Australian Government

Digital Transformation Agency

Onboarding - Standard Operating Procedure

March 2020

dta

Contents

Document Overview **4**

Background 4

Document Audience 4

Purpose 4

Prerequisites 4

Associated Documentation 5

Onboarding **6**

Account Creation 6

Autopilot Enrolment 9

Device Groups 12

Abbreviations and Acronyms **14**

Document Overview

Background

The agency is responsible for the ongoing management of people and devices as they join the agency and ensuring staff are provided with the system access required to perform their duties.

Document Audience

This Standard Operating Procedure (SOP) is intended to support the ongoing operation of the Agency's user and administrative device. It includes the required steps that a suitable trained administrator should follow to maintain the operational state of its devices and accounts when being onboarded.

Purpose

The purpose of this document is to provide the necessary steps to onboard a new user and their device.

Prerequisites

Before completing the procedures detailed in this document, the following prerequisites should be met:

- The account creation for a user has been approved and authorised through the agencies onboarding and security procedures.
- It is recommended that the reader/administrator performing the procedures in the document has certification and/or experience with Office 365 and Microsoft Azure.
- The system administrator has an active account in Azure AD with the appropriate roles and permissions.
- A basic understanding of user account creation.
- A basic understanding of device management in the context of a Mobile Device Management (MDM) solution.

Associated Documentation

Table 1 identifies the documents that should be referenced and understood before administering this solution

Table 1 Associated Documentation

Name	Version	Date
DTA – Solution Overview	March	03/2020
DTA – Platform Design	March	03/2020
DTA – Workstation Design	March	03/2020
DTA – Office 365 Design	March	03/2020
DTA – Office 365 - ABAC	March	03/2020
DTA – Platform – ABAC	March	03/2020
DTA – Intune Security Baselines - ABAC	March	03/2020
DTA – Software Updates - ABAC	March	03/2020
DTA – Intune Applications – ABAC	March	03/2020
DTA – Intune Enrolment – ABAC	March	03/2020
DTA – Conditional Access Policies – ABAC	March	03/2020
DTA – Intune Compliance – ABAC	March	03/2020
DTA – Intune Configuration – ABAC	March	03/2020

Onboarding

The authorisation and approval of users being granted access to the system is out of scope of this SOP.

Asset management of devices used by the agency and being connected to the systems is out of scope of this SOP

Before a device can be used there are a number of procedures that must be completed for it to be onboarded correctly, these include:

- Account Creation,
- Autopilot Enrolment, and
- Device Groups.

Account Creation

Before creating a user or privileged user account ensure the user has been authorised and approved to access the system and that Agency privileged management procedures for those users with administrative accounts have been complied with.

This instruction includes how to create a standard user or administrative account.

Once the below table has been followed for the creation of a user or administrative account a few additional steps will occur automatically. If a standard user account is created (e.g., joe.bloggs@domain.gov.au), the account will automatically be added to the dynamic Azure AD group **rol-Agency-users** using the following rule syntax:

(user.accountEnabled -eq true) and (user.userPrincipalName -notContains "_priv")

