Infinity Group

Scope of Works – Security Hardening

infinity group

Document Details:

Title:	**Scope of Works – Security Hardening**
Author:	

Contents:

Definition of Work

To increase security within the Microsoft 365 environment and reducing the risk of account breaches.

Prerequisites

1.1 Devices

Mobile phones that are to be enrolled within the Mobile Application Management (MAM) policies must meet firmware specifications, as listed within Section 4: Scope of Works (SOW). Windows Mobile devices cannot be enrolled.

The minimum Operating System (OS) levels are required:

- **iOS – Version 15 iOS**
- **Android – Version 11 OS**

1.2 Licences

All users to whom this solution will apply to are required to have appropriate licencing to enable the features. Those licences are:

- **Microsoft 365 Business Premium**
- **Microsoft 365 E3/E5**
- **Enterprise Mobility & Security E3/E5**

Infinity Group will provide a list of users to the client for cross-checking. Where licence changes or upgrades are required, they must be completed prior to solution deployment.

For users who just require a mailbox and currently use Exchange Online or Microsoft 365 Basic, the following additions will need be to be applied:

- **Defender for Office 365 Plan 1**
- **EM+S (Enterprise Mobility & Security)**

The Windows Defender Plan 1 licence will allow the ATP policies to be deployed and the EM+S licence will allow the user to enrol into MAM; details of which are found in the SOW.

1.3 Applications

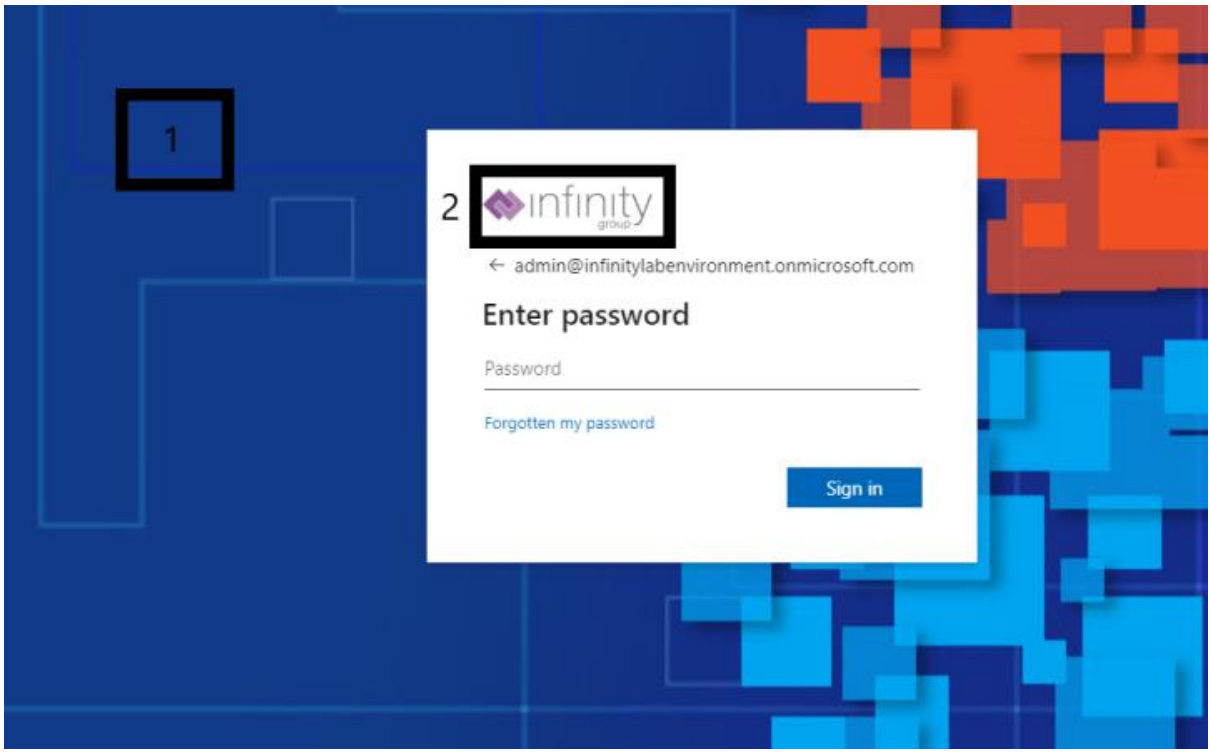
A component of the solution is that all users must access their emails using the Microsoft Outlook application without exception. Note that any users that sync their contacts using the native mail apps will need to ensure that Contacts are synced to Outlook to avoid losing access.

