Microsoft

Microsoft 365 Business Implementation Services Toolkit

Delivery Guide

http://aka.ms/m365bpartners

Table of Contents

Disclaimer

This Microsoft 365 Business Secure Deployment Toolkit is intended to assist organizations with the deployment and implementation of Microsoft 365 Business. This Microsoft 365 Business Secure Deployment Toolkit is provided for general public informational purposes only.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS MICROSOFT 365 BUSINESS SECURE DEPLOYMENT TOOLKIT. Microsoft disclaims any conditions, express or implied, or other terms that use of the Microsoft products or services will ensure the organization's compliance with the regulatory frameworks. This Microsoft 365 Business Secure Deployment Toolkit is provided "as-is." Information and recommendations expressed in this Microsoft 365 Business Secure Deployment Toolkit may change without notice.

This Microsoft 365 Business Secure Deployment Toolkit does not provide the user with any legal rights to any intellectual property in any Microsoft product or service. Use of the toolkit is for internal, reference purposes only; however, Microsoft partners may distribute the Microsoft 365 Business Secure Deployment Toolkit to their customers for such customers' internal, reference purposes only. Any distribution of the Microsoft 365 Business Secure Deployment Toolkit by a Microsoft partner to its customers must include terms consistent with those set forth in this disclaimer.

1 Introduction

Overview

The Microsoft 365 Business Secure Deployment Toolkit combines structured planning and implementation guidance with education and preparation of our partners and customers. This offer may be used as is by partners to quickly launch a service offering featuring Microsoft 365 Business or customized to combine their unique offers with this toolkit.

Who Should Read This Guide

This document is designed to assist the partner consultants and project managers responsible for delivering the offering. This document will also help partner business development managers understand how the offer is built and what is available for use before, during, and after an engagement.

How to Use This Guide

- This document will help partner consultants understand all deliverables they will produce as part of the offer, as well as the skills necessary to implement.
- This offering aims to make the partner led deployment of Microsoft 365 Business a high quality, predictable experience and leave the customers with valuable knowledge and documentation that will help them use the solution with confidence.
- The goals for the offer are to:
    - Assess the current security posture
    - Remediate high priority security concerns
    - Deploy Microsoft 365 Business
    - Configure advanced security features
    - Identify and protect sensitive data
    - Provide ongoing services
- The Engagement Delivery Guide is intended to guide you as the Microsoft partner and security expert, through a successful delivery of the offer using the structured approach that has been proven in the field with similar engagements.

2 Assumptions

The Engagement Delivery Guide makes the following assumptions:

- The partner has completed the business development process
- The customer will meet Microsoft 365 Business requirements/restrictions
- The customer can meet the Internet connectivity requirements to use the service
- The partner consultants will meet or exceed the experience and knowledge requirements outlined in this guide

- The partner consultants will provide feedback via Yammer to improve the overall quality of this material after an engagement takes place.

Engagement The following table identifies the main information categories for the delivery of the offer.

Table 1: Engagement delivery overview

Category	Description	
Timeline	Task Name	Duration
	Partner Delivery Phases	**5-10 days**
	Identify & Assess Security Gaps	1 day
	Deploy Microsoft 365 Business	1 day
	Enable Proactive Security	1 day
	Migrate Email & Files (Optional)	1-6 days
	Identify & Protect Sensitive Data	1 day
Resourcing	Resource Name	
	Senior Consultant	
	Project Manager	
Cost	Cost will vary based on partner rates for the above resources.	
Engagement scope	• Inform Customers on the importance of security and how Microsoft approaches security. • Gain a better understanding of customer goals and vision for the future pertaining to their detection strategy. • Guide the customer to optimize their response plan by understanding what the solutions detects. • Deploy the various products in the Microsoft Advanced Threat Detection Implementation Services offering as a threat detection and protection service for customers.	
Target audience	Project manager, project sponsors, technical decision makers, and customer security and IT personnel.	
Participant prerequisites for workshops	Participants should be technical leaders and influencers capable of and responsible for overseeing the delivery of tasks related to security and IT operations.	

