



Australian Government
Digital Transformation Agency

Offboarding - Standard Operating Procedure

March 2020

Contents

Document Overview	4
Background	4
Document Audience.....	4
Purpose	4
Prerequisites	4
Associated Documentation	5
Device Offboarding	6
Remove Device from Azure AD	6
Remove Device from Intune	8
Offboard a Device from Microsoft Defender - Manual	9
Offboard a Device from Microsoft Defender - Automated	11
Remove Device from Autopilot	13
Abbreviations and Acronyms	15

Document Overview

Background

Agencies are responsible for ensuring only authorised users and or devices are able to access the system. Agencies are responsible for ensuring users are to be removed from the system on the same day they no longer have a business need to access the system. Devices, in particular those that have been lost or stolen must be removed as a soon as practical.

Document Audience

This Standard Operating Procedure (SOP) is intended to support the ongoing operation of the Digital Transformation Agency (DTA) Blueprint. It includes the required steps that a suitably trained administrator should follow to maintain the operational state of the solution.

Purpose

The purpose of this document is to provide the necessary steps to offboard users and/or their devices. This includes when users leave the Agency and return the device, as well as when devices are lost or stolen.

Prerequisites

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

- It is recommended that the reader/administrator performing the procedures in the document has certification and/or experience with Office 365 and Microsoft Azure.
- Appropriate administrative privileges within the environment to manage user accounts and devices.
- The ID/asset number of the device in question.

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

Device Offboarding

Asset management and security procedures regarding lost and stolen devices are out of scope of this SOP and are expected to be managed by the Agency.

If a device is lost, stolen, broken or simply is being replaced, there are several tasks that must be completed to correctly offboard it. Offboarding simply means removing the device from the Agency Azure Active Directory (Azure AD) instance and anywhere else it can be identified within the overarching tenant.

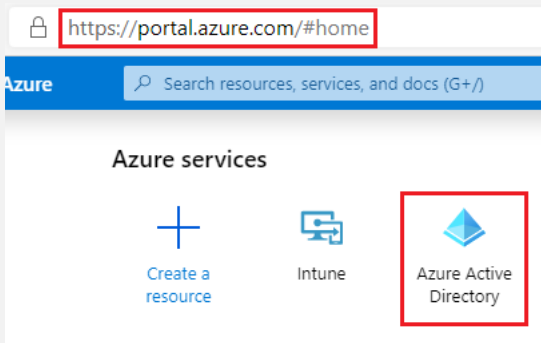
This includes the following tasks:

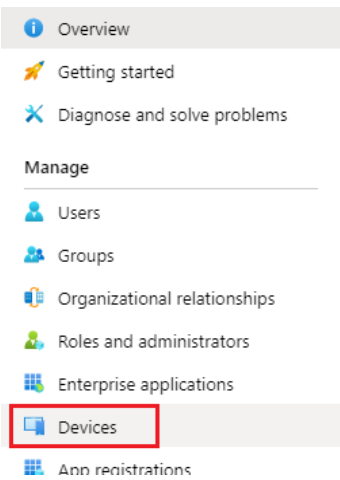
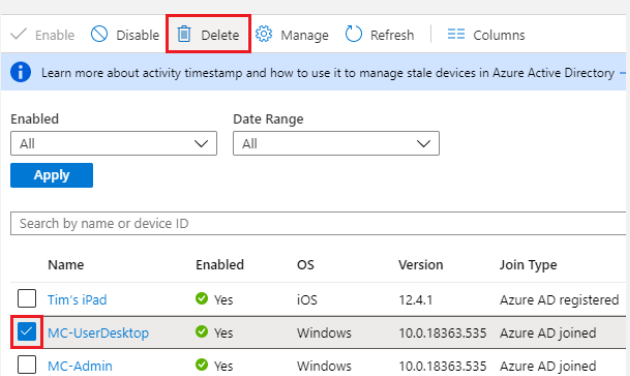
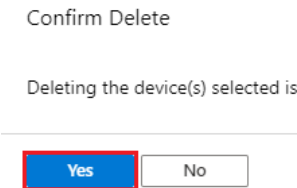
- Removal from Azure Active directory,
- Removal from Intune,
- Removal from Microsoft Defender Security Center, and
- Removed as a Windows Autopilot device.

