

# 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 through 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.

<b><u>Conditional Access Policy setting</u></b>	<b><u>Description</u></b>	<b><u>End Customer Setting</u></b>
<b>Outlook and other apps that use modern authentication</b>	Specifies which platforms and requirements must be met to allowed access to Exchange Online	<b>All Platforms/Specific Platforms:</b> iOS Android Windows 10 Mobile <b>Windows must meet the following requirements:</b> Devices must be domain joined or compliant Devices must be domain joined Devices must be compliant
<b>Exchange ActiveSync apps that use basic authentication</b>	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
<b>Targeted Groups</b>	Specifies the AD security groups to target with this policy	All users/Selected security groups
<b>Exempt Groups</b>	Specifies the AD security groups to exempt from this policy (overrides members in the Targeted Groups list)	No exempt users/Selected security groups

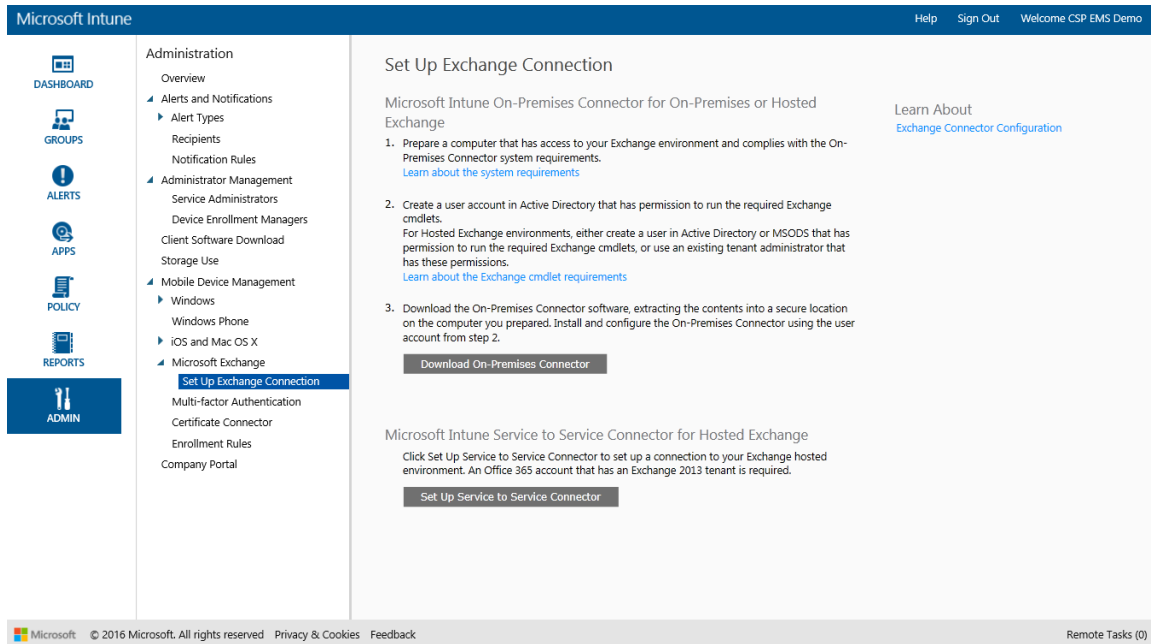
As an **example**, a conditional access policy will be created to further secure access to the organization's Exchange Online service. As part of the requirement to enabling Exchange Online Conditional Access, the Intune Service to Service connector is required to be configured in the Intune subscription.

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.

