# MiTeam Meetings

## SECURITY GUIDELINES

**NOTICE**

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.



TRADEMARKS



DISCLAIMER





MiTeam Meetings
June 2021

# Contents

# Overview

This document provides an overview of the security mechanisms that protect the MiTeam Meetings solution from network threats and maintain user data privacy. This document will be of interest to personnel who are responsible for ensuring the secure deployment and the secure operation of the MiTeam Meetings solution.

Mitel has a clearly defined IT security policy in place that defines goals, assets, trust levels, processes, and incident handling procedures. The security mechanisms implemented in the MiTeam Meetings solution are covered by and configured according to this policy. Security is an integral part of the MiTeam Meetings system design.

This document describes the Mitel Meetings security features that are designed to ensure a secure MiTeam Meetings deployment. MiTeam Meetings actively monitors for suspicious activities to address brute force attempts into the system. The MiTeam Meetings solution provides services that are designed to operate securely, which have security features that address identity, authentication, encryption, access, and authorization. The security features are mainly based on the following open standard technologies and access management mechanisms:

- Secure by Design: MiTeam Meetings is designed and developed using the Mitel Secure Development Life Cycle process. For more information, see the Mitel Secure Development Life Cycle whitepaper at Mitel Document Center.
- Secure by Default: Data in transit is encrypted by default using Transport Layer Security (TLS 1.2) and Web Real-Time Communication (WebRTC) protected by 256-bit or higher Advanced Encryption Standard (AES) encryption. Data at rest is protected by 256-bit Advanced Encryption Standard (AES) encryption.
- Built on Secure Platforms: MiTeam Meetings is empowered by services provided by Mitel’s CloudLink platform, Amazon Web Services (AWS) Chime SDK, AWS Pinpoint, and Bugsnag.
- Identity Access Management (IAM): CloudLink IAM uses CloudLink’s native IAM solution, which supports Open ID Connect 1.0 and OAuth 2.0. For information about identity access control, see the section Identity Access in this document.

The MiTeam Meetings solution has been designed in accordance with Mitel's Secure Development Life Cycle (MiSDLC). For details of MiSDLC, see the section Secure Development Life Cycle in this document.

# What is MiTeam Meetings?

MiTeam Meetings is a multi-party video meeting solution designed for users who want to improve work efficiency and enhance workplace communication with seamless transitions between voice, video, and chat capabilities. It enables users to access features such as:

- Collaborate: Perform audio, video, and web sharing
- Chat: Hold chat sessions and receive chat notifications within a meeting
- File Sharing: Store and share files
- Recordings: Record collaboration sessions

# About the MiTeam Meetings Documentation Set

Documentation for all Mitel® products are available at Mitel Document Center. For complete information about MiTeam Meetings Desktop and Web application, see MiTeam Meetings Online Help. For complete information about MiTeam Meetings Mobile application, see MiTeam Meetings Mobile Online Help.

## Additional Security-Related Documentation

### CloudLink Solutions Documentation

- While it is the responsibility of the CloudLink platform to protect the customer's data stored in the platform, Mitel applications are responsible for protecting the customer's data stored in the application. Customers are responsible for using the CloudLink user access controls to ensure that only authorized individuals are granted access. For a general security overview of the CloudLink Platform, see the CloudLink Security FAQ.

- For security details around the Chat Service powering MiTeam Meetings, see the CloudLink Chat Security Whitepaper.

### Documentation Related to AWS Chime SDK

- For information about the security aspects of the conferencing service used by MiTeam Meetings, see https://aws.amazon.com/chime/chime-sdk/.

### Documentation Related to AWS Pinpoint and Bugsnag

- Product improvements and quality is crucial to Mitel for providing the best experience to our customers. MiTeam Meetings uses the AWS Pinpoint and Bugsnag cloud services to give insight on what the next feature improvement should be and what bugs are priority to fix.

  For information about the security aspects of these services, see https://docs.aws.amazon.com/pinpoint/latest/developerguide/security.html.