Remove Device from Azure AD

Complete the below steps to remove the device from Azure AD. Prior to these steps being completed, the administrator performing them must know the ID/asset number of the device being removed from Azure AD.

Table 2 Delete Device from Azure AD

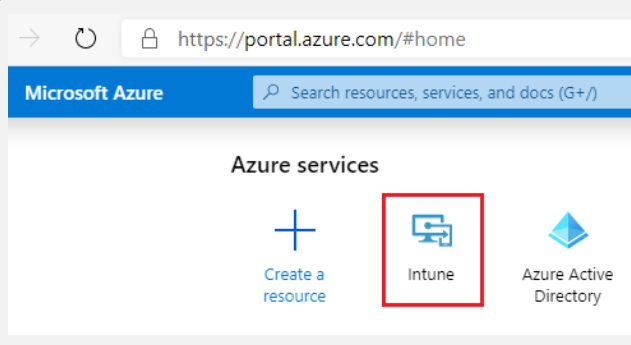
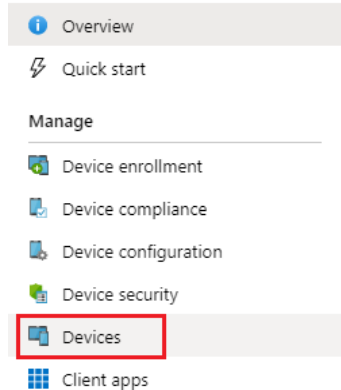
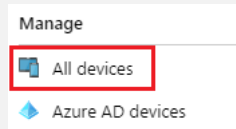
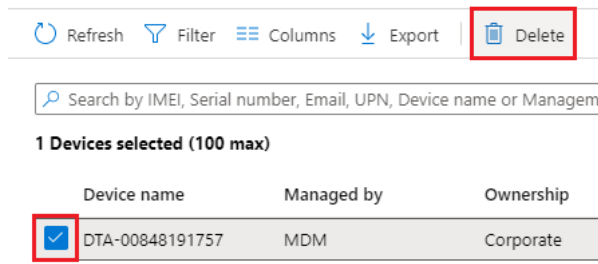

Steps	Instruction	Screenshot
1.	Within your internet browser navigate to the Azure Portal (https://portal.azure.com), then click on Azure Active Directory	

Steps	Instruction	Screenshot																																																												
2.	In the left-hand pane, select Devices																																																													
3.	Within the Devices blade, either by scrolling through the list, or using the search bar, identify your device, check the box, then press Delete	 <table><tr><td>✓ Enable</td><td>⏸ Disable</td><td>🗑 Delete</td><td>⚙ Manage</td><td>🔄 Refresh</td><td>☰ Columns</td></tr><tr><td colspan="6">Learn more about activity timestamp and how to use it to manage stale devices in Azure Active Directory</td></tr><tr><td colspan="2">Enabled</td><td colspan="4">Date Range</td></tr><tr><td colspan="2">All</td><td colspan="4">All</td></tr><tr><td colspan="6">Apply</td></tr><tr><td colspan="6">Search by name or device ID</td></tr><tr><td></td><td>Name</td><td>Enabled</td><td>OS</td><td>Version</td><td>Join Type</td></tr><tr><td><input type="checkbox"/></td><td>Tim's iPad</td><td>✔ Yes</td><td>iOS</td><td>12.4.1</td><td>Azure AD registered</td></tr><tr><td><input checked="" type="checkbox"/></td><td>MC-UserDesktop</td><td>✔ Yes</td><td>Windows</td><td>10.0.18363.535</td><td>Azure AD joined</td></tr><tr><td><input type="checkbox"/></td><td>MC-Admin</td><td>✔ Yes</td><td>Windows</td><td>10.0.18363.535</td><td>Azure AD joined</td></tr></table>	✓ Enable	⏸ Disable	🗑 Delete	⚙ Manage	🔄 Refresh	☰ Columns	Learn more about activity timestamp and how to use it to manage stale devices in Azure Active Directory						Enabled		Date Range				All		All				Apply						Search by name or device ID							Name	Enabled	OS	Version	Join Type	<input type="checkbox"/>	Tim's iPad	✔ Yes	iOS	12.4.1	Azure AD registered	<input checked="" type="checkbox"/>	MC-UserDesktop	✔ Yes	Windows	10.0.18363.535	Azure AD joined	<input type="checkbox"/>	MC-Admin	✔ Yes	Windows	10.0.18363.535	Azure AD joined
✓ Enable	⏸ Disable	🗑 Delete	⚙ Manage	🔄 Refresh	☰ Columns																																																									
Learn more about activity timestamp and how to use it to manage stale devices in Azure Active Directory																																																														
Enabled		Date Range																																																												
All		All																																																												
Apply																																																														
Search by name or device ID																																																														
	Name	Enabled	OS	Version	Join Type																																																									
<input type="checkbox"/>	Tim's iPad	✔ Yes	iOS	12.4.1	Azure AD registered																																																									
<input checked="" type="checkbox"/>	MC-UserDesktop	✔ Yes	Windows	10.0.18363.535	Azure AD joined																																																									
<input type="checkbox"/>	MC-Admin	✔ Yes	Windows	10.0.18363.535	Azure AD joined																																																									
4.	When prompted to delete, press Yes																																																													
5.	Confirm that the process has completed successfully in the Notifications button in the top right of the screen.	No screenshot required																																																												