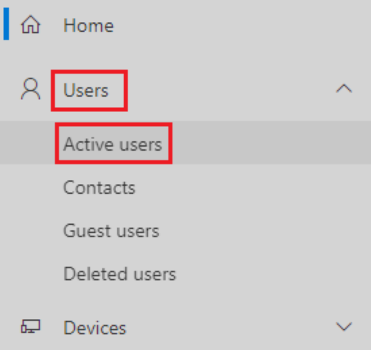
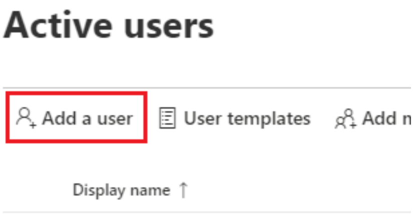
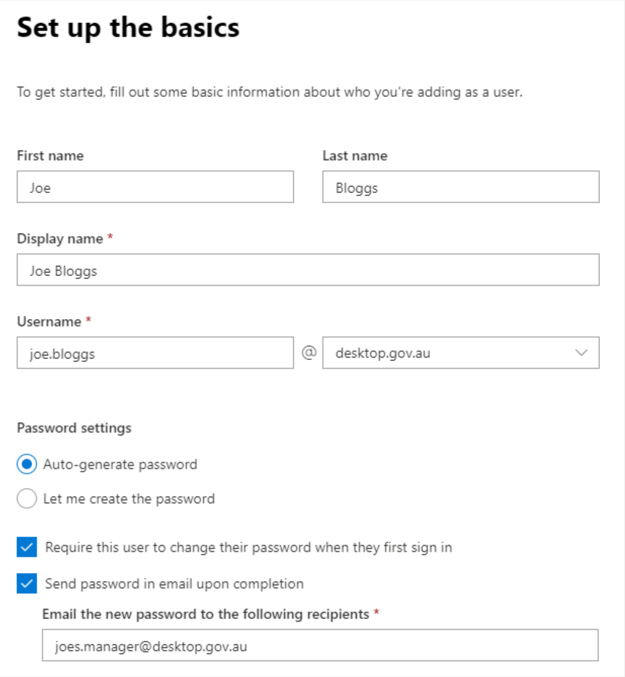
This will automatically provide access to a standard set of applications and apply licenses.

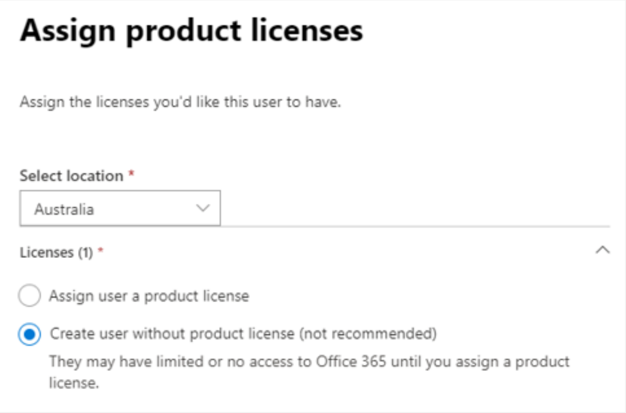
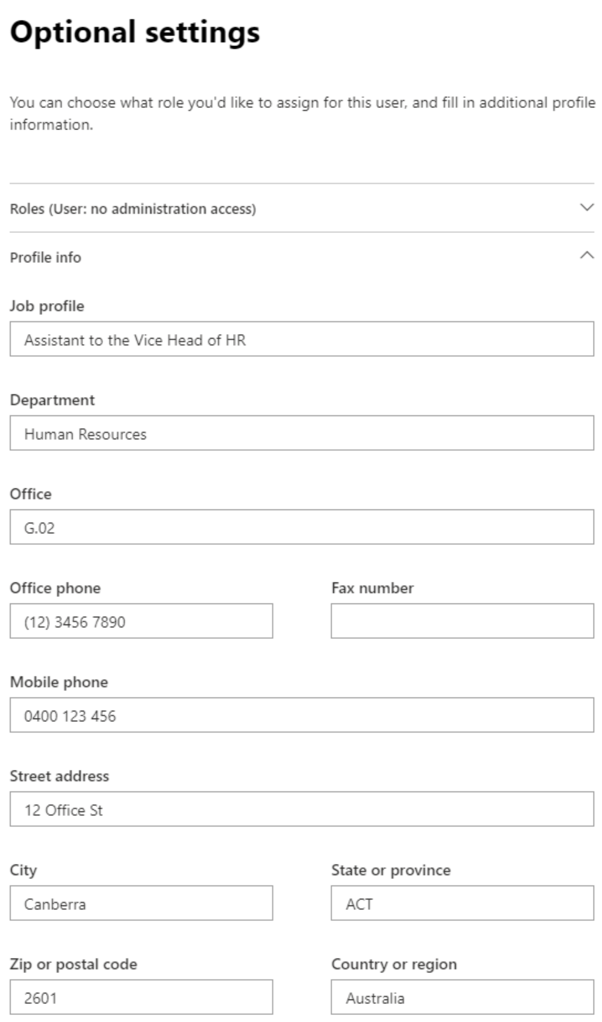
If an administrative account is created (e.g., joe.bloggs_priv@domain.gov.au) is created, the account will automatically be added to the dynamic Azure AD group **rol-Agency-Administrators** using the following rule syntax:

