

# Hybrid standard operating procedures

2021-05-04

## Device onboarding

The authorisation and approval of users being granted access to the system is out of scope of this Standard Operating Procedure (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.

## 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.

## 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 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 licencing.

**Step 1** Within your internet browser navigate to the Microsoft 365 admin center (<https://admin.microsoft.com>)

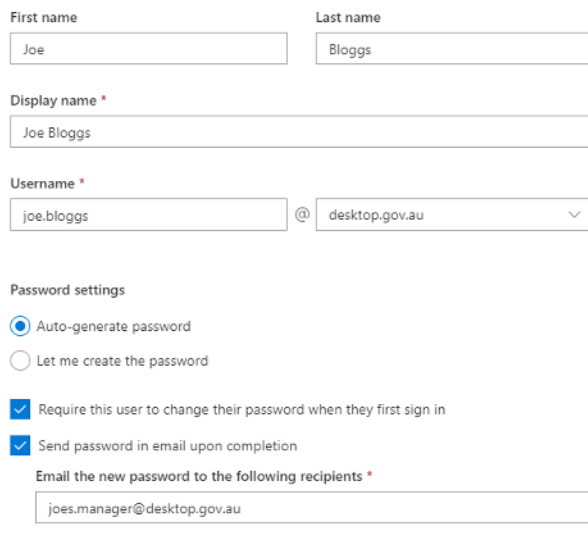
**Step 2** On the left-hand pane click **Users** then **Active users**

**Step 3** Click **Add a user**

**Step 4** The **Set up the basics** window will appear, complete all fields as shown in the screenshot.

### 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

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**

**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.

**Step 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**

**Step 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**

**Step 7** Review the user to be created and ensure all of the details you have entered are correct.

When complete press **Finish adding**

**Step 8** The account has now been created, press the **Close** button.

**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 Microsoft Endpoint Manager 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 Microsoft Endpoint Manager admin center.

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.

**Step 1** Navigate to the **Microsoft Endpoint Manager admin center** (<https://endpoint.microsoft.com/>) then select **Devices**

**Step 2** Within **Devices**, on the left-hand pane, select **Enroll Devices**

**Step 3** Within **Enroll Devices**, select **Windows enrollment** from the left-hand pane

**Step 4** Within the **Enroll Devices – Windows enrollment** blade, select **Devices** under the **Windows Autopilot Deployment Program** section

**Step 5** Within the **Windows Autopilot devices** screen, press the **Import** button

**Step 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.

**Step 7** Review whether the results are correct, and the rows are formatted correctly, if so, press **Import**

**Step 8** Allow the import to complete, note whether it has completed successfully via the **Notifications** bell icon in the top right of the screen.

### 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 describes how to add a device to a group.

**Step 1** Navigate to the Azure portal (<https://portal.azure.com>) then select Azure Active Directory

**Step 2** In the left-hand pane, click **Groups**

**Step 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**

**Step 4** In the left hand-pane, click on **Members**

**Step 5** Along the top ribbon, click **Add members**

**Step 6** In the pane that appears on the right of the screen, identify the devices to be added, click on them, then press **Select**

**Step 7** Ensure the device has been added to the group via the **Notifications** icon in the top right of the screen.

## 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 Microsoft Endpoint Manager (formerly Intune),
- Removal from Microsoft Defender Security Center, and
- Removed as a Windows Autopilot device.

## 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.

## Account disable

Depending on the Agency and security practices in place accounts may need to be disabled rather than deleted with the departure of a user from the Agency.

**Step 1** Within your internet browser navigate to the Microsoft 365 admin center (<https://admin.microsoft.com>)

**Step 2** On the left-hand pane click **Users** then **Active users**

**Step 3** Either by scrolling through the list, or using the search bar, identify the user and select them

**Step 4** With the user selected click on **Block sign-in** then tick the **Block this user from signing in** box

When complete press **Save changes** then the back arrow to return to the user

**Step 5** Select the **Licenses and Apps** tab on the user and **remove** any licenses that may be assigned to the user to ensure they are free for use for a new user

When complete press **Save changes**

**Note:** Allow up to one hour for any existing sessions to be completely logged out, new sign-ins are immediately blocked. Users Mail and OneDrive will remain intact in the event of an audit required

## Account deletion

Depending on the Agency and security practices in place accounts may need to be deleted rather than disabled with the departure of a user from the Agency.

