Office 365

# Controlling Access to Office 365 and Protecting Content on Devices

Published: July 18, 2016

**Document Classification: Public**
**Document Location:** http://aka.ms/Office365CA
**Document Feedback:** cxprad@microsoft.com

# Introduction

The move to cloud services and an always increasing need for mobility are driving organizations to look for solutions that protect data while enhancing user productivity and device flexibility. Organizations require the ability to control user access to online services based on a variety factors such as device compliance or network location, and to better protect content that is accessed from these devices.

This document describes the Conditional Access (CA) features in Microsoft Office 365 and Microsoft Enterprise Mobility + Security (EMS)[1], and how they are designed with built-in data security and protection to keep company data safe, while empowering users to be productive on the devices they love. It also provides guidance on how to address common concerns around data access and data protection using Office 365 features.

With Office 365 and EMS, customers can meet their user productivity and device flexibility requirements, while keeping their data secured. Access to company data stored in Office 365 can be restricted to corporate computers and mobile devices that meet configurable security standards. Even when accessed from personal mobile devices such as mobile phones and tablets, customer data remains protected.

# Terminology

The features and products referenced in this document are described below.

| Feature / Product | Description |
|---|---|
| Active Directory Federated Services (AD FS) | On-premises security token service (STS) that provides simplified, secure identity federation and Web single sign-on (SSO) capabilities for users who want to access applications within an AD FS-secured enterprise, in federation partner organizations, or in the cloud. Federated identities with Modern Authentication-enabled clients interoperate with EvoSTS, which is the Azure AD STS.<br>AD FS indirectly supports CA scenarios, as it offers a set of controls known as client access filtering that allow the creation of perimeter network-based policies for IP range filtering, accessed workload, or client type (browser vs rich client). |
| Multi-Factor Authentication (MFA) | Protects access to data and applications by requiring a second form of authentication. Strong authentication is available through a range of verification options. |
| Azure Active Directory Premium | All CA scenarios that leverage Azure AD require Azure AD Premium. Azure AD Premium adds feature-rich enterprise-level identity management capabilities and enables hybrid users to seamlessly access on-premises and cloud capabilities. It includes everything you need for information worker and identity administrators in hybrid environments across application access, self-service identity and access management, identity protection and security in the cloud. |
| Azure Rights Management Services (RMS) | Uses encryption, identity, and authorization policies to protect files and email. Information protection that is applied by using Azure RMS stays with the files and emails independently of the location, allowing customers to remain in control of their data even when this data is in motion. |
| Conditional Access (CA) | CA allows customers to selectively allow or disallow access to Office 365 based on attributes such as device enrollment, network location, group membership, etc.<br>• Device-based CA restricts access to devices that are managed by the organization and are in a healthy state. Device-based CA is a feature of Intune. Users must enroll their devices in Intune and validate that the device meets the organization's access rules regarding device health and security. |

[1] Formerly, Microsoft Enterprise Mobility Suite.

| Feature / Product | Description |
|---|---|
| | • There are other CA scenarios that do not require device enrollment, such as restrict access only from specific locations. These scenarios do not require Intune and are provided through Azure AD Premium access control features. |
| **Data Loss Prevention (DLP)** | Helps identify and monitor sensitive information, such as private identification numbers, credit card numbers, or standard forms used in your organization. DLP Policies enable you to notify users that they are sending sensitive information and to block the transmission of sensitive information. |
| **Microsoft Enterprise Mobility + Security (EMS)** | Provides identity and access management, MDM, MAM and Azure RMS. Intune is a part of EMS. |
| **Microsoft Intune (Intune)** | Intune is a cloud-based service that helps you manage Windows PCs, and iOS, Android, and Windows mobile devices. Intune also helps protect corporate applications and data. You can use Intune alone or you can integrate it with Microsoft System Center Configuration Manager 2012 R2 to extend your management capabilities. |
| **Mobile Application Management (MAM)** | Controls how corporate-managed applications work and interact with other managed applications and unmanaged applications (e.g., provides the ability to restrict user actions such as copy, paste, download, etc.). Available through Intune. |
| **Mobile Device Management (MDM)** | Provides the ability to configure mobile device policies, such as enforcing complex PINs or passwords, blocking devices that have been jail broken or rooted from syncing email, disabling Bluetooth, etc. Available through Office 365 MDM and Intune. |
| **Modern Authentication** | Provides OAuth-based authentication for Office clients against Office 365 using Active Directory Authentication Library (ADAL). Replaces the Microsoft Office Sign-In Assistant. Allows for CA policies, so administrators can define granular applications and device-based controls for corporate resources. |

*Table 1 - Features and Products referenced in this document*

# Customer Scenarios

Customer scenarios for CA vary. This document discusses the scenarios listed below. This is not a complete list; rather, these are the scenarios about which Microsoft is most commonly asked.

- Access control
  - Access to Office 365 must be permitted only from policy-compliant mobile devices
  - Access to Office 365 must be permitted only from corporate computers
  - Access to Office 365 must be permitted only from within the company network
  - Access to Office 365 must be permitted only for users who have successfully signed up with multi-factor authentication
- Data protection
  - Corporate data on user devices must be protected in case of device theft or loss
  - Corporate data on user devices must be protected against theft of account credentials
  - Users must be prevented from storing company data in untrusted locations
  - Users must be prevented from sharing sensitive data with unauthorized parties

# Key Concepts

To understand the solutions for the above scenarios, it is important to be familiar with Microsoft EMS, Office 365 MDM, Intune MDM, CA policies, and MAM. For an overview of security architecture for Office 365 and managed apps, see Architecture guidance for protecting company email and documents.

