Microsoft Intune Mobile Device Management compliance policies

Microsoft Intune compliance policies define the rules and settings that a device must comply with in order to be considered compliant by conditional access polices. Administrators can also use compliance policies to monitor and remediate compliance issues with devices independently of conditional access.

Compliance policies can remediate mobile device compliance for:

- PIN and passwords
- Encryption
- Whether the device is jailbroken (iOS) or rooted (Android), or if the device is reporting as unhealthy by the Windows device health attestation service
- Whether email on the device is managed by an Intune policy
- Minimum OS version required - This will depend on the end customer's company compliance policies and security requirements. This helps to prevent access to devices that might have security vulnerabilities because they are using an older OS version
- Maximum OS version allowed - Administrators may choose not to support the latest OS version available before testing or other reasons. Administrators can choose to block devices that have a version later than the one Administrators have specified. The device will not be able to access company resources until the policy is changed.

If no compliance policy is deployed to a device, then any applicable conditional access policy will treat the device as compliant.

Microsoft CSP Partners can leverage the table below to obtain the end customer's requirements and the settings needed to configure the compliance policy. As with Intune configuration policies, some of the settings below differ from platform to platform due to the features and settings available on each.

Compliance Policy setting	**Description**	**End Customer Setting**
Require a password to unlock mobile devices	Specified whether to require users to enter a password before access is granted to information on their mobile device	Yes/No
Allow simple passwords	Specifies whether to allow mobile devices to use simple password sequences, such as 1234 or 1111	Yes/No
Minimum password length is not configured	Specifies the minimum amount of digits or characters in the password	4 characters or more
Required password type	Specifies whether passwords are allowed to be comprised only of numeric characters, or whether they must contain characters other than characters	**Password Type:** Alphanumeric/Numeric **Minimum number of character types:** At least 1
Password quality	Sets the password requirement for Android devices	**Options:** Low security biometric Required At least numeric At least alphabetic At least alphanumeric Alphanumeric with symbols
Minutes of inactivity before password is required	Specifies the length of time without user input after which the mobile device screen is locked	1 minute 5 minutes 15 minutes 1 hour
Password expiration (days)	Specifies the length of time after which a mobile device password must be changed	Minimum 1 day Recommended 41 days
Remember password history	Specifies whether to restrict the reuse of previous passwords	Yes/No