**Step 1** Within your internet browser navigate to the Microsoft 365 admin center (<https://admin.microsoft.com>)

**Step 2** On the left-hand pane click Users then **Active users**

**Step 3** Either by scrolling through the list, or using the search bar, identify the user and select them

**Step 4** With the user selected click on **Delete user** then tick any requirements for the users Mail and OneDrive

When complete press **Delete user**

**Note:** Any assigned licenses will also be removed with this action

**Step 5** Confirmation will be provided for the account deletion

When complete press **Close**

**Step 6** The user will remain under **Deleted users** for 30 days where they can be restored if required

## 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.

**Step 1** Within your internet browser navigate to the Azure Portal (<https://portal.azure.com>), then click on **Azure Active Directory**

**Step 2** In the left-hand pane, select **Devices**

**Step 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**

**Step 4** When prompted to delete, press **Yes**

**Step 5** Confirm that the process has completed successfully in the **Notifications** button in the top right of the screen.

## Remove device from Microsoft Endpoint Manager

Complete the below steps to remove a device from Microsoft Endpoint Manager.

**Step 1** Within your internet browser navigate to the Microsoft Endpoint Manager admin center (<https://endpoint.microsoft.com/>), then click on **Devices**

**Step 2** Within the Devices blade, select **All devices**

**Step 3** Either by scrolling through the list, or using the search bar, identify your device, check the box, then press **Delete**

**Note,** Microsoft Endpoint Manager 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.

**Step 4** A blade will appear on the right of the screen, confirm that the device is correct, then press **Delete**

**Step 5** Confirm that the process has completed successfully in the **Notifications** button in the top right of the screen.

### 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.

**Step 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**)

**Step 2** Within the **Settings** screen, click on **Offboarding**

**Step 3** From the first dropdown menu, select **Windows 10**

**Step 4** From the second dropdown menu, select **Local Script (for up to 10 machines)**, then click **Download package**

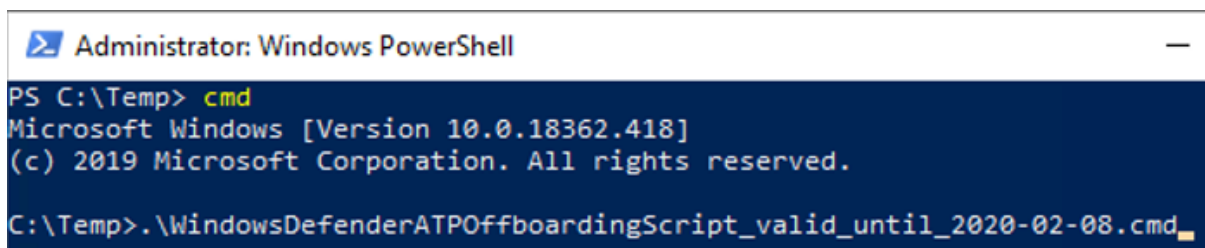
**Step 5** When prompted to download the package, click **Download**

**Step 6** When the package has downloaded, open the **.zip** file and extract the **.cmd** to the endpoint to be offboarded

**Step 7** From within this explorer window on the endpoint to be offboarded, click **File > Open Windows PowerShell > Open Windows PowerShell as administrator**. When prompted, enter your relevant administrative credentials

**Step 8** Once the PowerShell window launches, type **cmd** then press enter (this will launch command prompt within your PowerShell session)

**Step 9** Type **.\** then press tab, the name of the **.cmd** script you have downloaded should autofill per the screenshot, then press **Enter (Return)**



```
Administrator: Windows PowerShell
PS C:\Temp> cmd
Microsoft Windows [Version 10.0.18362.418]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\Temp>.\WindowsDefenderATPOffboardingScript_valid_until_2020-02-08.cmd
```

**Step 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.

### 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.

**Step 1** Within your internet browser navigate to the Azure Portal (<https://portal.azure.com>), then click on **Azure Active Directory**

**Step 2** Identify whether the device in question is a **USER** or **ADMINISTRATOR** device

**Step 3** In the left-hand pane, select **Groups**. Locate either the **grp-Admin-Workstations** or **grp-User-Workstations** group (as appropriate) and select it

**Step 4** In the left-hand pane, select **Members**

**Step 5** Within the list of direct members, locate the device in question, tick the box, then press **Remove**

**Step 6** When prompted to remove the selected member(s), click **Yes**

**Step 7** Navigate back to the **Groups – All groups** blade, then select **grp-RemoveFromDefenderATP**

**Step 8** Within the **grp-RemoveFromDefenderATP** select **Members**

**Step 9** Click **Add members**

**Step 10** Identify your device from the list, or use the Search bar, then press **Select**

**Step 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.

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 Microsoft Endpoint Manager. Once these steps have been completed the device will not be able to be rebuilt using Autopilot.

