Conditional Access Policies

Microsoft Intune conditional access policies are configured against particular services, helping to ensure that only managed and compliant devices can access the service.

They can define rules such as which Azure Active Directory security user group or which Intune user or device group will be targeted and how devices that cannot enroll with Intune will be managed.

Unlike other Intune policies, administrators do not deploy conditional access policies. Instead, these are configured within the Intune management portal once and can either apply all users, targeted security group users or security groups members that are exempt from this policy.

When mobile devices do not meet the conditions administrators configure, the user is guided though the process of enrolling the device and fixing the issue that prevents the device from being compliant.

Conditional Access Policies can remediate mobile device's compliance for:

- Exchange Online
- Exchange On-premises
- SharePoint Online
- Skype for Business

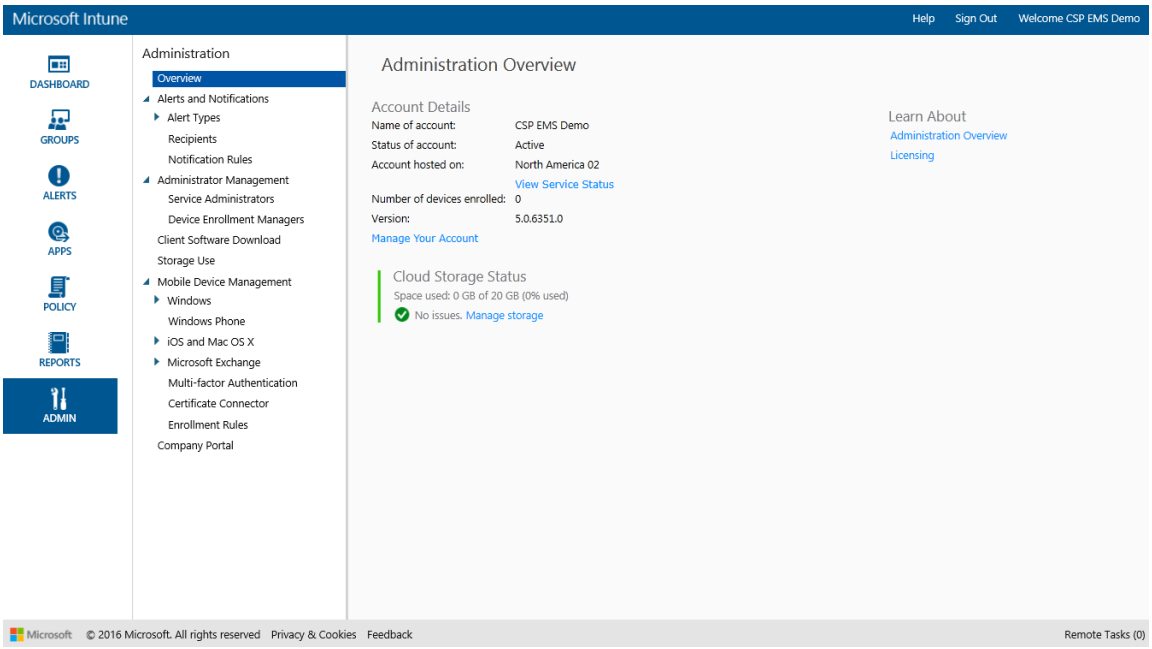
Use the table below to obtain the end customers' requirements and the settings needed to configure the conditional access policy.

