MiVoice Office Web Application

RELEASE 1.0.0

VERSION 1

SECURITY GUIDELINES

DISCLAIMER

This document is ‘as is” and “as available”. Mitel Networks™ Corporation and its affiliates make no any warranty of any kind whether express or implied (including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose) in respect of the information found herein or the products discussed herein. This document, and any product discussed herein, are subject to change without notice and this document should not be construed in any way as a commitment by Mitel or any of its affiliates. Revisions of this document or new editions of it may be issued to incorporate changes including changes in product. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation. NEITHER MITEL NETWORKS CORPORATION NOR ITS AFFILIATES SHALL HAVE ANY LIABILITY WHATSOEVER ARISING FROM OR RELATING TO THIS DOCUMENT.

TRADEMARKS

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

MiVoice Office Web Application

Version 1

August 2020

Contents

Overview

This document provides an overview of the security mechanisms used to protect the MiVoice Office Web Application 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 MiVoice Office Web Application.

Security is an integral part of the MiVoice Office Web Application system design. This document describes the security features used to ensure a secure MiVoice Office Web Application deployment; services that are designed to operate securely, address identity, authentication, encryption, access, and authorization.

MiVoice Office Web Application is a desktop web browser application that allows the user to communicate (voice, messaging, presence, user directory) with other web app users in the same company account. The web app also allows users to make and receive external voice calls and utilizes the Mitel CloudLink Platform for such communication and in turn relies on the security features offered by this platform. The Mitel CloudLink Platform security features include application user authentication and authorization, secure Cloud API access, protected cloud data used by the application, encrypted signaling, secure event notifications, and secure application software logs reporting.

The MiVoice Office Web Application (web app) strives to locally store as little solution and user data as possible. Examples of such data include call history, directory contacts, user favorites on the web app home screen, inbox communication / messages, user presence, user profile and settings. The web app allows each user to view cloud data and to activate cloud services executed in the cloud.

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 MiVoice Office Web Application solution are covered by and configured according to this policy. The security features are based on the following open standard technologies and access management mechanisms:

- Secure by Design: The MiVoice Office Web Application is designed and developed using the Mitel Secure Development Life Cycle process. For more information, see the Mitel Secure Development Life Cycle whitepaper available on the Mitel Document Center at https://www.mitel.com/en-ca/document-center/security/technical-papers
- Secure by Default: Data in transit is encrypted by default using Transport Layer Security (TLS 1.2 or later) 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 or higher Advanced Encryption Standard (AES) encryption in Amazon Web Services cloud.
- Built on a Secure Platform: The MiVoice Office Web Application is empowered by services provided by Mitel's CloudLink platform. See https://www.mitel.com/en-ca/document-center/technology/cloudlink-security for more details.
- Identity Access Management (IAM): Mitel's CloudLink IAM solution supports Open ID Connect 1.0 and OAuth 2.0. For information about identity access control, refer to the Identity Access section later in this document.

MiVoice Office Web Application Documentation

For complete information about the MiVoice Office Web Application, refer to https://www.mitel.com/en-ca/document-center/technology/cloudlink/all-releases/en/mivoice-office-web-html.

Documentation for all CloudLink products is available at https://www.mitel.com/document-center/technology/cloudlink.

Other Mitel® product documentation is available in the Mitel Document Center.

Additional Security-Related Documentation

To learn how the CloudLink platform protects customer data stored in the platform, refer to https://www.mitel.com/en-ca/document-center/technology/cloudlink-security.

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, refer to the CloudLink Security FAQ.

