Microsoft

Technical Guide

# Microsoft 365 MEA Blueprint – BYOD Access Patterns

*Prepared for*

MEA Government

03/2021

Version 1.0 Final

*Prepared by*

**Microsoft MEA**

# Table of Contents


1 Blueprint Summary ..... 5

2 Blueprint Overview ..... 9

2.1 Requirements ..... 9

2.2 Deployment Scenarios ..... 10

2.2.1 Office 365 Apps on Android or iOS devices ..... 10

2.2.2 Office 365 Web Application access on PC or Mac ..... 11

2.2.3 Office 365 desktop client access using a Virtual Desktop client ..... 12

3 Blueprint Components ..... 14

3.1 Azure AD ..... 14

3.1.1 Multi-factor Authentication ..... 14

3.1.2 Identity Protection ..... 15

3.1.3 Conditional Access ..... 16

3.2 Microsoft Intune ..... 18

3.2.1 App Protection Policies ..... 18

3.2.2 App Configuration Policies ..... 19

3.2.3 Device Enrolment Restrictions ..... 19

3.3 Microsoft Cloud App Security ..... 20

3.3.1 Session Controls ..... 20

3.3.2 Access Controls ..... 20

3.4 Office 365 ..... 21

3.5 Windows Virtual Desktop ..... 21

4 Blueprint Design Details ..... 24

4.1 Common Configuration ..... 24

4.1.1 Azure AD Groups ..... 24

4.1.2 Azure MFA ..... 25

4.1.3 Enrolment Restriction Policy ..... 26

4.1.4 Common scenario definition ..... 27

4.1.5 Common Configuration policies ..... 28
4.2 Good Configuration Design ..... 34
4.2.1 Good scenario definition ..... 37
4.2.2 Good Configuration Policies ..... 39
4.3 Better Configuration Design ..... 54
4.3.1 Better Use Cases ..... 54
4.3.2 Better Configuration Policies ..... 57
4.4 Best Configuration Design ..... 69
4.4.1 Best scenario definition ..... 70
4.4.2 Best Configuration Policies ..... 73

# 1 Blueprint Summary

This document came out of the need to support MEA Public Sector and Commercial organisations ability to provide additional capabilities to their employees to facilitate remote working by allowing personal unmanaged devices to connect to Office 365 services 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 government and industry and draws heavily on already existing "best practice".

This guidance is not designed to suggest that nothing else is required as *"we do not need to do anything else as we have followed the MOTC and Microsoft's guidance"*. Rather the controls described in this document are intended to help the reader understand why the specific security controls are used and provide step by step configuration guidance allowing organisations to understand how the features and capabilities in Azure AD, Microsoft Intune and Office 365 can be used to ensure that a common bar has been achieved when allowing Bring Your Own Device (BYOD) to access their Office 365 tenant.

To support this effort this blueprint has been developed to support the use of Bring Your Own Device (BYOD) scenarios where organisations are not able to provide corporate laptop or mobile devices.

> **Important**
>
> This blueprint is for configuring end users and not administrative access to Office 365 from BYOD. Administrative accounts should not use BYOD devices to perform administrative tasks nor should be using O365 productivity applications.

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

- Good
  - Forms the minimum level of configuration that all organisations should meet
  - Available with Microsoft 365 E3 license
  - Can be implemented using simple configuration tasks
  - Browser based access for PC and Mac
  - Conditional Access enforced approved apps for Mobile Devices (this is the best approach for Mobile devices that cannot be managed and is consistent in the better/best patterns)
  - Use of Conditional Access with MFA and Restricted Session Controls in Exchange Online and SharePoint Online

- Highest residual risk

- Better
  - Forms the level that organisations should aspire to
  - Available with Microsoft 365 E5
  - Might require more complex configuration tasks.
  - More flexible and granular control of user policies, session controls using Microsoft Cloud App Security
  - Conditional Access enforced browser-based access for PC and Mac.
  - Conditional Access enforced approved apps for Mobile Devices (this is the best approach for Mobile devices that cannot be managed and is consistent in the better/best patterns)
  - Lower residual risk than Good pattern

- Best
  - Available with Microsoft 365 E5
  - Utilises Windows Virtual Desktop (WVD) to provide a service that as closely as possible matches the experience offered when working in the office on corporate IT, from any device.
  - Conditional Access enforced browser or client app-based access to WVD service from PC and Mac.
  - Conditional Access enforced managed device requirement to access Office 365 services from Office client apps from WVD.
  - With good management it significantly reduces the unmanaged PC or Mac attack surface by providing a virtualised corporate desktop for home workers, whilst utilising their personal computing device as the access method
  - Lowest risk approach compared to Good and Better patterns


Figure 1: Blueprint components

The decision flow described in Figure 2 below is designed to help organisations determine which of the patterns described in this document should be used.

For example, if an organisation has M365 E5 licenses then the controls used in the Better or Best deployment scenarios will provide a lower residual risk and therefore should be used.

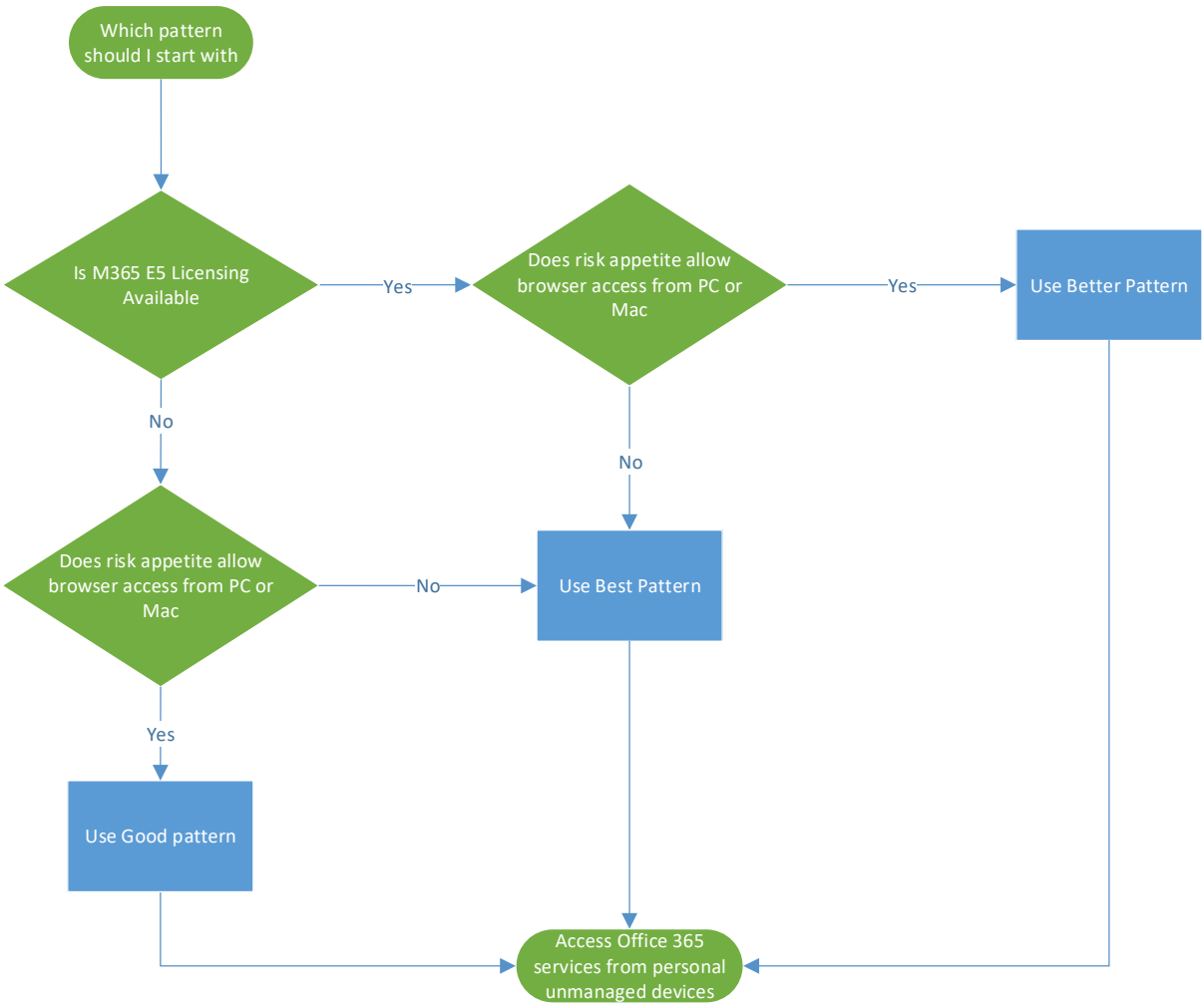



Figure 2: Pattern decision process

# 2 Blueprint Overview

The blueprint covers three primary deployment scenarios that have been identified as meeting the requirement to allow personal unmanaged devices to access corporate data, these are:

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

The following sections describe in more detail how each deployment scenario delivers its capability.

## 2.1 Requirements

The following are a list of the requirements that the Blueprint has been developed against:

1. Only allow approved apps on personal mobile devices
2. Only allow web apps on personal PC and Mac
3. Require MFA to access Office 365 services.
4. Control of files and attachments
    a. Prevent data files from leaving the approved apps (via the share icon - "Share File via")
    b. Prevent other apps from sending data to approved apps.
    c. Prevent copy/paste of data from approved apps to non-approved.
5. Block access from Jailbroken / Rooted devices
6. Only allow devices running an OS after a certain version
7. Wipe corporate data command if phone is lost or PIN entered wrongly [how many times]?

> **Important**
>
> This document intentionally does not cover controls available to you when devices are enrolled into Intune as managed devices; it focuses on the controls that are available for personal unmanaged devices. This document also does not cover Android Enterprise work profiles.

## 2.2 Deployment Scenarios

### 2.2.1 Office 365 Apps on Android or iOS devices

This capability will allow users to have access to Office 365 mobile applications on their personal unmanaged Mobile Devices[1].

**For the Good Pattern**, this capability leverages a combination of Microsoft Azure Active Directory - Multifactor Authentication (MFA) and Conditional Access - policies, and Microsoft Intune - Application Protection Policies

The outcome will allow the end user to:

- Access Exchange Online email using Outlook on their personal Mobile Device.
- Access Skype for Business and/or Teams on their personal Mobile Device
- Access OneDrive for Business on their personal Mobile Device
- Access SharePoint Online on their personal Mobile Device
- Use of Word, Excel, PowerPoint (and potentially other Office 365 approved client applications if required), refer to https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-grant#require-approved-client-app for details of these apps.

All access will be from within approved applications published by Microsoft to either the Apple AppStore or Google Play Store only. The deployment scenario will enforce a policy on the application to secure corporate data. The device will not be managed by the organisation, only the approved Applications will be managed by the organisations.

> **Important**
>
> Organisations will need to provide guidance to their employees on installing the Office Mobile Apps from Apple AppStore or Google Play store onto their mobile devices.

To protect the data in the event that a device is lost or stolen or if the employee leaves the organisation, the Selective Wipe capability in Intune allows any organisational app data and the apps themselves to be removed. Refer to How to wipe only corporate data from Intune-managed apps for more details.

**For the Better Pattern**, Azure AD Identity Protection will be utilised.

Azure AD Identity Protection will be added as condition to the Conditional Access policies to assist with protecting user identities from being utilised in an unsecure manner. Based on

[1] Smart Phones and Tablets running Apple iOS or Android Operating Systems

Medium or High-risk levels being detected, Azure AD Identity Protection will block access to the service until the defined action such as requiring a user the change their password or by forcing multi-factor authentication, has been completed.

For more detailed information on Azure AD Identity Protection refer to https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection

### 2.2.2 Office 365 Web Application access on PC or Mac

This capability will allow users to have access to Office 365 applications in a Web Browser from their personal PC or Mac devices.

**For the Good pattern**, this capability will leverage a combination of Microsoft Azure Active Directory, Multifactor Authentication (MFA), Conditional Access policies and Office 365 application configuration policies to prevent downloading of files or attachments.

The outcome will allow the end user to:

- Access Exchange Online email using Outlook Web Access using a web browser on their personal PC or Mac Device.
- Access Skype for Business and/or Teams web applications using a web browser on their personal PC or Mac Device
- Access OneDrive for Business using a web browser on their personal PC or Mac Device
- Access SharePoint Online using a web browser on their personal PC or Mac Device
- Use of Word, Excel, PowerPoint Web Apps (and potentially other Office 365 web apps.

**For the Better Pattern**, two additional capabilities are utilised:

1. Microsoft Cloud App Security and
2. Azure AD Identity Protection.

Microsoft Cloud App Security service which will enforce certain session controls such as Copy/Paste, Download and Upload in as user's session to prevent work data from being able to be downloaded onto a personal device. The end user device will not be managed by the organisation. The deployment scenario will also restrict access to Internet Browsers only and detect and reject out of date Operating Systems and Browsers[2]

Azure AD Identity Protection will be added as condition to the Conditional Access policies to assist with protecting user identities from being utilised in an unsecure manner. Based on Medium or High-risk levels being detected, Azure AD Identity Protection will block access to the

[2] Microsoft Intelligence have not published the list of supported OS or Browsers yet

service until the defined action such as requiring a user the change their password or by forcing multi-factor authentication, has been completed.

For more detailed information on Azure AD Identity Protection refer to https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection

### 2.2.3 Office 365 desktop client access using a Virtual Desktop client

This **Best Pattern** will allow users to have access to Office 365 applications that are hosted on a Windows Virtual Desktop instance using either a Web Browser or the Virtual Desktop client app from their personal PC or Mac devices.

Virtual desktops provide greater security to organisations as company data can be safely accessed when employees are working remotely. This also means employee productivity is increased as workers are empowered to access data and apps as if they were on their end user device from anywhere, at any time.

