## Table of Contents

1. Executive Summary .................................................................................................................. 7
2. Technical Design for Secure Configuration Alignment ................................................................. 8
   Good ........................................................................................................................................... 11
   2.1.1 Prevent use of Legacy Authentication Protocols ................................................................. 13
   Better ......................................................................................................................................... 14
   Best 17
2.2 Use of Office 365 Secure Score service .................................................................................... 18
3. Core Configuration Controls ......................................................................................................... 20
   3.1 Identity .................................................................................................................................. 20
       3.1.1 Authentication Methods ................................................................................................. 21
   3.2 Federated Hybrid-Identity Controls ......................................................................................... 24
       3.2.1 Configure AD FS to use Azure MFA as the primary authentication mechanism 24
       3.2.2 Configure ADFS to Block Legacy Authentication from the Extranet ............................ 24
       3.2.3 Enable ADFS Web Application Proxy Extranet Lockout .............................................. 26
       3.2.4 Configure Conditional Access using ADFS ................................................................. 27
   3.3 Recommended Identity Controls ............................................................................................ 29
       3.3.1 Prevent use of Legacy Authentication Protocols ................................................................. 29
       3.3.2 Configure Azure AD Password Protection ................................................................. 31
       3.3.3 Enable MFA for all users ............................................................................................... 32
       3.3.4 Implement a holistic identity-centric Conditional Access approach ............................ 33
       3.3.5 Do not expire passwords ............................................................................................... 36
       3.3.6 Disable accounts not used in last 30 days ..................................................................... 37
       3.3.7 Configure certificate-based authentication for mobile devices .................................... 37
   3.4 Specific considerations for protecting Privileged identity ...................................................... 39
       3.4.1 Prevent use of Legacy Authentication Protocols ................................................................. 40
       3.4.2 Location for privileged identities ..................................................................................... 40
       3.4.3 Use dedicated accounts to perform Administrative Tasks ................................................ 40
       3.4.4 Configure Office 365 Global Administrator role members ............................................ 40
       3.4.5 Use Non-Global Administrative roles .............................................................................. 41
3.4.6 Configure break glass accounts in Azure AD ........................................... 43
3.4.7 Enable MFA for all Global Admins ............................................................ 44
3.5 Office 365 Service Configuration ................................................................... 47
  3.5.1 Enable Modern Authentication ................................................................. 47
  3.5.2 Exchange Online ..................................................................................... 49
  3.5.3 Enable audit data recording ..................................................................... 49
  3.5.4 Enable mailbox auditing for all users ..................................................... 49
  3.5.5 Enable Client Rules Forwarding Block .................................................. 50
  3.5.6 Configure Transport rule for ransomware .............................................. 51
  3.5.7 Configure anti-malware protection in your tenant .................................. 55
  3.5.8 Do not allow anonymous calendar sharing ........................................... 55
  3.5.9 Secure external mail flow ....................................................................... 56
  3.5.10............................................................................................................. 61
  3.5.11............................................................................................................. 61
  3.5.12............................................................................................................. 62
  3.5.13............................................................................................................. 62
  3.5.14............................................................................................................. 62
  3.5.15............................................................................................................. 62
  3.5.16............................................................................................................. 63
  3.5.17............................................................................................................. 64

4 Security and Compliance Package enhancements ........................................ 65
  4.1 Enhanced Identity Protection controls ....................................................... 66
    4.1.1 Azure AD Identity Protection ................................................................. 66
    4.1.2 Azure AD Privileged Identity Management ......................................... 68
    4.1.3 Microsoft Office 365 Privileged Access Management ....................... 68
  4.2 Enhanced Service Configuration controls ............................................... 70
    4.2.1 Enable customer lockbox feature ....................................................... 70
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3</td>
<td>Enhanced Data Protection controls</td>
<td>70</td>
</tr>
<tr>
<td>4.3.1</td>
<td>Configure Office 365 Advanced Threat Protection Safe Attachments feature</td>
<td>70</td>
</tr>
<tr>
<td>4.3.2</td>
<td>Configure Office 365 Advanced Threat Protection Safe Links feature</td>
<td>72</td>
</tr>
<tr>
<td>4.3.3</td>
<td>Azure Information protection</td>
<td>75</td>
</tr>
<tr>
<td>Appendix A</td>
<td>Incident Response Guidance</td>
<td>77</td>
</tr>
<tr>
<td>Immediate actions</td>
<td></td>
<td>77</td>
</tr>
<tr>
<td>Improve the organisations overall security posture</td>
<td></td>
<td>78</td>
</tr>
<tr>
<td>Azure AD reporting API</td>
<td></td>
<td>78</td>
</tr>
<tr>
<td>Office 365 Security Best Practices</td>
<td></td>
<td>78</td>
</tr>
<tr>
<td>Enable mailbox audit logging</td>
<td></td>
<td>78</td>
</tr>
<tr>
<td>Finding Illicit Activity</td>
<td></td>
<td>78</td>
</tr>
<tr>
<td>Finding Breached Accounts</td>
<td></td>
<td>78</td>
</tr>
<tr>
<td>O365-InvestigationTooling</td>
<td></td>
<td>82</td>
</tr>
</tbody>
</table>
# Table of Tables

Table 1: List of controls considered appropriate to implement Good category .......................... 11
Table 2: Security controls consider appropriate for Better category............................................. 15
Table 3: Security controls consider appropriate for Best category............................................... 18
Table 4: Recommended ADFS claims rules for legacy protocol control........................................ 25
Table 5: Conditional Access claim rules overview........................................................................ 27
Table 6: Standard User Conditional Access policies ........................................................................ 35
Table 7: Recommended Conditional Access policies for Global Administrators.......................... 45
Table 8: CNAME records format.................................................................................................... 58
Table 9: CNAME records example ................................................................................................ 58
Table 10: Risk event categories...................................................................................................... 67
Tables of Figures

Figure 1: Authentication method decision tree................................................................. 23
Figure 2: Legacy Authentication control ........................................................................... 30
Figure 3: Conditional Access what if tool output............................................................... 46
Figure 4: Security and Compliance Package components .................................................. 65
Executive Summary

Microsoft provides a secure cloud service and has numerous independently verified attestation on its configuration state, from ISO the ISO 27000 family of standards, guidelines published by the National Institute of Standards and Technology (NIST) like NIST 80053, and others.

This document came out of a need to help UK Government departments configure Office 365 in a way that helps them meet their obligations and leverages the features and capabilities that are present within the service. It draws on broad experience across UK government, industry and draws heavily in already existing “best practice.”

This guidance is not designed to suggest that nothing else is required as “we do not need to do anything else as we have followed the NCSC and Microsoft’s guidance”. Rather the controls described in this document is intended to help the reader understand why the specific security controls are recommended and provide step by step configuration guidance allowing organisations to understand how the features and capabilities in Office 365 can be used to ensure that a common bar has been achieved for their Office 365 tenant.

The following sections of this document have been split into two major sections:

- **Core Configuration Controls**: addresses the recommended configuration of features that are included in the Microsoft M365 E3 license.
- **Enhanced Configuration Controls**: addresses the additional controls that are available when they purchase the Security and Compliance Package.

The guidance consists of the recommended security configuration controls that organisations should consider to securely configure and operate their Office 365 tenant.

For both the Core and Enhanced sections the guidance is broken down into three focus areas:

- **Identity** – recommended controls describing how to secure the identities that are used to authenticate against Office 365 services. This guidance includes both guidance for administrative privileged users as well as standard productivity users.
- **Service Configuration** – recommended controls for Office 365 applications that describe specific settings to secure the service thus raising the security posture of the organisations Office 365 tenant
- **Data Protection** – recommended controls that have been specifically identified to protect an organisations data as it is processed and handled in Office 365.

This guidance applies to all Office 365 services unless otherwise specified. This will allow you to make full use of all the newer features such as O365 Groups and Teams, as well as the components that more directly replace on-premises services such as Exchange and SharePoint.
2 Technical Design for Secure Configuration Alignment

The following sections describe the security controls that organisations should implement to align with NCSC and Microsoft guidance.

The technical controls that are described in this document have been grouped into three categories, good, better and best. The rationale for the groupings is described below:

- **Good** –
  - forms the minimum level of configuration that all organisations should meet
  - available with Microsoft 365 E3 license
  - can be implemented using simple configuration tasks

- **Better**
  - Forms the level that organisations should aspire to in order
  - available with Microsoft 365 E3 license but may require Security and Compliance Package components.
  - might require more complex configuration tasks

- **Best**
  - Solutions that help mitigate specific risks that an organisation may have identified in their wider IT deployment
  - Requires functionality only available with Security and Compliance Package
  - Requires more complex configuration of the feature

The following describes the technical controls that have been assigned to each of the groupings:

<table>
<thead>
<tr>
<th>Technical Function</th>
<th>Good</th>
<th>Better</th>
<th>Best</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticate Users</td>
<td>Cloud Authentication with</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Password Hash Sync</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>or Cloud Authentication with</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pass Through Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>or ADFS Federated authentication with</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technical Function</td>
<td>Good</td>
<td>Better</td>
<td>Best</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Password Hash Sync enabled</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block Legacy Authentication</td>
<td>Configure Azure AD Conditional Access to block legacy authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>and</td>
<td>Configure ADFS to Block Legacy Authentication from the Extranet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protect Privileged accounts</td>
<td>Anchor privileged accounts in Azure AD to mitigate threat from on-prem compromise</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use dedicated accounts to perform Administrative Tasks</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use Non-Global Administrative roles</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configure Office 365 Global Administrator role members</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configure break glass accounts in Azure AD</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enable MFA for all Global Admins</td>
<td></td>
<td>Azure AD Privileged Identity Management (requires SCP)</td>
</tr>
<tr>
<td>Secure Access to Resources</td>
<td>Enable Modern Authentication for O365 workloads</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Require MFA for External User Access</td>
<td>Implement a holistic identity-centric Conditional Access approach</td>
<td>Azure AD Identity Protection (requires SCP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Azure Information protection (requires SCP)</td>
</tr>
<tr>
<td>User Account Policies</td>
<td>Disable accounts not used in the last 30 days</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password Hygiene</td>
<td>Do not expire passwords</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technical Function</td>
<td>Good</td>
<td>Better</td>
<td>Best</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>and</td>
<td>Configure Azure AD Password Protection</td>
<td>Extend Azure AD Password Protection to AD DS</td>
<td></td>
</tr>
<tr>
<td>Protect Against Password Compromise</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reduce Use of Passwords</td>
<td>Implement Azure AD MFA as primary authentication at ADFS</td>
<td>Configure CBA for Mobile Device access (requires ADFS)</td>
<td></td>
</tr>
<tr>
<td>Auditing</td>
<td>Enable audit data recording</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enable mailbox auditing for all users</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enable customer lockbox feature (requires SCP)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ADFS Specific Controls</td>
<td>Configure ADFS to Block Legacy Authentication from the Extranet</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enable ADFS Web Application Proxy Extranet Lockout</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration Review</td>
<td>Periodically review O365 Secure Score service output</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exchange Online controls</td>
<td>Enable Client Rules Forwarding Block</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Do not allow anonymous calendar sharing</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configure Transport rule for ransomware</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configure anti-malware protection in your tenant</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Secure external mail flow</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configure Office 365 Advanced Threat Protection</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configure Office 365 Advanced Threat Protection</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configure Office 365 Advanced Threat Protection</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Prepared by Microsoft Services UK
<table>
<thead>
<tr>
<th>Technical Function</th>
<th>Good</th>
<th>Better</th>
<th>Best</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safe Links feature (requires SCP)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure data loss prevention (DLP)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SharePoint Online controls</td>
<td>Configure expiration time for external sharing links</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Skype for Business Online controls</td>
<td>Skype For Business User Policies</td>
<td></td>
<td>Skype For Business Federation</td>
</tr>
</tbody>
</table>

### Good

The following controls are included in the Good category:

Table 1: List of controls considered appropriate to implement Good category

<table>
<thead>
<tr>
<th>Control</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable audit data recording</td>
<td><strong>Applicable to all configurations</strong></td>
</tr>
<tr>
<td></td>
<td>Office 365 provides ability to audit user interaction with Office 365 service. Failure to enable auditing will severely impact the ability of incident response teams to investigate breaches.</td>
</tr>
<tr>
<td>Enable mailbox auditing for all users</td>
<td><strong>Applicable to all configurations</strong></td>
</tr>
<tr>
<td></td>
<td>By default, only non-owner access is audited. Attackers often look to exfiltrate data via a compromised accounts mailbox. Enabling auditing for mailbox owner will enable incident response teams to determine whether a mailbox has been used to exfiltrate data.</td>
</tr>
<tr>
<td>Use of Office 365 Secure Score service</td>
<td><strong>Applicable to all configurations</strong></td>
</tr>
<tr>
<td></td>
<td>Office Secure Score is an analytics tool that reviews the configuration of your Office 3665 tenant and makes recommendations on controls that are deemed to reduce the risk of compromise.</td>
</tr>
<tr>
<td>Configure AD FS to use Azure MFA as the primary authentication mechanism</td>
<td><strong>If Office 365 configured in Federated mode and Azure AD Conditional Access is not used, then is control is applicable</strong></td>
</tr>
<tr>
<td>Control</td>
<td>Notes</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Preference is to use Azure AD Conditional Access to implement MFA as it is more flexible than using AD FS and can be combined with additional Conditional Access controls</td>
<td></td>
</tr>
<tr>
<td>Configure ADFS to Block Legacy Authentication from the Extranet</td>
<td>If Office 365 configured in Federated mode and Azure AD Conditional Access is not used, then is control is applicable</td>
</tr>
<tr>
<td>Preference is to use Azure AD Conditional Access to implement MFA as it is more flexible than using AD FS and can be combined with additional Conditional Access controls</td>
<td></td>
</tr>
<tr>
<td>Enable ADFS Web Application Proxy Extranet Lockout</td>
<td>If Office 365 configured in Federated mode and Azure AD Conditional Access is not used, then is control is applicable</td>
</tr>
<tr>
<td>Preference is to use Azure AD Smart Lockout control</td>
<td></td>
</tr>
<tr>
<td>Prevent use of Legacy Authentication Protocols</td>
<td>This control is applicable for all organisations</td>
</tr>
<tr>
<td>This control is the preferred method to implement this control and is applicable to organisations who have chosen Azure AD Conditional Access and should be included in and Conditional Access policies implemented.</td>
<td></td>
</tr>
<tr>
<td>Legacy Authentication Protocols only support username and password as authentication method. This provides attackers with the opportunity to perform password spray attacks or similar.</td>
<td></td>
</tr>
<tr>
<td>Legacy Authentication Protocols also prevent the use of Azure MFA.</td>
<td></td>
</tr>
<tr>
<td>Do not expire passwords Disable accounts not used in last 30 days</td>
<td>The forced changing of passwords on a periodic basis has been demonstrated to lead to poor password selection. When combined with Azure AD Password Protection control (included in Better category) the need to enforce password complexity or expiry is significantly reduced.</td>
</tr>
<tr>
<td>Disable accounts not used in last 30 days</td>
<td>Accounts, especially those that perform privileged roles, should not be left active.</td>
</tr>
<tr>
<td>Configure certificate-based authentication for mobile devices</td>
<td>If Office 365 configured in Federated mode and Azure AD Conditional Access is not used, then is control is applicable. Mobile applications typically are configured to authenticate using username and password. This configuration makes their use an easy target for password spray attacks. Most mobile platforms have applications that are capable of using Modern Authentication which enables MFA or certificate-based authentication as a viable option.</td>
</tr>
</tbody>
</table>
## 2.1.1 Prevent use of Legacy Authentication Protocols

There are very few things an organisation can do which are as easy to deploy and can improve your security posture as much as blocking the use of Legacy Authentication Protocols. This is particularly important for Privileged Identities and therefore, it is therefore mandated that this security control is implemented for all Privileged Identities that are used to administer your Office 365 tenancy.