3 Recommended Consultant Training and Experience

The offer is delivered by the following key skillsets:

- Cyber/Security
- Identity & Access
- Device Management
- Email & Migration
  Data Governance

These skillsets can exist in one adequately qualified resource, or two resources can be leveraged. The following table described the skillset required by the delivery consultants:

Table 2: Consultant experience requirements

Functional Group	Consultant Experience Requirements
General	Delivered M365BIS engagements before or has extensive knowledge of the solution. Completed the activities in the M365B lab guide as part of this toolkit Understands scripting with PowerShell Understand Microsoft secure score
Cybersecurity	Familiar with the Cybersecurity Framework Core elements of Protect, Detect, Response Familiarity with Microsoft 365 Business online documentation Understands threat intelligence Read and understand Pass-the-Hash whitepapers v1 and v2 Microsoft Security Bulletin MS14-068 – Critical Brute Force Attacks Skeleton Key Malware Remote Code Execution
Identity and Access	Familiar with Role Based Access Control (RBAC) Understands identity and access management methodologies Familiar with Azure AD Connect Familiar with AD Group Policy
Device Management	Understands endpoint security Familiar with Intune
Email & Migration	Understands SMTP and ESMTP at the protocol level Understands DSNs and NDRs, including enhanced status codes Can read and analyze SMTP protocol headers and traces Understands how to create and modify DNS records Understands how to configure mail flow in Office 365 Understands how to secure mail flow in Office 365 Understands Exchange Online Protection capabilities Understands Office 365 ATP capabilities Understands email borne threat landscape such as Phish, Spear, and targeted malware Can test SMTP with telnet or Microsoft Remote Connectivity Analyzer
Data Governance	Familiar with regulations such as HIPAA & GDPR Familiar with security frameworks such as NIST 800-53 & ISO 27001:2013 Understands Azure Information Protection Understand Office 365 Data Loss Prevention

4 Prerequisites

- The partner with produce a specific statement of work (SOW) that provides guidelines for the engagement and should be reviewed in detail before the kickoff meeting.
- The customer kickoff presentation provides a template for the engagement kickoff meeting structure
- The kickoff meeting provides the opportunity to officially start the engagement, educate the customer on Microsoft 365 Business capabilities, and gather necessary information.

5 Pre-Engagement Tasks

Prior to kicking off this engagement, the following steps should be completed:

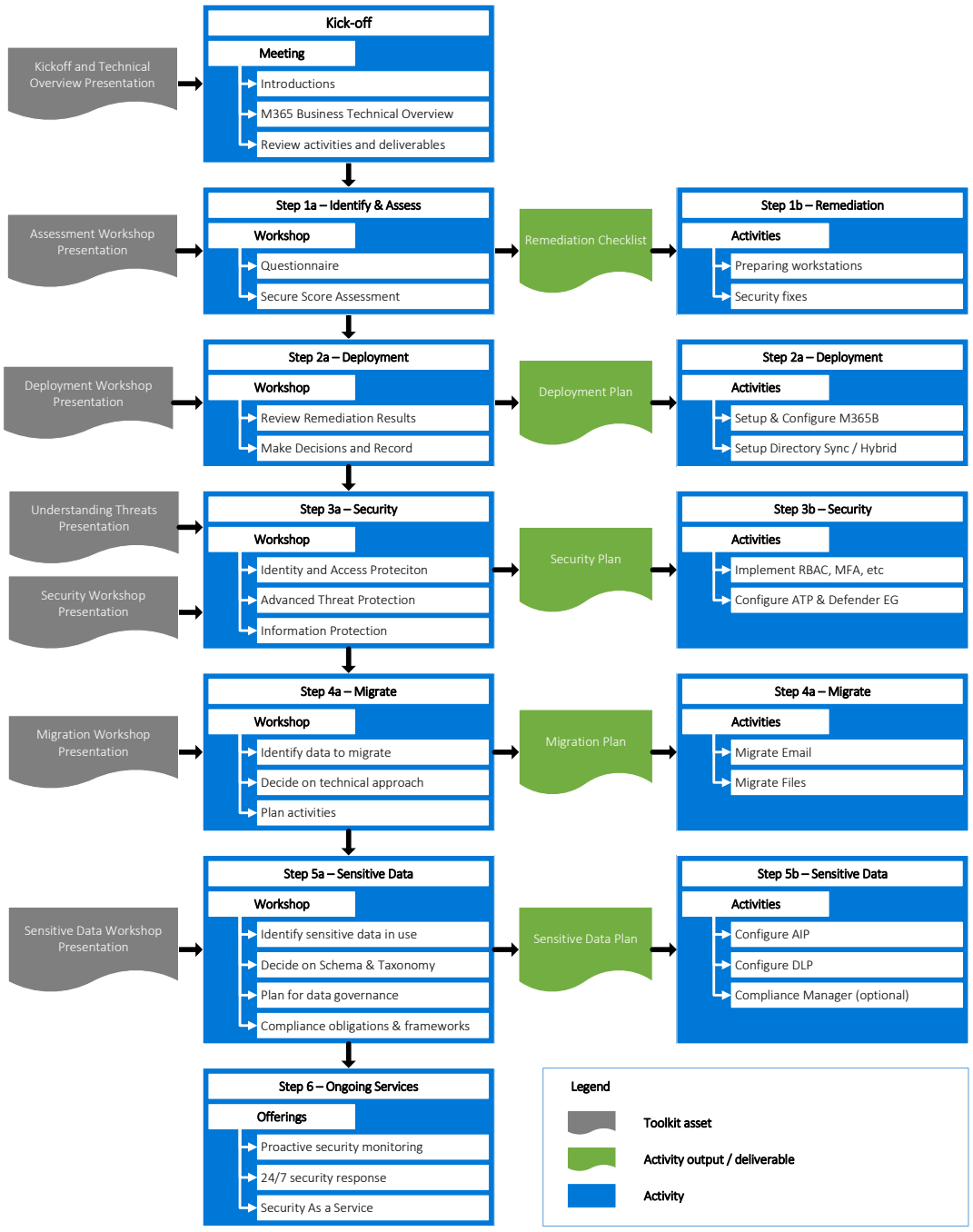
- Schedule the kickoff meeting with the customer, and make sure they have prescheduled all workshop sessions.
- The consultant(s) should review all IP and follow instructions, particularly within the PowerPoint files, for how you may need to adjust the materials for your particular customer.

6 Delivering the Microsoft 365 Business Secure Deployment Toolkit

The Microsoft 365 Business Secure Deployment Toolkit is a multi-step process that Microsoft partners can use to engage with their customers to deploy Microsoft 365 Business consistently, securely, and with high quality. The outcome of the engagement will be a fully configured, secure Microsoft 365 Business implementation.

This delivery guide describes the activities for each step, provides execution guidance and tips, and discusses resources and deliverables and is focused on a successful engagement and valuable outcome.

The illustration below depicts a high-level overview of the different steps and associated activities.



The following sections will describe each of the steps in more detail, provide background on the activities and provide further guidance on how to use Microsoft 365 Business Secure Deployment Toolkit.

The overall duration for a typical engagement with a simple customer scenario & requirements could be 1-2 weeks with a total effort of 40 to 60 project hours. The complexity of the organization and the amount of data to migrate will vary this estimate.

7 Key terms

These terms are intended to assist the partner in using and understanding the Microsoft 365 Business Secure Deployment Toolkit.

Confidentiality, integrity, and availability (CIA): primary objectives of information security. Confidentiality means only authorized individuals may access the information. Integrity means keeping the information accurate and modifiable by only authorized subjects. Availability means intended users can access and use the information, as expected in a timely manner.

Controls (noun): protections that help reduce security risk.

Data governance: the overall control and management of data's storage, usage, confidentiality, integrity, and availability.

Personal data: any information relating to an identified or identifiable natural person.

Personal identifiable information (PII), or sensitive personal information (SPI): information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

Personnel: people who perform work for an organization, such as employees or contractors.

Principle of least privilege: a concept that users and systems should be granted access to only the amount of data they need to perform their responsibilities.

