Microsoft Intune Mobile Device Management configuration policies

Microsoft Intune policies are groups of settings that control the settings and features on mobile devices and computers. Administrators create the various policies available to them by either utilizing the preconfigured Intune templates, which let them manage many of the settings and features on the end customer's mobile devices, or by the creation of custom policies for when the template policies do not contain the settings required, and then deploy these to Intune user or device groups.

As well as Microsoft Intune polices, applications can also be deployed to Intune users or devices groups.

There are three Intune policy types that can be configured to meet the end customer's requirements:

- **Configuration policies**. These policies allow administrators to manage the settings and features on the mobile devices enrolled with the end customer's organization.
- **Compliance policies**. These policies define the rules and settings that a mobile device must comply with in order to be considered compliant by conditional access polices. Administrators can also use compliance policies to monitor and remediate compliant issues with devices independently of conditional access.
- **Conditional Access**. These policies help to secure access to the end customer's Exchange on-premises, as well as their online services. This helps to ensure that only managed devices that pass administrator defined compliance checks and rules can access these services.

There are a number of elements to the configuration and setup of the Microsoft Intune service that need to be agreed upon with the end customer.

The tables in the following sections cover the different policy types to help provide guidance when identifying which policies and settings will be required to meet the end customer's mobile device and application management requirements.

Mobile Application Management (MAM) policies can be configured and applied to both;

- devices that are enrolled into Intune mobile device management and
- devices that are not enrolled into Intune mobile device management.

Both of these managed and unmanaged device scenarios are covered in the MAM IT Pro steps.

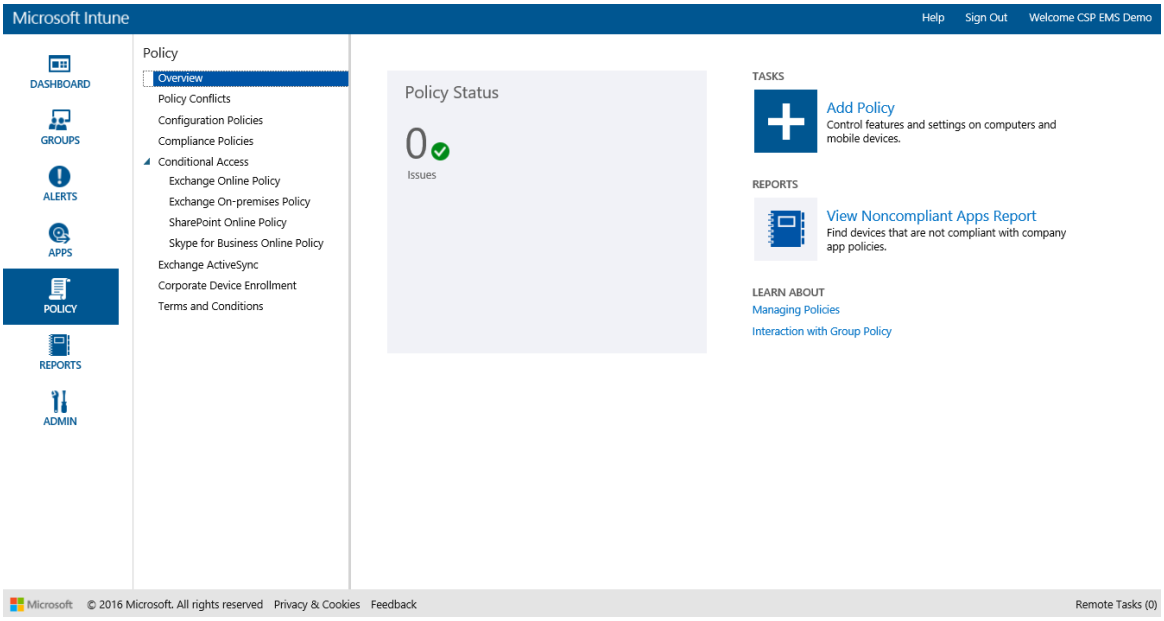
The table below can help obtain the end customer's requirements and the settings needed to configure the security section of the policy **General Configuration (iOS 7.1 and later)** for management of iOS mobile devices. As with Intune configuration policies, some of the settings below differ from platform to platform due to the features and settings available on each.

