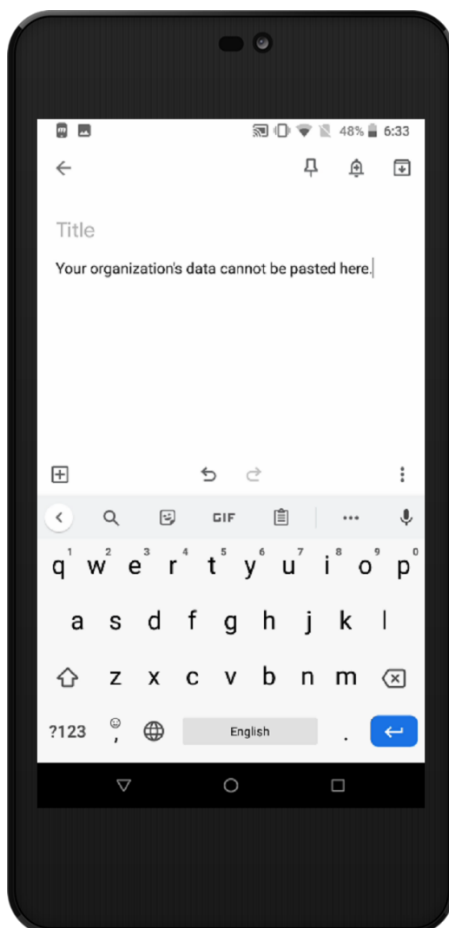
This means to install **Intune Company Portal**, to sign-in there and to make it device admin (this time if the user denies, the process fails)

5. The user goes back in Outlook and finishes the profile setup
6. All the restrictions are applied. For example, a PIN is required to be created for the Outlook app (where did this setting come from?). The device is enrolled in Intune and the MAM and MDM policies are applied

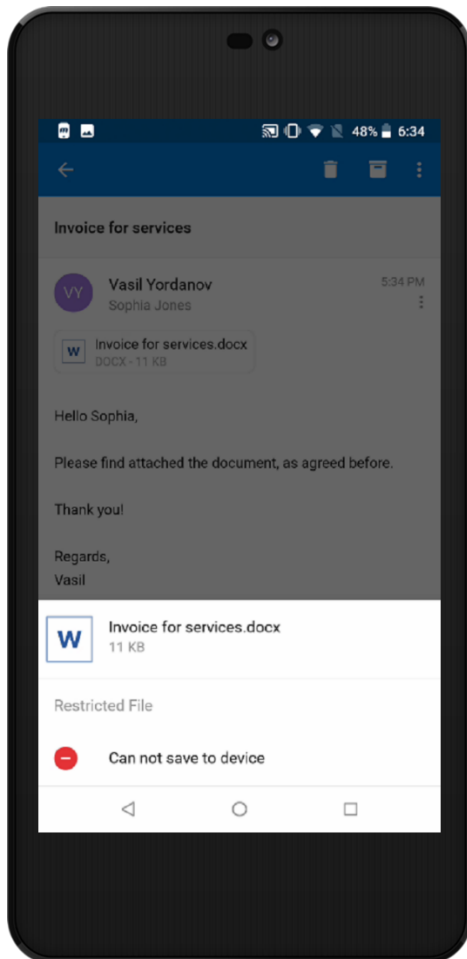
Test the MAM and MDM policies

Depending on your exact policies, you can try several things. For example:

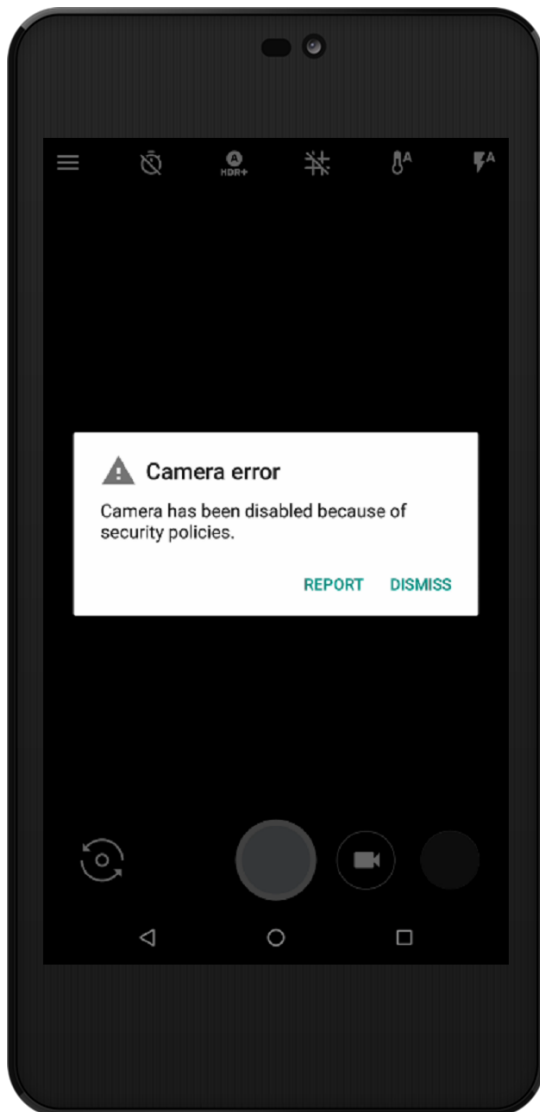
1. In Outlook, open a message, copy part of it and then go to some “external” app, like SMS, Docs or Google Keep. When you try to paste it, you will receive “Your organization’s data cannot be pasted here”. (This comes from the MAM policy)



2. In Outlook, go to a message that has attachment and try to download it. You will receive “Cannot save to device” message. (This comes from the MAM policy)



3. Try to use the camera. It will either not start or you will see a message like “Camera has been disabled because of security policies”



Retire the device (delete the company data)

Let's assume that the device has been stolen. The user reports this to you (as an administrator). You can either **Retire** (delete the company profiles and information) or **Wipe** (delete everything, make factory reset) the phone. In this example we will Retire it

1. Go to <https://portal.azure.com>
2. Navigate to Intune -> Devices and click on Intune enrolled devices

Microsoft Azure

Search resources, services, and docs (G+)

Home > Microsoft Intune > Devices

Devices
Microsoft Intune

Search (Ctrl+)

Overview

Manage

- All devices
- Azure AD devices
- Send custom notifications

Monitor

- Device actions
- Audit logs

Setup

- TeamViewer Connector
- Device cleanup rules

Help and support

- Help and support

Tenant name : smarttoys.ml

Tenant location : ---

Intune enrolled devices

LAST UPDATED 8/25/2019, 6:17:00 PM

PLATFORM	DEVICES
Android	1
iOS	0
macOS	0
Windows	0
Windows Mobile	0
Total	1

Enrolled devices
LAST UPDATED 8/25/2019, 6:17:00 PM

1

3. Find your device and click on it. Finally, click on Retire and confirm

Home > Microsoft Intune > Devices - All devices > Sophia.Jones_Android_8/23/2019_4:59 PM

Sophia.Jones_Android_8/23/2019_4:59 PM

Search (Ctrl+)

Retire Wipe Delete Remote lock Sync Reset passcode New Remote Assistance Sessi...

Overview

Manage

- Properties

Monitor

- Hardware
- Discovered apps
- Device compliance
- Device configuration
- App configuration
- Security baselines
- Recovery keys
- Managed Apps

Device name : Sophia.Jones_Android_8/23/2019_4:59 PM

Management name : Sophia.Jones_Android_8/23/2019_4:59 PM

Ownership : Personal

Serial number : 01e8c11473a24761

Phone number : ---

Primary User : Sophia Jones

Enrolled by : Sophia Jones

Compliance : Compliant

Operating system : Android

Device model : Nexus 5X

See more

Device actions status

ACTION	STATUS	DATE/TIME
No results		

You have completed LAB 4.