Microsoft Teams

M365 Minimum Viable Secure Configuration Baseline Draft Version 0.1

October 2022
Cybersecurity and Infrastructure Security Agency
Secure Cloud Business Applications (SCuBA)

Record of Changes

No.	Date	Reference	A=Add
			M=Modify
			D=Delete
				Description of Change

v0.1	17 October 2022	Entire document	M	Initial Draft w/Edit

Table of Contents

This page is intentionally blank.

1. Introduction

Microsoft Teams is a text and live chat workspace in Microsoft 365 (M365) that supports video calls, chat messaging, screen-sharing, and file sharing. It has a permission-based team structure for managing calls and files. Microsoft teams also enables teams to manage their own user access rights, security policies, and record video calls.

Access to Teams can be controlled by the user type. In this baseline, the types of users are defined as follows (Note: these terms vary in use across Microsoft documentation):

1. **Internal users**: members of the agency's M365 tenant.
2. **External users**: members of a different M365 tenant.
3. **Business to Business** (B2B) guest users: external users that are formally invited to collaborate with the team and added to the agency's Azure Active Directory (AAD) as guest users. These users authenticate with their home organization/tenant and are granted access to the team by virtue of being listed as guest users on the tenant's AAD.
4. **Unmanaged users:** users who are not members of any M365 tenant or organization (e.g., personal Microsoft accounts).
5. **Anonymous users**: Teams users joining calls that are not authenticated through the agency's tenant, including unmanaged users, external users (except for B2B guests), and true anonymous users, meaning users that are not logged in to any Microsoft or organization account, such as dial-in users.[1]

1.1 Assumptions

The **License Requirements** sections of this document assume the organization is using an M365 E3 or G3 license level. Therefore, only licenses not included in E3/G3 are listed.

1.2 Resources

License Compliance and Copyright
Portions of this document are adapted from documents in Microsoft's M365 and Azure GitHub repositories. The respective documents are subject to copyright and are adapted under the terms of the Creative Commons Attribution 4.0 International license. Source documents are linked throughout this document. The United States Government has adapted selections of these documents to develop innovative and scalable configuration standards to strengthen the security of widely used cloud-based software services.

[1] Note that B2B guest users and all anonymous users except for external users appear in Teams calls as *John Doe (Guest)*. To avoid any potential confusion this may cause, true guest users are always referred to as B2B guest users in this document.

2. Baseline

2.1 External Participants SHOULD NOT Be Enabled to Request Control of Shared Desktops or Windows in Meetings

This setting controls whether external meeting participants can request control of the shared desktop or window during the meeting. In this instance, the term “external participants” includes external users, B2B guest users, unmanaged users, and anonymous users.

While there is some inherent risk in granting an external participant control of a shared screen, legitimate use cases for this exist. Furthermore, the risk is minimal as users cannot gain control of another user’s screen unless the user giving control explicitly accepts a control request. As such, while enabling external participants to request control is discouraged, it may be done, depending on agency need.

2.1.1 Policy

External participants SHOULD NOT be enabled to request control of shared desktops or windows in the Global (Org-wide default) meeting policy or in custom meeting policies if any exist.

2.1.2 Resources

- Configure desktop sharing in Microsoft Teams | Microsoft Docs

2.1.3 License Requirements

N/A

2.1.4 Implementation

To ensure external participants do not have the ability to request control of the shared desktop or window in the meeting:

1. Sign in to the Microsoft Teams admin center.
2. Select **Meetings** -> **Meeting policie**s.
3. Select the **Global (Org-wide default)** policy.
4. Under the **Content sharing** section, set **Allow an external participant to give or request control** to **Off**.
5. If custom policies have been created, repeat these steps for each policy, selecting the appropriate policy in step 3.

2.2 Anonymous Users SHALL NOT Be Enabled to Start Meetings

This setting controls which meeting participants can start a meeting. In this instance, the term “anonymous users” refers to any Teams users joining calls that are not authenticated through the agency’s tenant.

