Microsoft

Technical Guide

Office 365 UK Blueprint - Secure Configuration Alignment

Prepared for UK Government

4/9/2021

Version 2 Final

Prepared by

Microsoft Consulting Services UK

Table of Contents

Table of Tables

Table of Figures

1 Blueprint summary

Microsoft provides a secure cloud service and has numerous independently verified attestation on its configuration state, from ISO the ISO 27000[1] 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 on already existing "best practice" that is published by the National Cyber Security Centre (NCSC) and Microsoft on their websites.

> **Important**
>
> 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 links to 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 blueprint is made up of the following major sections:

- Privileged Administration
    - Privileged Administration must be considered irrespective of which of the alignments, Good, Better, Best, is chosen for their Office 365 configuration.
    - Forms the recommended minimum configuration for Privileged users and the devices used to perform administrative tasks.
    - Requires Microsoft 365 E3 with Microsoft 365 E5 Security licenses to meet all the recommended configuration tasks for Privileged Administration controls. It also applies to organisations with Microsoft 365 E5 licenses available.
    - Removes all dependencies on on-premises components.
    - Built on Zero Trust Security principles.
- Good

[1] Office 365 ISO 27001 certificate can be found here https://aka.ms/o365iso27001cert

- Forms the minimum level of configuration that all organisations should meet.
- Available with Microsoft 365 E3 license.
- Can be implemented using simple configuration tasks.
- Use of Conditional Access with MFA and Restricted Session Controls in Exchange Online and SharePoint Online.
- Highest residual risk.

- Better

  - Forms the level of configuration that organisations should aspire to.
  - Available with Microsoft 365 Security and Compliance Package components or Microsoft 365 E3 with Microsoft 365 E5 Security.
  - Might require more complex configuration tasks.
  - Enforcement using Conditional Access to require a managed PC, Mac or mobile device is used to access Office 365 services using the Office client applications.
  - More flexible and granular control of user policies, session controls using Microsoft Cloud App Security.
  - Lower residual risk than Good pattern.

- Best

  - Forms the most complete protection available.
  - Available with Microsoft 365 E3 with Microsoft 365 E5 Security and Microsoft 365 E5 Compliance or Microsoft 365 E5.
  - More flexible and granular control of user policies, session controls using Microsoft Cloud App Security.
  - Enforcement using Conditional Access to require a managed PC, Mac or mobile device is used to access Office 365 services using the Office client applications.
  - Often requires more complex configuration tasks that also require integration between features.
  - Lowest risk approach compared to Good and Better patterns.

> ### Important
>
> For most central government departments and other high threat organisations we would expect that your desired security posture would start at "Better" as this will help you appropriately defend your Office 365 environment and perform investigations in case of incidents.

To support this effort this blueprint has been developed to support the recommended security configuration controls that organisations should consider when configuring and operating their Office 365 Tenant.

Each of the Good, Better, and Best sections contains guidance for the following areas:

- **Identity** – recommended controls describing how to secure the identities that are used to authenticate against Office 365 services.
- **Office 365 Service Configuration** – recommended controls for Office 365 environment that describe specific settings to secure the service thus raising the security posture of the organisation's Office 365 tenant.

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 Microsoft 365 Groups and Teams, as well as the components that more directly replace on-premises services such as Exchange and SharePoint.

Figure 1: Blueprint components

The features described in the Good, Better, and Best control groups described in Figure 1 above is designed to help organisations determine which of the patterns described in this document should be used.

For example, if an organisation has Microsoft 365 Security and Compliance Pack (SCP) or Microsoft 365 E3 with E5 Security licenses then the controls used in the Better deployment pattern will provide a lower residual risk and therefore should be used.

However, if an organisation requires Insider Risk Management then they would need the additional license of Microsoft E5 Compliance as well as Microsoft 365 E3 with Microsoft E5 Security or Microsoft 365 E5 licenses.

2 Blueprint Overview

The components that make up the Office 365 Blueprint design are illustrated in Figure 2 (below)

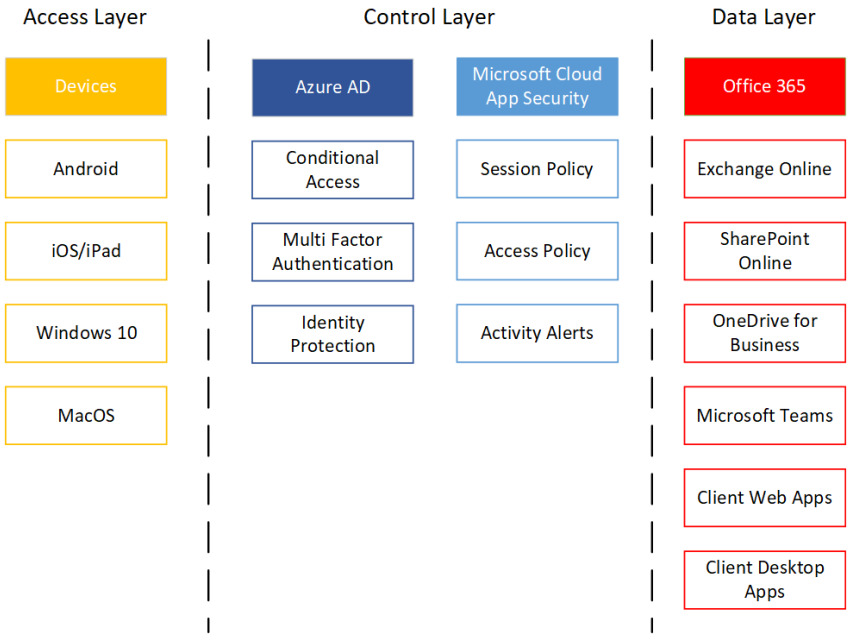

Figure 2: Office 365 Blueprint components

The blueprint covers privileged access and four primary configuration patterns that have been identified as meeting the requirement to allow managed devices to access corporate data in Microsoft Office 365 services, these are:

- Office 365 Apps on managed Android or iOS devices
- Office 365 Web Application access on managed PC or Mac
- Office 365 desktop client applications access on managed PC or Mac
- Office 365 desktop client using Windows Virtual Desktop from a PC or Mac

Requirements

The following list provides a set of prerequisite requirements that this Blueprint assumes that the following are in place:

1. The blueprint assumes that the End User Devices that are used to connect to the Office 365 services have been configured in accordance with the NCSC's Platform-specific guidance for mobile and PC devices
2. Only allow approved apps on managed mobile devices.
3. Only allow managed PC or Mac to access using web apps or desktop client applications.

4. Require MFA and Compliant or Hybrid Azure AD Joined devices to access Office 365 services.

> **Important**
>
> This document intentionally does not cover controls available to you when devices are personal unmanaged Bring Your Own Device (BYOD); it focuses on the controls that are available for Microsoft Intune as managed devices or Microsoft Intune and Configuration Manager co-managed devices.
>
> For BYOD refer to How to have secure remote working with a BYOD policy guidance.

3 Privileged Administration

Privileged access should be the top security priority at every organisation and Microsoft recently updated its Securing Privileged Access guidance to include not only on-premises environments but the more complex hybrid environments where enterprise IT organisations manage and support the workloads and the infrastructure they are hosted on, whether it's on-premises, on Azure, or a third-party cloud provider. For details of the configuration tasks to implement a Privileged Access Workstation refer to Privileged Access Implementation.

The National Cyber Security Centre (NCSC) has also published guidance on secure administration practices, in May 2019 Security Architecture anti-patterns was published with the first anti-pattern being "Browse-up" for administration,

> *"In computer systems where integrity is important (whether in digital services which handle personal data or payments, through to industrial control systems), if you don't have confidence in devices that have been used to administer or operate a system, you can't have confidence in the integrity of that system. There's a common misconception that a bastion host or jump box is a good way of injecting trust into the situation, to somehow get confidence in the actions an administrator is taking from a device you don't trust. Unfortunately, that's not possible."*

In September 2020, the NCSC published additional guidance on Secure Systems Administration which also specifically calls out that.

> *"The devices you use to access your system administration interfaces must be trustworthy.*
>
> *These dedicated management devices are often referred to as Privileged Access Workstations (PAWs). It is recommended to use these when administering cloud services.*
>
> *If you are allowing a device to connect to your administration interfaces, you need to be able to trust it. This lowers the chance of an attacker using the device to access your systems, instead of a legitimate system administration."*

It is also important that the accounts that are used to perform these administrative tasks are separate from the account they use for email, web browsing, and other productivity tasks, both Microsoft, Separate accounts for admins, and NCSC, Systems administration architectures recommend that administrators should.

"Have separate user accounts for administration and normal user activities. They should not use their administration accounts for normal business activities. This reduces the exposure of privileged accounts and reduces their risk of compromise."

The following table lists controls which are expected to be deployed for Privileged Administration, further details in sections following:

Control	Action
Isolate Microsoft 365 administrator accounts	Create dedicated accounts for administrative users They should be: • Mastered in Azure AD, i.e. cloud-only identities • Authenticated by using multifactor authentication. • Secured by Azure AD Conditional Access. • Accessed only by using Azure-managed workstations. These administrator accounts are restricted-use accounts. **No on-premises accounts should have administrative privileges in Microsoft 365.** For more information, see the overview of Microsoft 365 administrator roles and Roles for Microsoft 365 in Azure AD. Refer to Protecting Microsoft 365 from on-premises attacks and Securing Privileged Access for more details on how to
Manage Privileged Administration Workstations from Microsoft 365	Use Azure AD join and cloud-based mobile device management (MDM), e.g. Microsoft Intune, to eliminate dependencies on your on-premises device management infrastructure. These dependencies can compromise device and security controls. Refer to Privileged access devices and Privileged access implementation for more details on the benefits of Privileged Administration Workstations and how to implement them.
Ensure no on-premises account has elevated privileges to Microsoft 365.	Some accounts access on-premises applications that require NTLM, LDAP, or Kerberos authentication. • These accounts must be in the organisation's on-premises identity infrastructure. • Ensure that these accounts, including service accounts, aren't included in privileged cloud roles or groups. • Ensure that changes to these accounts can't affect the integrity of your cloud environment. **Privileged on-premises software must not be capable of affecting Microsoft 365 privileged accounts or roles.** Refer to Protecting Microsoft 365 from on-premises attacks for details on why on-premises accounts should not be assigned privileged roles in Microsoft 365

Use Azure AD as the Identity Provider for authentication	To eliminate dependencies on your on-premises credentials. Refer to Protecting Microsoft 365 from on-premises attacks for details on why Azure AD should be used as the Identity Provider for Privileged Accounts
Always use strong authentication controls through multi-factor authentication (MFA) and passwordless methods.	Such as Windows Hello, FIDO, Microsoft Authenticator, or Azure AD multifactor authentication. Refer to Privileged access accounts and Enable and require MFA / Passwordless for Azure AD privileged users for details on why Strong Authentication is required.
Use Emergency Access accounts	Ensure you have a mechanism for obtaining administrative access in case of an emergency. While rare, sometimes extreme circumstances arise where all normal means of administrative access are unavailable. These accounts should not be subject to any Identity Protection, MFA or Conditional Access policies and should be permanently assigned to the Global Administrator role in Azure AD Privileged Identity Management Refer to Section 3.2 Emergency access or 'Break Glass' accounts for why they are required as well as how to configure them.
Implement a Zero Trust Security approach for privileged users	Azure AD Conditional Access provides control based on a privileged user identity, network location, and risk signals to make decisions to allow or deny access, and any additional enforcement measures to be applied. Conditional Access will be used as the mechanism for implementing a Zero Trust Security approach. **Azure AD Conditional Access is the recommended method of implementing MFA for privileged user accounts.**
Control Access to Managed/Compliant Devices	Azure AD Conditional Access at time of logon can be used to decide on the application access that the user will have based on the device being used, and if necessary, require additional controls to be applied. Refer to Section 3.1.2 Azure AD Identity Protection for further detail on
Prevent use of Legacy Authentication Protocols	Legacy Authentication Protocols only support username and password as authentication method. This provides attackers with the opportunity to perform password spray attacks or similar. Legacy Authentication Protocols also prevent the use of Azure AD MFA.