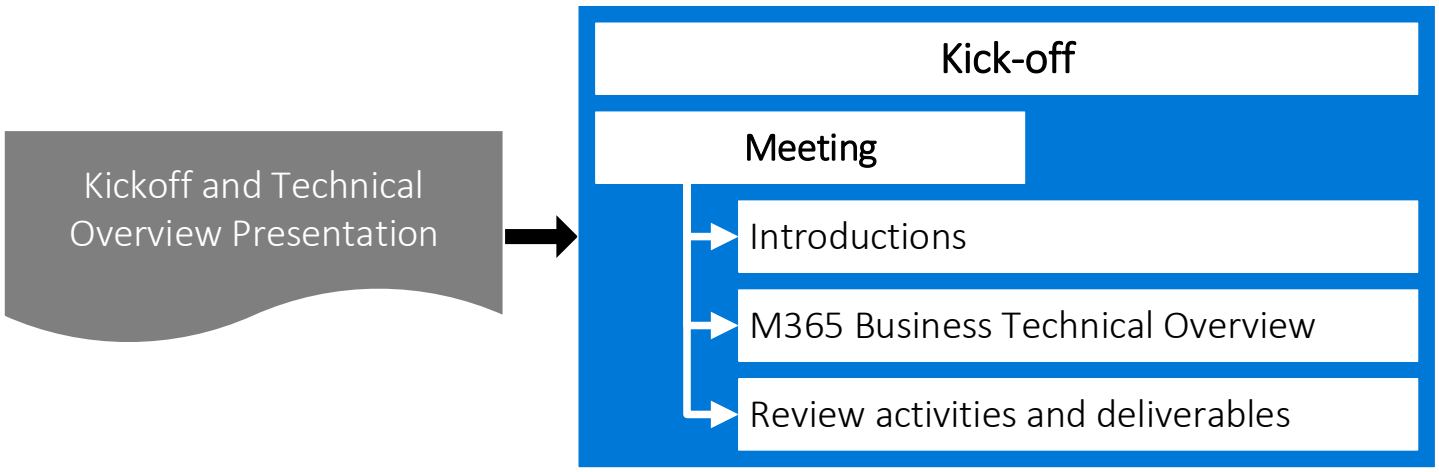
Schema: As related to data classification, the names of the labels used to identify categories

Sensitive data types: defines how the automated process recognizes specific information types such as bank account numbers, health service numbers or credit card numbers, also referred to as conditions. A sensitive information type is defined by a pattern that can be identified by a regular expression or a function. In addition, corroborative evidence such as keywords and checksums can be used to identify a sensitive information type. Confidence level and proximity are also used in the evaluation process.

Taxonomy: As related to data classification, the technique used to apply a classification or label.

8 Kick-off meeting

At the beginning of the engagement the customer and partner team will gather for a kickoff meeting. During this meeting, the team members will be introduced and the team will be briefed on the upcoming activities, proposed timelines and expected outcome.



Objectives

The objectives for the kick-off meeting are:

- Introduce the team members and their roles and responsibilities;
- Get a common understanding of the upcoming engagement;
- Discuss the assessment and deployment activities in detail;
- Assign customer and partner resources to activities and establish time lines;
- Align expectations.

Resources

The toolkit provides the following resources to use during the kick-off meeting:

- *<00 - Microsoft 365 Business Secure Deployment Toolkit - Kickoff and Technical Overview.pptx>*

Preparation

The partner consultant that will be leading the kick-off meeting should:

- Customize and update the *<00 - Microsoft 365 Business Secure Deployment Toolkit - Kickoff Presentation.pptx>* with customer specific details;
- Have a good understanding of security and how it relates to the people, technology and processes of the organization he/she is working with;
- Familiarize him/herself with key technology that will be used

Deliverables

The deliverables for the kick-off meeting are:

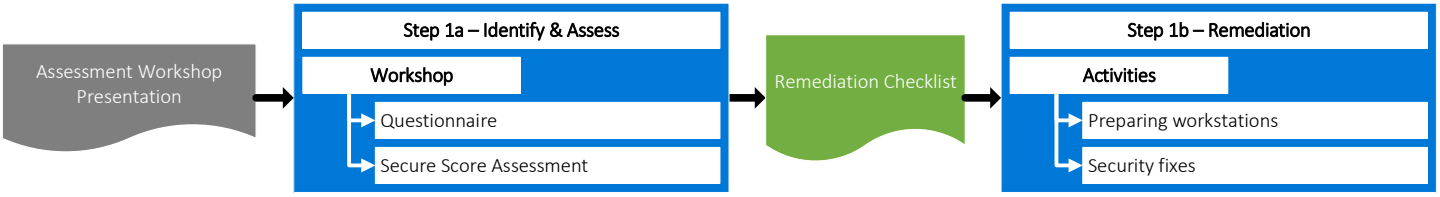
- Resource and activity planning;
- Established and confirmed timelines.

Duration

The typical duration for the kick-off meeting is 2 hrs.

9 Identify & Assess Security Gaps (Step 1)

During the Identify & Assess Security Gaps step, the partner works with the customer to begin the project, provide educational activities, identify security gaps that should be remediated as part of this project, and plan who will complete the remediation activities.



Objectives

- Understand customer's current security challenges
- Review customer's secure score if they already have Office 365
- Provide a prioritized list of recommendations
- Provide an actionable security roadmap
- Remediate high priority security concerns

Resources

The toolkit provides the following resources to use during the data source identification step:

- *<01 - Microsoft 365 Business Secure Deployment Toolkit – Assessment Workshop.pptx>*
- *<01 - Microsoft 365 Business Secure Deployment Toolkit - Remediation Checklist-v1.1.xlsx>*

Preparation

- Gather customer provided documentation

Activities

- Conduct workshop
- Lead the customer through secure score assessment
- Help the customer identify who will perform tasks necessary to prepare for devices for Windows 10 Business
- Help the customer identify who will remediate high priority security concerns

Deliverables

- Completed Remediation Checklist

Duration

- The typical duration for the Identify & Assess Security Gaps step is 1 day.

Summary

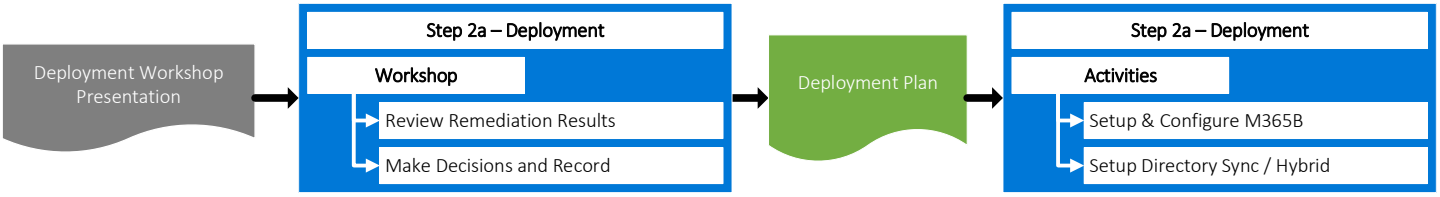
Each of the workshops in this toolkit has a very specific outcome. The table in this section provides you with the workshop title, planned duration (assuming that was not changed in your scope), which IP you should use from the IP Kit and a description of the workshop itself. Use this information to help you prepare for your delivery.

Table 2: Identify & Assess Security Gaps Activities

Activity Title	Duration	IP to be Used	Description	Guidance
Assessment Workshop	1.5 hours	01 - Microsoft 365 Business Implementation Services Toolkit – Assessment Workshop.pptx *01 - Microsoft 365 Business Secure Deployment Toolkit – Assessment Workshop.pptx*	The Assessment Workshop will cover the following topics: Cloud Security Objectives Cybersecurity Identity Access & Management Information Protection Secure Score	Clarify who will be responsible for remediation from the customer side and make sure to set dates for the next workshops.
Remediation	6 hours	*01 - Microsoft 365 Business Secure Deployment Toolkit - Remediation Checklist-v1.1.xlsx*	The partner or customer will address high priority security fixes identified in the workshop that should be done before deploying Microsoft 365 Business.	

10 Deploy Microsoft 365 Business (Step 2)

During the Deploy Microsoft 365 Business step, the partner works with the customer to prepare, configure, and implement the solution into their production environment.



