Navigating Microsoft 365 Security, Compliance, and Teams Management

This comprehensive guide provides detailed insights into securing your Microsoft 365 environment, managing user access, and leveraging Microsoft Teams for communication and compliance.

1. Strengthening Security with Multi-Factor Authentication (MFA)

Multi-factor authentication adds a critical layer of security to your Microsoft 365 accounts, reducing the risk of unauthorized access by requiring a second form of verification. According to Microsoft, enabling MFA can prevent up to 99.9% of account compromise attacks.[1][2]

How to Enable MFA:

There are three primary methods to enable MFA in Microsoft 365:

- **Security Defaults (Recommended for Small Organizations):** This is the most straightforward approach and is enabled by default for subscriptions created after October 21, 2019.[2][3] It enforces MFA for all users.[2] To enable or verify Security Defaults:
  1. Sign in to the Microsoft Entra admin center.
  2. Navigate to **Identity > Overview > Properties**.[3]
  3. Select **Manage security defaults** and set it to **Enabled**.[3]
- **Conditional Access Policies (Advanced):** This method offers more granular control and is suitable for organizations with specific security requirements.[4][5] It allows you to create policies that trigger MFA based on factors like user location, device status, and sign-in risk.[5] To create a Conditional Access policy for MFA:
  1. In the Microsoft Entra admin center, go to **Protection > Conditional Access**.
  2. Create a new policy and assign it to the desired users and groups.[1]
  3. Under **Access controls > Grant**, select **Require multi-factor authentication**.[1]
- **Per-User MFA (Legacy):** This method involves enabling MFA for individual users.[3] However, Microsoft is deprecating this method in September 2025 and recommends using Security Defaults or Conditional Access instead.[5]

Why MFA Works Even if it Shows Disabled (Security Defaults / Conditional Access):

You might observe that the per-user MFA status for an individual is "Disabled," yet they are still prompted for MFA. This occurs when either **Security Defaults** or a **Conditional Access** policy is enabled in your tenant. These modern authentication methods override the legacy per-user setting.[3][6]

- **Security Defaults:** When enabled, it applies a baseline security posture to all users, which includes enforcing MFA.[2][5]

- **Conditional Access:** Policies you create will enforce MFA based on the conditions you define, regardless of the per-user MFA status.[5][6]

Direct Link Options to Manage MFA and Security Defaults:

- **Manage Per-User MFA:** In the Microsoft 365 admin center, navigate to **Users > Active users > Multi-factor authentication**.[3]
- **Manage Security Defaults:** In the Microsoft Entra admin center, go to **Identity > Overview > Properties > Manage security defaults**.[3]
- **Manage Conditional Access:** In the Microsoft Entra admin center, go to **Protection > Conditional Access**.

2. Role-Based Access Control in Microsoft 365 (RBAC)

Role-Based Access Control (RBAC) is a security model that restricts user access based on their job roles.[7] This enforces the principle of least privilege, ensuring users only have the necessary permissions to perform their tasks.[7][8] This reduces the risk of accidental or malicious misuse of permissions.[7]

- **How it Works:** Instead of assigning permissions to individual users, you assign them to predefined roles.[7] These roles are then assigned to users.[9]
- **Implementation:** RBAC is implemented across various Microsoft 365 services, including Microsoft Entra ID (formerly Azure AD), Exchange Online, and Microsoft 365 Defender.[7][10]

3. Recording Calls and Messages in Teams

Microsoft Teams offers built-in features for recording calls and meetings.[11]

How to Record:

- During a call or meeting, click the **"..." (More actions)** icon and select **"Start recording."**.[11][12]
- All participants are notified that the recording has started.[11][12]
- Recordings are saved to the OneDrive of the person who initiated the recording.[13]

Auto-recording Teams Calls and Compliance Restrictions:

For regulatory compliance, manual recording is often insufficient.[14] True compliance recording must be automatic and tamper-proof.[14] This requires third-party solutions that integrate with Microsoft Teams.[14][15] These solutions can automatically record all communications, including calls, meetings, and chats, based on predefined policies.[16][17]

Certified Compliance Recording Providers:

Several Microsoft-certified providers offer robust compliance recording solutions for Teams. These include:

- NICE
- Verint[18]
- ASC[17][19]
- Smarsh
- AudioCodes[19]
- Red Box[19]
- CallCabinet[20][21]

4. Admin Access to Call Recordings and Teams Chat History

Admin Access to Recordings:

- By default, call and meeting recordings are stored in the OneDrive of the user who started the recording.[13]
- A SharePoint or Teams administrator can gain access to a user's OneDrive to retrieve recordings if necessary.[22]

Admin Access to Chat History:

- Yes, an administrator can access an employee's Teams chat history, including one-on-one and group chats.[23][24]
- This is typically done for compliance and security monitoring through the Microsoft Purview compliance portal's eDiscovery tools.[24][25]

5. Licensing and Costs for Compliance Recording

Implementing compliance recording involves several licensing components:

- **Microsoft 365 E3/E5 Licenses:**
  * A **Microsoft 365 E5** license provides a comprehensive suite of compliance features, including advanced eDiscovery, audit capabilities, and data loss prevention.[26][27][28]
  * While an **E3** license provides a solid foundation, the **E5** compliance add-on is often necessary for organizations with stringent regulatory needs.[29][30]
- **Advanced Communications Add-on:**
  * This add-on is required for third-party compliance recording solutions to integrate with Teams via APIs.[31][32]
  * The cost is approximately **$12 per user per month**.[31][32] Note that pricing may have been updated since initial announcements.[33][34][35]

- **Provider Fees:**
  * In addition to Microsoft's licensing, you will need to pay for the services of the certified compliance recording provider you choose. These fees vary depending on the provider and the specific features you require.