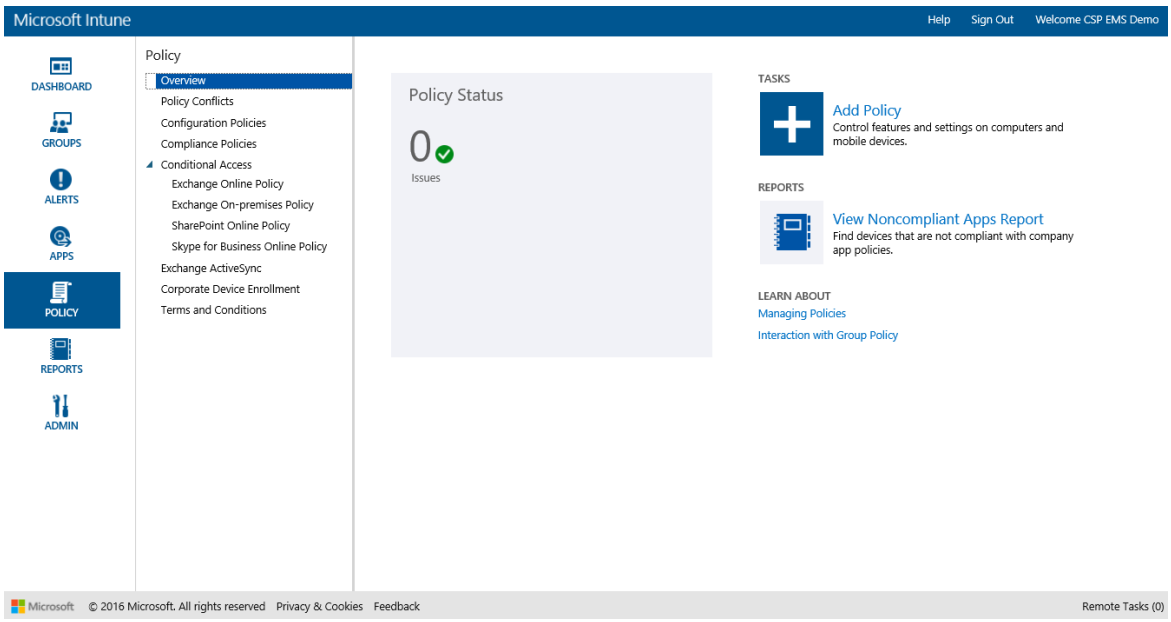
		Prevent reuse of previous passwords: Minimum of 1
Require a password to unlock an idle device	Force user to input password every time the device returns from an idle state Windows 10 mobile only	Yes/No
Require encryption on mobile device	This setting enables encryption on mobile devices, not all devices can enforce encryption.	Yes/No
Email account must be managed by Intune	A device will be considered noncompliant if Intune cannot deploy an email profile because one is already set up by the end user. Email profiles are not deployed by this compliance policy iOS 7.1 and later only	Yes/No **Select the email profile that must be managed by Intune:** Select the email profile deployed to iOS devices
Require devices to be reported as healthy	Windows 10 boot logs are remotely parsed and attested for health by the Windows Health Attestation Service (HAS). The following attributes are considered in the overall compliance state: Code integrity is enabled Bitlocker encryption is enabled Secure boot is enabled Early launch anti-malware driver is loaded (Windows 10 desktop only)	Yes/No
Device must not be jailbroken or rooted	Specifies whether to detect if the device is jailbroken or rooted	Yes/No

Minimum Windows Version	The operating system version, defined as major.minor.build, cannot be less than this version to enroll. The version number correspond to the version returned by the winver command	Yes/No Insert the version number required for this setting
Maximum Windows Version	The operating system version, defined as major.minor.build, cannot be greater than this version to enroll. The version number correspond to the version returned by the winver command	Yes/No Insert the version number required for this setting
Minimum Windows Phone or Windows 10 Mobile Version	The operating system version, defined as major.minor.build, cannot be less than this version to enroll. Windows Phone 8.1 and later only	Yes/No Insert the version number required for this setting
Maximum Windows Phone or Windows 10 Mobile Version	The operating system version, defined as major.minor.build, cannot be greater than this version to enroll. Windows Phone 8.1 and later only	Yes/No Insert the version number required for this setting
Minimum Android Version	The operating system version, defined as major.minor.build, cannot be less than this version to enroll. Android 4.0 or later or Samsung KNOX standard 4.0 and later only	Yes/No Insert the version number required for this setting
Maximum Android Version	The operating system version, defined as major.minor.build, cannot be greater than this version to enroll. Android 4.0 or later or Samsung KNOX standard 4.0 and later only	Yes/No Insert the version number required for this setting
Minimum iOS Version	The operating system version, defined as major.minor.build, cannot be less than this version to enroll.	Yes/No