Remove Device from Intune

Complete the below steps to remove a device from Intune.

Table 3 Remove Device from Intune

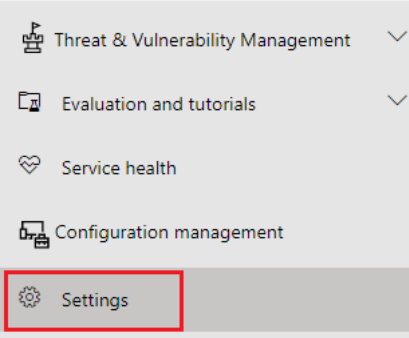
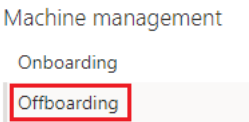
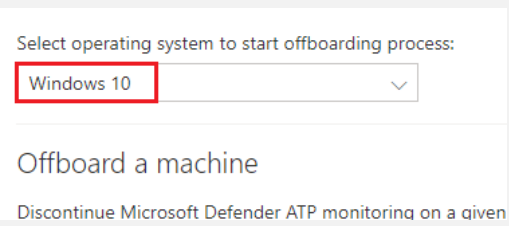
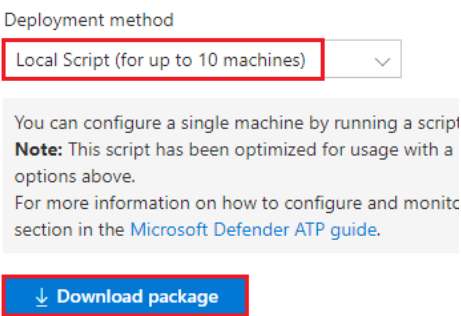
Steps	Instruction	Screenshot								
1.	Within your internet browser navigate to the Azure Portal (https://portal.azure.com), then select Intune									
2.	In the left-hand pane, select Devices									
3.	Within the Devices blade, select All devices									
4.	Either by scrolling through the list, or using the search bar, identify your device, check the box, then press Delete Note , Intune only allows 100 devices to be selected at one time. If more than 100 devices need to be deleted at one time deletion can be performed in batches.	 <div>Refresh Filter Columns Export Delete</div> <div>Search by IMEI, Serial number, Email, UPN, Device name or Management</div> <div>1 Devices selected (100 max)</div> <table><thead><tr><th></th><th>Device name</th><th>Managed by</th><th>Ownership</th></tr></thead><tbody><tr><td><input checked="" type="checkbox"/></td><td>DTA-00848191757</td><td>MDM</td><td>Corporate</td></tr></tbody></table>		Device name	Managed by	Ownership	<input checked="" type="checkbox"/>	DTA-00848191757	MDM	Corporate
	Device name	Managed by	Ownership							
<input checked="" type="checkbox"/>	DTA-00848191757	MDM	Corporate							
5.	A blade will appear on the right of the screen, confirm that the device is correct, then press Delete									
6.	Confirm that the process has completed successfully in the Notifications button in the top right of the screen.	No screenshot required								