<table>
<thead>
<tr>
<th>Control</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use dedicated accounts to perform Administrative Tasks</td>
<td>This control is applicable for all organisations&lt;br&gt;The location of where privileged identities are anchored is import to ensure that they are as secure as possible and not subject to traditional credential theft attacks which would allow cloud administration accounts to be compromised if an organisations traditional on-premises Active Directory were compromised.</td>
</tr>
<tr>
<td>Configure Office 365 Global Administrator role members</td>
<td>This control is applicable for all organisations&lt;br&gt;Keeping the number of Global Administrators to the minimum level is important part of a least privilege administration model</td>
</tr>
<tr>
<td>Use Non-Global Administrative roles</td>
<td>This control is applicable for all organisations&lt;br&gt;Implementing role based access model to reduce the number of Global Administrators is an important part of a least privilege administration model</td>
</tr>
<tr>
<td>Configure break glass accounts in Azure AD</td>
<td>This control is applicable for all organisations&lt;br&gt;Ensuring that in the event of either a malicious insider to external compromise of a Global Administrator account there are accounts that are not subject to MFA or other logon restrictions.</td>
</tr>
<tr>
<td>Enable MFA for all Global Admins</td>
<td>This control is applicable for all organisations&lt;br&gt;Enforcing the use of MFA for all Global Administrator members reduces the risk of account compromise when only username and password are used. It is recommended that Azure AD Conditional Access is used to implement this control</td>
</tr>
<tr>
<td>Enable Modern Authentication</td>
<td>This control is applicable for all organisations&lt;br&gt;Modern Authentication is a pre-requisite for MFA when connecting to Office 365 services.</td>
</tr>
<tr>
<td>Control</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable Client Rules Forwarding Block</td>
<td><strong>This control is applicable for all organisations</strong></td>
</tr>
<tr>
<td></td>
<td>This control not only prevents malicious actors from being able to exfiltrate data using compromised accounts but also prevents users from automatically forwarding emails to personal email accounts that are not subject to the same corporate policies that Office 365 is able to provide</td>
</tr>
<tr>
<td>Do not allow anonymous calendar sharing</td>
<td><strong>This control is applicable for all organisations</strong></td>
</tr>
<tr>
<td></td>
<td>This control prevents user’s calendars from be visible to unauthenticated users. This prevents attackers from being able to perform reconnaissance of user’s in your organisation before launching an attack</td>
</tr>
<tr>
<td>Configure expiration time for external sharing links</td>
<td><strong>This control is applicable for all organisations</strong></td>
</tr>
<tr>
<td></td>
<td>Securely sharing information with external parties is important. Configuring SharePoint to allow sharing with external parties ensures that collaboration is possible but configured so that external parties must authenticate to Office 365. Using SharePoint to share improves an organisations security posture as it removes the need for documents to be sent over email where they are no longer under the management or control of your organisation</td>
</tr>
<tr>
<td>Skype For Business User Policies</td>
<td><strong>This control is applicable for all organisations</strong></td>
</tr>
<tr>
<td></td>
<td>Skype for Business allows users to share files with other users. This is also possible when the participants are external to your organisation. Preventing files sharing using Skype for Business reduces the potential for unauthorised data exfiltration. Microsoft Teams does not share items using the same mechanism. Items shared in Teams use SharePoint or OneDrive to share the items which is the recommended approach</td>
</tr>
<tr>
<td>Enable Azure AD and Office 365 Cloud App Security</td>
<td><strong>This control is applicable for all organisations</strong></td>
</tr>
<tr>
<td></td>
<td>Office 365 Cloud App Security provides the ability to report and raise alerts on suspicious or anomalous activities of privileged and standard users.</td>
</tr>
</tbody>
</table>

**Better**

The list of controls included in the Best category are listed in Table 2 below. The majority of controls are included in the Microsoft 365 E3 license, where they are not it is indicated in the control details.
The controls listed below have been identified as requiring more complex configuration than those included in the Good category.

Table 2: Security controls consider appropriate for Better category

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Conditional Access using ADFS</td>
<td>If Office 365 configured in Federated mode and Azure AD Conditional Access is not used, then is control is applicable. Implementing Conditional Access using AD FS provides basic capability, control based on user identity or group membership, network location, device (whether it is workplace joined, to gate access to Office 365 services. Using Azure AD Conditional Access is the preferred method for implementing Conditional Access as it provides richer controls based on, MFA, device state, sign-in risk, Windows Defender ATP.</td>
</tr>
<tr>
<td>Configure Azure AD Password Protection</td>
<td>This control will improve password strength and should be considered a priority for organisations even though it requires additional configuration for on-premises AD DS service. Azure AD Password protection helps to raise the bar of passwords that are used in your organisation. It prevents users from choosing common passwords or variations of as well as the ability to add organisation specific bad password lists. Azure AD Password Protection has also been extended to integrate with on-premises Active Directory Domain Services (AD DS) so that the power of Azure AD can be utilised on-premises. Implementing Azure AD Password Protection allows greater confidence when considering whether to change your password policy to not expire passwords.</td>
</tr>
<tr>
<td>Enable MFA for all users</td>
<td>Using MFA for all standard user accounts will reduce risk of account compromise due to password spray and other credential theft attacks as the user’s username and password are not the only credentials that are required in order to access Office 365 services. Azure AD Conditional Access is the recommended way to meet this control as it can not only be used to enforce MFA but include other conditions, device state, sign-in risk, as well as prevent use of Legacy Protocols</td>
</tr>
<tr>
<td>Implement a holistic identity-centric Conditional Access approach</td>
<td>Azure AD Conditional Access provides the ability to combine multiple conditions, device compliance, sign-in risk, use of MFA, to grant or deny access to Office 365 services. Exploiting the capability of Azure AD Conditional Access to raise the security posture of users when they access Office 365 services whilst balancing the impact of repeated</td>
</tr>
<tr>
<td>Control</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Control Description</td>
<td><strong>Authentication requests will ease adoption of security enhancements for an organisation.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Azure AD Conditional Access is the recommended method of implementing MFA in an organisation.</strong></td>
</tr>
<tr>
<td>Configure Transport rule for ransomware</td>
<td><strong>This control is applicable only for organisations that have not purchased Security and Compliance Package</strong></td>
</tr>
<tr>
<td></td>
<td>For organisations that have chosen not to purchase the Security and Compliance Package which entitles them to use Office ATP they can configure Exchange Online Transport rules to control how attachments of defined file types are handled.</td>
</tr>
<tr>
<td></td>
<td>This approach does not allow machine learning or other intelligent security graph techniques to be used but will add a basic level of capability to control ransomware.</td>
</tr>
<tr>
<td>Configure anti-malware protection in your tenant</td>
<td><strong>This control is applicable only for organisations that have not purchased Security and Compliance Package</strong></td>
</tr>
<tr>
<td></td>
<td>For organisations that have chosen not to purchase the Security and Compliance Package which entitles them to use Office ATP they can configure Exchange Online Protections to include blocking of Common Attachments.</td>
</tr>
<tr>
<td></td>
<td>This approach does not allow machine learning or other intelligent security graph techniques to be used but will block common attachments that are known to be used to deliver malicious payloads.</td>
</tr>
<tr>
<td>Secure external mail flow</td>
<td><strong>This control is applicable for all organisations</strong></td>
</tr>
<tr>
<td></td>
<td>Configuring Exchange Online to use SPF, DKIM and DMARC will help to reduce spoofing of emails.</td>
</tr>
<tr>
<td></td>
<td>The NCSC also provides a Mailcheck program that organisations can enrol in that will continually assess email security compliance.</td>
</tr>
<tr>
<td>Skype For Business Federation</td>
<td>This control is only applicable to organisations who consider the risk of collaborating with other organisations using Skype for Business unacceptable or wish to block collaboration with certain domains.</td>
</tr>
<tr>
<td></td>
<td>By default, Skype for Business Online is federated with all other Office 365 tenancies. For organisations that feel that this is not appropriate for their risk appetite it is possible to define a white or black-list of approved domains that federation is allowed or blocked with.</td>
</tr>
<tr>
<td>Azure AD Identity Protection</td>
<td><strong>This control requires the Security and Compliance Package.</strong></td>
</tr>
<tr>
<td></td>
<td>If an organisation cannot justify the Security and Compliance Package they should as a minimum configure it for privileged accounts and consider it for accounts that are...</td>
</tr>
</tbody>
</table>
Control | Description
--- | ---
| deemed to be of high value, e.g. accounts that are used to post to Social Media or members of your senior leadership team. Identities and the protection of them is important when considering the overall security posture of your organisation. Azure AD Identity Protection helps organisations preventing credential form being used in an insecure manner. Machine learning is used to determine risk level of sign-ins, this information can be used as part of Azure AD Conditional Access polices. Based on the identified risk users might be asked to change their password or provide MFA to access Office 365 services. | Enable customer lockbox feature
| This controls requires the Security and Compliance Package. Customer lockbox allows you to control how a Microsoft support engineer accesses your data. Customer lockbox requests allows you to control whether to give the support engineer access to your data and audit that approval | Configure Office 365 Advanced Threat Protection Safe Attachments feature
| This controls requires the Security and Compliance Package. An enhanced security control that is recommended in this guidance is to enable the Office 365 Advanced Threat Protection Safe Attachments feature. This will extend the malware protections in the service to include routing all messages and attachments that don’t have a known virus/malware signature to a special hypervisor environment where a behaviour analysis is performed using a variety of machine learning and analysis techniques to detect malicious intent. | Configure Office 365 Advanced Threat Protection Safe Links feature
| This controls requires the Security and Compliance Package. This will extend the phishing protection in the service to include redirecting all email hyperlinks through a forwarding service which will block malicious ones even after it has been delivered to the end user. This will protect your organisation from a link that was found to be malicious after the email was originally delivered therefore reducing the chance of a successful phishing attack. ATP Safe Links can help protect your organization by providing time-of-click verification of web addresses (URLs) in email messages and Office documents | |

**Best**

The controls included in this category have been identified as providing the best security capability. The controls listed in Table 3 will require specific configuration that is
organisation specific. Two of the controls, Azure AD Privileged Identity Management and Azure Information Protection require the Security and Compliance Package.

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure data loss prevention (DLP)</td>
<td>If your organisation has a requirement to prevent certain data types from leaving your organisation, then consider using Office 365 Data Loss Prevention. The guidance is that DLP should be restricted to those data types that have easily recognisable patterns, National Insurance Number, Passport Number or bank account. For more complex requirements we recommend the use of Azure Information Protection and human selectable labels to control sharing of information.</td>
</tr>
<tr>
<td>Azure AD Privileged Identity Management</td>
<td>This controls requires the Security and Compliance Package. Giving standing access to privileged roles in Azure AD and Office 365 increases the opportunity for malicious actors to gain access to systems in a privileged context. Azure AD Privileged Identity Management (PIM) allows enhanced capabilities in Azure AD, Office 365 and Intune when privileged tasks are required to control, manage and monitor access to those resources</td>
</tr>
<tr>
<td>Azure Information protection</td>
<td>This controls requires the Security and Compliance Package. Azure Information Protection (AIP) is a cloud-based solution that helps an organization to classify, label, and protect its documents and emails. This can be done automatically by administrators who define rules and conditions, manually by users, or a combination where users are given recommendations</td>
</tr>
</tbody>
</table>

2.2 Use of Office 365 Secure Score service

Additional security controls are suggested as part of Office 365 Secure Score service. Office 365 Secure Score is a security analytics tool which can improve the security posture of an organisation and lessen the chances of being hacked or suffering from a data breach.

Secure Score analyses your Office 365 environment in terms of how secure it is and suggests refinements that can further reduce your overall risk.

Many of the security controls described in this guidance are included in Secure Score. Where possible the configuration guidance refers to secure score as it makes deploying some features easier and gives confidence that they have been successfully enabled. However, simply relying on Secure Score as the only source of security guidance is not recommended as understanding the risk of not performing a configuration control is essential and simply
performing “security by numbers” exercise will not address key elements required to secure your Office 365 implementation. An example of this is given below:

**Secure Score includes the action to enable MFA for all Global Administrators in your tenant.** The guidance in Secure Score recommends that the Per-User configuration pages where this guidance recommends that Conditional Access driven MFA is used as it allows more flexibility and allows more controls to be enforced against users, e.g. block access to legacy authentication protocols, or allows control to admin interfaces, Admin Portal UI and PowerShell, to be configured.

This is covered in more detail Sections 3.3.4 Implement a holistic identity-centric Conditional Access approach and 3.4.4 Configure Office 365 Global Administrator role members.

For more information on Conditional Access please refer to [Conditional Access in Azure AD](https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditional-access-configure).
3 Core Configuration Controls

The following sections describe the security controls that are recommended for organisations that have purchased Microsoft M365 E3 licenses.

Section 4 Security and Compliance Package enhancements provides additional recommendations for those customers who have purchased the Security and Compliance Package.

Where possible organisations should look to implement as many of the controls in this guidance as possible to ensure that the security of their Office 365 tenant addresses the threats identified by the NCSC. Where you choose to deviate from the recommendations:

1. you should determine if the remaining residual risk is organisationally acceptable
2. if you are still able to meet your organisations compliance obligations
3. make note of any compensating controls in your organisations risk register

3.1 Identity

Security breaches of an Office 365 subscription, including information harvesting and phishing attacks, are typically done by compromising the credentials of an Office 365 global administrator account. Security in the cloud is a partnership between you, the customer, and Microsoft:

- Microsoft cloud services are built on a foundation of trust and security. Microsoft provides you security controls and capabilities to help you protect your data and applications.
- You own your data and identities and the responsibility for protecting them, the security of your on-premises resources, and the security of cloud components you control.