# Product Architecture

MiTeam Meetings is Mitel's premier video conferencing and collaboration solution. It is a CloudLink- based multi-party video solution designed for MiCollab users who want to improve work efficiency and enhance workplace communication. The end-user experience is realized through a desktop, web, or mobile client delivering chat, video conferencing, or screen sharing. Users who have only PSTN access may join the meeting as voice-only participants.

Following is a schematic diagram of the MiTeam Meetings product architecture.

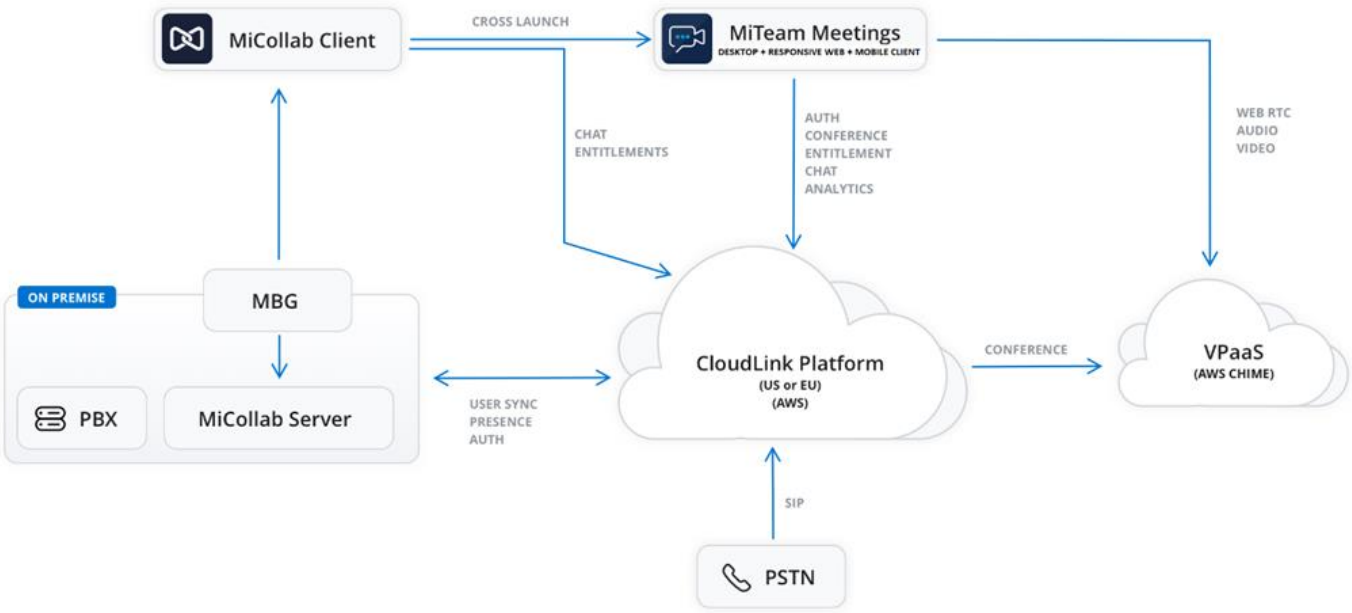


*Figure 1 Product Architecture*

**MiTeam Meetings Product Architecture**

MiTeam Meetings is empowered by services delivered by the CloudLink platform (chat, authorization and authentication, and dialing into meetings from the PSTN) and AWS Chime SDK (video conferencing and screen sharing).

MiTeam Meetings uses IP networks to transport data such as file sharing and audio, video, and chat streams.

# Client Security

The security framework for the MiTeam Meetings solution include:

- Data in transit is encrypted by default using Transport Layer Security (TLS 1.2) and Hypertext Transfer Protocol Secure (HTTPS) to provide secure endpoint authentication, IM, and file sharing.
- Web Real-Time Communication (WebRTC) is protected by 256-bit or higher Advanced Encryption Standard (AES) encryption.
- Secure Real Time Protocol (SRTP) to secure media streams associated with PSTN access. 128-bit AES encryption is used to encrypt data in transit.
- Data at rest is protected by 256-bit AES encryption.
- CloudLink Identity Access Management (IAM) to provide a single trusted location for users. CloudLink IAM uses CloudLink's native IAM solution, which supports Open ID Connect 1.0 and OAuth 2.0.