## Microsoft Enterprise Mobility + Security

EMS is a Microsoft cloud solution that provides identity and access management for mobile devices. Many scenarios discussed in this document require EMS, which includes the following services:

- Microsoft Azure AD Premium (for hybrid identity management)
- Microsoft Intune (for mobile device and application management)
- Microsoft Azure RMS (for information protection)

While customers can purchase each of the above services individually (based on their requirements), it is usually more cost-effective to purchase EMS. For more information, visit the Microsoft Enterprise Mobility + Security Web site.

## Office 365 Mobile Device Management

Office 365 includes native MDM capabilities with commercial subscriptions. MDM helps organizations manage their mobile device security and control access to Office 365 data across a diverse range of mobile phones and tablets.

With Office 365 MDM, organizations can restrict access to Exchange Online and SharePoint Online to mobile devices that are both managed and compliant with security policies:

- **Managed** A device is considered managed once it is enrolled in Office 365 MDM.
- **Compliant** A device is considered compliant when it meets the criteria defined in the MDM policy. A policy may enforce a PIN, a minimum PIN length, data encryption, prevent cloud backups, screen captures, photo synchronizations, etc.

Once policies are configured and scoped to users, devices that are not enrolled or are not policy-compliant will not be authorized or able to access Office 365 email and documents.

When trying to access Exchange Online or SharePoint Online data from an unregistered mobile device, users will be prompted to enroll their mobile devices to be granted access by installing and signing in to the Intune Company Portal app.

Throughout this process, compliance policies will be enforced on the device. Compliance policies help organizations keep data safe on mobile devices. Such policies may include:

- Enforcing use of PIN or passwords on the device
- Enforcing device encryption
- Preventing access from jail broken or rooted devices

With these policies in place, even if a device is lost or stolen, data on the device remains protected. In addition, company data can be wiped from the device—either locally (when too many incorrect PINs are entered), or remotely (as initiated by the user or administrator).

> **Note** Policies and access rules created through Intune or Office 365 MDM override Exchange ActiveSync mobile device mailbox policies and device access rules created in the Exchange admin center.

With Office 365 MDM, organizations can apply security policies to user mobile devices, manage access to corporate resources, and perform a selective wipe of Office 365 data from mobile devices. These capabilities are powered by Microsoft Intune. Office 365 MDM features are described in Capabilities of built-in Mobile Device Management for Office 365.

## Intune Mobile Device Management

Intune MDM provides all of the features available in Office 365 MDM, along with some extra features. Organizations that require advanced controls can purchase an Intune subscription, either in standalone form or as part of EMS.

> **Note** As customers use Office 365 and start shaping their data access and security requirements, they will need to determine whether the native Office 365 MDM capabilities are sufficient for their needs, or whether they require a more advanced solution. Customers can start with Office 365 MDM and upgrade to Intune MDM later.

From an MDM standpoint, Office 365 MDM provides standard features that will suit most organizations. Specifically, a subscription to Microsoft Intune is optional if all of the customer's devices are managed and domain-joined. However, Intune is required to manage PCs in addition to mobile devices, manage application security through MAM, or provide more granular control on CA policies.

For more information on Intune MDM, see Introduction to Intune. For a comparison of mobile security options, see What to know before you start Microsoft Intune.

## Conditional Access Policies

With CA policies, customers can control access to Office 365, based on various attributes such as group membership, authentication strength, device registration, device compliance, client platform, network location, and more. CA policies are configured per application, allowing customers to enforce different access rules for separate applications. They can also be scoped to specific groups or users.

It is important to understand that access controls are managed at multiple layers today (both of which require Azure AD Premium):

- **Intune Device-based Conditional Access** Allows customers to restrict access from devices that are either managed by Intune and compliant with security policies, or are domain-joined. Device-based CA is managed through the Intune Management Portal.
- **Azure Access Control** Allows customers to restrict access based on other attributes such as IP location, or whether the user signed in with MFA. Azure Access Control is managed through the Azure Management Portal.

The following table provides a high-level summary of the features, scope, and licensing requirements:

| Feature | Access conditions | Office 365 services in scope | Client platforms in scope | Licensing requirements |
|---|---|---|---|---|
| **Device-based CA (Intune)** | Restrict access to **managed** and **compliant** devices, or domain-joined devices. | Exchange Online<br>SharePoint Online<br>OneDrive for Business<br>Skype for Business | iOS<br>Android<br>Windows 8.1<br>ActiveSync<br>Web client | Basic features available with Office 365 MDM; Intune or EMS required for advanced features |

| Feature | Access conditions | Office 365 services in scope | Client platforms in scope | Licensing requirements |
|---|---|---|---|---|
| **Azure Access Control** | Require MFA,<br>Require MFA when not at work,<br>Block access when not at work | Exchange Online<br>SharePoint Online<br>OneDrive for Business<br>Skype for Business<br>Yammer Enterprise | All[2]<br>(not scoped by platform) | Requires Azure AD Premium or EMS |