	Refer to Block legacy authentication protocols for privileged user accounts
Do not expire passwords	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
Disable accounts not used in last 30 days	Accounts, especially those that perform privileged roles, should not be left active. Refer to Section 4.1.5.2 Disable accounts not used in the last 30 days for more details.
Use dedicated accounts to perform Administrative Tasks	Using the same account to perform privileged tasks as that used to browse the internet or are email enabled. Separating accounts reduces the likelihood of a successful phishing or other attack type leading to privileged identity being compromised
Configure Microsoft 365 Global Administrator role membership	Keeping the number of Global Administrators to the minimum level is an important part of a least privilege administration model. Use Global Reader role to allow administrators to review Office 365 policy and configuration settings without having to elevate into Global Administrator role Refer to Minimize number of critical impact admins for more details and Roles for Microsoft 365 in Azure AD for more details on Azure AD Roles.
Use Non-Global Administrative roles	Implementing role-based access model to reduce the number of Global Administrators is an important part of a least privilege administration model, e.g. use Azure AD roles, SharePoint Administrator, Exchange Administrator and Teams Administrator roles. Refer to Roles for Microsoft 365 in Azure AD for more details on Azure AD Roles
Develop a more granular Role Based Access Control (RBAC) model for Office 365 Services	As part of a least privilege administration model use less privileged built-in roles in Azure AD or develop application specific roles that grant administrators only the privileges they need to perform their tasks.
Enforce MFA for all Global Admins	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 Enable and require MFA / Passwordless for Azure AD privileged users. Refer to Deploying passwordless for further details on passwordless.
Reduce standing access to privileged roles	Implementing Azure AD Privileged Identity Management to remove standing access to privileged roles in Azure AD and Office 365. Refer to Section 3.1.1 Azure AD Privileged Identity Management for further details.

Table 1: Privileged Administration controls

Security of privileged access is critically important because it is foundational to all other security assurances, an attacker in control of your privileged accounts can undermine all other security assurances. From a risk perspective, loss of privileged access is a high impact event with a high likelihood of happening that is growing at an alarming rate across industries.

Securing privileged access effectively seals off unauthorised pathways completely and leaves a select few authorised access pathways that are protected and closely monitored.

Any compromise of these users has a high likelihood of significant negative impact to the organisation. Privileged users have access to business-critical assets in an organisation, nearly always causing major impact when attackers compromise their accounts.

Ensure all critical impact admins have a separate account for administrative tasks (vs the account they use for email, web browsing, and other productivity tasks). For these administrative accounts, block productivity tools like Office 365 email (remove license). If possible, block arbitrary web browsing (with proxy and/or application controls) while allowing exceptions for browsing to the Azure portal and other sites required for administrative tasks.

Phishing and web browser attacks represent the most common attack vectors to compromise accounts, including administrative accounts. Attackers frequently exploit weaknesses in privileged access security during human operated ransomware attacks and targeted data theft. Privileged access accounts and workstations are so attractive to attackers because these targets allow them to rapidly gain broad access to the business assets in the enterprise, often resulting in rapid and significant business impact.

These attack techniques were initially used in targeted data theft attacks that resulted in many high-profile breaches at familiar brands (and many unreported incidents). More recently these techniques have been adopted by ransomware attackers, fuelling an explosive growth of highly profitable human operated ransomware attacks that intentionally disrupt business operations across industry.

3.1 Start with Better configuration

Privileged administrators should start with the Better configuration pattern to provide an appropriate and proportionate level of protection to privileged identities and devices. This requires Microsoft 365 E3 and Microsoft 365 E5 Security licenses, at a minimum, which entitles organisations to Microsoft Defender for Endpoint to enhance the threat protection capabilities with detect and respond capabilities as well.

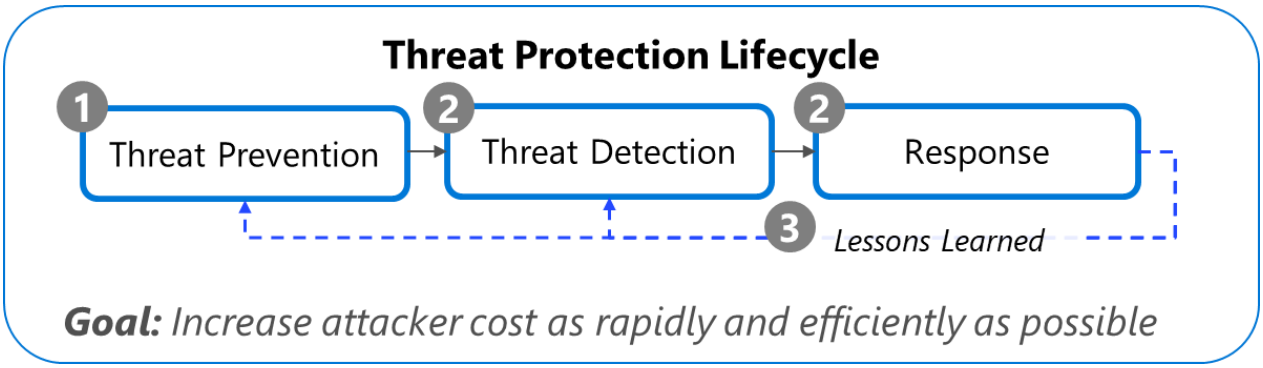

Figure 3: Threat Protection Lifecycle

1. Prevent as many threats as possible.
2. Rapidly Detect and Respond.
3. Continually apply learnings.

3.1.1 Azure AD Privileged Identity Management

An important consideration that needs to be considered with Privileged Identities is the need to minimise the likelihood a compromised account can operate with a privileged role. Avoid providing permanent "standing" access for Privileged Identities.

Permanent privileges increase business risk by increasing the time an attacker can use the account to do damage. Temporary privileges force attackers targeting an account to either work within the limited times the admin is already using the account or to initiate privilege elevation (which increases their chance of being detected and removed from the environment).

Azure AD Privileged Identity Management (PIM) helps you minimise account privileges by helping you:

- Identify and manage users assigned to administrative roles.
- Understand unused or excessive privilege roles you should remove.
- Establish rules to make sure privileged roles are protected by multi-factor authentication.

- Establish rules to make sure privileged roles are granted only long enough to accomplish the privileged task.

Enable Azure AD PIM, then view the users who are assigned administrative roles and remove unnecessary accounts in those roles. For remaining privileged users, move them from permanent to eligible. Finally, establish appropriate policies to make sure when they need to gain access to those privileged roles, they can do so securely, with the necessary change control.

Refer to No standing access / Just in Time privileges and Enable Azure AD Privileged Identity Management for more details.

3.1.2 Azure AD Identity Protection

Protecting the privileged accounts that are used to administer Office 365 is extremely important, these users have a normal pattern of behaviour that can be tracked, when they fall outside of this norm it could be risky to allow them to just sign in.

Identity Protection is the recommended tool that allows organisations to accomplish three key tasks:

- Automate the detection and remediation of identity-based risks.
- Investigate risks using data in the portal.
- Export risk detection data to third-party utilities for further analysis.

It is recommended that Azure AD Identity Protection policies are not enforced using the default policies, but instead Conditional Access policies are used.

A sign-in risk represents the probability that a given authentication request isn't authorised by the identity owner. For privileged users it is recommended that the Sign-in risk based Conditional Access policy described in the following link is configured to Block rather than perform MFA.

Sign-in risk-based Conditional Access - Azure Active Directory | Microsoft Docs

User risk based conditional access uses the data gathered as part of Microsoft's work with researchers, law enforcement, various security teams at Microsoft, and other trusted sources to find leaked username and password pairs. For privileged users it is recommended that the User risk based Conditional Access policy described in the following link is configured to Block rather than reset password.

User risk-based Conditional Access - Azure Active Directory | Microsoft Docs

3.2 Emergency access or 'Break Glass' accounts

It is important that you prevent being accidentally locked out of your Azure Active Directory (Azure AD) organisation because you can't sign in or activate another user's account as an administrator. You can mitigate the impact of accidental lack of administrative access by creating two or more emergency access accounts in your organisation.

Emergency access accounts are highly privileged, and they are not assigned to specific individuals. Emergency access accounts are limited to emergency or "break glass"' scenarios where normal administrative accounts can't be used. We recommend that you maintain a goal of restricting emergency account use to only the times when it is absolutely necessary.

We recommend looking at Emergency Access Accounts for more details and following the instructions at Managing emergency access administrative accounts in Azure AD and ensure that security operations monitor these accounts carefully.

3.3 Administer cloud services using the cloud

In light of the SolarWinds compromise in 2020 Microsoft published a blog article Protecting Microsoft 365 from on-premises compromise that highlighted the risk associated with managing Microsoft 365 using administrative accounts and devices that are mastered in an organisations on-premises infrastructure can propagate to the cloud services should a compromise of their on-premises infrastructure occur.

In hybrid deployments that connect on-premises infrastructure to Microsoft 365, organisations often delegate trust to on-premises components for critical authentication and directory object state management decisions. Unfortunately, if the on-premises environment is compromised, these trust relationships become an attacker's opportunities to compromise your Microsoft 365 environment.

The two primary threat vectors are ***federation trust relationships*** and ***account synchronisation***. Both vectors can grant an attacker administrative access to your cloud.

- **Federated trust relationships**, such as SAML authentication, are used to authenticate to Microsoft 365 through your on-premises identity infrastructure. If a SAML token-signing certificate is compromised, federation allows anyone who has that certificate to impersonate any user in your cloud. *We recommend you disable federation trust relationships for authentication to Microsoft 365 when possible.*
- **Account synchronisation** can be used to modify privileged users (including their credentials) or groups that have administrative privileges in Microsoft 365. *We recommend you ensure that synchronised objects hold no privileges beyond a user in*

Microsoft 365, either directly or through inclusion in trusted roles or groups. Ensure these objects have no direct or nested assignment in trusted cloud roles or groups.