Despite the benefits of VDI, previous virtualisation host options left organisations with two choices over the type of virtual machines that they can deploy to deliver desktops.

1. Deploying a Windows Server Desktop experience to achieve the cost savings of multi-session.
2. Deploying single session in Windows 10.

Windows Virtual Desktop utilises Windows 10 multi-session, with optimisations specifically for Office 365 Apps for enterprise, allowing support for either pooled multi-session or personal (persistent) desktops or individual published remote apps, and simplified virtual desktop management.

Windows Virtual Desktop allows organisations to provide a secure remote working capability where employees are no longer constrained to physical hardware or their location. Once they request access to a pooled multi-session virtual desktop or request that a personal desktop is provisioned, it can be quickly delivered and administered based on their profile and specific use case. Access to individual pooled apps provides a simple mechanism to provide access to only the applications that a user needs rather than a complete desktop.

Windows Virtual Desktop leverages Azure Active Directory (Azure AD) as the identity provider, allowing additional security controls like conditional access to require multi-factor authentication (MFA) to access the Windows Virtual Desktop service or that the Windows Virtual Desktop is Hybrid Azure AD joined when accessing the Office 365 services from the desktop device.

The outcome will allow the end user to:

- Access Windows Virtual Desktop instances using a HTML5 application in a web browser on their PC or Mac device
- Access Windows Virtual Desktop instances using the WVD Remote Desktop client application on their PC or Mac device
- Access Exchange Online email using Outlook desktop application or Outlook Web Access from the Windows Virtual Desktop instance.
- Access Skype for Business and/or Teams using the desktop client or web applications from the Windows Virtual Desktop instance
- Access OneDrive using the desktop client or web applications from the Windows Virtual Desktop instance
- Access SharePoint Online using a web browser from the Windows Virtual Desktop instance
- Use Edge to browse the internet whilst using your organisations outbound proxy and/or web content filtering system.
- Use Word, Excel, PowerPoint desktop or web applications on the Windows Virtual Desktop instance.

This pattern provides the lowest risk approach as the personal unmanaged device is only used to connect to the presentation interface of the virtual desktop all the access to documents, web browsing is performed form a managed device that has security policies, in the form of Group Policy, applied that align with the organisation's current policy.

# 3 Blueprint Components

The components that make up the BYOD Blueprint design are illustrated in Figure 3 (below)

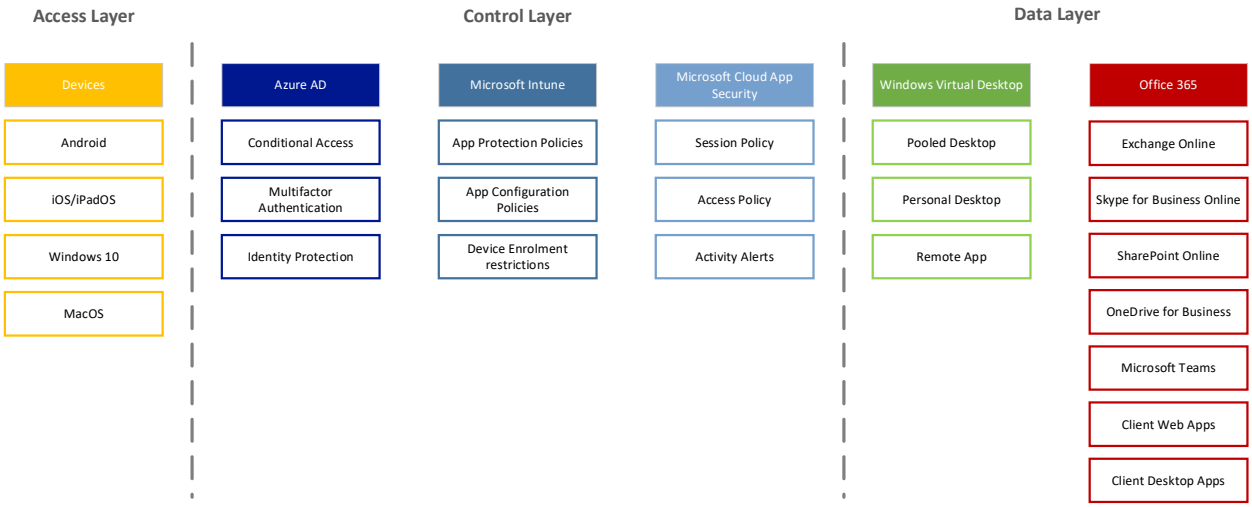



Figure 3: BYOD Blueprint components

## 3.1 Azure AD

The following components of Azure AD are used in the BYOD Blueprint.

### 3.1.1 Multi-factor Authentication

Multi-factor Authentication is used in all three profiles. Multi-factor Authentication (MFA) is a process where a user is prompted during the sign-in process for an additional form of identification, such as to enter a code on their mobile phone or to provide a fingerprint scan. The Blueprint design for MFA comprises a set of configurations made in Azure AD, and a conditional access policy driven deployment approach, i.e. Azure AD Conditional Access requires MFA before access to the application is granted. The user is forced to register in-line within the authentication experience if they are not already registered for MFA, the in-line registration experience is the easiest and most efficient way of forcing registration and widely deploying the service. MFA is an acknowledged approach to reduce the risk of credential stuffing[3] and password spray[4] attacks.

[3] Definition of Credential Stuffing, https://doubleoctopus.com/security-wiki/threats-and-tools/credential-stuffing/

[4] Definition of Password Spray, https://doubleoctopus.com/security-wiki/threats-and-tools/password-spraying/

### 3.1.2 Identity Protection

Identity Protection is used in the Better and Best profiles as it has an Azure AD P2 requirement which is included in M365 E5.

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

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

- Protect all identities regardless of their privilege level.
- Proactively prevent compromised identities from being abused.

Discovering compromised identities is no easy task. Azure Active Directory uses, amongst other inputs, adaptive machine learning algorithms and heuristics to detect anomalies and suspicious incidents that indicate potentially compromised identities. Using this data, Identity Protection generates reports and alerts that enable you to evaluate the detected issues and take appropriate mitigation or remediation actions.

Based on the gathered data in Azure AD Identity Protection generates the following types of risk events are described in Table 1 below:

Table 1: Risk event categories

| Risk event type | Explanation |
|---|---|
| Leaked credentials | Typically, when a breach occurs, credentials are sold or accessed on the dark web and used in attempt to access services. **Leaked credential detection is only supported for organisations using Password Hash Synchronisation** |
| Impossible travel to atypical locations | Multiple sign-ins from different locations across the globe.<br><br>This risk detection type identifies two sign-ins originating from geographically distant locations, where at least one of the locations may also be atypical for the user, given past behaviour. Among several other factors, this machine learning algorithm takes into account the time between the two sign-ins and the time it would have taken for the user to travel from the first location to the second, indicating that a different user is using the same credentials. |
| Sign-ins from infected devices | Device infected with malware that communicate with a bot server. |

| Risk event type | Explanation |
|---|---|
| Sign-ins from anonymous IP addresses | Typically done by proxying, for example using Tor browser. |
| Sign-ins from IP addresses with suspicious activity | IPs which a high number of failed sign-in attempts occurred. |
| Sign-ins from unfamiliar locations | Uses past sign-in locations to determine unfamiliar location. |
| Lockout events | |

Azure Active Directory Identity Protection is more than a monitoring and reporting tool. To protect your organisation's identities, you can configure risk-based policies that automatically respond to detected issues when a specified risk level has been reached.

For the Better profile these policies, in addition to other inputs, are used as signals in conditional access controls provided by Azure AD Conditional Access policies. The policy is configured to block access until the remediation actions including password resets and multi-factor authentication enforcement have been satisfied.

If a sign-in risk is detected they refer to the following link for information on how to remediate the risks and unblock users, https://docs.microsoft.com/en-gb/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock

> **Important**
>
> Self-Service Password Reset (SSPR) will be required to allow users to reset their password in the event of a sign-in risk event being triggered. refer to https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks and https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr for more details.

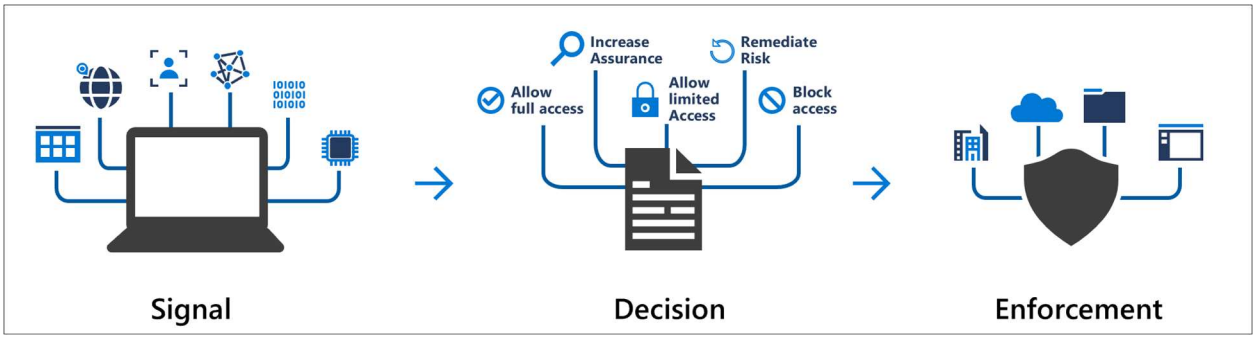
Read more about risk events here: https://azure.microsoft.com/en-us/documentation/articles/active-directory-identityprotection-risk-events-types/

For more detailed information on Azure AD Identity Protection refer to https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection

### 3.1.3 Conditional Access

Conditional Access is used in all three patterns and forms the basis for the control to the Office 365 services being accessed.

Conditional Access is at the heart of **Zero Trust Architecture** and forms the base of the BYOD Blueprint. Conditional Access is the 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.




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.

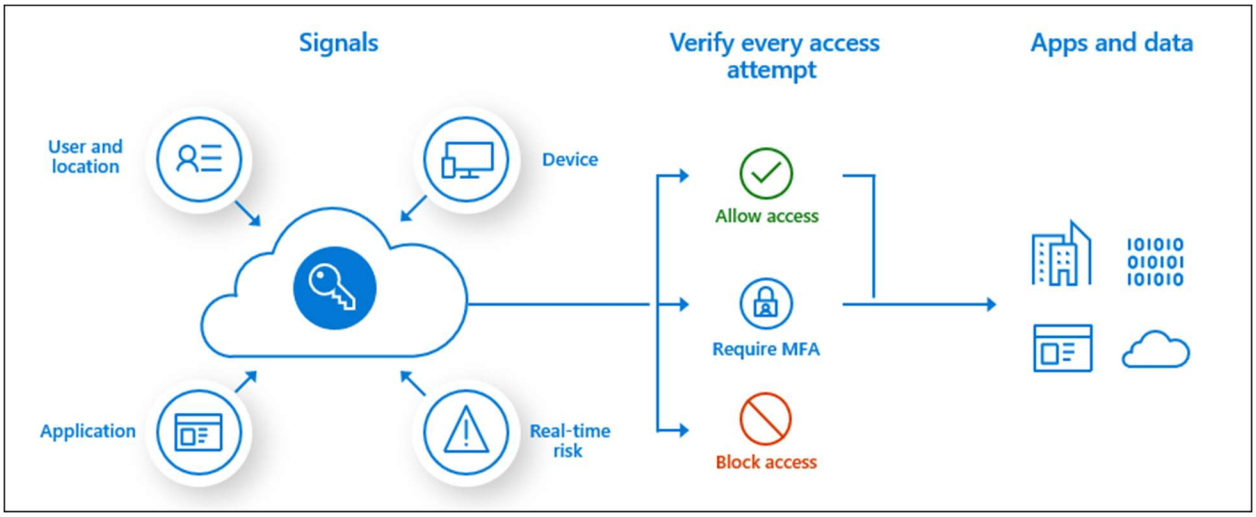


Figure 4 Conditional Access components and flow

> **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.

## 3.2 Microsoft Intune

The following components of Microsoft Intune are used in the BYOD Blueprint.

### 3.2.1 App Protection Policies

App Protection Policies are used in Good, Better and Best mobile device profiles. This blueprint requires that an access attempt to the selected cloud apps, for example, Exchange Online needs to be made from an approved client app such as Outlook for iOS or Android. These approved client apps support Intune app protection policies independent of any mobile-device management (MDM) solution

To utilise this grant control, Conditional Access requires that the device be registered in Azure Active Directory which requires the use of a broker app. The broker app can be either the Microsoft Authenticator for iOS, or the Microsoft Company portal for Android devices. If a broker app is not installed on the device when the user attempts to authenticate, the user gets redirected to the app store to install the broker app.

This setting applies to the following iOS and Android apps:

| | |
|---|---|
| Microsoft Azure Information Protection | Microsoft Bookings |
| Microsoft Cortana | Microsoft Dynamics 365 |
| Microsoft Edge | Microsoft Excel |
| Microsoft Flow | Microsoft Edge browser |
| Microsoft Intune Managed Browser | Microsoft Invoicing |
| Microsoft Kaizala | Microsoft Launcher |
| Microsoft Office | Microsoft OneDrive |

| | |
|---|---|
| Microsoft OneNote | Microsoft Outlook |
| Microsoft Planner | Microsoft PowerApps |
| Microsoft Power BI | Microsoft PowerPoint |
| Microsoft SharePoint | Microsoft Skype for Business |
| Microsoft StaffHub | Microsoft Stream |
| Microsoft Teams | Microsoft To-Do |
| Microsoft Visio | Microsoft Word |
| Microsoft Whiteboard | Microsoft Yammer |

### 3.2.2 App Configuration Policies

App Configuration Policies are used in all three mobile device patterns.

App configuration policies help eliminate app setup problems by letting you assign configuration settings to a policy that is assigned to end-users before they run the app. The settings are then supplied automatically when the app is configured on the end-user's device, and end-users don't need to act. The configuration settings are unique for each app.