*Table 2 - Conditional access management summary*

For services or platforms that are not explicitly listed in scope in the above table, CA is not available and cannot be configured. For example:

CA supports several scenarios such as (not a complete list):

- Allowing access to Exchange Online only from managed and compliant mobile devices
- Allowing access to SharePoint Online only from domain-joined PCs

CA does not support some scenarios such as (not a complete list):

- Allowing access to Yammer Enterprise, Sway, Delve, etc., only from managed and compliant mobile devices
- Allowing access to Exchange Online or SharePoint Online only from managed Mac OS devices

In addition to CA, organizations using a federated identity model with Office 365 may also configure AD FS rules to further control access. This is outside of the scope of this document, but for more information, see Limiting Access to Office 365 Services Based on the Location of the Client.

## Intune Mobile Application Management

Intune MAM provides application-level management for organizations seeking more protection for corporate data. MAM helps organizations who use the same devices and applications for both work and personal use. Users want to be able to access both their company and personal data from the same device, but organizations need to prevent users from transferring company data to personal applications or to personal data storage locations, such as personal e-mail, third-party cloud solutions, or locally on the device. For example, Intune MAM policies can dictate that data copied from a managed application (e.g., Outlook) can only be copied to another managed application (e.g., Word), but cannot be copied to an unmanaged application.

Some applications, such as Outlook, can be configured to access both company and personal resources. With the MAM multi-identity management feature, users are able to access both their personal and work email accounts in the same application, but with MAM applied only to their company account. For example, Intune MAM settings can dictate that corporate data can only be shared within the corporate identity boundaries (e.g., within a single corporate email profile, or within OneDrive for Business and SharePoint Online locations), but may not be transferred to other mailboxes or data storage locations, even within the same application (e.g., Outlook or OneDrive for Business). At the same time, users are permitted to access their personal email or documents on their device without IT controls, providing an optimal user experience.

[2] Requires clients that support Modern Authentication. For more information, see How modern authentication works for Office 2013 and Office 2016 client apps.

With Intune, organizations can protect against data leakage through MAM, with or without a MDM solution (MAM without enrollment or device management).

With MAM policies, organizations can both protect access to company data and control how data is used on the user device, by enforcing policies such as:

- Requiring a PIN to open an application
- Preventing actions such as copy from or paste to unmanaged applications
- Preventing the storage of company data to personal or other non-corporate locations

While MAM can be used without MDM, there are benefits to using MDM with MAM policies, and companies can use both MAM with and without MDM at the same time. For example, an employee can use a company-issued phone as well as a personal tablet. In this case, the company phone is enrolled in MDM and protected by MAM policies, while the personal device is not enrolled in MDM and protected by MAM policies only.

For organizations that want to keep company data in control, but do not want to enroll and manage their users' devices, Intune MAM is a great solution to the challenges of "bring your own device" (BYOD). Intune MAM is also an effective solution for organizations that have already deployed a third-party MDM solution and want greater control of their company data.

Intune MAM provides many advanced features designed for data protection, including the ability to:

- Protect company data in mobile apps without requiring IT to enroll and manage a user's entire device. The user only has to use their corporate credentials to authenticate to the app and then data loss protection capabilities are automatically set up.
- Isolate corporate and personal data within the same application—something as of this writing no other solution provides.

For more information about these features, see Announcing New Microsoft Enterprise Mobility Capabilities.

With MAM policies in place, data remains protected on user devices:

- Only devices that meet compliance policies will be able to access data from the service
- Company data remains isolated from personal data
- Restrictions apply that prevent transfer of company data from managed applications
- Company data can be wiped from a device in case of device loss or theft, or in case the employee leaves the company

MAM policies allow organizations to customize settings to achieve the protection level that meets the organization's needs with respect to:

- **Data relocation** Prevent corporate application data from being transferred to personal apps and locations, including backup, copy and paste, and sharing data to other apps or cloud services.
- **Application access** Require a PIN or corporate credentials to be entered when the user is accessing corporate content. Prevent access from a jail broken or rooted device.
- **Encryption** Encrypt corporate application data on the device.

- **Screenshots** Prevent user from taking screenshots while in the application on Android. In iOS, this can be configured via Intune device policies.

For more information on Intune MAM, see Protect app data using mobile app management policies with Microsoft Intune.

# Addressing Common Mobility Concerns

This section uses scenarios to illustrate how to address common security concerns associated with user mobility.

## Scenario: Restrict Access to Managed Devices with Office 365 MDM or Intune MDM

Organizations want their users to remain productive from anywhere using their mobile devices, while retaining control of corporate data. Ensuring that data is safe on mobile devices is a common customer concern. To meet this challenge, Microsoft provides the following options that may be used together or independently:

- Restricting access from managed devices with Office 365 MDM or Intune MDM
- Preventing data leakage with MAM

### Deployment considerations for Office 365 MDM

This scenario can be achieved using Office 365 MDM. The deployment steps involve:

- Activation and set up of Office 365 MDM
- Creation of security policies
- Application of security policies to user groups

To support this scenario, the customer must:

- Run Windows Phone 8.1, iOS 7.1, Android 4.0, or later versions of these operating systems; and
- Use the Company Portal application to enroll devices into Intune. Other enrollment methods such as the iOS Device Enrollment Program (DEP) and the Apple Configurator tool are not supported.