**Step 1** Within your internet browser navigate to the Azure Portal (<https://endpoint.microsoft.com>), then select **Devices**

**Step 2** In the left-hand pane, select **Device enrollment**

**Step 3** Within **Enroll Devices**, select **Windows enrollment**

**Step 4** Within the **Enrol Devices, Windows enrollment** blade, select **Devices** under the **Windows Autopilot Deployment Program** section

**Step 5** Within the **Windows Autopilot devices** screen, identify the device in question from the list or by using the search field.

Once identified, tick the box next to the device, then press **Delete**

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.

**Step 6** When prompted to delete, press **Yes**

**Step 7** Confirm that the process has completed successfully in the **Notifications** button in the top right of the screen.

## Remote wiping a device

A remote wipe of a device may be required in the event of a lost or stolen device and can be used as a last resort effort to secure the device. In order for the remote wipe to work correctly the device will need to have been powered on with internet access back to the tenant.

**Step 1** Within your internet browser navigate to the Microsoft Endpoint Manager admin center (<https://endpoint.microsoft.com>), then select **Devices**

**Step 2** Select **All Devices**

**Step 3** Either by scrolling through the list, or using the search bar, identify the device

Once identified click on the device

**Step 4** With the device selected you should now be able to select **Wipe**

**Step 5** For Windows 10 1709 and above devices the **Wipe device, but keep enrollment state and associated user account** can be used to keep certain data on the device. Not all data is retained.

**Step 6** **Wipe device and continue to wipe even if device loses power** can be used to ensure that the wipe is not circumvented by power cycling the device

In some instances this setting could render the device unable to power on correctly and should be used with some level of caution

**Step 7** When ready to confirm the wipe select **Yes**

The device should receive the wipe action within 15 minutes of confirmation

## USB device control

USB device control should be utilised to limit the use to USB ports on a Windows 10 device. Limiting users ability to use USB ports and devices ensures that the environment is not exposed to unwanted malicious content from untrusted sources as well as reduces the likelihood that a trusted insider is able to remove confidential material.

There are a number of methods that can be utilised from fully restricting USB ports, to restricting untrusted processes as well as trusting/denying specific devices.

### 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 Microsoft Azure.

### Blocking removable storage

The following describes the steps required to create an Microsoft Endpoint Manager profile that will block removable devices from use on a Windows 10 device.

**Step 1** Navigate to the Microsoft Endpoint Manager admin center (<https://endpoint.microsoft.com/>) then click on **Devices**

**Step 2** Within **Devices** click on **Configuration profiles**

**Step 3** Along the top ribbon, click **Create Profile**



**Step 4** The **Create a profile** blade will open, select **Windows 10 and later** platform and **Device restrictions** profile

When complete press **Create**

**Step 5** Enter an appropriate **Name** and **Description**.

When complete press **Next**

**Step 6** When presented with the **Device Configuration settings** screen expand **General** and select **Removable storage** and **USB connection** to ensure that they are set to **Block** then press **Next**

Note: **Removable storage** will block the use of removable storage devices within Windows, while **USB connection** will block USB ports on the device. **USB connection** setting will not block the use of USB charging though.

**Step 7** When presented with the **Assignments** screen select the groups that this profile is to be applied to.

In this example the update ring will apply to **rol-Agency-Administrators**, and **rol-Agency-Users**.

When complete, press **Next**

**Step 8** When presented with the **Applicability Rules** screen create an appropriate rule that this profile is to be applied to.

In this example they have been left blank

When complete, press **Next**

**Step 9** On the **Review + create** screen ensure that all of the settings are correct, if you're confident that they are, press **Create**

**Step 10** To confirm that these settings have been applied to an endpoint, plug in a USB device in to a Windows 10 device and ensure the USB device is blocked.

### **Blocking untrusted and unsigned processes running from USB**

USB devices may be allowed to be used within an Agency, however untrusted and unsigned process can be blocked to prevent infection. Alternatively, this setting can also be set to **Audit Only** to track the processes.

This will include executable files as well as script files.

Note: This will require Endpoint Protection running with real-time protection enabled.

