accenture NHS

NHSmail Intune Service

Session 8: iOS/iPadOS Deep Dive

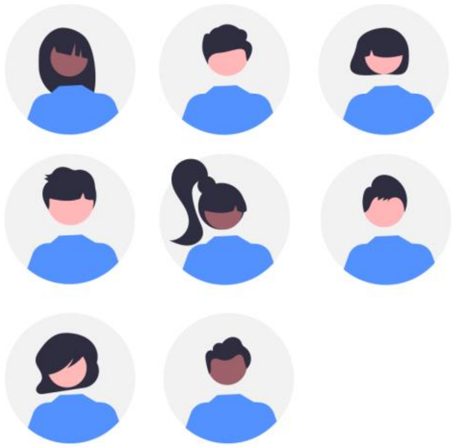
13th January 2022

Upskilling Series | Housekeeping

Event name:	Session 8: iOS/iPadOS Deep Dive
Date:	13 January 2022
Location:	Online Webinar
Start / end time:	15:00 – 16:00
Attendees:	NHSmail Intune Team and LAs from January onboarding organisations
Objectives & purpose:	To provide details specific to iOS/iPadOS device enrolment and management on NHSmail Intune and outline key iOS/iPadOS features on NHSmail Intune.
End goal:	Organisations onboarding in January feel more informed about how to enrol and manage iOS/iPadOS devices on NHSmail Intune and have the opportunity to ask any iOS/iPadOS-specific questions.

Housekeeping

- As this is a webinar, all attendees, other than the presenters will be on mute during the event.
- There will be a question and answer section at the end of the session, time permitting. If you wish to ask a question during this section, please raise your hand and you will be taken off mute.
- Any questions submitted in the chat which we don't have time to answer in the session will be answered via follow-up email after the session where appropriate.
- Information outlined in red indicates key information.



Agenda

Session 8: iOS/iPadOS Deep-Dive

01 Overview & Objectives

02 Device & Software Requirements

03 Apple Business Manager (ABM) Link

04 Device Enrolment

05 Configuration Profiles

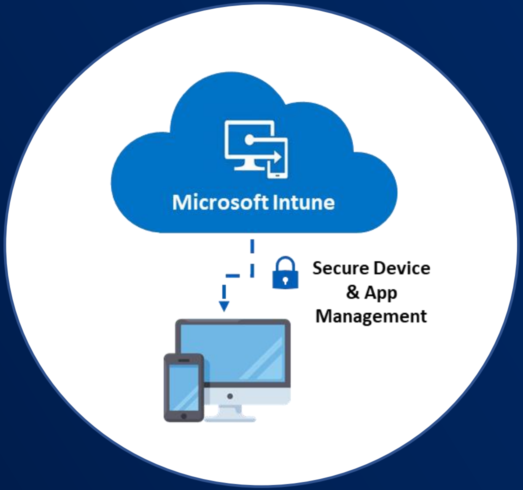
06 Compliance Policies

07 Application Management

08 Wiping and Removing an iOS/iPadOS device

09 Questions and Close

Session 8



iOS/iPadOS Deep-Dive

Overview & Objectives

Overview

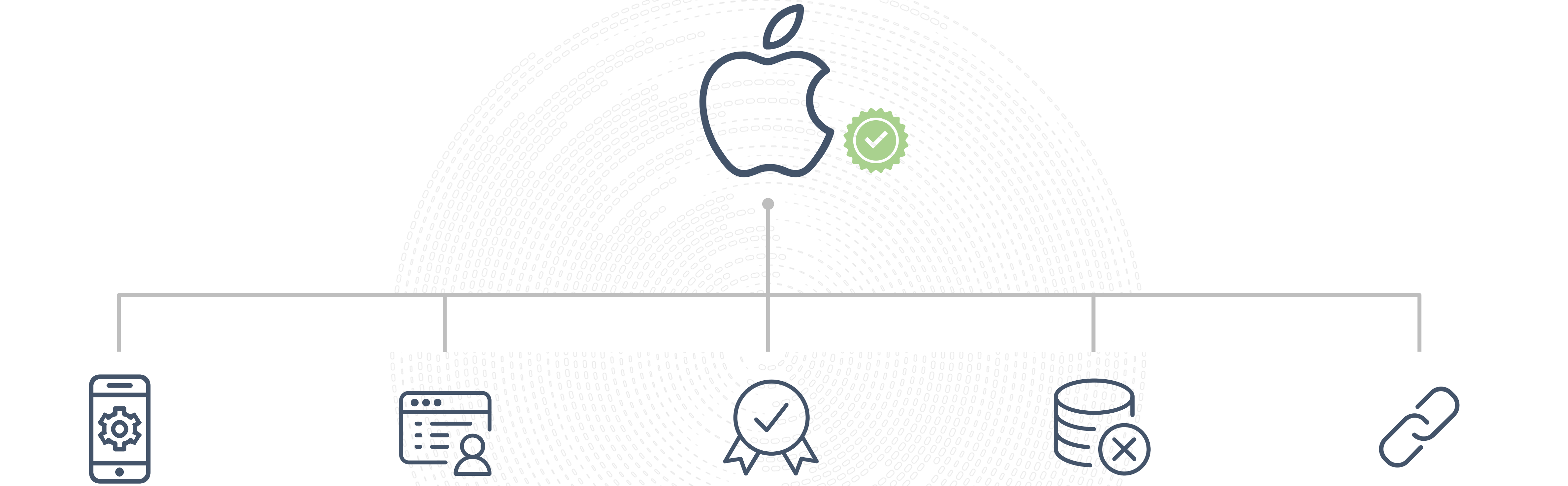
- As a result of organisations having the opportunity to purchase EMS E3 and AADP2 licenses, Intune for Mobile Device Management (MDM) capabilities have been enabled, in a way that supports the shared NHSmail tenant multi-organisation model.
- The NHSmail Intune Service is a supported live service with the onboarding of organisations proceeding in a phased manner.
- An upskilling series will be running each month to provide onboarding organisations with the knowledge to be able to begin rolling out NHSmail Intune across their device estates.
- Session 8 will look in more detail at the specifics of enrolling and managing iOS/iPadOS devices on NHSmail Intune including the ABM link and deploying iOS applications to devices.