The BYOD Blueprint App Protection policies for iOS / iPadOS and Android are configured to use Edge when opening hyperlinks in emails or links in Teams chats.

### 3.2.3 Device Enrolment Restrictions

Device Enrolment Restrictions are used in all three mobile device patterns. Device Enrolment Restrictions create and manage enrolment restrictions that define what devices can enrol into management with Intune.

The specific enrolment restrictions that you can create include:

- Maximum number of enrolled devices.
- Device platforms that can enrol:
  - Android device administrator
  - Android Enterprise work profile
  - iOS/iPadOS
  - macOS
  - Windows

  - Windows Mobile
- Platform operating system version for iOS/iPadOS, Android device administrator, Android Enterprise work profile, Windows, and Windows Mobile. (Only Windows 10 versions can be used. Leave this blank if Windows 8.1 is allowed.)
  - Minimum version.
  - Maximum version.
- Restrict personally owned devices (iOS, Android device administrator, Android Enterprise work profile, macOS, Windows, and Windows Mobile only).

The Blueprint includes an exemplar Device Restriction policy that should be adapted to meet your organisation's needs.

## 3.3 Microsoft Cloud App Security

Microsoft Cloud App Security (MCAS) is used in the Better Scenario as it is part of Microsoft 365 E5.

The following components of Microsoft Cloud App Security are used in the BYOD Blueprint.

### 3.3.1 Session Controls

Microsoft Cloud App Security provides capabilities that will restrict access to only authorised platforms and device types and implement the necessary session controls to minimise the risk of data loss. More information on MCAS session control can be found here, https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad.

MCAS Session Control is invoked by configuring Conditional Access policies to use Conditional Access App Control which then offloads the enforcement of the control to MCAS.

### 3.3.2 Access Controls

Many organisations that choose to use session controls for cloud apps to control in-session activities, also apply access controls to block the same set of native mobile and desktop client apps, thereby providing comprehensive security for the apps.

You can block access to native mobile and desktop client apps with access policies, by setting the **Client app** filter to **Mobile and desktop**. Some native client apps can be individually recognised, whilst others, that are part of a suite of apps, can only be identified as their top-level app, for example apps like SharePoint Online can only be recognised by creating an access policy applied to Office 365 apps.

## 3.4 Office 365

All Office 365 services that are covered by the Office 365 App type in Conditional Access are included in the patterns.

The key applications that are included in the Office 365 client app are:

- Microsoft Flow
- Microsoft Forms
- Microsoft Stream
- Microsoft To-Do
- Microsoft Teams
- Exchange Online
- SharePoint Online
- Microsoft 365 Search Service
- Yammer
- Office Delve
- Office Online
- Office.com
- OneDrive
- PowerApps
- Skype for Business Online
- Sway

## 3.5 Windows Virtual Desktop

Windows Virtual Desktop is Microsoft's desktop and application virtualisation service that runs on Azure. It allows you to virtualise a full Windows 10 or Windows Server operating system with scalability, virtualise Microsoft 365 Apps for enterprise (formerly called "Office 365 ProPlus") and optimize it to run in multi-user virtual scenarios, as well as virtualize other applications.

High-level service architecture

- Can connect to on-premises resources via ExpressRoute or VPN.

- Initial user authentication using Azure Active Directory identities (a domain account is required for local authentication).
- Integrates with Systems Center Configuration Manager and Microsoft Intune
- Supports devices running non-Windows operating systems with Linux thin-client SDK and other tools.

Figure 5 (below) describes the Windows Virtual Desktop service architecture it has also been annotated with the connection flows when a user initiates a connection to a Virtual Desktop. Note that number 0 is an outbound connection, the reverse connect eliminates the need to open inbound ports, reducing the attack surface. The WVD service uses outbound connectivity to connect WVD clients to resources.

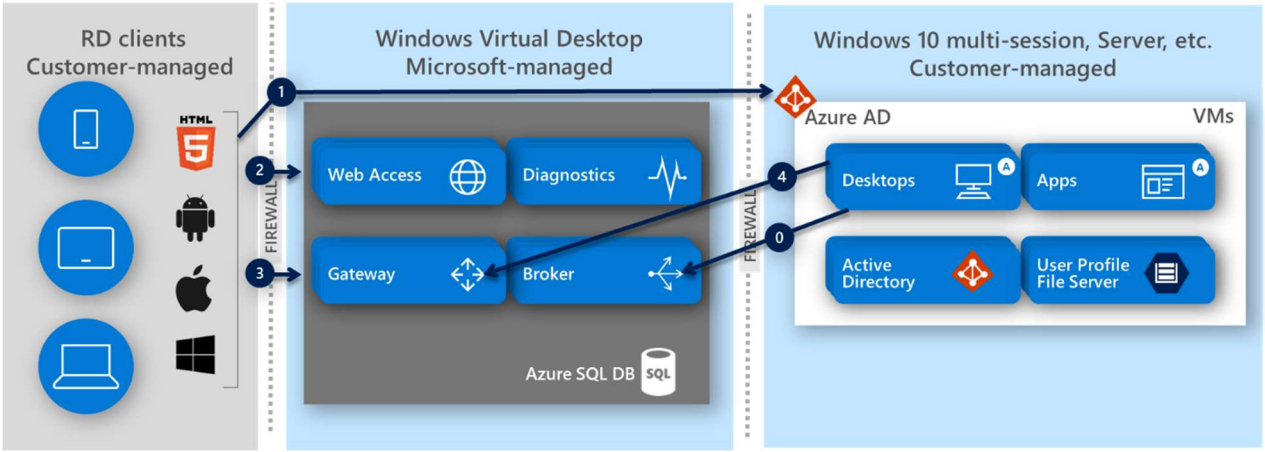



Figure 5: Windows Virtual Desktop Service Architecture and connection flow

User connection flow:

1. User launches RD client which connects to Azure AD, user signs in, and Azure AD returns token.
2. RD client presents token to Web Access, Broker queries DB to determine resources authorised for user.
3. User selects resource, RD client connects to Gateway.
4. Broker orchestrates connection from host agent to Gateway.
5. RDP traffic now flowing between RD client and session host VM over WebSocket connections 3 and 4.

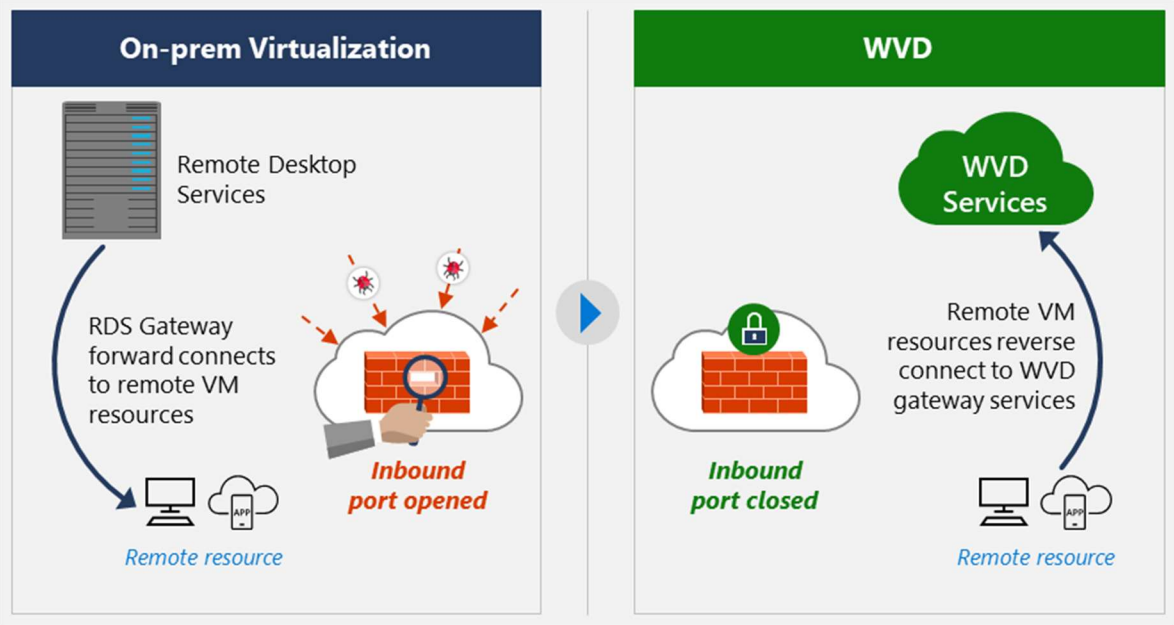



Figure 6: Reverse connect.

The reverse connect approach used by Windows Virtual Desktop has the following benefits:

1. Reduced exposure to attacks
2. Less time monitoring inbound ports.
3. Focus alerts on access and identity-based attacks.

# 4 Blueprint Design Details

This section addresses any major design considerations for the component that are not already documented publicly. This content will be most useful during the preparation of the design and plan. Not all notes will apply to every scenario, so read carefully and exercise good judgement when determining when to apply this guidance.

## 4.1 Common Configuration

The Common configuration components include the Conditional Access policies that should be used across all three configuration baselines.

### 4.1.1 Azure AD Groups

The following groups are used in this document to assign the appropriate policies and configuration settings to the appropriate deployment scenario.

Table 2: Azure AD Groups used in Blueprint deployment scenarios and definitions.

| Group Name | Purpose |
|---|---|
| BYOD-Good-Mobile Device-Users–Enabled | This group is used to apply Good configuration policies to users' mobile devices and place the appropriate configuration controls onto the user's mobile device |
| BYOD-Good-PC-Users–Enabled | This group is used to apply Good configuration policies to users' PC or Mac devices and place the appropriate configuration controls onto the user's mobile device |
| BYOD-Good-Exclude Mobile Device-Users | This group is used to exclude Good configuration policies being applied to users' mobile devices. This might be because they have a corporately issued mobile device but not a laptop device. |
| BYOD-Good-Exclude PC-Users | This group is used to exclude Good configuration policies being applied to users' PC or Mac devices. This might be because they have a laptop device but not a mobile device. |
| BYOD-Better-Mobile Device-Users–Enabled | This group is used to apply Better configuration policies to users' mobile devices and place the appropriate configuration controls onto the user's mobile device |
| BYOD-Better-PC-Users–Enabled | This group is used to apply Better configuration policies to users' PC or Mac devices and place the appropriate configuration controls onto the user's mobile device |
| BYOD-Better-Exclude Mobile Device-Users | This group is used to exclude Better configuration policies being applied to users' mobile devices. This might be because they have a corporately issued mobile device but not a laptop device. |

| Group Name | Purpose |
|---|---|
| BYOD-Better-Exclude PC-Users | This group is used to exclude Better configuration policies being applied to users' PC or Mac devices. This might be because they have a laptop device but not a mobile device. |
| BYOD-Best-Mobile Device-Users–Enabled | This group is used to apply Best configuration policies to users' mobile devices and place the appropriate configuration controls onto the user's mobile device |
| BYOD-Best-PC-Users–Enabled | This group is used to apply Best configuration policies to users' PC or Mac devices and place the appropriate configuration controls onto the user's mobile device |
| BYOD-Best-Exclude Mobile Device-Users | This group is used to exclude Best configuration policies being applied to users' mobile devices. This might be because they have a corporately issued mobile device but not a laptop device. |
| BYOD-Best-Exclude PC-Users | This group is used to exclude Best configuration policies being applied to users' PC or Mac devices. This might be because they have a laptop device but not a mobile device. |

### 4.1.2 Azure MFA

Table 3 (below) describes the MFA configuration settings that are recommended for the BYOD Blueprint.

All options are configured via the Azure MFA Service Settings:

- Azure Portal | Azure Active Directory | Security | Multi-Factor Authentication | Getting Started under Configure – Additional cloud-based MFA settings.

Table 3: MFA configuration settings

| Section | Option | Configuration |
|---|---|---|
| App passwords | Allow users to create app passwords to sign-in to non-browser apps.<br>Do not allow users to create app passwords to sign-in to non-browser apps | Do not allow users to create app passwords to sign-in to non-browser apps |
| Trusted IPs | Skip MFA from Trusted IPs<br>Skip multi-factor authentication for requests from following range of IP address subnets:<br><Add CIDR subnets> | Unchecked |

| Section | Option | Configuration |
|---|---|---|
| Verification options | Methods available to users:<br>• Call to phone<br>• Text message to phone<br>• Notification through mobile app<br>• Verification code from mobile app | Notification through mobile app<br>Verification code from mobile app<br>Call to phone[5]<br>Text message to phone[6] |
| Remember multi-factor authentication | Allow users to remember multi-factor authentication on devices they trust | Unchecked |
| | Days before a device must re-authenticate (1-60) | N/A |

> **Important**
>
> It is important that users are registered for MFA before they access Office 365 services. Microsoft's recommended approach for MFA registration may not be possible under current remote working constraints, refer to https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-registration.
>
> It is therefore recommended that out of band processes are developed to control the MFA registration process, for example, user calls helpdesk and is then added to a group that allows them to register for MFA. Once the registration has been validated, they are then added to the group that allows them access to the Office 365 Services.

### 4.1.3 Enrolment Restriction Policy

Table 4 (below) describes the recommended configuration for Enrolment Restriction policy. This policy will prevent personal devices from being able to join Azure AD and be managed by Microsoft Intune.

[5] Use only when user is unable or unwilling to use Authenticator application on Mobile Device.
[6] Use only when user is unable or unwilling to use Authenticator application on Mobile Device.

