Security Compliance settings required for BYOD Devices

The following lists all the minimum required compliance settings for each BYOD device type.

Personal devices must be marked as Compliant in Microsoft Intune so that personal devices can be used to access University Data.

Non Compliance

Devices will be marked as Non-compliant in Microsoft Intune should they fall below the security compliance requirements below. Once a device is marked as Non-compliant the following process will occur:

- Device will be given 14 days grace period
- An email notification will be sent to the owner of the device informing them of non-compliance
- After 14 days of non-compliance – device will be retired from Intune and will require registering/enrolling again to access university data.

Mobile device Security Compliance Settings

Android

Current Min supported Android Version

Version 10

Check and update your Android version - Android Help (google.com)

The following compliance settings are currently configured:

System Security	
Block apps from unknown sources	Block
Company Portal app runtime integrity	Require
Block USB debugging on device	Block
Require a password to unlock mobile devices	Require
Maximum minutes of inactivity before password is required	15 minutes
Password complexity	High
Required password type	At least numeric
Minimum password length	6

Settings which only apply to Android 11 and earlier

Require Password Type - At Least Numeric

Minimum password length - 6

Settings which only apply to Android 12 and later

Password complexity **- High (**PIN with repeating (4444) or ordered (1234, 4321, 2468) sequences are blocked. The length must be at least 8 characters. The alphabetic or alphanumeric length must be at least 6 characters.)

Please note the following Microsoft statement

On personally owned devices, there are two passwords affected by this **Password complexity** setting:

- The device password that unlocks the device
- The work profile password that allows users to access the work profile

If the device password complexity is too low, then the device password is automatically changed to require a **High** complexity. The end users must update the device password to meet the complexity requirements. Then, they sign into the work profile and are prompted to update the work profile complexity configured in the **Password complexity** setting in your policy.

For further information:

Android Enterprise compliance settings in Microsoft Intune | Microsoft Learn

iOS

Current Min supported iOS Version

Version 15

Check the following links to see if your devices supports the latest iOS

iPad models compatible with iPadOS 16 – Apple Support (UK)

iPhone models compatible with iOS 16 – Apple Support (UK)

The following compliance settings are currently configured:

System Security	
Require a password to unlock mobile devices	Require
Minimum password length	6
Maximum minutes after screen lock before password is required	Immediately
Maximum minutes of inactivity until screen locks	15 minutes

iOS/iPadOS device compliance settings in Microsoft Intune | Microsoft Learn

> ⓘ Note
>
> After a compliance or configuration policy is applied to an iOS/iPadOS device, users are prompted to set a passcode every 15 minutes. Users are continually prompted until a passcode is set. When a passcode is set for the iOS/iPadOS device, the encryption process automatically starts. The device remains encrypted until the passcode is disabled.

Biometrics

The use of Biometrics is supported as part of BYOD on all devices where it is supported by the Manufacturer

Using biometrics - NCSC.GOV.UK

Use Touch ID on iPhone and iPad – Apple Support (UK)

Use Face ID on your iPhone or iPad Pro – Apple Support (UK)

Biometrics | Android Open Source Project

MacOS/Windows Security Compliance Settings

Windows

Devices must be running a supported Operating System

Supported versions of Windows client | Microsoft Learn

Lifecycle FAQ - Windows | Microsoft Learn

Use the following to check your version

Which version of Windows operating system am I running? - Microsoft Support

The following compliance settings are currently configured:

System Security	
Require a password to unlock mobile devices	Require
Simple passwords	Block
Minimum password length	6
Maximum minutes of inactivity before password is required	15 minutes
Password expiration (days)	730
Firewall	Require
Antivirus	Require
Antispyware	Require

Please note the following Microsoft statement

> **ⓘ Important**
>
> When the password requirement is changed on a Windows desktop, users are impacted the next time they sign in, as that's when the device goes from idle to active. Users with passwords that meet the requirement are still prompted to change their passwords.

For further information: [Windows compliance settings in Microsoft Intune | Microsoft Learn]

MacOS

The following compliance settings are currently configured:

System Security	
Require a password to unlock devices.	Require
Simple passwords	Block
Minimum password length	6
Maximum minutes of inactivity before password is required	15 minutes
Password expiration (days)	730
Number of previous passwords to prevent reuse	5
Firewall	Enable

Please note the following Microsoft statement

> **ⓘ Important**
>
> When the password requirement is changed on a macOS device, it doesn't take effect until the next time the user changes their password. For example, if you set the password length restriction to eight digits, and the macOS device currently has a six digits password, then the device remains compliant until the next time the user updates their password on the device.

For further information: [macOS device compliance settings in Microsoft Intune | Microsoft Learn]