Objectives

- Inform organisations on the device enrolment process for iOS/iPadOS devices.
- Provide details on iOS/iPadOS management and features.
- Explain Apple Business Manager and it's role in enrolling and managing iOS/iPadOS devices.
- Answer any questions specific to Apple device enrolment and management.

iOS Deep Dive | Device and Software Reqs.

Key requirements to check prior to enrolling any iOS/iPadOS devices onto NHSmail Intune, in order to ensure a successful enrolment



Apple iOS must run Apple iOS 13.0 or later.

Apple iPads must run iPadOS 13.0 or later.

All LAs and end users who will be using an iOS/iPadOS Intune-enrolled device need to have an nhs.net account.

EMS E3 and AADP2 licences have been assigned to each LA / end user with a single-user device.

Unenroll devices from any existing device management platforms.

Note: Device estates can be split between different MDMs. Single device must only be managed by one.

iOS/iPadOS devices to be enrolled to NHSmail Intune need to be exist in an organisation's ABM instance.

Organisations will be required to link their ABM into NHSmail Intune.

iOS Deep Dive | Apple Business Manager (ABM)

Apple Business Manager (ABM) is a key part of enrolling and managing iOS/iPadOS devices on NHSmail Intune. ABM is relevant only to iOS/iPadOS devices

WHAT IS THE APPLE BUSINESS MANAGER (ABM)?

- Apple Business Manager (ABM) is the Apple portal that enables organisations to simplify and automate the bulk management and deployment of corporate-owned Apple devices, including iOS and iPadOS.
- ABM provides a tight integration with NHSmail Intune to allow secure and simplified user enrolment of devices.

WHY IS ABM IMPORTANT TO IOS DEVICE MANAGEMENT ON NHSMAIL INTUNE?

- Organisations are unable to successfully enrol iOS/iPadOS devices to NHSmail Intune if their ABM instance is not linked into NHSmail Intune.
- LAs will manage and assign applications pushed to iOS/iPadOS devices through the ABM Portal.

WHO MANAGES AN ORGANISATION'S ABM INSTANCE?

- It is the responsibility of an organisation to manage their own ABM tenant, including when linked to NHSmail Intune.
- The NHSmail Intune Live Service Team offer a session to support organisations to link their ABM into NHSmail Intune but can not support with the general management of an organisation's ABM instance. If support with ABM management is required, LAs should contact Apple directly.

WHAT IS THE APPLE MDM PUSH CERTIFICATE?

- The Apple MDM Push Certificate establishes a trusted connection between Intune and iOS /iPadOS devices within a domain. It is a prerequisite to successfully enrolling and managing iOS/iPadOS devices on NHSmail Intune.
- The Apple MDM push certificate is managed centrally. LAs do not need to configure this or renew it.

iOS Deep Dive | ABM Prerequisites

Key prerequisites and requirements organisations will need to fulfil before linking their ABM to NHSmail Intune

The ABM link to NHSmail Intune will need to be completed successfully before organisations can begin enrolling iOS/iPadOS devices. LAs should ensure that the following prerequisites and requirements have been met to make the link as simple and easy as possible. Full details can be found in the NHSmail Intune Terms of Reference.

If organisations are struggling to complete any of these prerequisites, the NHSmail Intune Live Service Team can provide support during an ABM link session, however please be aware that the team may not be able to complete the ABM link successfully over the course of one call if there are outstanding prerequisites which require support to fulfil.

Enrolment

□ To enrol iOS/iPadOS, devices need to exist in an Apple Business Manager (ABM) instance already.

Apple ID

□ When connecting your organisation's ABM into NHSmail Intune, the Apple ID used to connect into Intune should have either the **Administrator role** or the **Device Enrolment Manager (DEM) role assigned** to it in ABM.

Connection

□ Organisations will be required to associate their vendor management portals with Intune (e.g., connect ABM with NHSmail Intune) prior to beginning to enrol iOS/iPadOS devices onto the platform.

Locations

□ **Locations** will need to be set up within ABM and domain verification setup - including the acceptance of terms and conditions - should have been completed.

Ownership

□ Organisation **ownership and management** of ABM for iPads and iPhones is to be maintained, including Apple IDs.