Users are forced to change the default password provided in the welcome email that they receive for initializing the application. The password must contain:

- between 8 and 128 characters
- at least one special character (@ ! # $ % & _ - = +)
- at least one digit
- at least one uppercase letter and one lowercase letter

# Shared Responsibility Model

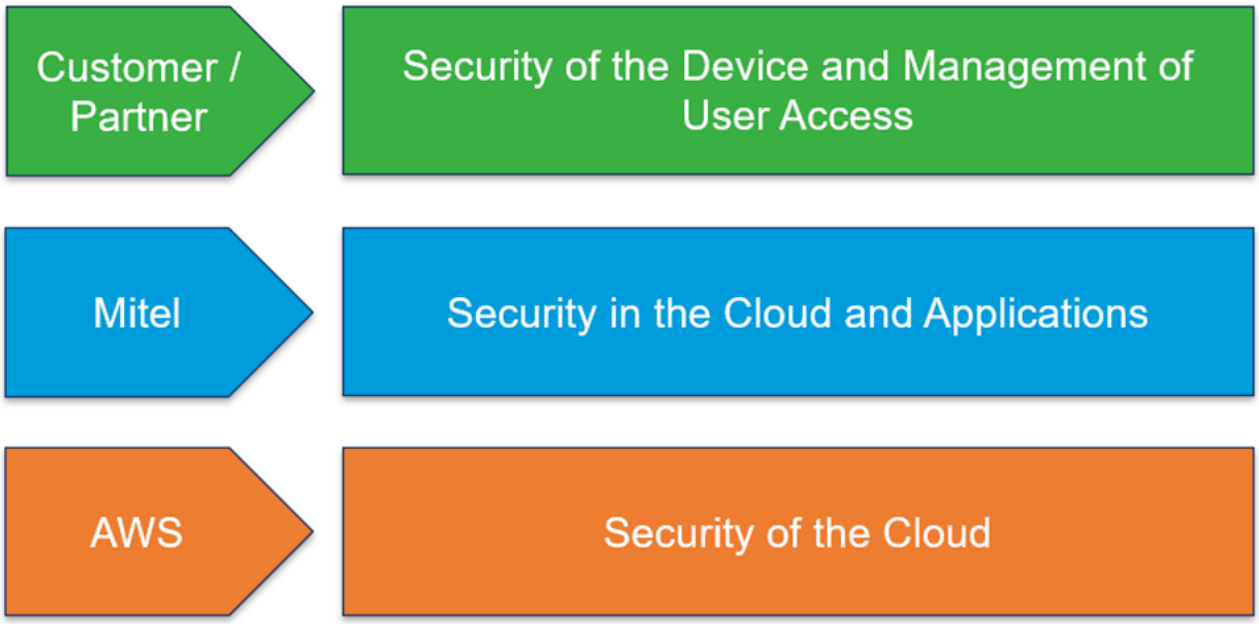


*Figure 2 Shared Responsibility Model*

The shared responsibility model is discussed in the CloudLink Chat Security document.

The Shared Responsibility Model is based on the AWS Shared Responsibility Model ("Shared Responsibility Model - Amazon Web Services (AWS)" Amazon Web Services (AWS) - Cloud Computing Services, Amazon.com, Inc., 3 August 2020.) since it is the Platform as a Service provider for CloudLink. As defined by the model, AWS is responsible for the "Security of the Cloud". Mitel is responsible for Security in the Cloud for the aggregate services and applications that Mitel provides. The customer/partner also has a key role in that they are responsible for the security of their own devices and the access they provide their users on those devices. Mitel recommends that the customer/partner fully understand and apply the best security practices as stated by the device manufacturer and Operating System supplier.

# Identity Access

Identity Access Control is also a shared responsibility between the CloudLink platform, Mitel Applications and the customer. The CloudLink platform is responsible for ensuring secure access to the AWS foundation services used by the CloudLink platform, restricting such access to Mitel employees, and limiting it to their job function. The best practices employed include the use of AWS Organizations, Role Based Access Control (RBAC) for limiting access to job functions of personnel, Multi-Factor Authentication for accessing AWS infrastructure, and dedicated security accounts in AWS (to ensure security events are monitored by the correct personnel).

