



# Mobile Secure Data Management (Jamf) Solution Description

## Contents

A note on 'you' .....	2
Words defined in the General Terms .....	2
Part A – This Solution .....	2
1 Introduction .....	2
2 Overview .....	2
3 Solution Description .....	2
Part B – Service Delivery .....	4
4 Ordering Process .....	4
5 Implementation Process .....	4
6 Service Support .....	4
7 Online Help Centre .....	4
8 BT Support details .....	4
9 Service Operations .....	4
Disclaimer .....	6



## A note on 'you'

'You' and 'your' mean you.

## Words defined in the General Terms

Words that are capitalised but have not been defined in these Solution Terms have the meanings given to them in the General Terms, BT Mobile Schedule, Orders and BT Price Guide.

## Part A – This Solution

### 1 Introduction

- 1.1 This Solution Description forms part of your Contract with BT. Words and expressions used in this document will, unless the context requires otherwise, have the meaning given to them in, and be interpreted in accordance with, the EE Mobile Schedule and the Solution Terms for the Mobile Secure Data Management (Jamf) Solution.

### 2 Overview

- 2.1 The Solution provides Customers with real-time visibility and analytic capability of mobile and Wi-Fi data across Compatible Devices and applications. Customers have the ability to manage data usage and apply limits and restrictions to Users via the Management Portal. In addition to data management, the Solution can also protect Users' Compatible Devices from mobile security threats, such as malware, phishing and man-in-the-middle network attacks.
- 2.2 BT will work with its Subcontractor to provide the Solution to you and provide direct support to you in the set-up and in-life management of the Solution.

### 3 Solution Description

- 3.1 The Solution is made up of 3 components as set out below:
  - (1) Device Application Software, including Licencing Options;
  - (2) Management Portal; and
  - (3) Access to a Technical Help Desk.
- 3.2 **Device Application Software**
  - (a) The Device Application Software is installed on Compatible through the Management Portal or using EE's Enterprise Mobility Management ("EMM") solution (which is not provided through this Solution and is subject to separate terms).
  - (b) You can choose any of the following Licencing Options:
    - (i) Jamf Threat Defence
    - (ii) Jamf Threat Defence protects Compatible Devices against threats, such as malware, rogue or insecure applications, phishing, cryptojacking, data exfiltration and network attacks. Threats are detected at the endpoint via the Jamf Trust Compatible Device Application Software, and prevented in the network via Jamf Cloud. Additionally, Jamf Threat Defence helps to detect vulnerabilities, flags potential risks like outdated OS versions or risky configuration settings.
    - (iii) Jamf Data Capping  
Jamf Data Capping provides the Customer with controls to cap data usage by megabyte for domestic and roaming, Website whitelisting, data usage reports and cap reports.
    - (iv) Jamf Data Policy  
Jamf Data Policy provides web content filtering across all remote user traffic (both cellular and Wi-Fi) and data management features like tethering control, data capping and compression. The solution features installation of an endpoint application and remote user traffic routing via the Jamf Cloud.
    - (v) Jamf Private Access  
Jamf Private Access provides secure remote access to applications using Zero Trust Network Access (ZTNA) principles.
    - (vi) Jamf Now  
Jamf Now is a Unified Endpoint management (UEM) focused on small and medium businesses to help organizations set up, manage, and secure Apple devices.
    - (vii) Jamf Fundamentals  
Jamf Fundamentals extends the Jamf Now solution beyond Apple's MDM Framework, with capabilities for connecting, protecting, and empowering the small and medium business workforce.

- (viii) Jamf Pro  
Jamf Pro — the standard for Apple management — is a solution that delivers the best and most secure end user experience for Mac, iPad, iPhone and AppleTV devices.
  - (ix) Jamf Connect  
Jamf Connect reduces support challenges for IT and addresses address security concerns with modern authentication. The Mac Password Sync. feature synchronises Mac passwords across all devices and all applications with a single identity.
  - (x) Jamf Protect  
Jamf Protect is an enterprise endpoint security solution for MacOS. It allows Customers to create custom detections that protect computers with real-time monitoring for suspicious and unwanted activities, while measuring computers against the Center for Internet Security (CIS) benchmarks with security insights. Jamf Protect runs without using kernel extensions to support continuous MacOS updates and preserve the Apple user experience. Features include blocking cyber threats like phishing and malicious downloads before they can compromise users or devices, blocking command and control (C2) traffic as well as risky domains.
  - (xi) Jamf BYOD  
Jamf BYOD is a bring-your-own-device (BYOD) workflow that preserves personal privacy by preventing IT from having too much control over an employee's device. It addresses IT concerns by allowing them to adequately manage and secure the device while it's accessing company resources.
  - (xii) Jamf Traffic Stream  
Jamf Network Traffic Stream is an integration that enables organisations to stream, record and review all network activity that is processed by the Jamf Security Cloud infrastructure via third-party log aggregators and analytics tools.
- (c) Full details of the supported Compatible Devices can be found on the Management Portal help centre by searching for 'System Requirements' <https://www.jamf.com/resources/product-documentation/>.