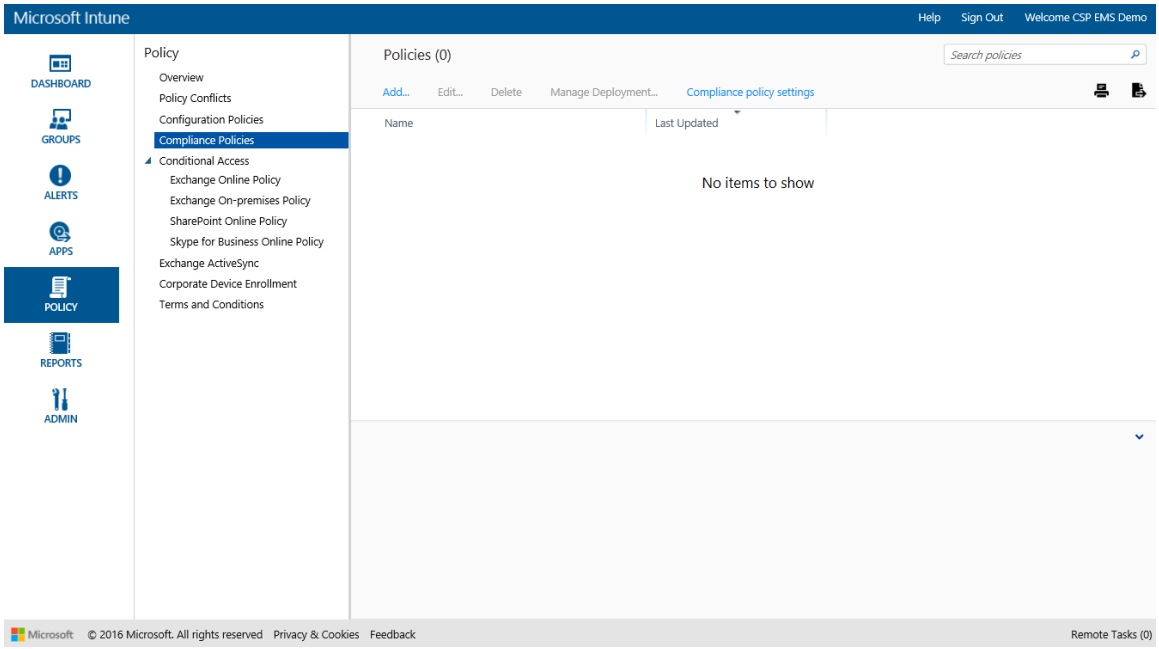
	iOS 7.1 and later only	Insert the version number required for this setting
Maximum iOS Version	The operating system version, defined as major.minor.build, cannot be greater than this version to enroll. iOS 7.1 and later only	Yes/No Insert the version number required for this setting

In the following **example**, a compliance policy will be created for the end customer

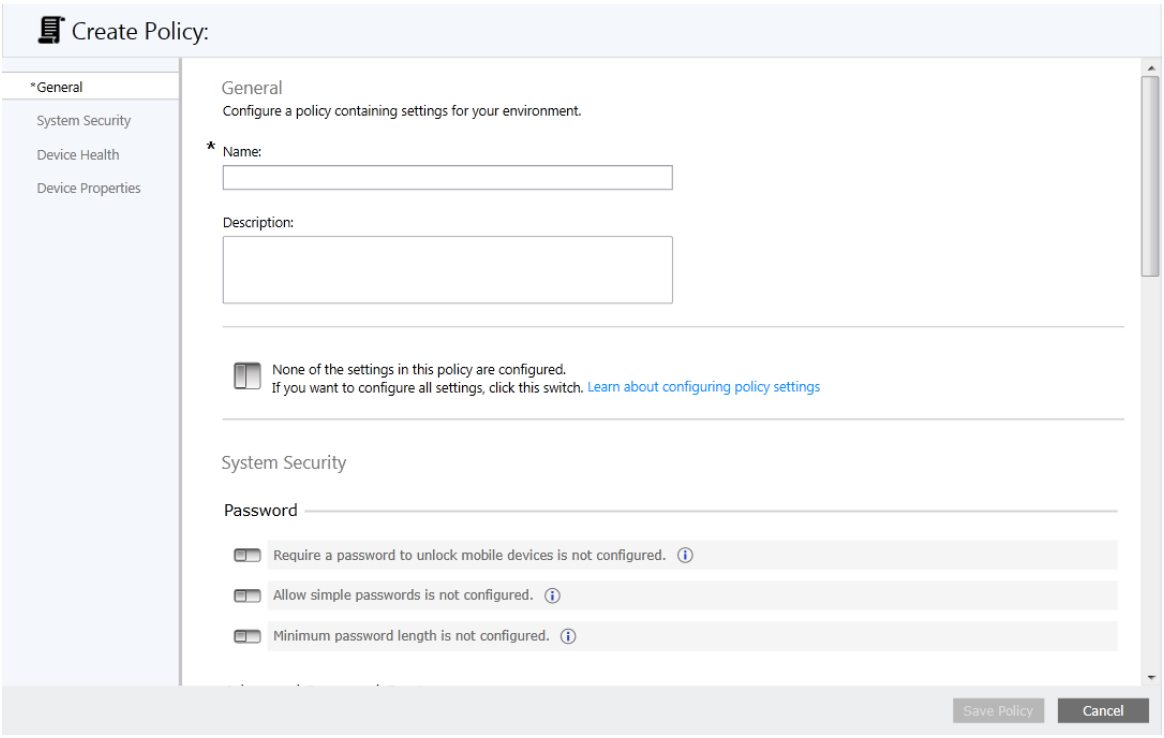
1. Login to the [Intune management portal] with the account with Office 365 Global Administrator privileges and select **Policy**.



