A quick guide to secure Office 365

V2.0

About the author

Nicki Borell is a Microsoft Reginal Director & MVP, Co-founder of Experts Inside, founder of the label *"Xperts at Work"* and partner of atwork GmbH. As a team, we successfully implement IT and strategy projects for mid-sized companies and large enterprise customers. Take advantage of the expertise, competence and specialized knowledge we bring to each of our projects.

Contact: www.xpertsatwork.com | nb@atwork-it.com | nb@expertsinside.com

Content

Cloud security strategy with Office 365

The default settings in Office 365 allow access to the services by entering a user name and password. There is no further evaluation of access. Depending on the licenses and roles assigned to the user he can access and use Office 365 after the login. Several solutions are available to prevent unauthorized access or to prevent users from performing actions that are unmeant. The following matrix illustrates a security setup based on 5 levels and lists the effects and required licenses:

Level	Explanation	Effect on usability	Effect on security	Licensing
Default	Default settings of Office 365	• All functions are available to the user according to his license. • They can work with internal and external people and share any content. • E-mails can be sent with any attachments to any recipient. • Access can take place from any device by entering a user name and password.	There is no security measure in addition to entering the user name and password.	No additional license required
Medium	Adjustments of the default Office 365 settings without the use of additional functions / licenses. Configuring Office 365 MFA and Office 365 MDM	**Measures:** • All functions are available to the user according to his license. • He can work with internal and external people according to the settings for sharing files in OneDrive for Business and SharePoint Online • E-mails can be sent with any attachments to any recipient. • Users must specify an additional factor (SMS, App Auth, etc.) in addition to their user name and password for each logon process. For more details, see: Azure AD Premium & Office 365 MFA • Only managed devices can access the Office 365 environment. Managed devices can be wiped remotely. For more details, see: Intune & Office 365 MDM **Effects:** • These measures result in additional doings for each logon process. • The possibilities for working with external parties are limited.	• The activation of O365 MFA and O365 MDM significantly increases safety. • The implementation of the specifications for OneDrive for Business and SharePoint increases security and the unwanted loss of data.	No additional license required

		• Office 365 can only be accessed from managed devices.		
High	like "**Medium**" plus: Use Cloud App Security to monitor Office 365 and configure actions. Use Azure AD Premium to enforce MFA and conditional access rules for external users, apps and devices.	**Measures:** • Cloud App Security allows you to monitor Office 365 and automatically apply actions. For more details, see: Cloud App Security These measures are automatically applied without the user's intervention. • MFA and Conditional Access as part of Azure AD Premium provides advanced features such as creating access policies (secure IP address ranges, trusted apps, etc.). For more details, see: Azure AD Premium & Office 365 MFA **Effects:** The measures do not result in any additional work for the user. The implementation of MFA and registration rules with Azure AD Premium significantly reduces the workload for users. Logons from e.g. the company network or from managed devices and apps can then be done without MFA etc.	• The use of Cloud App Security significantly increases security. Reports and automatic actions for e.g. unusual logon activities are now available. • MFA and Conditional Access as part of Azure AD Premium enable additional scenarios and thus further increase security.	• CAS • Azure AD Premium P1 or P2 Both licenses are part of EMS or M365 and can also be purchased separately.
Very High	Like "**High**" plus: use Intune to control device access and access to applications and manage devices.	**Measures:** • It can be explicitly managed which application is allowed to access which data from where and from which device and how. You can manage which data may be copied or further processed with which apps, for example "Copy & Past" or download into private Dropbox folders etc. • Devices and applications can be managed. **Effects:** The security requirements can be explicitly and granularly adapted to the requirements of the company.	• The ability to configure granular and explicit rules for accessing Office 365 / Azure and data further increases security. • Rules for non-Office 365 apps can also be implemented	Intune is part of EMS or M365 and can also be purchased separately.
Deactivating all external accesses		**Measures:** • Access to Office 365 is only possible for employees. • Access is only possible from the company network	Maximum security	No additional license required

		• Cooperation with external persons is no longer possible **Effects:** The usability of Office 365 is very limited. The service can only be used to a limited extent.		