> **Important**
>
> If an organisation decides that they are going to ask their employees to enrol their personal devices into Intune for management then this policy will need to be updated to allow personal iOS / iPadOS or Android devices to be enrolled into Intune

Table 4: Intune Enrolment Restriction Policy

| Policy Setting | Value |
|---|---|
| **Name** | CONTOSO-Personal Device Enrolment-Restriction |
| **Description** | Disable Device Enrolment for Personal Devices |
| **Platform Settings** | All device platforms blocked. |
| **Personally Owned** | All device platforms blocked |
| **Assignments** | |
| Included groups | Contoso-Intune-DeviceEnrolment-RestrictPersonal<br>Contoso-O365-BYOD-Enable |
| Excluded groups | -- |

### 4.1.4 Common scenario definition

The following table details common scenarios, segregated by application /workload that are applicable across the three deployment scenarios:

1. Prevent use of Legacy Authentication protocols that use basic authentication. Typically, these protocols cannot enforce any type of second factor authentication.
2. Block Unapproved client app use on all platforms, i.e. block all apps except for Microsoft Intune, Office 365 (Preview), Microsoft Search in Bing, and Microsoft Intune Enrolment. this will prevent those users that can use personal devices to access Office 365 services.

Table 5: Common configuration Conditional Access use cases

| App/ workload | Use case/client | | Desired result |
|---|---|---|---|
| Legacy Authentication Protocols | Browser access to apps using legacy authentication protocol | Unenrolled Mobile Device | Blocked |
| | | Unenrolled PC / Mac | Blocked |
| | | Unenrolled Mobile Device | Blocked |

| App/ workload | Use case/client | | Desired result |
|---|---|---|---|
| | Access Approved client app using legacy authentication protocol | Unenrolled PC / Mac | Blocked |
| Block use of unapproved apps | Browser access to unapproved web apps | Unenrolled Mobile Device | Blocked |
| | | Unenrolled PC / Mac Device | Blocked |
| | Unapproved client app | Unenrolled Mobile Device | Blocked |
| | | Unenrolled PC / Mac Device | Blocked |
| | Browser access to approved web apps | Unenrolled Mobile Device | Allowed with Configuration Baseline controls |
| | | Unenrolled PC / Mac Device | Allowed with Configuration Baseline controls |
| | Approved client app | Unenrolled Mobile Device | Allowed with Configuration Baseline controls |
| | | Unenrolled PC / Mac Device | Allowed with Configuration Baseline controls |

### 4.1.5 Common Configuration policies

This section describes the configuration tasks and settings that are required to configure the Common profile

#### 4.1.5.1 Conditional Access

Table 6 (below) provides the key to all of the Conditional Access policies that are used in this document.

Table 6: Key to Conditional Access tables

| Key | Definition |
|---|---|
| ~~Strikethrough text~~ | Used to indicate that the policy setting is not selected in the policy |
| **Bold** | Used to indicate that the policy setting is selected and if needed describe what value has been selected, e.g. **Office 365 (Preview)** from Cloud apps |
| Approved Client apps | With Conditional Access, organisations can restrict access to approved (modern authentication capable) client apps.<br><br>This blueprint requires that an access attempt to the selected cloud apps, e.g. Exchange Online needs to be made from an approved client app, e.g. Outlook for iOS or Android. These approved client apps support Intune app protection policies independent of any mobile-device management (MDM) solution. Refer to Section 0<br><br>App protection policies (MAM-WE) below for the specific App protection policy configuration |

The following tables detail each Conditional Access policy required to achieve the desired results described in the preceding use cases for the Common configuration.

## Block Legacy Authentication

Legacy authentication refers to protocols that use basic authentication. Typically, these protocols cannot enforce any type of second factor authentication. Examples for apps that are based on legacy authentication are:

- Older Microsoft Office apps
- Apps using mail protocols like POP, IMAP, and SMTP

Single factor authentication (for example, username and password) is not enough these days. This policy setting is used to prevent a user from being able to connect to Office 365 services using only their username and password rather than requiring MFA as well.

Refer to the following link for more details on Legacy authentication protocols

Table 7 (below) describes the Conditional Access policy to block legacy authentication use.

Table 7: BYOD – Common - Block Legacy Authentication

| BYOD-Common-Block Legacy Authentication | | | |
|---|---|---|---|
| Assignments | Users and groups | Include | **BYOD-Good-Mobile Device-Users–Enabled**<br>**BYOD-Good-PC-Users–Enabled**<br>**BYOD-Better-Mobile Device-Users–Enabled**<br>**BYOD-Better-PC-Users–Enabled**<br>**BYOD-Best-Mobile Device-Users–Enabled**<br>**BYOD-Best-PC-Users–Enabled** |
| | | Exclude | |
| | Cloud apps or actions | Include | **All Apps** |
| | | Exclude | |
| | Conditions | Sign-in Risk | |
| | | Device Platforms | Include | **Any Device** |
| | | | Exclude | |
| | | Locations | Include | |
| | | | Exclude | |
| | | Client apps | Include | ~~Browser~~ |

## BYOD-Common-Block Legacy Authentication

| | | | |
|---|---|---|---|
| | | | **Mobile apps and desktop clients** |
| | | | ~~Modern Authentication clients~~ |
| | | | **Exchange ActiveSync clients** |
| | | | **Other clients** |
| | | Device State | Include |
| | | | Exclude |
| Access controls | Grant | **Block Access** | |
| | | Grant Access | ~~Require multi-factor authentication~~ |
| | | | ~~Require device to be marked as compliant~~ |
| | | | ~~Require domain joined (Hybrid Azure AD)~~ |
| | | | ~~Require approved client app~~ |
| | | | ~~Require app protection policy~~ |
| | | For multiple controls | ~~Require one of the selected controls~~ |
| | | | ~~Require all the selected methods~~ |
| | Session | | ~~Use app enforced restrictions~~ |
| | | | ~~Use Conditional Access App Control~~ |
| | | | ~~Sign-in frequency~~ |
| | | | ~~Persistent browser session~~ |
| Enable policy | | | **On** |

## Block unapproved apps

Table 8 (below) describes the Conditional Access policy to only allow BYOD devices to access Office 365 and Bing approved app services.

> ### Important
>
> The Block Unapproved apps Conditional Access policy will need to be modified for the Best Configuration to include the Windows Virtual Desktop and Windows Virtual Desktop Client in the Excluded list of Cloud Apps or Actions to allow users to connect to these service endpoints.

Table 8: BYOD – Common - Block unapproved apps

| **BYOD-Common-Block unapproved apps** | | | |
|---|---|---|---|
| Assignments | Users and groups | Include | **BYOD-Good-Mobile Device-Users–Enabled**<br>**BYOD-Good-PC-Users–Enabled**<br>**BYOD-Better-Mobile Device-Users–Enabled**<br>**BYOD-Better-PC-Users–Enabled**<br>**BYOD-Best-Mobile Device-Users–Enabled**<br>**BYOD-Best-PC-Users–Enabled** |
| | | Exclude | |
| | Cloud apps or actions | Include | **All Apps** |
| | | Exclude | **Office 365 (Preview)**<br>**Microsoft Search in Bing** |
| | Conditions | Sign-in Risk | |
| | | Device Platforms | Include: **Any Device**<br>Exclude: |

| BYOD-Common-Block unapproved apps | | | | |
|---|---|---|---|---|
| | | Locations | Include | |
| | | | Exclude | |
| | | Client apps | Include | ~~Browser~~ |
| | | | | ~~Mobile apps and desktop clients~~ |
| | | | | ~~Modern Authentication clients~~ |
| | | | | ~~Exchange ActiveSync clients~~ |
| | | | | ~~Other clients~~ |
| | | Device State | Include | |
| | | | Exclude | |
| Access controls | Grant | **Block Access** | | |
| | | Grant Access | ~~Require multi-factor authentication~~ | |
| | | | ~~Require device to be marked as compliant~~ | |
| | | | ~~Require domain joined (Hybrid Azure AD)~~ | |
| | | | ~~Require approved client app~~ | |
| | | | ~~Require app protection policy~~ | |
| | | For multiple controls | ~~Require one of the selected controls~~ | |
| | | | ~~Require all the selected methods~~ | |
| | Session | | ~~Use app enforced restrictions~~ | |
| | | | ~~Use Conditional Access App Control~~ | |
| | | | ~~Sign-in frequency~~ | |

| BYOD-Common-Block unapproved apps | | | |
|---|---|---|---|
| | | ~~Persistent browser session~~ | |
| Enable policy | | **On** | |

## Block unapproved Sign-in location

Table 8 (above) describes the Conditional Access policy to only allow BYOD devices to access Office 365 and Bing approved app services from approved countries only.

> ### Important
>
> Block unapproved countries except approved countries Conditional Access policy will need to be modified to allow users to access Office 365 from other countries.

Create a Named Locations policy that based on Countries location, refer to Countries and Regions for more information.

Table 9: BYOD – Common - Block unapproved apps

| BYOD-Common-Block unapproved apps | | | |
|---|---|---|---|
| Assignments | Users and groups | Include | **BYOD-Good-Mobile Device-Users–Enabled**<br>**BYOD-Good-PC-Users–Enabled**<br>**BYOD-Better-Mobile Device-Users–Enabled**<br>**BYOD-Better-PC-Users–Enabled**<br>**BYOD-Best-Mobile Device-Users–Enabled**<br>**BYOD-Best-PC-Users–Enabled** |
| | | Exclude | |
| | Cloud apps or actions | Include | **All Apps** |

| BYOD-Common-Block unapproved apps | | | | |
|---|---|---|---|---|
| | | | Exclude | |
| | Conditions | Sign-in Risk | | |
| | | Device Platforms | Include | |
| | | | Exclude | |
| | | Locations | Include | **Selected Locations**<br>**BYOD Blocked Countries (Allow Approved Countries Only)** |
| | | | Exclude | |
| | | Client apps | Include | ~~Browser~~ |
| | | | | ~~Mobile apps and desktop clients~~ |
| | | | | ~~Modern Authentication clients~~ |
| | | | | ~~Exchange ActiveSync clients~~ |
| | | | | ~~Other clients~~ |
| | | Device State | Include | |
| | | | Exclude | |
| Access controls | Grant | **Block Access** | | |
| | | Grant Access | ~~Require multi-factor authentication~~ | |
| | | | ~~Require device to be marked as compliant~~ | |
| | | | ~~Require domain joined (Hybrid Azure AD)~~ | |
| | | | ~~Require approved client app~~ | |
| | | | ~~Require app protection policy~~ | |

| BYOD-Common-Block unapproved apps | | | |
|---|---|---|---|
| | | For multiple controls | ~~Require one of the selected controls~~ |
| | | | ~~Require all the selected methods~~ |
| | Session | | ~~Use app enforced restrictions~~ |
| | | | ~~Use Conditional Access App Control~~ |
| | | | ~~Sign-in frequency~~ |
| | | | ~~Persistent browser session~~ |
| Enable policy | | | **On** |

## 4.2 Good Configuration Design

The Good Configuration uses only components that are available with a Microsoft 365 (M365) E3 license.

The Good  uses the following components:

- Azure Multi-factor Authentication
- Azure AD Conditional Access
- Intune App Protection policies
- Intune App Configuration policies
- Device Enrolment Restriction policies

### 4.2.1 Good scenario definition

The Good Use Case also includes the Common User Cases for Blocking Legacy Authentication and Blocking Unapproved Apps, refer to Section 4.1 Common Configuration above for details of the use cases and configuration policies.

The following table details each use case, segregated by application/workload.  The client type is broken into two scenarios:

1. Browser-based on PC or Mac, i.e. the web browser on the device, e.g. Microsoft Edge, Chrome, Safari.
2. Approved client app on iOS or Android, i.e. apps developed for the platform, e.g. Microsoft Outlook for Android and iOS/iPadOS, Microsoft Teams for Android and iOS/iPadOS, Office Apps for Android, and iOS/iPadOS.

Table 10: Good configuration Conditional Access use cases

| App/ workload | Use case/client | | Desired result |
|---|---|---|---|
| Exchange Online | Browser access to Outlook on the Web (OWA) | Unenrolled Mobile Device | Blocked |
| | | Unenrolled PC / Mac | Allow with MFA and<br>Use App enforced restrictions |

| App/ workload | Use case/client | | Desired result |
|---|---|---|---|
| | Access via Outlook Approved client app | Unenrolled Mobile Device | Allow with MFA and Require approved client app |
| | | Unenrolled PC / Mac | Blocked |
| | Access via OS native mail client | Unenrolled Mobile Device | Blocked |
| | | Unenrolled PC / Mac | Blocked |
| Teams and/or Skype for Business | Browser access to web apps | Unenrolled Mobile Device | Blocked |
| | | Unenrolled PC / Mac Device | Allow with MFA and Use Conditional Access App Control |
| | Approved client app | Unenrolled Mobile Device | Allow with MFA and Use Conditional Access App Control |
| | | Unenrolled PC / Mac Device | Blocked |
| OneDrive for Business | Browser access to web apps | Unenrolled Mobile Device | Blocked |
| | | Unenrolled PC / Mac Device | Allow with MFA and App Enforced Restrictions |
| | Approved client app access | Unenrolled Mobile Device | Allow with MFA and Require approved client app |
| | | Unenrolled PC / Mac Device | Blocked |
| | | Unenrolled Mobile Device | Allow with MFA |

| App/ workload | Use case/client | | Desired result |
|---|---|---|---|
| SharePoint Online | Browser access to web app | Unenrolled PC / Mac Device | Allow with MFA and App Enforced Restrictions |
| | Approved client app (OneDrive Sync) | Managed desktop client | Blocked |
| | | Enrolled and compliant device | Blocked |
| | | Unenrolled Mobile Device | Allow with MFA and Require approved client app |
| | | Unenrolled PC / Mac Device | Blocked |

### 4.2.2 Good Configuration Policies

This section describes the configuration tasks and settings that are required to configure the Good profile

#### 4.2.2.1 Exchange Online

To support the desired behaviour for the Good Configuration it is necessary to perform some configuration tasks in Exchange Online, refer to https://techcommunity.microsoft.com/t5/outlook-blog/conditional-access-in-outlook-on-the-web-for-exchange-online/ba-p/267069

Outlook Web App supports the configuration of Conditional Access policies which restrict the ability for users to download attachments from email to a local machine when the devices are not compliant. With the power of the Office Web Apps, users can continue to view and edit these files safely, without leaking data to a personal machine.