To address the threat vectors outlined above, Microsoft recommends that organisations adhere to the principles illustrated in the following diagram:

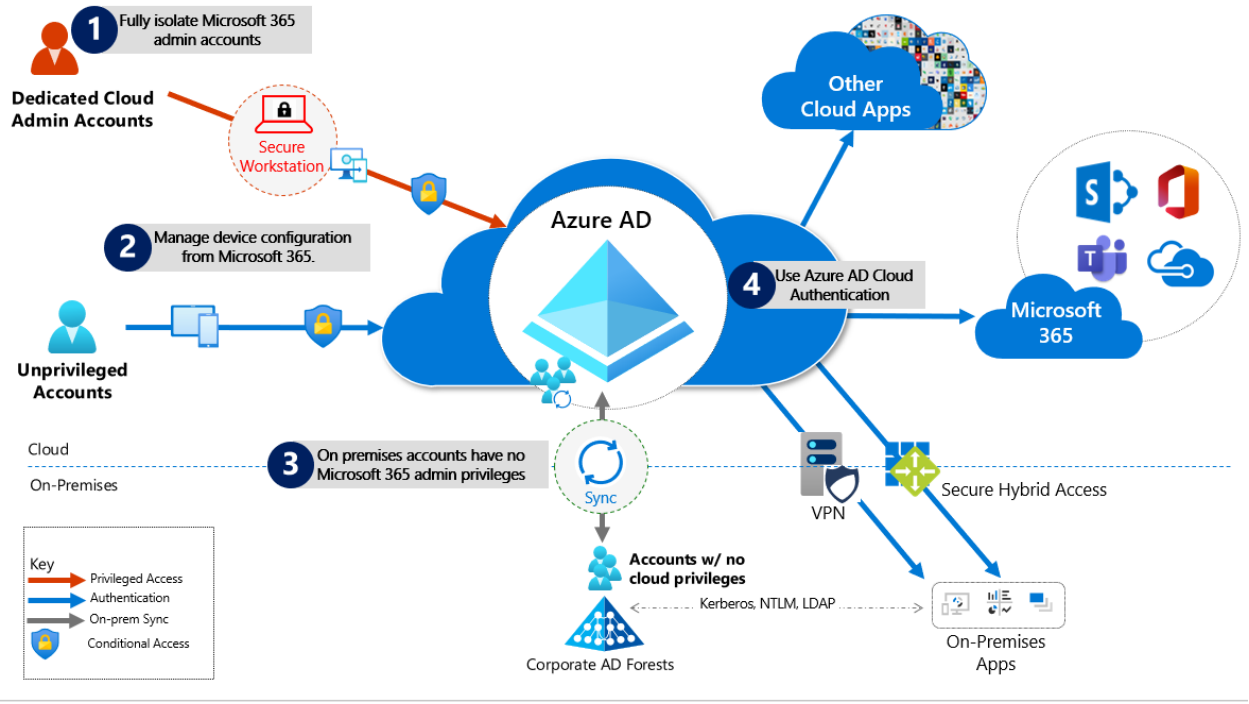

Figure 4: Cloud Authentication principles

1. Fully isolate your Microsoft 365 administrator accounts. They should be:
    - Mastered in Azure AD.
    - Authenticated by using multifactor authentication.
    - Secured by Azure AD Conditional Access.
    - Accessed only by using Azure-managed workstations.

    These administrator accounts are restricted-use accounts. **No on-premises accounts should have administrative privileges in Microsoft 365.**

    For more information, see the overview of Microsoft 365 administrator roles. Also see Roles for Microsoft 365 in Azure AD.

2. **Manage devices from Microsoft 365.** Use Azure AD join and cloud-based mobile device management (MDM) to eliminate dependencies on your on-premises device management infrastructure. These dependencies can compromise device and security controls.
3. **Ensure no on-premises account has elevated privileges to Microsoft 365.** Some accounts access on-premises applications that require NTLM, LDAP, or Kerberos authentication.
    - These accounts must be in the organisation's on-premises identity infrastructure.
    - Ensure that these accounts, including service accounts, aren't included in privileged cloud roles or groups.
    - Ensure that changes to these accounts can't affect the integrity of your cloud environment.

    Privileged on-premises software must not be capable of affecting Microsoft 365 privileged accounts or roles.
4. **Use Azure AD authentication method** to eliminate dependencies on your on-premises credentials. Always use strong authentication, such as Windows Hello, FIDO, Microsoft Authenticator, or Azure AD multifactor authentication.
5. **Use Emergency Access accounts** to ensure you have a mechanism for obtaining administrative access in case of an emergency. While rare, sometimes extreme circumstances arise where all normal means of administrative access are unavailable. Refer to Manage emergency access admin accounts - Azure AD | Microsoft Docs for more details.

4 Good

The following sections describe the security controls that are recommended for organisations which have purchased Microsoft 365 E3 licenses.

Where possible organisations should configure as many of the controls as possible to ensure the security of their Office 365 tenant. Where an organisation chooses not to implement a recommended control:

- You should determine if the residual risk is organisationally acceptable.
- You can meet organisational compliance obligations.
- Any compensating or mitigations should be noted in the organisations' risk register.

The following table lists controls which are expected to be deployed as a baseline level, further details in sections following:

Control	Action
Verify that Microsoft 365 Audit logging is enabled	Use the Microsoft 365 Compliance Center to verify that Audit logging is enabled Refer to Section 4.2.1 Microsoft 365 Audit logging
Enable mailbox auditing for all users	Verify Exchange Online Mailbox Auditing is turned on. Manually enable O365 E3 licenced mailboxes for searches in the Security & Compliance Center Refer to Section 4.2.5.1 Mailbox auditing
Use of Microsoft Secure Score service	Review and record current secure score, take note of improvement actions and evaluate the value to the organisation of implementing them. Schedule a monthly review of the Secure Score to monitor for changes to the score and new measures. Refer to Section 4.2.2 Secure Score reviews
Implement Cloud authentication model for Office 365.	Configure Azure Active Directory as the Primary authentication mechanism. Refer to Section 4.1.2.1 Cloud authentication
Configure Admin Consent for OAUTH Apps	Configure Azure Active Directory User consent for applications to Do not allow user consent

	Refer to Section 4.1.1 Configure Admin Consent for OAUTH Apps
Enable Multi Factor Authentication for all users	Enable Azure AD MFA for all users. Refer to Section 4.1.4.1 Enable Azure AD MFA for all users
Implement a holistic identity-centric Conditional Access approach	Plan and implement Conditional Access polices in Azure AD for authentication to Office 365 services. Refer to Section 4.1.4 Conditional Access
Control Access to Managed/Compliant Devices	Configure Azure AD Conditional Access policies to require the use of a managed device to access Office 365 services. Refer to Section 4.1.4.2 Control Access to Managed/Compliant Devices
Prevent use of Legacy Authentication Protocols	Configure Azure AD to block the use of Legacy Authentication methods. Refer to Section 4.1.4.3 Block Legacy Authentication method
Do not expire passwords	Set the Azure AD password expiration policy to not expire users' passwords. Refer to Section 4.1.5.1 Do not expire passwords
Disable accounts not used in last 30 days	Schedule reporting of inactive user accounts, and disable accounts. Refer to Section 4.1.5.2 Disable accounts not used in the last 30 day
Use dedicated accounts to perform Administrative Tasks	Create and use dedicated Azure AD User accounts for performing administrative roles. Refer to Section 3.3 Administer cloud services using the cloud
Configure Microsoft 365 Global Administrator role members	Remove all User accounts from the Azure AD Global Administrator Role, except for Break Glass accounts and a minimal number Administrator accounts required to support the platform at this level. Refer to Section 3.3 Administer cloud services using the cloud
Use non-global admin accounts to perform Office 365 administrative tasks	Delegate access to Office 365 administrators by utilising role other than the Global Administrator role Refer to Section 3.3 Administer cloud services using the cloud
Configure break glass accounts in Azure AD	Create and maintain two (2) Global Administrator user accounts in Azure AD which are excluded from Conditional Access and MFA policies. The details for these accounts are to be stored and only used for emergency access to the platform.

	Refer to Section 3.2 Emergency access or 'Break Glass' accounts
Enforce MFA for all Global Administrators	Configure Azure AD Conditional Access policies to require Azure MFA when an Identity with the Global Administrator role authenticates. Refer to Section 4.1.4 Conditional Access
Enable Client Rules Forwarding Block	Block automatic external email forwarding in Exchange Online Protection Refer to Section 4.2.5.2 Prevent email forwarding to personal email
Do not allow anonymous calendar sharing	Disable the option to "Allow anyone to access calendars with an email invitation" in the Microsoft 365 admin center. Refer to Section 4.2.5.3 Do not allow anonymous calendar sharing
Configure Transport rule for ransomware	**This control is applicable only for organisations that have not purchased Microsoft 365 E5 Security or Microsoft 365 E5 Full licenses** Configure Exchange Online transport rules to block email with attachments which are commonly used by ransomware. Refer to Section 4.2.5.4 Transport rule for ransomware
Configure anti-malware protection in your tenant	**This control is applicable only for organisation that have not purchased Microsoft 365 E5 Security or Microsoft 365 E5 Full licenses** Configure Exchange Online Protection to block common attachment types. Refer to Section 4.2.5.5 Anti-malware protection in your tenant
Secure external mail flow	Configure Exchange Online to use SPF, DKIM and DMARC will help to reduce spoofing of emails. Sign up for the NCSC Mail Check service. Refer to Section 4.2.5.6 Secure external mail flow
Disable Basic authentication in Exchange Online	Create and apply authentication policy to all users which block legacy auth protocols Refer to Section 4.2.5.10 Disable Basic authentication in Exchange Online
Microsoft Teams External Access (Federation)	**This control is only applicable to organisations who consider the risk of collaborating with other organisations using Microsoft Teams unacceptable or wish to block collaboration with certain domains.**

	Configure external access in Microsoft Teams Admin Center with an Allowed list model. Refer to Section 4.2.6.1 External Access (Federation)
Microsoft Teams Guest Access	**This control is applicable to organisations who consider the risk of collaborating with other organisations using Microsoft Teams unacceptable.** Allow Guest Access in the Microsoft Teams Admin Center Configure the Azure External collaboration settings: • Guest user access is restricted to properties and memberships of their own directory objects (most restrictive) • Only users assigned to specific admin roles can invite guest users • Allow invitations only to the specified domains (most restrictive) • List allowed domains Refer to Section 4.2.6.2 Guest Access
Allow SharePoint users to invite and share with new and Existing Guests	Configure external sharing in SharePoint Refer to Section 4.2.7.1 External Sharing
Site Classification	Enable SharePoint site classification. Refer to Section 4.2.7.6 Enable site classifications
Sharing - Default link type	Configure the "These links must expire within this many days" in the Sharing Policy in SharePoint Online Admin Center Refer to Section 4.2.7.1 External Sharing
Sharing - Guests must sign in using the same account to which sharing invitations are sent	Enable Guests must sign in using the same account to which sharing invitations are sent. Refer to Section 4.2.7.1 External Sharing
Sharing – Disable Allow guests to share items they don't own	Configure Disable Allow guests to share items they don't own Refer to Section 4.2.7.1 External Sharing
Block custom scripts in SharePoint	Disable customer scripts from being used in SharePoint. Refer to Section 4.2.7.3 Block custom script

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.** Define Sensitive Information Types and configure Data Loss Prevention Policies in the Microsoft 365 Compliance portal. Refer to Section 4.2.3 Configure data loss prevention (DLP)
Enable Office 365 Cloud App Security	**This control is applicable only for organisation that have not purchased Microsoft 365 E5 Security or Microsoft 365 E5 Full licenses** Connect Office 365 to the Microsoft Cloud App Security service. Use Office 365 Cloud App Security to investigate suspicious user activity Refer to Section 4.2.4 Office 365 Cloud App Security
Application Consent for Data Access	All requests for Third Party applications to access data on the users behalf should be approved by an Administrator Refer to Section 4.2.6.5 App permission policy

Table 2: Good controls

4.1 Identity

Organisations today typically need to use a mixture of on-premises and cloud hosted applications. Users require access to those applications both on-premises and in the cloud. Managing users both on-premises and in the cloud poses challenging scenarios.