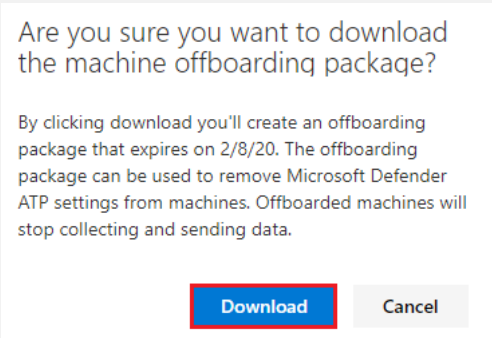
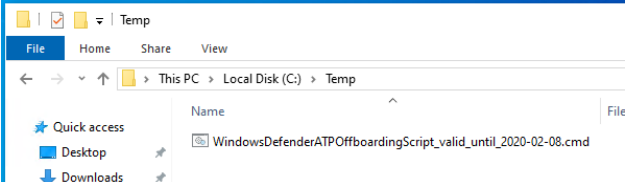
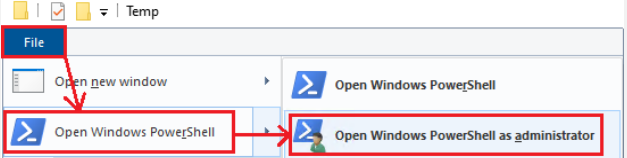
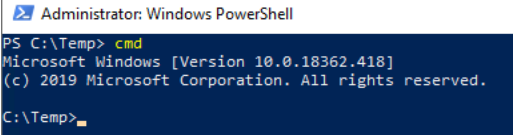
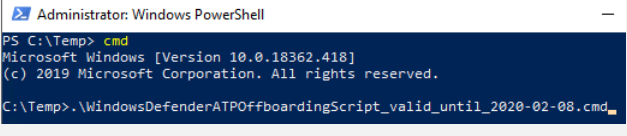
Offboard a Device from Microsoft Defender - Manual

Follow the below steps to manually offboard a device from Microsoft Defender Advanced Threat Protection (ATP). These steps can only be followed if the device is available to be logged into.

Please also note that an administrator with appropriate permissions is required to perform these steps.

Table 4 Offboard a Device from Microsoft Defender - Manual

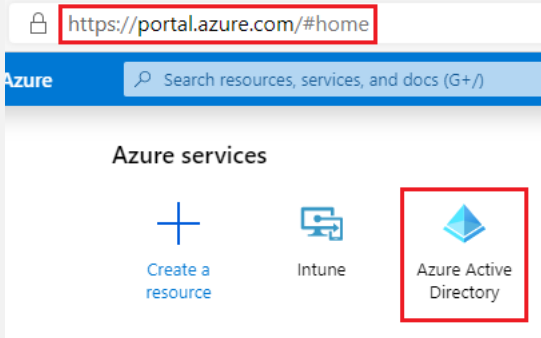
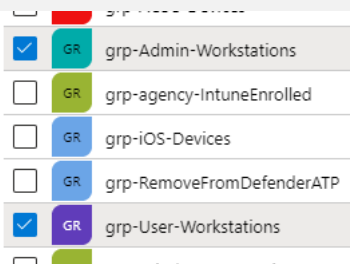
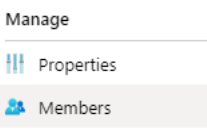
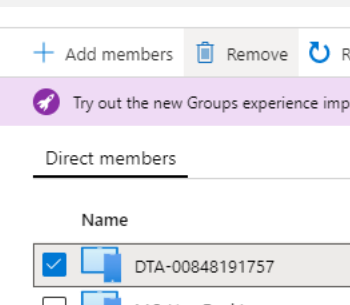
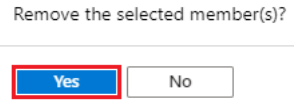
Steps	Instruction	Screenshot
1.	Within your internet browser navigate to the Microsoft Defender Security Center (https://securitycenter.windows.com/), then click on Settings in the left-hand pane (note: you may need to expand the left-hand pane to see Settings)	
2.	Within the Settings screen, click on Offboarding	
3.	From the first dropdown menu, select Windows 10	
4.	From the second dropdown menu, select Local Script (for up to 10 machines) , then click Download package	