Configuration Policy setting	**Description**	**End Customer Setting**
Require a password to unlock mobile devices	Specifies whether to require users to enter a password before access is granted to information on their mobile device	Enabled/Disabled Yes/No
Required password type	Specifies whether passwords are allowed to be comprised only of numeric characters, or whether they must contain characters other than numbers	Enabled/Disabled Alphanumeric/Numeric
Number of complex characters required in password	Select the number of complex (non-alphanumeric) characters like #,%,!, etc. that the password must contain	Enabled/Disabled 0 characters or more
Minimum password length	Specifies the minimum number of digits or characters in the password	Enabled/Disabled 4 characters or more
Allow simple passwords	Specifies whether to allow mobile devices to use simple password sequences, such as 1234 or 1111	Enabled/Disabled Yes/No

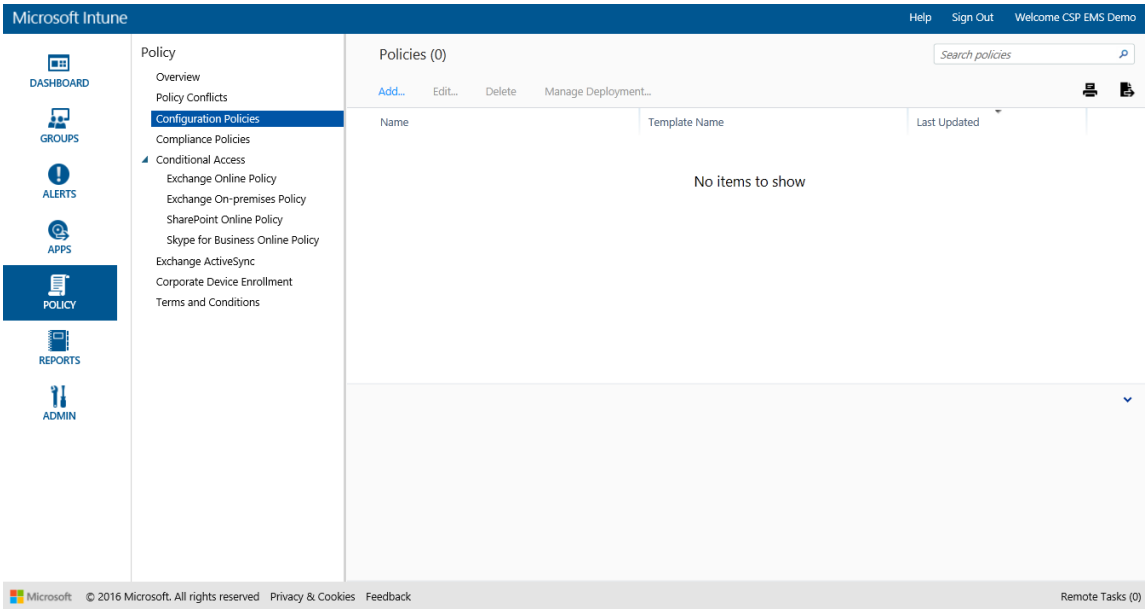
Number of repeated sign-in failures to allow before the device is wiped	Specifies the number of consecutive times an incorrect password can be entered before the mobile device is wiped of all data	Enabled/Disabled At least 4 or more password failures
Minutes of inactivity before password is required	Minutes of inactivity before the password is required	Enabled/Disabled 1 minute 5 minutes 15 minutes 1 Hour
Password expiration (days)	Specifies the length of time after which the mobile device password must be changes	Enabled/Disabled Minimum 1 day Recommended 41 days
Remember password history	Specifies the number of previous passwords that cannot be reused by the user	Enabled/Disabled Yes/No Prevent reuse of previous passwords: Minimum of 1 previous password, recommendation is 5
Minutes of inactivity before screen turns off	Specifies the length of time without user input after which the mobile device screen is locked	Enabled/Disabled 1 minute 5 minutes 15 minutes 30 minutes 1 Hour
Allow fingerprint unlock	Allow a fingerprint to unlock a device	Enabled/Disabled Yes/No

In the following **example**, a Microsoft Intune configuration policy is created for **iOS** devices, implementing the password security settings as agreed upon with the end customer.