A core aspect of using Office 365 is the planning and security of the identities in your organisation. Previously organisations stored their identities on-premises in Active Directory Domain Services but when Office 365 (and other cloud services) are introduced the identity need to shift from being solely on-premises to a hybrid-identity model that allows organisations to access both on-premises resources as well as cloud services as well. Microsoft Azure Active Directory (Azure AD) is the cloud identity solution that provides the capability to extend users identities into the cloud.

Securing identity and more specifically the authentication process when users access cloud applications is critical to ensuring that your organisation remains secure. Users’ ability to sign in to cloud apps by using their on-premises usernames and passwords. This sign-in process to and how users authenticate make everything in the cloud possible.
Choosing the correct authentication method is the first concern for organizations wanting to move their apps to the cloud. Don't take this decision lightly, for the following reasons:

1. It's the first decision for an organization that wants to move to the cloud.
2. The authentication method is a critical component of an organization’s presence in the cloud. It controls access to all cloud data and resources.
3. It's the foundation of all the other advanced security and user experience features in Azure AD.
4. The authentication method is difficult to change after it's implemented.

Identity is the new control plane of IT security. So, authentication is an organization’s access guard to the new cloud world. Organizations need an identity platform that strengthens their security and keeps their cloud apps safe from intruders.

### 3.1.1 Authentication Methods

When the Azure AD hybrid identity solution is your new identity platform, authentication is the foundation of securing cloud access. Choosing the correct authentication method is a crucial first decision in setting up an Azure AD hybrid identity solution. Implement the authentication method that is configured by using Azure AD Connect, which also provisions users in the cloud.

To choose an authentication method, you need to consider the time, existing infrastructure, complexity, and cost of implementing your choice. These factors are different for every organization and might change over time.

Azure AD supports the following authentication methods for hybrid identity solutions.

#### 3.1.1.1 Cloud authentication

When using this authentication method, Azure AD handles users' sign-in process. Coupled with seamless single sign-on (SSO), users can sign in to cloud apps without having to re-enter their credentials. With cloud authentication, you can choose from two options:

- **Azure AD password hash synchronization.** The simplest way to enable authentication for on-premises directory objects in Azure AD. Users can use the same username and password that they use on-premises without having to deploy any additional infrastructure. Some premium features of Azure AD, like Identity Protection, require password hash synchronization for no matter which authentication method you choose. Passwords are never stored in clear text or encrypted with a reversible algorithm in Azure AD. For more information on the actual process of password hash
synchronization, see Implement password hash synchronization with Azure AD Connect sync.

- **Azure AD Pass-through Authentication.** Provides a simple password validation for Azure AD authentication services by using a software agent that runs on one or more on-premises servers. The servers validate the users directly with your on-premises Active Directory, which ensures that the password validation doesn’t happen in the cloud.

  Companies with a security requirement to immediately enforce on-premises user account states, password policies, and sign-in hours might use this authentication method. For more information on the actual pass-through authentication process, see User sign-in with Azure AD pass-through authentication.

3.1.1.2 Federated authentication

When you choose this authentication method, Azure AD hands off the authentication process to a separate trusted authentication system, such as on-premises Active Directory Federation Services (AD FS), to validate the user’s password.

The authentication system can provide additional advanced authentication requirements. Examples are smartcard-based authentication or third-party multifactor authentication. For more information, see Deploying Active Directory Federation Services.

The following section helps you decide which authentication method is right for you by using a decision tree. It helps you determine whether to deploy cloud or federated authentication for your Azure AD hybrid identity solution.
3.1.1.3 Decision tree

Use the decision tree in Figure 1 below to assist in making the cloud authentication model that is right for your organisation.

![Decision Tree Diagram]

Figure 1: Authentication method decision tree

The recommendation for this guidance in order of preference is as follows:

**Greenfield implementations**

For new environments, the preferred hybrid identity model in order of preference is:

1. Password Hash Sync plus Seamless SSO
2. Azure AD Pass-through Authentication plus Seamless SSO with Password Hash Sync
3. Federated Authentication with Password Hash Sync

**Brownfield implementations**

For organisations that have already implemented Office 365 it is likely that the hybrid-identity model that was used was Federated Authentication. This is still acceptable however strategically unless ADFS is required for other business requirements it is recommended that organisations move to a Password Hash Sync plus Seamless SSO hybrid authentication model. This is primarily to protect against loss of ADFS availability which will impact on an organisation's ability to access Office 365 services.

If Password Hash Sync has not been enabled as part of the Federated Authentication implementation then it is recommended that it is enabled in Azure AD Connect as this will
reduce the impact of AD FS not being available as part of either a unscheduled outage or ransomware attach.

Refer to Choose Azure AD authentication for more detailed explanation of how to choose the correct hybrid identity implementation.

### 3.2 Federated Hybrid-Identity Controls

The following controls are specific to organisations that have implemented Federated Hybrid-Identity but have not implemented Azure AD Conditional Access.

#### 3.2.1 Configure AD FS to use Azure MFA as the primary authentication mechanism

In ADFS 2016, you have the ability use Azure MFA as primary authentication for password-less authentication. Implementing this control is recommended to guard against password spray and password theft attacks: if there’s no password, it can’t be guessed. This works for all types of devices with various form factors.

It is now possible to use a password as the second factor only after your OTP has been validated with Azure MFA. Learn more about using password as the second factor here.

Whilst for federated identity scenarios this might seem the ideal solution as it enforces MFA and drops all username and password authentication attempts before they are even processed which is what is needed to address password spray attacks enforcing MFA on AD FS does still have limitations.

Azure AD Conditional Access provides additional security controls, such as preventing Legacy Authentication Protocols, device health, enforcement based on directory role, and device compliance.

Refer to the following article to configure Azure MFA as the Primary Authentication Mechanism

#### 3.2.2 Configure ADFS to Block Legacy Authentication from the Extranet

There are very few things an organisation can do which are as easy to deploy and can improve your security posture as much as blocking the use of Legacy Authentication Protocols. Legacy authentication is a term that refers to authentication protocols used by apps like:
• Older Office clients that do not use modern authentication (e.g., Office 2010 client)
• Clients that use mail protocols such as IMAP/SMTP/POP

Attackers look to abuse legacy authentication protocols as part of **password spray attacks**! This is because legacy authentication protocols don’t support interactive sign-in, which is required for additional security challenges like multi-factor authentication and device authentication.

If your organisation identifies an application that does not support Modern Authentication but is required by the business, then password spray attacks will continue to be a problem. If this is the case, then implementing MFA as the primary authentication method for AD FS is recommended. To help reduce the impact of applications that do not support Modern Authentication Azure MFA service includes the ability to use **App Passwords**. An app password is used in place of your original password with these non-browser apps. This is because when you register for two-step verification, you’re telling Microsoft not to let anyone sign in with your password if they can’t also perform the second MFA verification.

For example, the Apple native email client on your phone can’t sign in as you because it can’t ask for two-step verification. The solution for this is to create a more secure app password that you don’t use day-to-day, but only for those apps that can’t support two-step verification. Use the app password so that apps can bypass multi-factor authentication and continue to work.

Therefore, it is strongly recommended that this security control is implemented for your Office 365 tenancy.

Where Azure AD Conditional Access is not possible legacy authentication protocols don’t have the ability to enforce MFA, so the best approach is to **block them from the extranet**. This will prevent password spray attackers from exploiting the lack of MFA on those protocols.

The article referenced above describes how to use ADFS rules to control legacy protocols from the Extranet. The article gives several possible options for the ADFS rules. The rules listed below are the recommended ones for this guidance.

### Table 4: Recommended ADFS claims rules for legacy protocol control

<table>
<thead>
<tr>
<th>Recommended Claims Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>@RuleName = &quot;Block Exchange ActiveSync&quot;</td>
</tr>
<tr>
<td>@RuleName = &quot;Allow all intranet traffic&quot;</td>
</tr>
<tr>
<td>c1:[Type == &quot;<a href="http://schemas.microsoft.com/ws/2002/01/insidcorporatenetwork">http://schemas.microsoft.com/ws/2002/01/insidcorporatenetwork</a>&quot;, Value == &quot;true&quot;] =&gt; issue(Type = &quot;<a href="http://schemas.microsoft.com/authorization/claims/permit">http://schemas.microsoft.com/authorization/claims/permit</a>&quot;, Value = &quot;true&quot;);</td>
</tr>
</tbody>
</table>
**Recommended Claims Rules**

@RuleName = "Allow extranet browser and browser dialog traffic"

c1:[Type == "http://schemas.microsoft.com/ws/2012/01/insidecorporatenetwork", Value == "false"] &&
c2:[Type == "http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-endpoint-absolute-path", Value =~ "/(adfs/ls)|(adfs/oauth2)"]

=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true");

Azure AD Conditional Access now includes the ability to prevent the use of legacy authentication protocols, refer to Section 3.3.1 Prevent use of Legacy Authentication Protocols later in this document for details of how to use Azure AD Conditional Access to meet this security control.

It is recommended that where possible Azure AD Conditional Access is used to prevent the use of Legacy Authentication Protocols rather than using ADFS claims rules to implement this technical control.

### 3.2.3 Enable ADFS Web Application Proxy Extranet Lockout

If you do not have extranet lockout in place at the ADFS Web Application proxy, it is recommended that it is enabled as soon as possible to protect your users from potential password brute force compromise.

The Extranet Lockout feature in AD FS works independently from the AD lockout policy. However, you do need to make sure the settings for the Extranet Lockout is properly configured so that it can serve its security purpose with the AD lockout policy. Refer to Working with the Active Directory Lockout Policy

Microsoft has just released Smart Lockout which uses data from Azure AD to lock out attackers who have been observed trying to perform password spray attacks or trying to brute force specific user accounts. That intelligence can recognize sign-ins coming from valid users and treats those differently than ones that attackers and other unknown sources. This means smart lockout can lock out the attackers while letting your users continue to access their accounts and be productive.

Using Azure AD backed Smart Lockout is the preferred method for blocking attackers from attempting to compromised passwords. Refer to Azure AD Password Protection and Smart Lockout
3.2.4 Configure Conditional Access using ADFS

The overall function of AD FS is to issue an access token that contains a set of claims. The decision regarding what claims AD FS accepts and then issues is governed by claim rules.

Access control in AD FS is implemented with issuance authorization claim rules that are used to issue a permit or deny claims that will determine whether a user or a group of users will be allowed to access AD FS-secured resources or not. Authorization rules can only be set on relying party trusts.

<table>
<thead>
<tr>
<th>Rule option</th>
<th>Rule Logic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit all users</td>
<td>If incoming claim type equals <em>any claim type</em> and value equals <em>any value</em>, then issue claim with value equals Permit</td>
</tr>
<tr>
<td>Permit access to users with this incoming claim</td>
<td>If incoming claim type equals <em>specified claim type</em> and value equals <em>specified claim value</em>, then issue claim with value equals Permit</td>
</tr>
<tr>
<td>Deny access to users with this incoming claim</td>
<td>If incoming claim type equals <em>specified claim type</em> and value equals <em>specified claim value</em>, then issue claim with value equals Deny</td>
</tr>
</tbody>
</table>

In AD FS in Windows Server 2012 R2 or later, access control is enhanced with multiple factors, including user, device, location, and authentication data. This is made possible by a greater variety of claim types available for the authorization claim rules. In other words, in AD FS in Windows Server 2012 R2, you can enforce conditional access control based on user identity or group membership, network location, device (whether it is workplace joined, for more information, see Join to Workplace from Any Device for SSO and Seamless Second Factor Authentication Across Company Applications), and the authentication state (whether multifactor authentication (MFA) was performed).

Conditional access control in AD FS in Windows Server 2012 R2, offers the following benefits:

- Flexible and expressive per-application authorization policies, whereby you can permit or deny access based on user, device, network location, and authentication state
- Creating issuance authorization rules for relying party applications
- Rich UI experience for the common conditional access control scenarios
- Rich claims language & Windows PowerShell support for advanced conditional access control scenarios
- Custom (per relying party application) 'Access Denied' messages. For more information, see Customizing the AD FS Sign-in Pages. By being able to customize these messages, you can explain why a user is being denied access and also facilitate
self-service remediation where it is possible, for example, prompt users to workplace join their devices

examples of implementing conditional access control in AD FS in Windows Server 2012 R2 include the following:

- Permit access to an application secured by AD FS only if this user’s identity was validated with MFA

```xml
@RuleTemplate = "Authorization"
@RuleName = "PermitAccessWithMFA"
```

- Permit access to an application secured by AD FS only if the access request is coming from a workplace joined device that is registered to the user

```xml
@RuleTemplate = "Authorization"
@RuleName = "PermitAccessFromRegisteredWorkplaceJoinedDevice"
c[:Type == "https://schemas.microsoft.com/2012/01/devicecontext/claims/isregistereduser", Value =~ "^(?i)true$"] => issue(Type = "https://schemas.microsoft.com/authorization/claims/permit", Value = "PermitUsersWithClaim");
```

- Permit access to an application secured by AD FS only if the access request is coming from a workplace joined device that is registered to a user whose identity has been validated with MFA

```xml
@RuleTemplate = "Authorization"
@RuleName = "RequireMFAOnRegisteredWorkplaceJoinedDevice"
```

- Permit extranet access to an application secured by AD FS only if the access request is coming from a user whose identity has been validated with MFA.
The functionality ADFS to implement Conditional Access is not nearly as rich as that of Azure AD Conditional Access. Where possible Azure AD Conditional Access should be used in preference to the ADFS controls.

Refer to Section 3.3.4 Implement a holistic identity-centric Conditional Access approach later in this guidance.

### 3.3 Recommended Identity Controls

The following sections the recommended security controls that apply to both standard and privileged identities. Section 3.4 Specific considerations for protecting Privileged identity provides additional controls that are deemed appropriate for Privileged Identities.

#### 3.3.1 Prevent use of Legacy Authentication Protocols

There are very few things an organisation can do which are as easy to deploy and can improve your security posture as much as blocking the use of Legacy Authentication Protocols.

Therefore, it is strongly recommended that this security control is implemented for your Office 365 tenancy.

Legacy authentication is a term that refers to authentication protocols used by apps like:

- Older Office clients that do not use modern authentication (e.g., Office 2010 client)
- Clients that use mail protocols such as IMAP/SMTP/POP

Legacy Authentication Protocols do not support MFA making user name and password the only authentication mechanism available. The use of user name and password only opens organisations up to many attack-vectors the most common one being password spray attacks. Microsoft wrote a blog about how to mitigate password spray attacks here, [Azure AD and ADFS best practices: Defending against password spray attacks](https://aka.ms/AzureADAdfs-spray).

One of the mitigations described in the blog was to Block legacy authentication from the Extranet using ADFS, this is described earlier in this document in Section 3.2.2 Configure ADFS to Block Legacy Authentication from the Extranet.
The ability to block Legacy Authentication Protocols is now available as part of Azure AD Conditional Access policies. Inclusion in Azure AD Conditional Access means that blocking the use of Legacy Authentication Protocols is now achievable as part of your organisation's holistic conditional access strategy.

Refer to https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-conditions#legacy-authentication for more information.