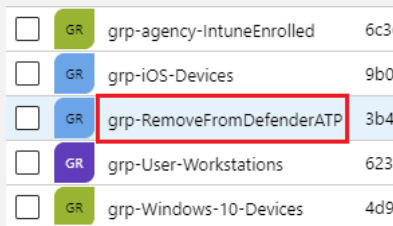
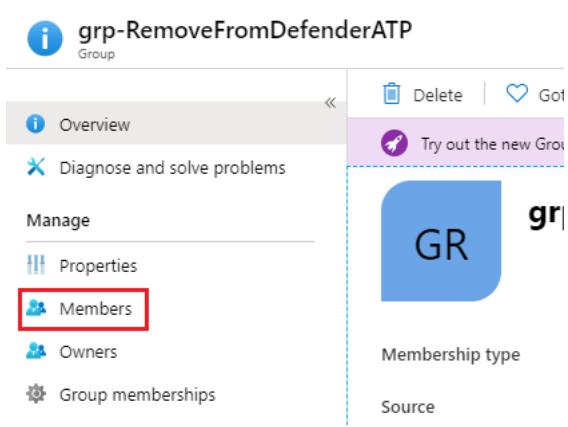
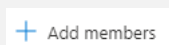
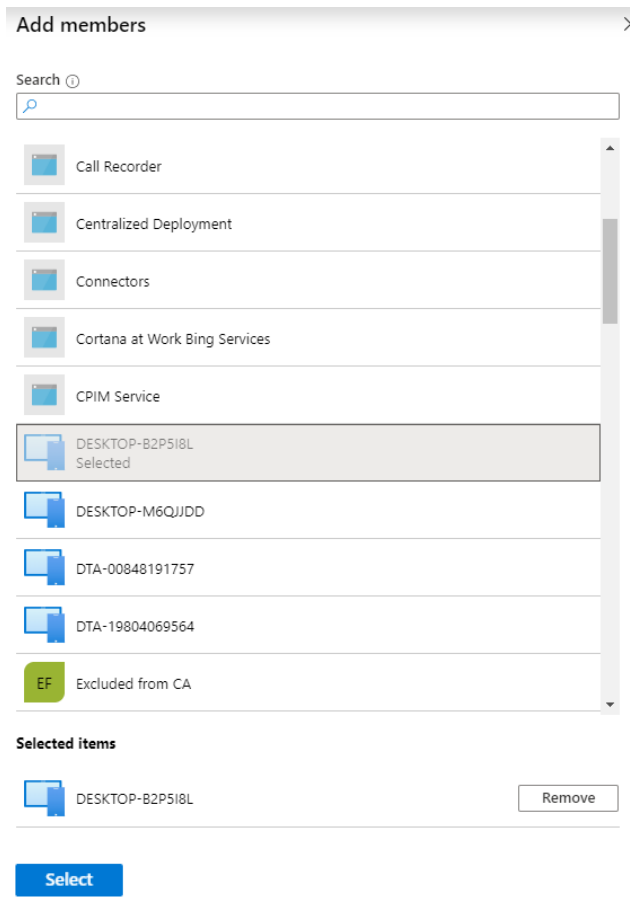
Steps	Instruction	Screenshot
5.	When prompted to download the package, click Download	
6.	When the package has downloaded, open the .zip file and extract the .cmd to the endpoint to be offboarded	
7.	From within this explorer window, click File > Open Windows PowerShell > Open Windows PowerShell as administrator . When prompted, enter your relevant administrative credentials	
8.	Once the PowerShell window launches, type cmd then press enter (this will launch command prompt within your PowerShell session)	
9.	Type “.” then press tab, the name of the .cmd script you have downloaded should autofill per the screenshot, then press Enter (Return)	
10.	Allow the script to run, once it has completed allow up to 24 hours for the offboarding to be complete and the results reflected in the portal. Note , the machine being offboarded does not need to be continuously online during this period.	No screenshot required