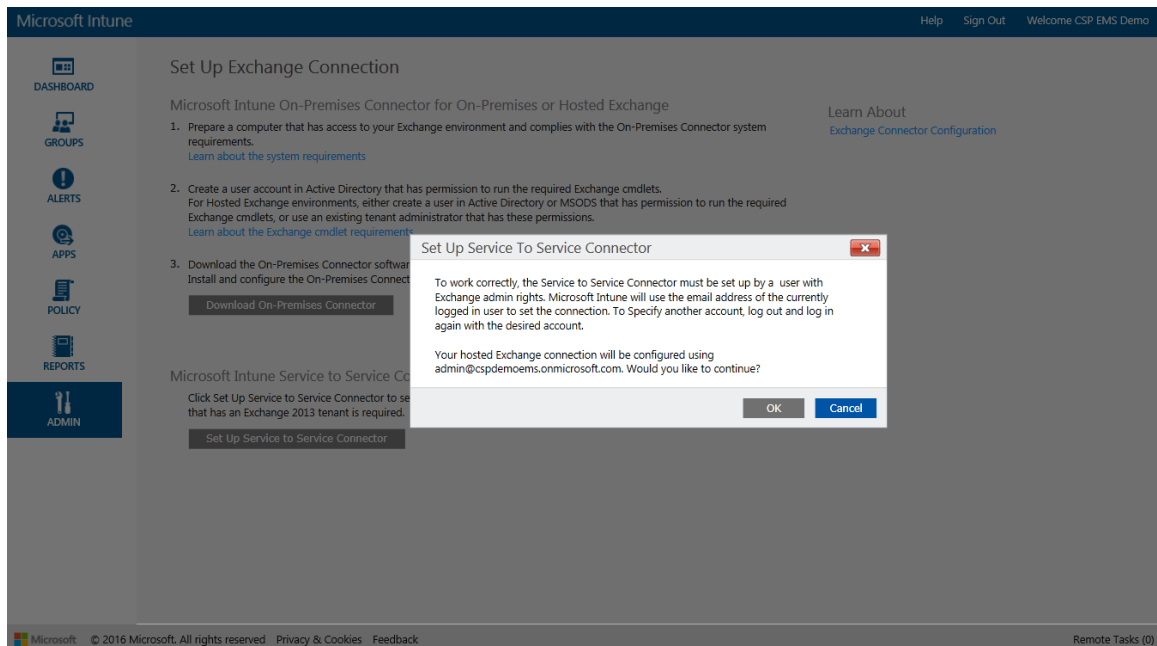
1. Login to the [Intune management portal](#) with an account with Office 365 Global Administrator privileges, and select **Admin**.

The screenshot displays the Microsoft Intune management portal interface. The top navigation bar includes the 'Microsoft Intune' logo, a 'Help' link, a 'Sign Out' button, and a 'Welcome CSP EMS Demo' message. On the left, a vertical sidebar contains icons for 'DASHBOARD', 'GROUPS', 'ALERTS', 'APPS', 'POLICY', 'REPORTS', and 'ADMIN' (which is highlighted in blue). The main content area is titled 'Administration Overview' and is divided into two columns. The left column lists administrative categories: 'Overview' (selected), 'Alerts and Notifications' (with sub-items 'Alert Types', 'Recipients', and 'Notification Rules'), 'Administrator Management' (with sub-items 'Service Administrators', 'Device Enrollment Managers', 'Client Software Download', and 'Storage Use'), and 'Mobile Device Management' (with sub-items 'Windows' (including 'Windows Phone'), 'iOS and Mac OS X', and 'Microsoft Exchange' (including 'Multi-factor Authentication', 'Certificate Connector', 'Enrollment Rules', and 'Company Portal')). The right column provides account details for 'CSP EMS Demo', showing an active status, North America 02 hosting, 0 enrolled devices, and version 5.0.6351.0. It also includes a 'Cloud Storage Status' section indicating 0 GB of 20 GB is used. A footer at the bottom contains the Microsoft logo, copyright information for 2016, and links for 'Privacy & Cookies' and 'Feedback'. A 'Remote Tasks (0)' indicator is visible in the bottom right corner.