OneDrive for Business and SharePoint Online

OneDrive for Business and SharePoint access and sharing settings can be configured in the admin center. The following matrix shows the relevant settings to secure OneDrive for Business and SharePoint based on you needs:

	Setting	**Details / Options**
OneDrive for Business Sharing Settings	Default link type	*Shareable: Anyone with this link *Internal links *Direct links: Specific people
Change sharing link settings	Advanced settings for shareable links	*Links expire within drop-down list *choose whether shareable links can give people permission to edit shared files and folders
	External Sharing	*Anyone *New and existing external users *Existing external users *Only people in your organization
	Specify any advanced settings for external sharing	*Allow or block sharing with people on specific domains *External users must accept sharing invitations using the same account that the invitations were sent to *Let external users share items they don't own
	Other settings	Display to owners the names of people who viewed their files
Syncing	Show the sync button on the OneDrive website	
	Allow syncing only on PCs joined to specific domains	
	Block syncing of specific filetypes	
Storage	Default storage space for OneDrive users	
	Days to retain files in OneDrive after a user account is marked for deletion	
Accessing OneDrive for Business	Control access based on network location	Allow access only from specific IP address locations
	Control access from apps that don't use modern authentication	YES or NO
	Control access to features in the OneDrive mobile apps	Needs to have an Intune license assigned to change these settings in the OneDrive admin center.
Notifications	Display notifications to users when OneDrive files are shared with them	YES or NO

	Email OneDrive owners when…:	*Other users invite additional users to shared files *External users accept invitations to access files *An anonymous access link is created or changed
SharePoint Online sharing settings	Sharing outside your organization	*Don't allow sharing outside your organization *Allow sharing only with the external users that already exist in your organization's directory *Allow users to invite and share with authenticated external users *Allow sharing to authenticated external users and using anonymous access links **Anonymous access links expire in this many days: **Anonymous access links allow recipients to:
	Who can share outside your organization	*Let only users in selected security groups share with authenticated external users *Let only users in selected security groups share with authenticated external users and using anonymous links
	Default link type	*Direct - specific people *Internal - only people in your organization *Anonymous Access - anyone with the link
	Default link permission	*View *Edit
	Additional settings	*Limit external sharing using domains (applies to all future sharing invitations). Separate multiple domains with spaces. Learn more. *Prevent external users from sharing files, folders, and sites that they don't own *External users must accept sharing invitations using the same account that the invitations were sent to *Require recipients to continually prove account ownership when they access shared items
	Unmanaged devices	*Allow full access from desktop apps, mobile apps, and the web *Allow limited, web-only access *Block Access
	Control access based on network location	Only allow access from specific IP address locations
	Apps that don't use modern authentication	YES or NO
Useful settings with PowerShell	BccExternalSharingInvitations	All external sharing invitations will be bcc e-mail to:
	BccExternalSharingInvitationsList	All external sharing invitations will be bcc e-mail to:
	DisallowInfectedFileDownload	Prevents the Download button from being displayed on the Virus Found warning page
	NotificationsInSharePointEnabled	
	ODBAccessRequests	Set a policy on re-sharing behavior in OneDrive for Business
	UserVoiceForFeedbackEnabled	

Enhance security using additional services and features

The security of Office 365 can be further enhanced by proactive and reactive monitoring. More details are described in Security & Compliance Reports and Office 365 Advanced Threat Protection & Office 365 Threat Intelligence and Office 365 Secure Score. In addition, Microsoft offers "Microsoft Advanced Threat Analytics", "Windows Defender Advanced Threat Protection" and "Windows Information Protection" solutions for protection of the entire IT infrastructure. This is all bundled in the new Microsoft Threat Protection. However, these scenarios are not part of this concept.

Office 365 Secure Score

Office 365 Secure Score analyzes which Office 365 services such as OneDrive, SharePoint or Exchange are used and checks their settings. The settings are then compared with a baseline setup provided by Microsoft. A report and recommendations to increase security are then generated. For details see https://support.office.com/en-us/article/introducing-the-office-365-secure-score-c9e7160f-2c34-4bd0-a548-5ddcc862eaef

Cloud App Security

Cloud App Security provides access security and auditing at application level. The service generates a report on the cloud apps and services that are used. The extended analyses make it possible to detect and defend against unusual login behavior, atypical actions such as high download rates and cyber threats in general. Integration with DLP and AIP enables extensive data control.

Typical scenarios:

- **Detect threats and automatically take action:** e.g.: Identify risky user activity and unusual access behavior.
- **Protect data:** e.g.: Detailed control over data and enforce integrated or custom data sharing policies to prevent data loss.
- **Control access in real time:** e.g.: Manage and limit access to cloud apps based on conditions and session context, including user identity, devices and location.
- **Discovering and assessing risks:** e.g.: Identify cloud apps used on the network. Insight into applications used, risk assessments and ongoing analysis.

For details see also: https://www.microsoft.com/en-us/cloud-platform/cloud-app-security

Policy types and details:

Policy type	Usage
Access policy	Access policies enable real-time monitoring and control of user logins to cloud apps.
Activity policy	Activity policies enables automated processes to be enforced. These policies can be used to monitor activities performed by users. Unexpectedly high rates of a certain type of activity are detected.
Anomaly detection policy	Anomaly detection policies detect unusual activities based on risk factors.
App discovery policy	App Discovery policies will set alerts to notify administrators when new apps are detected.
Cloud Discovery anomaly detection policy	Cloud Discovery anomaly detection policies examine protocols to detect unknown apps and search for anything unusual. For example, if a user who has never used Dropbox before suddenly uploads 600 GB, or if many more transactions than usual are recorded for a particular app.
File policy	File policies are used to monitor specified files or file types (shared with external domains) and data (proprietary information, credit card data, etc.) and apply governance actions to these files.
Session policy	Session policies allow real-time monitoring and control of user activity.