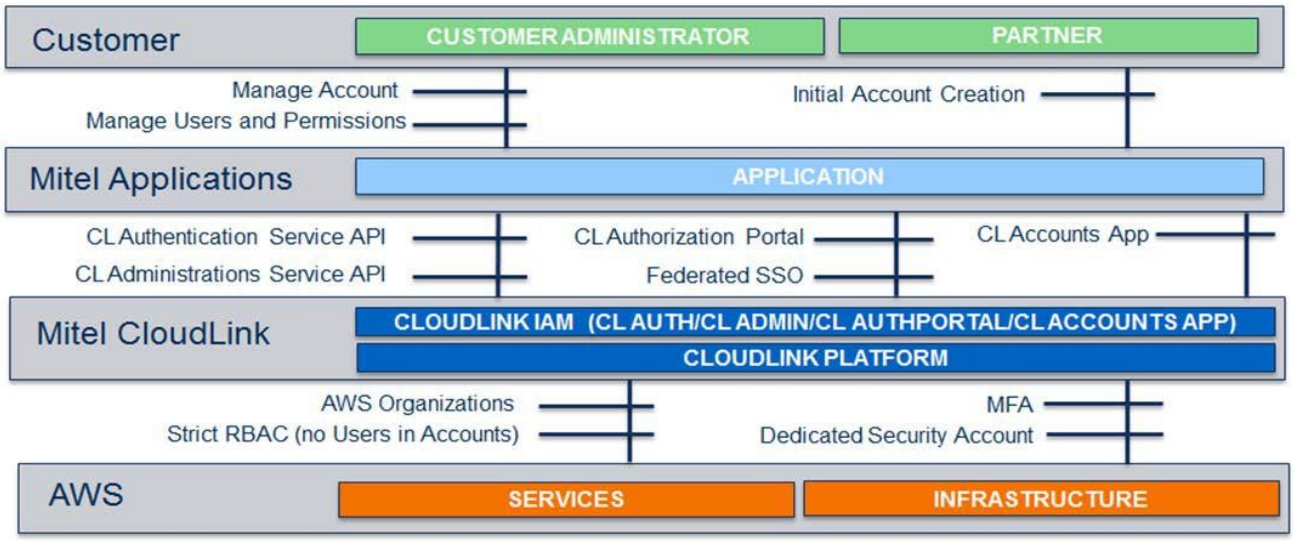


*Figure 3 Identity Access*

**Identity Access Management in the Shared Responsibility Model**

Mitel applications are designed to ensure that identity and access for the accounts and users of that application are properly reflected within the CloudLink platform. The Mitel application performs these functions through secure APIs provided by the CloudLink Identity Access Management (IAM) solution, which is designed to ensure access to the services and data is isolated to the appropriate account and limited to the responsibilities of the users defined by the customer.

The CloudLink IAM solution is an open solution supporting Open ID Connect 1.0 with support for federated single sign-on (SSO) using SAML 2.0. The CloudLink IAM solution offers a common login portal (CloudLink Authorization Portal) which the Mitel application can redirect to for its SSO requirements.

The partner/customer is responsible for managing the account, users, and permissions within the Mitel Application.

**NOTE**: A Mitel partner is required to initially create the customer account in CloudLink from the CloudLink Accounts Application, which can be launched via MiAccess.

# Managing Meetings

MiTeam Meetings enables entitled users to create and join multi-part video conferences and to invite guest users and registered users. Additional safeguards to protect meetings are described in the following sections.

## Types of Participants

**Registered User**: a licensed MiTeam Meetings user (that is a user who has been provisioned for MiTeam Meetings services by an account administrator of the entity who subscribes to MiTeam Meetings). Registered users can create and schedule meetings. They can also verify guest users in the waiting room to allow them to join meetings, remove a user from a meeting, and invite more users into a meeting while it is active. registered users can video meeting, chat, and share files and their screen.

**NOTE**: You cannot share your screen if you are using MiTeam Meetings mobile application.

**Guest User**: an unlicensed MiTeam Meetings user (that is a participant who has not been provisioned for the MiTeam meetings service or is not currently logged in to the service.). A guest user joins the meeting through the Web according to directions from the meeting invite they receive and must wait in the waiting room until a registered user allows them entry. Guest users can video meeting, chat, and share files and their screen.