Conditional Access Policy setting	**Description**	**End Customer Setting**
Outlook and other apps that use modern authentication	Specifies which platforms and requirements must be met to allowed access to Exchange Online	**All Platforms/Specific Platforms:** iOS Android Windows 10 Mobile **Windows must meet the following requirements:** Devices must be domain joined or compliant Devices must be domain joined Devices must be compliant
Exchange ActiveSync apps that use basic authentication	Specifies whether to allow or block access to Exchange Online on non-compliant, or non-supported devices	Block non-compliant devices on platforms supported by Microsoft Intune/Block all other devices on platforms not supported by Microsoft Intune
Targeted Groups	Specifies the AD security groups to target with this policy	All users/Selected security groups
Exempt Groups	Specifies the AD security groups to exempt from this policy (overrides members in the Targeted Groups list)	No exempt users/Selected security groups

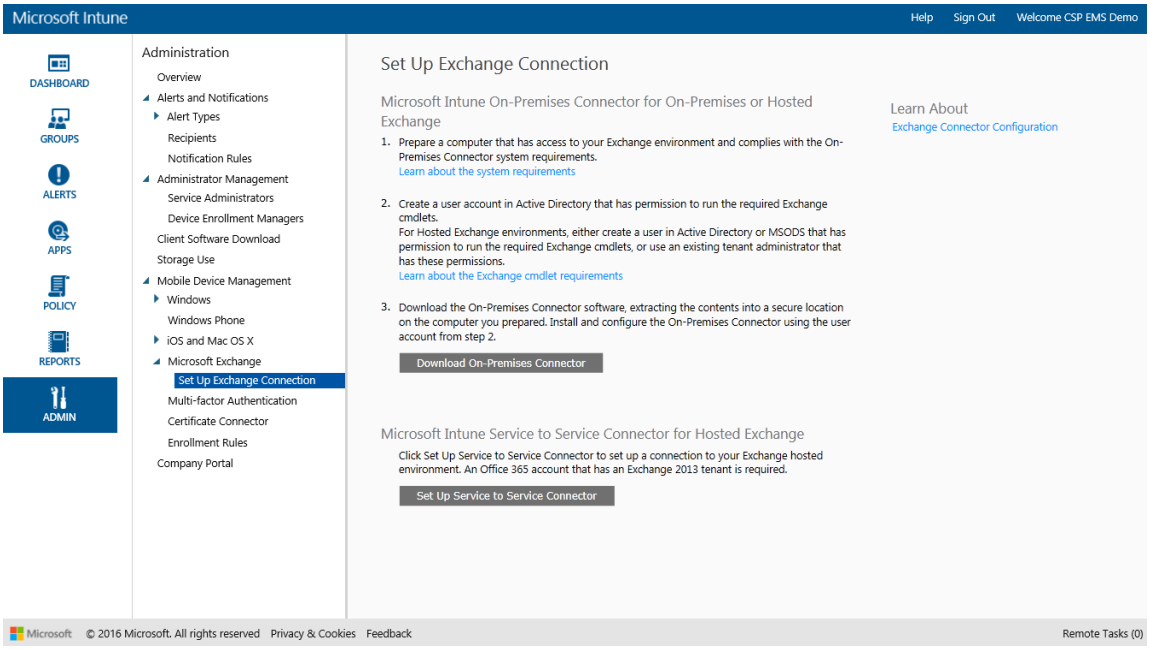
As an **example**, a conditional access policy will be created to further secure access to the organization's Exchange Online service. As part of the requirement to enabling Exchange Online Conditional Access, the Intune Service to Service connector is required to be configured in the Intune subscription.

The Service connector creates the relationship between the Intune subscription and the Exchange Online service, allowing for both compliance and conditional access conditions to be verified on enrolled devices prior to gaining access to the Exchange Online service.