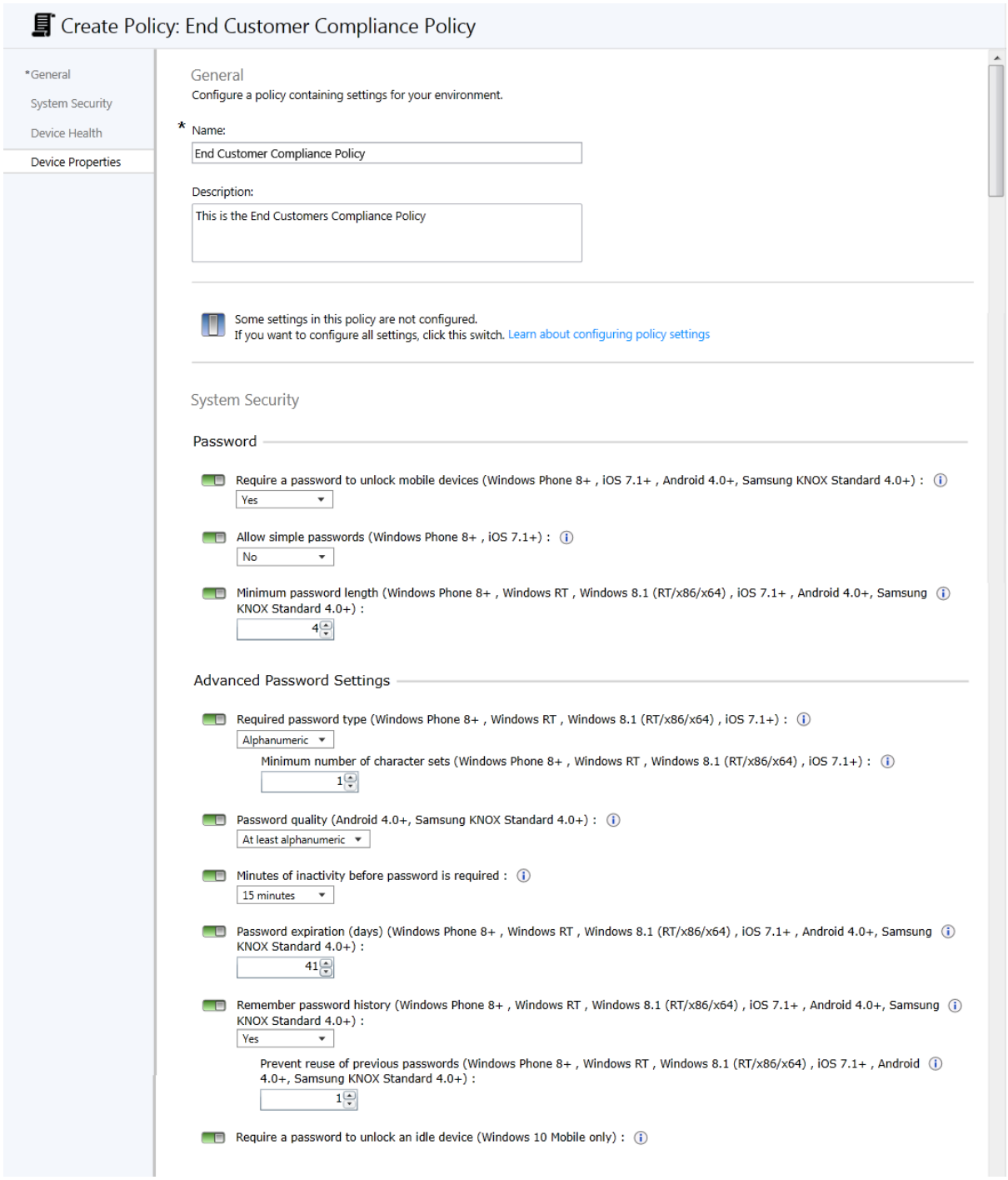
2. Select **Compliance Policies**

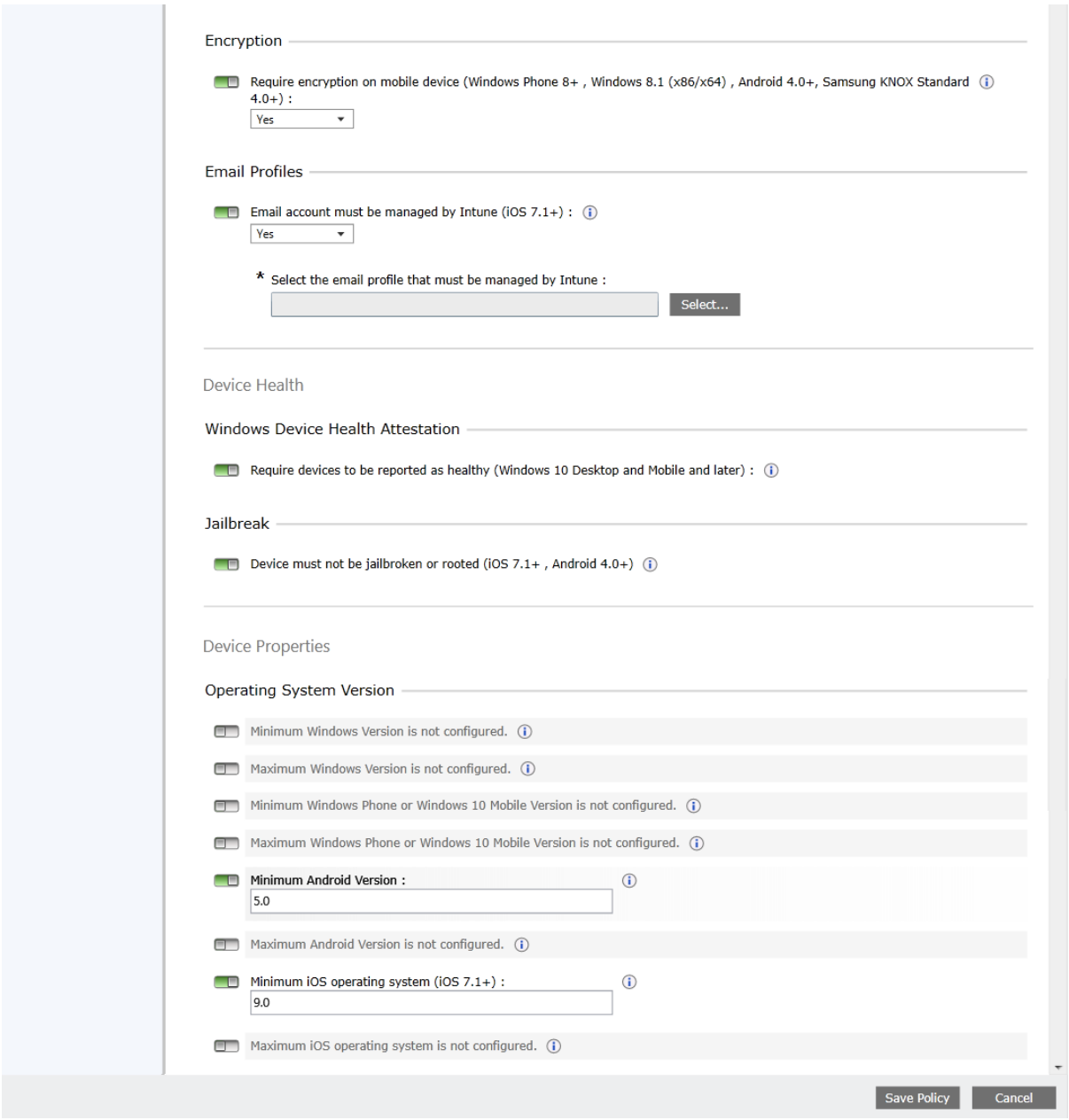


3. Select **Add...**

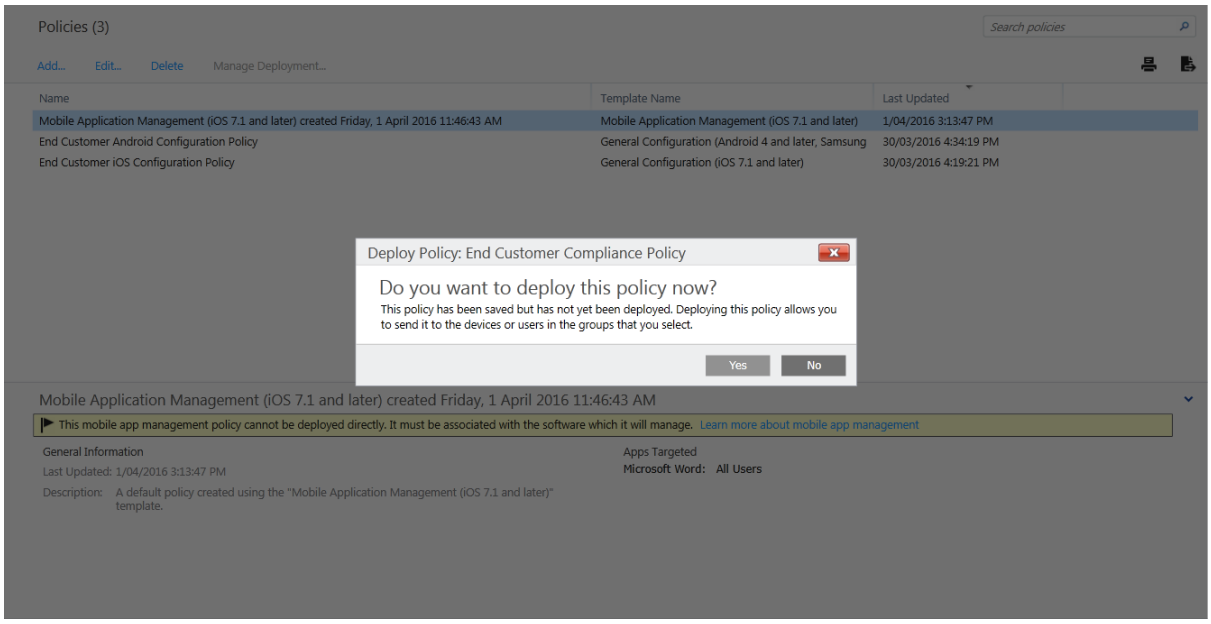


4. Enter the settings as agreed upon with the end customer, the image below shows **example** of these settings

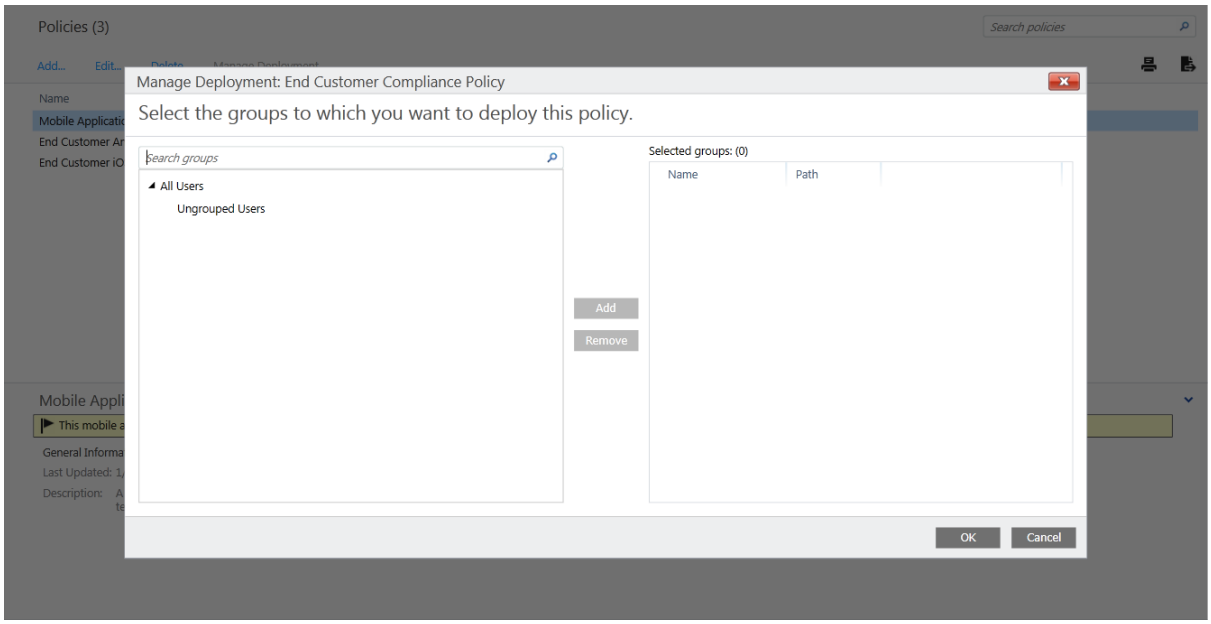

Create Policy: End Customer Compliance Policy
*General
System Security
Device Health
Device Properties
General
Configure a policy containing settings for your environment.