Objectives

- Review results from remediation
- Plan for the deployment of Microsoft 365 Business
- Setup & Configure Microsoft 365 Business
- Install and configure Azure Active Directory Connect (AAD Connect)
- Enable device management via Azure Active Directory Join or Hybrid Azure Active Directory Join

Resources

The toolkit provides the following resources to use during the data source identification step:

- *<02 - Microsoft 365 Business Secure Deployment Toolkit – Deployment Workshop.pptx>*
- *<02 - Microsoft 365 Business Secure Deployment Toolkit – Deployment Plan.docx>*
- *< A1 - Microsoft 365 Business Secure Deployment Toolkit – Hybrid AADJ Addendum.docx>*

Preparation

Review the following materials for latest guidance:

- Setup Microsoft 365 Business
- Configure hybrid AAD join
- Intune network configuration requirements and bandwidth
- Office 365 URLs and IP address ranges

Activities

- Conduct workshop
- Lead the customer through decision points
- Draft deployment plan
- Deploy Microsoft 365 Business

Deliverables

- Deployment Plan
- Functional Microsoft 365 Business tenant

Duration

- The typical duration for the Deployment step is 1 day.

Summary

Each of the workshops in this toolkit has a very specific outcome. The table in this section provides you with the workshop title, planned duration (assuming that was not changed in your scope), which IP you should use from the IP Kit and a description of the workshop itself. Use this information to help you prepare for your delivery.

Table 3: Deployment Activities

Activity Title	Duration	IP to be Used	Description	Guidance
Deployment Workshop	2 hours	*02 - Microsoft 365 Business Secure Deployment Toolkit – Deployment Workshop.pptx* *02 - Microsoft 365 Business Secure Deployment Toolkit – Deployment Plan.docx*	The Deployment Workshop will cover the following topics: M365 Business Overview M365 Tenant Security Custom Domains Users & Devices Cloud vs. Hybrid Directory Directory Synchronization M365 Business Configuration	
Deployment	6 hours	*02 - Microsoft 365 Business Secure Deployment Toolkit – Deployment Plan.docx*		

Deployment Best Practices

M365B Configuration Wizard

- Discuss each configuration item during the workshop. While the default options are a good starting point, each one deserves individual consideration

Azure AD Connect

- The default options are usually the simplest
- If you configure a custom scope for synchronization, ensure all users and devices are contained in scope. If devices are excluded accidentally, they will not sync to Azure Active Directory

- Password hash synchronization is the recommended option for users and the simplest to deploy and has inherently higher availability compared to the other options.
    - Pass-through authentication is supported; however, you must consider high availability to account for the possibility the service will not be able to reach the customer's domain controller if there is a network disruption – link https://aka.ms/auth-options
- We recommend seamless SSO for either password hash synch or pass-through auth
    - This requires a GPO to add sign in site to browser Intranet zone

Azure Active Directory

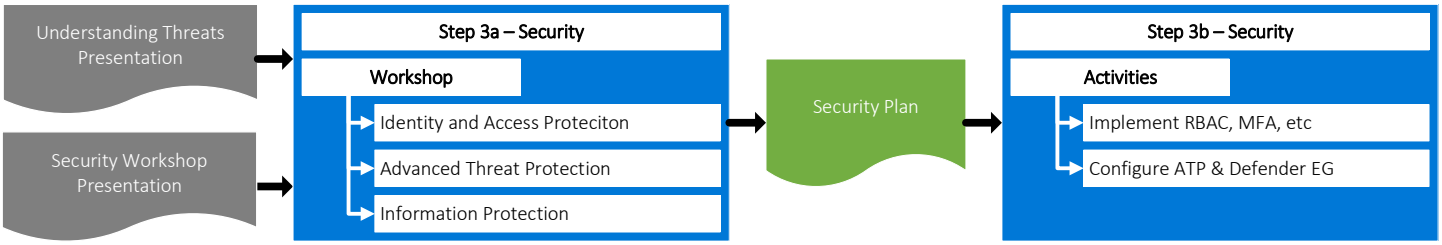
- If a customer currently has AD with machines joined to it, lead with Hybrid Azure Active Directory Joined devices. This will allow the customer to continue to manage Windows PC's with the group policy as they are used to and transition to using Intune over time. This will also reduce friction related to user profile migration. Be sure to check the current guidance before implementing.
- If a customer does not have AD with machines joined to it –lead with Azure Active Directory Joined devices.