Please note: The NHSmail Intune platform is not supporting the management of any Apple devices which are not enrolled into ABM.

iOS Deep Dive | Schedule ABM Link Session

All organisations wishing to onboard iOS devices onto NHSmail Intune **will** need to connect their ABM instance to NHSmail Intune

We strongly recommend organisations request an ABM link session so the Intune Live Service Team can support with the connection and ensure it is completed correctly, however organisations who feel they have the expertise to do this independently can follow the full steps in the Operations Guide for Local Administrators and Onboarding Managers.

1

Organisations wishing to onboard their **Apple Business Manager (ABM)** with support from the Intune Live Service Team will need to raise a service request: *Request to onboard your organisation's Apple Business Manager (ABM) for Apple Devices.*

Service Requests

- Request an update to the Windows 10 baselines (centrally managed)
- Windows 10 BitLocker Recovery key
- Request an Android enrolment profile (Shared Device)
- Request a new Microsoft store application
- Request to offboard an organisation from NHSmail Intune
- ✓ Request to onboard your organisation's Apple Business Manager (ABM) for Apple Devices
- Other

2

Form Description:
ABM Link Service Request Form

Fields to complete:

Request Type: *

Description: *

Attachments: *

Requestor Details: *

Requested for: *

ODS code: *

Location: *

3

An ABM Link Session (**usually 30 minutes long**) will be held with the NHSmail Intune Live Service Team in order to support the organisation to complete the ABM link.

At a high-level, the ABM link session will achieve the following:

1. Obtain Apple Device Enrolment (ADE) Token
2. Connect VPP Token to NHSmail Intune
3. Assign a Company Portal licence

4

ABM Link complete

iOS Deep Dive | ABM Management

Organisations are responsible in managing their ABM, including once it has been linked to NHSmail Intune

In order to ensure continuity of service from NHSmail Intune for iOS/iPadOS devices, LAs will need to manage their ABM instance, including once it has been linked to NHSmail Intune.

The following considerations will need to be borne in mind:

RENEWING THE ABM TOKEN

- ABM tokens expire every 365 days.
- This token will need to be renewed and this is the responsibility of organisations.
- If this token is not renewed, LAs cannot maintain the management of devices.
- Full details on how to renew this token can be found in the Operations Guide for Local Administrators and Onboarding Managers.

ADDING A NEW LOCATION

- LAs can add a new location on ABM through the locations tab.
- LAs should enter the location name *(<ODS>-VPP-Token)* and *address* when creating a new location.

RENEWING THE VPP TOKEN

- Volume Purchase Program (VPP) tokens expire every 365 days.
- This token will need to be renewed and this is the responsibility of organisations.
- If this token is not renewed, LAs cannot maintain the management of devices.
- Full details on how to renew this token can be found in the Operations Guide for Local Administrators and Onboarding Managers. .

iOS Deep Dive | Device Enrolment

iOS/iPadOS devices can be enrolled for single users and iPadOS devices can be enrolled as shared devices. The enrolment processes for single and shared devices differ slightly

Below is a high-level overview of the steps required to enrol either a single-user iOS/iPadOS device or shared iPadOS device onto NHSmail Intune. Full steps are included in the Operations Guide for Local Administrators and Onboarding Managers and we will be going through these enrolment steps in more detail during Session 14.

Single User iOS/iPadOS Device Enrolment

1

Create User Enrolment Profiles

User enrolment profiles define the experience and settings applied to a group of devices during the enrolment phase.

Create a User Enrolment profile in Intune once the ABM instance is connected to the Intune portal.

2

Enrol iOS/iPadOS devices using User Affinity

User Affinity allows mapping of an Intune device to a single user.
In the Intune portal, proceed with the 'User Affinity' option for the enrolment profile created and then configure the Apple Setup Assistant.
Once this is done, you add the device to the ABM tenant and this should sync in the Intune Portal.

Shared iPadOS Device Enrolment

1

Create User Enrolment Profiles

To enrol a iOS/iPadOS shared device, there is a separate enrolment profile for shared devices.

If an LA wants to set up a shared device, they will need to apply the shared device enrolment profile to that group.

Ensure you add the correct naming standards:
<ODS>-SharedDevice-{{DEVICETYPE}}-{{SERIAL}}

2

Enrol iOS/iPadOS devices without User Affinity

In the Intune Portal, proceed with the 'without User Affinity' option for the enrolment profile created and then configure the Apple Setup Assistant.

Once this is done, you add the device to the ABM tenant and this should sync in the Intune Portal.

iOS Deep Dive | Device Enrolment

To enrol iOS/iPadOS devices onto NHSmail Intune Service, LAs are required to create and configure enrolment profiles for single user and shared devices

USER ENROLMENT PROFILES

To enrol iOS/ iPadOS devices, LAs need to create a user enrolment profile for Apple Device Enrolment (ADE) devices once the ADE token has been installed via ABM.