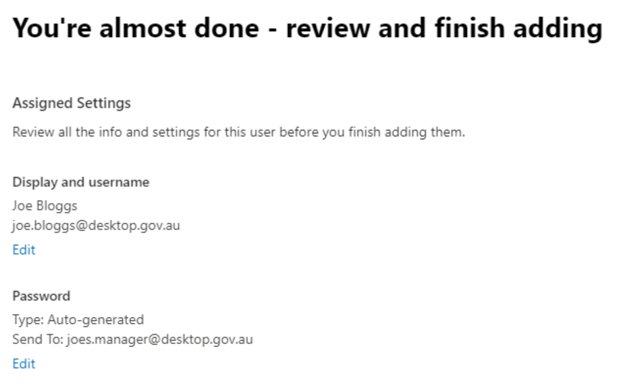
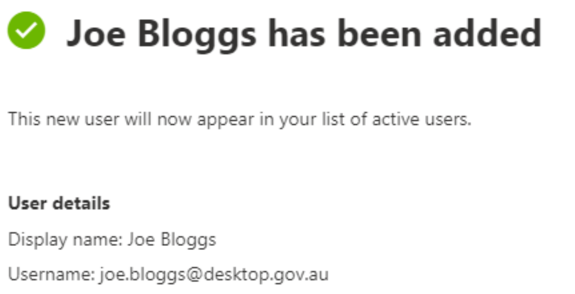
(user.accountEnabled -eq true) and (user.userPrincipalName -contains "_priv")

In this manner, user licencing and standard user applications are controlled automatically. To allow this process to occur, please allow up to 30 minutes to pass before providing login credentials to users to ensure correct propagation of group membership and licensing.

Table 2 Account Creation

Steps	Instruction	Screenshot
1.	Within your internet browser navigate to the Microsoft 365 admin center (https://admin.microsoft.com)	No screenshot required
2.	On the left-hand pane click **Users** then **Active users**	 Home Users Active users Contacts Guest users Deleted users Devices
Note: *this instruction will only cover the creation of a single user, users can be created via template and in bulk via a similar method.*		
3.	Click **Add a user**	 Active users Add a user User templates Add n Display name ↑
4.	The **Set up the basics** window will appear, complete all fields as shown in the screenshot. Use the following password settings: - **Auto-generate password** - **Require this user to change their password when they first sign in**: Ticked - **Send password in email upon completion**: Ticked The new password should be sent to the users' manager or another trusted source. When complete press **Next**	Set up the basics To get started, fill out some basic information about who you're adding as a user. First name: Joe Last name: Bloggs Display name *: Joe Bloggs Username *: joe.bloggs @ desktop.gov.au Password settings ● Auto-generate password ○ Let me create the password ☑ Require this user to change their password when they first sign in ☑ Send password in email upon completion Email the new password to the following recipients *: joes.manager@desktop.gov.au