**Step 1** Navigate to the Microsoft Endpoint Manager admin center (<https://endpoint.microsoft.com>) then click on **Devices**

**Step 2** Within **Devices** click on **Configuration profiles**

**Step 3** Along the top ribbon, click **Create Profile**

**Step 4** The **Create a profile** blade will open, select **Windows 10 and later** platform and **Endpoint Protection** profile

When complete press **Create**

**Step 5** Enter an appropriate **Name** and **Description**.

When complete press **Next**

**Step 6** When presented with the **Endpoint Protection settings** screen expand **Microsoft Defender Exploit Guard** and **Attack Surface Reduction** then select **Untrusted and unsigned process that run from USB** to ensure that it is set to **Block** then press **Next**

**Step 7** When presented with the **Assignments** screen select the groups that this profile is to be applied to.

In this example the update ring will apply to **rol-Agency-Administrators**, and **rol-Agency-Users**.  
When complete, press **Next**

**Step 8** When presented with the **Applicability Rules** screen create an appropriate rule that this profile is to be applied to.

In this example they have been left blank

When complete, press **Next**

**Step 9** On the **Review + create** screen ensure that all of the settings are correct, if you're confident that they are, press **Create**

**Step 10** To confirm that these settings have been applied to an endpoint, plug in a USB device in to a Windows 10 device and test running some executable and script files.

### **Allow or prevent installation of specific peripherals**

Allowing or preventing the installation of specific peripherals can allow more granular control of USB devices based off of their hardware ID's or their setup classes.

**Step 1** Navigate to the Microsoft Endpoint Manager admin center (<https://endpoint.microsoft.com>) then click on **Devices**

**Step 2** Within **Devices** click on **Configuration profiles**

**Step 3** Along the top ribbon, click **Create Profile**

**Step 4** The **Create a profile** blade will open, select **Windows 10 and later platform** and **Administrative Templates** profile

When complete press **Create**

**Step 5** Enter an appropriate **Name** and **Description**.

When complete press **Next**

**Step 6** When presented with the **Settings** screen expand **Computer Configuration/System/Device Installation/Device Installation Restrictions** then select the appropriate policy depending on the requirement.

In this example the **Allow installation of devices that match any of these device IDs** is being used

Note: When using an allow policy the **Prevent installation of devices not described by other policy settings** will also need to be set to ensure that only peripherals on the allow list can be used.

**Step 7** Select *Enable* and enter in the appropriate **device ID** or **setup class** depending on the policy in use

When complete press **OK** then **Next**

**Step 8** A **Scope tag** can be created if required

In this example they have been left as **Default**

When complete, press **Next**

**Step 9** When presented with the **Assignments** screen select the groups that this profile is to be applied to.

In this example the update ring will apply to **rol-Agency-Administrators**, and **rol-Agency-Users**.

When complete, press **Next**

**Step 10** On the **Review + create** screen ensure that all of the settings are correct, if you're confident that they are, press **Create**

**Step 11** To confirm that these settings have been applied to an endpoint, plug in a USB device in to a Windows 10 device that matches the policy that has been set and observe if it has been allowed or prevented depending on the policy that was set

## Microsoft Defender ATP

Microsoft Defender Advanced Threat Protection is a complete endpoint security solution powered by the Microsoft cloud. The following details a few of the functions that the product can be utilised for.

### 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 Microsoft Azure.
- Licensing for Microsoft Defender ATP is required.

### Advanced Hunting in Microsoft Defender ATP

Advanced hunting utilises a query-based approach to search for known or potential new threats to the environment.

**Step 1** Navigate to the Security Center (<https://securitycenter.windows.com/>) then click on **Advanced Hunting**

**Step 2** Click on **Query** which will allow custom queries to be written

**Step 3** The new **query** should be written in the text field

When the query is ready select **Run query**

**Step 4** Results will be displayed underneath the text box

**Step 5** The **Schema** section can be used to assist with building custom queries

**Step 6** The **Shared queries** section list a number of community based queries that can be used as starter queries or as if they meet the specific requirement

**Step 7** Custom queries can be saved using the **Save** button

**Step 8** Provide a name and save location for the query

**Step 9** Saved queries can be retrieved from **My queries** section

**Step 10** Queries can be used for detection by using the **Create detection rule**

Detection rules can be run on set intervals to proactively monitor for issues within the environment

**Step 11** Fill in the required details for the **Detection rule**

When ready click **Next**

**Step 12** Enable any required **Actions** as a result of the detection

When ready click **Next**

**Step 13** Review the **Summary** and validate the previously configured settings

When ready click **Create**

**Step 14** Any **Detection rules** will be available under the **Custom detections** section

**Step 15** When the **Detection rule** is opened the option to **Edit detection rule** will be available to change any details with the detection rule

## Windows Update for Business

Windows Update for Business is utilised for all Windows 10 endpoints within the tenant. It manages and deploys the latest security updates, Windows features, and patches by directly connecting to the Windows Update service. It also provides management capability for devices within the tenant.