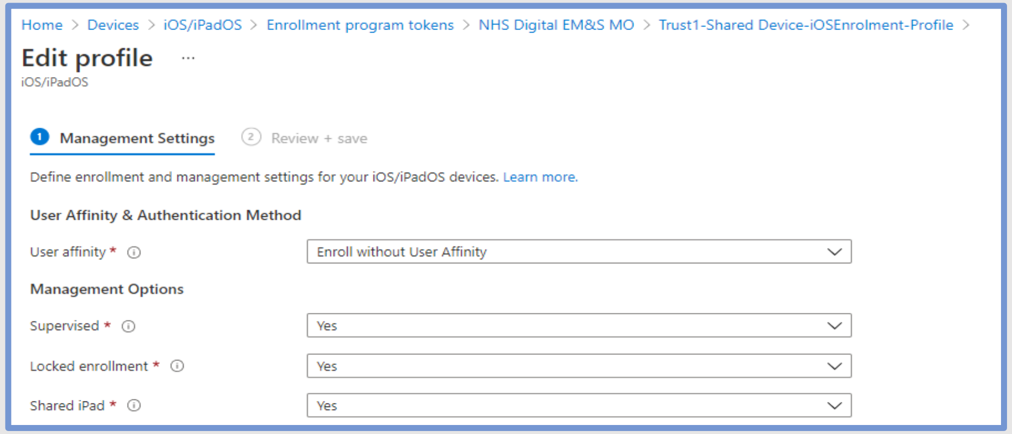
What are User Enrolment Profiles?

- User enrolment profiles define the experience and settings applied to a group of devices during the enrolment phase.
- Each new enrolment profile will require an AAD Dynamic group to be created, in order to pull devices into their relevant groups. This is required to ensure devices can be managed within the Intune Portal.
- When entering a new profile name please follow the correct naming standard: Trust ODS Code - Device Type Enrolment Profile.

How do LAs create dynamic Groups?

- LAs are unable to create or amend dynamic groups via the Security Group Management Application.
- If a dynamic group needs to be created or amended, LAs will need to raise a service request via Helpdesk Self-Service.

USER AFFINITY OPTIONS



Home > Devices > iOS/iPadOS > Enrollment program tokens > NHS Digital EM&S MO > Trust1-Shared Device-iOSEnrolment-Profile >

Edit profile ...

iOS/iPadOS

1 Management Settings   2 Review + save

Define enrollment and management settings for your iOS/iPadOS devices. Learn more.

User Affinity & Authentication Method

User affinity * : Enroll without User Affinity

Management Options

Supervised * : Yes

Locked enrollment * : Yes

Shared iPad * : Yes

Enrol with User Affinity

- This option allows users to enrol using their Azure AD nhs.net credentials and is designed for a single user.
- *Use Case*: iOS Single User device enrolment

Enrol without User Affinity

- This option is shared/kiosk mode device mode and does not require the Company Portal app.
- *Use Case*: iOS Shared devices enrolment

Reminder: Only iPads are currently able to be enrolled as Shared Devices and are therefore the only device type which will require enrolment without user affinity.

iOS Deep Dive | Configuration Profiles

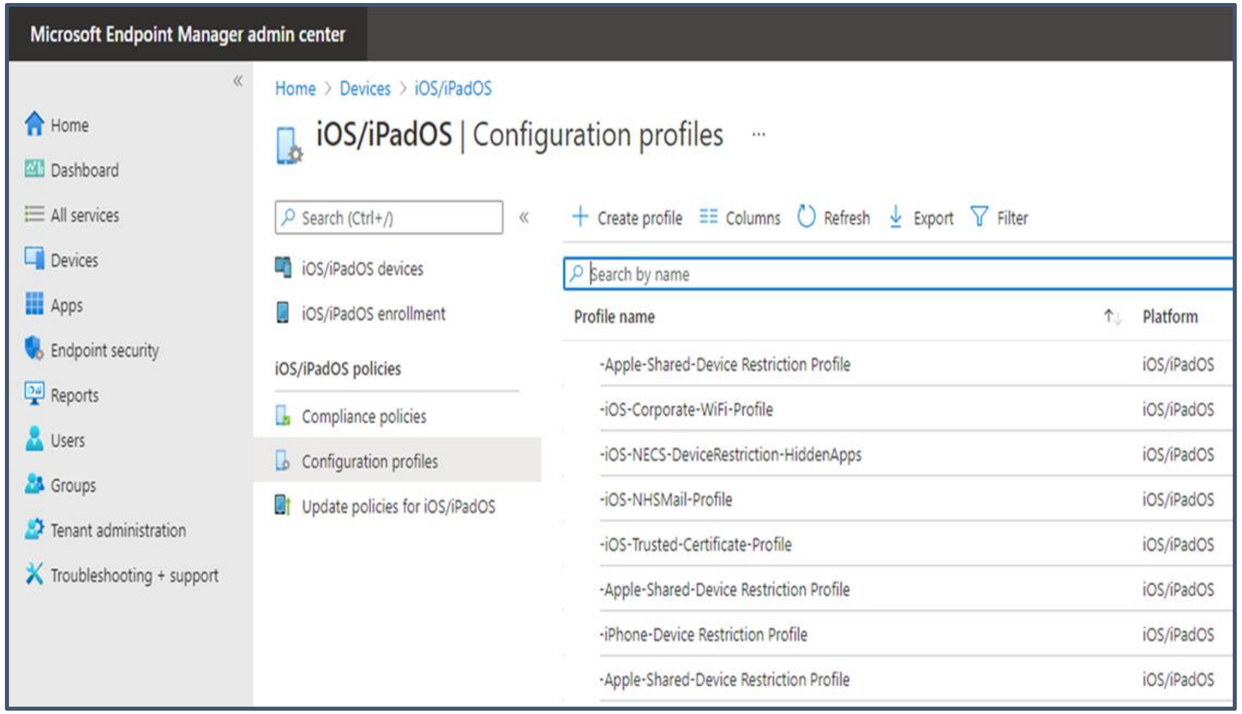
Configuration profiles allows LAs to set up specific features on iOS/iPadOS devices and manage what end users can do/see on their devices