For more information on the end-user enrollment process, see What to tell your users about using Microsoft Intune. For more information on how to create and deploy Office 365 MDM policies, see Create and deploy device security policies.

> **Note** Access control may be provided through Office 365 MDM as discussed above, or through Intune. Customers that have purchased Intune should use the Intune Management Portal to configure MDM and CA policies, instead of using Office 365 security policies.

### Deployment Considerations for Intune MAM

You can use Intune MAM to prevent data leakage. Unlike other Intune policies, MAM policies are not deployed directly to users and devices. Instead, policies must be associated with applications. The settings take effect when application is deployed and installed.

MAM policies can be applied to:

- Applications with built-in support for MAM. Supported applications include Microsoft Excel, OneNote, PowerPoint, Power BI, Word, Skype for Business, OneDrive for Business, and more. To see the complete list, visit the Microsoft Intune mobile application gallery.
- In-house applications that can be repackaged by organizations using the Microsoft Intune App Wrapping tool.

To support this scenario, the customer must:

- Use devices running iOS 8.1, Android 4.0, or later versions of these operating systems
- Purchase Intune licenses for their users, either in standalone form or as part of EMS

For more information, see Configure and deploy mobile application management policies in the Microsoft Intune console.

## Scenario: Managing Data Access and Data Protection on Desktop Computers

Most organizations expect their users to be able to access corporate data from their corporate-issued desktop or laptop computers at any time and from any location, as long as user credentials are valid and the device remains trusted. At the same time, these organizations may want to prevent access from untrusted computers, even if valid user credentials are used, to protect against scenarios such as access from unprotected computers (kiosk PCs, shared family PCs, etc.) and the use of compromised credentials from unknown computers.

By default, any user withy valid credentials can access Office 365 from any computer. Microsoft Intune provides CA policies that enable customers to restrict access to Exchange Online, SharePoint Online, and Skype for Business from computers that are either domain-joined to the customer's on-premises Active Directory or enrolled in Intune and compliant with policies:

- **Domain-joined** Corporate computers are typically domain-joined and organizations want their users to be able to access corporate data from these computers at any time and from any location. This is provided that user credentials are verified and that the security posture of the user and their device is unchanged.
- **Enrolled and compliant** Computers that are not domain-joined can be enrolled with Intune. Upon enrollment, device policies are enforced on the computer.

Domain-joined computers do not need to enroll in Intune, but must be registered in Azure AD. Computers that are not domain-joined, or that do not meet compliance policies after enrollment, will be denied access to services configured in the scope of the CA policies.

> **Note** Currently, CA policies cannot be configured to only allow access from computers that are domain-joined, while denying access from computers that are not domain-joined, but enrolled and compliant.

Currently, CA policies are not available for Mac computers. Customers using Mac computers have the following options:

- Configure CA to apply to Windows computers only (and optionally to mobile devices). In this case, CA policies will not apply to computers running Mac OS. Mac OS users will be able to access Office 365 services, whether or not their computer is managed and compliant with Intune policies.

- Configure CA to apply to all device types. In this case, access to services in scope from Mac OS devices will be blocked. If necessary, organizations can exclude Mac OS users from CA policies.

## Scenario: Protecting Data Stored Locally on Computers

Corporate computers often store data locally. This can be a combination of content stored by the user, such as cached Outlook data, or synchronized OneDrive for Business or SharePoint Online content.

For domain-joined computers, locally-stored data can be protected through policies enforced by the customer at the Active Directory domain level, which include at minimum:

- Complex password requirements to protect against unauthorized access to local data
- Antivirus and antimalware software to protect against malicious software
- Patch management to ensure security updates are applied promptly
- BitLocker enforcement to protect operating system drives and fixed data drives

For Windows 8.1 and later computers that are enrolled in Intune (whether they are domain-joined or not), locally-stored data may be protected through Intune PC management functionalities (patch management, antivirus and antimalware protection, Windows Firewall settings, etc.), as well as compliance policies.

Compliance policies must include:

- Enforcement of password type, length, and complexity
- Enforcement of device encryption
- Enforcement of automatic updates

**Note** Compliance policies are only applicable to devices that are MDM-enrolled with Intune. They cannot be enforced on Windows 7 PCs (since they cannot be enrolled), or on devices not enrolled in Azure AD (even if they are registered or domain-joined).

Intune MDM also supports the management of Mac OS X 10.9 or later devices with compliance policies. For more information, see Introducing Intune support for Mac OS X management.

For a complete list of policies that may be applied to computers, see:

- Windows policy settings in Microsoft Intune (Windows 8 and 8.1)
- Windows 10 policy settings in Microsoft Intune
- Mac OS X configuration policy settings in Microsoft Intune

## Deployment Considerations for CA policies on Windows computers

For this scenario, the following requirements apply:

- Microsoft Intune must be purchased for all users, in standalone form or as part of EMS
- Windows 7.0 or later is required on all computers
    - Windows 7.0 or later is required to allow Azure AD Device Registration
    - Windows 8.1 or later is required to enforce compliance policies

- Users must run Office 2013 or Office 2016 with the latest updates[3]
- The Office 365 tenant must be enabled for Modern Authentication[4]
- Domain-joined PCs must be registered with Azure AD. The device's identity and attributes are used to enforce CA policies. Azure AD Device Registration can be achieved silently in the background. For information about how to register Windows clients through the Azure AD device registration service, see: Get started with Azure Active Directory Device Registration.