2.2.1 Policy

Anonymous users SHALL NOT be enabled to start meetings in the Global (Org-wide default) meeting policy or in custom meeting policies if any exist.

2.2.2 Resources

Meeting policy settings - Participants & guests | Microsoft Docs

2.2.3 License Requirements

N/A

2.2.4 Implementation

To configure settings for anonymous users:

1. Sign in to the Microsoft Teams admin center.
2. Select **Meetings -> Meeting policies.**
3. Select the **Global (Org-wide default)** policy.
4. Under the **Participants & guests** section, set **Let anonymous people start a meeting** to **Off.**
5. If custom policies have been created, repeat these steps for each policy, selecting the appropriate policy in step 3.

2.3 Automatic Admittance to Meetings SHOULD Be Restricted

This setting controls which meeting participants wait in the lobby before they are admitted to the meeting.

2.3.1 Policy

- Anonymous users, including dial-in users, SHOULD NOT be admitted automatically.
- Internal users SHOULD be admitted automatically.
- B2B guest users MAY be admitted automatically.
- The above settings SHOULD be set in the Global (Org-wide default) meeting policy.
- Custom meeting policies MAY be created that allow more flexibility for specific users.

2.3.2 Resources

- Meeting policy settings - Participants & guests | Microsoft Docs

2.3.3 License Requirements

N/A

2.3.4 Implementation

To configure settings for automatic meeting admittance:

1. Sign in to the Microsoft Teams admin center.
2. Select **Meetings -> Meeting policies.**
3. Select the **Global (Org-wide default)** policy.
4. Under the **Participants & guests** section, ensure **Automatically admit people** is *not* set to **Everyone.**

5. In the same section, set **Dial-in users can bypass the lobby** to **Off**.
6. If custom policies have been created, repeat these steps for each policy, selecting the appropriate policy in step 3.

2.4 External User Access SHALL Be Restricted

External access allows external users to look up internal users by their email address to initiate chats and calls entirely within Teams. Blocking external access prevents external users from using Teams as an avenue for reconnaissance or phishing. Even with external access disabled, external users will still be able to join Teams calls, assuming anonymous join is enabled. Depending on agency need, if both external access and anonymous join need to be blocked—neither required nor recommended by this baseline—external collaborators would only be able to attend meetings if added as a B2B guest user.

External access may be granted on a per-domain basis. This may be desirable in some cases, e.g., for agency-to-agency collaboration (see the CIO Council's Interagency Collaboration Program's OMB Max Site for a list of .gov domains for sharing).

Importantly, this setting only pertains to external users (i.e., members of a different M365 tenant). Access for unmanaged users is controlled separately.

2.4.1 Policy

External access SHALL only be enabled on a per-domain basis.

Anonymous users SHOULD be enabled to join meetings.

2.4.2 Resources

- Manage external access in Microsoft Teams | Microsoft Docs
- Allow anonymous users to join meetings | Microsoft Docs
- Use guest access and external access to collaborate with people outside your organization | Microsoft Docs

2.4.3 License Requirements

N/A

2.4.4 Implementation

To enable external access for only specific domains:

1. Sign in to the **Microsoft Teams admin center**.
2. Select **Users** -> **External access.**
3. Under **Choose which external domains your users have access to**, select **Allow only specific external domains.**
4. Click **Allow domains** to add allowed external domains. All domains not added in this step will be blocked.
5. Click **Save.**

To enable anonymous users to join meetings:

1. Sign in to the Microsoft Teams admin center.
2. Select **Meetings -> Meeting settings**.
3. Under **Participants**, set **Anonymous users can join a meeting** to **On**.
4. Click **Save**.

Anonymous users can also be enabled/blocked on a per-policy basis.

1. Sign in to the Microsoft Teams admin center.
2. Select **Meetings -> Meeting policies**.
3. Select the **Global (Org-wide default)**, or other policy as needed.
4. Under **Participants & guests**, set **Let anonymous people join a meeting** to **On**.
5. Click **Save**.