WHAT ARE IOS/IPADOS CONFIGURATION PROFILES?

- Configuration profiles for iOS/iPadOS are the different policies that configure iOS and iPadOS devices; providing the ability for LAs to allow or disable features, set password rules, allow, or restrict specific policies.
- Configuration profiles allows LAs to determine what settings are applied to a device. They operate in a similar manner to group policies in SCCM for example.

WHAT CAN LAS DO WITH IOS/IPADOS CONFIGURATION PROFILES?

- LAs have the rights to change the recommended polices to suit their organisation.
- LAs can assign policies to groups. Once the policy has been assigned to a particular group, all the iOS/iPadOS devices in that group will have that policy applied to it.



iOS/iPadOS | Configuration profiles

Profile name	Platform
-Apple-Shared-Device Restriction Profile	iOS/iPadOS
-iOS-Corporate-WiFi-Profile	iOS/iPadOS
-iOS-NECS-DeviceRestriction-HiddenApps	iOS/iPadOS
-iOS-NHSMail-Profile	iOS/iPadOS
-iOS-Trusted-Certificate-Profile	iOS/iPadOS
-Apple-Shared-Device Restriction Profile	iOS/iPadOS
-iPhone-Device Restriction Profile	iOS/iPadOS
-Apple-Shared-Device Restriction Profile	iOS/iPadOS

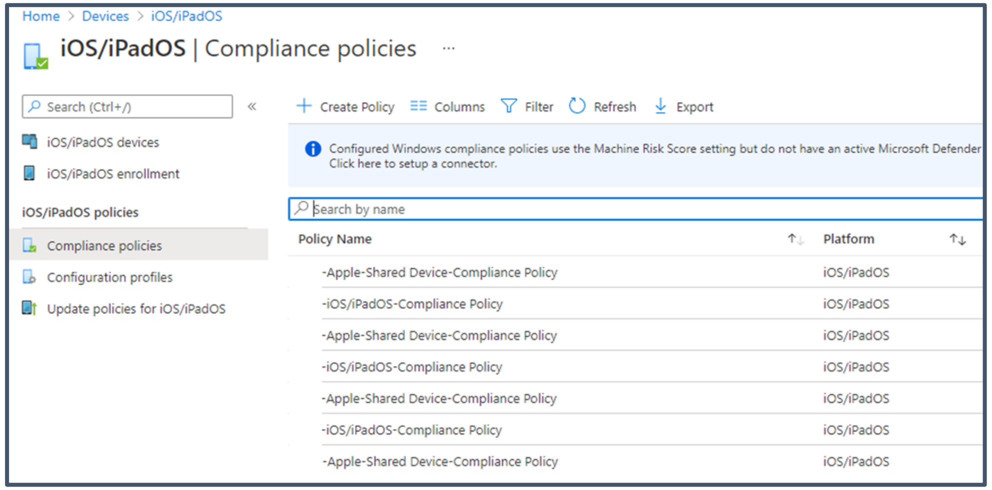
Note: Any deviation from the pencilled-in baseline settings and configuration should be done with consideration and prior testing. Organisations are solely responsible for changes made by their LAs that have been provided with Intune RBAC permissions.

iOS Deep Dive | Compliance Policies

Compliance policies are a feature of Intune which gives LAs the ability to set requirements on iOS devices

WHAT ARE IOS/IPAD OS COMPLIANCE POLICIES?

- iOS/iPadOS compliance policies determine what makes Apple devices compliant.
- They are platform-specific rules that can be configured and deployed to groups of users or devices.
- These rules define requirements for devices, like minimum operating systems or the use of disk encryption.
- Devices must meet these rules to be considered compliant.



Configured Windows compliance policies use the Machine Risk Score setting but do not have an active Microsoft Defender
Click here to setup a connector.

Policy Name	Platform
-Apple-Shared Device-Compliance Policy	iOS/iPadOS
-iOS/iPadOS-Compliance Policy	iOS/iPadOS
-Apple-Shared Device-Compliance Policy	iOS/iPadOS
-iOS/iPadOS-Compliance Policy	iOS/iPadOS
-Apple-Shared Device-Compliance Policy	iOS/iPadOS
-iOS/iPadOS-Compliance Policy	iOS/iPadOS
-Apple-Shared Device-Compliance Policy	iOS/iPadOS

WHAT CAN LAS DO WITH COMPLIANCE POLICIES?

