✓ 100 XP

Investigate the Microsoft Teams security model

6 minutes

As part of the Microsoft 365 suite of services, Microsoft Teams uses best practices and procedures to implement security.

Since the board of directors has made you personally responsible for security in your company's Teams roll out, you want to investigate Microsoft's approach to security and verify that it meets your needs.

Here, you'll learn how Microsoft Teams is designed to be secure. You'll also see common security threats and the Microsoft Teams security framework.

Trustworthy by design

Security is part of the design process for Microsoft Teams. It was developed to comply with the Microsoft Trustworthy Computing Security Development Lifecycle (SDL), which uses a series of security focused activities. SDL is a way of designing software so that it can withstand malicious attacks.

Security activities include developing threat models to test each Microsoft Teams feature, code reviews, and security testing during a focused "security push". There's a focus on security at each stage of the software development process. Multiple security-related improvements were built into the coding process and practices. While no system guarantees complete security, the SDL development process does produce systems with a lower rate of security vulnerabilities.

Microsoft Teams incorporates industry-standard security technologies as part of its architecture. Data is protected by encrypting network communications in Teams by default and requiring all servers to use certificates. Teams uses OAUTH, Transport Layer Security (TLS), Secure Real-Time Transport Protocol (SRTP), and other industry-standard encryption techniques, including 256-bit Advanced Encryption Standard (AES) encryption.

Common security threats

Microsoft Teams mitigates many common security threats. To mitigate the risk of encryption keys being compromised, Microsoft Teams uses the public key infrastructure (PKI) features in the Windows Server operating system. Microsoft Teams encrypts data in transit using Transport Layer Security (TLS) connections. The keys used for media encryptions are exchanged over TLS connections. To keep the keys safe, Teams uses PKI features.

A distributed denial-of-service attack (DDOS) occurs when the attacker prevents normal network use and function by valid users. Teams mitigates against DDOS attacks by running Azure DDOS network protection, and by throttling client requests from the same endpoints, subnets, and federated entities. This protection prevents attackers from pushing invalid data to applications and services, sending a large amount of traffic that overloads the system, and hiding the evidence of attacks.

Eavesdropping occurs when an attacker accesses the data path in a network and reads the network traffic. Teams uses Mutual TLS (MTLS) for server communications within Microsoft 365, and TLS from clients to the service. These precautions make this attack difficult within the time period in which a conversation could be compromised. TLS authenticates all parties and encrypts all traffic.

The **traversal using relays around network address translation (TURN)** protocol is used for real-time media. The Teams service ensures data is valid by checking the message integrity using the key derived from a few items. These items include a TURN password, which is never sent in clear text. Secure real-time transport protocol (SRTP) is used for media traffic and is also encrypted.

Spoofing occurs when the attacker uses an IP address of a network, computer, or network component without authorization. It allows the attacker to operate as if it were the entity normally identified by the IP address. TLS authenticates all parties and encrypts data in transit. TLS prevents an attacker from doing IP address spoofing on a specific connection, such as mutual TLS connections. An attacker could spoof the address of a Distributed Name Service (DNS) server but, as Teams uses authentication certificates, this would prevent an attack without a valid certificate.

See the **Security and Microsoft Teams** link in the **Learn more** section for details of other common threats.

Microsoft Teams security framework

The Microsoft Teams security framework helps to ensure that information and identities within Teams is protected. It has three core components:

- **Azure Active Directory (Azure AD)** functions as the directory service for Microsoft 365. It stores all user directory information and policy assignments.
- **TLS** and **Mutual TLS (MTLS)** are the protocols used by Teams to create a network of trusted servers. TLS and MTLS ensure that all communication over that network is encrypted. Communications between servers occur over MTLS, and any remaining or legacy SIP communications from client to server occur over TLS.
- **Industry-standard protocols** are used in Teams for user authentication, wherever possible. All three components work together to make sure data and identities are

protected.

Security for Microsoft Teams meetings

To make Teams meetings more secure, you control who can and can't automatically join a meeting. You also control who has access to the information you present. The first is controlled through settings for the lobby. The second is done through structured meetings. How the lobby works is determined by how you set meetings policies. You control who can join a meeting directly, and who has to wait in the lobby before being admitted. Amend the settings in the Microsoft Teams admin center > Meetings policies > Participants & guests > Automatically admit people. There are three choices: Everyone, Everyone in your organization, or Everyone in your organization and federated organizations:

Selection	Join the meeting directly	Wait in the lobby before joining the meeting
Everyone in your organization	In-tenant users and guests of tenant users	Federated, anonymous, and PSTN dial-in users
Everyone in your organization and federated organizations	In-tenant users, guests of tenant users, and federated	Anonymous and PSTN dial-in users
Everyone	In-tenant users, guest of tenant users, federated, anonymous, and PSTN dial-in users	-

Structured meetings allow the presenter to do everything needed to run the meeting. Presenters control what attendees do. The following table summarizes what each role can do:

Actions	Presenters	Attendees
Speak and share their video	Y	Y
Participate in meeting chat	Y	Y
Change settings in meeting options	Y	N
Mute other participants	Y	N
Remove other participants	Y	N

Actions	Presenters	Attendees
Share content	Y	N
Admit other participants from the lobby	Y	N
Make other participants presenters or attendees	Y	N
Start or stop recording	Y	N
Take control when another participant shares a PowerPoint	Y	N

Learn more

- Microsoft Security Development Lifecycle
- Securing Public Key Infrastructure (PKI)
- Security and Microsoft Teams

Next unit: Manage security and compliance for Microsoft Teams

Continue >