2.5 Unmanaged User Access SHALL Be Restricted

Blocking contact with unmanaged Teams users prevents these users from looking up internal users by their email address and initiating chats and calls within Teams. These users would still be able to join calls, assuming anonymous join is enabled. Additionally, unmanaged users may be added to Teams chats if the internal user initiates the contact.

2.5.1 Policy

- Unmanaged users SHALL NOT be enabled to initiate contact with internal users.
- Internal users SHOULD NOT be enabled to initiate contact with unmanaged users.

2.5.2 Resources

- Manage contact with external Teams users not managed by an organization | Microsoft Docs

2.5.3 License Requirements

N/A

2.5.4 Implementation

Steps are outlined in Manage contact with external Teams users not managed by an organization.

1. Sign in to the Microsoft Teams admin center**.**
2. Select **Users -> External access.**
3. To completely block contact with unmanaged users, under **Teams accounts not managed by an organization**, set **People in my organization can communicate with Teams users whose accounts aren't managed by an organization** to **Off**.
4. To allow contact with unmanaged users only if the internal user initiates the contact:

a. Under **Teams accounts not managed by an organization**, set **People in my organization can communicate with Teams users whose accounts aren't managed by an organization** to **On**.

b. Clear the check next to **External users with Teams accounts not managed by an organization can contact users in my organization.**

2.6 Contact with Skype Users SHALL Be Blocked

Microsoft officially retired Skype for Business Online on July 31, 2021, and it is no longer supported.

2.6.1 Policy

- Contact with Skype users SHALL be blocked.

2.6.2 Resources

- Communicate with Skype users | Microsoft Docs
- Skype for Business Online to Be Retired in 2021 | Microsoft Teams Blog

2.6.3 License Requirements

N/A

2.6.4 Implementation

Instructions for *enabling* communications with Skype users are outlined in Communicate with Skype users.

1. Sign in to the **Microsoft Teams admin center**.
2. Select **Users -> External access.**
3. Under **Skype** users, set **Allow users in my organization to communicate with Skype users** to **Off.**
4. Click **Save.**

2.7 Teams Email Integration SHALL Be Disabled

Teams provides an optional feature that allows channels to have an email address and receive email. These channel email addresses are not under the tenant's domain; rather, they are associated with a Microsoft-owned domain, teams.ms. As such, although some basic checks are performed, agencies do not have control over the security settings associated with this email. For this reason, email channel integration should be disabled.

2.7.1 Policy

- Teams email integration SHALL be disabled.

2.7.2 Resources

- Email Integration | Microsoft Docs

2.7.3 License Requirements

- Teams email integration is only available with E3/E5 licenses. It is not available in GCC or DoD tenants.

2.7.4 Implementation

To ensure that teams email integration is disabled:

1. Sign in to the **Microsoft Teams admin center**.
2. Select **Teams** -> **Teams Settings**.
3. Under the **Email integration** section, set **Allow users to send emails to a channel email address** to **Off**.

2.8 Only Approved Apps SHOULD Be Installed

Teams can integrate with the following classes of apps:

- *Microsoft apps*: apps published by Microsoft.
- *Third-party apps*: apps not authored by Microsoft, published to the Teams store.
- *Custom apps*: apps not published to the Teams store, such as apps under development, that users “sideload” into Teams.

2.8.1 Policy

- Agencies SHOULD allow all apps published by Microsoft, but MAY block specific Microsoft apps as needed.
- Agencies SHOULD NOT allow installation of all third-party apps or custom apps, but MAY allow specific apps as needed.
- Agencies SHALL establish policy dictating the app review and approval process to be used by the agency.

2.8.2 Resources

- Manage app permission policies in Microsoft Teams | Microsoft Docs
- Upload your app in Microsoft Teams | Microsoft Docs

2.8.3 License Requirements

- N/A

2.8.4 Implementation

To restrict which Team apps can be installed:

1. Sign in to the **Microsoft Teams admin center**.
2. Select **Teams apps** -> **Permission policies.**
3. Select **Global (Org-wide default)**.