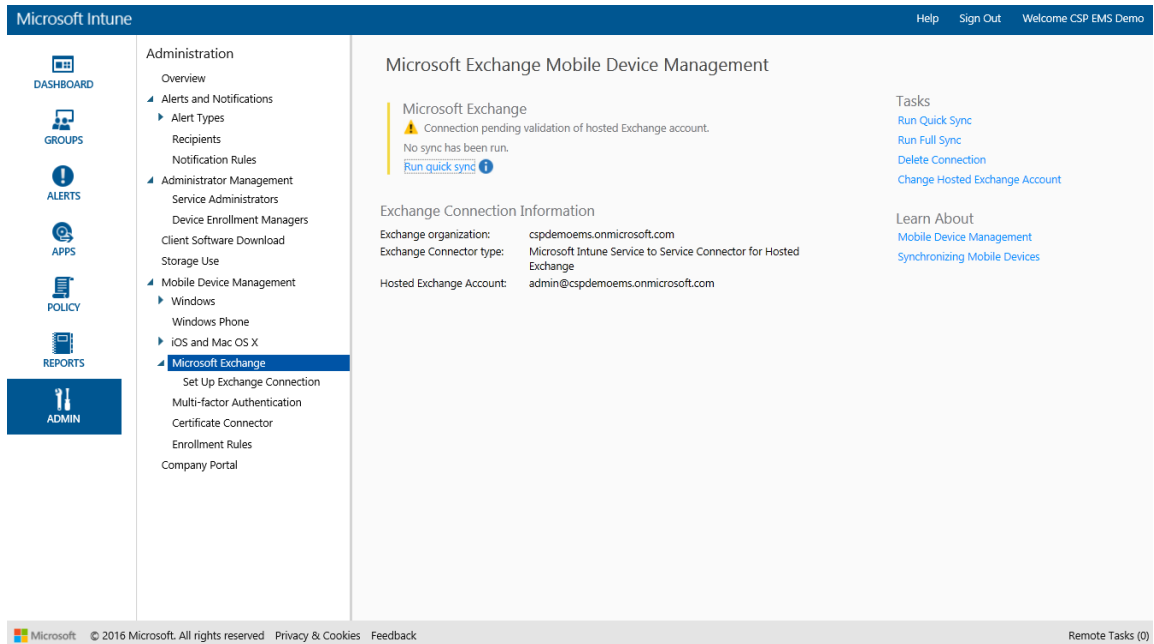
- Expand **Mobile Device Management**, then **Microsoft Exchange** and select **Set Up Exchange Connection**.



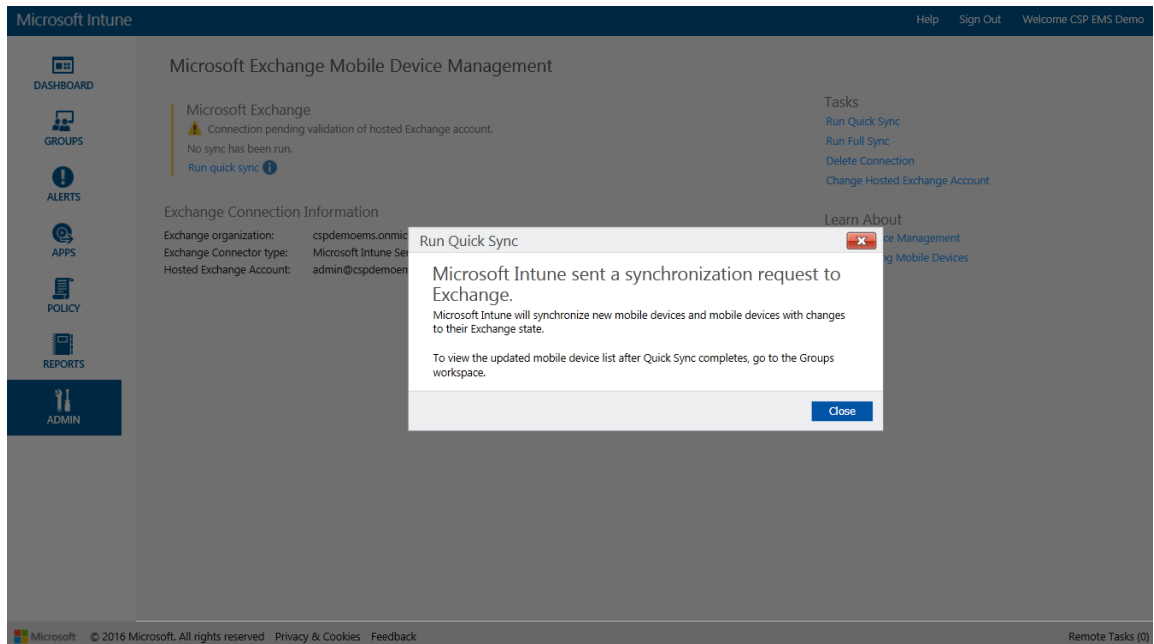
- Select **Set Up Service to Service Connector**.