Steps	Instruction	Screenshot
IMPORTANT NOTE: when selecting a username, ensure that the standard user account follows the Agency naming standard of user.name@domain.gov.au, for an Administrative account however ensure the suffix '_**priv**' is appended to the username (e.g., user.name_**priv**@domain.gov.au). The reason for this is because dynamic groups exist within Azure AD that will automatically control what licenses are added to the user account.		
5.	On the **Assign product licenses** screen, select **Australia** as the location, and then select **Create user without product license (not recommended)**. When complete press **Next**	 Assign product licenses Assign the licenses you'd like this user to have. Select location * Australia Licenses (1) * ○ Assign user a product license ● Create user without product license (not recommended) They may have limited or no access to Office 365 until you assign a product license.
6.	On the **Optional settings** page, leave the **Role** as **User: no administration access**. Complete all appropriate fields in the **Profile info** section. When complete press **Next**	 Optional settings You can choose what role you'd like to assign for this user, and fill in additional profile information. Roles (User: no administration access) Profile info Job profile: Assistant to the Vice Head of HR Department: Human Resources Office: G.02 Office phone: (12) 3456 7890 Fax number: Mobile phone: 0400 123 456 Street address: 12 Office St City: Canberra State or province: ACT Zip or postal code: 2601 Country or region: Australia

Steps	Instruction	Screenshot
7.	Review the user to be created and ensure all of the details you have entered are correct. When complete press **Finish adding**	 You're almost done - review and finish adding Assigned Settings Review all the info and settings for this user before you finish adding them. Display and username Joe Bloggs joe.bloggs@desktop.gov.au Edit Password Type: Auto-generated Send To: joes.manager@desktop.gov.au Edit
8.	The account has now been created, press the **Close** button.	 Joe Bloggs has been added This new user will now appear in your list of active users. User details Display name: Joe Bloggs Username: joe.bloggs@desktop.gov.au

Note: *allow up to 1 hour for the account to fully create as dynamic group changes will propagate on the back-end.*

Autopilot Enrolment

The following instruction advises how to enrol a device within Autopilot. This must be completed for each device that is used within the environment. This ensures that the device builds correctly with the right settings and Intune policies applied.

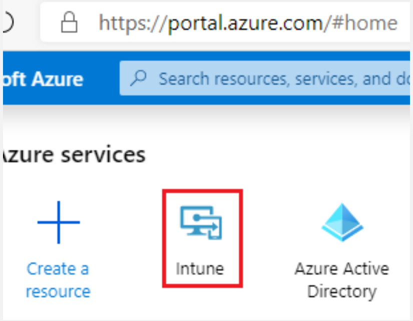
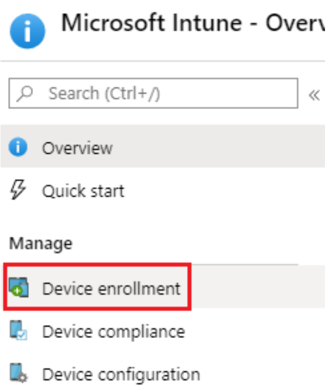
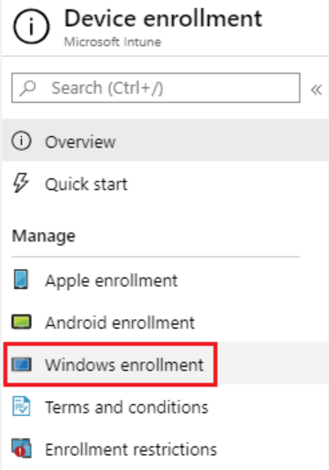
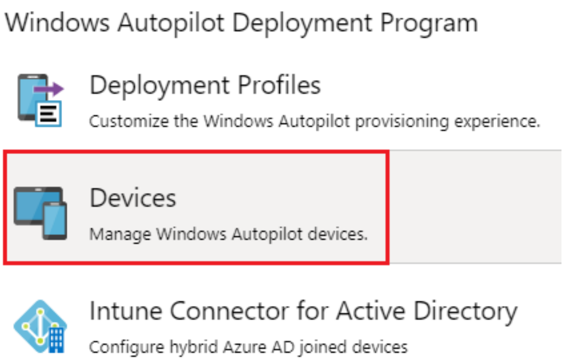
There are a number of prerequisites required for this section, the primary of which is to supply a .CSV file with the following fields prefilled.