- Include actions that apply to devices that are noncompliant. Actions for noncompliance can alert users to the conditions of noncompliance and safeguard data on noncompliant devices.
- When combined with Conditional Access, compliance policies can block users and devices that don't meet the rules and are noncompliant until the device is compliant.
- LAs can view a report (monitoring section of the Intune Portal) detailing all devices which are noncompliant as well as also viewing reports that will help troubleshoot policies that have conflicts or errors.

- Compliant devices – the device will have access to resources.
- Noncompliant devices (with conditional access) – the device will be unable to access resources until the compliance requirements are met by the end user. For example, adding a password to unlock the device.

Note: Any deviation from the pencilled-in baseline settings and configuration should be done with consideration and prior testing. Organisations are solely responsible for changes made by their LAs that have been provided with Intune RBAC permissions.

iOS Deep Dive | Application Management

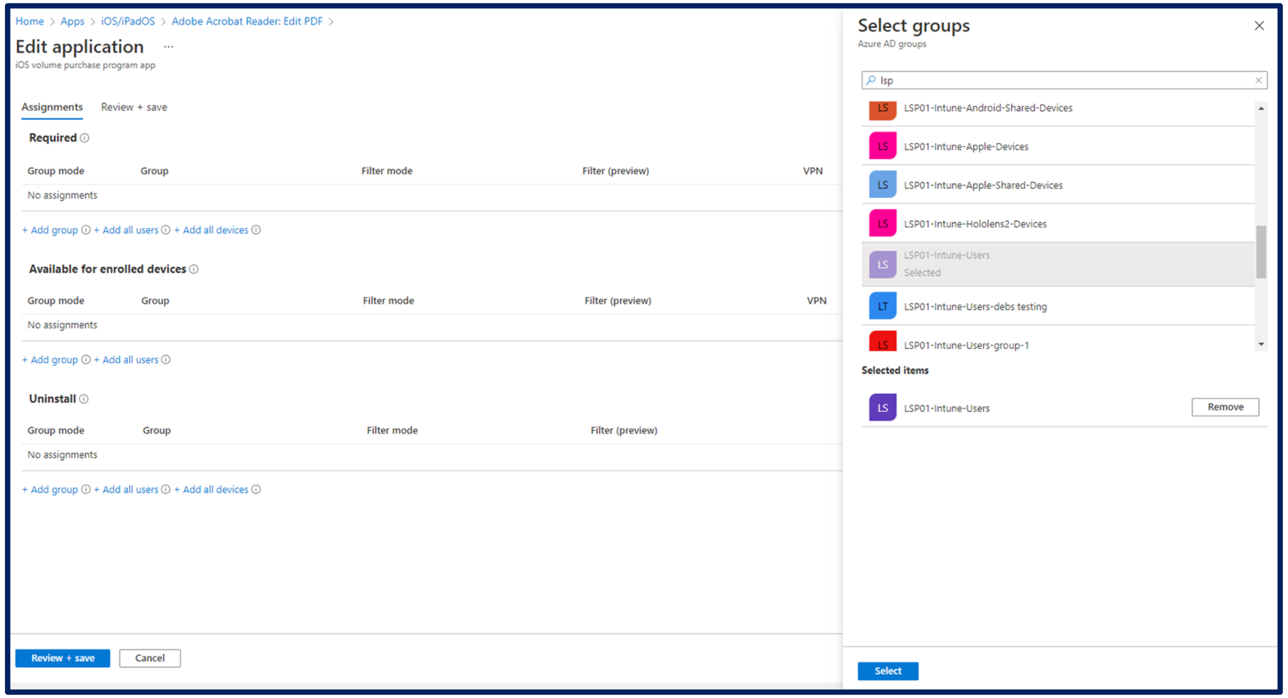
Organisations can assign and manage applications for iOS/iPadOS devices via the ABM Portal and App Store

WHAT IS IOS/IPAD OS APPLICATION MANAGEMENT?

- iOS/iPadOS application management gives LAs the ability to manage and push applications to the iOS/iPadOS devices which have been successfully enrolled to NHSmail Intune.
- Applications need to be purchased via the ABM App Store and then assigned through Intune.

WHAT CAN LAS DO WITH IOS/IPADOS APPLICATION MANAGEMENT?

- LAs have the ability to push various iOS apps to enrolled iOS/iPadOS devices through the ABM portal. The Operations Guide covers the steps to successfully deploy an iOS app to an iOS/iPadOS device via the Intune Portal.
- When deploying an app, LAs can change several default settings, for example:
  - Description of the app
  - Minimum Operating System
  - Applicable Device Type


Home > Apps > iOS/iPadOS > Adobe Acrobat Reader: Edit PDF >

Edit application ...

iOS volume purchase program app

Assignments | Review + save

Required

Group mode	Group	Filter mode	Filter (preview)	VPN
No assignments				

+ Add group + Add all users + Add all devices

Available for enrolled devices

Group mode	Group	Filter mode	Filter (preview)	VPN
No assignments				

+ Add group + Add all users

Uninstall

Group mode	Group	Filter mode	Filter (preview)
No assignments			

+ Add group + Add all users + Add all devices

Review + save | Cancel

Select groups

Azure AD groups

lsp

- LS LSP01-Intune-Android-Shared-Devices
- LS LSP01-Intune-Apple-Devices
- LS LSP01-Intune-Apple-Shared-Devices
- LS LSP01-Intune-Hololens2-Devices
- LS LSP01-Intune-Users Selected
- LT LSP01-Intune-Users-debs testing
- LS LSP01-Intune-Users-group-1

Selected items

LS LSP01-Intune-Users — Remove

Select

✓ There are **no** limits to number of applications you can deploy and there are **no** restrictions on application types. The only restrictions for applications relate to storage on the device.

iOS Deep Dive | Volume Purchase Program

VPP is a feature of ABM and organisations can utilise VPP in Intune for their iOS/iPadOS devices

WHAT IS A VPP?