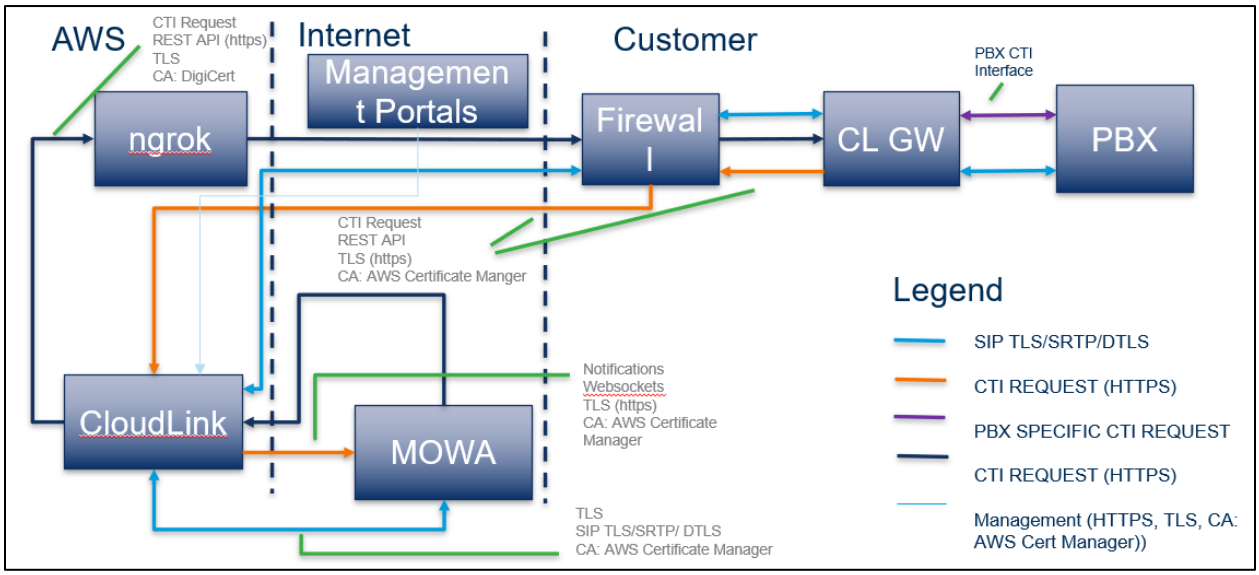
For security details related to the Chat Service powering MiVoice Office Web Application, refer to the CloudLink Chat Security Whitepaper.

For MiVoice Office Web Application security guidelines, refer to the respective security guidelines document at https://www.mitel.com/en-ca/document-center/security/technical-papers.

Product Architecture

The MiVoice Office Web Application is a CloudLink-based voice and messaging solution designed for users who want to improve work efficiency and enhance workplace communication. The end-user experience is realized through a Progressive Web Application (PWA) or Web Application delivering voice, messaging (Direct messages and Streams), user presence, call history, cloud directory, home screen favorites, and so on.

The following is a schematic diagram of the MiVoice Office Web Application solution architecture.



The MiVoice Office Web Application (MOWA) uses services provided by the Mitel CloudLink platform (CloudLink) including voice, chat, cloud user directory, user presence, user call history, user authorization and authentication. The Mitel CloudLink platform utilizes AWS to offer customers a Platform as a Service (PaaS). MOWA uses the internet to transport data related to voice, files, audio, and chat. Internet access to Mitel's cloud services hosted in Amazon Web Services (AWS) The Management Portals are used to administer the overall solution including creating company and user accounts.

Application users, Mitel employees and administrator access to the AWS PaaS follows a principle of least privilege. Practices of strict Role Based Access Control (RBAC) and Multi-Factor Authentication (MFA) are implemented at the Identity Access Management (IAM) level in AWS. The RBAC implementation ensures that the correct individuals have access only to the appropriate tenant data. Identity Access Management (IAM) utilizes the Open ID Connect 1.0 protocol and OAuth 2.0.

The Mitel CloudLink platform implements user password rules derived from NIST 800-63. Users are forced to change the default password provided in the welcome email that they receive for accessing the application on initial login. 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.

The Mitel CloudLink Gateway connects the on-site Mitel communication system (PBX) to the Mitel CloudLink Platform (noted as CL GW in the above diagram).

The CloudLink's three primary access roles are described as follows:

Role	Access
Mitel Partner System Administrator	Access and management to tenants managed by the partner
Customer System Administrator	Access and management to tenant where customer admin is employed
Application End User	Access and management to individual user account

A Mitel CloudLink Gateway web portal (Management Portal) is used during the provisioning process and registers the Mitel CloudLink Gateway with Mitel CloudLink Platform. An Accounts Console is used to create a customer account. For more details, see CloudLink Accounts documentation.