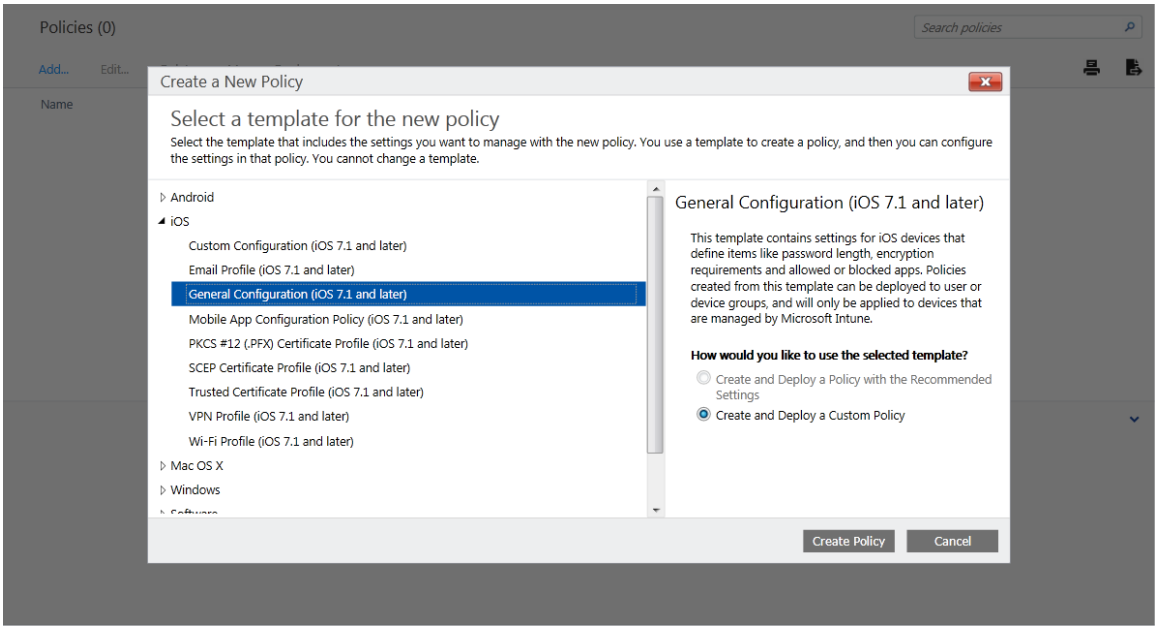
1. Login to the [Intune management portal] with an account with Office 365 Global Administrator privileges, and select **Policy**.