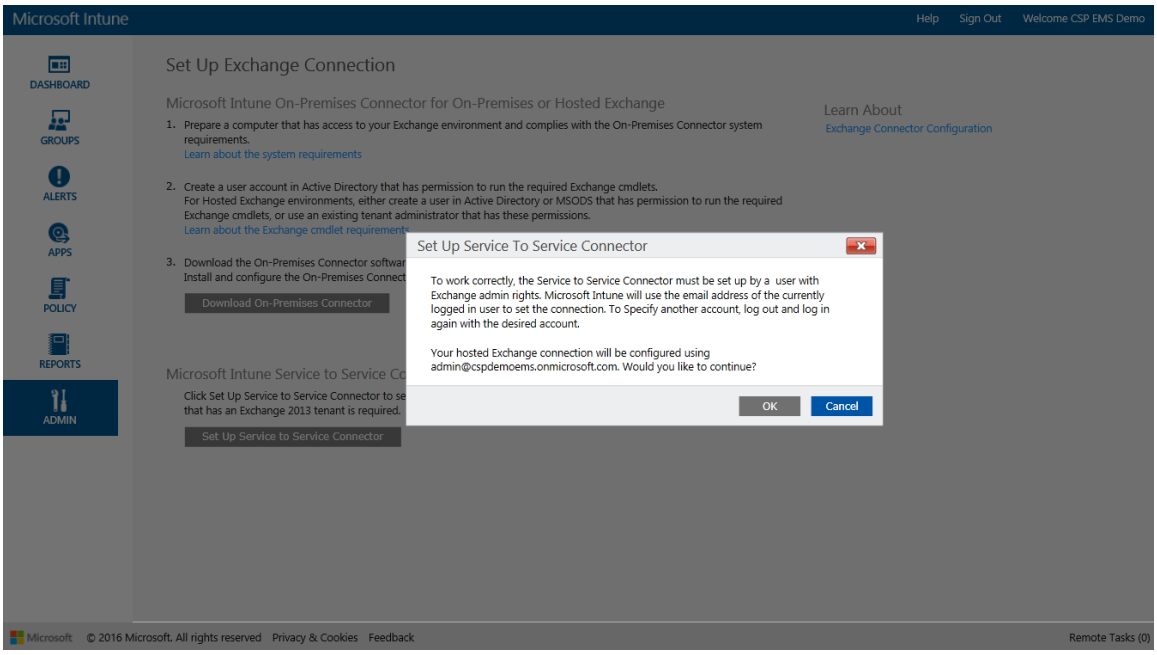
1. Login to the [Intune management portal] with an account with Office 365 Global Administrator privileges, and select **Admin**.



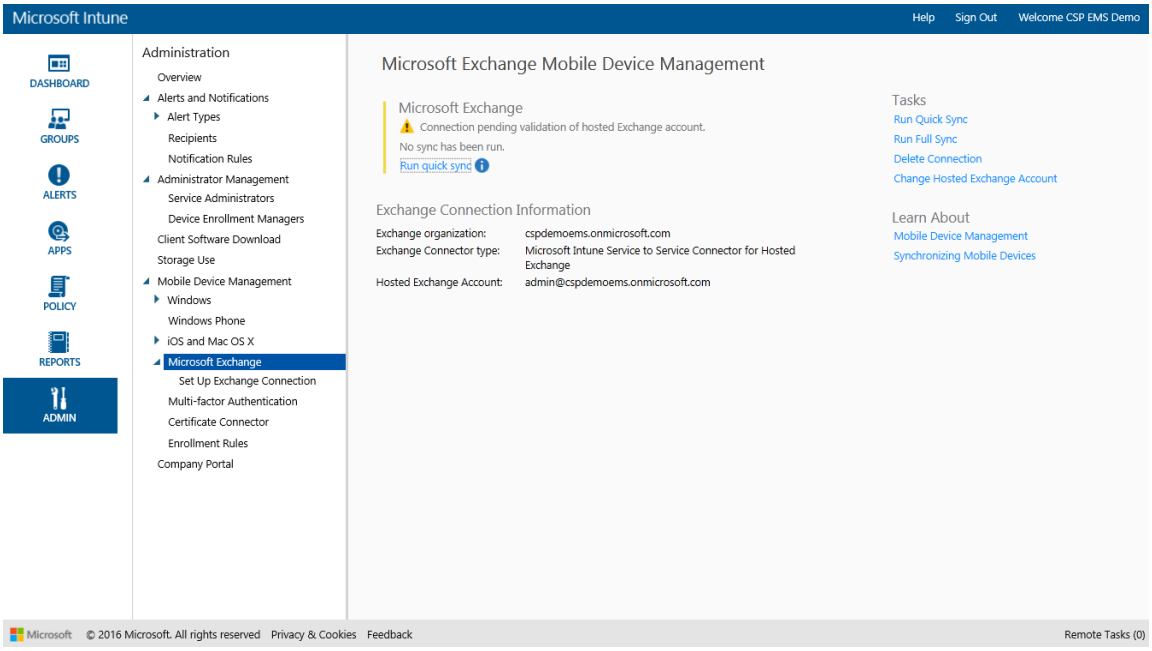
2. Expand **Mobile Device Management**, then **Microsoft Exchange** and select **Set Up Exchange Connection.**