### 3.3 Management Portal

- (a) The Management Portal will manage all aspects of the Solution, including:
  - (1) deployment of the Device Application Software on to Compatible Devices;
  - (2) adding, removing and maintaining Compatible;
  - (3) your policies and service settings;
- (b) a wide range of graphical and tabular reports for administrators Full details of Solution supported browsers can be found through the Management Portal help centre by searching for 'System Requirements' or online at <https://www.jamf.com/resources/product-documentation/>.

### 3.4 Product Dependencies

- (a) This product is not dependant on any another BT product but will benefit from using alongside EE's Enterprise Mobility Management Service which BT can provide to you under additional terms.



## Part B – Service Delivery

### 4 Ordering Process

4.1 You will contract with BT for the Solution and you will be billed on your BT bill.

### 5 Implementation Process

5.1 You will confirm your administration credentials to BT and BT will set you up with your Management Portal. Once provisioned, your administrator will receive an email with their login details for the Management Portal. At this point, the administrator can access the Management Portal and start enrolling Compatible Devices.

5.2 BT is able to support the set up of the Solution through BT's technical and support teams.

5.3 If you have purchased EMM through EE then the same technical delivery resource will be able to set up EMM and the Solution to ensure it is optimised to operate together.

### 6 Service Support

6.1 BT's support teams will provide:

(a) First line support which includes basic support for End Users queries and triage as appropriate:

(b) Second line support which includes investigation and resolution of incidents such as adding new devices to Management, exporting data from Management and configuration.

6.2 BT's Subcontractor's support team shall provide third line support outside of BT's first- and second-line support responsibilities.

6.3 This helpdesk is not a User's support team and therefore will only deal with queries from your nominated points of contact.

6.4 BT will continue to provide User support via their standard support process but if the issue relates specifically to the Solution then Users should contact their internal IT and admin teams prior to calls be raised with the specialist BT Solution support team.

### 7 Online Help Centre

7.1 Your administrators are provided with log in access to the Management Portal. The Management Portal is designed to provide you with intuitive Device administration, incorporating a self-contained help centre that is accessible from the main dashboard. This includes information on frequently used functionality, release notes and tutorials to get the most from the Solution. From here, incidents can be raised and tracked with BT's Subcontractor support teams. Users are able to raise support tickets themselves from the management Portal.

7.2 Online resources including product documentation, best practice workflows, technical papers, and more can be accessed at <https://www.jamf.com/resources/>

7.3 For Apple IT managers, a Jamf National Community open platform is available at <https://www.jamf.com/community/jamf-nation/>

### 8 BT Support details

8.1 Support email: Jamf@ee.co.uk

8.2 Support phone: 0800 079 0163

### 9 Service Operations

#### 9.1 Incident Management

(a) Incidents are categorised on impact and urgency and the incident and problem management processes are aligned to the below:

**P1 – Critical:** Access to the Solution is lost for a substantial number of Compatible Devices. These requests must be logged via phone to ensure a prompt response.

**P2 – Major Incident:** One element of the Solution is unavailable or degraded but the Solution as a whole remains operational.

**P3 - Minor incident:** Any Incident that does not fall under the above two categories or a Service Request (administrative task)

#### 9.2 Service Maintenance

(a) From time to time, BT's Subcontractor may perform scheduled maintenance to update the servers and software that are used to provide BT and you with the Solution. BT's Subcontractor will make all



- reasonable attempts to notify BT and you at least ten business days in advance of any planned downtime or scheduled maintenance, to ensure you are aware of any possible service interruptions and impacts.
- (b) However, in certain situations, BT's Subcontractor may need to perform emergency maintenance without any advance notice.
  - (c) BT's Subcontractor may modify and update the features and functionality of the Solution. These updates may include any subsequent release or version of the Solution containing functional enhancements, extensions, error corrections or fixes which are generally made available at no additional cost to customers who have contracted for the appropriate Solution.
  - (d) BT's Subcontractor will ensure that any modifications or updates do not materially affect the performance or use of the Solution.



### Disclaimer

This document has been produced by BT and, unless the recipient of it has contracted with BT to take the Mobile Secure Data Management (Jamf) from BT Solution (in which case this document forms part of your Contract with BT), it is provided to the recipient solely for its information in order to assess the purchase or implementation of the Solution from BT (the "Purpose"). This document is strictly private and confidential between the recipient and BT and may only be shared with the recipient's employees, agents, advisors, subcontractors or suppliers as strictly necessary for the Purpose. This document may not be disclosed, used, reproduced or redistributed, in whole or in part, for any other purpose or to any other person or legal entity without the prior written consent of BT.

As between BT and the recipient, this document and all intellectual property in the document (including without limitation relating to its format and presentation) is, and shall remain the sole property of BT.

Whilst BT has taken care to ensure that the information contained in this document is accurate and up-to-date, it shall have no liability to any person or legal entity in respect of errors or omissions except as provided by law or as set out in your Contract with BT (where the recipient has contracted with BT to purchase the Mobile Secure Data Management (Jamf) from BT Solution).

By accepting this document, the recipient agrees to be bound by the above limitations.