**PSTN User**: A user who has only PSTN access can join a meeting as a voice-only participant by using an advertised access dial-in number specified in the meeting invite.

**Organizer**: The registered user who creates the meeting.

**Invited Participant**: A registered user that has been invited to attend a meeting by an organizer.

**Attended Participant**: A registered user or guest that has attended a meeting.

## Waiting Room

Guest users must first wait in the Waiting Room, which is a temporary parking spot outside of the meeting. This allows any registered user to verify guest users before allowing them into the meeting by vetting the identity information which the guest provided.

**NOTE**: Waiting Room feature is currently not available in MiTeam Meetings mobile application.

## Naming Meetings

It is highly recommended that a meeting be given a unique humanly identifiable name that is easy to remember for the participants. This will enable registered users to easily identify which meeting space to use for their collaboration and facilitate meeting searches.

**CAUTION:**

- Customers should exercise caution to prevent accidental disclosure of Meeting Access Codes.
- Mitel recommends that at least one participant in a meeting use the Mitel Meetings client to provide visibility to other participants in the meeting.

## Meeting Lifecycle

MiTeam meetings comprise a virtual collaboration space (the “meeting space”) and 0 or more live audio, video and/or screen sharing collaboration sessions (“live sessions”), which can be recorded. Both the meeting space and the live session have a unique URL.

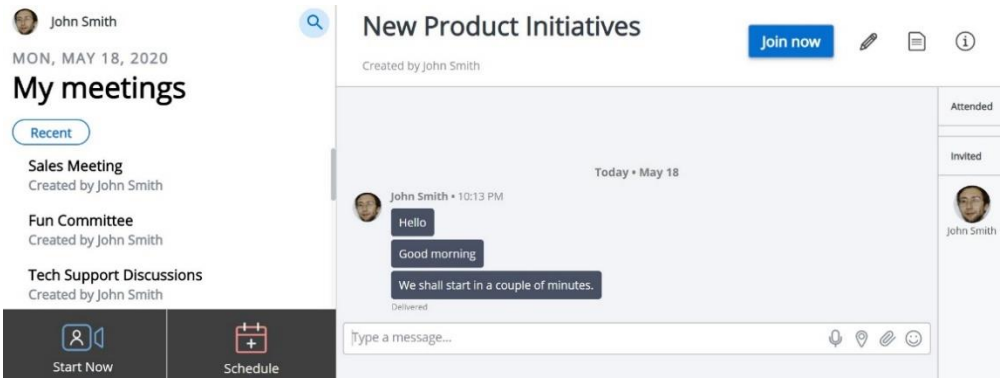


*Figure 4 Meeting Space*

A meeting space consists of a meeting name, participants, a chat conversation, and files from live sessions. Each meeting space is identified by a unique sequence of nine or more digits (“access code”).

A meeting space is created when the organizer schedules a meeting in the calendar or can be created on an ad hoc basis at any time. In the meeting space, the registered user can schedule and join live sessions, discuss topics via chat, share files, and access recordings of live sessions (chats, shared files, and recordings are individually and collectively “content”).

Invited participants can collaborate in the meetings space prior to the live session, for example the invited participant may attach documents or seed the chat conversation with initial messages.

Meetings are listed on the home page of the organizer as well as home page of invited or attended participants. The registered user can hide meetings so that they no longer appear in the list. The organizer can delete meetings which deletes all the content associated with the meeting. Hiding a meeting does not delete it.

