Deployment Plan

M365B Secure Deployment Plan

Prepared for

NOTE: This is an early release preview. Please check [http://aka.ms/bsecure for the v1.0](http://aka.ms/bsecure%20for%20the%20v1.0) release.

[Type Customer Name Here]

7/10/2018

Version Draft

Prepared by

**[Author]**

[Type Author Position Here]

[Type Author Email Here]

Contributors

**[Type Contributors Here]**

MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation. Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, our provision of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property. The descriptions of other companies’ products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers. © 2018 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corp. is strictly prohibited. Microsoft Corp. is strictly prohibited. Microsoft, Microsoft Active Directory, Microsoft Hyper-V, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other products mentioned that are not trademarks include Microsoft Internet Information Services. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Revision and Signoff Sheet

Change Record

| Date | Author | Version | Change Reference |
| --- | --- | --- | --- |
|  |  | .1 | Initial draft for review/discussion |
|  |  |  |  |
|  |  |  |  |

Reviewers

| Name | Version Approved | Position | Date |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Overview 5](#_Toc518996765)

[2 Technical Design 6](#_Toc518996766)

[2.1 Set up and pre-requisite information 6](#_Toc518996767)

[2.2 Solution Design 6](#_Toc518996768)

[2.3 Design Decisions 8](#_Toc518996769)

[2.4 Deployment Activities and Tasks 9](#_Toc518996770)

[2.5 Verifying the Implementation 10](#_Toc518996771)

1. Overview

Provide an overall summary of the contents of this document. This should include the criteria by which the design was established and how it was validated. It should also clearly identify the intended audience.

Justification: Some project participants may need to know only the document’s highlights, and summarizing creates that user view. It also enables the full reader to know the essence of the document before they examine the details. Expand below on the customer architecture.

This document details the design and implementation of Microsoft 365 Business at Customer Name. The design meets the requirements and goals that were stated in the Statement of Work document.

The overall solution design describing both products is visualized in an architecture overview and explained in detail. After providing an overview of the in-scope infrastructure, general information about the prerequisites are given. The document also includes a general description of the implementation of the two products referring to the relevant documentation where necessary.

1. Technical Design

This chapter details the technical design of Microsoft 365 Business at Customer Name.

After providing information about the prerequisites which must be in place for a successful deployment of Microsoft 365 Business, the design is explained in detail. After that, all design decisions that were made during the Deployment Workshop which led to the design are documented.

* 1. Set up and pre-requisite information

Before starting the implementation of Microsoft 365 Business, several preparation steps must be in place. A current and up-to-date list of all prerequisites can be found on Microsoft Docs online:

* [Pre-requisites for protecting data on devices with Microsoft 365 Business](https://support.office.com/en-us/article/pre-requisites-for-protecting-data-on-devices-with-microsoft-365-business-7770e280-3a6c-436f-a157-b008a2744f51?ui=en-US&rs=en-US&ad=US)
	1. Solution Design

**Please adapt the design diagram to reflect the Microsoft 365 Business at your customer. Pick the drawing the best reflects their architecture (AADJ or Hybrid AADJ) and adapt it as needed.**

Figure 1 illustrates the solution design of Microsoft 365 Business. All design decisions which led to this solution design are listed in section 2.3: Design Decisions.



Figure 1: Solution Design of Microsoft 365 Business at Customer Name with Azure Active Directory domain joined devices



Figure 1: Solution Design of Microsoft 365 Business at Customer Name with Hybrid Azure Active Directory domain joined devices

* 1. Design Decisions

In this section all design decisions that led to the solution depicted in the previous section are documented. All design options are listed for reference and the choice and rationale that was made is documented in the right most column.

**Please customize all Design Decisions according to your need. Also, please be sure to include plenty of context with each decision (for example by also including the alternatives and marking the actual choices. This makes sure the customer can deduct the reasoning of the design at a later point in time. Don’t delete any of the design decisions even if they’re not applicable as they can provide context to the customer and serve as documentation.**