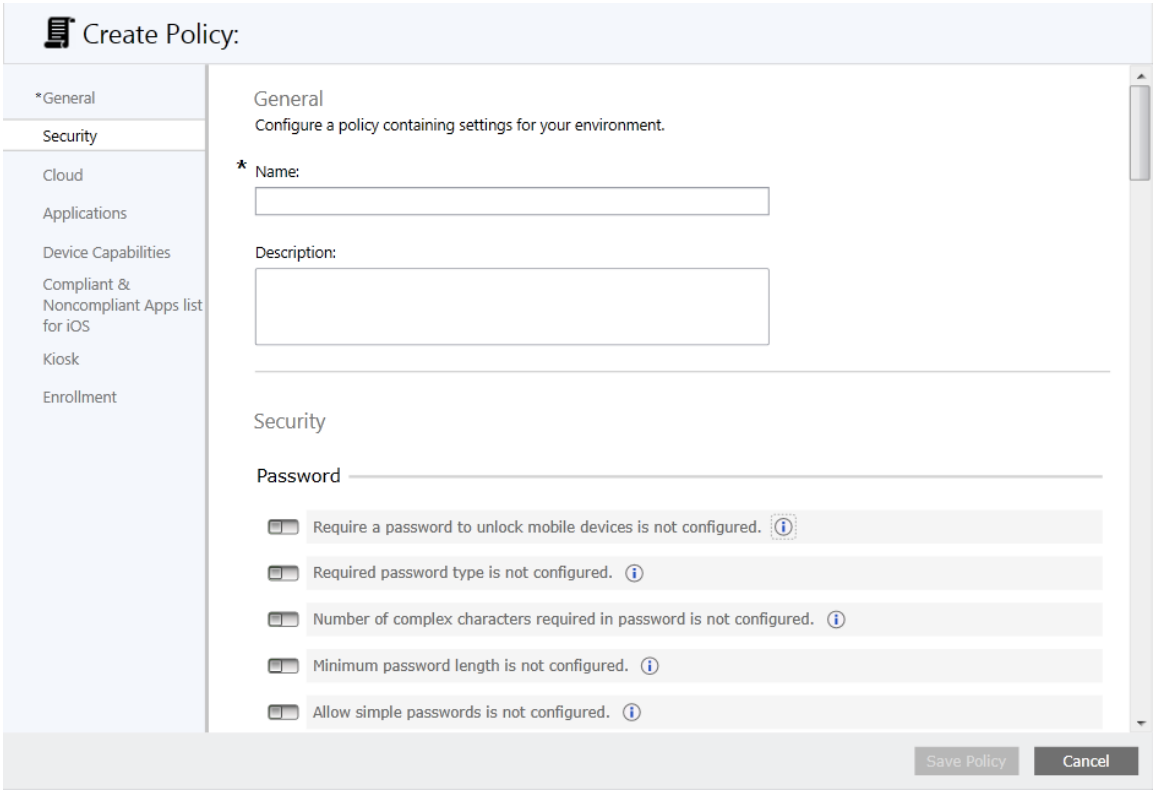
2. Select **Configuration Policies**



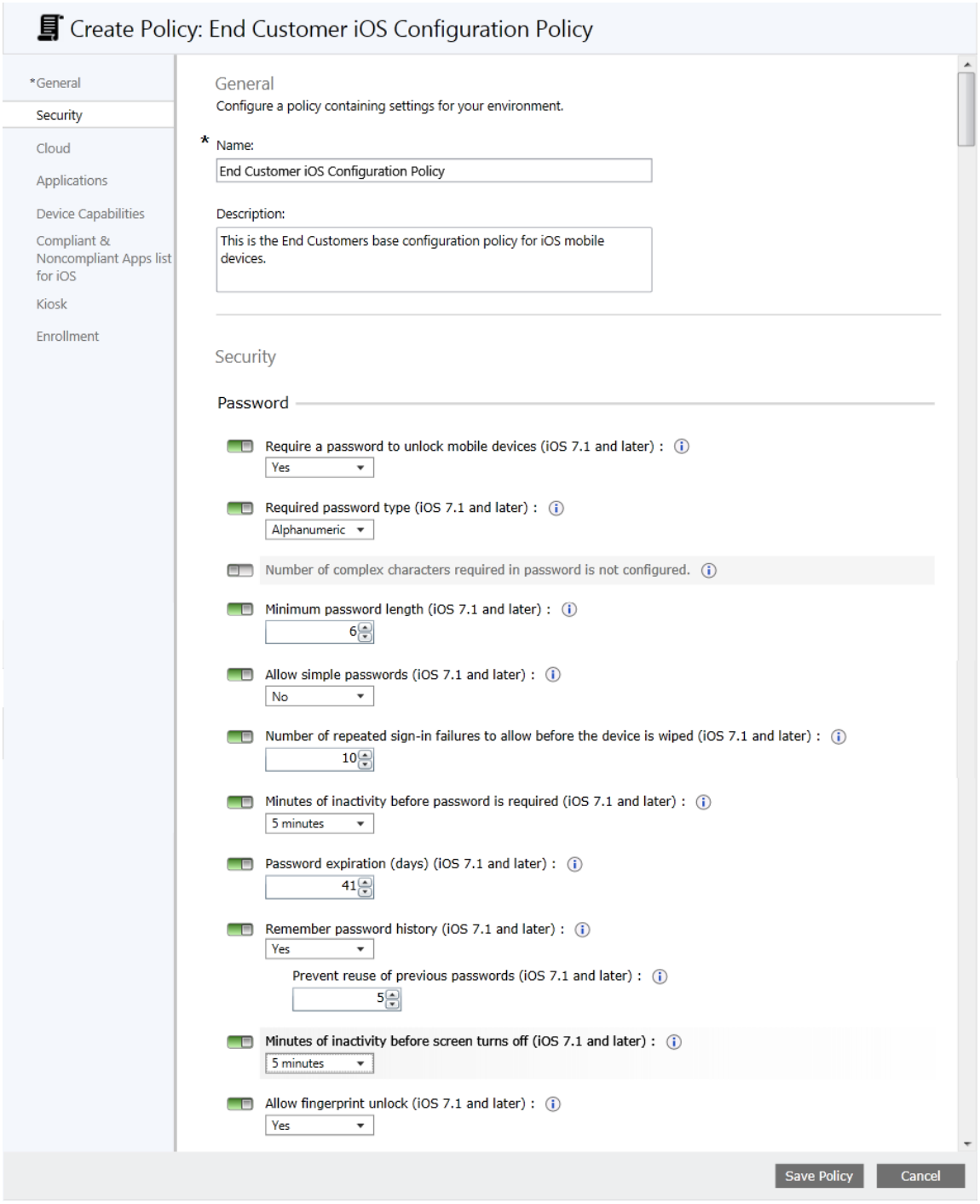
3. Select **Add...**. Expand **iOS** and then select **General Configuration (iOS 7.1 and later)**.