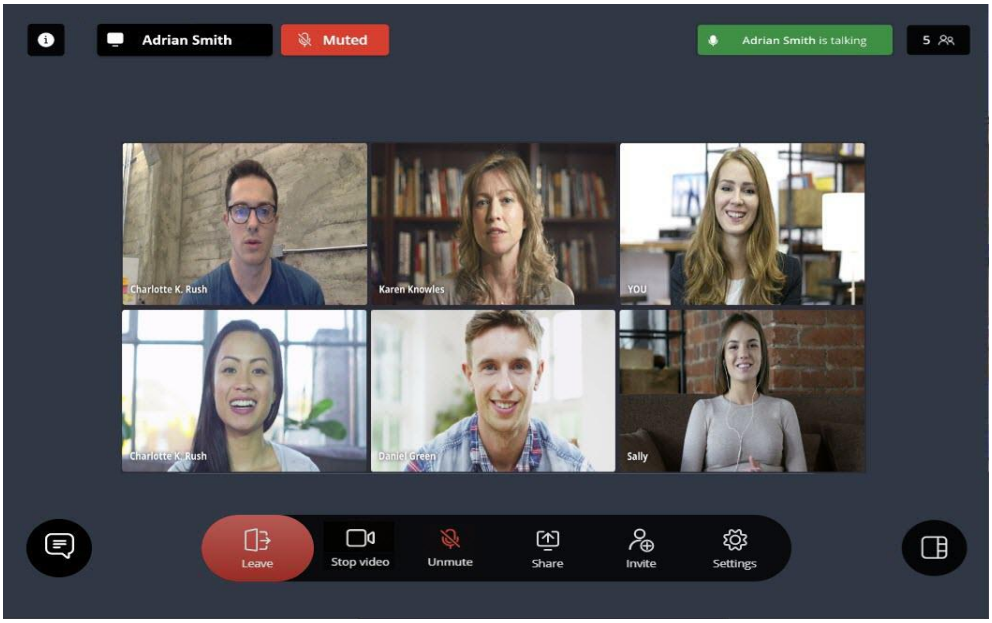


*Figure 5 Live Session*

All live sessions occur at the same URL. The meeting space URL and live session(s) URLs individually and collectively are referred to as the “meeting URL”. The meeting access code is part of the meeting URL.

Live sessions have a maximum duration of 24 hours.

Content is mirrored between the meeting space and live sessions, where it is available for read/write purposes. Ending a live session does not end or delete the meeting.

Meeting do not have an expiration date. Meetings spaces, including the live session URL (and the live sessions themselves), are deleted only if the organizer deletes the meeting, or the corporate account which the organizer belongs to is terminated. Content is deleted only as set out below.

## Access to Meeting Space

Any registered user who obtains a meeting URL or has a meeting access code can enter the meeting space or a live session, as the case may be, at any time. By contrast a guest, who can enter only into a live session, is taken to the waiting room and can enter only a live session upon acceptance by a registered user who is already in the live session.

## Chat

- All messages are accessible to all registered users via the meeting space as well as all registered users and guests in live sessions.
- Unless disabled by the corporate administrator, chat messages can be edited and/or deleted by the sender. The Edit/Delete feature is enabled by default. If another registered user(s) or guest had replied to a message that is being deleted, the original content of the message is still retained in the reply.
- Unless deleted by the sender, chat messages remain in the meeting space until the meeting space is deleted by the organizer.
- Edits are accessible to all participants in the meeting space and live session.

## Attachments

- All shared files are accessible to all registered users via the meeting space and registered users and guests in live sessions.
- Shared files remain in the meeting space until the meeting space is deleted by the organizer.

## Recordings

- Recording can be initiated by any registered user in a live session.
- Only the registered user who initiated the recording can stop the recording.
- When a recording is initiated, all participants are notified including those attending by telephone only. Notifications are presented to new attendees who join a meeting where recording is in progress.
- Recordings are accessible to all registered users via the meeting space and to all registered users and guests during live sessions.
- Any registered user or guest with access to a recording can download the recording for offline viewing and share the downloaded files with others.
- The maximum space available to a registered user in cloud to store the recordings is 5 GB.
- There is not limit on the duration of recordings.
- Effective July 1. 2021, recordings will remain in the meeting space until the earlier of 12 months from the recording date, or the meeting space is deleted by the organizer. Recording made prior to July 1, 2021 will remain in the meeting space until the earlier of 12 month from July 1, 2021 or the meeting space is deleted by the organizer.

## Audit Logs

- For security and regulatory purposes, Mitel may capture the following types of meeting metadata: Initiator’s and each participants’ name & username (as applicable), phone number & IP address and port as applicable, location, conference date, time & duration, chat, chat edit, chat delete date and time, location, network path, details of any files exchanged including file size, file edits and deletes, call recording size, start, stop, and deletion & location of system used.

