Australian Government
Digital Transformation Agency

BitLocker Recovery - Standard Operating Procedure

March 2020

dta

Contents

Document Overview

Background

Microsoft BitLocker is implemented on all laptops and computers using the Blueprint. BitLocker is a security feature that encrypts the device making the data inaccessible to prevent unauthorised access to the data stored on the device. If a user incorrectly enters their password and or username a certain number of times the device will lock and all data is encrypted. The device may be unlocked, and the data unencrypted by providing the device specific recovery key.

Document Audience

This Standard Operating Procedure (SOP) is intended to advise administrators how to recover a Digital Transformation Agency (DTA) Blueprint endpoint's BitLocker key ID and recovery key in the situation that a device must be 'unlocked'. It includes the required steps that a suitably trained administrator should follow to complete this task.

Purpose

The purpose of this document is to provide the necessary steps to locate BitLocker recovery keys.

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 Azure, specifically Intune.
- 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.

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

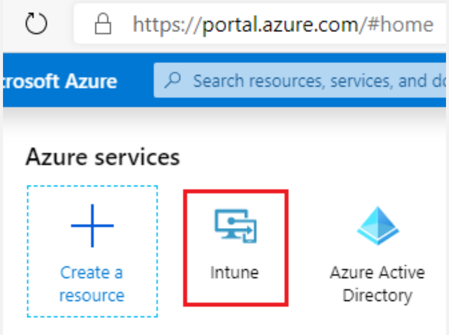
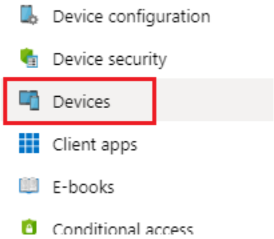
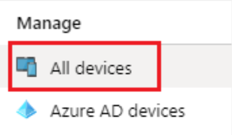
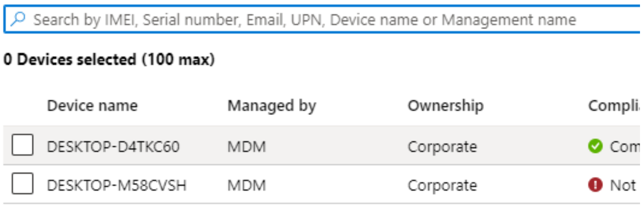
BitLocker Recovery

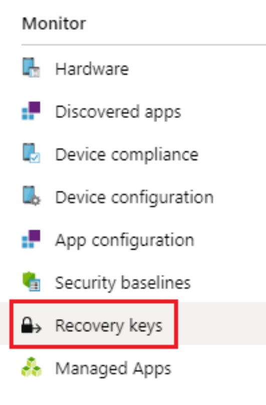
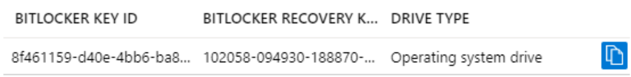
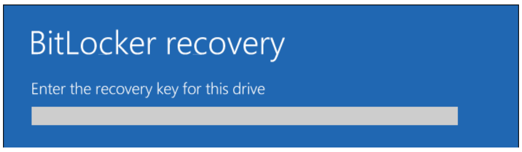
BitLocker drive encryption is applied to all Agency devices upon first login via a set of pre-defined Intune policies. BitLocker drive encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately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

Locate BitLocker Recovery Key

The following table describes how to locate a BitLocker recovery key.

Table 2 Locate BitLocker Recovery Key

Step	Instruction	Screenshot
1.	Navigate to the Azure Portal (https://portal.azure.com) then click on **Intune**	 https://portal.azure.com/#home rosoft Azure Search resources, services, and do Azure services Create a resource Intune Azure Active Directory
2.	Within **Intune** click on **Devices**	 Device configuration Device security Devices Client apps E-books Conditional access
3.	Within **Devices** click on **All devices**	
4.	Identify the device in question, or use the search bar to find it via the device ID, Asset number, or device name	 Search by IMEI, Serial number, Email, UPN, Device name or Management name **0 Devices selected (100 max)** Device name | Managed by | Ownership | Compli □ DESKTOP-D4TKC60 | MDM | Corporate | ✓ Com □ DESKTOP-M58CVSH | MDM | Corporate | ● Not

Step	Instruction	Screenshot
5.	Select **Recovery keys**	 Monitor Hardware Discovered apps Device compliance Device configuration App configuration Security baselines Recovery keys Managed Apps
6.	Provide the **BitLocker Recovery Key** to the user, or enter into the device that requires it	BITLOCKER KEY ID · BITLOCKER RECOVERY K... · DRIVE TYPE 8f461159-d40e-4bb6-ba8... · 102058-094930-188870-... · Operating system drive BitLocker recovery Enter the recovery key for this drive

Abbreviations and Acronyms

Table 3 details the abbreviations and acronyms used throughout this document.

Table 3 Abbreviations and Acronyms

Acronym	Meaning
DTA	Digital Transformation Agency
SOP	Standard Operating Procedure