Configure technical control

To configure a Azure AD Conditional Access Policy to prevent use of Legacy Authentication Protocols follow the steps outlined below:

1. In the Azure AD portal, go to “Conditional access” and create a new policy.
2. Select the users for your pilot group. As with all conditional access policies, we recommend starting with a small set of users to be sure you understand the support and end user experience impact.
3. Select “All cloud apps”.
4. Under the “Client apps” conditions, you should now see the “Other clients” checkbox. The “Other clients” checkbox includes older Office clients that do not support modern authentication, as well as clients that use mail protocols like POP, IMAP, SMTP, etc.

![Client apps (preview)](image)

Figure 2: Legacy Authentication control

5. Select the “Block access” control.
6. Save the policy.
Validate technical control

To validate that Legacy Authentication Protocols are disabled perform the following

1. Open Azure AD PowerShell
2. Run the following PowerShell cmd
   
   ```powershell
   Revoke-AzureADUserAllRefreshToken -ObjectID <GUID of User Object>
   ```

   Remember to wait for at least 1 hour before running the next step.

3. Attempt to connect to Office 365 service using an old version of Office client, e.g. Office 2010
4. Access should be blocked.

### 3.3.2 Configure Azure AD Password Protection

Azure AD Password Protection helps you eliminate easily guessed passwords from your environment, which can dramatically lower the risk of being compromised by a password spray attack. Specifically, these features let you:

1. Protect accounts in Azure AD and Windows Server Active Directory by preventing users from using passwords from a list of more than 500 of the most commonly used passwords, plus over 1 million character substitution variations of those passwords.
3. Customize your Azure AD smart lockout settings and specify a list of additional company specific passwords to block.

The fix to all of this is to apply a banned password system when users change their passwords, like Azure AD Password Protection. This is both the NIST recommendation and what we do in the cloud for Microsoft accounts and Azure AD accounts.

Microsoft recently announced that it would extend this capability to on-premises ADDS, wherever your users change their passwords. This feature is powered by Azure AD, which regularly updates the database of banned passwords by learning from billions of authentications and analysis of leaked credentials across the web.

By checking all the password set or reset operations for your organization, password protection ensures that only passwords meeting your, and our, standards exist in your directory. Azure AD Password Protection also provides an integrated admin experience to control checks for passwords in your organization, in Azure and on-premises.

Refer to [Azure AD Password Protection and Smart Lockout](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/password-protection)
3.3.3 Enable MFA for all users

The secure score service recommends MFA for all users, however the user community typically prefer a more unobtrusive solution, achievable with a Conditional Access design that utilises one or more Conditional Access grant controls to supplement the basic, single-factor user credentials with either multi-factor authentication, compliant or domain-joined device, or an enlightened app subject to app protection policies or mobile device management policies.

The Secure Score recommendation for implementing MFA is to use per-user MFA using the following link, https://account.activedirectory.windowsazure.com/UserManagement/MultifactorVerification.aspx. Refer to multi-factor authentication deployment guide

This guidance recommends that MFA is implemented as part of utilizing Azure AD Conditional Access policies, refer to Section 3.3.4, Implement a holistic identity-centric Conditional Access approach, as this provides more pragmatic guidance than a blanket MFA policy that is implemented using the per-user model.

Refer to the previous notes for Blocking Legacy Authentication protocols as they apply to Standard users.

The NCSC has recently issued guidance on Multi-Factor Authentication for online services

The MFA approach described in this document aligns with the characteristics described in the NCSC guidance.
3.3.4 Implement a holistic identity-centric Conditional Access approach

MFA can be enabled in one of two ways:

- **Per-user.** Users are set to an ENABLED state, which means they must register; when registered they are ENFORCED, which means any refresh token that does not have an MFA attribute (or claim) undergoes MFA
- **Conditional Access-driven.** Users are not ENFORCED and are instead subject to MFA invocation based on one or more Conditional Access policies

The Office 365 Secure Score recommends that MFA is enabled for all users, as per Section 3.3.3 Enable MFA for all users this meets the “Good” bar when considered in the context of the Good, Better, Best rationale that was described previously in Section 2 Technical Design for Secure Configuration Alignment. However, such an approach is atypical and generally unpalatable from a business requirements perspective, i.e. it is a pure security requirement and control and too aggressive for the business.

Azure Active Directory Conditional Access provides the ability to utilise a layered, more structured approach with less impact on business users and as such meets the “Better” bar when considered under the Good, Better, Best model. As a result, implementing MFA using Azure Active Directory Conditional Access is the recommended approach for this guidance.

The Conditional Access driven approach is the most flexible and recommended and is the only approach discussed here. Unfortunately, Secure Score information redirects administrators to the per-user configuration pages. Furthermore, the secure score service recommends MFA for all users, however the user community typically prefer a more unobtrusive solution, generally layered with the other Conditional Access grant controls:

- **Multi-factor authentication.** Use this control to require multi-factor authentication to access specified cloud apps. Using multi-factor authentication helps protect resources from being accessed by an unauthorised user who might have gained access to the primary credentials of a valid user
- **Compliant device.** Use this control to require a compliant device to access specified cloud apps. Requiring a compliant device grants access to access attempts made with devices that are joined to the Azure Active Directory tenant and are marked as compliant by Intune or a compliant MDM solution
- **Domain-joined device.** Use this control to require an Active Directory Domain Services domain-joined device to access specified cloud apps. Requiring a domain-joined device grants access to access attempts made with Windows desktops, laptops, and enterprise tablets that are joined to an on-premises Active Directory domain and the Azure Active Directory tenant
- **Approved client app.** Use this control to require Intune enlightened apps to access specified cloud apps. Requiring approved client apps grants access to access
attempts made by a client app that supports Intune app protection policies. For example, restrict access to Exchange Online to the Outlook app.

Conditional Access policies that implement multiple grant controls provide higher levels of security than a set of basic credentials alone without introducing the additional burden of many multi-factor verification responses. Consider implementing the following Conditional Access policies as a baseline.

Conditional Access also uses Conditions to capture an occurrence and stipulate an action based on that condition. Conditional Access used a number of conditions, refer to this article for more details. Specifically Sign-in Risk, Device State and Locations are useful for controlling access for both standard and privileged accounts.

**Sign-in Risk**

A sign-in risk is an indicator for the likelihood (high, medium, or low) that a sign-in attempt was not performed by the legitimate owner of a user account. Azure AD calculates the sign-in risk level during the sign-in of a user. You can use the calculated sign-in risk level as condition in a conditional access policy.

Common use cases for this condition are policies that:

- Block users with a high sign-in risk to prevent potentially non-legitimate users from accessing your cloud apps.
- Require multi-factor authentication for users with a medium sign-in risk. By enforcing multi-factor authentication, you can provide additional confidence that the sign-in is performed by the legitimate owner of an account.

The Sign-in risk condition required Azure AD Identity Protection to be enabled which requires that Security and Compliance Package has been licensed. Refer to Section 4.1.1 Azure AD Identity Protection later in this document for more details.

**Device State**

The device state condition allows Hybrid Azure AD joined and devices marked as compliant, Azure AD joined devices, to be excluded from a conditional access policy. This is useful when a policy should only apply to unmanaged device to provide additional session security. Refer to device-based conditional access for more details of how to utilise this condition.

**Locations**

With locations, you have the option to define conditions that are based on where a connection attempt was initiated from. Common use cases for this condition are policies that:

- Require multi-factor authentication for users accessing a service when they are off the corporate network.
• Block access for users accessing a service from specific countries or regions.

Refer to [What is the location condition in Azure Active Directory conditional access](#) for more details.

For more details on Conditional Access refer to [What is conditional access in Azure Active Directory](#)

**Configure technical control(s)**

It is expected that additional policies will supplement this baseline, based on the security requirements that surround the data classification around the in-scope apps, however as a baseline Policy 2 provides greater control and protection without mandating lots of MFA verification responses.

<table>
<thead>
<tr>
<th>Table 6: Standard User Conditional Access policies</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Users, groups or Roles</strong></td>
</tr>
<tr>
<td><strong>Policy 1</strong></td>
</tr>
<tr>
<td><strong>Policy 2</strong></td>
</tr>
</tbody>
</table>

The Conditional Access policy assignment is scoped to the appropriate security group; all cloud apps; and has the conditions: all platforms, all locations, and all client apps; and has grant controls: require MFA and Compliant (for Intune managed devices) or Domain-joined (for Active Directory managed devices). Use of these grant controls prevents access from unmanaged devices and when combined with the new capability to block access to [legacy authentication protocols](#). Conditional Access is able to address concerns about password used when access cloud services as all of the interfaces that accept username and password are blocked by the Conditional Access policy.

For more information, see:

- [Azure Active Directory device-based conditional access policies](#)
- [Approved client app requirement](#)

¹ This assumes that devices will be Intune Managed. If devices are on-premises Active Directory joined then change the condition to Domain-joined Device.
Validate technical control(s)

Validation of the control is achieved in two ways. Firstly, the Azure Active Directory conditional access what if tool can demonstrate whether an actor is in-scope of the policy and the outcome of the policy application:

- [https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-whatif](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-whatif)

The what if tool outputs in-scope and out-of-scope policies, i.e. what will apply and what will not apply, for a given actor (user) under a set of conditions (cloud app, client app, IP address and location, sign-in risk).

Secondly, simple testing substantiates, i.e. sign-on as a non-administrative user and ascertain whether MFA is required when not using a compliant or domain-joined device.

Lastly, Azure AD sign-in logs provide MFA status.

3.3.5 Do not expire passwords

The NCSC’s own password guidance was updated in 2016. One of the key changes in this guidance was the removal of regular password changes for standard users as part of an organisations password policy

Configure technical control

To configure Office 365 password policy so that it is set to never expire perform the following actions:

2. Click the “Set passwords to never expire” checkbox
3. Click “Save” to confirm the policy setting.

It is also recommended that once you configure this setting that you also enable Self-Service Password Reset (SSPR) in Azure AD admin centre.

After you turn on self-service password reset, you need to send your people to the following website, so they can set up their alternate phone number or email address. [Don’t lose access to your account](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-whatif)

Validate technical control

To validate that user’s passwords have been correctly set to never expire run the following from an elevated PowerShell console
Get-MSOLUser | Select UserPrincipalName, PasswordNeverExpires

3.3.6 Disable accounts not used in last 30 days

You should disable any accounts that have not been used in the last 30 days. While there may be legitimate circumstances where an account is unused for 30 days, these accounts can also be targets for attackers who are looking to find ways to access your data without being noticed.

Configure technical control

This is not a technical control it is an operational review of logon information

Validate technical control

Review information in Office 365 Admin Center using the following link, https://portal.office.com/Admin/Default.aspx#ActiveUsersPage

For accounts that are anchored against on-premises AD DS you can run the following command form an elevated PowerShell console.

```
Search-ADAccount -AccountInactive -TimeSpan ([timespan]10d) -UsersOnly | Set-ADUser -Enabled $false -WhatIf
```

3.3.7 Configure certificate-based authentication for mobile devices

Certificate-based authentication (CBA) enables you to be authenticated by Azure Active Directory with a client certificate on a Windows, Android, or iOS device when connecting your Exchange online account to:

- Microsoft mobile applications such as Microsoft Outlook and Microsoft Word
- Exchange ActiveSync (EAS) clients

Configuring this feature eliminates the need to enter a username and password combination into certain mail and Microsoft Office applications on your mobile device.

Certificate-based authentication (CBA) is only supported for Federated environments for browser applications or native clients using modern authentication (ADAL). The one exception is Exchange Active Sync (EAS) for Exchange Online (EXO), which can be used for federated and managed accounts.

Refer to CBA Requirements for additional requirements for CBA.

CBA is available for Android and iOS based devices, refer to Azure Active Directory certificate-based authentication on iOS devices and Azure Active Directory certificate-based authentication on Android devices.
Configure technical control

To configure CBA for either iOS or Android devices refer to Enable device based certificate-based authentication in Azure Active Directory and the following blog article, Certificate based authentication – O365

Validate technical control

To validate that CBA is being used to authenticate to Office 365 services from iOS and Android devices simply attempt to open Office Mobile application on your phone. If you are not prompted to enter a username or password, then CBA is working as expected.
3.4 Specific considerations for protecting Privileged identity

The security of most or all business assets in the modern organization depends on the integrity of the privileged accounts that administer and manage IT systems. Malicious actors including cyber-attackers often target admin accounts and other elements of privileged access to attempt to rapidly gain access to sensitive data and systems using credential theft attacks. For cloud services, prevention and response are the joint responsibilities of the cloud service provider and the customer.

Make sure you have at least two Global Admins designated to ensure that you can protect against a rogue insider and to ensure a breach of one of those accounts can be recovered. Refer to Section 3.4.6 Configure break glass accounts in Azure AD and Securing Privileged Roles for more details.

In addition to the recommended controls listed in the following section refer to Securing privileged access for hybrid and cloud deployments in Azure AD. This article describes the recommended roadmap to securing privileged access in four stages.

The following describes the recommended practices that should be used to secure privileged identities used to administer Azure AD and Office 365:

- Use a dedicated account for administration tasks
- Operate a least privileged model by keeping the number of Global Administrators to more than two but less than five individuals. These accounts should not be routinely used and should be monitored for their use.
- Operate a least privileged model by assigning non-global admin roles to other people who administer Office 365 Services, e.g. Password Administrator, User management administrator or the highly privileged eDiscovery administrator role which still does not get Global Administrator privilege
- Configure Emergency Accounts in case of emergency

It is recommended that the Security and Compliance Package is purchased for all Privileged Administrator accounts in an organisation the additional security benefits, specifically Azure AD Privileged Identity Management, Azure AD Identity Protection and Windows Defender Advanced Threat Protection will enable organisations to maintain security posture that will help to secure their Office 365 service.

The following sections describe how to configure the suggested controls as well as how to validate that the controls have been implemented correctly.
3.4.1 Prevent use of Legacy Authentication Protocols

There are very few things an organisation can do which are as easy to deploy and can improve your security posture as much as blocking the use of Legacy Authentication Protocols. This is particularly important for Privileged Identities and therefore, it is therefore mandated that this security control is implemented for all Privileged Identities that are used to administer your Office 365 tenancy.

3.4.2 Location for privileged identities

The location where the accounts are anchored that are used to administer Microsoft Azure AD and Office 365 is important. The following are the recommendations for where privileged identities should be anchored.

- It is important that no on-premises privileged AD DS accounts, e.g. Tier 0 admin accounts (including accounts, groups, and other assets that have direct or indirect administrative control of the AD forest, domains, or domain controllers, and all assets) must only be used for on-premises administrative tasks. These accounts should not be synchronized with Azure AD therefore granting access to cloud services.
- It is recommended that cloud identity, .onmicrosoft.com accounts are used to perform all privileged administration tasks in Azure AD and Office 365.

Refer to Securing privileged access for hybrid and cloud deployments in Azure AD for a more detailed roadmap.