Within the environment, updates are maintained and controlled by Update Rings. Update Rings have been deployed within the environment already however more may need to be created dependant on a number of factors such as what hardware and operating systems are supported.

### 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 Microsoft Azure.

### Create update ring

The following describes the steps required to create a Windows 10 update ring.

**Step 1** Navigate to the Microsoft Endpoint Manager admin center (<https://endpoint.microsoft.com>) then click on **Devices**

**Step 2** Within **Devices** click on **Windows 10 updates rings**

**Step 3** Along the top ribbon, click **Create**

**Step 4** The **Create Windows 10 update ring** blade will open, enter an appropriate **Name** and **Description**.

When complete press **Next**

**Step 5** When presented with the **Update ring settings** screen select the appropriate settings then press **Next**

**Step 6** When presented with the **Assignments** screen select the groups that this update ring is to be applied to.

In this example the update ring will apply to **rol-Agency-Administrators**, and **rol-Agency-Users**.

When complete, press **Next**

**Step 7** On the **Review + create** screen ensure that all of the settings are correct, if you're confident that they are, press **Create**

**Step 8** To confirm that these settings have been applied to an endpoint, navigate to **Settings > Update & Settings > Advanced Options** on a Windows 10 device and ensure the settings match your update ring.

## Manage update ring

Update rings are able to be modified, this includes settings within the update ring itself, as well as assignments. The following explains how to complete these changes.

**Step 1** Navigate to the Microsoft Endpoint Manager admin center (<https://endpoint.microsoft.com>) then click on **Devices**

**Step 2** Within **Devices** click on **Windows 10 updates rings**

**Step 3** Identify the update ring you wish to modify; in this instance it is **Semi Annual Channel Ring** then click on it

**Step 4** Within **Semi Annual Channel Ring**, click on **Properties**

**Step 5** Within the **Properties** screen there are 3 sections that can be modified:

- Basics
- Update ring settings
- Assignments

Identify what needs to be adjusted, then press the **Edit** button to adjust.

**Step 6** Within the edit window, make the required changes then click **Review + save** when complete

## Litigation hold

There are a number of methods that can be employed to place a mailbox on litigation hold. Two examples have been provided to show different ways of enabling litigation hold.

## 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 Exchange Online and/or Office 365.
- An understanding of PowerShell in an Office 365 and/or Azure context.
- An administrative account with the required permissions, including to install the Exchange Online PowerShell Module.
- The administrator performing these steps may need to be a member of the Organization Management or Role Management roles to be able to perform the steps in the Assign eDiscovery Permissions section.

## PowerShell litigation hold

This example explains how to place a single users' mailbox on litigation hold via PowerShell.

Please note that these steps require the Exchange Online PowerShell Module to be installed by an authorised administrator.

**Step 1** Launch the Microsoft Exchange Online PowerShell module

**Step 2** Connect to the tenant using the following command:

```
Connect-EXOPSSession -UserPrincipalName your.name@desktop.gov.au
```

**Step 3** A pop-up window will appear asking for your password, enter it and press Sign in.

You will also be requested for a MFA challenge response, accept it, the pop-up window will close when authentication is successful.

**Step 4** Run the following command to place a mailbox on litigation hold:

```
Set-Mailbox user.name@desktop.gov.au -LitigationHoldEnabled $true -LitigationHoldDuration 365
```

**Step 5** Run the following command to put all mailboxes in the tenant in litigation mode:

```
Get-Mailbox -ResultSize Unlimited -Filter {RecipientTypeDetails -eq "UserMailbox"} | Set-Mailbox -Li
```

**Step 6** When complete, close your session with the following command:

```
Remove-PSSession
```

## Web interface litigation hold

This example explains how to place a single users' mailbox on litigation hold via the Exchange Admin Center (EAC) web interface.