4. Under **Microsoft apps**, select **Allow all apps**, unless specific apps need to be disallowed, in which case select **Block specific apps and allow all others**.
5. Set **Third-party apps** to **Block all apps**, unless specific apps have been approved by the agency, in which case select **Allow specific apps and block all others**.
6. Set **Custom apps** to **Block all apps**, unless specific apps have been approved by the agency, in which case select **Allow specific apps and block all others**.
7. Click **Save**.
8. If custom policies have been created, repeat these steps for each policy, selecting the appropriate policy in step 3.

2.9 Cloud Recording of Teams Meetings SHOULD Be Disabled for Unapproved Users

This setting determines whether video can be recorded in meetings hosted by a user, during one-on-one calls, and on group calls started by a user. Agencies should comply with any other applicable policies or legislation in addition to this guidance.

2.9.1 Policy

- Cloud video recording SHOULD be disabled in the global (org-wide default) meeting policy.
- Alternate meeting policies MAY be created that allow agency-approved users the ability to record.
- For all meeting polices that allow cloud recording, recordings SHOULD be stored inside the country of that agency's tenant.

2.9.2 Resources

- Teams cloud meeting recording | Microsoft Docs
- Assign policies in Teams – getting started | Microsoft Docs

2.9.3 License Requirements

N/A

2.9.4 Implementation

To configure the Meeting policies for cloud video recording:

1. Sign in to the **Microsoft Teams admin center**.
2. Select **Meetings** -> **Meeting policies**.
3. Select the **Global (Org-wide default)** policy.
4. Under the **Recording & transcription** section, set **Cloud recording** to **Off**.
5. Select **Save**.

If there is a legitimate business need, *specific* users can be given permission to record meetings. To allow specific users the ability to record meetings:

1. Sign in to the Microsoft Teams admin center**.**
2. Select **Meetings** -> **Meeting policies**.
3. Create a new policy by selecting **Add**. Give this new policy a name and appropriate description.
4. Under the **Recording & transcription** section, set **Cloud recording** to **On**.
5. Under the **Recording & transcription** section, set **Store recordings outside of your country or region** to **Off**.
6. Select **Save**.
7. After selecting **Save**, a table displays the set of policies. Select the row containing the new policy, then select **Manage users**.
8. Assign the users that need the ability to record to this policy.
9. Select **Apply**.

2.10 Only the Meeting Organizer SHOULD Be Able to Record Live Events

Live events are recorded by default. Agencies should increase their privacy by changing the policy so that events are only recorded at the organizer's discretion.

2.10.1 Policy

Record an event SHOULD be set to Organizer can record.

2.10.2 Resources

Live Event Recording Policies | Microsoft Docs

2.10.3 License Requirements

N/A

2.10.4 Implementation

1. Sign in to the Microsoft Teams admin center**.**
2. Select **Meetings** -> **Live events policies**.
3. Select **Global (Org-wide default)**.
4. Set **Record an event** to **Organizer can record**.
5. Click **Save**.

2.11 Data Loss Prevention Solutions SHALL Be Enabled

Data loss prevention (DLP) helps prevent both accidental leakage of sensitive information as well as intentional exfiltration of data. DLP forms an integral part of securing Microsoft Teams. There a several commercial DLP solutions available that document support for Microsoft Teams. Agencies may select any service that fits their needs and meets the requirements outlined in this baseline control.

Microsoft offers DLP services, controlled within the M365 compliance admin center. Though use of Microsoft's DLP solution is not strictly required, guidance for configuring Microsoft's DLP solution can be found in the "Data Loss Prevention SHALL Be Enabled" section of the *Defender for Office 365 Minimum Viable Secure Configuration Baseline*. The DLP solution selected by an agency should offer services comparable to those offered by Microsoft.

2.11.1 Policy

- A DLP solution SHALL be enabled.
- Agencies SHOULD use either the native DLP solution offered by Microsoft or a DLP solution that offers comparable services.
- The DLP solution SHALL protect Personally Identifiable Information (PII) and sensitive information, as defined by the agency. At a minimum, the sharing of credit card numbers, taxpayer Identification Numbers (TIN), and Social Security Numbers (SSN) via email SHALL be restricted.