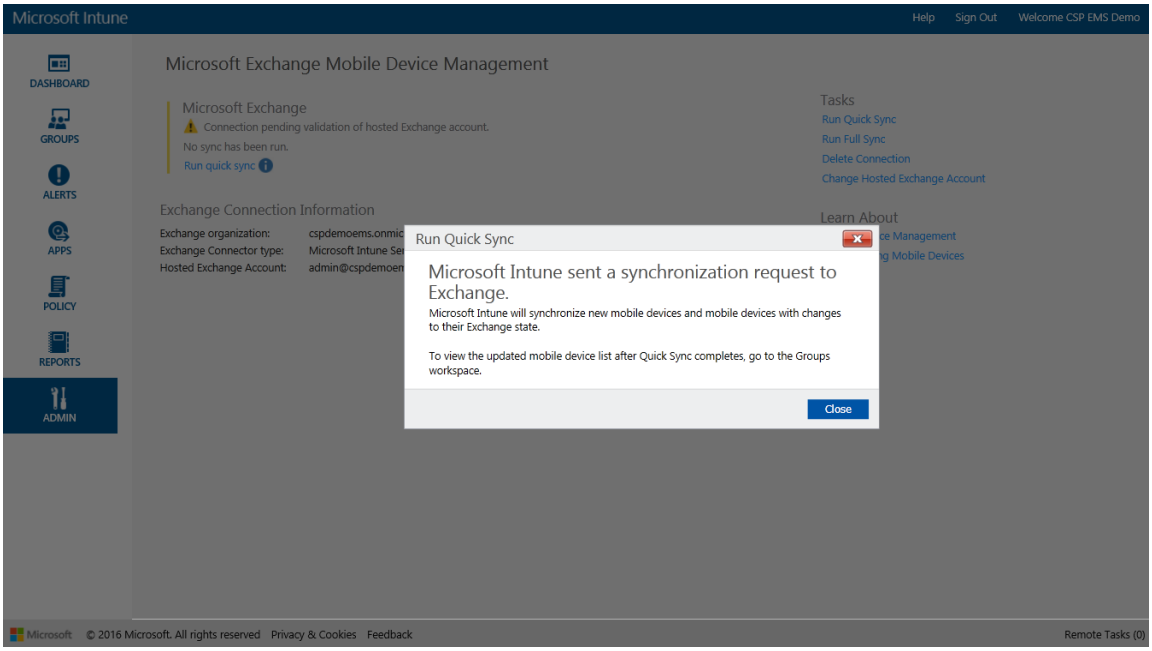
3. Select **Set Up Service to Service Connector.**



4. Select **OK** when prompted to use the signed-in Global Administrator account to configure the Service to Service Connector.