The Mitel CloudLink Platform implements industry standard defenses to protect against Man-in-the-Middle (MitM) attacks using Transport Layer Security (TLS 1.2 or later) for encrypting data in transit. CloudLink service certificates are verified by the MiVoice Office Web Application. CloudLink certificates are provided and managed by the AWS Certificate Manager service. Access to resources on CloudLink from the MiVoice Office web Application or the CloudLink Gateway, is managed centrally through the CloudLink Authentication Service.

Communication between the secure CloudLink Platform and the CloudLink Gateway is powered by a tunneling service provided by ngrok which exposes local servers behind NATs and firewalls to the public internet over secure tunnels. For more information regarding the security details for ngrok, see ***"ngrok – documentation." ngrok - secure introspectable tunnels to localhost, ngrok, 4 August 2020 https://www.ngrok.com.***

ngrok provides a certificate from DigiCert which is verified by both ends of the connection (the CloudLink Platform and the CloudLink Gateway) to prevent spoofing. Protecting against MitM attacks when

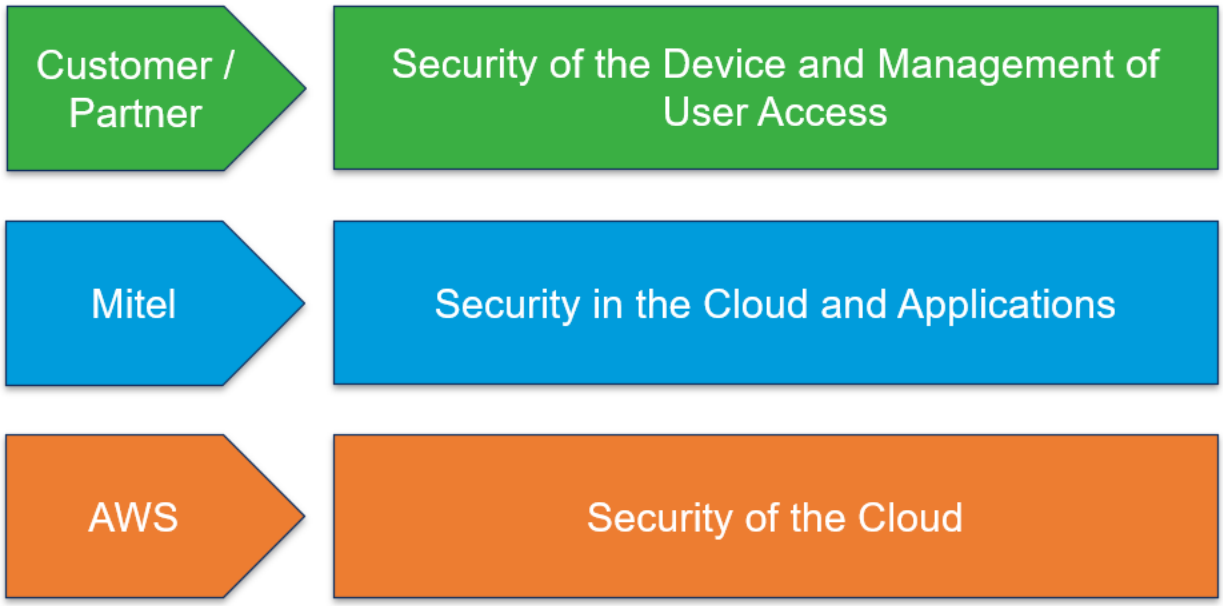
establishing a communication channel through the ngrok tunnel is described below along with tenanting and privilege escalation protection.