It is also recommended that AD FS be deployed for this scenario. This is required to support automatic registration of domain-joined computers in Azure AD and to block non-Modern Authentication protocols. To configure AD FS, follow the instructions in *Scenario 3: Block all access to Office 365 except browser-based applications* in the Enabling Client Access Policy section of Configuring Client Access Policies.

Once corporate computers are successfully registered with Azure AD, CA policies can be configured to control access to Office 365. For information about creating policies in Intune, see Manage settings and features on your devices with Microsoft Intune policies.

> **Note** Currently, CA policies only apply to Modern Authentication rich clients. Preventing access from non-Modern Authentication clients must be addressed through AD FS configuration. Preventing access from Web browsers from Windows computers is currently in preview.

## Scenario: Restricting Access through Web Browsers

Conditional Access policies are available to protect Exchange Online and SharePoint Online content accessed from Web browsers on iOS and Android. When configured, users who try to sign in to Outlook on the web and SharePoint Online sites from unregistered iOS and Android devices will be prompted to enroll their device with Intune and to fix any non-compliance issues before they can complete sign-in.

## Scenario: Restricting Access to Company Data from Untrusted Networks

Many large companies expect to prevent access to Office 365 from networks outside their perimeter for all services or for a subset of clients only. For example, some customers want to prevent access to Office 365 from rich clients only, or from clients on external networks, while allowing browser access.

Therefore, some customers implement client access policies at the AD FS level to implement common scenarios, such as:

- Blocking all external access to Office 365
- Blocking all external access to Office 365, except Exchange ActiveSync
- Blocking all external access to Office 365, except browser-based applications
- Blocking all external access to Office 365, except for designated Active Directory groups

[3] Once CA policies are enforced, only rich clients that are enabled for Modern Authentication will be able to access Office 365 content. For Office 2013, registry keys must be set to enable Modern Authentication. For more information, see Enable Modern Authentication for Office 2013 on Windows devices. For more information on Modern Authentication clients, see How modern authentication works for Office 2013 and Office 2016 client apps and Office 2013 and Office 365 ProPlus modern authentication and client access filtering policies: Things to know before onboarding.

[4] Modern Authentication for Exchange Online and Skype for Business can be enabled using remote PowerShell. No action is required for SharePoint Online.

> **Note** Blocking all external access to Office 365, except browser-based applications, cannot be done using AD FS rules for customers that have enabled Modern Authentication on their tenant because rich clients (Outlook and other Office apps) bypass the client-access-filtering policies. For more information, see Office 2013 and Office 365 ProPlus modern authentication and client access filtering policies: Things to know before onboarding.

As an alternative to client access policies, consider using the following options:

- Location-based CA using Azure AD access rules to prevent access to Office 365 from external networks
    - This policy can be scoped to specific users or groups
    - This policy will apply to Web clients and Modern Authentication rich clients
    - This policy will apply to all devices, regardless of their registration or compliance status
- Device-based CA using Microsoft Intune or Office 365 MDM to allow only trusted devices to access Office 365 independently from their network location, and to enforce device compliance

Many customers block external access to Office 365 to reduce the risk of data leakage from external clients such as kiosk devices or home PCs that are not appropriately protected and therefore constitute a security risk. Microsoft recommends that customers manage access to Office 365 through MDM and device-based CA, rather than through location-based access rules. This is a better solution because:

- Client access policies apply to all devices, including devices that are corporate-owned and domain-joined, unnecessarily requiring users on corporate devices to use VPN or other similar measures to access data when outside of work. In this case, preventing access based on network location is a technical choice rather than a strategic security decision.
- CA offers centralized management, more granularity, and better reporting for access control.

### Deployment Considerations for Location-based Access Control

For customers that choose to implement location-based access control, Azure AD Premium must be purchased for all users, in standalone form or as part of EMS. Location-based access control is configured using the Azure Management Portal. It must be configured separately for each Office 365 service (e.g., Exchange Online, SharePoint Online, Skype for Business, Yammer Enterprise, etc.).

It is important to note that access control policies apply only to clients that are enabled for Modern Authentication. Other rich clients that are not affected by these policies can be blocked through AD FS claim-based rules. This is achieved by following instructions in *Scenario 3: Block all access to Office 365 except browser-based applications* in the Enabling Client Access Policy section of Configuring Client Access Policies.

## Scenario: Restricting Access Based on Other Business Criteria

Some organizations in retail and other sectors have requirements to restrict hourly workers or vendors from logging into corporate resources based on criteria such as time, group membership, etc.

To restrict access based on the time of day for a user with federated credentials, the tenant admin can define login hour policies on the user's AD account. However, note that login restrictions are enforced only at the time of authentication; they do not revoke an existing session once it falls outside the defined login hour policy.[5] This can be addressed by limiting the session token lifetime so that the client will need to refresh the token on a more frequent basis.

To restrict access based on group membership, some customers may require enforcing restrictions for vendor access to Office 365. To achieve this requirement, the vendor accounts can be placed in specific AD groups that prevent access from external networks or enforce other restrictions through either AD FS claim-based rules or CA policies.