- Location tokens are volume purchase licences that were commonly known as Volume Purchase Program (VPP) tokens.

WHAT CAN LAS DO WITH LOCATION TOKENS?

- Location tokens are used to assign and manage licences purchased using Apple Business Manager. Content Managers can purchase and associate licences with location tokens they have permissions to in Apple Business Manager.
- These location tokens are then downloaded from Apple Business Manager and uploaded in Microsoft Intune.

WHAT CAN ORGANISATIONS DO WITH THEIR VPP ON INTUNE?

- Microsoft Intune can help organisations manage apps purchased through the VPP program by:
  - ✓ Synchronizing location tokens that are downloaded from Apple Business Manager.
  - ✓ Tracking how many licences are available and have been used for purchased apps.
  - ✓ Monitor app installs up to the number of licences you own.

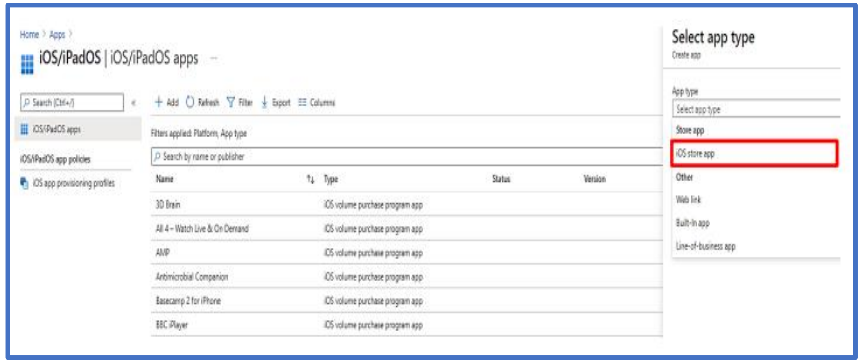
iOS Deep Dive | How to Assign Apps

Organisations can assign applications using Intune to iOS/iPadOS devices. The Operations Guide contains full instructions on how to assign applications

START

STEP 1

LAs should go to the Intune portal and locate the Apps page for iOS/iPadOS devices.



Home > Apps >

iOS/iPadOS | iOS/iPadOS apps ...

Filters applied: Platform, App type

Search by name or publisher

Name	Type	Status	Version
3D Brain	iOS volume purchase program app		
All 4 – Watch Live & On Demand	iOS volume purchase program app		
AMP	iOS volume purchase program app		
Antimicrobial Companion	iOS volume purchase program app		
Basecamp 2 for iPhone	iOS volume purchase program app		
BBC iPlayer	iOS volume purchase program app		

Select app type

Create app

App type: Select app type

Store app

- iOS store app

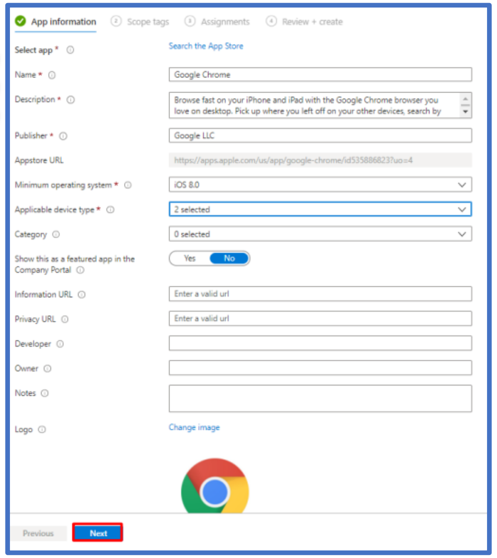
Other

- Web link
- Built-In app
- Line-of-business app

STEP 2

Search for the application you would like to add and input the relevant details (optional):

- Description of the app
- Minimum Operating System
- Applicable Device Type



Select app * ⓘ: Search the App Store

Name * ⓘ: Google Chrome

Description * ⓘ: Browse fast on your iPhone and iPad with the Google Chrome browser you love on desktop. Pick up where you left off on your other devices, search by

Publisher * ⓘ: Google LLC

Appstore URL: https://apps.apple.com/us/app/google-chrome/id535886823?uo=4

Minimum operating system * ⓘ: iOS 8.0

Applicable device type * ⓘ: 2 selected

Category ⓘ: 0 selected

Show this as a featured app in the Company Portal ⓘ: Yes [✓ No]