**Step 1** Log into the Exchange Admin center at <https://outlook.office365.com/>

**Step 2** On the **Dashboard**, click on **mailboxes** under the **recipients** heading

**Step 3** Within the **mailboxes** screen, identify the mailbox to be placed on litigation hold then double click it.

**Step 4** A pop-up window will appear, when it does, select **mailbox features** from the left-hand pane

**Step 5** Within **mailbox features**, scroll down until you see the **Litigation hold** section and enable/disable as required

**Step 6** If enabling litigation hold, please note that you will be prompted to enter the following:

- Litigation hold duration (days)
- A note/description for the hold
- A URL to direct users to for further information

## Assign eDiscovery permissions

The following describes the steps required to modify **eDiscovery Manager** permissions within the tenant.

**Step 1** Navigate to the Office 365 Security & compliance Center (<https://protection.office.com/>)

**Step 2** In the left-hand pane, click on **Permissions**

**Step 3** Within the **Permissions** window, tick the **eDiscovery Manager** checkbox

**Step 4** Within the **eDiscovery Manager** pane that appears, make any changes that are required.

Within this pane, you are able to assign an **eDiscovery Manager**, and **eDiscovery Administrator**, modify the existing assigned roles

### Create eDiscovery case

The following describes how to create a new eDiscovery case within the Microsoft 365 Compliance Center.

**Step 1** Navigate to the Microsoft 365 Compliance Center (<https://compliance.microsoft.com/>)

**Step 2** In the left-hand pane, select **eDiscovery**, then click on **Core**

**Step 3** Within the **Core eDiscovery** screen click the **Create a case** button

**Step 4** In the pane that appears on the right of the window, enter a **Case name** and **Case description** then press **Save**

### Manage eDiscovery case

The following describes how to manage an existing eDiscovery case within the Microsoft 365 Compliance Center.

**Step 1** Navigate to the Microsoft 365 Compliance Center (<https://compliance.microsoft.com/>)

**Step 2** In the left-hand pane, select **eDiscovery**, then click on **Core**

**Step 3** Within the **Core eDiscovery** window, identify your case, then click on it

**Step 4** The **Manage this case** window will appear, within it you can manage members, role groups, and the case status. You can also close or delete the case.

When these changes have been made, press either **Save** or **Close**

**Step 5** Back in the **Core eDiscovery** screen, check the radio tick box for your case then press **Open case**

**Step 6** A new browser tab will open, within it you can view holds, perform searches, and perform exports.

## System configuration restoration

The solution is primarily cloud based, and as such the systems and services used to support it have been configured in the various portals that comprise the Microsoft Office 365 and Microsoft Azure platforms.

The services and settings provided by the HybridSystem should not be modified without fully understanding the security and operational consequence of the change.

If there have been changes (authorised or otherwise) that need to be rolled back or reverted, the original As-Built As-Configured (ABAC) documents are to be referenced as a gold-source.

### 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 Microsoft Azure and Office 365.

## ABAC restore

When a system or service must be restored to its original state, the relevant ABAC document should be referred to and used to reconfigure the system or service back to its intended working order.

The following is an example of how to restore settings to the original HybridSystem build state within Azure Active Directory (Azure AD). In this scenario the LinkedIn account connections setting has been adjusted and is being reset.

**Step 1** Log into the Microsoft Azure portal, then select **Azure Active Directory**

<https://portal.azure.com/>

**Step 2** Additionally, open the corresponding ABAC. In this instance, the ABAC in question is DTA – Platform – ABAC.

**Step 3** Review the original ABAC, specifically looking for the settings in question.

**Step 4** Identify the setting within the ABAC and ensure that it is configured correctly within the portal.

Note: In the above example the LinkedIn account connections setting has been adjusted, this will of course change based on the service/system in question and this should only be used as an example.

## Important file restoration

All data that is considered important will be stored in a corporate data store, such as OneDrive for Business, SharePoint Online, or Exchange Online. As such, these locations are controlled by retention policies and can be configured to retain deleted items potentially indefinitely. Within the solution a number of retention policies have been created as a baseline, if identified by Agency or business, further can be created with the steps listed below.

### 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 Microsoft Azure and Office 365.

### Retention & backup policies

For full detail of the retention and backup policies employed within the tenant, the design documents and ABACs should be referred to. This example will show how to review and modify existing retention policies.

**Step 1** Navigate to the Microsoft 365 compliance portal (<https://compliance.microsoft.com>) then click on **Policies**

**Step 2** Within **Policies** click on **Retention**

**Step 3** Within the **Information governance** screen, you are able to create new retention policies, and modify existing policies.

In this example we will be modifying the **OneDrive Indefinite Hold** policy.

Open the policy by clicking on it.