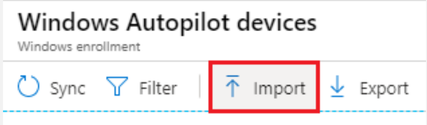
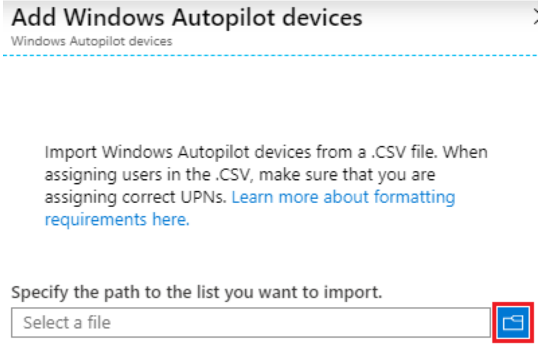
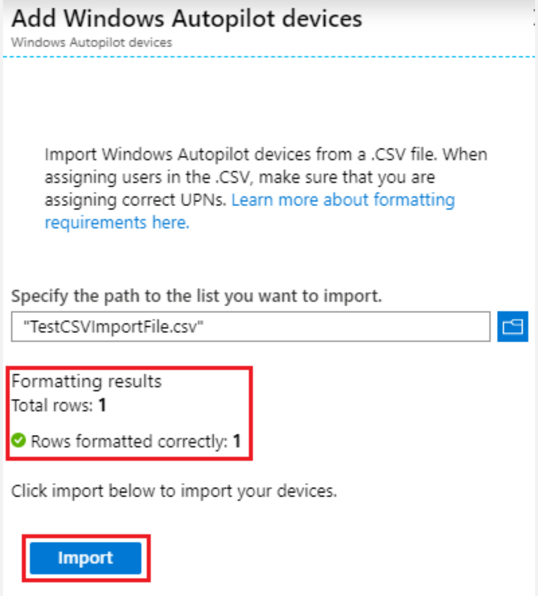
<Serial Number>, <Windows Product ID>, <Hardware Hash>, <Order ID>

In many cases, when hardware is ordered from a vendor, they can provide this information prior to the devices being delivered. This instruction will assume that the .CSV exists and you as an administrator are ready to upload it into the Azure portal.

Please also note that there are a number of different avenues/portals that you can use to access Autopilot and this simply describes one of them, which is accurate as of the time of writing.

Table 3 Autopilot Enrolment

Steps	Instruction	Screenshot
1.	Navigate to the **Azure portal** (https://portal.azure.com) then select **Intune**	 https://portal.azure.com/#home oft Azure Search resources, services, and do ızure services Create a resource Intune Azure Active Directory
2.	Within **Intune**, on the left-hand pane, select **Device enrollment**	 Microsoft Intune - Overv Search (Ctrl+/) « Overview Quick start Manage Device enrollment Device compliance Device configuration
3.	Within **Device enrollment**, select **Windows enrollment** from the left-hand pane	 Device enrollment Microsoft Intune Search (Ctrl+/) « Overview Quick start Manage Apple enrollment Android enrollment Windows enrollment Terms and conditions Enrollment restrictions
4.	Within the **Device enrollment – Windows enrollment** blade, select **Devices** under the **Windows Autopilot Deployment Program** section	 Windows Autopilot Deployment Program Deployment Profiles Customize the Windows Autopilot provisioning experience. Devices Manage Windows Autopilot devices. Intune Connector for Active Directory Configure hybrid Azure AD joined devices