3.4.3 Use dedicated accounts to perform Administrative Tasks

It is recommended that users do not use their day to day account to perform administrative tasks. Using the same account for both general web browsing, and email increases the chance that a privileged administration account will be phished or subject to another attack which will lead to compromise of the cloud service.

Refer to Securing Privileged Access roadmap and Securing privileged access for hybrid and cloud deployments in Azure AD

3.4.4 Configure Office 365 Global Administrator role members

By default, the account that initially sets up Office 365 subscription is made a member of the Global Administrators group for Azure AD and each of the Office 365 services. However, the person who originally set up the Office 365 Subscription might not be the person or persons who are going to be responsible for administration of the Office 365 Service.

It is recommended that a naming standard is used to easily identify privileged accounts in your organisation, e.g. JohnDoe-GA or JohnDoe-ADM.
This control reviews the membership of Global Administrators group for standard user accounts and privileged accounts that have no need to be members of the Azure AD Global Administrator role.

These accounts must be monitored so their use is included in alerts. Extending this to your SIEM product as a high priority alert to notify your SOC / security team if one of these accounts is used.

**Configure technical control**

1. Identify at least two and no more than five individuals that will be members of the Azure AD Global Administrator role.
2. Sign into your Office 365 subscription with a user account that has been assigned the global admin role.
3. Determine the set of user accounts that have been assigned the global admin role. You can do this with this command at the Microsoft Azure Active Directory Module for Windows PowerShell command prompt:
   
   `Get-MsolRoleMember -RoleObjectId (Get-MsolRole -RoleName "Company Administrator").ObjectId`

4. Review the output and identify any accounts that are standard user accounts or administrative accounts that should not be members of the Azure AD Global Administrator group.
5. Create a new dedicated privileged account for any identified users who are not currently members of the Global Administrators role.
6. Remove any accounts that are currently member of the Global Administrator role but are either normal user accounts or belong to administrators who have not been identified as Global Administrators for your organisation.

**Validate technical control**

Once the configuration tasks have been completed review the members of the Global Administrators group.

1. Re-run the command at the Microsoft Azure Active Directory Module for Windows PowerShell command prompt:
   
   `Get-MsolRoleMember -RoleObjectId (Get-MsolRole -RoleName "Company Administrator").ObjectId`

It is important to monitor for suspicious global administrator account activity. Refer to Section 3.5.17 Enable for details of how to monitor for Global Administrator activity.

**3.4.5 Use Non-Global Administrative roles**

Operating a least privilege model is an important control to reduce the impact should a privileged identity be breached. Ensuring that wherever possible non-global administrator
roles are used to perform administrative tasks against Azure AD, Intune and Office 365 services will help to reduce the overall risk exposure of your cloud services.

Designate alternate roles for global admins such that they can complete needed tasks but only with the least privileged required for the task. For example, if your user is primarily responsible for Exchange Online administration, you should use that role instead of the Global admin role to reduce the impact of a potential breach of that account.

Configure technical control

**Secure Score Portal**

2. Scroll down to All Actions and locate the **Use non-global administrative roles** action from the list
3. Expand the action and click the Update link
4. Review the returned list of Global Administrators. If any of the returned accounts can be assigned a non-global administrative role either select the role from the dropdown list or click the **More** button to launch the Office 365 Admin Center Active Users blade, https://portal.office.com/AdminPortal/Home#/users
5. Select the account identified previously
6. Under the Roles select a more appropriate privileged role for the user.
7. If the administrative role is not displayed in the list switch to the Azure AD blade in Azure Admin Portal, https://portal.azure.com/#blade/Microsoft_AAD_IAM/UsersManagementMenuBlade/All%20users
8. Select the identified user and then Directory Role from the options under Manage
9. Change the Directory Role to Limited Administrator and select the appropriate roles for that user from the list displayed, e.g. Password Administrator or User Administrator

**Information**

It is recommended that you also configure Conditional Access for any accounts that are granted additional directory roles in your organisation. Conditional Access supports the use of Directory Roles as a condition for the policy. Refer to [Users and Groups](#) details in Conditional Access documentation

**Further reading**

For more details about the administrative roles available by default in Azure AD refer to [Assigning administrator roles in Azure Active Directory](#).

For more details about RBAC models for


SharePoint Online refer to [https://support.office.com/en-us/article/About-the-SharePoint-Online-admin-role-f08144d5-9d50-4922-8e77-4e1a27b40705](https://support.office.com/en-us/article/About-the-SharePoint-Online-admin-role-f08144d5-9d50-4922-8e77-4e1a27b40705) and [https://support.office.com/en-us/article/understanding-permission-levels-in-sharepoint-87ecbb0e-6550-491a-8826-c075e4859848](https://support.office.com/en-us/article/understanding-permission-levels-in-sharepoint-87ecbb0e-6550-491a-8826-c075e4859848)

Skype for Business Online does not have a RBAC model. The Skype for Business administrator role is described here, [https://support.office.com/en-us/article/about-the-skype-for-business-admin-role-aeb35bda-93fc-49b1-ac2c-c74fbeb737b5](https://support.office.com/en-us/article/about-the-skype-for-business-admin-role-aeb35bda-93fc-49b1-ac2c-c74fbeb737b5)

Validate technical control

**PowerShell**

TechNet Script gallery has a nice script that will list all of the [Office 0365 Admin Role Groups Memberships Report](https://support.office.com/en-us/article/About-the-Exchange-Admin-Role). Review the csv file generated for accounts that are members of the Company Administrators and all other privileged roles in Azure AD.

### 3.4.6 Configure break glass accounts in Azure AD

In addition to users' taking on administrative access rights for themselves, you need to prevent being inadvertently locked out of the administration of your Azure AD tenant because you can neither sign in nor activate an existing individual user's account as an administrator. You can mitigate the impact of inadvertent lack of administrative access by storing two or more *emergency access accounts* in your tenant.

Emergency access accounts can help organizations restrict privileged access within an existing Azure Active Directory environment. Such accounts are highly privileged, and they are not assigned to specific individuals. Emergency access accounts are limited to emergency or ‘break glass' scenarios, situations where normal administrative accounts cannot be used. Organisations must maintain a goal of restricting the emergency account’s usage to only that time during which it is necessary.

These accounts must be monitored so their use is included in alerts. Extending this to your SIEM product as a high priority alert to notify your SOC / security team if one of these accounts is used.
These accounts should be cloud-only identities that use .onmicrosoft.com and are not federated or synchronised from your on-premises Active Directory environment.

Refer to Manage emergency access administrative accounts for more detailed information.

### 3.4.7 Enable MFA for all Global Admins

It is mandated that organisations enable MFA to protect all Global Administrator accounts. Enabling MFA for these privileged accounts will make it significantly more difficult for these accounts to be compromised because a breach of any of those accounts can lead to a breach of your data.

For organisations that use or plan to use Windows Hello for Business, the MFA requirement can be met using the Windows Hello sign in experience. For more information, see Windows Hello

Azure Identity Protection can help to address the risk of using passwords, see Section 4.1.1 Azure AD Identity Protection later in this document.

It is sufficient that the use of Conditional Access rules that require MFA meet this recommendation

Configure technical control

MFA can be enabled in one of two ways:

- **Per-user.** Users are set to an ENABLED state, which means they must register; when registered they are ENFORCED, which means any refresh token that does not have an MFA attribute (or claim) undergoes MFA

- **Conditional Access driven.** Users are not ENFORCED and are instead subject to MFA invocation based on one or more Conditional Access policies

The Conditional Access driven approach is the most flexible and recommended and is the only approach discussed in this guidance. Unfortunately, Secure Score information redirects administrators to the per-user configuration pages.
It is recommended that you implement the following Conditional Access policies:

Table 7: Recommended Conditional Access policies for Global Administrators

<table>
<thead>
<tr>
<th>Policy</th>
<th>Users, groups or Role</th>
<th>Cloud apps</th>
<th>Risk</th>
<th>Platform</th>
<th>Location</th>
<th>Client apps</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy 1</td>
<td>Global Administrator</td>
<td>All cloud apps</td>
<td>iOS</td>
<td>Android</td>
<td>Browser</td>
<td>MFA and Compliant</td>
<td></td>
</tr>
<tr>
<td>Policy 2</td>
<td>All users except administrators group</td>
<td>All cloud apps</td>
<td>iOS</td>
<td>Android</td>
<td>Windows</td>
<td>Mobile and desktop</td>
<td>MFA OR Compliant OR Domain Joined</td>
</tr>
</tbody>
</table>

The Global Administrator role is used to apply the Conditional Access Policy to all Global Administrators. The CA policy assignment is scoped to the security group; all cloud apps; and has the conditions: all platforms, all locations, and all client apps; and has two grant controls: require MFA and Compliant.

The table above illustrates how non-administrative users are subject to different controls, i.e. MFA or compliance/hybrid domain-joined.

Validate technical control

Validation of the control is achieved in two ways. Firstly, the Azure Active Directory conditional access what if tool can demonstrate whether an actor is in-scope of the policy and the outcome of the policy application:

- [https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-whatif](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-whatif)

The what if tool outputs in-scope and out-of-scope policies, i.e. what will apply and what will not apply, for a given actor (user) under a set of conditions (cloud app, client app, IP address and location, sign-in risk).
Figure 3: Conditional Access what if tool output

Secondly, simple testing substantiates that the control is in place, i.e. sign-on as an administrative user and ascertain whether MFA is required.

Lastly, Azure AD sign-in logs provide MFA status.
3.5 Office 365 Service Configuration

The following section outlines the recommended security controls for Office 365 services.

3.5.1 Enable Modern Authentication

A core aspect of the identity controls discussed previously related to the disabling of Legacy Authentication Protocols. In order to move away from the use of these Legacy Authentication Protocols Modern Authentication must be enabled.

Modern Authentication is a pre-requisite for using Multi-factor authentication. As described in Section 3.3.1 Prevent use of Legacy Authentication Protocols earlier in this document it also allows you to disable the use of legacy authentication protocols that are used by older clients, Exchange Active Sync, IMAP and POP3. It is using these legacy authentication protocols that is abused as part of a password spray attack.

By default, all new Office 365 tenants are configured with Modern Authentication enabled for the application services.

However, it is recommended that you verify that Modern Authentication is enabled for Exchange Online, SharePoint Online and Skype for Business Online if your Office 365 tenant was created before the default configuration was changed to enabled.

Verify Technical Control

To verify that Modern Authentication is enabled for Office 365 services perform the following:

Exchange Online

1. Open Exchange Management Shell
2. Connect to Exchange Online as a user who is a member of the Exchange Global Admin role
3. Run the following

   Get-OrganizationConfig | Format-Table -Auto Name, OAuth*

4. Verify that OAuth2ClientProfileEnabled value returned is True

SharePoint Online

1. Open SharePoint Management Shell
2. Run the following command

   (Get-SPOTenant).LegacyAuthProtocolsEnabled
3. If the returned value is False, then only Modern Authentication is enabled for SharePoint

Skype for Business Online

1. Connect to Skype for Business Online using remote PowerShell:
2. Run the following command:
3. Verify that Modern Authentication is configured by running the following:
4. If the returned value is Allowed, then Modern Authentication is configured

Configure Technical Control

To enable Modern Authentication for Exchange Online, SharePoint Online and Skype for Business Online perform the following steps.

Exchange Online

1. Open Exchange Management Shell
2. Connect to Exchange Online as a user who is a member of the Exchange Global Admin role
3. Run the following
4. If the returned value is Allowed, then Modern Authentication is configured

SharePoint Online

1. Open SharePoint Management Shell
2. Connect to SharePoint Online as a user who is a member of SharePoint Global Administrators role
3. Run the following command
4. If the returned value is False, then only Modern Authentication is enabled for SharePoint

Skype for Business Online

1. Connect to Skype for Business Online using remote PowerShell:
2. Run the following command:
3. Verify that Modern Authentication is configured by running the following:
4. If the returned value is Allowed, then Modern Authentication is configured
3.5.2 Exchange Online

The following controls a specific to Exchange Online.

3.5.3 Enable audit data recording

Failure to enable auditing impacts incident response teams ability to be able to investigate breaches

When an Organization has already deployed Office 365, it is critical for Administrators to be able to keep track of what users do with Documents, Emails, SharePoint etc. for various security and compliance reasons of the organization.

Configure technical control

Before audit log data is available in the unified audit log, user tracking must be enabled. This is done via the security and compliance centre audit log search or using PowerShell. Both methods are documented in this article [https://support.office.com/en-us/article/turn-office-365-audit-log-search-on-or-off-e893b19a-660c-41f2-9074-d3631c95a014](https://support.office.com/en-us/article/turn-office-365-audit-log-search-on-or-off-e893b19a-660c-41f2-9074-d3631c95a014)

3.5.4 Enable mailbox auditing for all users

Configuring the correct audit settings for all mailboxes it extremely important when investigating incidents or potential breaches. Unless this is correctly configured incident response teams will not be able to obtain the full picture of what occurred as part of the incident and the exact details of what data was exfiltrated will never be able to be identified

By default, all non-owner access is audited, but you must enable auditing on the mailbox for owner access to also be audited. This will allow you to discover illicit access of Exchange Online activity if a user’s account has been breached.

This is one of the most important configuration tasks as it allows incident response teams to determine whether data has been exfiltrated from a compromised accounts mailbox.

Configure technical control

Microsoft provides a script that enables non-owner mailbox access auditing on every mailbox in your organisations tenancy. The script can be downloaded from here, [https://github.com/OfficeDev/O365-InvestigationTooling/blob/master/EnableMailboxAuditing.ps1](https://github.com/OfficeDev/O365-InvestigationTooling/blob/master/EnableMailboxAuditing.ps1)

1. Open Admin PowerShell session
2. Run the script
3. Enter Exchange GA credentials
4. Verify that returned users all have audit enabled

Validate technical control

To validate that all users have mailbox auditing enabled run the following PowerShell

```
Get-Mailbox -ResultSize Unlimited | Select Name, AuditEnabled, AuditLogAgeLimit | Out-GridView
```

3.5.5 Enable Client Rules Forwarding Block

Client created rules, that Auto-Forward email from user’s mailboxes to an external email address, are becoming an increasingly common and fruitful data exfiltration method being used by bad actors today and something Microsoft incident response see quite a lot of in the Office 365 Service. This control is also relevant when preventing users from configuring auto-forward rules to an external email address.

There are several ways today that a bad actor can use external mail forwarding to exfiltrate data.