**Step 4** Within the policy, review the existing settings then click on **Edit policy**

**Step 5** Within the **Policy name** screen, ensure there is a name and description for the policy in question.



**Step 6** Within the **Locations applied** screen, set the locations to be affected by this policy.

**Step 7** Within the **Policy settings** screen set how long the data is to be retained for.

Press **Save** to ensure settings across the 3 aforementioned sections are saved.

### **OneDrive data restoration**

Data saved to OneDrive for Business is saved indefinitely, if data is deleted it can be restored by various methods based on where it was deleted from.

If a file is located on a user's device in their OneDrive for Business folder, it can simply be restored from the Recycling Bin.

Note: deleted folders do not end up in the Computer Recycle Bin, only files. Additionally, sync must be configured in OneDrive for Business on the user's device, if not, restoring from the Computer Recycle Bin will not work.

Files can also be restored from the OneDrive web interface by following the steps outlined below.

**Step 1** Log into OneDrive through the web interface by visiting the Office 365 portal ([www.office.com](http://www.office.com)) then clicking on **OneDrive**

**Step 2** Within OneDrive, click on **Recycle bin**

**Step 3** Within the **Recycle bin** you will see data that has been deleted in the last 93 days

**Step 4** If the file you're looking for isn't in the Recycle bin, it may have been moved to the **Second-stage recycle bin**.

Click **Second-stage recycle bin** to access it

**Step 5** Within the **Recycle bin** or **Second-stage recycle bin** files can be restored by clicking on them then clicking **Restore** from the ribbon

**Step 6** This will restore the file to its original location, including files restored from the **Second-stage recycle bin**

### **SharePoint data restoration**

Data saved to SharePoint Online is saved indefinitely, if data is deleted however it can be restored by simply following the steps below.

Note: Teams data resides within a SharePoint site on the back-end, as such, this method can be used to restore Teams data as well as general SharePoint Online data.

**Step 1** Log into **SharePoint Online** through the web interface by visiting the Office 365 portal ([www.office.com](http://www.office.com)) then clicking on **SharePoint**

**Step 2** Click on the Site you wish to restore data to, in this example, it will be **Digital Transformation Agency**

**Step 3** From the Sites landing page, click on **Recycle bin**

**Step 4** Find your file, click on it, then press **Restore** to restore it to its original location

**Step 5** If you're unable to locate your file, check the **Second-stage recycle bin** by following the link at the bottom of the page.

## Mail restoration

The following sections detail how to restore archived data from the Outlook desktop and web applications.

### 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 Microsoft Azure and Office 365.

### Restore mail from archive (desktop)

If mail is Archived within the Outlook desktop application, it will initially appear within the **Archive** folder and can be restored by following the steps below.

**Step 1** Navigate to the **Archive** folder and select the email to be restored.

**Step 2** Drag and drop the mail item from the right-hand pane to the destination folder, in this example the item is being restored to the **Inbox**

**Step 3** Alternatively, the item can be right clicked, then moved via the **Move** option.

### Restore mail from archive (web application)

If mail is Archived within the Outlook Web application, it will initially appear within the Archive folder and can be restored by following the steps below.

**Step 1** Within the Outlook Web Application, navigate to the **Archive** folder

**Step 2** Drag and drop the mail item from the right-hand pane to the destination folder, in this example the item is being restored to the **Inbox**

**Step 3** Alternatively, the item can be right clicked, then moved via the **Move** option.

### Release mail from quarantine (user)

If a message has been quarantined from Outlook a user will be able to release certain types of types depending why it was quarantined. Typically, a user will be able release a message if it has been tagged as spam or bulk email.

Any messages being released from quarantine should be reviewed to ensure that they are not malicious.

**Step 1** Navigate to the Security & Compliance Center (<https://protection.office.com>) then click on **Threat management** then **Review**

**Step 2** Select **Quarantine** which will list any quarantined messages

**Step 3** Select the individual message which will list the information on the message

From here the message can be **Released**, **Previewed** or **Removed**

When ready select **Release message**

Note: Bulk messages up to 100 at a time can be selected here with bulk actions to release or remove available

**Step 4** The **Release messages & report them to Microsoft** confirmation screen will be presented.

Validate the details and select **Release message**

**Step 5** The message may take a few minutes to be release successfully after which a confirmation will be displayed

Select **Done**

**Step 6** The message should now be delivered to the user's mailbox

### **Release mail from quarantine (admin)**

If a message has been quarantined from Outlook and the user is unable to release the message, an Admin will be able to release all types of messages on behalf of the user. The process to release the message is identical to the user process, however the admin also has other options available to them to download or submit the message, as well as options to release to other users.