## Scenario: Protecting Data in Motion

On personal computers running Windows or Mac OS, users typically have full control over corporate content they are authorized to access once the content is downloaded locally. Therefore, users can compromise data safety by sharing sensitive documents via email or by storing information in unsafe locations, such as personal cloud storage or unencrypted USB devices.

Office 365 and Azure include features that provide solutions to protect content on corporate computers and to prevent data leakage, even when accessed from a trusted user on a trusted device. These features are Azure RMS and DLP, and these solutions also apply to mobile devices, and can be combined with other mobile data safety solutions, such as MAM, to provide additional security.

To use Azure RMS, customers must purchase it, either in standalone form or as part of EMS. With Azure RMS, customers can apply persistent protection to content. Content protection remains with the data, even when the data is saved to an unsecure location or sent by email. Protection can be applied to any data type providing different levels of access (e.g., read, edit, print, etc.). Through encryption, identity, and authorization policies, customers can ensure that only authorized parties can access the content. In addition, auditing features allow the customer to control whether protected content was accessed and when, and whether unauthorized people attempted to access the content. For more information on using Azure RMS with Office 365, see How applications support Azure Rights Management.

Office 365 provides DLP features for Exchange Online and SharePoint Online, which enable customers to protect sensitive information whether in email, a document library, a OneDrive for Business folder, or an actual Office file itself. DLP features help enforce compliance policies by detecting and protecting sensitive data in real time. Organizations can define policies to detect sensitive information based on a custom set of rules, and to take appropriate actions, such as:

- **Notifying the user** Organizations can empower their users to make the right choice by informing users that they may be about to violate one of the configured policies. This is achieved by configuring Policy Tips that will inform the user about the possible policy breach.
- **Preventing the data from being transmitted** DLP can also prevent data from being transmitted over email or shared with unauthorized parties. Organizations can set up rules allowing users to override policies by providing a business justification, which allows users to be productive while still being compliant.
- **Reporting** Administrators can track how effective policies are with the reporting features built into Office 365, and create admin-facing incident reports with information about each incident that can later be reviewed by their security teams.

[5] For more information, see Session timeouts for Office 365.

For more information, see Data Loss Prevention and Find sensitive data stored in SharePoint Online sites.

## Scenario: Protecting Against Compromised Credentials

Usernames and passwords can be compromised in a variety of ways including through malware, keystroke loggers, phishing attacks, and others. Microsoft has services like Exchange Online Advanced Threat Protection that protect against the attacks themselves, as well as provide solutions to mitigate the organizational risk resulting from an attack.

These solutions include:

- Enabling MFA
- Implementing polices to prevent access from external networks (discussed earlier)

MFA for Office 365 mitigates risks by providing an extra authentication layer in addition to user credentials, which ensures that compromised credentials do not gain access to Office 365. Users enabled with MFA are prompted to acknowledge a phone call or text message after entering their credentials. MFA is included at no additional charge with most Office 365 subscriptions.

In an event where credentials are compromised, whether by interception, malware, etc., an attacker is unable to use these credentials to access Office 365. Customers may also leverage an existing on-premises MFA solution to protect access to Office 365. For more information about enabling MFA for Office 365, see Set up multi-factor authentication for Office 365 users.

Customers can also elect to prevent the transmission of usernames and passwords with basic authentication by enabling Modern Authentication. Office 2013 and 2016 client applications can use the ADAL to engage in browser-based authentication. This transition enforces claim-based authentication, which reduces the risk of credentials being compromised and enables enhanced features such as smart card and MFA.

### Deployment considerations for MFA-based Access Control

For this scenario, Azure AD Premium must be purchased for all users, in standalone form or as part of EMS. MFA-based access control is configured using the Azure Management Portal. It must be enabled separately for each application.

## Scenario: Detecting and Handling Compromised User Accounts

Multiple solutions are available to customers, to help detect and handle security events associated with compromised user accounts, including:

- Audit Logging   Office 365 natively provides reporting solutions, such as the audit log search tool and Azure AD access and usage reports in the Security & Compliance Center, to give visibility into the security of an organization's directory. Anomaly reports show sign-in events that were detected to be suspicious based on various criteria such as sign ins from multiple geographies, multiple sign-in failures, or sign ins from unknown sources.
- Anomalous Activity   By subscribing to Azure AD Premium, tenant admins can also be notified when the service detects other anomalous activity based on machine learning algorithms.
- Azure Active Directory Identity Protection   A security service that provides a consolidated view into risk events and potential vulnerabilities affecting your organization’s identities. Microsoft

has been securing cloud-based identities for over two decades, and with Azure AD Identity Protection, Microsoft is making these same protection systems available to enterprise customers. Azure AD Identity Protection leverages existing Azure AD's anomaly detection capabilities, and introduces new risk event types that can detect anomalies in real-time and block or secure risky user accounts.

- Office 365 Management Activity API   For customers who require more advanced solutions and are also ready to purchase third-party solutions or develop custom solutions, the Office 365 Management Activity API provides the ability to aggregate actions and events from Azure AD. Organizations can import this content into a security incident event management tool for custom analysis and correlation.