1. Client created external mail forwarding Rules, such as the Outlook desktop client.
2. Admins can set up external mail forwarding for a user via setting ForwardingSmtpAddress on a user object.
3. Admins can create external transport rules to forward messages.
4. Client created ForwardingSmtpAddress via Outlook Web Access interface

Using a properly configured Transport Rule we can control the impact of data exfiltration via Client created external mail forwarding rules. This approach has a couple of advantages:

1. Clients will receive a custom Non Delivery Receipt (NDR) message, useful for highlighting to end users external forwarding rules they may have not known existed (accidental exfiltration), or external forwarding rules created by a bad actor on a compromised mailbox.
2. Allows a whitelist of users or groups to be configured to allow business approved exceptions to the policy.
3. Provides some mitigation, for when an Admin account has been used to create a Remote Domain with auto-forwarding enabled to specific namespace to exfiltrate data.
4. Provides some mitigation, for when an Admin account has been used to alter the Default Remote Domain settings.
Configure technical control

This control creates a transport rule that will stop external messages leaving your Tenant, that are of the type AutoForward, mitigating the use of Client created external mail forwarding rules and malicious Remote Domain entries as a data exfiltration vector.

1. If The Sender is located 'Inside the organization'
2. If The Recipient is located 'Outside the organization'
3. If The message type is 'Auto-Forward'
4. Reject the message with the explanation 'External Mail Forwarding via Client Rules is not permitted'

To implement the technical control, perform the following steps:

1. Logon to Secure Score https://securescore.office.com
2. Locate the Enable Client Rules Forwarding Block control
3. Click update to display the detailed information page
4. Click Apply to create the Transport Rule

This creates a Transport rule in Exchange Online described above.

Validate technical Control

Validate the technical control by performing the following steps:

1. Logon onto Exchange Admin Portal
2. Select Mail Flow, the Rules page should be displayed
3. Verify that a transport rule has been created named “Client Rules to External Block – Secure Score”
4.

3.5.6 Configure Transport rule for ransomware

For organisations that have not purchased Office 365 ATP as part of the Security and Compliance Package this control is recommended. If the Security and Compliance Package has been purchased, then there is no need to implement this control.

Transport rules can also be used to block email with attachments that are commonly used by Ransomware.

Common executable file types are: ade, adp, ani, bas, bat, chm, cmd, com, cpl, crt, hlp, ht, hta, inf, ins, isp, job, js, jse, lnk, mda, mdb, mde, mdz, msc, msi, msp, mst, pcd, reg, scr, sct, shs, url, vb, vbe, vbs, wsc, wsf, wsh, exe, pif

Office file types that contain macros are: doc, xls, docm, xlsx, pptm
Before implementing the following rule, it is important that you review the list of file types to ensure that there is not a valid business reason that file types that are in the list are not blocked.

If an individual or business unit has a valid business reason to receive files that are on the list of common Ransomware types, then create more granular rules to allow these users to receive these files but prevent the entire organisation from being at risk.

Keep in mind that you can create multiple rules. For example, you can create a block rule for executables and a separate rule to track and warn users about Office documents that support macros.

Configure Technical Control

To implement this technical control, perform the following steps:

1. Go to the Exchange admin portal.
2. Click Mail Flow | Rules.
3. Create a new rule by clicking the "+", Create new rule...
   - Enter the rule Name (e.g. "Anti-Ransomware rule") and click more options.
4. Modify Apply this rule if... Any Attachment... file extension includes these words...

5. Enter the file extensions you want to track by clicking the "+" icon and then click Ok. You should consider:

6. Executables (ade, adp, ani, bas, bat, chm, cmd, com, cpl, crt, hlp, ht, hta, inf, ins, isp, job, js, jse, lnk, mda, mdb, mde, mdz, msc, msi, msp, mst, pcd, reg, scr, sct, shs, url, vb, vbe, vbs, wsc, wsf, wsh, exe, pif, etc.)

7. Office files that support macros (doc, xls, docm, xlsx, pptm, etc.)
8. Do the Following:

9. **Track emails**: Generate incident report and send it to... Your account... Custom Content: Select all of them.

10. **Warn the Users**: Add Action, Append the disclaimer (for example: “Do not open these types of documents from people you do not know since they might contain macros that will allow malicious code to be executed in your machine. Thanks.”) and select a fall-back action (for example, Wrap)
11. **Block Messages**: Add Action, Block the message... Use this option only if you are certain your organization does not use these types of files.

![Block Messages Image]

Validate Technical Control

To validate this control from an external domain, send an email with an attachment that matches one of the types in the Anti-Ransomware transport rules, e.g. .zip or .xlsm.

### 3.5.7 Configure anti-malware protection in your tenant

For organisations that have not purchased Office 365 ATP as part of the Security and Compliance Package this control is recommended. If the Security and Compliance Package has been purchased, then there is no need to implement this control.

Office 365 anti-malware protection is provided by Exchange Online Protection and is on by default.

It is recommended that you edit the default policy and set Common Attachment Filter to on.

**Configure technical control**

1. Open Exchange Admin Center
2. Select protection from the list
3. Select Default policy and click edit
4. Click settings and change the Common Attachment Types filter to On
5. Add additional
6. Click Save to make the change to the policy

### 3.5.8 Do not allow anonymous calendar sharing

Anonymous calendar sharing should be disabled in your tenant. This feature allows your users to share the full details of their calendars with external, unauthenticated users. Attackers will very commonly spend time learning about your organization (performing reconnaissance) before launching an attack. Publicly available calendars can help attackers understand organizational relationships and determine when specific users may be more vulnerable to an attack, such as when they are traveling.
Configure technical control

For details on how to configure this technical control please refer to the following article, https://support.office.com/en-us/article/Share-calendars-with-external-users-FB00DD4E-2D5F-4E8D-8FF4-94B2CF002BDD

2. Under Settings select Services and add-ins
3. Select Calendar from this list displayed
4. set the “Allow anonymous users to access calendars with an email invitation” to Off

The recommended setting is:

- set the “Allow anonymous users to access calendars with an email invitation” to Off

Validate technical control

To validate calendar sharing configuration for your Office 365 tenant.

2. Under Settings select Services and add-ins
3. Select Calendar from this list displayed
4. Verify that “Allow anonymous users to access calendars with an email invitation” is set to Off

3.5.9 Secure external mail flow

The following sections refer to the recommended configurations for securing email flow using Sender Policy Framework, DomainKeys Identified Mail, and Domain-based Message Authentication, Reporting, and Conformance.

The NCSC provides guidance for configuring e-mail including anti-spoofing here: https://www.ncsc.gov.uk/guidance/email-security-and-anti-spoofing

The NCSC also provides its Mail Check platform for assessing email security compliance here: https://www.ncsc.gov.uk/mailcheck

3.5.9.1 Configure Sender Policy Framework to prevent spoofing for Office 365 custom domain

When using a custom domain for email, e.g. contoso.com, Office 365 requires that you add a Sender Policy Framework (SPF) TXT record to your DNS record to help prevent spoofing.
SPF identifies which mail servers can send mail on your behalf. SPF when used in conjunction with DKIM, DMARC, and other technologies supported by Office 365 help prevent spoofing and phishing.

SPF is added as a TXT record that is used by DNS to identify which mail servers can send mail on behalf of your custom domain. Recipient mail systems refer to the SPF TXT record to determine whether a message from your custom domain comes from an authorized messaging server.

If you’ve already set up mail for Office 365, then you have already included Microsoft’s messaging servers in DNS as an SPF TXT record.

Validate Technical control

Logon to your organisations DNS service and verify that a TXT record exists with the following defined:

```
v=spf1 include:spf.protection.outlook.com -all
```

### 3.5.9.2 Configure DKIM for Office 365 custom domain

In addition to SPF it is also recommended that organisations use DomainKeys Identified Mail (DKIM) with Office 365 to ensure that destination email systems trust messages sent from your custom domain.

Configure technical control

To enable DKIM on your Office 365 tenant you need to publish two CNAME records for each domain name that is used to send and receive email and configure Exchange Online to use DKIM.

**Configure DNS CNAME records:**

The following format is used for the CNAME records

<table>
<thead>
<tr>
<th>CNAME records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
</tr>
<tr>
<td>Points to address or value</td>
</tr>
<tr>
<td>TTL:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CNAME records</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
</tr>
<tr>
<td>Points to address or value</td>
</tr>
<tr>
<td>TTL:</td>
</tr>
</tbody>
</table>
Table 8: CNAME records format

Where:

For Office 365 the selectors will always be selector1 and selector2
domainGUID is the same as the domainGUID I the customised MX record for your custom domain

```
contoso.com.  3600  IN  MX  5 contoso-com.mail.protection.outlook.com
```

InitialDomain is the domain that you used when you signed up for Office 365.

So, for contoso.com the two CNAME records would be as follows:

<table>
<thead>
<tr>
<th>Host name</th>
<th>Points to address or value</th>
<th>TTL</th>
</tr>
</thead>
<tbody>
<tr>
<td>selector1._domainkey</td>
<td>selector1-contoso-com._domainkey contoso.onmicrosoft.com</td>
<td>3600</td>
</tr>
<tr>
<td>Selector2._domainkey</td>
<td>Selector2-contoso-com._domainkey contoso.onmicrosoft.com</td>
<td>3600</td>
</tr>
</tbody>
</table>

Table 9: CNAME records example

**Enable DKIM in Exchange Online:**

**Office Admin UI**

To enable DKIM signing for your custom domain through the Office 365 admin centre

1. Sign in to Office 365 with your work or school account.
2. Select the app launcher icon in the upper-left and choose Admin.
3. In the lower-left navigation, expand Admin and choose Exchange.
4. Go to Protection > dkim.
5. Select the domain for which you want to enable DKIM and then, for Sign messages for this domain with DKIM signatures, choose Enable. Repeat this step for each custom domain.

**Using PowerShell**

To enable DKIM signing for your custom domain by using PowerShell

1. Connect to Exchange Online using remote PowerShell.
2. Run the following cmdlet:
3. New-DkimSigningConfig -DomainName <domain> -Enabled $true
Where *domain* is the name of the custom domain for which you want to enable DKIM signing.

For example, for the domain contoso.com:

```
New-DkimSigningConfig -DomainName contoso.com -Enabled $true
```

**Validate technical control**

To Confirm DKIM signing is configured properly for Office 365

Wait a few minutes before you follow these steps to confirm that you have properly configured DKIM. This allows time for the DKIM information about the domain to be spread throughout the network.

- Send a message from an account within your Office 365 DKIM-enabled domain to another email account such as outlook.com or Hotmail.com.
- Open the message and look at the header. Instructions for viewing the header for the message will vary depending on your messaging client. For instructions on viewing message headers in Outlook, see [View e-mail message headers](https://support.office.com/en-us/article/view-email-message-headers-380a95a8-bd68-4ff7-b00f-48f963b8d0f0).

The DKIM-signed message will contain the host name and domain you defined when you published the CNAME entries. The message will look something like this example:

**From:** Example User <example@contoso.com>

**DKIM-Signature:** v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed;

  - s=selector1; d=contoso.com; t=1429912795;
  - h=From:To:Message-ID:Subject:MIME-Version:Content-Type;
  - bh=<body hash>;
  - b=<signed field>;

- Look for the Authentication-Results header. While each receiving service uses a slightly different format to stamp the incoming mail, the result should include something like **DKIM=pass** or **DKIM=OK**.

Refer to the following article for detailed instructions on configuring DKIM for your organisation, [https://technet.microsoft.com/en-us/library/mt695945(v=exchg.150).aspx](https://technet.microsoft.com/en-us/library/mt695945(v=exchg.150).aspx)

**3.5.9.3 Configure DMARC to validate email in Office 365**

Domain-based Message Authentication, Reporting, and Conformance (DMARC) works with Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) to authenticate mail senders and ensure that destination email systems trust messages sent from your domain. Implementing DMARC with SPF and DKIM provides additional protection against spoofing...
and phishing email. DMARC helps receiving mail systems determine what to do with messages sent from your domain that fail SPF or DKIM checks.

Configure technical control

Inbound mail

No action is required to configure DMARC for inbound email as Office 365 is configured to do this by default.

Outbound mail

If you use Office 365 but you aren’t using a custom domain, that is, you use onmicrosoft.com, you don’t need to do anything else to configure or implement DMARC for your organization. SPF is already set up for you and Office 365 automatically generates a DKIM signature for your outgoing mail.

If you have a custom domain or you are using on-premises Exchange servers in addition to Office 365, you need to manually implement DMARC for your outbound mail. Implementing DMARC for your custom domain includes these steps:

1. Identify valid sources of mail for your custom domain
2. Set up SPF for your domain in Office 365, refer to the steps outlined in Configure Sender Policy Framework to prevent spoofing for Office 365 custom domain previously for details on how to configure SPF.
3. Set up DKIM for your custom domain in Office 365, refer to the steps outlined in Configure DKIM for Office 365 custom domain previously for details on how to configure DKIM
4. Create DMARC TXT record for your domain in Office 365, follow the steps outline below to perform this task.

Although there are other syntax options that are not mentioned here, these are the most commonly used options for Office 365. Form the DMARC TXT record for your domain in the format:

_dmarc.domain TTL IN TXT "v=DMARC1; pct=100; p=policy"

where:

- **domain** is the domain you want to protect. By default, the record protects mail from the domain and all subdomains. For example, if you specify _dmarc.contoso.com, then DMARC protects mail from the domain and all subdomains, such as housewares.contoso.com or plumbing.contoso.com.
- **TTL** should always be the equivalent of one hour. The unit used for TTL, either hours (1 hour), minutes (60 minutes), or seconds (3600 seconds), will vary depending on the registrar for your domain.
- **pct=100** indicates that this rule should be used for 100% of email.
• **policy** specifies what policy you want the receiving server to follow if DMARC fails. You can set the policy to none, quarantine, or reject.

For information about which options to use, become familiar with the concepts in Best practices for implementing DMARC in Office 365.

Examples:

Policy set to none

_{dmarc.contoso.com} 3600 IN  TXT  "v=DMARC1; p=none"

Policy set to quarantine

_{dmarc.contoso.com} 3600 IN  TXT  "v=DMARC1; p=quarantine"

Policy set to reject

_{dmarc.contoso.com} 3600 IN  TXT  "v=DMARC1; p=reject"

Once you have formed your record, you need to update the record at your domain registrar. For instructions on adding the DMARC TXT record to your DNS records for Office 365, see Create DNS records for Office 365 when you manage your DNS records.

### 3.5.10 SharePoint Online

The following controls a specific to SharePoint Online.

### 3.5.11 Configure expiration time for external sharing links

External sharing is enabled by default in SharePoint Online and is the preferred method to collaborate with both internal and external users.

An attacker can compromise a user account for a short period of time, send anonymous sharing links to an external account, then take their time accessing the data. They can also compromise external accounts and steal the anonymous sharing links sent to those external entities well after the data has been shared. It is therefore recommended that external sharing is configured correctly it is recommended that the “Allow users to invite and share with authenticated external users” policy is used.

While it might seem counterintuitive to allow external sharing, this approach provides more control over and provides audit and logging capabilities for file sharing compared to sending files in email. SharePoint Online and Outlook work together to provide secure collaboration on files.

• By default, Outlook shares a link to a file instead of sending the file in email.
• SharePoint Online and OneDrive for Business make it easy to share links to files with contributors who are both inside and outside your organization.