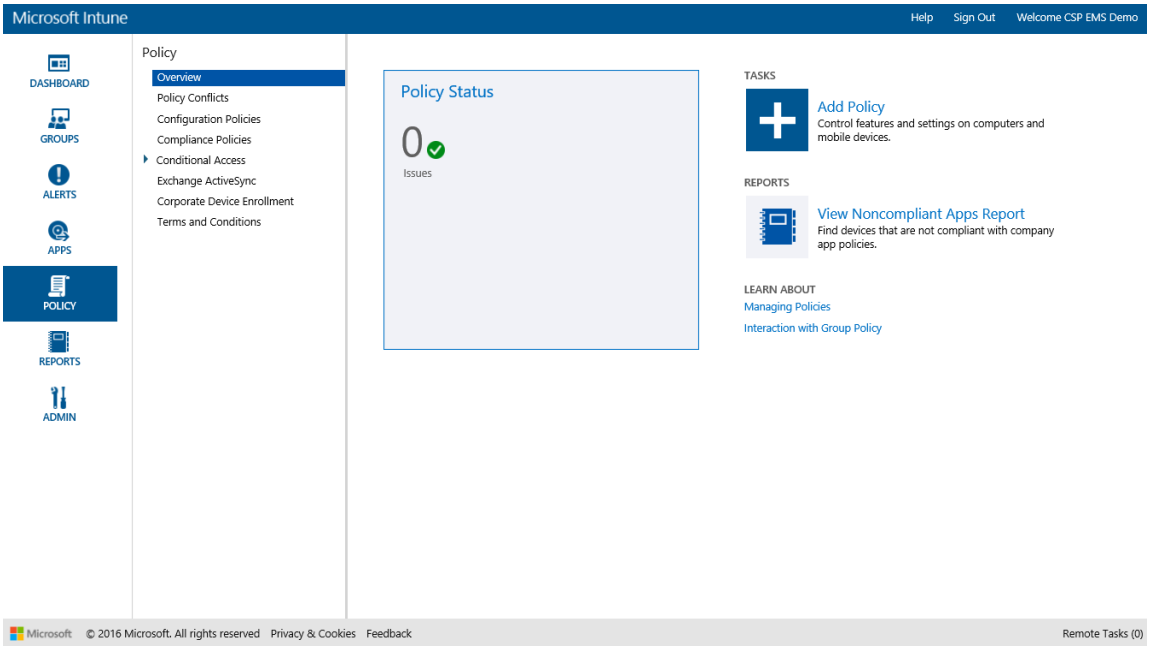


5. Select **Run quick sync.**

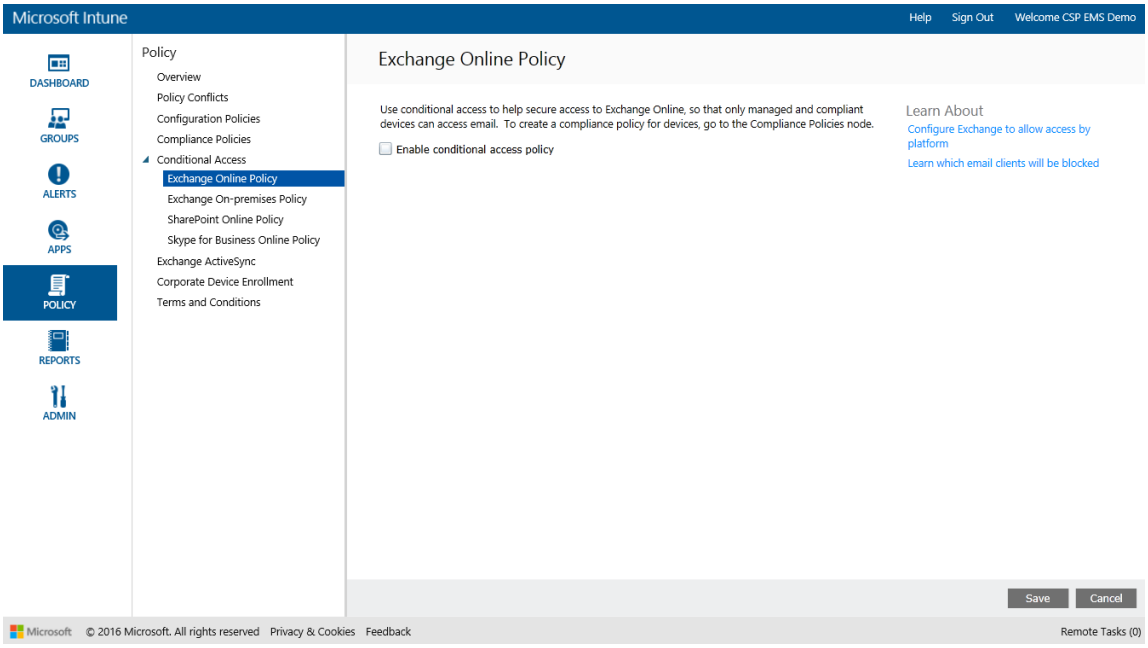


6. Select **Close** when prompted. The connector will synchronize mobile devices and new mobile devices with changes to their Exchange state.