There is no UI option to configure the conditional access policy for the OWA Mailbox Property the only option is use PowerShell to perform this.

To configure the policy setting use the following PowerShell

For the default OWA Mailbox Policy

```
Set-OwaMailboxPolicy -Identity OwaMailboxPolicy-Default -ConditionalAccessPolicy ReadOnly
```

For a new OWA Mailbox Policy

```
New-OwaMailboxPolicy -Name "Restricted Download Access"
Set-OwaMailboxPolicy -Identity "Restricted Download Access" -ConditionalAccessPolicy ReadOnly
```

> **Information**
>
> The Conditional Access policy setting that is used to enforce this behaviour is “Use app enforced restrictions” under Session in the UI

#### 4.2.2.2 SharePoint Online

To support the desired behaviour for the Good Configuration it is necessary to perform some configuration tasks in SharePoint Online.

> **Important**
>
> Controlling the download of documents from SharePoint Online document libraries and OneDrive for Business is important because other Office 365 applications like Microsoft Teams, Planner and Office 365 Groups all use SharePoint behind the scenes to store documents.

SharePoint exposes the application setting for conditional access in both the UI and in PowerShell. The UI policy is found in the Access control section of the SharePoint Online Admin Center

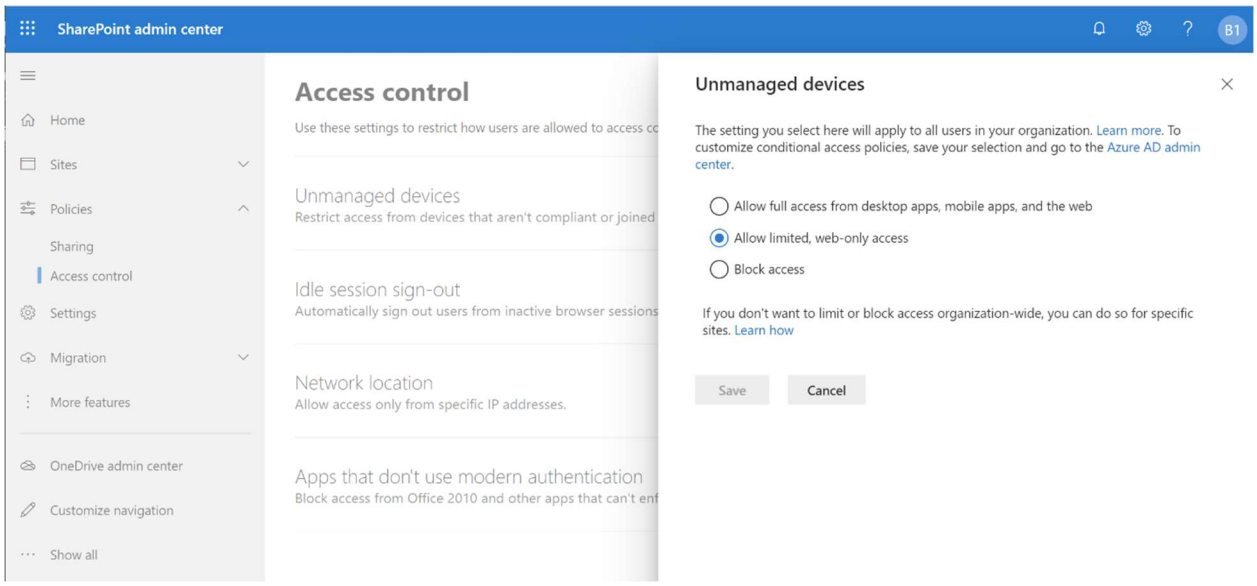



Figure 7: SharePoint Online Conditional Access policy configuration

Click Unmanaged Devices and then select “Allow limited, web-only access”

To set this policy using PowerShell use the Set-SPOTenant cmdlet.

```
Set-SPOTenant -ConditionalAccessPolicy AllowLimitedAccess
```

> **Information**
>
> The SharePoint Online policy setting creates two Conditional Access policies, [SharePoint admin center] Block access from apps on unmanaged devices and [SharePoint admin center] Use app-enforced Restrictions for browser access. These polices are applied to All Users with no exclusions.
>
> The Require MFA for Office 365 using Browser Only on PC and Mac Conditional Access policy implements equivalent settings so the two policy settings created automatically should be unassigned.

#### 4.2.2.3 Conditional Access

The following tables detail each Conditional Access policy required to achieve the desired results described in the preceding use cases for the Good configuration.

The Approved Client Apps policy is defined in Section 0

App protection policies (MAM-WE) Table 14 for iOS and iPadOS and Table 15 for Android later in this document.

##### iOS and iPadOS

Table 11 (below) describes the Conditional Access policy to allow iOS and iPadOS devices to connect to Office 365 applications and Bing using MFA and approved apps.

Table 11: BYOD - Good - Require MFA for Office 365 and Bing using Approved Client Apps on iOS

| **BYOD–Good-Require MFA for Office 365 and Bing using Approved Apps on iOS** | | | |
|---|---|---|---|
| Assignments | Users and groups | Include | **BYOD-Good-Mobile Device-Users–Enabled**<br>**BYOD-Better-Mobile Device-Users–Enabled**<br>**BYOD-Best-Mobile Device-Users–Enabled** |
| | | Exclude | |

| BYOD–Good-Require MFA for Office 365 and Bing using Approved Apps on iOS | | | | |
|---|---|---|---|---|
| | Cloud apps or actions | | Include | **Office 365 (Preview)**<br>**Microsoft Search in Bing** |
| | | | Exclude | |
| | Conditions | Sign-in Risk | | |
| | | Device Platforms | Include | **iOS** |
| | | | Exclude | |
| | | Locations | Include | |
| | | | Exclude | |
| | | Client apps | Include | ~~Browser~~ |
| | | | | **Mobile apps and desktop clients** |
| | | | | **Modern Authentication clients** |
| | | | | ~~Exchange ActiveSync clients~~ |
| | | | | ~~Other clients~~ |
| | | Device State | Include | |
| | | | Exclude | |
| Access controls | Grant | Block Access | | |
| | | **Grant Access** | **Require multi-factor authentication** | |
| | | | ~~Require device to be marked as compliant~~ | |
| | | | ~~Require domain joined (Hybrid Azure AD)~~ | |
| | | | **Require approved client app** | |
| | | | ~~Require app protection policy~~ | |

| BYOD–Good-Require MFA for Office 365 and Bing using Approved Apps on iOS | | | |
|---|---|---|---|
| | | For multiple controls | ~~Require one of the selected controls~~ |
| | | | **Require all the selected methods** |
| | Session | | ~~Use app enforced restrictions~~ |
| | | | ~~Use Conditional Access App Control~~ |
| | | | ~~Sign-in frequency~~ |
| | | | ~~Persistent browser session~~ |
| Enable policy | | | On |

## Android Devices

Table 12 (below) describes the Conditional Access policy to allow Android devices to connect to Office 365 applications and Bing using MFA and approved apps

Table 12: BYOD - Good - Require MFA for Office 365 and Bing using Approved Apps on Android

| BYOD-Good-Require MFA for Office 365 and Bing using Approved Apps on Android | | | |
|---|---|---|---|
| Assignments | Users and groups | Include | **BYOD-Good-Mobile Device-Users–Enabled**<br>**BYOD-Better-Mobile Device-Users–Enabled**<br>**BYOD-Best-Mobile Device-Users–Enabled** |
| | | Exclude | |
| | Cloud apps or actions | Include | **Office 365 (Preview)**<br>**Microsoft Search in Bing** |
| | | Exclude | |
| | Conditions | Sign-in Risk | |
| | | Include | **Android** |

| BYOD-Good-Require MFA for Office 365 and Bing using Approved Apps on Android | | | | |
|---|---|---|---|---|
| | | Device Platforms | Exclude | |
| | | Locations | Include | |
| | | | Exclude | |
| | | Client apps | Include | ~~Browser~~ |
| | | | | **Mobile apps and desktop clients** |
| | | | | **Modern Authentication clients** |
| | | | | ~~Exchange ActiveSync clients~~ |
| | | | | ~~Other clients~~ |
| | | Device State | Include | |
| | | | Exclude | |
| Access controls | Grant | Block Access | | |
| | | **Grant Access** | **Require multi-factor authentication** | |
| | | | ~~Require device to be marked as compliant~~ | |
| | | | ~~Require domain joined (Hybrid Azure AD)~~ | |
| | | | **Require approved client app** | |
| | | | ~~Require app protection policy~~ | |
| | | For multiple controls | ~~Require one of the selected controls~~ | |
| | | | **Require all the selected methods** | |
| | Session | | ~~Use app enforced restrictions~~ | |
| | | | ~~Use Conditional Access App Control~~ | |

| BYOD-Good-Require MFA for Office 365 and Bing using Approved Apps on Android | | | |
|---|---|---|---|
| | | ~~Sign-in frequency~~ | |
| | | ~~Persistent browser session~~ | |
| Enable policy | | On | |

## PC or Mac Devices

Table 13 (below) describes the Conditional Access policy to allow PC and Mac devices to connect to Office 365 applications and Bing using MFA and a web browser.

Table 13: BYOD - Good - Require MFA for Office 365 using Browser Only on PC or Mac

| BYOD-Good-Require MFA for Office 365 using Browser Only on PC or Mac | | | | |
|---|---|---|---|---|
| Assignments | Users and groups | | Include | **BYOD-Good-PC-Users–Enabled** |
| | | | Exclude | **BYOD-Better-PC-Users–Enabled**<br>**BYOD-Best-PC-Users–Enabled** |
| | Cloud apps or actions | | Include | **Office 365 (Preview)**<br>**Microsoft Search in Bing** |
| | | | Exclude | |
| | Conditions | Sign-in Risk | | |
| | | Device Platforms | Include | **Any Device**[7] |
| | | | Exclude | **iOS**<br>**Android** |
| | | Locations | Include | |

[7] The scope for Any device will include Linux desktops and Windows Phone devices and has been used to be more inclusive for the Blueprint. Changing the Device platforms to Windows and macOS will change the policy to only those platforms.

| BYOD-Good-Require MFA for Office 365 using Browser Only on PC or Mac | | | | |
|---|---|---|---|---|
| | | | Exclude | |
| | | Client apps | Include | **Browser** |
| | | | | ~~Mobile apps and desktop clients~~ |
| | | | | ~~Modern Authentication clients~~ |
| | | | | ~~Exchange ActiveSync clients~~ |
| | | | | ~~Other clients~~ |
| | | Device State | Include | |
| | | | Exclude | |
| Access controls | Grant | Block Access | | |
| | | **Grant Access** | **Require multi-factor authentication** | |
| | | | ~~Require device to be marked as compliant~~ | |
| | | | ~~Require domain joined (Hybrid Azure AD)~~ | |
| | | | ~~Require approved client app~~ | |
| | | | ~~Require app protection policy~~ | |
| | | For multiple controls | ~~Require one of the selected controls~~ | |
| | | | **Require all the selected methods** | |
| | Session | | **Use app enforced restrictions** | |
| | | | ~~Use Conditional Access App Control~~ | |
| | | | ~~Sign-in frequency~~ | |
| | | | ~~Persistent browser session~~ | |

| BYOD-Good-Require MFA for Office 365 using Browser Only on PC or Mac | |
|---|---|
| Enable policy | On |

#### 4.2.2.4 App protection policies (MAM-WE)

### iOS and iPadOS

Table 14 (below) describes the app protection policy for iOS and iPadOS devices.

Table 14, iOS App Protection Policy

| Policy Setting | Value |
|---|---|
| **Name** | Contoso_Apple_AppProtectionPolicy |
| **Description** | |
| **Platform** | iOS/iPadOS |
| **Apps** | |
| Target Apps on all device types | Yes |
| Public Apps | Microsoft Dynamics CRM on iPad<br>Microsoft Dynamics CRM on iPhone<br>Skype for Business<br>PowerApps<br>Edge<br>Excel<br>Outlook<br>PowerPoint<br>Word<br>Office Hub<br>OneNote<br>Microsoft Planner<br>Microsoft Power BI<br>Microsoft Flow<br>Microsoft SharePoint<br>OneDrive |

| Policy Setting | Value |
|---|---|
| | Microsoft Teams<br>Microsoft Stream<br>Microsoft To-Do<br>Microsoft Vision Viewer<br>Yammer |
| Custom Apps | |
| **Data Protection** | |
| Prevent Backups | Block |
| Send org data to other apps | Policy managed apps with Open-In/Share filtering |
| Select apps to exempt | |
| Save copies of org data | Block |
| Allow user to save copies to selected services | OneDrive for Business<br>SharePoint |
| Transfer telecommunications data to | Any dialler app |
| Receive data from other apps | Policy managed apps |
| Restrict cut, copy, and paste between other apps | Policy managed apps with paste in |
| Cut and copy character limit for any app | 0 |
| Third party keyboards | SwiftKey Keyboard: com.touchtype.swiftkey |
| Sync app with native contacts app | Block |
| Printing org data | Block |
| Restrict web content transfer with other apps | Microsoft Edge |
| Unmanaged browser protocol | -- |
| Org data notifications | Allow |
| **Access Requirements** | |
| PIN for access | Require |
| PIN type | Numeric |

| Policy Setting | Value |
|---|---|
| Simple PIN | Block |
| Select minimum PIN length | 4 |
| Touch ID instead of PIN for access (iOS 8+/iPadOS) | Allow |
| Override biometrics with PIN after timeout | Require |
| Timeout (minutes of inactivity) | 30 |
| Face ID instead of PIN for access (iOS 11+/iPadOS) | Allow |
| PIN reset after number of days | No |
| Number of days | 0 |
| App PIN when device PIN is set | Require |
| Work or school account credentials for access | No required |
| Recheck the access requirements after (minutes of inactivity) | 10 |
| **Conditional Launch** | |
| Max PIN attempts | 5 – Reset PIN |
| Offline grace period | 720 - Block access (minutes) |
| Offline grace period | 90 – Wipe data (days) |
| Jailbroken/rooted devices | Block access |
| Min OS Version | 13.0 |
| Disabled Account | Block |
| **Assignments** | |
| Included Groups | BYOD-Good-Mobile Device-Users–Enabled<br>BYOD-Better-Mobile Device-Users–Enabled<br>BYOD-Best-Mobile Device-Users–Enabled |
| Excluded Groups | |

## Android

Table 15 (above) describes the app protection policy for Android devices.