## Security and Privacy

- For security and privacy purposes, it is recommended
    - not to re-use meetings unless the meeting is a re-occurring meeting with the same group of participants. The reason is that content is accessible to all participants and if the meeting is re-used for a different purpose and/or with a different group of participants, there may be details in the content that should not be shared across groups. Also new participants will have access to previous recordings.
    - consider deleting the meeting after the live session has finished and any attachments/recordings have been downloaded by any participants that need those artifacts.
    - consider deleting files, recordings, and chat messages appropriately to address invitee and attendee changes.
    - assess whether it is appropriate for participants to be able to edit/delete messages and set admin setting accordingly.

## Storage Location[1]

Meetings (and all chats, and files in a meeting) and Audit Logs are stored as follows:

| Account Cloud Region | Storage Location |
|---|---|
| Europe/EEA | Europe/EEA |
| United States | United States |
| Canada | United States |
| Australia | Australia |

[1]Location set out herein are default locations but are not absolute.

# Hosts and Ports Required to Support MiTeam Meetings

For authentication, chat, and file sharing requirements:

- Host: *.mitel.io, *.amazonaws.com, fonts.gstatic.com
- IP address: N/A
- Port:  TCP/443, UDP/3478

For audio, video, and screen sharing requirements, see https://answers.chime.aws/articles/123/hosts-ports-and-protocols-needed-for-amazon-chime-sdk.html.

Audio, video, and screen sharing are empowered by AWS Chime SDK, which uses Amazon Elastic Compute Cloud (Amazon EC2) and other AWS services including AWS Pinpoint on port TCP/443. Include *.amazonaws.com on an allow list for port TCP/443. Request to the Google fonts are made to the domain fonts.gstatic.com. Bugsnag and Google fonts also use port 443.

Web sockets used in the solution also require an entry in the allowed list for *.amazonaws.com for the ports defined here: https://docs.aws.amazon.com/iot/latest/developerguide/protocols.html.

# Audio Considerations with Windows and MacOS

Personal computers and laptops running Microsoft Windows or MacOS natively share microphones between applications that can stream to the same output. Users must exercise caution when using MiTeam Meetings in a scenario where apart from the communication application being used for the meeting, other communication applications such as softphone applications in their device are active at the same time. The microphone audio stream may be played into the MiTeam Meetings application and into the other communication applications under certain conditions. In addition, the audio output of MiTeam Meetings and another communication application(s) may be joined at the meeting's communication application if the other communication applications are using the same audio output device setting as that of the meeting's communication application.

## Receiving a Call on a local Softphone Application and Maintaining the Meet Session

Though it is not recommended that a user participate in a MiTeam Meeting session and at the same time communicate on a local softphone session, the following tips will help guard the user's privacy in such a scenario:

- Ensure that the MiTeam Meetings session is muted during the softphone call
- If the user does not want to hear the audio of the MiTeam meeting session during the call, it is recommended that the user disconnect the audio output of the MiTeam Meetings application via settings while the softphone call is active. To do this, users can set their speaker setting to **None**.

# Product Hardening for Security during Development

The following section describes the product security hardening steps that were taken during the MiTeam Meetings client application development cycle.

- MiTeam Meetings software has been written in such a way that it does not use privileged (administrative) accounts.
- All unnecessary diagnostic and debug software have been removed from the released version of the MiTeam Meetings software.
- The software delivery process and change management policy are extensively automated through multiple CI/CD pipelines for deployment into staging and production environments. The automated process includes code reviews and execution of automated testing and supports the separation of duties. Security best practices are implemented through configuration options to ensure that the application is secure every time it is built and deployed.

## In-House Product Security Verification

MiTeam Meetings regularly undergoes Software Composition Analysis and Vulnerability scans by using scanners such as Nessus and AppScan.

# Secure Development Life Cycle

Security and privacy threats are constantly increasing, and existing threats are fast evolving. To combat these threats, product designers need to continuously evaluate product security risks and ensure that robust controls are included in the design. The practice of evaluating security risks and incorporating protective measures in the design must be an integral part of the product design process itself.