The settings described below are the recommended Sharing settings for this guidance:

• Allow users to invite and share with authenticated external users (default setting).
• Default link type — select Internal (people in the organization only). Users who wish to share using anonymous links must choose this option from the sharing menu.

Configure technical control

To configure the recommended sharing configuration for SharePoint Online follow these steps:

1. Logon to SharePoint admin centre
2. Select the Sharing page
3. Check the Allow users to invite and share with authenticated external users:
4. Under Default Link Type change the selection to **Internal – only people in your organization.**

Validate technical control

3.5.12 Skype for Business Online

The following controls are specific to Skype for Business Online.

3.5.13 Skype For Business Federation

Skype for Business Online is automatically federated will all other tenancies. If an organisation feels that this model is not appropriate for its risk appetite, then it is possible to configure an allowed or denied list based on the organisation requirements.

3.5.14 Skype For Business User Policies

Allowing only Items that can be archived for compliance. It may be beneficial for compliance to turn off non-archived features.

In order to prevent both egress of files form an organisation as well as the ingress of files form external organisations it is recommended that the use of File Transfer using instant messaging is blocked.
Configure technical control

All of the controls for this area is controlled through Conferencing policies even if the call/session is a peer to peer session.

Whilst the general process is discussed in section Error! Reference source not found., for the File Sharing and other elements listed above use the following switches with either the “New-CsConferencingPolicy” or “set-csconferencingpolicy” cmdlet:

-EnableFileTransfer
-EnableP2PFileTransfer

Validate technical control

3.5.15 Data Protection

The following controls have been groups as controls that protect data that is stored and processed on an organisations Office 365 tenant.

3.5.16 Configure data loss prevention (DLP)

If your organisation has a requirement to prevent certain data types from leaving your organisation, then consider using Office 365 Data Loss Prevention. The guidance is that DLP should be restricted to those data types that have easily recognisable patterns, National Insurance Number, Passport Number or bank account. For more complex requirements we recommend the use of Azure Information Protection and human selectable labels to control sharing of information.

The use of Data Loss Prevention in Office 365 is not considered as a mandatory control but as a capability that can increase the overall security posture of an organisation.

If your organisation has a requirement for Data Loss Prevention, then Office 365 Data Loss Prevention (DLP) allows you to identify sensitive data and create policies that help prevent your users from accidentally or intentionally sharing the data. DLP works across Office 365 including Exchange Online, SharePoint Online, and OneDrive so that your users can stay compliant without interrupting their workflow.

DLP policies are created and managed on the Data loss prevention page in the Office 365 Security & Compliance Center.

For more details on the capabilities of Office 365 data loss prevention policies.

Microsoft has produced guidance for Secure SharePoint Online sites and files which includes the use of DLP as a core component, specifically Protect SharePoint Online files with Office 365 labels and DLP.
3.5.17 Enable Azure AD and Office 365 Cloud App Security

Office 365 Cloud App Security (CAS) is a subset of full Microsoft Cloud App Security product that provides enhanced visibility and control for Office 365. This includes threat detection based on user activity logs, discovery of Shadow IT for apps that have similar functionality to Office 365 offerings and control app permissions to Office 365.

For more information on the differences between Office 365 Cloud App Security, Azure AD Cloud App Security and Microsoft Cloud App Security refer to:


It is recommended that both Azure AD and Office 365 Cloud App Security is enabled as they are available at no extra cost to M365 E3 customers.

If an organisation determines that its security model requires the use of a CAS then consider upgrading to the Security and Compliance Package as Microsoft Cloud App Security is included.

Configure technical control

To enable the Office 365 Cloud App Security, follow the guidance in the article below:


To enable Azure AD Cloud App Security, follow the guidance in the article below:

Set up Cloud App Discovery in Azure AD for more details.

Validate technical control

To access your Cloud App Security portal open Office Admin Portal
Under Admin Centres select Cloud App Security
Security and Compliance Package enhancements

UK Public Sector customers can take advantage of the Microsoft 365 Security and Compliance Package (SCP). SCP is a special package of licences that are available for eligible public-sector customers as part of the Digital Transformation Arrangement (DTA) MoU with Crown Commercial Services. This has been created to meet the increasing needs for increased levels of protection from cybersecurity threats as well as support the demands for greater compliance, particularly with the introduction of GDPR.

Figure 4: Security and Compliance Package components

The SCP provides an advanced set of capability that builds on the base line functionality found in Microsoft 365 E3, see Figure 4. This includes Advanced Threat Protection tools to reduce the attacks from email attachments, advanced eDiscovery tools, which uses machine learning, predictive coding, and text analytics to reduce the costs and challenges of sorting through large quantities of data.

The SCP package also provides Privileged Identity Management, Policy setting and enforcement for Classification and Labelling capabilities with advanced Information Protection.

It also includes Cloud App Security which is a comprehensive service providing deep visibility, granular controls and enhanced threat protection for your cloud apps. It can currently identify over 14,000 cloud applications in your network, from all devices, and
provides ongoing risk assessment and analytics. No agents required: information is collected from your firewalls and proxies to give you complete visibility and context for cloud usage and shadow IT.

Finally, Windows Defender Advanced Threat Protection helps protect against many different types of cyberattacks and emerging threats with tools to detect, investigate and remediate. The telemetry gathered from Windows Defender Advanced Threat Protection can be used as part of Azure AD Conditional Access decision process to gate access to Office 365 services based on the threat status of devices.

The following sections describe the enhance configuration controls that are recommended for those organisations that have purchased the Microsoft Security and Compliance Package.

Microsoft recommends the controls described in this section as they raise the overall security posture for organisations however, they are not mandatory.

As previously stated the controls in Section 3 Core Configuration Controls described previously in this document should be considered the minimum bar that organisations should meet for standard users. The SCP package is recommended for Privileged Accounts or any accounts that have been identified as being high value by your organisation, e.g. social media accounts or senior leadership team members.

4.1 Enhanced Identity Protection controls

The following controls are used to enhance the security of identities when accessing Office 365.

- Azure AD Identity Protection is applicable to both privileged and standard users when enabled.
- Azure AD Privileged Identity Management specifically targets privileged identities used to perform administrative tasks.

4.1.1 Azure AD Identity Protection

To combat against stolen credentials, Microsoft has released a solution called Azure AD Identity Protection that will assist with protecting user identities from being utilized in an unsecure manner. Based on the risk level, Azure AD Identity Protection will take appropriate action (based on a risk profile) such as requiring a user the change their password or by forcing multi-factor authentication.

As a result of the focus on identities it is important that organisations:

- Protect all identities regardless of their privilege level
- Proactively prevent compromised identities from being abused
Discovering compromised identities is no easy task. Azure Active Directory uses, amongst other inputs, adaptive machine learning algorithms and heuristics to detect anomalies and suspicious incidents that indicate potentially compromised identities. Using this data, Identity Protection generates reports and alerts that enable you to evaluate the detected issues and take appropriate mitigation or remediation actions.

Based on the gathered data in Azure AD Identity Protection generates the following types of risk events are described in Table 10 below:

<table>
<thead>
<tr>
<th>Risk event type</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leaked credentials</td>
<td>Typically, when a breach occurs, credentials are sold or accessed on the dark web and used in attempt to access services.</td>
</tr>
<tr>
<td>Impossible travel to atypical locations</td>
<td>Multiple sign-ins from different locations across the globe. When all internet access is routed via a VPN and Internet Gateway Service (Outbound Proxy) then being able to spot logon attempts from anywhere other than the known and expected location will give a good indication that an attempted</td>
</tr>
<tr>
<td>Sign-ins from infected devices</td>
<td>Device infected with malware that communicate with a bot server.</td>
</tr>
<tr>
<td>Sign-ins from anonymous IP addresses</td>
<td>Typically done by proxying, for example using Tor browser.</td>
</tr>
<tr>
<td>Sign-ins from IP addresses with suspicious activity</td>
<td>IPs which a high number of failed sign-in attempts occurred.</td>
</tr>
<tr>
<td>Sign-ins from unfamiliar locations</td>
<td>Uses past sign-in locations to determine unfamiliar location.</td>
</tr>
</tbody>
</table>

Azure Active Directory Identity Protection is more than a monitoring and reporting tool. To protect your organization’s identities, you can configure risk-based policies that automatically respond to detected issues when a specified risk level has been reached. These policies, in addition to other inputs, can be used as parameters in conditional access controls provided by Azure AD Conditional Access policies. These policies can either automatically block or initiate adaptive remediation actions including password resets and multi-factor authentication enforcement.

If Azure AD Identity Protections is available it is recommended that it is used as part of any Azure AD Conditional Access policies for Privileged Identities as well as standard user identities.

4.1.2 Azure AD Privileged Identity Management

Giving standing access to privileged roles in Azure AD and Office 365 increases the opportunity for malicious actors to gain access to systems in a privileged context.

To further enhance the security of privileged accounts in Azure AD and Office 365 it is recommended that organisations consider implementing Azure AD Privileged Identity Management (PIM). It allows enhanced capabilities in Azure AD, Office 365 and Intune when privileged tasks are required to control, manage and monitor access to those resources.

A key feature of Azure AD PIM is the concept of Just-in-Time administrator access. Typically, would assign a user to an admin role through the Azure portal, other Microsoft Online Services portals, or the Azure AD cmdlets in Windows PowerShell. As a result, that user becomes a permanent admin, always active in the assigned role. The goal is to eliminate standing access to privileged roles which is addressed by implementing Azure AD PIM.

Azure AD PIM introduces the concept of an eligible admin. Eligible admins should be users that need privileged access now and then, but not all-day, every day. The role is inactive until the user needs access, then they complete an activation process and become an active admin for a predetermined amount of time. It is recommended that organisations use this approach for reducing or eliminating “standing admin access” to privileged roles.

Detailed configuration of Azure AD PIM is organisation specific. It is therefore recommended that organisations refer to Privileged Identity Management for details of how to enable and configure Azure AD Privileged Identity Management.

4.1.3 Microsoft Office 365 Privileged Access Management

Privileged Access Management is currently in Public Preview for Microsoft Office 365. Azure AD Privileged Identity Management (PIM) and privileged access management (PAM) in Office 365 together provide a robust set of controls for protecting privileged access to your corporate data. With Azure AD PIM, customers can secure admin roles to ensure protection across Office 365 and Azure clouds. PAM in Microsoft Office 365 can provide another granular layer of protection by controlling access to tasks within Microsoft Office 365.

New privileged access management capabilities in Microsoft Office 365 provides an approval workflow that’s scoped to your high-risk tasks within Microsoft Office 365. For example, standing admin privileges enable admins to execute tasks that can provide unfettered access...
to organizational data, such as a journal rule, which can copy emails to a shadow mailbox and exfiltrate sensitive data undetected.

Privileged access management in Microsoft Office 365 was designed based on the principle of Zero Standing Access, which is how we run our own data centres at Microsoft through Lockbox and Customer Lockbox. With privileged access management in Microsoft Office 365, access requests must be approved by an authorized set of approvers. Access is then time-bound for a limited duration, often referred to as “Just-In-Time” (JIT) access. This level of rigor is how we manage administrative access privileges internally for Microsoft Office 365 today.

Requests for access can be automatically or manually approved. Either way, all the activity is logged and auditable, so that both privileged access requests and approvals can be reviewed and seamlessly provided for internal reviews and auditor requests.

Refer to Announcing preview of privileged access management in Office 365 for further details.
4.2 Enhanced Service Configuration controls

The following section outlines additional Office 365 service capabilities that are available as part of the Security and Compliance Package.

4.2.1 Enable customer lockbox feature

Customer lockbox allows you to control how a Microsoft support engineer accesses your data. In some cases, the support engineer will require access to your Office 365 content to troubleshoot and fix the issue. Customer lockbox requests allows you to control whether to give the support engineer access to your data and audit that approval.

Configure technical control

Customer lockbox requires little configuration and is simply enabled. Follow the guidance in the article below to enable and manage lockbox requests.

https://support.office.com/en-ie/article/office-365-customer-lockbox-requests-36f9cdd1-e64c-421b-a7e4-4a54d16440a2

Validate technical control

No validation.

4.3 Enhanced Data Protection controls

The following section outlines additional Office 365 data protection capabilities that are available as part of the Security and Compliance Package.

4.3.1 Configure Office 365 Advanced Threat Protection Safe Attachments feature

Office 365 Advanced Threat Protection Safe Attachments is one of the additional services included for Organisations that have purchased the Security and Compliance Package.

An enhanced security control that is recommended in this guidance is to enable the Office 365 Advanced Threat Protection Safe Attachments feature. This will extend the malware protections in the service to include routing all messages and attachments that don’t have a known virus/malware signature to a special hypervisor environment where a behaviour analysis is performed using a variety of machine learning and analysis techniques to detect malicious intent.
The ATP Safe Attachments feature checks to see if email attachments are malicious, and then acts to protect your organization. The ATP Safe Attachments feature protects your organization according to ATP Safe Attachments policies that are set by your Office 365 global or security administrators.

In addition to Exchange Online attachments ATP protection has been extended to files in SharePoint Online, OneDrive for Business, and Microsoft Teams. To learn more, see Office 365 Advanced Threat Protection for SharePoint, OneDrive, and Microsoft Teams.

Configure technical control

By default, no Safe Attachment policy is configured when Office 365 Advanced Threat Protection is configured.

1. As a global administrator or security administrator, go to https://protection.office.com and sign in with your work account.
2. In the Office 365 Security & Compliance Center, in the left navigation pane, under Threat management, choose Policy > Safe Attachments.
3. If you see Turn on ATP for SharePoint, OneDrive, and Microsoft Teams, it is recommended that this option is selected. This will enable Office 365 Advanced Threat Protection for SharePoint, OneDrive, and Microsoft Teams for your Office 365 environment.
4. Choose New (the New button resembles a plus sign (+)) to start creating your policy.
5. Specify the name, description, and settings for the policy.
   **Example:** To set up a policy called "no delays" that delivers everyone's messages immediately and then reattaches attachments after they're scanned, you might specify the following settings:
   - In the Name box, type no delays.
   - In the Description box, type a description like, “Delivers messages immediately and reattaches attachments after scanning”.
   - In the response section, choose the Dynamic Delivery option. ([Learn more about dynamic delivery and previewing with ATP Safe Attachments](#))
   - In the Redirect attachment section, select the option to enable redirect and type the email address of your Office 365 global administrator, security administrator, or security analyst who will investigate malicious attachments.
   - In the Applied To section, choose The recipient domain is, and then select your domain. Choose Add, and then choose OK.
6. Choose Save.

Consider setting up multiple ATP Safe Attachments policies for your organization. These policies will be applied in the order they're listed on the ATP Safe Attachments page. After
a policy has been defined or edited, allow at least 30 minutes for the polices to take effect throughout Microsoft datacentres.