|  |  |  |
| --- | --- | --- |
| **Design Decision** | **Description** | **Choice and Rationale** |
|  | **M365B Tenant Security** |  |
|  | These will be the global administrator(s). |  |
|  | Custom permissions related to discovery or content search |  |
|  | Custom permissions related to security and compliance |  |
|  | Custom permissions related to email handling |  |
|  | All administrative accounts will/will not require multi-factor authentication? |  |
|  | **Custom Domains** |  |
|  | Domains will be used with M365B |  |
|  | Custom email routing for on-premises servers or other cloud services |  |
|  | On-premises email enabled devices |  |
|  | External email domains that require special considerations |  |
|  | **Users & Devices** |  |
|  | List user accounts |  |
|  | List organization owned device names & types |  |
|  | Personal devices will/will not be allowed and will/will not be enrolled in Intune. |  |
|  | **Cloud vs Hybrid Discovery** |  |
|  | Will customer maintain a Windows Server based Active Directory on premises? |  |
|  | Will devices be managed with Azure Active Directory (AAD) only or Hybrid AAD? |  |
|  | **Directory Synchronization** |  |
|  | Use Default AADC Settings? |  |
|  | Which UPN suffix will be used in a local AD? |  |
|  | **M365B Configuration** |  |
|  | Configure new tenant? |  |
|  | If existing tenant, what are tenant details? |  |
|  | If existing tenant, will all users migrate to Microsoft 365 Business? |  |
|  | Protect work files when devices are lost or stolen? |  |
|  | Force users to save all work files to OneDrive for Business? |  |
|  | Encrypt work files? |  |
|  | Require a PIN or fingerprint to access Office apps? |  |
|  | Reset PIN when login fails this many times? |  |
|  | Require users to sign in again after Office apps have been idle for (minutes)? |  |
|  | Deny access to work files on jailbroken or rooted devices? |  |
|  | Don’t’ allow users to copy content from Office apps into personal apps? |  |
|  | Help protect PCs from viruses and other threats using Windows Defender Antivirus? |  |
|  | Help protect PCs from web-based threats in Microsoft Edge? |  |
|  | Use rules that reduce the attack surface of devices? |  |
|  | Protect folders from threats such as ransomware? |  |
|  | Prevent network access to potentially malicious content on the Internet? |  |
|  | Help protect files and folders on PCs from unauthorized access with BitLocker? |  |
|  | Allow users to download apps from Microsoft Store? |  |
|  | Allow users to access Cortana? |  |
|  | Allow users to receive Windows tips and advertisements from Microsoft ? |  |
|  | Keep Windows 10 devices up to date automatically? |  |
|  | Turn off device screen when idle for 5 minutes? |  |
|  | Install Office on Windows 10 devices? |  |
|  | Create an organization wide ATP anti-phishing policy? |  |
|  | Create an organization wide ATP safe attachments policy? |  |
|  | Create an organization wide ATP safe links policy? |  |

* 1. Deployment Activities and Tasks

The best source for up-to-date deployment information for M365 Business is Microsoft’ public documentation site: [Get started with Microsoft 365 Business](https://support.office.com/en-us/article/get-started-with-microsoft-365-business-496e690b-b75d-4ff5-bf34-cc32905d0364?ui=en-US&rs=en-US&ad=US).

A Microsoft 365 Business deployment generally follows the flow described below:

|  |
| --- |
| **Step Description** |
| 1. [Get Microsoft Business](https://support.office.com/en-us/article/get-microsoft-365-business-5abfef7b-5957-484a-b06b-a7c55e013e44?ui=en-US&rs=en-US&ad=US)
 |
| 1. [Set up Microsoft 365 Business by using the setup wizard](https://support.office.com/en-us/article/set-up-microsoft-365-business-by-using-the-setup-wizard-6e7a2dfd-8ec4-4eb7-8390-3ee103e5fece?ui=en-US&rs=en-US&ad=US)
 |
| 1. [Mange Microsoft 365 Business](https://support.office.com/en-us/article/manage-microsoft-365-business-27ff1678-865a-4707-8145-e1155aa815d6?ui=en-US&rs=en-US&ad=US)
 |
| 1. Manage mobile devices
 |
| 1. Manage Windows 10 PCs
 |
| 1. Use AutoPilot to deploy Windows 10 devices (optional)
 |

**Use the following only if implementing Hybrid Azure Active Directory:**

If your customer currently has an Active Directory domain managing PCs, you may simply configure Hybrid Azure Active Directory to continue to manage the devices with AD and get the benefits on Intune device management.

For customers that do not have devices connected to an Active Directory domain, the simplest option is to join them directly to Azure Active Directory.

Configuration instructions for a Hybrid Azure Active Directory joined devices is a <https://aka.ms/hybridaadj>

This toolkit contains an addendum with step by step guidance for enabling Hybrid Azure Active Directory joined devices: <A1 - Microsoft 365 Business Secure Deployment Toolkit – Hybrid AADJ Addendum.docx>

* 1. Verifying the Implementation

After Microsoft 365 Business is deployed, you can validate it is working by performing a few simple steps.