Hybrid Azure Active Directory joined devices

- Ensure the Service Connection Point (SCP) is created correctly in AD
- Ensure you are using the latest Windows 10 Administrative Templates (.admx)
- Ensure devices are able to connect to the Internet and probe the Azure Device Registration Service. Remember that filtering and proxies can interfere with this.

11 Enable Proactive Security in Microsoft 365 Business (Step 3)

During the Deploy Microsoft 365 Business step, the partner works with the customer to prepare, configure, and implement the solution into their production environment.



Objectives

- Educate the customer on current cybersecurity threats
- Plan for the configuration of advanced security in Microsoft 365 Business
- Implement Identity and Access Protection
- Implement Advanced Threat Protection
- Implement Information Protection

Resources

The toolkit provides the following resources to use during the data source identification step:

- *<03 - Microsoft 365 Business Secure Deployment Toolkit – Security Workshop.pptx>*
- *<03 - Microsoft 365 Business Secure Deployment Toolkit – Security Plan.docx>*

Preparation

Read and understand the following:

- Office ATP anti-phishing
- Office ATP safe attachments
- Office ATP safe links

Activities

- Conduct workshop
- Lead the customer through decision points
- Draft security plan
- Enable additional security for Microsoft 365 Business workloads
- Configure Office 365 ATP policies
- Configure Windows Defender Exploit Guard

Deliverables

- Security Plan
- Secure Microsoft 365 Business tenant

Duration

- The typical duration for the Security step is 1 day.

Each of the workshops in this toolkit has a very specific outcome. The table in this section provides you with the workshop title, planned duration (assuming that was not changed in your scope), which IP you should use from the IP Kit and a description of the workshop itself. Use this information to help you prepare for your delivery.

Summary

Table 4: Security Activities

Activity Title	Duration	IP to be Used	Description	Guidance
Security Workshop	1.5 hours	*03 - Microsoft 365 Business Secure Deployment Toolkit – Security Workshop.pptx* *02 - Microsoft 365 Business Secure Deployment Toolkit – Security Plan.docx*	The Security Workshop will cover the following topics:	
Secure	6 hours	*03 - Microsoft 365 Business Secure Deployment Toolkit – Security Plan.docx*		

Security Best Practices

While Microsoft 365 is simple to deploy, the service configuration allows for very advanced implementations … It is important to realize there is no one-size-fits-all solution. When designing and implementing policies, please consider following these recommendations:

Multifactor Authentication

- At a minimum, all administrative accounts should be protected with MFA
- Enforcing MFA for all users is a very effective protection against credential compromise

RBAC

- The default options are usually the simplest and appropriate for most scenarios
- If you configure a custom scope for synchronization, ensure all users and devices are contained in scope. If devices are excluded accidentally, they will not sync to Azure Active Directory
- Password hash synchronization is the default option for users and the simplest to deploy
- Passthrough authentication is supported; however, you must consider high availability to account for the possibility the service will not be accessible to users should the customer experience a network disruption

Single Sign on

- SSO makes it easier for users to access the services, and for administrators to manage their users