2.11.2 Resources

The "Data Loss Prevention SHALL Be Enabled" section of the *Defender for Office 365 Minimum Viable Secure Configuration Baseline*.

2.12 Attachments SHOULD Be Scanned for Malware

Though any product that fills the requirements outlined in this baseline control may be used, for guidance on implementing malware scanning using Microsoft Defender, see the "Data Loss Prevention SHALL Be Enabled" section of the *Defender for Office 365 Minimum Viable Secure Configuration Baseline*.

2.12.1 Policy

- Attachments included with Teams messages SHOULD be scanned for malware.
- Users SHOULD be prevented from opening or downloading files detected as malware.

2.12.2 Resources

The "Data Loss Prevention SHALL Be Enabled" section of the *Defender for Office 365 Minimum Viable Secure Configuration Baseline.*

2.13 Link Protection SHOULD Be Enabled

Microsoft Defender protects users from malicious links included in Teams messages by prependinghttps://*.safelinks.protection.outlook.com/?url= to URLs included in the messages. By prepending the safe links URL, Microsoft can proxy the initial URL through their scanning service. Their proxy performs the following checks:

- Compares the URL with a block list
- Compares the URL with a list of know malicious sites
- If the URL points to a downloadable file, applies real-time file scanning

If all checks pass, the user is redirected to the original URL.

Though Defender's use is not strictly required for this purpose, guidance for enabling link scanning using Microsoft Defender is included in the "Safe Links Policies SHALL Be Enabled" section of the *Defender for Office 365 Minimum Viable Secure Configuration Baseline.*

2.13.1 Policy

- URL comparison with a block-list SHOULD be enabled.
- Direct download links SHOULD be scanned for malware.
- User click tracking SHOULD be enabled.

2.13.2 Resources

- The "Safe Links Policies SHALL Be Enabled" section of the *Defender for Office 365 Minimum Viable Secure Configuration Baseline.*

3. Acknowledgements

In addition to acknowledging the important contributions of a diverse team of Cybersecurity and Infrastructure Security Agency (CISA) experts, CISA thanks the following federal agencies and private sector organizations that provided input during the development of the Secure Business Cloud Application's security configuration baselines in response to Section 3 of Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*:

- Consumer Financial Protection Bureau (CFPB)
- Department of the Interior (DOI)
- National Aeronautics and Space Administration (NASA)
- Sandia National Laboratories (Sandia)
- U.S. Census Bureau (USCB)
- U.S. Geological Survey (USGS)
- U.S. Office of Personnel Management (OPM)
- U.S. Small Business Administration (SBA)

The cross-agency collaboration and partnerships developed during this initiative serve as an example for solving complex problems faced by the federal government.

Cybersecurity Innovation Tiger Team (CITT) Leadership
Beau Houser (USCB), Sanjay Gupta (SBA), Michael Witt (NASA), James Saunders (OPM), Han Lin (Sandia), Andrew Havely (DOI).

CITT Authors
Trafenia Salzman (SBA), Benjamin McChesney (OPM), Robert Collier (USCB), Matthew Snitchler (Sandia), Darryl Purdy (USCB), Brandon Frankens (NASA), Brandon Goss (NASA), Nicole Bogeajis (DOI/USGS), Kevin Kelly (DOI), Adnan Ehsan (CFPB), Michael Griffin (CFPB), Vincent Urias (Sandia), Angela Calabaza (Sandia).

CITT Contributors

M365 Minimum Viable Secure Configuration Baseline

Dr. Mukesh Rohatgi (MITRE), Lee Szilagyi (MITRE), Nanda Katikaneni (MITRE), Ted Kolovos (MITRE), Thomas Comeau (MITRE), Karen Caraway (MITRE), Jackie Whieldon (MITRE), Jeanne Firey (MITRE), Kenneth Myers (General Services Administration).