Table 15, Android App Protection Policy

| Policy Setting | Value |
|---|---|
| **Name** | Contoso-Android-AppProtectionPolicy |
| **Description** | Android MAM Policy for Office Applications and BYOD |
| **Platform** | Android |
| **Apps** | |
| Target Apps on all device types | Yes |
| Public Apps | Dynamics CRM for Phones<br>Dynamics CRM for Tablets<br>Skype for Business<br>PowerApps<br>Edge<br>Excel<br>Outlook<br>PowerPoint<br>Word<br>Office Hub<br>Office Hub [HL]<br>Office Hub [ROW]<br>OneNote<br>Microsoft Planner<br>Microsoft Power BI<br>Microsoft Flow<br>Microsoft SharePoint<br>OneDrive<br>Microsoft Teams<br>Microsoft Stream<br>Microsoft To-Do<br>Yammer |
| Custom Apps | |
| **Data Protection** | |

| Policy Setting | Value |
|---|---|
| Prevent Backups | Block |
| Send org data to other apps | Policy managed apps |
| Select apps to exempt | -- |
| Save copies of org data | Block |
| Allow user to save copies to selected services | OneDrive for Business<br>SharePoint |
| Transfer telecommunications data to | Any dialer app |
| Receive data from other apps | All apps |
| Restrict cut, copy, and paste between other apps | Policy managed apps with paste in |
| Cut and copy character limit for any app | 0 |
| Screen capture and Google Assistant | Disable |
| Approved keyboards | Require |
| Select keyboards to approve | Gboard - the Google Keyboard: com.google.android.inputmethod.latin<br>SwiftKey Keyboard: com.touchtype.swiftkey<br>Samsung Keyboard: com.sec.android.inputmethod<br>Google Indic Keyboard: com.google.android.apps.inputmethod.hindi<br>Google Pinyin Input: com.google.android.inputmethod.pinyin<br>Google Japanese Input: com.google.android.inputmethod.japanese<br>Google Korean Input: com.google.android.inputmethod.korean<br>Google Handwriting Input: com.google.android.apps.handwriting.ime<br>Google voice typing com.google.android.googlequicksearchbox<br>Samsung voice input: com.samsung.android.svoiceime |
| Encrypt org data | Require |
| Encrypt org data on enrolled devices | Require |

| Policy Setting | Value |
|---|---|
| Sync app with native contacts app | Block |
| Printing org data | Block |
| Restrict web content transfer with other apps | Microsoft Edge |
| Unmanaged Browser ID | -- |
| Unmanaged Browser Name | -- |
| Org data notifications | Allow |
| **Access Requirements** | |
| PIN for access | Require |
| PIN type | Numeric |
| Simple PIN | Block |
| Select minimum PIN length | 4 |
| Fingerprint instead of PIN for access (Android 6.0+) | Allow |
| Override fingerprint with PIN after timeout | Require |
| Timeout (minutes of inactivity) | 30 |
| PIN reset after number of days | No |
| Number of days | 0 |
| Select number of previous PIN values to maintain | 0 |
| App PIN when device PIN is set | Require |
| Work or school account credentials for access | No required |
| Recheck the access requirements after (minutes of inactivity) | 10 |
| **Conditional Launch** | |
| Max PIN attempts | 5 – Reset PIN |
| Offline grace period | 720 - Block access (minutes) |
| Offline grace period | 90 – Wipe data (days) |

| Policy Setting | Value |
|---|---|
| Jailbroken/rooted devices | Block access |
| Min OS Version | 8.0 |
| SafetyNet device attestation | Basic integrity and certified devices |
| Disabled Account | Block |
| **Assignments** | |
| Included Groups | BYOD-Good-Mobile Device-Users–Enabled<br>BYOD-Better-Mobile Device-Users–Enabled<br>BYOD-Best-Mobile Device-Users–Enabled |
| Excluded Groups | |

#### 4.2.2.5 App configuration polices

### Microsoft Edge

Assign this policy to BYOD-Good-Mobile Device-Users–Enabled, BYOD-Better-Mobile Device-Users–Enabled, BYOD-Best-Mobile Device-Users–Enabled

Table 16 (below) describes the recommended configuration for the BYOD Blueprint. For additional Edge specific configuration controls refer to https://docs.microsoft.com/en-us/mem/intune/apps/manage-microsoft-edge

Assign this policy to BYOD-Good-Mobile Device-Users–Enabled, BYOD-Better-Mobile Device-Users–Enabled, BYOD-Best-Mobile Device-Users–Enabled

Table 16: Application configuration for Microsoft Edge on Mobile

| Name | Value |
|---|---|
| com.microsoft.intune.useEdge | true |
| com.microsoft.intune.mam.managedbrowser.defaultHTTPS | true |
| com.microsoft.intune.mam.managedbrowser.NewTabPage.BrandLogo | true |
| com.microsoft.intune.mam.managedbrowser.NewTabPage.BrandColor | True |

## 4.3 Better Configuration Design

The Better Configuration uses components that are available with a Microsoft 365 E5 license.

The Better configuration uses the following components:

- Azure Multi-factor Authentication
- Azure AD Conditional Access
- Intune App Protection policies
- Intune App Configuration policies
- Intune Device Enrolment Restriction policies
- Microsoft Cloud App Security Session Control policies
- Microsoft Cloud App Security Access policies
- Azure AD Identity Protection policies

The Better configuration includes:

- Microsoft Cloud App Security (MCAS) application session controls to provide more granular control of user actions such as block printing of documents, block uploading documents
- Azure AD Identity Protection sign-in risk controls in Conditional Access.

> **Important**
>
> The Better configuration does not require the configuration of Exchange Online or SharePoint Online to prevent the download of attachments or items that are described in Sections 4.2.2.1 Exchange Online and 4.2.2.2 SharePoint Online above.

The Better configuration design is described in the following sections.

### 4.3.1 Better Use Cases

The Better Use Case also includes the Common User Cases for Blocking Legacy Authentication and Blocking Unapproved Apps, refer to Section 4.1 Common Configuration above for details of the use cases and configuration policies.

The Better Use Case also uses the Conditional Access policies for iOS / iPadOS and Android mobile devices described in the Good Configuration Policies for iOS and iPadOS and Android Devices. Refer to Section 4.2.2.3 Conditional Access for the configuration details.

For the Better use case the browser session to Office 365 applications is protected using MCAS session control, this allows more granular control of the actions that a user can perform, block

printing, block upload as well as blocking download that was controlled in the Good scenario which was provided using configuration of EXO and SPO.

The Better use case also includes Azure AD Identity Protection to provide additional protections to user identities when they access Office 365 services, a Conditional Access policy uses these signals to block High and Medium Sign-in risk events. The Conditional Access policy will also apply to Mobile Device users to provide risk-based identity protection.

The following table details each use case, segregated by application/workload. The client type is broken into two scenarios:

1. Approved client app on iOS or Android, i.e. apps developed for the platform, e.g. Microsoft Outlook for Android and iOS/iPadOS, Microsoft Teams for Android and iOS/iPadOS, Office Apps for Android, and iOS/iPadOS.
2. Browser-based on PC or Mac, i.e. the web browser on the device, e.g. Microsoft Edge, Chrome, Safari to Office 365 and Bing for Business
3. Blocking access to Office 365 and Bing for Business from web browsers on PC or Mac or approved client apps on mobile devices if the sign-in risk is Medium or High in Identity Protection

Table 17: Good configuration Conditional Access use cases

| App/ workload | Use case/client | | Desired result |
|---|---|---|---|
| Exchange Online | Browser access to OWA | Personal Unenrolled Mobile Device | Blocked |
| | | Personal Unenrolled PC / Mac | Allow with MFA and Conditional Access App Control Custom Policy<br>Block access if Sign-in Risk is Medium or High |
| | Access via Outlook Approved client app | Unenrolled Mobile Device | Allow with MFA and Require approved client app<br>Block access if Sign-in Risk is Medium or High |
| | | Unenrolled PC / Mac | Blocked |

| App/ workload | Use case/client | | Desired result |
|---|---|---|---|
| | Access via OS mail client | Unenrolled Mobile Device | Blocked |
| | | Unenrolled PC / Mac | Blocked |
| Teams and/or Skype for Business | Browser access to web apps | Unenrolled Mobile Device | Blocked |
| | | Unenrolled PC / Mac Device | Allow with MFA and Condition Access App Control Custom Policy<br>Block access if Sign-in Risk is Medium or High |
| | Approved client app | Unenrolled Mobile Device | Allow with MFA and Require approved client app<br>Block access if Sign-in Risk is Medium or High |
| | | Unenrolled PC / Mac Device | Blocked |
| OneDrive for Business | Browser access to web apps | Unenrolled Mobile Device | Allow with MFA and App Enforced Restrictions |
| | | Unenrolled PC / Mac Device | Allow with MFA and Condition Access App Control Custom Policy |
| | Approved client app | Unenrolled Mobile Device | Allow with MFA and Require approved client app<br>Block access if Sign-in Risk is Medium or High |
| | | Unenrolled PC / Mac Device | Blocked |

| App/ workload | Use case/client | | Desired result |
|---|---|---|---|
| SharePoint Online | Browser access to web app | Unenrolled Mobile Device | Allow with MFA and Require approved client app<br>Block access if Sign-in Risk is Medium or High |
| | | Unenrolled PC / Mac Device | Allow with MFA and Condition Access App Control Custom Policy<br>Block access if Sign-in Risk is Medium or High |
| | Approved client app (OneDrive Sync) | Unenrolled Mobile Device | Allow with MFA and Require approved client app<br>Block access if Sign-in Risk is Medium or High |
| | | Unenrolled PC / Mac Device | Blocked |

## 4.3.2 Better Configuration Policies

### 4.3.2.1 Conditional Access

The following tables detail the two Conditional Access policies required to achieve the desired results described in the preceding use cases for the Better configuration.

#### All Platforms - Block High or Medium Sign-in Risk

Table 18 (below) describes the Conditional Access policy to Block access to Office 365 applications and Bing from all platforms a PC or Mac and Mobile Devices  when the users Sign-in Risk is High or Medium.

Table 18: BYOD - Better - Block access to Office 365 using Browser and Modern Apps with Sign-in Risk Medium and High for all platforms

| **BYOD-Better-Block access to Office 365 with Sign-in Risk Medium and High on all platforms** | | | |
|---|---|---|---|
| Assignments | Users and groups | Include | **BYOD-Better-PC-Users–Enabled** |
| | | Exclude | **BYOD-Good-PC-Users–Enabled** |
| | Cloud apps or actions | Include | **Office 365 (Preview)**<br>**Microsoft Search in Bing** |
| | | Exclude | |
| | Conditions | Sign-in Risk | **High**<br>**Medium** |
| | | Device Platforms | Include |
| | | | Exclude |
| | | Locations | Include |
| | | | Exclude |
| | | Client apps | Include | **Browser** |
| | | | | **Mobile apps and desktop clients** |
| | | | | **Modern Authentication clients** |
| | | | | ~~Exchange ActiveSync clients~~ |
| | | | | ~~Other clients~~ |
| | | Device State | Include |
| | | | Exclude |

| BYOD-Better-Block access to Office 365 with Sign-in Risk Medium and High on all platforms | | | |
|---|---|---|---|
| Access controls | Grant | **Block Access** | |
| | | Grant Access | ~~Require multi-factor authentication~~ |
| | | | ~~Require device to be marked as compliant~~ |
| | | | ~~Require domain joined (Hybrid Azure AD)~~ |
| | | | ~~Require approved client app~~ |
| | | | ~~Require app protection policy~~ |
| | | For multiple controls | ~~Require one of the selected controls~~ |
| | | | ~~Require all the selected methods~~ |
| | Session | | ~~Use app enforced restrictions~~ |
| | | | ~~Use Conditional Access App Control~~<br>~~Use custom policy~~ |
| | | | ~~Sign-in frequency~~<br>~~1 Hour~~ |
| | | | ~~Persistent browser session~~ |
| Enable policy | | | **On** |

## PC or Mac Devices - Browser Only with Session Control

Table 19 (below) describes the Conditional Access policy to allow PC and Mac devices to connect to Office 365 applications and Bing using MFA and MCAS Session Control using a web browser.