For additional information about the audit and reporting features in Office 365, see Auditing and Reporting in Office 365.

If an account is detected to be compromised, the tenant admin must take several actions to limit the potential damage as a result. Changing the user's password will immediately invalidate the access token for the session and terminate any existing sessions to force the user to re-authenticate. The account may also be disabled to prevent any new sessions.

### Scenario: Dealing with a Lost or Stolen Device

With increasing BYOD trends and more employees conducting business on personal devices, device theft exposes company-owned data to risk of being compromised. Native Office 365 MDM features can help secure data on stolen devices. When a device is compromised, Office 365 admins, or the affected user, can initiate a selective wipe of data owned by the organization. Further, mobile device policies can be created that automatically take effect when a device is suspected to be lost or stolen. For example, tenant admins can define policies that lock devices after a certain time of inactivity or locally wipe the device when an incorrect password is tried over a set amount of times in sequence.

## Summary

Organizations require the ability to control user access to online services based on a variety factors such as device compliance or network location, and to better protect content that is accessed from mobile devices. Office 365 includes native MDM capabilities which help organizations manage mobile device security and control access to Office 365 data across a diverse range of mobile phones and tablets. Access to company data stored in Office 365 can be restricted to corporate computers and mobile devices that meet configurable security standards. Even when accessed from personal mobile devices such as mobile phones and tablets, data remains protected.

With Office 365 and EMS, customers can meet their user productivity and device flexibility requirements, while keeping their data secure. In addition, with CA policies, customers can control access to Office 365, based on various attributes such as group membership, authentication strength, device registration, device compliance, client platform, network location, etc. CA policies are configured per application, allowing customers to enforce different access rules for separate applications. They can also be scoped to specific groups or users.

# Frequently Asked Questions

1. What is the difference between a domain-joined device and a compliant device?

   In the context of CA, computers must be either domain-joined or compliant to be allowed access to services:

   - A domain-joined device is joined to an on-premises Active Directory. It can optionally be registered with Azure AD, for customers who want to support CA on Windows, or managed with Intune for customers who want to manage their computers using Intune.
   - A device is compliant when it is registered in Azure AD and meets all device-based compliance rules that were defined by the administrator. It can optionally be domain-joined or managed with Intune.

2. If a customer has a hybrid environment, can CA apply to both on-premises and cloud environments?

   A hybrid environment allows an on-premises environment to work seamlessly with a cloud environment. In Office 365, all plans that support Azure AD sync can deploy a hybrid environment.

   In addition to supporting Office 365, CA policies can apply to on-premises Exchange servers. To learn more about CA support in Exchange Server on-premises, see The New and Improved Quarantine Experience in Conditional Access for On-Premises Exchange using Microsoft Intune.

3. Can a customer switch from Office 365 MDM to Intune?

   Yes. After acquiring Intune, administrators can switch MDM capabilities to Intune by resetting the MDM Authority from Office 365 MDM to Intune. Mobile devices already enrolled in Office 365 MDM will have to be re-enrolled in Intune. For more information, see Enroll devices for management in Intune.

4. What is MAM without enrollment?

   MAM without enrollment allows you to protect company data at the application level with MAM, without enrolling a device in Intune MDM. Reasons to choose MAM without enrollment include:

   - Users do not want to enroll personal devices and want complete control over their devices
   - You want to move from your current MDM provider to Intune, but need MAM now
   - You have a third-party MDM provider and you want to add MAM capabilities

   A list of applications that include Intune MAM functionality can be found in the Microsoft Intune mobile application gallery.

5. When are CA policies applied?

   CA policies are enforced each time the user is required to authenticate to the application. How often that occurs is governed by the access and refresh token lifetimes for the OAuth protocol:

   - An access token is attached on request to server resources and is valid for one hour
   - A refresh token is used to request a new access token and is valid for 14 days by default and up to 90 days with continuous use

- Refresh tokens are invalidated when user changes password
- Administrators cannot customize token lifetimes, and device IP changes currently have no effect on refresh token lifetime
- A user is not required to authenticate again if authentication was previously successful with another Office application on the same device and has a valid access token

In practices, this means that:

- CA policies are evaluated at a minimum every hour
- When the CA policy governing an application changes, the automatic renewal of an access token by refresh token will fail and the user will be required to re-authenticate.

6. Can an organization control the enrollment of devices and what types can be enrolled?

   Organizations can control how many devices a user may enroll, and the minimum operating system required for enrollment. There is no way to restrict enrollment to specific devices, (e.g., block all tablets but allow mobile phones). Office 365 also does not recognize whether a device is personal or corporate-owned. For more information, see Set up Mobile Device Management (MDM) in Office 365.

7. What is the difference between Remote Wipe and Local Wipe?

   A Remote Wipe allows a customer to erase data from a device remotely (through the cloud) without having physical access to the device. A customer can perform either a Selective or Full Wipe. Reasons to perform a Remote Wipe can be that the device is stolen or lost, the employee leaves the company, etc.

   Local Wipe is when the device automatically wipes itself when certain conditions occur. Customers can set a policy on the device that states that when a certain action is performed the device will wipe itself to mitigate a threat like an unauthorized user. For example, a device can be configured to perform a Local Wipe if more than five consecutive incorrect passwords are entered.

