

TSOC CTI

Microsoft Teams Recommendations



Date	19.03.2020
Version	v1.0
Document name	MS_Teams_recommendation_1.0.dox
Author	Asaf Twizer, Trustnet LTD

Contents

1	Introduction	3
2	Objectives	3
3	Authentication.....	3
4	Access Control	4
5	Roles (RBAC)	4
5.1	MS Teams role-based admin groups.....	4
5.2	RBAC model access per entity	5
6	File Sharing	5
7	CASB Integration.....	6
8	Intune Integration (MDM/MAM).....	6
9	Azure Information Protection.....	7
10	Auditing and Logging	7
11	Approved/unapproved applications	8
11.1	Approved applications.....	8
11.2	Unapproved applications.....	8
12	Data Retention	8

1 Introduction

COVID-19, one of the most advanced pandemics is a growing global concern that has started to impact the entire world's economy. Organizations are thus mandated to find new solutions to maintain business continuity while enabling employees to work remotely, ensuring confidentiality, integrity, and availability.

Many organizations have thus chosen Microsoft Teams. Microsoft Teams is a unified communication and collaboration platform that combines persistent workplace chat, video meetings, file storage (including collaboration on files), and application integration. This service also integrates with Office 365 subscription, office productivity suite and features that can integrate with non-Microsoft products.

2 Objectives

The objectives of this document is to:

- Provide organizations a baseline for working with MS Teams
- Provide guidelines on implementing comprehensive security controls
- Highlight areas which need to be considered when enabling MS Teams
- Highlight potential controls an organization can have while using MS Teams

3 Authentication

Microsoft Teams authentication is based on Azure Active Directory (AAD). Identities and access management are easily managed using AAD and organizations can utilize comprehensive security features to secure access to MS Teams.

Multi-Factor Authentication (MFA) is another important aspect of an authentication mechanism. Since, MS Teams is accessible everywhere, ensure that you can verify any user identity using Azure MFA.

4 Access Control

Microsoft's risk based conditional access also covers MS Teams. You can deploy the existing conditional access strategy and policies across MS Teams or create a dedicated policy to control access and block it from unwanted (or unmanaged) devices, locations and more.

The following lists the restrictions you should consider from a security standpoint:

- Block access from unusual **geographies (Geo-Locations)**
- Block access based on **device risk**
- Monitor or restrict access and permissions based on **user risk**
- Control access based on **conditional access** (MFA, Managed Device, etc.)

5 Roles (RBAC)

5.1 MS Teams role-based admin groups

There are four admin roles primarily available for MS Teams:

- Teams service administrator
- Teams communications administrator
- Teams communications support specialist
- Teams communications support engineer

These groups provide different levels of access for managing MS Teams, from an all-access admin group to tier 1 or 2 helpdesk-type groups. You should manage and control those roles cautiously, as per business objectives.

Administrator Roles	Associated Privileges
Teams Service Administrator	Can manage the Microsoft Teams service and all its features as well as Office 365 groups
Teams Communications Administrator	Can manage calling and meetings features and policies

Administrator Roles	Associated Privileges
Teams Communications Support Engineer	Can access a user's profile page with call history (with full details of participants) and advanced quality of experience data
Teams Communications Support Specialist	Can access a user's profile page with anonymized participant data and quality information

5.2 RBAC model access per entity

Access should be managed and controlled per entity. You can use the following matrix to define the needs of each entity and user. We have illustrated below a matrix, as a sample, for various Business Units. The model can be modified and adapted to any organization, as per the defined requirements or case scenario:

Department	Access to main Teams	Access to channels	Calls with other Teams	Access to colleagues' Teams	File sharing
Table of department (A) RBAC					
Business Unit (A)	A	A	A	N	A
Business Unit (B)	N	N	A	N	N
Business Unit (C)	N	N	A	N	A

Permissions	Users	Guest Users
Sharing files with internal users (other Teams)	A	N
Sharing files with external users	N	N
Creating new Teams*	N	N
Creating new channels	A	N
Adding new Teams members	AO	N
Download files to Teams	A	N
Upload files to Teams	A	N
Calls with external users	A	A

A - Allowed, N – Not Allowed for Teams' owners, *only administrators can create new Teams

6 File Sharing

Microsoft Teams enable users to add external participants to their respective Teams channels. The users external to the organization such as vendors, partners and brokers once invited can then access Teams resources, conversations, and shared files.

It is recommended to engage team owners to ensure they manage and review access to the data and channels they own in the teams. Besides, as a best practice, they should:

- Verify guest access in Microsoft Teams
- Review sharing links for each Team's SharePoint site
- Schedule periodic review for external shares (automate the process)
- Track sharing progress and log changes

7 CASB Integration

Cloud Access Security Broker (CASB) can be integrated with Microsoft Teams to provide monitoring and ensure adequate governance and control over data and user activities. CASBs also provide organizations the flexibility to:

- Prevent sensitive data that should not be stored in the cloud from being uploaded to Teams
- Prevent sharing sensitive or regulated data with unauthorized parties
- Enforce context-specific policies limiting end-user actions and access control
- Provide an audit trail of user activities enriched with threat intelligence to facilitate post-incident forensic investigations.
- Detect threats from compromised accounts, insider threats, privileged access misuse, and malware infection.

8 Intune Integration (MDM/MAM)

Teams meeting room can be enrolled and managed by Microsoft Intune. It provides a massive set of security capabilities, including:

- Restricting copy-and-paste and save-as functions
- Configuring web links to open inside the secure Microsoft browser
- Enabling multi-identity use and app-level Conditional Access
- Applying data loss prevention policies without managing the user's device
- Enabling app protection without requiring enrollment
- Enabling app protection on devices managed with 3rd party EMM tools

9 Azure Information Protection

Azure Information Protection is a cloud-based solution that helps organizations to classify and optionally, protect its documents and emails by applying labels. Labels can be applied automatically by administrators who define rules and conditions, manually by users, or a combination where users are given recommendations. Once data is labeled, it can then be controlled and managed through all of Microsoft applications including Teams.

10 Auditing and Logging

Teams audit log is included within Office 365 Security & Compliance Center. You should ensure that all the actions are being audited and have dedicated alerts setup, directly from the compliance center or using your SIEM solution. Auditing and monitoring access, file shares and unauthorized activity can help reduce the attack surface and data exposure. Organizations already monitoring Office 365 using their SIEM solution, can also emphasize on the following security controls:

- User and administrator access
- Administrator actions
- File access and sharing
- Policy changes
- Activities with known bad actors

Microsoft provides many tools, capabilities, and resources for security and compliance, but, provisioning, configuring and use each service independently can be tremendously challenging. While the user experience is one of the major considerations, there are many other reasons for which you may want to consider using a third-party security monitoring solution for Office 365 such as using SIEM inside the organization or using SOC services.

11 Approved/unapproved applications

A list of available applications for Teams is available on Microsoft's official AppSource.

11.1 Approved applications

Organizations should define approved applications while considering the following:

- Business requirement
- Software usage and exposure
- Free\Licensed software
- Personal or work usage

11.2 Unapproved applications

An application that is not defined as approved applications should be blocked by default.

12 Data Retention

Organizations should ensure to manage MS Teams data and have data retention processes in the same manner they manage any other data within any other channel or platform. It is also recommended to consider the following:

- Follow internal policies that define the minimum retention period
- Define data usage policy - retained, deleted, retained and deleted based on specific periods
- Use the SCC Policy creation user experience or Teams Retention PowerShell cmdlets
- Set different retention durations for Teams Chats vs Teams Channel Messages