* Name:
End Customer Compliance Policy
Description:
This is the End Customers Compliance Policy
Some settings in this policy are not configured.
If you want to configure all settings, click this switch. Learn about configuring policy settings
System Security
Password
Require a password to unlock mobile devices (Windows Phone 8+ , iOS 7.1+ , Android 4.0+, Samsung KNOX Standard 4.0+) :
Yes
Allow simple passwords (Windows Phone 8+ , iOS 7.1+) :
No
Minimum password length (Windows Phone 8+ , Windows RT , Windows 8.1 (RT/x86/x64) , iOS 7.1+ , Android 4.0+, Samsung KNOX Standard 4.0+) :
4
Advanced Password Settings
Required password type (Windows Phone 8+ , Windows RT , Windows 8.1 (RT/x86/x64) , iOS 7.1+) :
Alphanumeric
Minimum number of character sets (Windows Phone 8+ , Windows RT , Windows 8.1 (RT/x86/x64) , iOS 7.1+) :
1
Password quality (Android 4.0+, Samsung KNOX Standard 4.0+) :
At least alphanumeric
Minutes of inactivity before password is required :
15 minutes
Password expiration (days) (Windows Phone 8+ , Windows RT , Windows 8.1 (RT/x86/x64) , iOS 7.1+ , Android 4.0+, Samsung KNOX Standard 4.0+) :
41
Remember password history (Windows Phone 8+ , Windows RT , Windows 8.1 (RT/x86/x64) , iOS 7.1+ , Android 4.0+, Samsung KNOX Standard 4.0+) :
Yes
Prevent reuse of previous passwords (Windows Phone 8+ , Windows RT , Windows 8.1 (RT/x86/x64) , iOS 7.1+ , Android 4.0+, Samsung KNOX Standard 4.0+) :
1
Require a password to unlock an idle device (Windows 10 Mobile only) :



