How to configure Microsoft Intune / Azure AD Conditional Access to Microsoft Office 365 Exchange Online

With Microsoft Intune you can do great things. You can enroll all kind of mobile devices to enforce MDM policies, push applications and even configure managed mobile applicaties like the Microsoft Office applications. You can add an additional security layer to these managed applications by applying an additional access pincode and encrypt the data within the applications. Data can be isolated, so it can only be exchanged between other managed apps. In this way you can prevent that users can save email attachments to the local device if they use the management Microsoft Outlook application.

But what makes this all useful if you can just configure mail in an unmanaged native mail client on your iPhone or Android device?

For that, we have the option to configure Conditional Access. With Conditional Access you can control under what conditions the user or device has access to SaaS applications like SharePoint and Exchange Online. The most common Conditional Access policies that I use are;

* Enforce the user to enroll the device before access to email is granted (any mail client)
* Enforce the user to use the managed Microsoft Outlook app for email (native mail clients cannot be used to access email anymore)

In this blog I will show you how to configure Conditional Access to Exchange Online. First I will show you how to enforce device enrollment and second how to enforce the use of the Microsoft Outlook application. You must know that in both cases you **need to configure two separate Conditional Access to let this fully work**! I show you why…

**Configuring Conditional Access to enforce device enrollment (Part 1)**

The first step for this blog is to create a Conditional Access policy to enforce device enrollment for modern apps (apps that support modern authentication like Microsoft Outlook).

[Graphical user interface

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-001.jpg)

Within the [Microsoft Azure Portal](https://portal.azure.com/), navigate to **Intune > Conditional access**

[Graphical user interface, text, application

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-002.jpg)

Click **Policies** and click the **“+ New policy”**button.

[Graphical user interface, application

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-003.jpg)

Give the new policy a name. For this blog I will give it the name : **CA-ExchangeOnline-ModernApps**

Under Assignment click **Users and groups** and select an Azure AD security group if you want to apply this policy to a selected group of users (optional). All users is also an option. Click **Done**

[Graphical user interface, application

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-004.jpg)

Click on **Cloud apps**, click **Select apps** en search for **Office 365 Exchange Online**. Click on **Select** and **Done**

[Graphical user interface, application, email

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-005.jpg)

Select **Conditions**, and then choose for **Client apps**. On the right hand side click **Select client apps** and select both **Browser** and **Mobile apps and desktop clients**. Click **Done**twice.

[Graphical user interface, application

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-006.jpg)

Under **Access controls** select **Grant**. On the right hand side of the screen click **Grant access** and select **Require device to be marked as compliant**. Click on **Select**in the bottom of the screen.

[Graphical user interface, application

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-007.jpg)

Make sure that **Enable policy** is set to **On** and click on **Create**

**Testing the Conditional Access policy to enforce device enrollment (Part 1)**

I will now show you what the effect of this policy is on a Apple iPad device within the Microsoft Outlook app and also the native Mail app.

[Graphical user interface, application

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-008.png)

Open the **Microsoft Outlook** app and click **Get Started**

[Graphical user interface, application

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-009.png)

Fill in your email address and click **Add account**

[Graphical user interface, website

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-010.png)

Enter your password and click **Sign in**

[Graphical user interface

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-011.png)

As you can see, the user is forced to Enroll the device before access to email is granted. So far so good…

[Graphical user interface, application

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-012.png)

Let’s do the same test with the native Mail client. Start the **Mail** app and click **Exchange**

[Graphical user interface, application

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-013.png)

Fill in your email address and click **Next**

[Graphical user interface, text, application, chat or text message

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-014.png)

This is an important step. If you choose for **Sign In** the modern authorization method will be used with Autodiscovery. If you choose for **Configure Manually**.. well just like the name says. You have to configure everything yourself without Autodiscovery but also not with modern authorization. We will come back to that later. For now choose **Sign In**.

[Graphical user interface, website

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-015.png)

Fill in the password en click **Sign in**

[Graphical user interface, application, Word

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-016.png)

As you can see, this time the user is also enforced to enroll the device, so that’s OK. But what if you hit the **Cancel** button or if you had chosen **Configure Manually**in the previous step? Lets find out.. Hit the **Cancel**button.