Self Service Password Reset

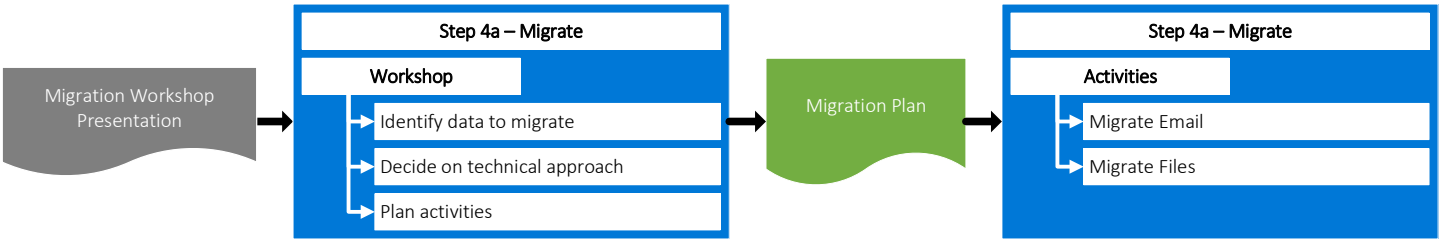
- In a cloud-only tenant, SSPR is very easy to enable and included
- In a federated account tenant (on-prem AD) SSPR is straightforward to set up, but does require additional licensing. Ensure customers have the necessary licensing before discussing this, or frame the conversation around available benefits at cost

Office 365 Advanced Threat Protection

- Get customer to DKIM p=reject
- Applying a single, consistent policy to all users should be the default approach for both Safe Links and Safe Attachments. Only deploy multiple policies if business needs require this.
- Microsoft does not recommend that customers bypass Safe Attachments for internal email

12 Migrate Email and Files (Step 5)

During the Migrate to Microsoft 365 Business step, the partner works with the customer to transfer email and files from on-premises or 3rd party cloud solutions to the customer's Microsoft 365 Business production environment.



Objectives

- Plan for the migration of email & files
- Plan for minimum disruption to user productivity
- Migrate email to Exchange Online
- Migrate files to OneDrive for Business

Resources

The toolkit provides the following resources to use during the data source identification step:

- *<05 - Microsoft 365 Business Secure Deployment Toolkit – Migration Workshop.pptx>*
- *<05 - Microsoft 365 Business Secure Deployment Toolkit – Migration Plan.docx>*

Preparation

- Ensure production tenant is fully configured and secured
- Ensure target mailboxes have sufficient capacity

Activities

- Conduct workshop
- Lead the customer through decision points regarding migration tooling & approach

- Draft migration plan
- Migrate email
- Migrate files

Deliverables

- Migration Plan
- Emails & files migrated

Duration

- The typical duration for the Migration step is 1 to 6 days.

Summary

Each of the workshops in this toolkit has a very specific outcome. The table in this section provides you with the workshop title, planned duration (assuming that was not changed in your scope), which IP you should use from the IP Kit and a description of the workshop itself. Use this information to help you prepare for your delivery.

Table 5: Migration Activities

Activity Title	Duration	IP to be Used	Description	Guidance
Migration Workshop	1.5 hours	*05 - Microsoft 365 Business Secure Deployment Toolkit – Migration Workshop.pptx* *05 - Microsoft 365 Business Secure Deployment Toolkit – Migration Plan.docx*	The Migration Workshop will cover the following topics:	
Migrate	6+ hours	*05 - Microsoft 365 Business Secure Deployment Toolkit – Migration Plan.docx*		

Migration Best Practices

While Microsoft 365 is simple to deploy, migration is key to obtaining full benefit of the customer's investment. Migration is often best left to partners who can ensure it is done correctly and promptly. When planning for migration, please consider following these recommendations:

13 Provide ongoing services

Maximize Secure Score

- Develop a Roadmap
- Quarterly Briefing/Update

API Integration

- Aggregate your customers secure scores with Partner Smart Office
- Correlate security events using the Microsoft GRAPH Security API

Provide 24/7 security monitoring and response

14 Engagement Closeout

A formal engagement closeout is a key component in managing customer satisfaction. Ensure that you schedule a formal closeout with the key Customer resources. The following topics should be discussed during the project closeout

- Review of project scope and SOW
- Identify the areas where partner went beyond the scope to provide value-add
- Discuss lessons-learned, what went well and what did not
- Discuss potential for additional assistance to mature their security posture

Note: this may be a good time to consider additional solutions or partner services deliveries if you feel the customer has a need or interest in them

- Deliver all project deliverables in final format to the customer
- Identify next steps and closeout the engagement

A PowerPoint template titled "99 -Microsoft 365 Business Secure Deployment Toolkit – Project Closeout" has been provided to you as a part of this offers bill of materials. Please review this template and update with the topics and use during your project closeout meeting.