Offboard a Device from Microsoft Defender - Automated

Follow the below steps to offboard a device from Microsoft Defender ATP using the automated 'offboarding' process. These steps do not require that the device is available to be logged into and are recommended in the event a device is reported lost or stolen.

Table 5 Offboard a Device from Microsoft Defender - Automated

Steps	Instruction	Screenshot
1.	Within your internet browser navigate to the Azure Portal (https://portal.azure.com), then click on Azure Active Directory	
2.	Identify whether the device in question is a USER or ADMINISTRATOR device	No screenshot required
3.	In the left-hand pane, select Groups . Locate either the grp-Admin-Workstations or grp-User-Workstations group (as appropriate) and select it	
4.	In the left-hand pane, select Members	
5.	Within the list of direct members, locate the device in question, tick the box, then press Remove	
6.	When prompted to remove the selected member(s), click Yes	

Steps	Instruction	Screenshot
7.	Navigate back to the Groups – All groups blade, then select grp-RemoveFromDefenderATP	
8.	Within the grp-RemoveFromDefenderATP select Members	
9.	Click Add members	
10.	Identify your device from the list, or use the Search bar, then press Select	

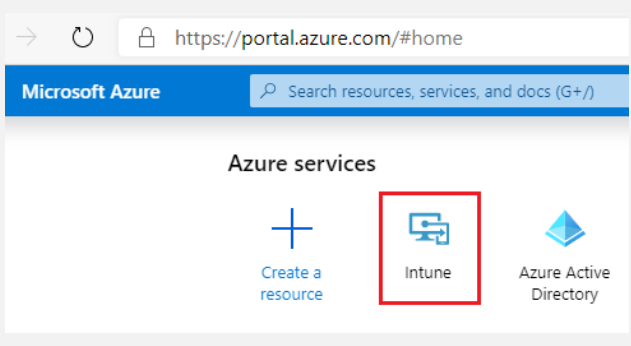
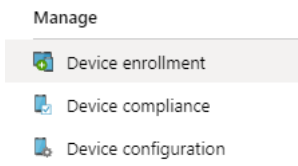
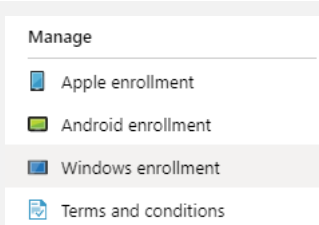
Steps	Instruction	Screenshot
11.	Allow some time for the process to complete, it can take some time as it relies on the device syncing back up with Azure.	No screenshot required

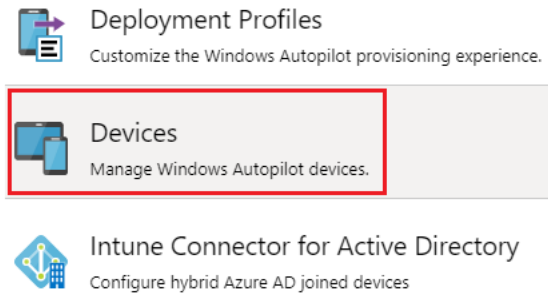
Note: this process could take some time as the endpoint device may be switched off, or not have an internet connection. Additionally, the logs for the device will remain in the Security Center by design.

Remove Device from Autopilot

As a prerequisite to this step, you must first delete the device from Azure Active Directory and Intune. Once these steps have been completed the device will not be able to be rebuilt using Autopilot.