Microsoft's Active Directory and Azure Active Directory services span on-premises and cloud-based capabilities. These solutions create a common user identity for authentication and authorisation to all resources, regardless of location. This is referred to as a Hybrid Identity.

Synchronising identities from on-premises Active Directory has benefits to security as well as usability. Fewer accounts reduce the likelihood of passwords being reused in multiple directories.

Security breaches of an Office 365 subscription, including information harvesting and phishing attacks, are typically done by compromising the credentials of an on-premises Active Directory account and using techniques to gain control of an account with an Administrative Role in Azure AD. Refer to Section 3 Privileged Administration above for recommendation on how to secure privileged accounts.

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.

For more information on protecting Office 365 from on-premises compromises refer to: [Protecting Microsoft 365 from on-premises attacks - Microsoft Tech Community]

4.1.1 Configure Admin Consent for OAUTH Apps

You can integrate your applications with the Microsoft identity platform to allow users to sign in with their work or school account and access your organisation's data to deliver rich data-driven experiences.

Before an application can access your organisation's data, a user must grant the application permissions to do so. Different permissions allow different levels of access. By default, all users are allowed to consent to applications for permissions that don't require administrator consent. For example, by default, a user can consent to allow an app to access their mailbox but can't consent to allow an app unfettered access to read and write to all files in your organisation.

For a secure organisation, all requests for access to data should be approved by an administrator. This can be configured using the settings detailed at: [Configure how end-users consent to applications using Azure AD | Microsoft Docs]

The following shows the optimal configuration.

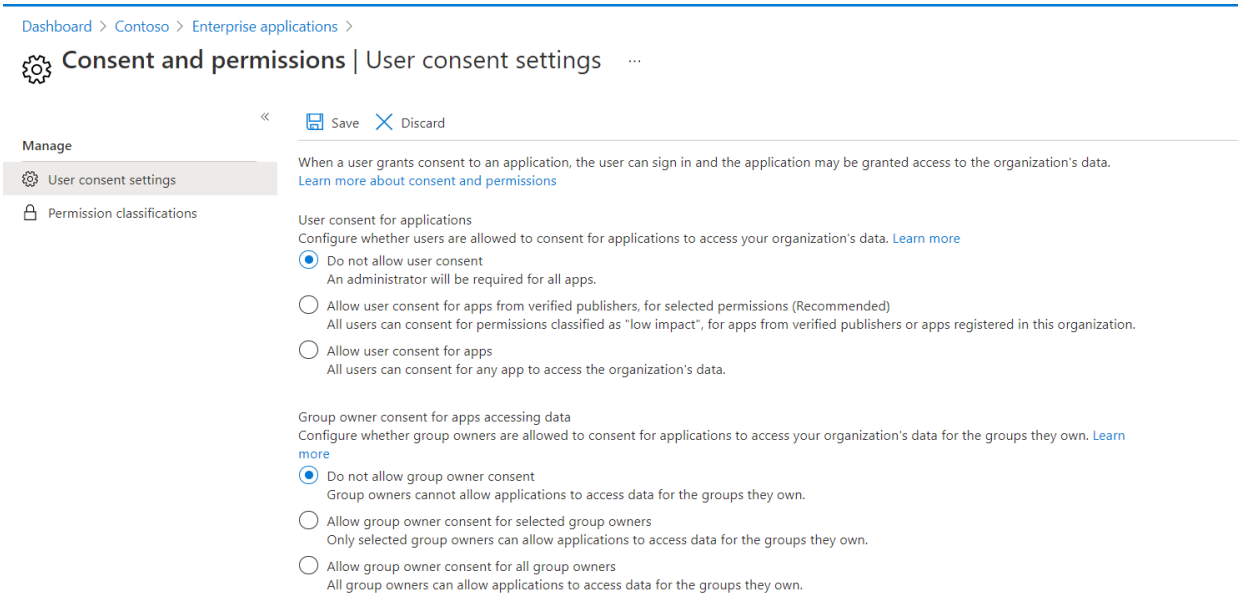

Figure 5: Optimal Configuration for Admin Consent for OAUTH Apps

4.1.2 Authentication Methods

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

4.1.2.1 Cloud authentication

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 synchronisation 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 synchronisation, 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 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.

4.1.2.2 Federated authentication

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

Federated authentication is recommended to be disabled as an authentication method to Office 365 and instead use Password Hash Sync (PHS). This is because on-premises AD Domain Services and ADFS infrastructure has been frequently targeted and compromised by threat actors with well documented methods of attack, specifically SolarWinds breach, Primary threat vectors from compromised on-premises environments. It is also important to consider the maintenance and availability of ADFS or other federation services as this will impact the ability to connect to Office 365 and other cloud services.

Refer to Protecting Microsoft 365 from on-premises attacks | Microsoft Docs for details.

4.1.2.3 Decision tree

Use the decision tree in Figure 6 below to assist in making the cloud authentication model that is right for your organisation.

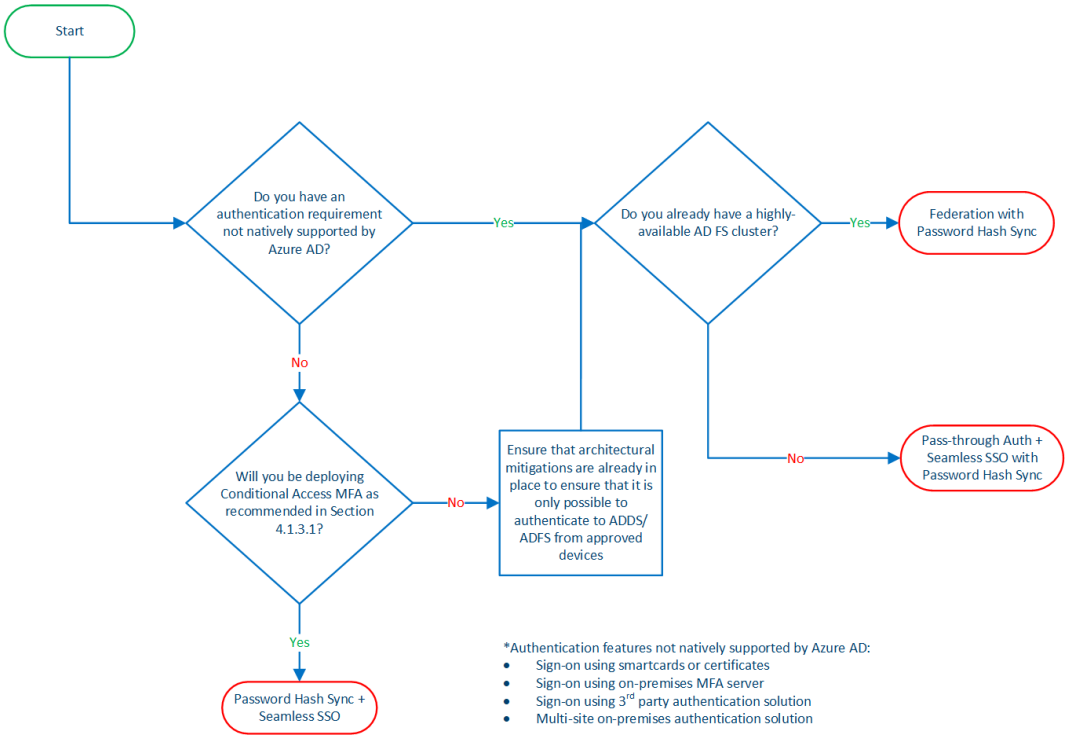

Figure 6: Authentication model decision tree

4.1.3 Recommended Authentication Methods

Azure Active Directory benefits from an extensive monitoring and security infrastructure. Using machine learning and human intelligence that looks across worldwide traffic can rapidly detect attacks and allow you to reconfigure in near-real-time. With this being considered it is recommended that **Azure AD password hash synchronization** is deployed as the authentication method for Office 365 services. Refer to Implement password hash synchronization with Azure AD Connect sync which provides more information and considerations for Azure AD Password Hash Synchronisation.

4.1.4 Conditional Access

Conditional Access is at the heart of the new identity driven control plane. Conditional Access is a feature used to bring signals together, to make decisions, and enforce organisational policies. Think of Conditional Access as a coarse-grained authorisation engine that grants or denies

access to applications based on signals provided and then allows the application to make the fine-grained authorisation decision of what the user can access.

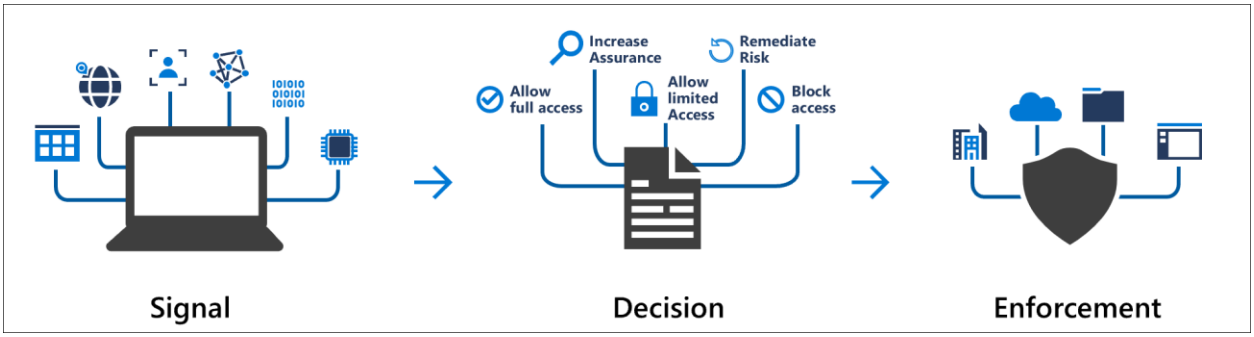

Figure 7: Conditional Access decision-based authorisation

Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action. For example: A payroll manager wants to access their email from their Mac they are required to perform multi-factor authentication to access it and will only be able to use Outlook Web Access not the Outlook client for MacOS or the native email client on a Mac.

By using Conditional Access policies, the right access controls can be applied when needed to keep organisations secure and stay out of your user's way when not needed.