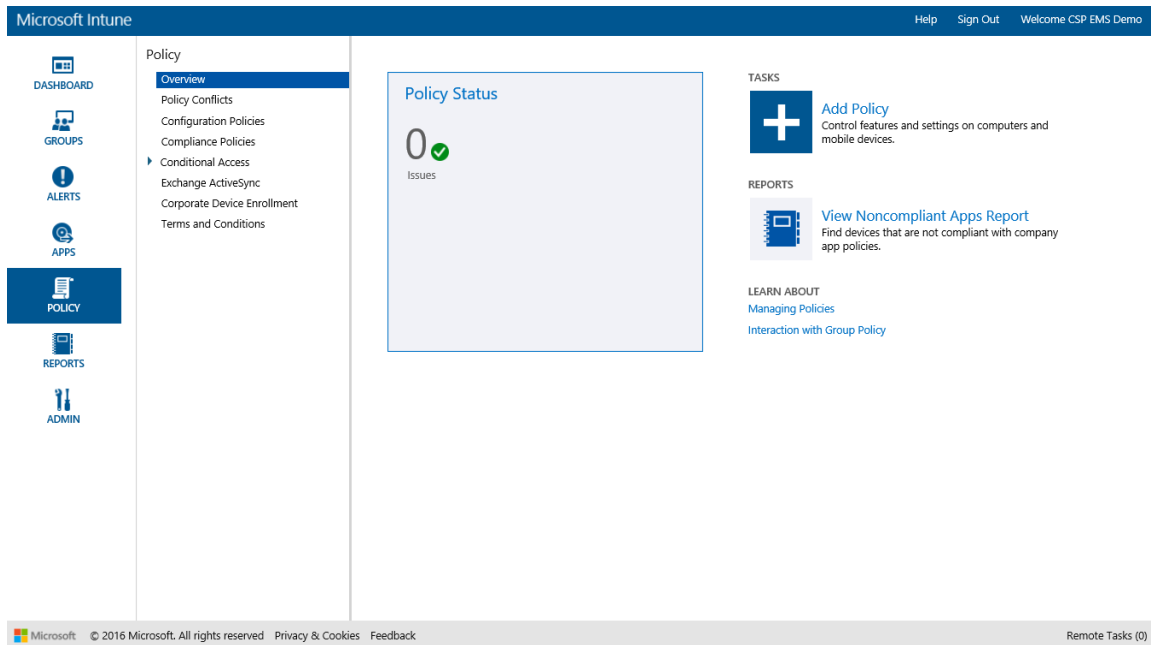
4. Select **OK** when prompted to use the signed-in Global Administrator account to configure the Service to Service Connector.