Mitel's Secure Development Life Cycle (MiSDLC) policy was created to ensure that product developers will employ the latest information security and privacy best practices throughout the product development process.

MiTeam Meetings was developed in accordance with Mitel's Secure Development Life Cycle policy, which is designed to ensure that MiTeam Meetings is designed with best practice safeguards to mitigate risks to confidentiality, integrity, and/or availability of data contained within MiTeam Meetings and to all data related to the functionality provided by MiTeam Meetings.

# Product Security Information

## Mitel Product Security Vulnerabilities

The Product Security Policy discusses how Mitel assesses security risks, resolves confirmed security vulnerabilities, and how the reporting of security vulnerabilities is performed.

Mitel's Product Security Policy is available at:

www.mitel.com/support/security-advisories/mitel-product-security-policy

## Mitel Product Security Advisories

Mitel Product Security Advisories are available at:

www.mitel.com/support/security-advisories

# Appendix A – Definitions and Glossary

**AES: Advanced Encryption Standard.** A specification for electronic data encryption adopted by the U.S. government to protect classified information. The algorithm used by AES is a symmetric-key algorithm; that is, the same key is used for both encrypting and decrypting the data.

**Audit trials**: A series of documents, computer files, and other records that are periodically examined to track how transactions are handled and to identify conditions that call for actions to be taken.

**Authentication**: The process by which a system ascertains that a person or entity trying to access it is actually the person or entity it claims to be.

**AWS Chime SDK**: The Amazon Chime SDK is a set of real-time communications components that developers can use to quickly add audio calling, video calling, and screen sharing capabilities to their own applications.

**Guest user**: With regard to MiTeam Meetings, a guest user is an unregistered user attending a meeting. A guest user joins the meeting through the Web according to directions from the meeting invite they receive and must wait in the waiting room until a registered user allows them entry.

**HTTPS**: Hypertext Transfer Protocol Secure. It is the secure version of the standard Hypertext Transfer Protocol, the protocol that web browsers use for communicating with websites.

**Network threats**: Attempts by attackers to execute commands designed to intercept traffic traversing a network or to disrupt normal operation of a network. These attacks typically involve breaching a company's infrastructure by exploiting software vulnerabilities to execute such commands.

**Open ID Connect**: An authentication protocol that enables clients to verify the identity of the end-user based on the authentication.

**Open standard technologies**: Technologies based on open standards. *Open standards* are *standards* available to the general public (in contrast to propriety standards) and are developed, approved, and maintained through a collaborative and consensus based process.

**Product hardening**: The process of reducing vulnerability in applications, systems, infrastructure, firmware, and other areas by pre-empting potential attack vectors and limiting the system's vulnerability surface. Reducing vulnerability typically includes changing default passwords; removing unnecessary software, user names, or logins; and disabling or removing of unnecessary services.

**PSTN**: Public Switched Telephone Network. It comprises all of the world's communication infrastructure including systems, devices, transmission lines, and networks, interconnected through switching centers to enable telephones to communicate with one another.

**PSTN user**: With regard to MiTeam Meetings, a PSTN user is a user who dials in to a meeting using a phone. A PSTN user can join a meeting only through audio and only from the Public Switched Telephone Network by using an advertised access dial-in number specified in the meeting invite.

**Registered user**: With regard to MiTeam Meetings, a registered user is a licensed user registered in CloudLink and belonging to a specific registered account. A registered user can create and schedule

meetings. They can validate a guest user, who only then can join a meeting, remove a user from a meeting, and invite more users into a meeting while it is active.

**SDLC**: Secure Development Life Cycle. An application development approach in which security is treated as a continuous concern in all phases of application development. In SDLC, security-related procedures such as penetration testing, code review, and architectural analysis are an integral part of the development schedule.

**TLS**: Transport Layer Security. A security protocol that provide privacy and data security for communications over the Internet. TLS encrypts all communication between web applications and servers. TLS can also be used to encrypt other communications such as email, chat, and Voice over IP (VoIP).

**Waiting room**: A temporary parking spot outside of a meeting where Guest users must wait until any Registered user verifies them allowing them entry into the meeting.