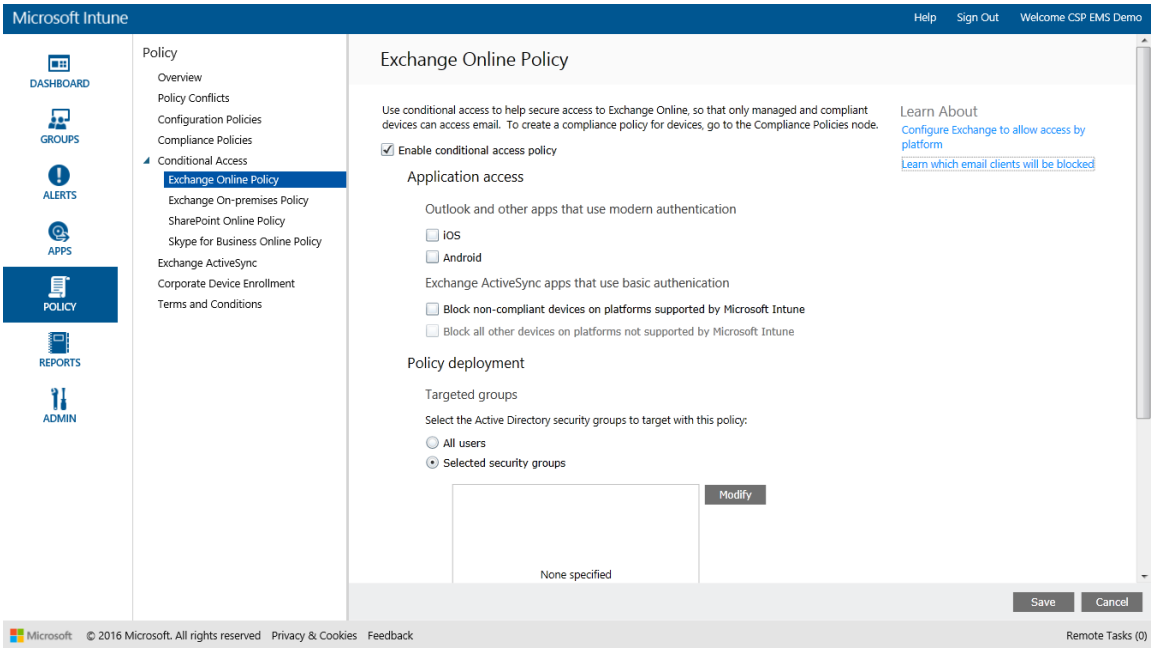
7. Select **Policy.**



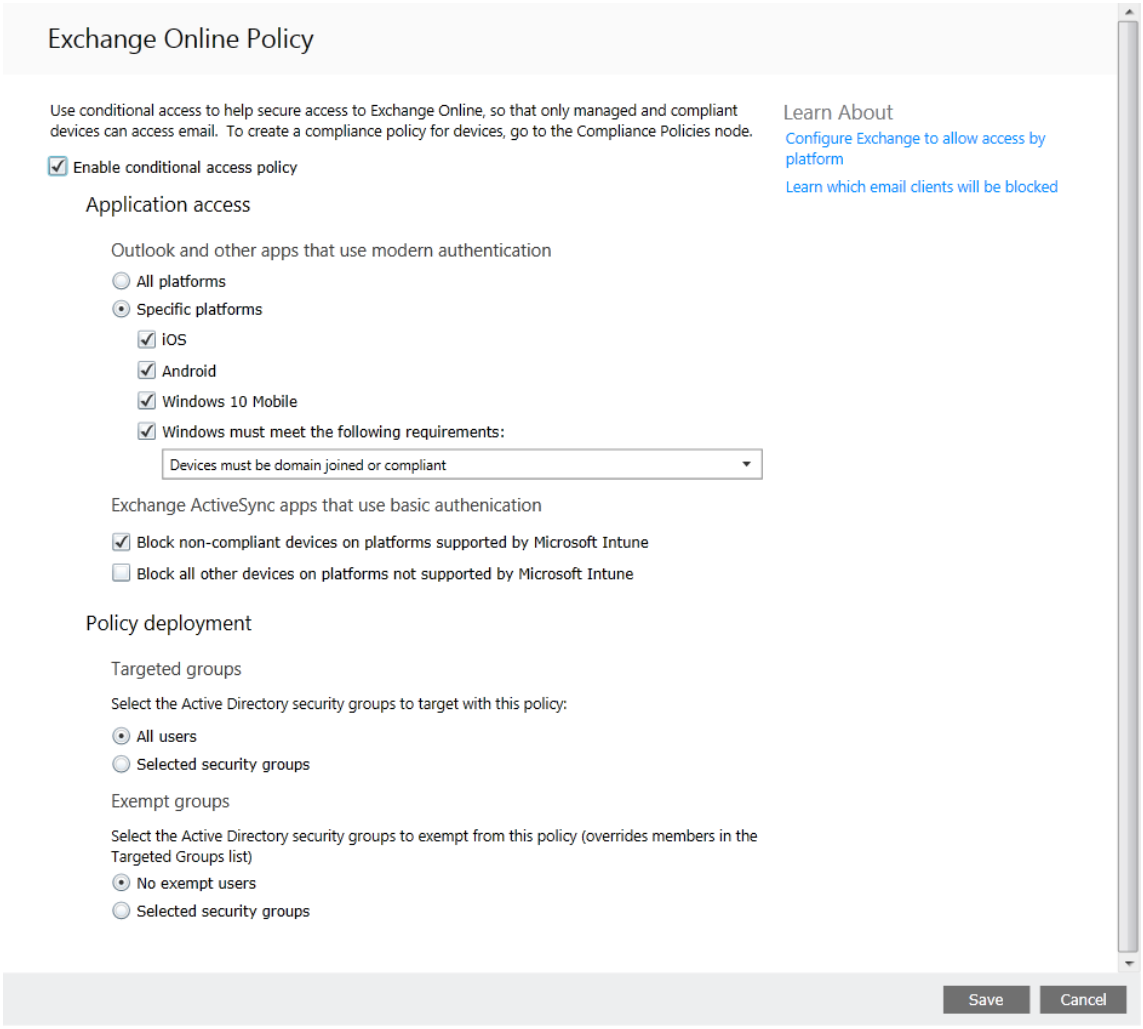
8. Expand **Conditional Access** and select **Exchange Online Policy.**



9. Tick the checkbox for **Enable conditional access policy.**



10. Configure the settings as agreed upon with the end customer.



11. Select **Save**. This conditional access policy is now configured to help secure the end customers Exchange Online service, and references the compliance policy already deployed.