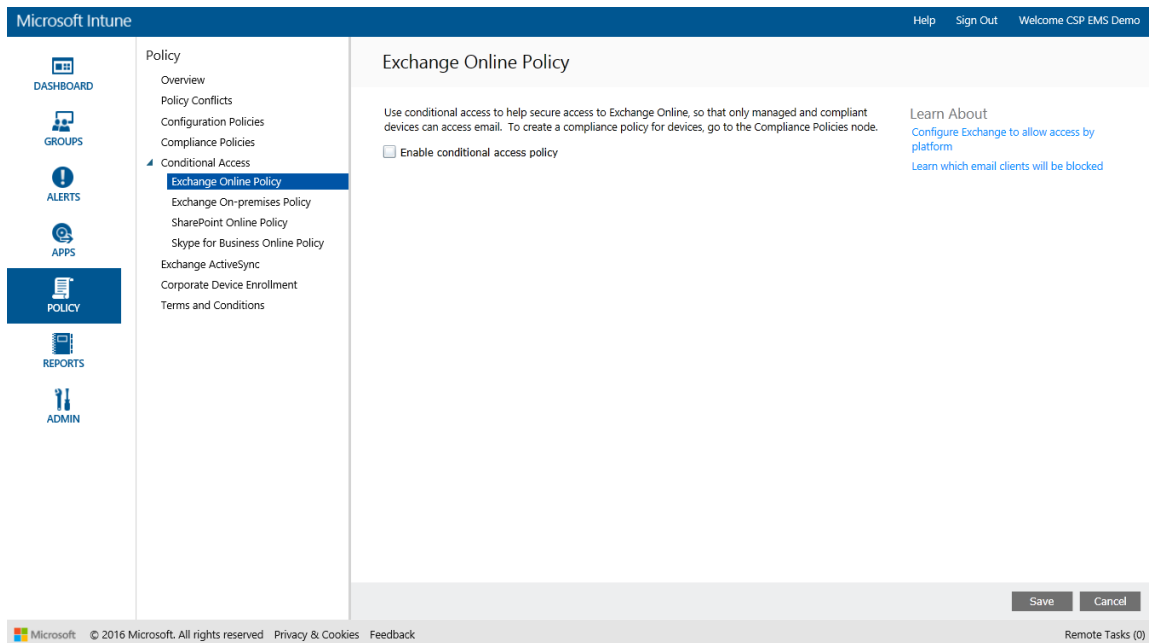
5. Select **Run quick sync**.



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**.

The screenshot shows the Microsoft Intune management console. The left-hand navigation pane includes links to Dashboard, Groups, Alerts, Apps, Policy (selected), Reports, and Admin. The 'Policy' section is expanded, showing 'Exchange Online Policy' as the selected item. The main content area is titled 'Exchange Online Policy' and contains the following sections:

- Introduction:** A paragraph explaining conditional access for Exchange Online, followed by links for 'Learn About', 'Configure Exchange to allow access by platform', and 'Learn which email clients will be blocked'.
- Enable conditional access policy:** A checkbox that is checked.
- Application access:**
  - Outlook and other apps that use modern authentication:** Includes checkboxes for 'iOS' and 'Android'.
  - Exchange ActiveSync apps that use basic authentication:** Includes checkboxes for 'Block non-compliant devices on platforms supported by Microsoft Intune' and 'Block all other devices on platforms not supported by Microsoft Intune'.
- Policy deployment:**
  - Targeted groups:** A section with the instruction 'Select the Active Directory security groups to target with this policy:'. It has two radio button options: 'All users' and 'Selected security groups' (which is selected).
  - A text box below the radio buttons contains 'None specified', and a 'Modify' button is to its right.

At the bottom right of the main content area are 'Save' and 'Cancel' buttons. The footer of the page includes the Microsoft logo, copyright information for 2016, and links for Privacy & Cookies and Feedback. On the far right of the footer, it says 'Remote Tasks (0)'.

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

**Exchange Online Policy**

Use conditional access to help secure access to Exchange Online, so that only managed and compliant devices can access email. To create a compliance policy for devices, go to the Compliance Policies node.

☒ Enable conditional access policy

**Application access**

Outlook and other apps that use modern authentication

☐ All platforms

☒ Specific platforms

☒ iOS

☒ Android

☒ Windows 10 Mobile

☒ Windows must meet the following requirements:

Devices must be domain joined or compliant

Exchange ActiveSync apps that use basic authentication

☒ Block non-compliant devices on platforms supported by Microsoft Intune

☐ Block all other devices on platforms not supported by Microsoft Intune

**Policy deployment**

Targeted groups

Select the Active Directory security groups to target with this policy:

☒ All users

☐ Selected security groups

Exempt groups

Select the Active Directory security groups to exempt from this policy (overrides members in the Targeted Groups list)

☒ No exempt users

☐ Selected security groups

Save Cancel

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.