For more information refer to: Set up Office 365 ATP safe attachments policies

To configure Office 365 Advanced Threat Protection Safe Attachments feature, refer to the following article:


In addition to configuring Exchange Online safe attachment policy it is also recommended that you perform the steps outlined in Turn on Office 365 ATP for SharePoint, OneDrive, and Microsoft Teams. Specifically, disallowing downloads of infected files and configuring alerts for infected files.

**Validate technical control**

To validate whether Office 365 Advanced Threat Protection Safe Attachments feature has been configured perform the following steps:

1. Logon to Exchange Admin Portal
2. Select advanced threats from the options on the left of the web page
3. Select the safe attachments page
4. Verify that the Turn on ATP for SharePoint, OneDrive and Microsoft Teams checkbox is checked
5. Verify that there is a Safe Attachments Policy defined and enabled in the table

In order to test whether Office 365 Advanced Threat Protection Safe Attachments is working refer to the following article, https://docs.microsoft.com/en-gb/office365/enterprise/advanced-threat-protection-for-your-office-365-dev-test-environment

**4.3.2 Configure Office 365 Advanced Threat Protection Safe Links feature**

It is recommended that organisations enable the Office 365 Advanced Threat Protection Safe Links feature. This will extend the phishing protection in the service to include redirecting all email hyperlinks through a forwarding service which will block malicious ones even after it has been delivered to the end user. This will protect your organisation from a link that was found to be malicious after the email was originally delivered therefore reducing the chance of a successful phishing attack.
ATP Safe Links can help protect your organization by providing time-of-click verification of web addresses (URLs) in email messages and Office documents. Protection is defined through ATP safe links policies that are set by your Office 365 security team.

Once your ATP Safe Links policies are in place, Office 365 global administrators, security administrators, and security readers can view reports for Advanced Threat Protection. The information in those reports can help your security team take further steps to protect your organization or research security incidents.

Configure technical control

When you have Advanced Threat Protection in Office 365 Enterprise, you will have an ATP Safe Links policy to define that applies to everyone in your organization. You can edit your policy in either the Security & Compliance Center or the Exchange admin centre. We recommend using the Security & Compliance Center to review or edit any of your ATP policies.

1. Go to https://protection.office.com and sign in with your work or school account.
2. In the left navigation, under Threat management, choose Policy > Safe Links.
3. In the Policies that apply to the entire organization section, select Default, and then choose Edit (the Edit button resembles a pencil).
4. In the Block the following URLs section, specify one or more URLs that you want to prevent people in your organization from visiting. (See Set up a custom blocked URLs list using ATP Safe Links.)
5. In the Settings that apply to content except email section, select (or clear) the options you want to use. (We recommend that you select all the options.)
6. Choose Save.

Add a policy for specific email recipients

After you have defined a policy for all users, consider adding policies for specific groups of email recipients. This enables you to specify exceptions to your default policy. You can add policies using either the Security & Compliance Center (recommended) or the Exchange admin centre. We recommend using the Security & Compliance Center to review or edit any of your ATP policies.

1. Go to https://protection.office.com and sign in with your work or school account.
2. In the left navigation, under Threat management, choose Policy.
3. Choose Safe Links.
4. In the Policies that apply to specific recipient’s section, choose New (the New button resembles a plus sign (+)).

5. Specify the name, description, and settings for your policy.

Example: To set up a policy called "no direct click through" that does not allow people in a certain group in your organization to click through to a specific website without ATP Safe Links protection, you might specify the following recommended settings:

- In the Name box, type no direct click through.
- In the Description box, type a description like, “Prevents people in certain groups from clicking through to a website without ATP Safe Links verification”.
- In the Select the action section, choose On.
- Select Use Safe Attachments to scan downloadable content.
- If this option is available, select Apply Safe Links to messages sent within the organization.
- Select Do not allow user to click through to original URL.
- (This is optional) In the Do not rewrite the following URLs section, specify one or more URLs that are safe for your organization. (See Set up a custom "Do not rewrite" URLs list using ATP Safe Links)
- In the Applied To section, choose The recipient is a member of, and then choose the group(s) you want to include in your policy. Choose Add, and then choose OK.

6. Choose Save.

Validate technical control

In order to test whether Office 365 Advanced Threat Protection Safe Attachments is working refer to the following article, https://docs.microsoft.com/en-gb/office365/enterprise/advanced-threat-protection-for-your-office-365-dev-test-environment
4.3.3 Azure Information protection

Azure Information Protection (AIP) is a cloud-based solution that helps an organization to classify, label, and protect its documents and emails. This can be done automatically by administrators who define rules and conditions, manually by users, or a combination where users are given recommendations.

Azure Information Protection uses labels to apply classification to documents and emails. When you do this, the classification is identifiable always, regardless of where the data is stored or with whom it’s shared. The labels include visual markings such as a header, footer, or watermark. Metadata is added to files and email headers in clear text. The clear text ensures that other services, such as data loss prevention solutions, can identify the classification and take appropriate action.

The protection technology used in AIP is Azure Rights Management (often abbreviated to Azure RMS). This technology is integrated with other Microsoft cloud services and applications, such as Office 365 and Azure Active Directory. It can also be used with your own line-of-business applications and information protection solutions from software vendors, whether these applications and solutions are on-premises, or in the cloud.

This protection technology uses encryption, identity, and authorization policies. Similarly, to the labels that are applied, protection that is applied by using Rights Management stays with the documents and emails, independently of the location, inside or outside your organization, networks, file servers, and applications. This information protection solution keeps you in control of your data, even when it is shared with other people.

For example, you can configure a report document or sales forecast spreadsheet so that it can be accessed only by people in your organization, and control whether that document can be edited, or restricted to read-only, or prevent it from being printed. You can configure emails similarly and prevent them from being forwarded or prevent the use of the Reply All option.

Microsoft has produced guidance for Secure SharePoint Online sites and files which includes the use of DLP as a core component, specifically Protect SharePoint Online files with Azure Information Protection

SharePoint External Sharing Enhancement

When AIP is implemented it is acceptable to use Anonymous sharing as the external sharing configuration for SharePoint as AIP protection policy will provide the ability to prevent sharing of items with people not expressly granted permission.
Configure technical control

To configure the recommended sharing configuration for SharePoint Online follow these steps:

1. Logon to SharePoint admin centre
2. Select the Sharing page
3. Check the Allow sharing to authenticated external users and using anonymous access links: checkbox and enter 30 as the number of days

The number of days can be changes to a value that is appropriate for your organisation.

4. Under Default Link Type change the selection to **Internal – only people in your organization**.

Users who wish to share using anonymous links must choose this option from the sharing menu.
Appendix A – Incident Response Guidance

This Appendix covers the immediate steps an organisation should take if they are experiencing an attack.

For organisations that use the Federated authentication model where AD FS is used to authenticate users to Office 365 the following mitigations:

Immediate actions

- Log a Security Incident in the Admin Portal or with your Technical Account Manager
- Get all users registered for MFA, and disable legacy protocols (PoP3 etal) Push notifications app preferred.
- Enable device based certificate-based authentication in Azure Active Directory
  - Azure Active Directory certificate-based authentication on iOS
  - Azure Active Directory certificate-based authentication on Android
- Use latest ADFS with ADFS lockout threshold set very low.
- Set up AAD rules to require MFA when outside of corp network
- Set up ADFS rules to require MFA when outside of corp network (for assets AAD doesn’t cover)
- Update password policy:
  - Master passwords in AAD – password changes should happen there. That allows for banned password checking, etc.
  - If not – get some sort of dictionary checker in place for password setting
  - If not – establish a min length requirement but DO NOT HAVE ROTATION OR COMPLEXITY REQUIREMENTS – [http://aka.ms/passwordguidance](http://aka.ms/passwordguidance) explains why THESE RULES MAKE PASSWORDS EASIER TO GUESS.
Improve the organisations overall security posture

We suggest that you review and take appropriate action against the following material:

**Azure AD reporting API**

The following articles provide more details on how to use the Azure AD reporting API:


**Office 365 Security Best Practices**


**Enable mailbox audit logging**

Some audit logging is automatically enabled for you in Office 365; however, mailbox audit logging is not turned on by default. You turn on audit logging for all user mailboxes in Office 365 by using Exchange Online PowerShell. For information, see [Enable mailbox auditing in Office 365](https://support.office.com/en-us/article/Security-best-practices-for-Office-365-9295e396-e53d-49b9-ae9b-0b5828cdedc3).

After you’ve enabled audit logging you can [Search the audit log in the Office 365 Security & Compliance Center](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-reporting-api-audit-samples) to find out who has logged into your user mailboxes, sent messages, and other activities performed by the mailbox owner, a delegated user, or an administrator. For a list of mailbox activities that are included in the Office 365 audit log by default, see [Exchange mailbox activities](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-reporting-api-getting-started-azure-portal).

For information about other actions you can perform with the audit log, such as changing the amount of time to save entries in the audit log, see [Mailbox audit logging in Exchange 2016](https://support.office.com/en-us/article/Security-best-practices-for-Office-365-9295e396-e53d-49b9-ae9b-0b5828cdedc3).

**Finding Illicit Activity**

Refer to the following blog article to help understand how to find illicit activity in your Office 365 tenant:


**Finding Breached Accounts**

Breached accounts are the most common, and often most damaging breaches an Office 365 customer can experience. It is usually the first step an attacker will take in a larger effort to
steal your money or your data. The breached account security reviews are important because most breaches require some sort of privileged access (in the form of an owned account!).

- Review Sign-Ins After Multiple Failures
  - Where is it? Azure Management Portal --> Directory --> Reports --> Sign Ins After Multiple Failures
  - What's in the report? This report shows user accounts that have successfully signed in after multiple consecutive failed sign in attempts. While there are legitimate reasons for this behaviour, it also could indicate that an attacker successfully performed a brute force password cracking attack. The report itself includes the name of the user, the number of failed attempts before the successful sign in, and the time of the first successful sign in.
  - What do I look for? Any records in this report warrant at least a check-in with the user to ensure it was them. If it was not them, you should undertake a robust account breach remediation and investigation to determine where the account came from, and whether the breached account is associated with any other illicit activity.
  - How often should I review? You should review this report at least weekly.

- Review Sign-Ins from Unknown Sources
  - Where is it? Azure Management Portal --> Directory --> Reports --> Sign Ins From Unknown Sources
  - What's in the report? This report shows users who have successfully signed in while assigned a client IP address that has been recognized by Microsoft as an anonymous proxy IP address (such as for the TOR network). These proxies are often used by users that want to hide their computer's IP address, and may be used for illicit activity. The report shows the user, the number of successful sign ins, the IP address, and the time of the last successful logon.
  - What do I look for? Any records in this report warrant a check-in with the user to verify that the logon was legitimate.
  - How often should I review? You should review this report at least weekly.

- Review Sign-Ins from Multiple Geographies
  - Where is it? Azure Management Portal --> Directory --> Reports --> Sign Ins From Multiple Geographies
  - What’s in the report? This report includes successful sign ins from a user where two sign ins appeared to originate from different regions and the time between sign ins makes it impossible for the user to have travelled between those regions. Essentially, the user appears to be in two places at once. There are several potential causes, including sharing passwords (which is bad), using
VPN's or remote desktop, or using two devices and one device has an unusual IP address. The report includes the user, the first sign in location, the second sign in location, the time between sign ins, the estimated travel time, and the time of the 2nd sign in.

- What do I look for? This report can contain a very high false positive rate, especially if you have a geographically disperse workforce. When you are looking for illicit activity, watch for sign ins (either first or second) from geographies where it doesn't make sense for your workforce to be signing in from. For example, if you team operates primarily out of Europe, and you see logons from Russia, but no one on your team is traveling there, and you have no vendor relationships with anyone from there, it might be illicit. Another thing to look for is sign ins at times when your users would not normally be signing in (such as a 3am). You should contact the user to determine if there is a reasonable explanation.

- How often should I review? You should review this report at least weekly.

- Search Audit Log for User Administration Activities

- Where is it? [https://protection.office.com/#/unifiedauditlog](https://protection.office.com/#/unifiedauditlog) --> Activities Filter Drop Down --> User administration Activities

- What's in the report? This report will show you all of the user administration activities including new users, updated users, password requirement changes, and user deletions. The summary record shows you the date the event happened, the IP address (if available), the impacted user, and the activity performed. The detailed list will show you the actor who made the change, and all of the other details to help correlate the activity. Depending on how many users you have, this list could get very large, in which case you should export and analyse offline in a tool like Excel.

- What do I look for? Newly created users, or out of band password changes can be signs of an attacker either taking over an account or creating a new account from which to operate. Look for events from unusual IP addresses, or at unusual times of the day. Also look for odd usernames. If you find something unusual, you should first try to validate whether the activity is legitimate by contacting the user that made the change.

- How often should I review? You should review this report at least weekly.

- Review Malware Detections Report

- Where is it? [https://portal.office.com/AdminPortal/Home#/reportsSecurityAndCompliance](https://portal.office.com/AdminPortal/Home#/reportsSecurityAndCompliance) --> Malware Detections
- What's in the report? This report shows the number of malware detections sent or received in mail before the malware action was applied (usually a delete action). The report includes a date and the number of received and sent malware instances. Details about individual malware-filtered messages are available by selecting a point in the graph.

- What do I look for? You should think about this report as an indicator of the volume of malware that is being attempted to be transacted to and from your users. The report only shows instances where malware was correctly identified and handled, so there isn't any specific action to take. The sent volume is probably more important to flag because it means one of your users attempted to send it outbound. Think of this report as a way to understand how targeted your organization is by attackers with malware. High volumes of inbound malware means your users are more likely to get a piece of malware that slipped through protections, and you should have robust anti-virus and anti-malware protections installed on your client machines. Big spikes in volumes means that attackers may be targeting you particularly.

- How often should I review? You should review this report at least weekly.

- **Review Exchange Mailbox Activity**

  - Where is it? [https://protection.office.com/#/unifiedauditlog](https://protection.office.com/#/unifiedauditlog) --> Activities Filter Drop Down --> Exchange Mailbox Activities

  - What’s in the report? This report shows activity that could indicate a mailbox is being accessed illicitly. It includes created or received messages, moved or deleted messages, copied or purged messages, sent messages using send on behalf or send as, and all mailbox sign ins. The data include date, IP address, user, activity performed, the item affected, and any extended details. Note that you must [enable mailbox auditing](https://protection.office.com/#/unifiedauditlog) to have the data be recorded.

  - What do I look for? The volume of data included here could be very substantial, so focus your search on users that would be high impact if breached. Look for unusual patterns such as odd times of the day, or unusual IP addresses, and look for patterns such as high volumes of moves, purges, or deletes.

  - How often should I review? You should review this report at least every other week.
O365-InvestigationTooling

If the customer thinks they have been breached a series of tools/scripts are available here: https://github.com/OfficeDev/O365-InvestigationTooling

These scripts will help to facilitate the investigation and provide remediation’s to common attacker actions such as creating mail forwarding rules.