5. Select **Save Policy**.

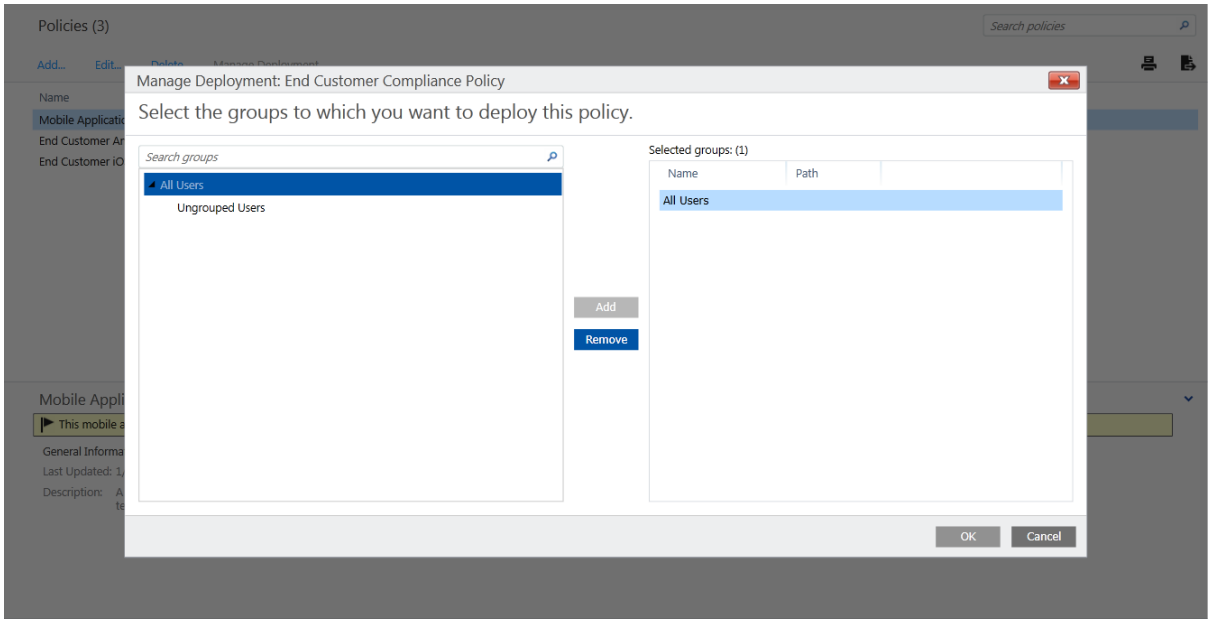


6. When prompted to deploy this policy, select **Yes**



7. Select **All Users** to assign this policy to all Intune users and then select **Add**. The compliance policy can also be deployed to a custom user or device group to cater for different policies required, e.g. for testing different policy configurations by the end customers administrators or deployment of different policies per organization

department.



8. Select **OK**. This policy will be displayed in the compliance policy pane.