1.4 Additional Requirements

Company Branding

To enable company branding on the Office login page, the following images are required:

(The numbers correspond to the image below, providing an example of what each image will be used for).



- **Sign-in page background image (1):**
  - **Image size: 1920 x 1080px**
  - **File size: <300KB**
  - **File type: PNG, JPG or JPEG**

- **Banner logo (2):**
  - **Image size: 280 x 60px**
  - **File size: 10KB**
  - **File type: PNG, JPG or JPEG**

- **Sign-in page background colour:**
  - **The standard background colour is white, however you may want this customised to match your branding. This website below can be used to identify the exact colour for the background: *https://www.rapidtables.com/convert/color/rgb-to-hex.html***

Alerts

If you are an Infinity Group IT Support client, this information is not required as Infinity Group will deal with the alerts. If your business is not on IT Support with Infinity Group, then please provide the email address for alerts to be sent to. The alerts configured will be confirmed within the SOW.

Trusted Sites

As part of the multi-factor authentication (MFA) roll-out, Trusted Sites are excluded from the requirement to use MFA. For this to work, Infinity Group require the IP addresses of your public-facing interfaces; this can be provided for single or multiple locations. If you are an Infinity Group IT Support client, then this information is not required.

Risky Countries

The following countries are deemed most prevalent for hacking attempts. To further reduce risk access, *https://www.office.com/* will not be accessible from the following countries:

- **Iran**
- **China**
- **Russia**
- **Ukraine**
- **Turkey**
- **Taiwan**
- **Hungary**
- **Brazil**
- **South Korea**
- **Nigeria**
- **Romania**

Objectives

The project objective is to add additional security features within the Microsoft 365 environment that will reduce the likelihood of account breaches, phishing attempts and provide control over business data (in Microsoft Applications) on mobile devices.

Scope of Works

- **Turn on auditing**
- **Disable customer Lockbox**
- **Configure MFA as a Conditional Access policy**
- **Configure Microsoft default alerts:**
    - **Suspicious email sending patterns detected**
    - **Elevation of admin privilege**
    - **Email sending limit exceeded**
    - **Creation of forwarding rule**
    - **User restricted from sending email**
    - **eDiscovery search started/exported**
    - **Messages have been delayed**
    - **Tenant restricted from sending email**

- **Recommended Security Settings:**
    - **Prevent rules being created that forward all users' emails to external recipients**
    - **Turn off anonymous sharing of calendars to prevent hackers from tracking users' movements**
    - **Prevent sign-in for shared mailboxes**
    - **Do not expire password once self-service password and MFA are enforced**

- **Password Policy:**
  - **Default password policy including password restrictions, characters allowed and not allowed**
  - **Configure Password Protection in Azure Active Directory (Azure AD)**

- **ATP Policies:**
  - **Anti-Phishing**
  - **Safe Attachments**
  - **Safe Links**
  - **Anti-Spam**
  - **Anti-Malware**
  - **Safety-Tips**

- **Company branding – Add company branding to the Office 365 Landing Page**

- **The baseline policies for Mobile Application Management (MAM):**

  - **iOS:**

Device Types	Unmanaged
Applications	Microsoft Bookings Microsoft Dynamics 365 Microsoft Dynamics 365 for mobile phones Microsoft Edge Microsoft Excel Microsoft Invoicing Microsoft Kaizala Microsoft OneDrive Microsoft OneNote Microsoft Outlook Microsoft Planner Microsoft Power BI Microsoft PowerApps Microsoft PowerPoint Microsoft SharePoint Microsoft StaffHub Microsoft Stream Microsoft Teams Microsoft To-Do Microsoft Visio Viewer Microsoft Whiteboard Microsoft Word Office Hub
Backup organisation (org) data to iTunes and iCloud backups	Block
Receive data from other apps	All apps