Information URL ⓘ: Enter a valid url

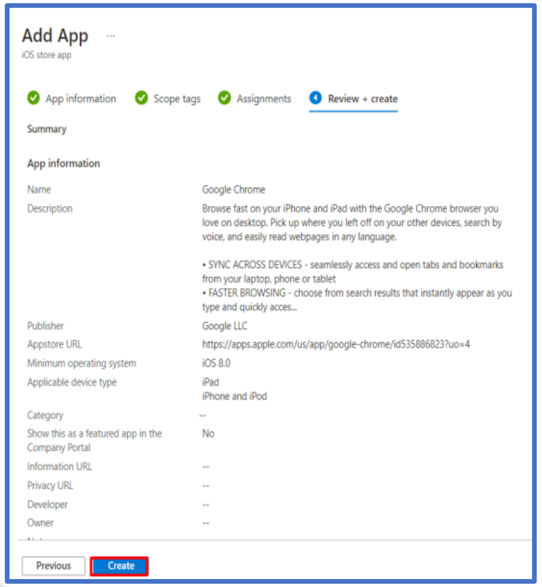
Privacy URL ⓘ: Enter a valid url

Developer ⓘ:

Owner ⓘ:

Notes ⓘ:

Logo ⓘ: Change image



Add App ...

iOS store app

Summary

App information

Name	Google Chrome
Description	Browse fast on your iPhone and iPad with the Google Chrome browser you love on desktop. Pick up where you left off on your other devices, search by voice, and easily read webpages in any language. • SYNC ACROSS DEVICES - seamlessly access and open tabs and bookmarks from your laptop, phone or tablet • FASTER BROWSING - choose from search results that instantly appear as you type and quickly acces...
Publisher	Google LLC
Appstore URL	https://apps.apple.com/us/app/google-chrome/id535886823?uo=4
Minimum operating system	iOS 8.0
Applicable device type	iPad iPhone and iPod
Category	--
Show this as a featured app in the Company Portal	No
Information URL	--
Privacy URL	--
Developer	--
Owner	--

STEP 3

Your organisation's scope tag will be automatically assigned allowing the application to be applied to all devices or users in a group.

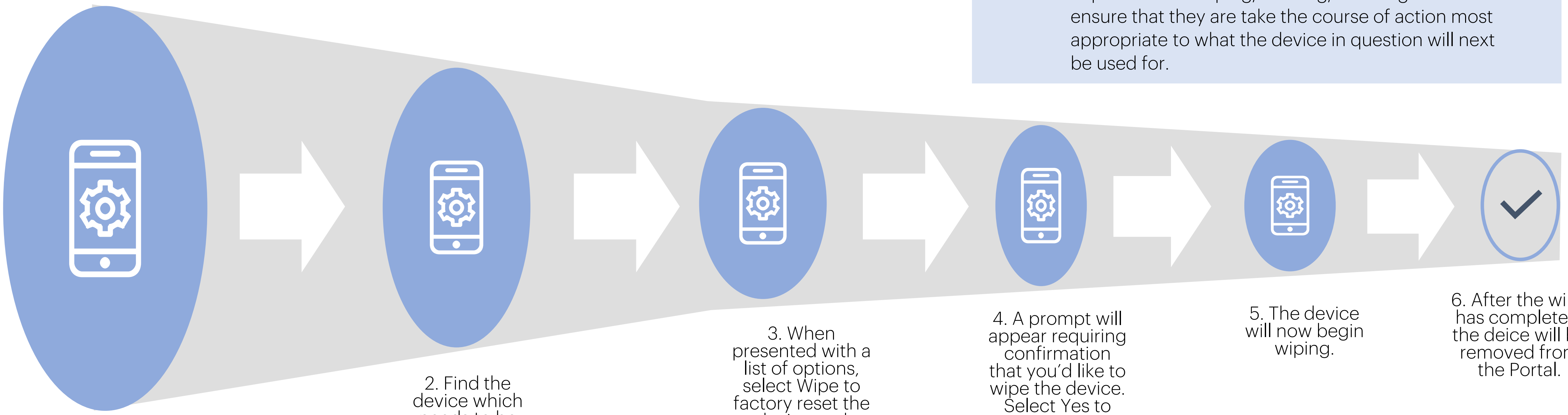
iOS Deep Dive | Wiping and Removing

iOS and iPadOS devices enrolled onto NHSmail Intune can be remotely wiped and removed from the platform by LAs with the correct RBAC permissions

- With delegated RBAC controls, LAs have the permissions to remotely wipe and remove iOS/iPadOS and Android devices from the NHSmail Intune platform. This action should be performed only as a last resort for devices experiencing issues and LAs are not required to seek support from the Intune Live Service Team to complete this.
- Devices can be wiped via the Intune Portal by following the below steps:

Important note:

LAs should always consider the data retention implications of wiping/deleting/resetting a device and ensure that they are take the course of action most appropriate to what the device in question will next be used for.



1. Sign into the Intune Portal and select the Devices page.

2. Find the device which needs to be wiped and select this device.

3. When presented with a list of options, select Wipe to factory reset the device and remove all data.

4. A prompt will appear requiring confirmation that you'd like to wipe the device. Select Yes to progress.

5. The device will now begin wiping.

6. After the wipe has completed, the deice will be removed from the Portal.

THANK YOU