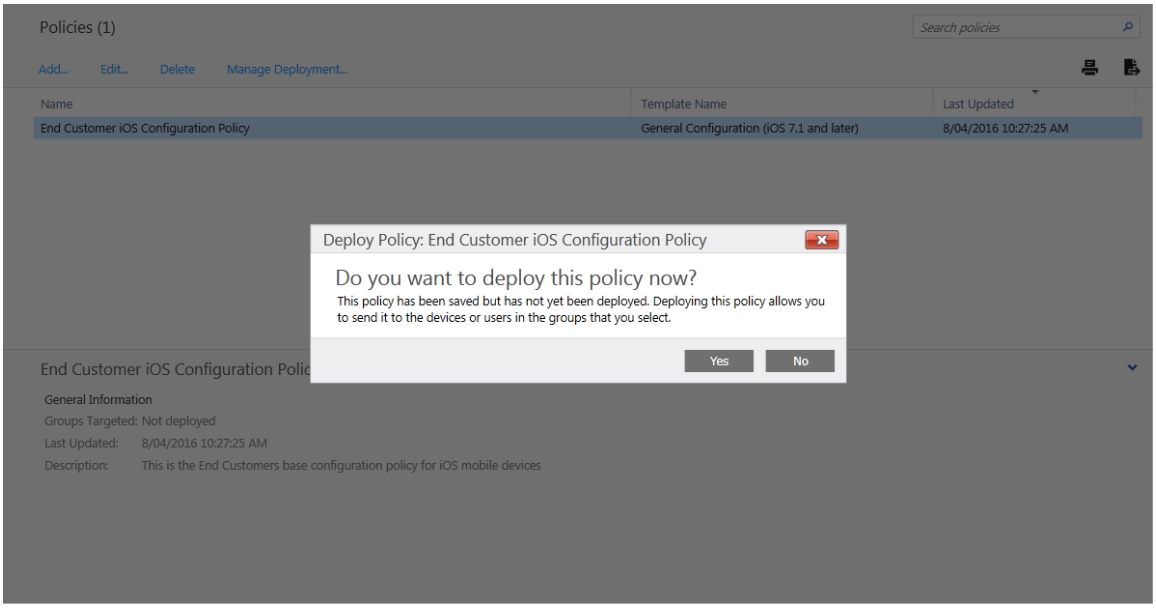
4. Select **Create Policy**.



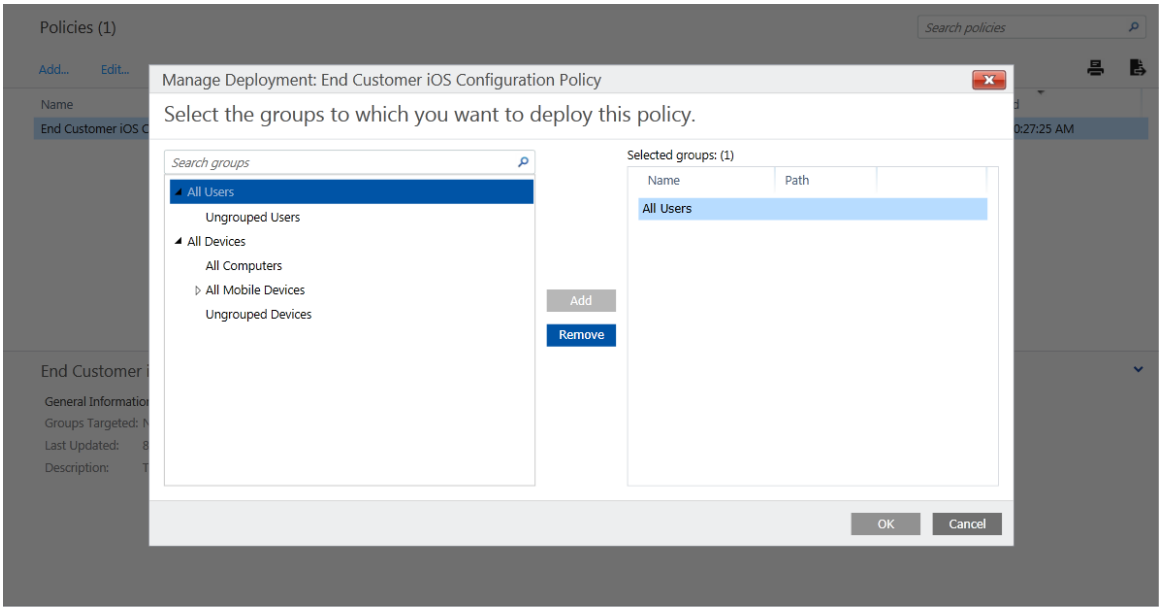
5. In this **example**, the settings are configured as agreed upon with the end customer.



6. Select **Save Policy**, then **Yes** to deploy to policy.



7. Select **All Users** and then **Add**



This completes the creation and deployment of an Intune configuration policy, setting up the password policy required for iOS devices when being enrolled into the organization's mobile device management. This policy has been deployed to **All Users** but will only apply to an iOS device at enrollment time.