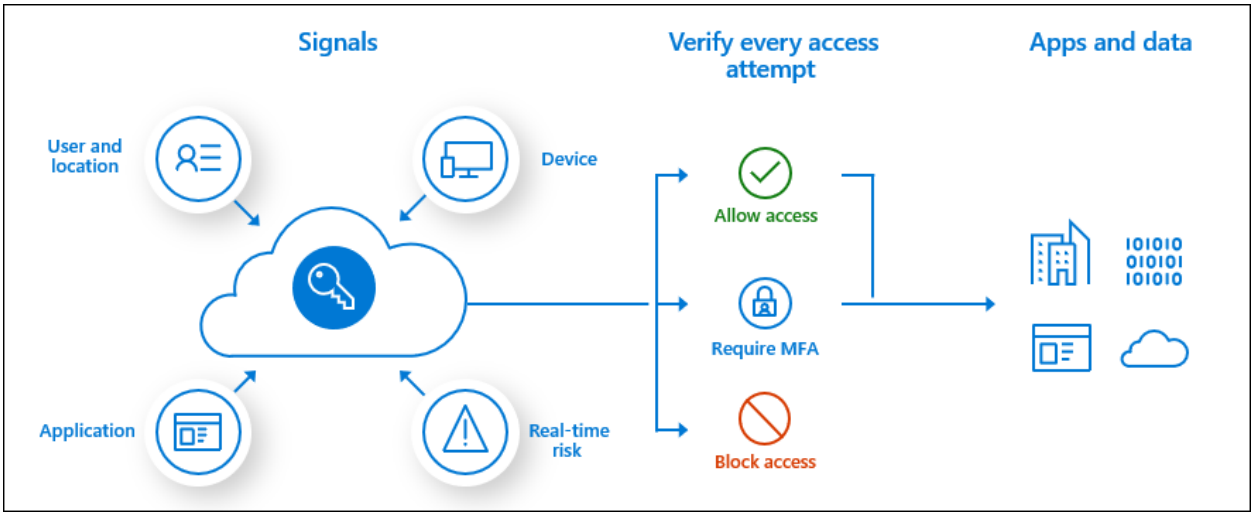

Figure 8: Conditional Access components and flow

> **Important**
>
> Conditional Access policies are enforced after the first-factor authentication has been completed. Conditional Access is not intended as an organisation's first line of defence for scenarios like denial-of-service (DoS) attacks but can use signals from these events to determine access.

4.1.4.1 Enable Azure AD MFA for all users

Multi-factor authentication (MFA) is a process where a user is prompted during a Conditional Access sign in event for additional forms of identification.

Azure AD Multi-Factor Authentication works by requiring two or more of the following authentication methods:

- Something you know, typically a password.
- Something you have, such as a trusted device that is not easily duplicated, like a phone or hardware key.
- Something you are - biometrics like a fingerprint or face scan. When you require a second form of authentication, security is increased as this additional factor isn't something that's easy for an attacker to obtain or duplicate.

By enabling Azure AD MFA for all, users will be required to enrol to the Azure AD MFA service and provide details which can be invoked by Conditional Access to ask for an additional form of authentication as required. For organisations which currently use the Per-User enrolment for Azure AD MFA it is recommended to switch to the CA based enrolment approach.

Refer to the following article for Azure AD Multi-Factor Authentication overview | Microsoft Docs

> **Note**
>
> Azure AD MFA registration is now combined with Azure AD Self-Service Password reset. Refer to Security information registration

4.1.4.2 Control Access to Managed/Compliant Devices

Managed devices are devices which have a method of organisational control applied to them. This control can be a Hybrid AD Joined device using GPO or SCCM policy, or an MDM enrolled device reporting providing its compliance status.

It is recommended that only managed devices are granted access to Office 365. Refer to Require Managed Devices for more details on how configure Conditional Access for this scenario.

As well as the Microsoft Intune Endpoint Management service a small number of third-party MDM services can report device compliance. Refer to Device compliance partners in Microsoft Intune for details.

Where an organisation needs to allow unmanaged devices to access Office 365 services refer to How to have secure remote working with a BYOD policy guidance.

4.1.4.3 Block Legacy Authentication method

For Multi-Factor Authentication to be effective, you also need to block legacy authentication which uses Username and Password only. This is because legacy authentication protocols like POP, SMTP, IMAP, and MAPI can't enforce MFA, making them entry points for adversaries attacking your organisation using Password Spray or similar attacks. The NCSC published a blog post Defending against password spraying attacks

Conditional Access is easiest way to block legacy authentication across your entire organisation by configuring a policy that applies specifically to legacy authentication clients, and taking the action to block.

Refer to the following article to Block legacy authentication - Azure Active Directory | Microsoft Docs

Blocking legacy authentication is the recommended approach however it is acknowledged that that some workloads may still need to use legacy authentication until its use can be blocked. Refer to Blocking legacy authentication for details on how to identify which users and apps are still using legacy authentication and how to then move away from its use. Remember that conditional access policies can be targeted at groups of users, so where possible enforce blocking of legacy authentication using Conditional Access to these users and as more users are identified as no longer needed legacy authentication protocols add them to the Conditional Access policy.

> **Important**
>
> Just because one or two devices/users need to use legacy authentication (i.e. SMTP) does not mean that the rest of the users cannot be protected by Conditional Access blocking it.

4.1.5 Account policy

4.1.5.1 Do not expire passwords

Password expiration policies do more harm than good, because these policies drive users to very predictable passwords composed of sequential words and numbers which are closely related to each other (that is, the next password can be predicted based on the previous password). Password change offers no containment benefits cyber criminals almost always use credentials as soon as they compromise them.

The NCSC publish guidance on password strategies that can help organisations remain secure Password administration for system owners.

Refer to the following article to Set the password expiration policy for your organisation - Microsoft 365 admin | Microsoft Docs and to the Microsoft Password Guidance for more information on password policy.

To further reduce an organisations reliance and exposure on passwords consider moving to a Passwordless approach, refer to Plan a passwordless authentication deployment in Azure Active Directory.

4.1.5.2 Disable accounts not used in the last 30 days

User accounts are not always deleted when employees leave an organisation. Organisations must detect and disable these obsolete user accounts as they are a threat to security.

To detect user accounts which have not logged on to Azure AD can be discovered using the Microsoft Graph API, see How to manage inactive user accounts in Azure AD | Microsoft Docs for details of the query.

Once inactive accounts have been identified these must be reviewed for validity and where possible disabled using the appropriate method.

4.2 Office 365 Service Configuration

4.2.1 Microsoft 365 Audit logging

Audit logging is turned on by default for Microsoft 365 enterprise organisations. When audit log search in the compliance centre is turned on, user and admin activity from your organisation is recorded in the audit log and retained for 90 days, and up to one year depending on the license assigned to users.

Refer to the following article Turn on audit log search to confirm the audit log search function is enabled

4.2.2 Secure Score reviews

Regularly reviewing Secure Score allows organisations to monitor for changes to their security posture and re-evaluate as new controls are made available.

Microsoft Secure Score is a measurement of an organisation's security posture, with a higher number indicating more improvement actions taken. It can be found at https://security.microsoft.com/securescore

Secure Score helps organisations:

- Report on the current state of the organisation's security posture.
- Improve their security posture by providing discoverability, visibility, guidance, and control.
- Many of the security controls described in this guidance are included in Secure Score. 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.

4.2.3 Configure data loss prevention (DLP)

Data loss prevention (DLP) policies in Microsoft 365 are a package of rules which looks at sharing activities, externally and internally, across Exchange, SharePoint, OneDrive and Teams. DLP policies can protect against incidental sharing of sensitive information either by accident, or if a user is unaware that a type information is not to be shared.

DLP uses either predefined or custom "Sensitive Information Types" (SITs) to define and identify information which could be considered private to the organisation. The SITs are used as the basis for DLP policies which if an undesirable volume of sensitive content was attempted to be shared, actions such as Audit, Notify, and Block will be applied, with the optional capability for a user override with reason.

Organisations which have a requirement to prevent certain sensitive information types from leaving the organisation are recommended to configure DLP for that data type.

Refer to Data loss prevention | Microsoft Docs for further information on configuring, and to Sensitive information type entity definitions - Microsoft 365 Compliance | Microsoft Docs for information about the predefined Sensitive Information Types.

4.2.4 Office 365 Cloud App Security

Office Cloud App Security discovers Shadow IT, provides threat protection across Office 365, and can control which apps have permission to access data.

Office 365 Cloud App security is subset of the functionality provided in the Microsoft Cloud App Security service, and as such is accessed and configured using a common administration portal.

To enable the Office 365 Cloud App security service refer to Connect Office 365 to Cloud App Security | Microsoft Docs

Once connected Office Cloud App Security can be used to investigate user activities and apply policies to control user behaviour in Office 365. Refer Investigate risky users tutorial | Microsoft Docs for further information on

Refer to What is Cloud App Security? | Microsoft Docs for more information and Differences between Cloud App Security and Office 365 Cloud App Security | Microsoft Docs to compare the available capabilities with Microsoft Cloud App Security.

4.2.5 Exchange Online

4.2.5.1 Mailbox auditing

Starting in January 2019, mailbox audit logging in enabled by default for all organisations. This means that certain actions performed by mailbox owners, delegates, and admins are automatically logged, and the corresponding mailbox audit records will be available when you search for them in the mailbox audit log.

To verify that mailbox auditing is on for all mailboxes and to view the list of audited actions, refer to this article Verify mailbox auditing on by default is turned on.

By default, only events for Office 365 E5 users are available in audit log searches in the Security & Compliance Center or via the Office 365 Management Activity API.

Mailboxes licenced with Office 365 E3 can be manually enabled for audit log searches in the Security & Compliance Center or via the Office 365 Management Activity API, or alternative search methods used. For details on enabling, refer to Manage mailbox auditing - Microsoft 365 Compliance | Microsoft Docs.

4.2.5.2 Prevent email forwarding to personal email

Client created rules, that Auto-Forward email from user's mailboxes to an external email address, are an increasingly common data exfiltration method being used by threat actors today. This

control is also relevant when preventing users from configuring auto-forward rules to an external email address which could result in unexpected data loss.

The Exchange Admin Center Mail flow reports provides an Auto forwarded messages report which displays information on messages that are automatically forwarded from your organisation to recipients in external domains. This report can be used to look for cases of Mailbox forwarding. Refer to Auto forwarded messages report in the new EAC | Microsoft Docs for report details.

It is recommended that external email forward control is managed using the Exchange Online Protection (EOP) Anti-spam settings to create an Outbound spam filter policy to set automatic forwarding to Off – Forwarding is disabled.

For full details on how to configure external forwarding, please see Configuring and controlling external email forwarding.

In the event that external forwarding is required on a case by case basis, this can be configured using Mail Flow rules or Remote Domains as needed. This should be an exception and in most cases should not be needed.

4.2.5.3 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 organisation (performing reconnaissance) before launching an attack. Publicly available calendars can help attackers understand organisational relationships and determine when specific users may be more vulnerable to an attack, such as when they are traveling.