Table 19: BYOD - Better - Require MFA for Office 365 using Browser Only with Session Control on PC or Mac

| **BYOD-Better-Require MFA for Office 365 using Browser Only with Session Control on PC or Mac** | | | | |
|---|---|---|---|---|
| Assignments | Users and groups | | Include | **BYOD-Better-PC-Users–Enabled** |
| | | | Exclude | **BYOD-Good-PC-Users–Enabled** |
| | Cloud apps or actions | | Include | **Office 365 (Preview)** |
| | | | Exclude | |
| | Conditions | Sign-in Risk | | |
| | | Device Platforms | Include | |
| | | | Exclude | |
| | | Locations | Include | |
| | | | Exclude | |
| | | Client apps | Include | **Browser** |
| | | | | ~~Mobile apps and desktop clients~~ |
| | | | | ~~Modern Authentication clients~~ |
| | | | | ~~Exchange ActiveSync clients~~ |
| | | | | ~~Other clients~~ |
| | | Device State | Include | |
| | | | Exclude | |
| Access controls | Grant | Block Access | | |
| | | **Grant Access** | **Require multi-factor authentication** | |

| BYOD-Better-Require MFA for Office 365 using Browser Only with Session Control on PC or Mac | | | |
|---|---|---|---|
| | | | ~~Require device to be marked as compliant~~ |
| | | | ~~Require domain joined (Hybrid Azure AD)~~ |
| | | | ~~Require approved client app~~ |
| | | | ~~Require app protection policy~~ |
| | | For multiple controls | ~~Require one of the selected controls~~ |
| | | | **Require all the selected methods** |
| | Session | | ~~Use app enforced restrictions~~ |
| | | | **Use Conditional Access App Control**<br>**Use custom policy** |
| | | | **Sign-in frequency**<br>**1 Hour**[8] |
| | | | ~~Persistent browser session~~ |
| Enable policy | | | **On** |

### 4.3.2.2 Microsoft Cloud App Security (MCAS)

#### MCAS Copy/Paste Session Control

Table 20 (below) describes the MCAS Session Control policy to prevent Copy/Paste.

Table 20, MCAS Copy/Paste Session Control Policy

| Policy Setting | Value |
|---|---|
| Policy Template | Block cut/copy and paste based on real time content inspection |
| Policy Name | CONTOSO-Block-CopyPaste |

[8] Sign-in frequency can be modified to balance security and usability if feedback is that having to sign-in and MFA every hour is too much

| Policy Setting | Value |
|---|---|
| Description | Block Copy/Cut and Paste functionality |
| Policy Severity | Low |
| Category | DLP |
| Session Control Type | Block Activities |
| Activity Filters | Activity type equals (Cut/Copy Item OR Paste Item) |
| Content Inspection | False |
| Actions | Block |
| Also notify user by email | False |
| Customize block message | 'Copy and Paste functionality has been disabled when accessing from personal devices' |
| Create an alert matching event with the policy's severity | False |

## MCAS Print Session Control

Table 21 (below) describes the MCAS Session Control policy to prevent Printing

Table 21, MCAS Print Session Control Policy

| Policy Setting | Value |
|---|---|
| Policy Template | Block Print functionality |
| Policy Name | Contoso-Block-Print |
| Description | Block Print functionality |
| Policy Severity | Low |
| Category | DLP |
| Session Control Type | Block Activities |
| Activity Filters | Activity type equals (Print) |
| Content Inspection | False |
| Actions | Block |
| Also notify user by email | False |

| Policy Setting | Value |
|---|---|
| Customize block message | 'Printing has been disabled when accessing from personal devices' |
| Create an alert matching event with the policy's severity | False |

## MCAS File Download Session Control

Table 22 (below) describes the MCAS Session Control policy to prevent File Downloads.

Table 22, MCAS File Download Session Control Policy

| Policy Setting | Value |
|---|---|
| Policy Template | Block download based on real-time content inspection |
| Policy Name | CONTOSO-Block-FileDownload |
| Description | Block File Download functionality |
| Policy Severity | Low |
| Category | DLP |
| Session Control Type | Control file download (with DLP) |
| Activity Filters | None |
| Inspection Method | None |
| Actions | Block |
| Also notify user by email | False |
| Customize block message | 'File Download functionality has been disabled when accessing from personal devices' |
| Create an alert matching event with the policy's severity | False |

## MCAS File Upload Session Control

Table 23 (below) describes the MCAS Session Control policy to prevent File Uploads.

Table 23, MCAS File Upload Session Control Policy

| Policy Setting | Value |
|---|---|
| Policy Template | Block upload based on real-time content inspection |

| Policy Setting | Value |
|---|---|
| Policy Name | Contoso-Block-File-Upload |
| Description | Block File Upload functionality |
| Policy Severity | Low |
| Category | DLP |
| Session Control Type | Control file upload (with DLP) |
| Activity Filters | None |
| Inspection Method | None |
| Actions | Block |
| Also notify user by email | False |
| Customize block message | 'File upload functionality has been disabled when accessing from personal devices' |
| Create an alert matching event with the policy's severity | False |

## MCAS Non-Mobile Not-Browser Access Control

Table 24 (below) describes the MCAS Session Control policy to prevent NonMobile-NotBrowser

Table 24, MCAS Outdated OS Access Policy

| Policy Setting | Value |
|---|---|
| Policy Name | Contoso-Block-Access-NonMobile-NotBrowser |
| Description | Block access to Office 365 if the client application is not a Browser and the device is not a Mobile or Tablet |
| Policy Severity | Medium |
| Category | Access Control |
| Activity Filters | Device Type Does Not Equal Mobile OR Tablet<br>Client App Equals Mobile and Desktop<br>App Equals Office 365 |
| Actions | Block |
| Also notify user by email | False |

| Policy Setting | Value |
|---|---|
| Customize block message | 'Access from this application is not supported when using a personal device' |
| Create an alert matching event with the policy's severity | True |
| Send alert as email | TBA |

## MCAS Outdated OS Access Control

Table 25 (below) describes the MCAS Access Control policy to block Outdated OS

Table 25, MCAS Outdated OS Access Policy

| Policy Setting | Value |
|---|---|
| Policy Name | Contoso-Block-Outdated-OS |
| Description | Block Access for Outdated Operating Systems |
| Policy Severity | Low |
| Category | Access Control |
| Activity Filters | User Agent Tag Equals Outdated Operating System<br>App Equals Office 365 |
| Actions | Block |
| Also notify user by email | False |
| Customize block message | 'Access to CONTOSO systems is prohibited from your operating system version' |
| Create an alert matching event with the policy's severity | False |

## MCAS Outdated Browser Access Control

Table 26 (below) describes the MCAS Access Control policy to block Outdated Browser

Table 26, MCAS Outdated Browser Access Policy

| Policy Setting | Value |
|---|---|
| Policy Name | Contoso-Block-Outdated-Browser |
| Description | Block Access for Outdated Browsers |

| Policy Setting | Value |
|---|---|
| Policy Severity | Low |
| Category | Access Control |
| Activity Filters | User Agent Tag Equals Outdated Browser<br>App Equals Office 365 |
| Actions | Block |
| Also notify user by email | False |
| Customize block message | 'Access to CONTOSO systems is prohibited from your Internet Browser version' |
| Create an alert matching event with the policy's severity | False |

#### 4.3.2.3 Azure AD Identity Protection (AAD IdP)

### AAD IdP User Risk Policy

Table 27 (above) describes the Identity Protection policy for User Risk Policy

Table 27: IdP – User Risk Policy

| | | | |
|---|---|---|---|
| Assignments | Users | Include | **BYOD-Better-Mobile Device-Users–Enabled**<br>**BYOD-Better-PC-Users–Enabled**<br>**BYOD-Best-Mobile Device-Users–Enabled**<br>**BYOD-Best-PC-Users–Enabled** |
| | | Exclude | |
| Conditions | User Risk | | **Medium and above** |
| Controls | Access | Block access | |
| | | **Allow access** | **Require password change** |

## AAD IdP Sign-in Risk Policy

Table 28 (above) describes the Identity Protection policy for Sign-in Risk Policy

Table 28: Identity Protection – Sign-in Risk Policy

| | | | |
|---|---|---|---|
| Assignments | Users | Include | **BYOD-Better-Mobile Device-Users–Enabled**<br>**BYOD-Better-PC-Users–Enabled**<br>**BYOD-Best-Mobile Device-Users–Enabled**<br>**BYOD-Best-PC-Users–Enabled** |
| | | Exclude | |
| Conditions | Sign-in Risk | | **Medium and above** |
| Controls | Access | Block access | |
| | | **Allow access** | **Require multi-factor authentication** |

## AAD IdP MFA Registration Policy

Table 29 (above) describes the Identity Protection policy for MFA Registration Policy

Table 29: Identity Protection – MFA Registration policy

| | | | |
|---|---|---|---|
| Assignments | Users | Include | **BYOD-Better-Mobile Device-Users–Enabled**<br>**BYOD-Better-PC-Users–Enabled**<br>**BYOD-Best-Mobile Device-Users–Enabled**<br>**BYOD-Best-PC-Users–Enabled** |
| | | Exclude | |
| Controls | Access | **Allow access** | **Require Azure MFA registration** |

## 4.4 Best Configuration Design

The Best Configuration uses components that are available with a Microsoft 365 E5 license.

The Best configuration uses the following components:

- Azure Multi-factor Authentication
- Azure AD Conditional Access
- Intune App Protection policies
- Intune App Configuration policies
- Intune Device Enrolment Restriction policies
- Microsoft Cloud App Security Session Control policies (if Web Apps used)
- Microsoft Cloud App Security Access policies ((if Web Apps used)
- Azure AD Identity Protection policies
- Windows Virtual Desktop

The Best configuration includes:

- Windows Virtual Desktop to provide a fully managed desktop experience that allows users to work as if they were on their normal office machine. This allows users to choose between the Office Web Apps or Desktop Applications when accessing Office 365.

> ### Important
>
> The Best configuration does not require the configuration of Exchange Online or SharePoint Online to prevent the download of attachments or items that used in the Good Configuration Policies Sections 4.2.2.1 Exchange Online and 4.2.2.2 SharePoint Online above as this functionality is provided by MCAS as well as the other scenarios like block printing and block upload of files.

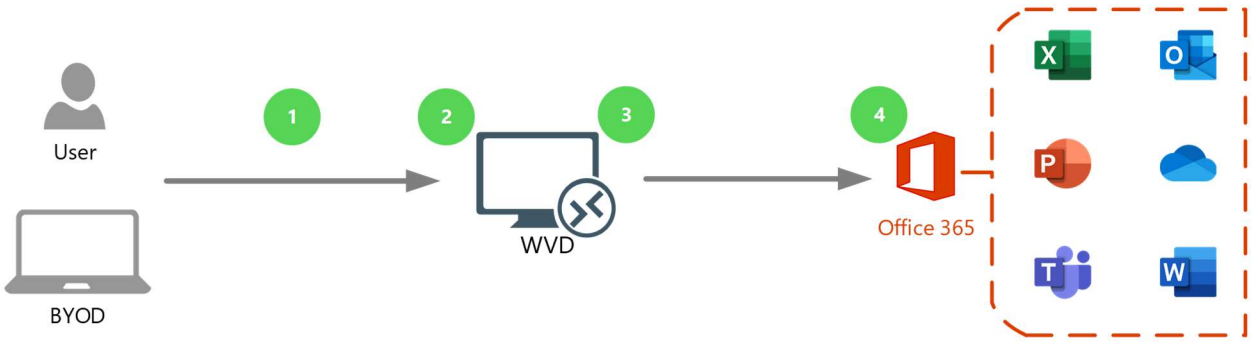



Figure 8: Windows Virtual Desktop access flow

The flow illustrated in Figure 8 above described in Table 30 below.

Table 30: Windows Virtual Desktop connection flow

| Step | Description |
|---|---|
| 1 | From their PC or Mac device the user connects to the Windows Virtual Desktop service either using HTML5 browser or Remote Desktop client app.<br>User needs to satisfy that MFA was used as part of Conditional Access policy to connect to the Windows Virtual Desktop service |
| 2 | From the Windows Virtual Desktop landing page, the user then selects the type of resource, Pooled Desktop, Personal Desktop, Published App, that they wish to use and connects to that resource |
| 3 | From the Windows Virtual Desktop, the user then launches the Office 365 application as required |
| 4 | The Office 365 application is launched<br>This connection is subject to a Conditional Access rule that requires that the connection to Office 365 services is made from a Hybrid Azure AD joined device |

The Best configuration design is described in the following sections.

### 4.4.1 Best scenario definition

The Best scenario also includes the Common User Cases for Blocking Legacy Authentication and Blocking Unapproved Apps, refer to Section 4.1 Common Configuration above for details of the use cases and configuration policies.

The Best scenario also uses the Conditional Access policies for iOS / iPadOS and Android mobile devices described in the Good Configuration Policies for iOS and iPadOS and Android Devices. Refer to Section 4.2.2.3 Conditional Access for the configuration details.

The Best configuration adds an additional use case where access to the Windows Virtual Desktop service is made from an unmanaged BYOD PC or Mac device.

Two conditional access policies are used to control access to the WVD service. Access to the virtual desktop device itself is allowed using a HTML5 compliant browser or client app is controlled with a conditional access policy which requires MFA, once the connection to the domain joined virtual desktop is established access to Office 365 services and the internet (Microsoft Edge, Outlook, Teams and other Office 365 client apps) is controlled using a conditional access policy that requires that the virtual desktop device is Hybrid Azure AD joined.

Table 31 details each use case, segregated by application / workload. The client type is broken into four scenarios:

1. Approved client app on iOS or Android, i.e. apps developed for the platform, e.g. Microsoft Outlook for Android and iOS/iPadOS, Microsoft Teams for Android and iOS/iPadOS, Office Apps for Android, and iOS/iPadOS.

2. Browser-based on PC or Mac, i.e. the web browser on the device, e.g. Microsoft Edge, Chrome, Safari to the Windows Virtual Desktop HTML5 web client.
3. Approved client app on PC or Mac, e.g. Windows Virtual Desktop client.
4. Access from Hybrid Azure Joined Windows Virtual Desktop device to Microsoft Outlook for PC or Mac, Microsoft Teams for PC or Mac, Office Apps for PC or Mac.