8. What is the difference between Selective Wipe and Full Wipe?

   When Remote Wipe is performed, it erases data from the targeted device. A Selective Wipe erases company data and apps, but does not erase personal data (e.g., photos, personal email, etc.). A Full Wipe erases all data (personal and company) and returns the phone to its factory out-of-the-box state.

   Choosing Selective Wipe or Full Wipe is typically based on whether the device is personal or corporate-owned and the individual situation.

   With Office 365 MDM, customers can remotely initiate either a Selective Wipe or a Full Wipe on managed devices. Selective Wipe applies only to data managed by apps that support MDM for Office 365 access control (currently Outlook and OneDrive for Business) and for email profiles that were created by MDM for Office 365. For more information, see Wipe a mobile device in Office 365.

   With Intune MDM, customers can remotely initiate either a Selective Wipe or Full Wipe on managed devices. Selective Wipe applies to all managed applications, e.g., apps that an Intune admin publishes and deploys using the Intune admin console. Selective Wipe does not apply to unmanaged applications. For more information, see Understanding the capabilities of unmanaged apps, managed apps, and MAM-protected apps.

With MAM, only Selective Wipe is available. When issuing a wipe request for a specific device, separate wipe requests will actually be issued and tracked for each protected application on the device.

9. What are Policy Tips?

   Policy Tips are a DLP feature. Policy Tips display notices to end-users, as they try to share sensitive content (sending an e-mail, sharing a document library, etc.) that may be in violation with established policies, enabling users to make informed decisions. For more information, see Policy Tips.

# Materials in this Library

Microsoft publishes a variety of content for customers, partners, auditors, and regulators around security, compliance, risk, trust, privacy, and related areas. Below are links to other content currently in our library. Many of these links point to content available for download from the Microsoft Cloud Service Trust Portal (STP). For information on how to access the STP, see Get started with the Service Trust Portal for Office 365 for business, Azure, and Dynamics CRM Online subscriptions.

| Name | Abstract |
|---|---|
| Auditing and Reporting in Office 365 | Describes the auditing and reporting features in Office 365 and Azure Active Directory available to customers. Also details the various audit data that is available to customers via the Office 365 Security & Compliance Center, remote PowerShell, and the Management Activity API. Also describes the internal logging data that is available to Microsoft Office 365 engineers for detection, analysis, and troubleshooting. |
| Controlling Access to Office 365 and Protecting Content on Devices | Describes the Conditional Access (CA) features in Microsoft Office 365 and Microsoft Enterprise Mobility + Security, and how they are designed with built-in data security and protection to keep company data safe, while empowering users to be productive on the devices they love. It also provides guidance on how to address common concerns around data access and data protection using Office 365 features. |
| Data Encryption Technologies in Office 365 | Provides an overview of the various encryption technologies that are currently available or recently announced for Office 365, including features deployed and managed by Microsoft, and features managed by customers. |
| Data Resiliency in Office 365 | Describes how Microsoft prevents customer data from becoming lost or corrupt in Exchange Online, SharePoint Online, and Skype for Business, and how Office 365 protects customer data from malware and ransomware. |
| Defending Office 365 Against Denial of Service Attacks | Discusses different types of Denial of Service attacks and how Microsoft defends Office 365, Azure, and their networks against attacks. |
| Financial Services Compliance in Microsoft's Cloud Services | Describes how the core contract amendments and the Microsoft Regulatory Compliance Program work together to support financial services customers in meeting their regulatory obligations as they relate to the use of cloud services. |
| **Microsoft Response to New FISC Guidelines in Japan (English) (Japanese)** | Explains how Microsoft addresses the risks and requirements described in the FISC Revised Guidelines, and it describes features, controls, and contractual commitments that customers can use to meet the requirements in the Revised Guidelines. |
| Microsoft Threat, Vulnerability, and Risk Assessment of Datacenter Physical Security | Provides an overview regarding the risk assessment of Microsoft datacenters, including potential threats, controls and processes to mitigate threats, and indicated residual risks. |
| Office 365 Customer Security Considerations | Provides organizations with quick access to the security and compliance features in Office 365 and considerations for using them. |
| Office 365 End of Year Security Report 2014 | Covers security and legal enhancements made to Office 365 in calendar year 2014 than enables customers and partners to meet legal requirements surrounding independent verification and audits of Office 365. |
| Office 365 End of Year Security Report and Pen Test Summary 2015 | Office 365 End of Year Security Report and Pen Test Summary for CY 2015. |
| Office 365 Mapping of CSA Cloud Control Matrix 3.0.1 | Provides a detailed overview of how Office 365 maps to the security, privacy, compliance, and risk management controls defined in version 3.0.1-11-24-2015 of the Cloud Security Alliance's Cloud Control Matrix. |
| Office 365 Risk Management Lifecycle | Provides an overview of how Office 365 identifies, evaluates, and manages identified risks. |
| Office 365 Security Incident Management | Describes how Microsoft handles security incidents in Microsoft Office 365. |
| Self-Service Handling of Data Spills in Office 365 (restricted to Federal customers) | Reviews the spillage support provided by Office 365, the tools available to customers, and the configuration settings that should be reviewed in environments that are prone to data spills. |
| Tenant Isolation in Office 365 | Describes how Microsoft implements logical isolation of tenant data within Office 365 environment. |