[Graphical user interface, text, application, chat or text message

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-017.png)

Click **Ok**

[Graphical user interface, application

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-018.png)

Manually fill in the requested information and click **Next**

[Graphical user interface, application

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-019.png)

Everything is correct

[Graphical user interface

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-020.png)

Click **Save**

[Graphical user interface, text, application, email

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-021.png)

And now I have access to my email without enrolling the device. To solve this “problem” we need to configure a second policy.

**Configuring Conditional Access to enforce device enrollment (Part 2)**

[Graphical user interface, text, application, email

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-022.jpg)

Within the Microsoft Azure portal go back to **Intune > Conditional access**. Select Policies and click the “**+New Policy**” botton.

[Graphical user interface, application

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-023.jpg)

Give the new policy a name. For this blog I will give it the name : **CA-ExchangeOnline-EAS**

Under Assignment click **Users and groups** and select an Azure AD security group if you want to apply this policy to a selected group of users (optional) Click **Done**

[Graphical user interface, application

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-024.jpg)

Click on **Cloud apps**, click **Select apps** en search for **Office 365 Exchange Online**. Click **Select** and **Done**

[Graphical user interface, application

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-025.jpg)

Select **Conditions**, and then choose for **Client apps**. This time select **Exchange ActiveSync**. Click **Done**twice.

[Graphical user interface, text, application

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-026.jpg)

Under **Access controls** select **Grant**. On the right hand side of the screen click **Grant access** and select **Require device to be marked as compliant**. Click on **Select**in the bottom of the screen.

[Graphical user interface, application

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-027.jpg)

Make sure that **Enable policy** is set to **On** and click on **Create**

**Testing the Conditional Access policy to enforce device enrollment (Part 2)**

I will now show you what the effect of this policy is on a Apple iPad device within the native Mail app with manual configuration.

[Graphical user interface, application

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-028.png)

Start the native **Mail** app and click **Exchange**

[Graphical user interface, application

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-029.png)

Fill in your email address and click **Next**

[Graphical user interface, text, application, chat or text message

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-030.png)

Click **Configure Manually**

[Graphical user interface, application

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-031.png)

Fill in the password en click **Next**

[Graphical user interface, application

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-032.png)

Fill in the requested information and click **Next**

[Graphical user interface

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-033.png)

Click **Save**

[Graphical user interface, text, application, email

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-034.png)

As you can see, the policy is applied and no mail can be received before enrolling the device.

**Configuring Conditional Access to enforce the Microsoft Outlook App (and block the use of the native mail apps)**

In the next step I show you how to enforce the use of the (managed) Microsoft Outlook app and blocking the use of any native mail client. If you are using Microsoft Intune and configure Mobile Application Management (MAM) policies to protect company data (like email and documents) this would be the minimum Conditional Access policy to configure.

The steps of this Conditional Access policy are, except for one step, the same as the previously made Conditional Access policies to enforce device enrollment. Therefore, I only show you the setting that is different. Create also two policies for this scenario, one for the modern apps, and one for Exchange ActiveSync! You can also combine the settings into one policy (Enrollment enforcement and Outlook enforcement, but again, you still need to create two policies, one for ModernApps, one for EAS).

[Graphical user interface, text, application

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-035.jpg)

Create a new Conditional Access policy (or edit the first one) and walk through the same steps as with the first created CA policy. The only difference is under **Access controls**. Select **Grant**. On the right hand side of the screen click **Grant access** and select **Require approved client app**. Click on **Select**in the bottom of the screen and **Save**. Repeat this step for both policies (EAS and Modern Apps).

**Test the Microsoft Outlook Conditional Access enforcement policy**

Lets take a look at the results of the second Conditional Access policy.

[Graphical user interface, Word

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-036.png)

These are the results when you choose the **Sign In** option (Autodiscovery) when configuring the native mail client

[Graphical user interface, text, application, email

Description automatically generated](http://www.robinhobo.com/wp-content/uploads/2017/12/How-to-configure-Microsoft-Intune-Azure-AD-Conditional-Access-to-Office-365-Exchange-Online-037.png)

These are the results when you choose the **Configure Manually** option when configuring the native mail client.

**Conclusion**

When using Microsoft Intune to manage mobile devices and manage applications in combination with Microsoft Office 365 / Exchange Online, Conditional Access policies are a very powerful way to protect company email and data. Enforcing the end user to enroll their mobile devices or to force the end user to use a managed version of the Microsoft Outlook mobile app (instead of the unmanaged native mail client) gives the company the power to keep in control of the company data at any time.