Table 31: Best configuration: Conditional Access use cases

| App/ workload | Use case/client | | Desired result |
|---|---|---|---|
| Windows Virtual Desktop (WVD) | Browser access to WVD | Unenrolled Mobile Device | Blocked |
| | | Unenrolled PC / Mac | Allow with MFA<br>Block access if Sign-in Risk is Medium or High |
| | Access via WVD client app | Unenrolled Mobile Device | Blocked |
| | | Unenrolled PC / Mac | Allow with MFA<br>Block access if Sign-in Risk is Medium or High |
| Internet Access | Browser access to Internet | Enrolled and compliant device | Allow with Hybrid Azure AD joined device |
| | | Unenrolled Mobile Device | Blocked |
| | | Unenrolled PC / Mac | Blocked |
| Exchange Online | Browser access to OWA | Enrolled and compliant device | Allow with Hybrid Azure AD joined device |
| | | Unenrolled Mobile Device | Blocked |
| | | Unenrolled PC / Mac | Blocked |
| | Access via Outlook Approved client app | Enrolled and compliant device | Allow with Hybrid Azure AD joined device |
| | | Unenrolled Mobile Device | Blocked |

| App/ workload | Use case/client | | Desired result |
|---|---|---|---|
| | | Unenrolled PC / Mac | Blocked |
| | Access via OS mail client | Enrolled and compliant device | Blocked |
| | | Unenrolled Mobile Device | Blocked |
| | | Unenrolled PC / Mac | Blocked |
| Teams and/or Skype for Business | Browser access to web apps | Enrolled and compliant device | Allow with Hybrid Azure AD joined device |
| | | Unenrolled Mobile Device | Blocked |
| | | Unenrolled PC / Mac Device | Blocked |
| | Approved client app | Enrolled and compliant device | Allow with Hybrid Azure AD joined device |
| | | Unenrolled Mobile Device | Blocked |
| | | Unenrolled PC / Mac Device | Blocked |
| OneDrive for Business | Browser access to web apps | Enrolled and compliant device | Allow with Hybrid Azure AD joined device |
| | | Unenrolled Mobile Device | Blocked |
| | | Unenrolled PC / Mac Device | Blocked |
| | OneDrive client app access | Managed desktop client | Blocked |
| | | Enrolled and compliant device | Allow with Hybrid Azure AD joined device |
| | | Unenrolled Mobile Device | Blocked |
| | | Unenrolled PC / Mac Device | Blocked |
| SharePoint Online | Browser access to web app | Enrolled and compliant device | Allow with Hybrid Azure AD joined device |

| App/ workload | Use case/client | | Desired result |
|---|---|---|---|
| | | Unenrolled Mobile Device | Blocked |
| | | Unenrolled PC / Mac Device | Blocked |
| | Approved client app (Word, Excel, PowerPoint) | Enrolled and compliant device | Allow with Hybrid Azure AD joined device |
| | | Unenrolled Mobile Device | Blocked |
| | | Unenrolled PC / Mac Device | Blocked |

## 4.4.2 Best Configuration Policies

### 4.4.2.1 Conditional Access

The following tables detail the Conditional Access policies required to achieve the desired results described in the preceding use cases for the Best configuration.

#### All Platforms - Block High or Medium Sign-in Risk

Table 32 (below) describes the Conditional Access policy to Block access to Office 365 applications and Bing from a PC or Mac and Mobile Devices (iOS, iPadOS and Android) when the user Sign-in Risk is High or Medium.

> **Important**
>
> The **Windows Virtual Desktop** and **Windows Virtual Desktop Client** apps have been added to the included Cloud Apps defined in the policy.

Table 32: BYOD – Best - Block access to Windows Virtual Desktop and Office 365 using Browser or Modern Apps with Sign-in Risk Medium and High on all platforms

| **BYOD-Best-Block access to Windows Virtual Desktop and Office 365 using Browser or Modern Apps with Sign-in Risk Medium and High on all platforms** | | | |
|---|---|---|---|
| Assignments | Users and groups | Include | **BYOD-Best-PC-Users–Enabled** |

| BYOD-Best-Block access to Windows Virtual Desktop and Office 365 using Browser or Modern Apps with Sign-in Risk Medium and High on all platforms | | | |
|---|---|---|---|
| | | Exclude | **BYOD-Good-PC-Users–Enabled**<br>**BYOD-Better-PC-Users–Enabled** |
| Cloud apps or actions | | Include | **Office 365 (Preview)**<br>**Microsoft Search in Bing**<br>**Windows Virtual Desktop**<br>**Windows Virtual Desktop Client** |
| | | Exclude | |
| Conditions | Sign-in Risk | | **High**<br>**Medium** |
| | Device Platforms | Include | |
| | | Exclude | |
| | Locations | Include | |
| | | Exclude | |
| | Client apps | Include | **Browser** |
| | | | **Mobile apps and desktop clients** |
| | | | **Modern Authentication clients** |
| | | | ~~Exchange ActiveSync clients~~ |
| | | | ~~Other clients~~ |
| | Device State | Include | |

| BYOD-Best-Block access to Windows Virtual Desktop and Office 365 using Browser or Modern Apps with Sign-in Risk Medium and High on all platforms | | | |
|---|---|---|---|
| | | | Exclude |
| Access controls | Grant | **Block Access** | |
| | | Grant Access | ~~Require multi-factor authentication~~ |
| | | | ~~Require device to be marked as compliant~~ |
| | | | ~~Require domain joined (Hybrid Azure AD)~~ |
| | | | ~~Require approved client app~~ |
| | | | ~~Require app protection policy~~ |
| | | For multiple controls | ~~Require one of the selected controls~~ |
| | | | ~~Require all the selected methods~~ |
| | Session | | ~~Use app enforced restrictions~~ |
| | | | ~~Use Conditional Access App Control~~<br>~~Use custom policy~~ |
| | | | ~~Sign-in frequency~~<br>~~1 Hour~~ |
| | | | ~~Persistent browser session~~ |
| Enable policy | | | **On** |

## PC or Mac Devices

Table 33(below) describes the Conditional Access policy to allow PC and Mac devices to connect to Windows Virtual Desktop service using either the Windows Virtual Desktop Client or HTML5 web browser client.

Table 33: BYOD – Best - Require MFA for Windows Virtual Desktop using Browser to Client App on PC or Mac

| **BYOD–BEST-Require MFA for Windows Virtual Desktop using Browser to Client App on PC or Mac** | | | |
|---|---|---|---|
| Assignments | Users and groups | Include | **BYOD-Best-PC-Users–Enabled** |
| | | Exclude | **BYOD-Good-PC-Users–Enabled**<br>**BYOD-Better-PC-Users–Enabled** |
| | Cloud apps or actions | Include | **Windows Virtual Desktop**<br>**Windows Virtual Desktop Client** |
| | | Exclude | |
| | Conditions | Sign-in Risk | |
| | | Device Platforms | Include | **Any Device** |
| | | | Exclude | **iOS**<br>**Android** |
| | | Locations | Include | |
| | | | Exclude | |
| | | Client apps | Include | **Browser** |
| | | | | **Mobile apps and desktop clients** |
| | | | | **Modern Authentication clients** |
| | | | | ~~Exchange ActiveSync clients~~ |
| | | | | ~~Other clients~~ |
| | | Device State | Include | |

| BYOD–BEST-Require MFA for Windows Virtual Desktop using Browser to Client App on PC or Mac | | | |
|---|---|---|---|
| | | | Exclude |
| Access controls | Grant | Block Access | |
| | | **Grant Access** | **Require multi-factor authentication** |
| | | | ~~Require device to be marked as compliant~~ |
| | | | ~~Require domain joined (Hybrid Azure AD)~~ |
| | | | ~~Require approved client app~~ |
| | | | ~~Require app protection policy~~ |
| | | For multiple controls | **Require one of the selected controls** |
| | | | ~~Require all the selected methods~~ |
| | Session | | ~~Use app enforced restrictions~~ |
| | | | ~~Use Conditional Access App Control~~ |
| | | | ~~Sign-in frequency~~ |
| | | | ~~Persistent browser session~~ |
| Enable policy | | | **On** |

## Windows Virtual Desktop domain joined devices.

Table 34 (below) describes the Conditional Access policy to allow WVD devices to connect to Office 365 applications and the internet by requiring "Require domain joined (Hybrid Azure AD)" condition to be satisfied.

Hybrid Azure AD join must be enabled in Azure AD Connect, please refer to the following articles Hybrid Azure AD join for Federated domains and Hybrid Azure AD join Managed domains. **Please note that this is not supported if using Azure AD Directory Services for WVD domain authentication.**

Table 34: BYOD – Best - Require Hybrid Azure AD joined device for WVD access to Office 365 on PC or Mac

| **BYOD–Best-Require Hybrid Azure AD joined device for WVD access to Office 365 on PC or Mac** | | | |
|---|---|---|---|
| Assignments | Users and groups | Include | **BYOD-Best-PC-Users–Enabled** |
| | | Exclude | **BYOD-Good-PC-Users–Enabled**<br>**BYOD-Better-PC-Users–Enabled** |
| | Cloud apps or actions | Include | **Office 365 (Preview)**<br>**Microsoft Search in Bing** |
| | | Exclude | |
| | Conditions | Sign-in Risk | |
| | | Device Platforms | Include | **Any Device** |
| | | | Exclude | **iOS**<br>**Android** |
| | | Locations | Include | |
| | | | Exclude | |
| | | Client apps | Include | ~~Browser~~ |
| | | | | **Mobile apps and desktop clients** |
| | | | | **Modern Authentication clients** |
| | | | | ~~Exchange ActiveSync clients~~ |
| | | | | ~~Other clients~~ |
| | | Device State | Include | |

| BYOD–Best-Require Hybrid Azure AD joined device for WVD access to Office 365 on PC or Mac | | | |
|---|---|---|---|
| | | | Exclude |
| Access controls | Grant | Block Access | |
| | | **Grant Access** | ~~Require multi-factor authentication~~ |
| | | | ~~Require device to be marked as compliant~~ |
| | | | **Require domain joined (Hybrid Azure AD)** |
| | | | ~~Require approved client app~~ |
| | | | ~~Require app protection policy~~ |
| | | For multiple controls | **Require one of the selected controls** |
| | | | ~~Require all the selected methods~~ |
| | Session | | **Use app enforced restrictions** |
| | | | ~~Use Conditional Access App Control~~ |
| | | | ~~Sign-in frequency~~ |
| | | | ~~Persistent browser session~~ |
| Enable policy | | | **On** |

### 4.4.2.2 Windows Virtual Desktop policies

Refer to https://docs.microsoft.com/en-us/azure/virtual-desktop/security-guide for recommended security configuration for Windows Virtual Desktop.

For the BYOD Blueprint the policy defined in RDP Session controls see the settings described in the following section.

## RDP Session Controls

Figure 9 (below) illustrates the recommended RDP settings for Windows Virtual Desktop sessions. They are designed to prevent users being able to copy data out of the desktop session and prevent printing.

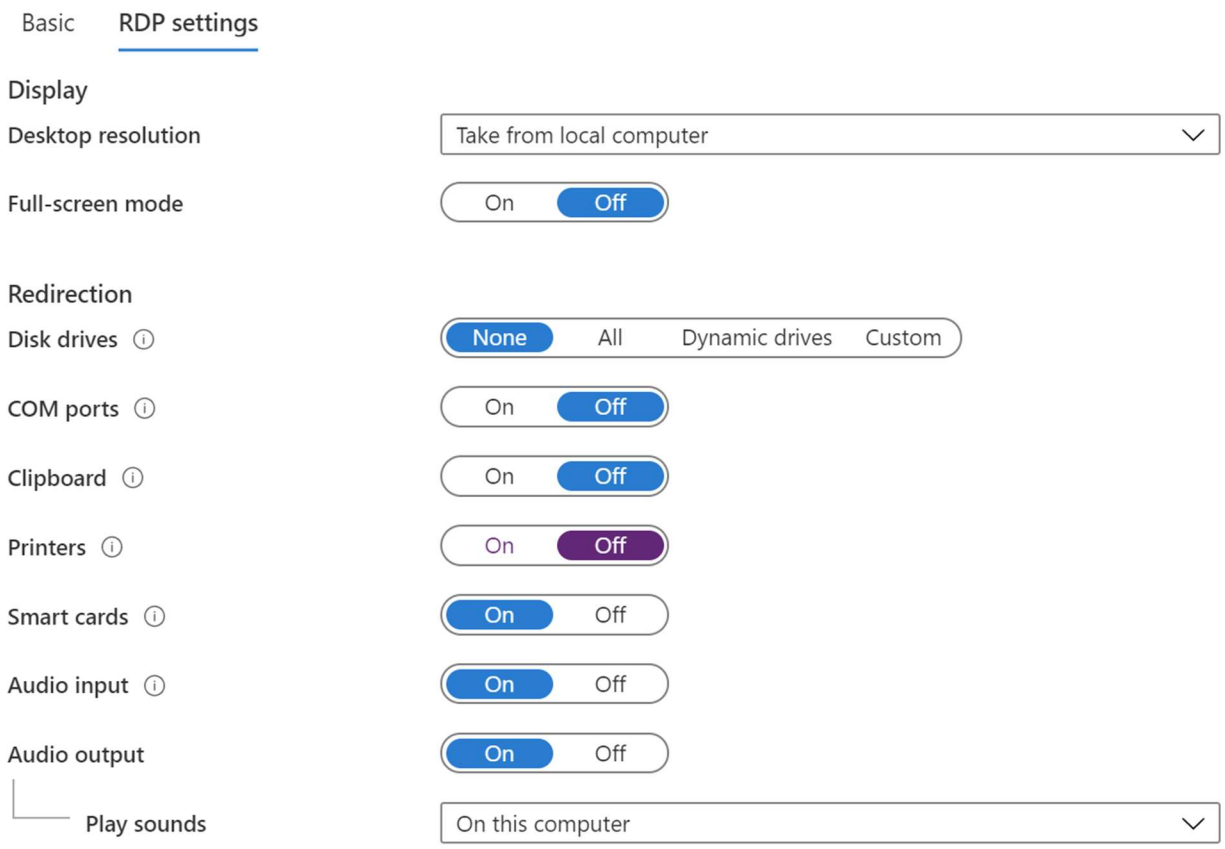



Figure 9: Windows Virtual Desktop RDP settings