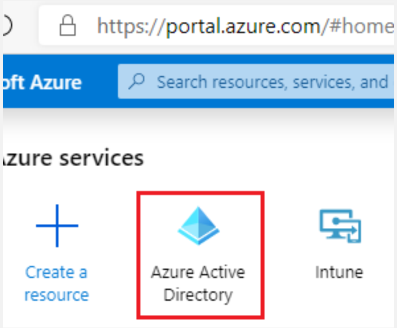
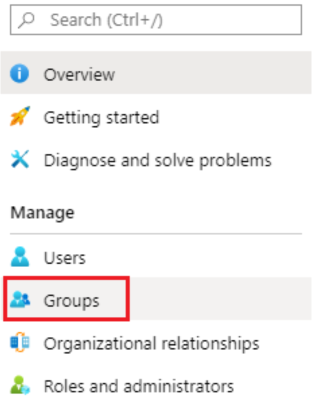
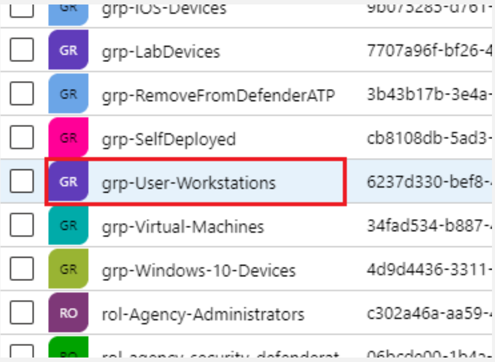
Steps	Instruction	Screenshot
5.	Within the **Windows Autopilot devices** screen, press the **Import** button	 Windows Autopilot devices Windows enrollment Sync Filter Import Export
6.	When the **Add Windows Autopilot devices** pane appears on the right of the screen, click the '**Choose file**' icon, then select your .CSV file.	 Add Windows Autopilot devices Windows Autopilot devices Import Windows Autopilot devices from a .CSV file. When assigning users in the .CSV, make sure that you are assigning correct UPNs. Learn more about formatting requirements here. Specify the path to the list you want to import. Select a file
7.	Review whether the results are correct, and the rows are formatted correctly, if so, press **Import**	 Add Windows Autopilot devices Windows Autopilot devices Import Windows Autopilot devices from a .CSV file. When assigning users in the .CSV, make sure that you are assigning correct UPNs. Learn more about formatting requirements here. Specify the path to the list you want to import. "TestCSVImportFile.csv" Formatting results Total rows: **1** ✓ Rows formatted correctly: **1** Click import below to import your devices. Import
8.	Allow the import to complete, note whether it has completed successfully via the **Notifications** bell icon in the top right of the screen.	No screenshot required