For details see also: https://docs.microsoft.com/en-us/cloud-app-security/control-cloud-apps-with-policies

Office 365 Cloud App Security:

Office 365 E5 also includes the Cloud App Security feature, but in a very limited version. Differences between Cloud App Security and Office 365 Cloud App Security are:

Capability	Feature	Microsoft Cloud App Security	Office 365 Cloud App Security
Cloud Discovery	Discovered apps	16,000 + cloud apps	750+ cloud apps Cloud apps with similar functionality to Office 365
	Deployment for discovery analysis	Manual and automatic log upload	Manual log upload
	Log anonymization for user privacy	●	
	Access to full Cloud App Catalog	●	
	Cloud app risk assessment	●	
	Cloud usage analytics per app, user, IP address	●	
	Ongoing analytics & reporting	●	
	Anomaly detection for discovered apps	●	
Information Protection	Data Loss Prevention (DLP) support	Cross-SaaS DLP and data sharing control	Uses existing Office DLP (available in Office E3 and above)
	App permissions and ability to revoke access	●	●
	Policy setting and enforcement	●	
	Integration with Azure Information Protection	●	
	Integration with third party DLP solutions	●	
Threat Detection	Anomaly detection and behavioral analytics	For Cross-SaaS apps including Office 365	For Office 365 apps
	Manual and automatic alert remediation	●	●
	SIEM connector	Yes. Alerts and activity logs for cross-SaaS apps.	Yes. Office 365 alerts only.
	Integration to Microsoft Intelligent Security Graph	●	●
	Activity policies	●	●

For details see also: https://docs.microsoft.com/en-us/cloud-app-security/editions-cloud-app-security-o365

Intune & Office 365 MDM

By default, Office 365 comes with standalone options for managing mobile devices and mobile access that are included in user licenses. This is a limited version of MDM and only covers basic functions.

Functional area	MDM for Office 365	Microsoft Intune
Device management	Devices are managed through the Security and Compliance Center in Office 365.	Intune management console in Azure or integration in System Center
Manageable devices	Cloud-based management iOS, Android and Windows devices.	Cloud-based management for iOS, Mac OS X, Android, Windows 8.1 (phone and computer) and later included in Windows 10
Important functions	• Ensure that corporate e-mail and documents in Office 365 can only be accessed from smartphones and tablets that are managed by the company and fit to IT policies. • Set and manage security policies such as device-level PIN locking and jailbreak detection to prevent unauthorized users from accessing corporate email and data from a device if it is lost or stolen. • Remove company data from an employee's device while preserving personal data.	MDM for Office 365 functions and the following additional functions: • Secure user access to corporate resources with certificates, Wi-Fi, VPN and email profiles • Register and manage company devices to deploy policies and apps • Providing Apps for Users • More secure access to corporate data while ensuring data security by limiting actions such as "Copy", "Cut", "Paste" and "Save As" to Apps managed by Intune. • Manage PCs, Macs, Linux and UNIX servers, and mobile devices

For details see also: https://support.office.com/en-us/article/choose-between-mdm-for-office-365-and-microsoft-intune-c93d9ab9-efb2-4349-9b93-30c30562ee22 and https://support.office.com/en-us/article/capabilities-of-built-in-mobile-device-management-for-office-365-a1da44e5-7475-4992-be91-9ccec25905b0?ui=en-US&rs=en-US&ad=US

Azure AD Premium & Office 365 MFA

By default, Office 365 comes with standalone multi-factor authentication options included in user licenses. This is a limited version of MFA and only covers basic functions.

Feature	MFA for Office 365	MFA for Azure AD Administrators	Azure MFA
Protect Azure AD admin accounts with MFA	●	● (Azure AD Global Administrator accounts only)	●
Mobile app as a second factor	●	●	●
Phone call as a second factor	●	●	●
SMS as a second factor	●	●	●
App passwords for clients that don't support MFA	●	●	●
Admin control over verification methods	●	●	●
Protect non-admin accounts with MFA	● (Only for Office 365 applications)		●
PIN mode			●

Fraud alert			●
MFA Reports			●
One-Time Bypass			●
Custom greetings for phone calls			●
Custom caller ID for phone calls			●
Trusted IPs			●
Remember MFA for trusted devices	●	●	●
MFA SDK			● (Deprecated)
MFA for on-premises applications			●

For details see: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing

Other features of Azure AD Premium

Conditional Access:
Azure Active Directory Premium Conditional Access feature controls access for Apps and users based on specific conditions. Event-related access control is implemented with guidelines for conditional access.