Refer to Share calendars with external users - Microsoft 365 admin | Microsoft Docs

4.2.5.4 Transport rule for ransomware

For organisations that have not purchased or entitled to use Microsoft Defender for Office 365 this control is recommended. If Microsoft Defender for Office 365 is used, there is no need to implement this control.

Exchange Online mail flow rules can 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, xlsm, 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 for any of the file types that are listed to be allowed. 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.

Multiple mail flow rules can be created and maintained in Exchange Online. For example discrete rules can be created to block executable files, and a separate rule used to warn users about Office documents which contain macros.

For details on how to create an Exchange online mail flow rule refer to Use the EAC to create a mail flow rule.

4.2.5.5 Anti-malware protection in your tenant

For organisations that have not purchased or entitled to use Microsoft Defender for Office 365 this control is recommended. If Microsoft Defender for Office 365 is used, 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.

For details on how to edit the policy refer to Configure anti-malware policies - Office 365 | Microsoft Docs

4.2.5.6 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

Mail Transfer Agent Strict Transport Security (MTA-STS) is a protocol which tells services that are sending your organisation email that your domain supports Transport Layer Security (TLS) 1.2 or higher. For full details refer to Using the Mail Transfer Agent Strict Transport Security (MTA-STS) protocol in your organisation - GOV.UK (www.gov.uk)

Updated government guidance on enforcing TLS between organisations is available here: https://www.gov.uk/guidance/securing-government-email, this is necessary until MTA-STS is

available. Refer to Set up connectors for secure mail flow with a partner organization | Microsoft Docs for details on how to configure TLS between organisations.

The NCSC provides its Mail Check Service for assessing email security compliance here:

https://www.ncsc.gov.uk/mailcheck

4.2.5.7 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 authorised messaging server.

Refer to Set up SPF to help prevent spoofing - Office 365 | Microsoft Docs.

4.2.5.8 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.

Refer to How to use DKIM for email in your custom domain - Office 365 | Microsoft Docs for details on how to setup DKIM for your domains.

4.2.5.9 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.

To setup DMARC refer to Use DMARC to validate email - Office 365 | Microsoft Docs

4.2.5.10 Disable Basic authentication in Exchange Online

As noted in the 4.1.3.3 Block Legacy Authentication control, it is highly recommended to disable legacy authentication with conditional access.

It should be noted that legacy authentication can also be disabled at the Exchange Online service level by assigning authentication policies to users. The policies define the client protocols where Basic authentication is blocked and assigning the policy to all users blocks their Basic authentication requests for the specified protocols.

It is recommended that organisations create an authentication policy using the procedure at Create the authentication policy. By default all basic authentication methods are blocked when an authentication policy is created without options. Once the policy is successfully created it should be assigned to all users using the procedure Assign the authentication policy to users.

For full details on Authentication polices refer to Disable Basic authentication in Exchange Online | Microsoft Docs

4.2.6 Microsoft Teams

The following controls are specific to Microsoft Teams.

4.2.6.1 External Access (Federation)

Microsoft Teams by default allows Teams users to communicate with Teams users in all external organisations. Microsoft Teams allows administrators to control communication with other external organisations using Teams with an Allow list or Block list model.

If an organisation chooses the Block List model, they will be able to communicate with all other external Teams organisations except ones added to the block list.

If an organisation chooses the Allow List model, they will be able to communicate only with Teams organisations added to the allow list.

For most organisations this external communication will be an acceptable state and only if a domain is found to be undesirable it can be added to the Block list to prevent communication from that domain.

However, organisations may wish to limit communication either to only specifically allowed external domains, or to block individual domains for communication. In this instance the organisation should use the Allowed list model to limit communication only to domains listed.

It is recommended that Configure external access in Microsoft Teams Admin Center with an Allowed list model.

Refer to Manage external access (federation) - Microsoft Teams | Microsoft Docs for information of configuring Microsoft Teams external access.

4.2.6.2 Guest Access

Guest access in Teams allows someone who isn't a member of your organisation access to specified teams, documents, channels, resources, chats, and applications which are part of your Teams platform.

By default Microsoft Teams allows Guest users.

Allowing guest access in Teams can appear to increase the risk of data loss, however guest users operate under the same audit and compliance protection as regular users of the service.

It is recommended that organisations allow the use of Guest accounts. Guest accounts should be restricted to permissions and membership of their own directory objects. Guest invites are only sent from specific admin roles.

For details on how to change the Teams guest access setting refer to Teams guest access settings.

For more information on guest access in Teams refer to Guest access in Microsoft Teams - Microsoft Teams | Microsoft Docs.

Organisations are strongly encouraged to enhance their overall Identity Governance capability by becoming familiar with, and implementing Azure AD entitlement management to provide a more robust approach to managing Guest access. With entitlement management, organisations can define a policy that allows users from other organisations you specify to be able to self-request an access package. Access packages specify whether approval is required and an expiration date for the access. Refer to Govern access for external users in Azure AD entitlement management - Azure Active Directory | Microsoft Docs for details

4.2.6.3 Meeting policies

To limit the control guests, have by default in meetings it is recommended that the following changes are made to any global meeting policy. See Manage meeting policies - Microsoft Teams | Microsoft Docs for more information.

A. Disable "Let anonymous people start a meeting". This ensures participates are placed in the lobby until admitted by a presenter.
B. Change "Roles that have presenter rights in meetings" to "Everyone in the organisation, but the user can override". This prevents guests from having the ability to mute participates and other interactive features unless explicitly given present rights during the meeting.
C. Change "Automatically admit people" to "Everyone in your organisation excluding guests". This ensures participates outside of the organisation are added to the lobby and must be admitted to the meeting by a presenter.

4.2.6.4 Control unsanctioned cloud file storage

To prevent the use of unsanctioned file sharing and cloud file storage options for the File tab in Teams we would recommend access to non-organisationally approved third-party cloud storage providers is blocked. This is configured in Organisation-wide settings under the files section. See Manage settings for your organisation - Microsoft Teams | Microsoft Docs for more information.

4.2.6.5 App permission policy

Organisations can use app permission policies to control what apps are available to Microsoft Teams users in your organisation.

It is recommended that the use of third-party apps is managed through an allow list. The organisation should add any third-party apps or services they are happy to permit to the allow list in the app permission policy.

Refer to Manage app permission policies in Microsoft Teams - Microsoft Teams | Microsoft Docs for more information.

4.2.7 SharePoint

4.2.7.1 External Sharing

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 with the following "Allow users to invite and share with authenticated external users" policy.

While it might seem counterintuitive to allow external sharing, this approach provides more control over sharing 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 and revoke links to files with contributors who are both inside and outside your organisation.

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

- Allow users to invite and share with new and existing guests (default setting). Manage sharing settings - SharePoint in Microsoft 365 | Microsoft Docs
- Default link type — select "Only specific people" as this ensures the person sharing the file makes a conscious decision to create a sharing link that they want to share more widely with a "people within organisation link". Manage sharing settings - File and folder links | Microsoft Docs
- Enable "Guests must sign in using the same account to which sharing invitations are sent" to avoid sharing invitations being forwarded on and use with a different account.
- To avoid guests from sharing files inappropriately disable "Allow guests to share items they don't own".

If an organisation wishes to limit who can share files externally then sharing can be limited to named users or preferably via security groups. See Manage security groups - SharePoint in Microsoft 365 | Microsoft Docs for more information.

Sharing settings can also be changed on a site-by-site basis but only made less permissive than the organisation setting i.e. disabled. More information via Change the external sharing setting for a site - SharePoint in Microsoft 365 | Microsoft Docs

4.2.7.2 Block legacy authentication in SharePoint Online

As noted in the 4.1.4.3 Block Legacy Authentication method it is highly recommended to disable legacy authentication with conditional access but it should be noted that legacy authentication can be disabled at the SharePoint service level by a SharePoint Admin.

To block legacy authentication, navigate to the SharePoint admin centre, under Access Control, "Apps that don't use modern authentication" select "Block Access". This can also be configured via PowerShell.

```
# Connect to the tenant
Connect-SPOService -Url https://<tenant>-admin.sharepoint.com

# Check the setting
```

```
Get-SPOTenant -LegacyAuthProtocolsEnabled

# To disable Legacy Auth
Set-SPOTenant -LegacyAuthProtocolsEnabled:$false
```

4.2.7.3 Block custom script

While the majority of SharePoint sites will now be modern sites, it is still possible for an admin to create classic SharePoint sites and there may be some classic sites still serving content. In these classic sites is possible to add custom scripts to these sites using the content editor or script editor web parts whereby JavaScript can run in the context on the user visiting the page. This means:

- Scripts have access to everything the user has access to.
- Scripts can access content across several Microsoft 365 services and even beyond with Microsoft Graph integration.

The following security considerations should be considered before enabling however we would recommend blocking custom scripts and instead use the SharePoint Framework. The SharePoint Framework is a page and web part model that provides a governed and fully supported way to build solutions using scripting technologies with support for open-source tooling.

To disable:

1. Browse to the SharePoint admin centre.
2. Navigate to settings and follow the "Go to classic settings page" link
3. Ensure "Custom Script" has these two values set:
    a. Prevent users from running custom script on personal sites
    b. Prevent users from running custom script on self-service created sites

The following PowerShell can be used on a site-by-site basis to prevent custom scripts.

```
Set-SPOsite <SiteURL> -DenyAddAndCustomizePages 0
```

4.2.7.4 SharePoint Framework API access

When developers build SharePoint Framework solutions, they might need to connect to an API that's secured through Azure Active Directory (Azure AD). Developers can specify which Azure AD applications and permissions their solution requires, and an administrator can manage the permission request from the API access page of the SharePoint admin centre. Any previously approved requests can also be reviewed and removed on this same page and it also details which requests apply to any SharePoint Framework component or custom script in your organisation (organisation-wide) and which requests apply to only the specific component (isolated). More information can be found on the API access page in SharePoint section of Microsoft Docs.

4.2.7.5 Authoritative pages

While typically a topic driven through Intranet like projects if sites are used to publish organisational news or content consider making these sites organisational news sites. This places a visual block to any news published which can be usual to differentiate between news published by organisational sites vs. other sites users follow. For more information see Create an organisation news site - SharePoint in Microsoft 365 | Microsoft Docs

4.2.7.6 Enable site classifications

It is possible to display a classification within modern SharePoint sites (including those created for Teams and Groups). It should be noted this classification is for information purposes only as it does not drive any configurational change or automation like a Sensitivity Label however site classifications are still helpful to provide users with information about how the contents of the site should be handled. It is recommended that site classifications are used and the organisation creates a number of classification labels appropriate to their organisation. Refer to SharePoint "modern" sites classification | Microsoft Docs for more information.

4.2.8 OneDrive

4.2.8.1 Sync settings

For Active Directory domain joined devices to prevent files from being synced to unmanaged devices configure OneDrive to only sync files to PCs that are joined to a specific domain. To enable this you must know the GUID of the domain. See Allow syncing only on computers joined to specific domains - OneDrive | Microsoft Docs for more information.

For Azure AD joined devices conditional access policies to only allow sync to compliant devices should be considered.