Table 6 Remove Device from Autopilot

Steps	Instruction	Screenshot
1.	Within your internet browser navigate to the Azure Portal (https://portal.azure.com), then select Intune	
2.	In the left-hand pane, select Device enrollment	
3.	Within Device enrollment , select Windows enrollment	

Steps	Instruction	Screenshot																		
4.	Within the Windows enrollment blade, select Devices under the Windows Autopilot Deployment Program section	<p>Windows Autopilot Deployment Program</p>  <p>Deployment Profiles Customize the Windows Autopilot provisioning experience.</p> <p>Devices Manage Windows Autopilot devices.</p> <p>Intune Connector for Active Directory Configure hybrid Azure AD joined devices</p>																		
5.	<p>Within the Windows Autopilot devices screen, identify the device in question from the list or by using the search field.</p> <p>Once identified, tick the box next to the device, then press Delete</p>	<p>Windows Autopilot devices</p> <p>Windows enrollment</p> <p>Sync Filter Import Export Assign user Refresh Delete</p> <p>Last sync request : 1/09/20, 10:10 AM</p> <p>Windows Autopilot lets you customize the out-of-box experience (OOBE) for your users.</p> <p>Search by serial number</p> <table border="1"> <thead> <tr> <th>Serial number</th><th>Manufacturer</th><th>Model</th></tr> </thead> <tbody> <tr> <td><input type="checkbox"/> 000848191757</td><td>Microsoft Corporation</td><td>Surface Book 2</td></tr> <tr> <td><input type="checkbox"/> 0945-2527-6262-4291-9804-0695-64</td><td>Microsoft Corporation</td><td>Virtual Machine</td></tr> <tr> <td><input type="checkbox"/> 2196-9507-8707-3652-6719-0684-92</td><td>Microsoft Corporation</td><td>Virtual Machine</td></tr> <tr> <td><input checked="" type="checkbox"/> 7128-0670-3001-4762-8972-4121-57</td><td>Microsoft Corporation</td><td>Virtual Machine</td></tr> <tr> <td><input type="checkbox"/> 7256-0794-8797-9172-0372-8599-65</td><td>Microsoft Corporation</td><td>Virtual Machine</td></tr> </tbody> </table>	Serial number	Manufacturer	Model	<input type="checkbox"/> 000848191757	Microsoft Corporation	Surface Book 2	<input type="checkbox"/> 0945-2527-6262-4291-9804-0695-64	Microsoft Corporation	Virtual Machine	<input type="checkbox"/> 2196-9507-8707-3652-6719-0684-92	Microsoft Corporation	Virtual Machine	<input checked="" type="checkbox"/> 7128-0670-3001-4762-8972-4121-57	Microsoft Corporation	Virtual Machine	<input type="checkbox"/> 7256-0794-8797-9172-0372-8599-65	Microsoft Corporation	Virtual Machine
Serial number	Manufacturer	Model																		
<input type="checkbox"/> 000848191757	Microsoft Corporation	Surface Book 2																		
<input type="checkbox"/> 0945-2527-6262-4291-9804-0695-64	Microsoft Corporation	Virtual Machine																		
<input type="checkbox"/> 2196-9507-8707-3652-6719-0684-92	Microsoft Corporation	Virtual Machine																		
<input checked="" type="checkbox"/> 7128-0670-3001-4762-8972-4121-57	Microsoft Corporation	Virtual Machine																		
<input type="checkbox"/> 7256-0794-8797-9172-0372-8599-65	Microsoft Corporation	Virtual Machine																		
<p>Note: if you require further information about the device, you can click on it, a pane should appear on the right with further information about that specific device.</p>																				
6.	When prompted to delete, press Yes	<p>Are you sure you want to delete the selected devices? (1 selected)</p> <p>Note that only devices that are not enrolled will be deleted.</p> <p>Yes No</p>																		
7.	Confirm that the process has completed successfully in the Notifications button in the top right of the screen.	No screenshot required.																		

Abbreviations and Acronyms

Table 7 details the abbreviations and acronyms used throughout this document.

Table 7 Abbreviations and Acronyms

Acronym	Meaning
ATP	Advanced Threat Protection
Azure AD	Azure Active Directory
DTA	Digital Transformation Agency
SOP	Standard Operating Procedure