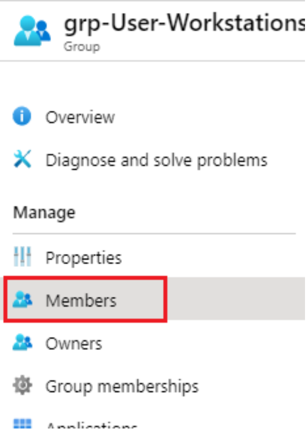
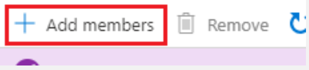
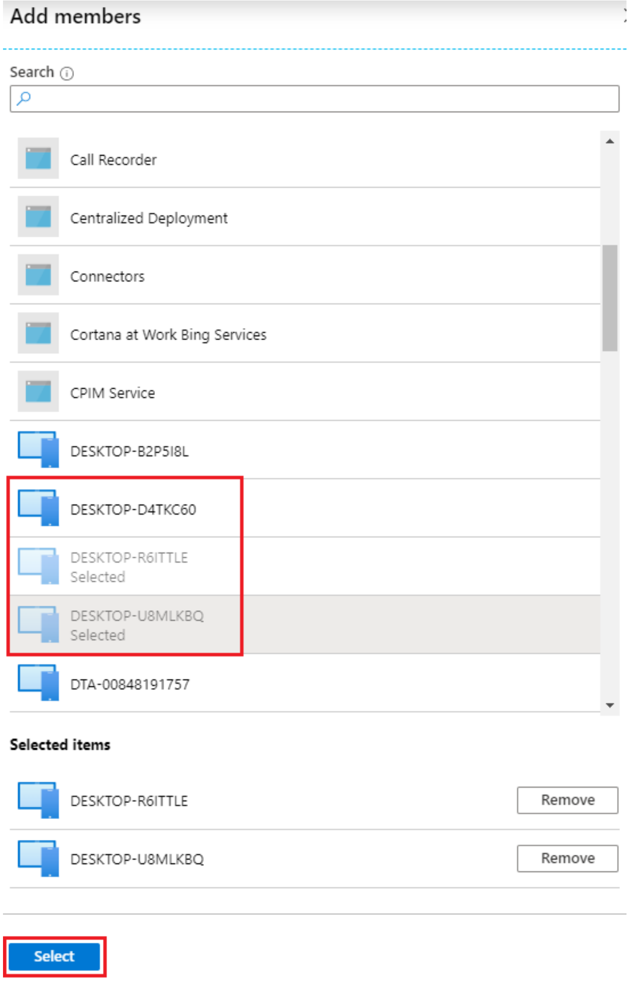
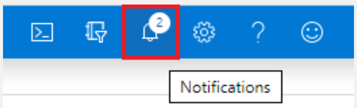
Once the import has completed successfully your device(s) can be powered on and will pick up the appropriate deployment profile and Intune policies upon first boot.

Device Groups

To ensure devices receive the correct policy assignments they must be added to the correct groups within Azure Active Directory (Azure AD). The following table describes how to add a device to a group.

Table 4 Device Groups

Steps	Instruction	Screenshot
1.	Navigate to the **Azure portal** (https://portal.azure.com) then select **Azure Active Directory**	 https://portal.azure.com/#home oft Azure Search resources, services, and ızure services Create a resource Azure Active Directory Intune
2.	In the left-hand pane, click **Groups**	 Search (Ctrl+/) Overview Getting started Diagnose and solve problems Manage Users Groups Organizational relationships Roles and administrators
3.	Identify the group that your device is to be added to and click on it. In this example we will select **grp-User-Workstations**	 grp-iOS-Devices GR grp-LabDevices 7707a96f-bf26-4 GR grp-RemoveFromDefenderATP 3b43b17b-3e4a- GR grp-SelfDeployed cb8108db-5ad3- GR grp-User-Workstations 6237d330-bef8- GR grp-Virtual-Machines 34fad534-b887- GR grp-Windows-10-Devices 4d9d4436-3311- RO rol-Agency-Administrators c302a46a-aa59-

Steps	Instruction	Screenshot
4.	In the left hand-pane, click on **Members**	 grp-User-Workstations Group Overview Diagnose and solve problems Manage Properties Members Owners Group memberships Applications
5.	Along the top ribbon, click **Add members**	
6.	In the pane that appears on the right of the screen, identify the devices to be added, click on them, then press **Select**	 Add members Search Call Recorder Centralized Deployment Connectors Cortana at Work Bing Services CPIM Service DESKTOP-B2P5I8L DESKTOP-D4TKC60 DESKTOP-R6ITTLE Selected DESKTOP-U8MLKBQ Selected DTA-00848191757 Selected items DESKTOP-R6ITTLE Remove DESKTOP-U8MLKBQ Remove Select
7.	Ensure the device has been added to the group via the **Notifications** icon in the top right of the screen.	

Abbreviations and Acronyms

Table 5 details the abbreviations and acronyms used throughout this document.

Table 5 Abbreviations and Acronyms

Acronym	Meaning
Azure AD	Azure Active Directory
DTA	Digital Transformation Agency
MDM	Mobile Device Management
SOP	Standard Operating Procedure