4.2.8.2 Known folder move

Redirecting Windows known folders to OneDrive allows users to continue using folders they're familiar with while not changing work habits to save files to OneDrive. As files are saved they're backed up OneDrive and available across devices. Additionally, if a user is affected by ransomware then files can be retrieved from OneDrive and even restored to a point in time using the SharePoint Library restore feature. There are different ways to enable known folder move. It is advised the organisation identifies the right approach based on factors such as the number of users and files. See Redirect and move Windows known folders to OneDrive - OneDrive | Microsoft Docs for more information.

5 Better

For central government and organisations with a higher threat profile this should be the starting point your desired security posture would start at the Better level.

The following controls are included in the Better category:

Control	Action
Azure AD Identity Protection	Configure Conditional Access policy to require MFA when a Sign-In risk value of High or Medium is applied to an identity. Configure a Conditional Access policy to require a password change when a User risk value of High is applied to an identity. Configure Users at risk email alert. Refer to Section 5.1.1 Azure AD Identity Protection
Monitor user accounts for suspicious activity	**This control is applicable for organisations which synchronise user identities from Active Directory Domain Services.** Deploy Microsoft Defender for Identity sensors on on-premises ADDS infrastructure. Configure Defender for Identity to send security alerts to the organisations Security Operations contacts. Refer to Section 5.1.2 Monitor user accounts for suspicious activity
Azure AD Privileged Identity Management	Configure Just-in-time access for the following privileged roles in Azure Active Directory: • Global administrator • Privileged role administrator • Privileged authentication administrator • Security administrator • Compliance administrator • Conditional access administrator • Application administrator • Cloud application administrator • Intune administrator • Exchange Administrator • SharePoint Administrator Refer to Section 5.1.3 Azure AD Privileged Identity Management (PIM)
Schedule access reviews for privileged roles	Create Access reviews for the following Azure AD roles: • Global administrator • Privileged role administrator • Privileged authentication administrator • Security administrator

	• Compliance administrator • Conditional access administrator • Application administrator • Cloud application administrator • Intune service administrator • Intune administrator • Exchange Administrator • SharePoint Administrator Refer to Section 5.1.4 Schedule access reviews for privileged roles
Azure AD Entitlement Management	Investigate the use of Azure AD entitlement management to create access packages to greater control internal and external users to resources. Refer to Section 5.1.5 Azure AD Entitlement Management
Configure Office 365 Advanced Threat Protection Safe Attachments feature	Use the Security & Compliance Center to create Safe Attachments policy. The policy should be set to Block attachments with detected malware and applied to all recipients. Refer to Section 5.2.1 Configure Office 365 Advanced Threat Protection Safe Attachments feature
Configure Office 365 Advanced Threat Protection Safe Links feature	Use the Security & Compliance Center to create Safe Links policy. The policy should be set for URLs to be rewritten and checked against a list of known links when the user clicks on a link. Refer to Section 5.2.2 Configure Office 365 Advanced Threat Protection Safe Links feature
Microsoft Information protection - Labelling/Visible marking	Use Information Protection to add a Sensitivity Label to emails and documents in Office 365. The sensitivity label should be configured to add a Header, Footer or Watermark to the document. Refer to Section 5.2.3 Microsoft Information Protection (Labelling/Visible marking)
Perform a simulated Attack campaign	Schedule regular Attack Simulations using the Microsoft 365 Security Center Attack simulation training. Use the results to train users to be more aware of the threats they are vulnerable to. Refer to Section 5.2.4 Perform a simulated Attack campaign
Connect Microsoft Defender for Office to Azure Sentinel	In Azure Sentinel select Microsoft Defender from the Data connectors gallery Refer to Section 5.2.5 Connect Microsoft Defender for Office to Azure Sentinel

Idle session timeout for SharePoint and OneDrive	Enable idle session timeout for guest users and unmanaged devices. Refer to Section 5.2.7 Turn on idle session timeout for SharePoint and OneDrive
Mark new files in SharePoint and OneDrive as sensitive by default	Turn on mark new files as sensitive by default Refer to Section 5.2.8 Turn on Mark new files as sensitive by default

Table 3: Better controls

5.1 Identity

5.1.1 Azure AD Identity Protection

Azure AD Identity Protection uses signals gathered from Azure AD, consumer cloud (Live.com, Xbox Live, etc) and other third-party sources to measure the risk of an identity having been compromised, or if a particular user sign-in activity is unusual (foreign location, anonymous IP address). A risk score is assigned to the account and sign in activity, which is then fed to Conditional Access for a determination on user access to services or to take action to reset the account.

It is recommended that Azure AD Identity Protection policies are not enforced using the default policies, but instead Conditional Access policies are used.

Refer to the following articles for details on how to configure Conditional Access for Sign-in and User based risks:

Sign-in risk-based Conditional Access - Azure Active Directory | Microsoft Docs

User risk-based Conditional Access - Azure Active Directory | Microsoft Docs

It is recommended that alerts are sent to the relevant Security Operations teams to investigate. Refer to Azure Active Directory Identity Protection notifications | Microsoft Docs for details.

5.1.2 Monitor user accounts for suspicious activity

Microsoft Defender for Identity (MDI) is a cloud-based solution which takes signals from on-premises Active Directory Domain Controllers uses them to identify, detect and investigate threats, compromised accounts, and malicious actions inside the organisation.

It is recommended that Microsoft Defender for Endpoint is deployed with sensors installed on Active Directory Domain Controllers, and ADFS servers if deployed. Security alerts are to be sent to the relevant Security Operations teams and/or SIEM.

Refer to What is Microsoft Defender for Identity? | Microsoft Docs for information and

Microsoft Defender for Identity security alert guide | Microsoft Docs for details on how to deploy Microsoft Defender for Identity.

5.1.3 Azure AD Privileged Identity Management (PIM)

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 provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources.

Azure Active Directory Privileged Identity Management is strongly recommended to provide Just-In-Time access to the following Azure AD administrative roles if they are in use, removing standing user account access:

- Global administrator
- Privileged role administrator
- Privileged authentication administrator
- Security administrator
- Compliance administrator
- Conditional access administrator
- Application administrator
- Cloud application administrator
- Intune service administrator
- Exchange administrator
- Teams administrator
- SharePoint administrator

Refer to What is Privileged Identity Management? - Azure AD | Microsoft Docs for more information.

5.1.4 Schedule access reviews for privileged roles

Membership of privileged roles should be reviewed regularly to ensure that only those people have continued access.

Azure Active Directory Privileged Access Management has an automated process which can be used to create recurring Access Reviews. Refer to Create an access review of Azure AD roles in PIM - Azure AD | Microsoft Docs to learn how to create an Access Reviews.

It is recommended that regular Access Reviews are created for the following Azure AD privileged roles:

- Global administrator
- Privileged role administrator
- Privileged authentication administrator
- Security administrator
- Compliance administrator
- Conditional access administrator
- Application administrator
- Cloud application administrator
- Intune administrator
- Exchange administrator
- Teams administrator
- SharePoint administrator

5.1.5 Azure AD Entitlement Management

Azure AD entitlement management is an identity governance feature that enables organisations to manage identity and access lifecycle at scale, by automating access request workflows, access assignments, reviews, and expiration.

Employees in organisations need access to various groups, applications, and sites to perform their job. Managing this access is challenging, as requirements change - new applications are added or users need additional access rights. This scenario becomes more complicated when external collaboration between organisations is required, you may not know who in the other organisation needs access to your organisation's resources, and they won't know what applications, groups, or sites your organisation is using.

Azure AD entitlement management is the recommended approach to help manage access to groups, applications, SharePoint Online sites and Microsoft Teams for internal users, and also for users outside your organisation who need access to those resources.

Refer to What is Azure AD entitlement management for further details on how to configure Entitlement Management to allow greater control of both internal and external users to resources.

5.2 Office 365 Service Configuration

5.2.1 Configure Office 365 Advanced Threat Protection Safe Attachments feature

The Microsoft Defender for Office 365 Safe Attachments feature extends the malware protections in the Exchange Online Protection service to include routing all messages and attachments that don't have a known virus/malware signature to a hypervisor environment where a behaviour analysis is performed using a variety of machine learning and analysis techniques to detect malicious intent.

Use the Security & Compliance Center to create Safe Attachments policy. The policy should be set to Block attachments with detected malware and applied to all recipients.

- Refer to Set up Safe Attachments policies in Microsoft Defender for Office 365 - Office 365 | Microsoft Docs for details on how to configure the feature.

5.2.2 Configure Office 365 Advanced Threat Protection Safe Links feature

Safe Links is a feature that provides URL scanning and rewriting of inbound email messages in mail flow, and time-of-click verification of URLs and links in email messages. Safe Links scanning occurs in addition to the regular anti-spam and anti-malware protection in inbound email messages in Exchange Online Protection (EOP). Safe Links scanning can help protect the organisation from malicious links that are used in phishing and other attacks.

Use the Security & Compliance Center to create Safe Links policy. The policy should be set for URLs to be rewritten and checked against a list of known links when the user clicks on a link.

Set up Safe Links policies in Microsoft Defender for Office 365 - Office 365 | Microsoft Docs

5.2.3 Microsoft Information Protection (Labelling/Visible marking)

Microsoft Information Protection (MIP) is a cloud-based solution that enables organisations to classify and protect documents and emails by applying labels.

The requirements for labelling will differ depending on the size and function of each organisation. At a minimum level, a label should be created for internal use which can be applied to documents, emails, groups and sites. The label policy should add a header marking to documents, disable external sharing and block access from unmanaged devices. For more information about settings up Sensitivity Labels for sites and groups refer here Use sensitivity

labels with Microsoft Teams, Microsoft 365 groups, and SharePoint sites - Microsoft 365 Compliance | Microsoft Docs.

When configuring sensitivity labels to Teams, SharePoint sites, and Microsoft 365 Groups, you must first complete the steps to enable the feature. See Use sensitivity labels with Microsoft Teams, Microsoft 365 groups, and SharePoint sites - Microsoft 365 Compliance | Microsoft Docs for more information.

Once the organisation has completed the configurations steps the organisation should create sensitivity labels relevant to the organisation which apply visible markings to documents. Refer to Create and publish sensitivity labels - Microsoft 365 Compliance | Microsoft Docs.

The implementation of sensitivity labels in an organisation must take in to account an element of user education and organisational change which is required to be successful. The technical implementation will provide the capability for an organisation to apply labels, but there is an onus on the creators and owners of content to apply appropriate labels. To support users with labels the configuration allows for URLs to guidance to be added in places and it is highly recommended these are used.

5.2.4 Perform a simulated Attack campaign

The Microsoft Security Center Attack simulation training allows organisations to run simulated phishing attacks on their Office 365 tenant, reporting on user behaviour and offering training if required. For details on how to run a phishing simulation and the type of campaign available refer to Get started using Attack simulation training - Office 365 | Microsoft Docs

5.2.5 Connect Microsoft Defender for Office to Azure Sentinel

Azure Sentinel's Microsoft Defender connector with incident integration allows the stream all Microsoft Defender incidents and alerts into Azure Sentinel, this keeps incidents synchronised between both portals. Microsoft Defender incidents include all alerts, entities, and other relevant information, they are enriched and grouped together alerts from Microsoft Defender for Endpoint, Microsoft Defender for Identity, Microsoft Defender for Office 365, and Microsoft Cloud App Security.