Restrict Cut, Copy and Paste between other apps	Policy managed apps	
Third-party keyboards	Allow	
Encrypt org data	Require	
Sync app with native contacts app	Allow	
Printing org data	Allow	
Restrict web content transfer with other apps	Any app	
Org data notifications	Allow	
PIN for access	Require	
PIN type	Numeric	
Simple PIN	Allow	
Select minimum PIN length	8	
Touch ID instead of PIN for access (iOS 8+/iPadOS)	Allow	
Override biometrics with PIN after timeout	Require	
Timeout (minutes of inactivity)	60	
Face ID instead of PIN for access (iOS 11+/iPadOS)	Allow	
PIN reset after number of days	No	
App PIN when device PIN is set	Not required	
Work or school account credentials for access	Not required	
Re-check the access requirements after (minutes of inactivity)	60	
Conditional Launch		
Max PIN attempts	5	Reset PIN
Offline grace period	720	Block access (minutes)
Offline grace period	90	Wipe data (days)
Jailbroken/rooted devices		Block access
Min OS version	15.0.0	Block access

- **Android:**

Device Types	Unmanaged
Applications	Microsoft Bookings Microsoft Dynamics 365 for phones Microsoft Dynamics 365 for tablets Microsoft Edge Microsoft Excel Microsoft Invoicing

	Microsoft Kaizala Microsoft Launcher Microsoft OneDrive Microsoft OneNote Microsoft Outlook Microsoft Planner Microsoft Power BI Microsoft PowerPoint Microsoft SharePoint Microsoft StaffHub Microsoft Stream Microsoft Teams Microsoft To Do Microsoft Word Power Automate Power Apps PrinterOn for Microsoft Skype for Business Yammer	
Backup org data to Android backup services	Block	
Receive data from other apps	All apps	
Restrict Cut, Copy and Paste between other apps	Policy managed apps	
Screen capture and Google Assistant	Block	
Encrypt org data	Require	
Sync app with native contacts app	Allow	
Printing org data	Allow	
Org data notifications	Allow	
PIN for access	Require	
PIN type	Numeric	
Simple PIN	Allow	
Minimum PIN length	8	
Fingerprint instead of PIN for access (Android 6.0+)	Allow	
Override fingerprint with PIN after timeout	Require	
Timeout (minutes of inactivity)	60	
PIN reset after number of days	No	
App PIN when device PIN is set	Not required	
Re-check the access requirements (after minutes of inactivity)	60	
Conditional Launch		
Max PIN attempts	5	Reset PIN
Offline grace period	720	Block access (minutes)
Offline grace period	90	Wipe data (days)
Jailbroken/rooted devices		Block access
Min OS version	11.0.0	Block access

Conditional Access Policy

- BLOCK – Legacy Authentication – This global policy blocks all connections from unsecure Legacy protocols like ActiveSync, IMAP, PO3 etc.
- BLOCK – Risky Countries – This global policy blocks access from the 'Risky Countries'.
- GRANT – Enforce MFA when 'Out of Office' – This global policy enforces all users to require MFA when logging into cloud apps from an untrusted location.
- GRANT – Intune Enrolment – Devices can authenticate to Intune for enrolment.
- GRANT – Mobile Device Access – Grants access to mobile devices that use an approved Microsoft app.
- BLOCK – Windows Phone – Blocks access to corporate resources for Windows phone devices.

Delivery Method

The policies outlined in the SOW will be configured and implemented on an agreed date with advance notice. All changes are noted within the Welcome Pack provided as part of the project. Prior to the agreed date, end users will be required to pre-enrol in MFA – This process takes around 15 minutes, with a guide provided by Infinity Group. On the date selected to implement the policies, remote assistance, through a dedicated number, will be provided should any issues arise.

Project Management

A project manager will be assigned to this work once signed off. They will be the primary point of contact, co-ordinating consultants, engineers and managing timelines for completion.

Prior to commencement of the works, a kick-off call will be booked to walk through the changes and expected timeline.

Disruption/Changes to BAU

- All users will only be able to access their email using the Microsoft Outlook application
- MFA will be enforced
- To access company data, users must enrol in the MAM policies
- ATP policies will be enabled

All the above are detailed within the accompanying Welcome Pack document.

Additional Notes

1.5 Synced Contacts

Users wishing to sync their iPhone Mail contacts to Outlook will need to action the following, noting that accessing email through the iPhone Mail app will no longer be available:

- **Settings**
- **Mail**
- **Accounts**
- **Select Mail client (Outlook), then toggle the 'Contacts' button.**
- **Settings**
- **Outlook**
- **Enable contacts**

1.6 Hardware Support

Infinity Group are not responsible for mobile hardware support.