- **Applicant risk:** Azure AD Identity Protection detects risks and automatically takes action according to the configured rules. For details see: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-conditions#sign-in-risk
- **IP Ranges:** Rules are used to enforce MFA when logging in from an unknown network, for example. Login from the company network, for example, no MFA is forced. For details see: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-locations
- **Device management:** Users can access from a wide range of devices, including mobile and home devices. For example, access is only possible via managed devices. Another option is to allow access to certain Apps only from managed devices, etc.

  Example:
  - Microsoft Teams can only be accessed from a managed device
  - Email can be accessed from any device. However, if the accesses is from outside the company network, MFA is enforced.

  For details see: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-conditions#device-platforms

- **Client application:** This function is used to determine which applications can be used to access which resources. For example, it can be forced to use the Outlook App to access Emails. For details see: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-conditions#client-apps

Further information about Conditional Access can be found here: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-conditional-access-azure-portal

In addition, Conditional Access of Azure Active Directory Premium provides the "Terms of Use" feature. It is requires that a user is notified of relevant disclaimers, legal or compliance requirements or information regarding privacy and datasecurity when logging in and that the user confirm these before they are forwarded. For details see: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-tou

Role-Based Access Control and Privileged Identity Management:

Azure Active Directory Privileged Identity Management (PIM) can be combined with Role Based Access Control (RBAC). Thus, administrators do not have to have the "global Admin" role permanently. An administrative role can be requested for a specific scenario via a workflow.

Functions / Scenarios:

- Demand-driven just-in-time access with extended rights
- Temporary extended rights for short tasks or on-call times
- Enforce multi-factor authentication when accessing with extended privileges
- Reports on accesses with extended rights
- Notifications when access with extended rights is requested

For details see also: https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/azure-pim-resource-rbac

MAM and MDM in the context of Azure AD Premium:

MAM (Mobile Application Management) and MDM (Mobile Device Management) are usually combined. The two solutions can be distinguished as follows:

- **MDM:** addresses lack of control over corporate and personal devices, and lost device security
    - Ensures device compliance through user and device registration, configuration and passcode management
    - Secures devices on the network so you can monitor, report, track and update devices – and even locate, lock and wipe devices, if lost or stolen
- **MAM:** addresses lack of compliance with data and privacy requirements, and lost data retrieval
    - User identity policy, single sign-on and conditional access tailored by role and device (with Intune or Active Directory on premises or in the cloud)
    - Monitors and pushes App updates, including mobile document management for online or cloud-provisioned apps like SharePoint and OneDrive

With Azure AD Premium you have the option to combine MAM and MDM (Intune) or to use MAM without MDM (Intune) or MDM with a 3rd party solution.

For details see also: https://docs.microsoft.com/en-us/intune/mam-faq

Office 365 Advanced Threat Protection & Office 365 Threat Intelligence

Office 365 Threat Intelligence:

Office 365 Threat Intelligence is a collection of reports available in the Security & Compliance Center. Threat Intelligence monitors and collects data from multiple sources, such as user activity, authentication, Email, and more. This feature is included in Office 365 Enterprise E5.

For details see: https://support.office.com/en-us/article/get-started-with-office-365-threat-intelligence-38e9b67f-d188-490f-bc91-a1ae4b270441?ui=en-US&rs=en-US&ad=US

Office 365 Advanced Threat Protection:

Office 365 Advanced Threat Protection is used for the following scenarios:

- E-mail attachment scanning
- Scanning Web addresses and Office documents in an Email message
- Identify and block malicious files in SharePoint, OneDrive, and Microsoft Teams
- Identify Email messages with spoofing attacks
- Detection of phishing attacks

Office 365 Advanced Threat Protection is included with Office 365 Enterprise E5. For details see also: https://support.office.com/en-us/article/office-365-advanced-threat-protection-e100fe7c-f2a1-4b7d-9e08-622330b83653

Security & Compliance Reports

The Office 365 Security & Compliance Center provides reports and functions to secure the environment. A distinction is made between the following topics:

- Protection for data and services in Office 365
- Prevent data loss in Office 365
- Managing data control in Office 365
- Threat protection in Office 365
- Content search in Office 365
- Managing legal investigations in Office 365
- Browse log for user and administrator activity in Office 365
- Monitoring security and compliance in Office 365

Depending on the details, different licenses are required.

How to deal with external Sharing Sketchnote at Microsoft Ignite 2018

Sketchnote by Luise Freese. Download Sketchnote: LINK