For more details on how to implement the connector and advanced settings refer to Connect Microsoft 365 Defender data to Azure Sentinel | Microsoft Docs

5.2.6 Turn off Allow users to shop in the Microsoft Store for Business

Microsoft Store for Business allows organisations a storefront to find, manage, and distribute free and paid apps. From the 14th April 2021 only free Apps will be available from the Microsoft Store for Business however this should still be configured to Turn Off users ability to shop for Apps to prevent any unwanted software being deployed.

Refer to Microsoft Store for Business – Allow users to shop for details on how to configure this setting.

5.2.7 Turn on idle session timeout for SharePoint and OneDrive

Idle session sign-out lets you specify a time at which users are warned and subsequently signed out of Microsoft 365 after a period of browser inactivity in SharePoint and OneDrive on unmanaged devices. The feature defaults to "Sign out users after: 1 hours" and "Give users this much notice before signing them out: 5 minutes."

For more information see Sign out inactive users - SharePoint in Microsoft 365 | Microsoft Docs.

5.2.8 Turn on Mark new files as sensitive by default

When new files are added to SharePoint or OneDrive in Microsoft 365, it takes a while for them to be crawled and indexed. It takes additional time for the DLP policy to scan the content and apply rules to help protect sensitive content. If external sharing is turned on, sensitive content could be shared and accessed by guests before the Office DLP rule finishes processing.

Instead of turning off external sharing entirely, you can address this issue by using a new PowerShell cmdlet. The cmdlet prevents guests from accessing newly added files until at least one Office DLP policy scans the content of the file. If the file has no sensitive content based on the DLP policy, then guests can access the file. If the policy identifies sensitive content, then guests will not be able to access the file. They will receive the following access denied error message: "This file is being scanned right now. Please try again in a few minutes. If you still don't have access, contact the file owner." For more information see Mark new files as sensitive by default - SharePoint in Microsoft 365 | Microsoft Docs.

6 Best

The following controls are included in the Better category:

Control	Action
Enable Customer Lockbox to control Microsoft's access to organisational data.	In the Microsoft 365 Admin Center configure Customer lockbox to Require approval for all data access requests. Refer to Section 6.2.1 Enable Customer Lockbox
Insider risk management	Investigate the use of Microsoft 365 Insider Risk management for the organisation using the Insider risk analytics evaluation tool in the Microsoft 365 Compliance center. Plan and deploy Insider Risk policies using the results from the analytics tool. Refer to Section 6.2.2 Insider risk management
Endpoint Data Loss Protection	Onboard devices for Endpoint DLP. Use Sensitive Information Types defined for DLP to extended use on devices. Refer to Section 6.2.3 Endpoint data loss protection
Extend data loss prevention to Teams chat and channel messages	Configure DLP policies in compliance Center to target Teams Chat Refer to Section 6.2.4 Extend data loss prevention to Teams chat and channel messages
Protect against data loss from cloud apps using Microsoft Cloud App Security	Use Conditional Access policies to enforce Session Control for Office 365 and third-part Web services federated with Azure AD for authentication. Apply session policies in MCAS to enforce DLP. Refer to Section 6.2.5 Protect against data loss from cloud apps using Microsoft Cloud App Security
Restrict access to content by using sensitivity labels	Configure Sensitivity Labels in Microsoft 365 to encrypt content and add additional controls to how the content can be used Refer to Section 6.2.6 Restrict access to content by using sensitivity labels

Table 4: Best controls

6.1 Identity

No additional Identity configuration guidance at the best level.

6.2 Office 365 Service Configuration

6.2.1 Enable Customer Lockbox

Customer Lockbox ensures that Microsoft cannot access your content to perform a service operation without your explicit approval.

Microsoft engineers help troubleshoot and fix issues reported by organisations in the support process. Usually, issues are fixed through telemetry and debugging tools Microsoft has in place for its services. However, some cases require a Microsoft engineer to access customer content to determine the root cause and fix the issue. Customer Lockbox requires the Microsoft engineer to request access from the customer as a final step an approval workflow. This gives organisations the option to approve or deny these requests and provide direct-access control to the customer.

You can turn on Customer Lockbox controls in the Microsoft 365 admin center. When you turn on Customer Lockbox, Microsoft must obtain your organisation's approval before accessing any of your tenant's content.

Refer to Turn Customer Lockbox requests on or off for details on how to turn on the Customer Lockbox.

6.2.2 Insider risk management

Increasingly, employees have more access to create, manage, and share data across a broad spectrum of platforms and services. In most cases, organisations have limited resources and tools to identify and mitigate organisation-wide risks while also meeting compliance requirements and privacy standards. These risks include data theft by departing employees and data leaks of information outside your organisation by accidental oversharing or malicious intent.

Insider risk management in Microsoft 365 uses the full breadth of service and 3rd-party indicators to quickly identify and alert on risky user activity. By using logs from Microsoft 365 and Microsoft Graph, insider risk management allows policies to be defined to identify risk indicators and to take action to mitigate these risks.

Insider risk policies are based on predefined templates that define the risk activities to detect. The following templates are available to organisations:

- Data theft by departing users
- General data leaks
- Data leaks by priority users
- General security policy violations
- Security policy violations by priority users

Insider risk analytics enables you to conduct an evaluation of potential insider risks in your organisation without configuring any insider risk policies. This evaluation can help your organisation identify potential areas of higher user risk and help determine the type and scope of insider risk management policies you may consider configuring. Policy recommendations from analytics

Refer to Get started with insider risk management - Microsoft 365 Compliance | Microsoft Docs for full information.

6.2.3 Endpoint data loss protection

Microsoft Endpoint data loss prevention (Endpoint DLP) is an extension of the Microsoft 365 data loss prevention service described in Section 4.2.3 Configure data loss prevention (DLP)

Microsoft Endpoint DLP allows you to monitor Windows 10 devices and detect when sensitive items are used and shared. When sensitive information is detected, controls are available to audit or restrict:

- Upload to cloud services, e.g. OneDrive Personal, DropBox, Google Drive, or access by unauthorised browser.
- Copy to clipboard.
- Copy to a network share.
- Access by unallowed apps.
- Print.

For details on configuring Endpoint DLP policy refer to Using Endpoint data loss prevention - Microsoft 365 Compliance | Microsoft Docs

To use Endpoint DLP, the devices must be Azure AD or Hybrid Azure AD joined, and if the organisation is not using Microsoft Defender for Endpoint then an onboarding procedure followed. Refer to Onboarding devices for details.

6.2.4 Extend data loss prevention to Teams chat and channel messages

In the Better configuration guidance files shared through teams will have been protected by DLP policies as these use SharePoint and OneDrive as the storage mechanism. However, Chats and Channel messages will not have been analysed for sensitive contents. At the best level it is possible to apply the Data Loss Prevention policies to these messages.

Refer to Data loss prevention and Microsoft Teams - Microsoft 365 Compliance | Microsoft Docs for details.

6.2.5 Protect against data loss from cloud apps using Microsoft Cloud App Security

Microsoft Cloud App Security integrates Azure Active Directory Conditional Access policies to provide a reverse proxy architecture, enabling the enforcement of access and session controls.

Conditional Access App Control enables user app access and sessions to be monitored and controlled in real time based on access and session policies. Access and session policies are used within the Cloud App Security portal to further refine filters and set actions to be taken on a user. The access and session policies can:

- **Prevent data exfiltration**: You can block the download, cut, copy, and print of sensitive documents on, for example, unmanaged devices.
- **Protect on download**: Instead of blocking the download of sensitive documents, you can require documents to be labelled and protected with Azure Information Protection. This action ensures the document is protected and user access is restricted in a potentially risky session.
- **Prevent upload of unlabelled files**: Before a sensitive file is uploaded, distributed, and used by others, it's important to make sure that the file has the right label and protection. You can ensure that unlabelled files with sensitive content are blocked from being uploaded until the user classifies the content.
- **Block potential malware**: You can protect your environment from malware by blocking the upload of potentially malicious files. Any file that is uploaded or downloaded can be scanned against Microsoft threat intelligence and blocked instantaneously.
- **Monitor user sessions for compliance**: Risky users are monitored when they sign into apps and their actions are logged from within the session. You can investigate and analyse user behaviour to understand where, and under what conditions, session policies should be applied in the future.
- **Block access**: You can granularly block access for specific apps and users depending on several risk factors. For example, you can block them if they are using client certificates as a form of device management.

- **Block custom activities**: Some apps have unique scenarios that carry risk, for example, sending messages with sensitive content in apps like Microsoft Teams or Slack. In these kinds of scenarios, you can scan messages for sensitive content and block them in real time.

For further configuration information refer to Protect with Microsoft Cloud App Security Conditional Access App Control | Microsoft Docs

6.2.6 Restrict access to content by using sensitivity labels

When you create a sensitivity labels for the organisation, it is possible to control access to content that the label will be applied to. For example, with the encryption settings for a sensitivity label, you can protect content so that:

- Only users within your organisation can open a document or email.
- Only specified users can edit and print a document or email, while all other users in your organisation can only read it.
- Users cannot forward an email or copy information from it.
- Marked content sent to external parties cannot be opened after a specified date.
- When a document or email is encrypted, access to the content is restricted, so that it:
    - Can be decrypted only by users authorised by the label's encryption settings.
    - Remains encrypted no matter where it resides, inside or outside your organisation, even if the file's renamed.
    - Is encrypted both at rest (for example, in a OneDrive account) and in transit (for example, email as it traverses the internet).

For details on how to configure sensitivity labels to apply encryption and enable additional controls refer to Restrict access to content using sensitivity labels to apply encryption - Microsoft 365 Compliance | Microsoft Docs

7 Incident Response

This Section 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 refer to the Appendix in the previous version of this Blueprint available here, Office 365 Secure Configuration Alignment.

The NCSC recently published What exactly should we be logging? blog post which gives an explanation of what an organisation should be looking to log in support of incident management

7.1 Immediate Actions

- Log a Security Incident in the Admin Portal or with your Technical Account Manager
- Report a cyber security incident with NCSC at Reporting a cyber security incident (ncsc.gov.uk)
- Ensure that Microsoft 365 audit logging is configured correctly, refer to Section 4.2.1 Microsoft 365 Audit logging
- Interfaces where alerts are exposed to users that customers should keep an eye on
    - Security & Compliance Center portal and Microsoft 365 Security Center reports here
    - Exchange malicious content alerts (Safe Links/Safe attachment/Forwarding reports etc) Use mail protection reports
    - Azure AD risky sign in/login reports – refer to Azure Active Directory sign-in activity reports
    - Investigate OCAS/MCAS activity using MCAS dashboards and Generate data management reports
- Set up email notification for security alerts, or messages into Teams using Alert policies in the security and compliance center

Microsoft also publishes guidance on basic Security Incident Response which provides details on

- Detect and Remediate Illicit Consent Grants in Office 365
- Detect and Remediate Outlook Rules and Custom Forms Injections Attacks in Office 365
- Responding to a Compromised Email Account in Office 365