**Step 1** Navigate to the Security & Compliance Center (<https://protection.office.com>) then click on **Threat management** then **Review**

**Step 2** Select **Quarantine** which will list any quarantined messages

**Step 3** Select the individual message which will list the information on the message

From here the message can be **Released, Previewed, Removed, Downloaded** or **Submitted**

When ready select **Release message**

Note: Bulk messages up to 100 at a time can be selected here with bulk actions to release or remove available

**Step 4** The **Release messages & report them to Microsoft** confirmation screen will be presented.

Validate the details and select **Release message**

**Step 5** The message may take a few minutes to be release successfully after which a confirmation will be displayed

Select **Done**

**Step 6** The message should now be delivered to the user's mailbox

## **Data loss prevention**

Within the Microsoft 365 Compliance Center, Data Loss Prevention (DLP) policies can be configured to identify and protect Agency data and other sensitive information. DLP can be configured for multiple applications, such as:

- Exchange Online,
- SharePoint Online,
- OneDrive for Business, and
- Microsoft Teams.

The following sections describe how to maintain and manage DLP and its policies, including the creation of new policies.

### **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.
- Identified their sensitive info types, classification labels/types, and retention labels.

## Implement new policy

The following describes how to implement a new DLP policy.

This example describes the scenario where an Agency wants to implement a DLP rule to prevent emails or other information containing Australian driver's license numbers is not shared with unauthorised users.

**Step 1** Open an internet browser and navigate to the Microsoft 365 Compliance Center.

<https://compliance.microsoft.com/>

**Step 2** In the left-hand pane, click **Policies**

**Step 3** Within the **Policies** window, click on **Data loss prevention**

**Step 4** Within the **Data loss prevention** window, click **Create policy**

**Step 5** Click **Next**

**Step 6** On the **Name your policy** page, enter a **Name** and **Description**. Enter as detailed a description as possible.

When complete press **Next**

**Step 7** On the **Choose locations** page, select the relevant radio button based on what the policy is protecting.

When complete press **Next**

**Step 8** On the **Customize the type of content you want to protect** page, select the content type you wish to protect and where it is protected from.

In this example we are detecting Australian Driver's Licence Numbers when shared outside of the organisation.

When complete press **Next**

**Step 9** Select the appropriate settings on the next page as relevant to your policy.

When complete press **Next**

**Step 10** If prompted to customise access and override permissions, do so as appropriate

**Step 11** When prompted to turn the policy on, or test first, it is suggested to always test policies first – as such, select **I'd like to test it out first** then press **Next**

**Step 12** Review your settings, if they all look correct, click **Create**

**Step 13** Allow some time for the policy to run.

## Modify existing policy

The following describes the steps required to modify an existing DLP policy within the Microsoft 365 Compliance Center.

The default DLP settings provided by the HybridSystem should not be modified without fully understanding the security and operational consequence of the change.

**Step 1** Open an internet browser and navigate to the Microsoft 365 Compliance Center.

<https://compliance.microsoft.com/>

**Step 2** In the left-hand pane, click **Policies**

**Step 3** Within the **Policies** window, click on **Data loss prevention**

**Step 4** Within the **Data loss prevention** screen identify the policy you wish to modify, tick the radio button on its left, then click **Edit policy**

**Step 5** When the editing pane shows up, make the required changes then press **Save**

## **BitLocker recovery**

BitLocker drive encryption is applied to all Agency devices upon first login via a set of pre-defined Microsoft Endpoint Manager policies. BitLocker drive encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned devices.

### **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 Microsoft Azure.
- The appropriate permissions within Microsoft Endpoint Manager.
- The ID/asset number of the device in question.
- Physical or phone contact with the owner of the endpoint device that requires the recovery key.
- Positive confirmation that the owner of the device using agency processes for identity verification.

### **Locate BitLocker recovery key**

The following describes how to locate a BitLocker recovery key.

**Step 1** Navigate to the Microsoft Endpoint Manager (<https://endpoint.microsoft.com/>) then click on **Devices**

**Step 2** Within **Devices** click on **All devices**

**Step 4** Identify the device in question, or use the search bar to find it via the device ID, Asset number, or device name

**Step 5** Select **Recovery keys**

**Step 6** Provide the **BitLocker Recovery Key** to the user, or enter into the device that requires it