Web Application Communication Security

The security framework for the MiVoice Office Web Application solution includes:

- Data in transit is encrypted by default using Transport Layer Security (TLS 1.2 or later) and Hypertext Transfer Protocol Secure (HTTPS) is used to provide secure endpoint authentication.
- Web Real-Time Communication (WebRTC) is protected by Advanced Encryption Standard (AES) 256-bit encryption.
- Secure Real Time Protocol (SRTP) is used to secure media streams (AES 256 encryption).
- Data at rest is protected by AES 256 encryption.
- CloudLink Identity Access Management (IAM) is used 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.

Shared Responsibility Model

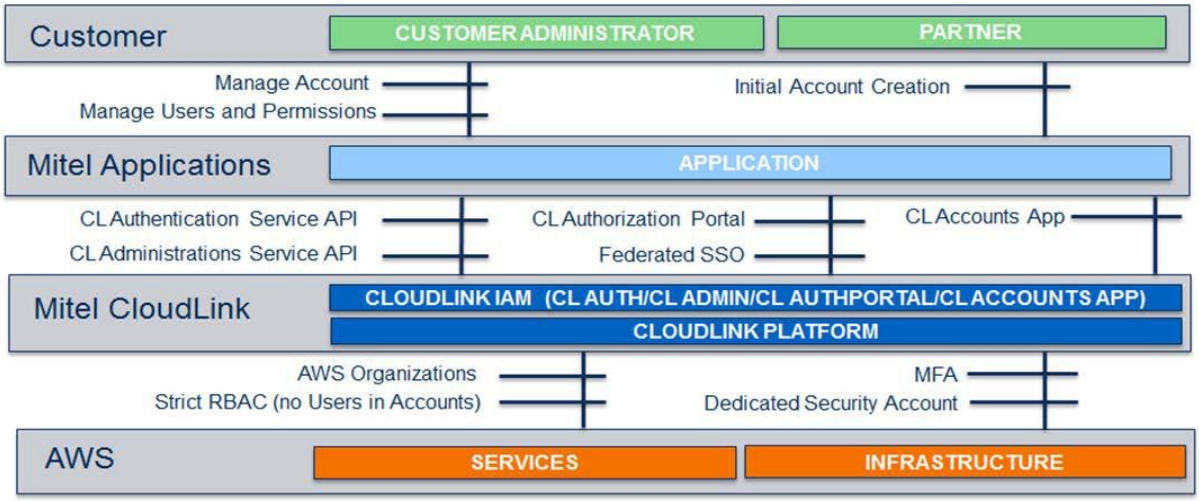


The shared responsibility model is discussed in the CloudLink Security FAQ.

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 utilizes 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 access to a specific 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).



Mitel applications are designed to ensure that identity and access related to application accounts and users are accurately reflected within the CloudLink platform. The Mitel application performs these functions through secure APIs provided by the CloudLink Identity Access Management (IAM) solution. The IAM solution is designed to ensure access to 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 based on 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 uses for SSO requirements.

The partner/customer is responsible for managing the company account, users, and permissions to the overall solution.

NOTE: A certified Mitel partner is required to initially create the customer account in CloudLink from the CloudLink Accounts Application. All cloud data used in the web application is stored on the Mitel CloudLink platform and is identified with company account ID, user ID and other globally unique identifiers associated with a fully authenticated and verified account.

MiVoice Office Web Application Solution Management

The MiVoice Office Web Application solution enables entitled users to communicate in different ways with other application users. Safeguards to protect the application user are described in the following sections.

Type of Application User:

All MOWA users have the following type: Cloud App user. A system administrator must invite a user by email to complete their user account before the user can access the web application. A MOWA user can use all features available in the web application. Before gaining access to such features in the web application the user must authenticate with the cloud. When a user's browser accesses the CloudLink

Login web page they are presented a page requesting username and password. The MOWA user must remember their own password as this information is not stored in their device.

To be able to use the MiVoice Office Web Application each system administrator must also be aware of the URLs the web app uses and ensure that the IP network ports required by the overall solution are open.

The open port list for the CloudLink Gateway at the customer's site to AWS is as follows:

- 22 - TCP
- 80 - TCP
- 8086 - TCP
- 5060 – TCP and UDP
- 5061 - TCP
- 65336-65534 - UDP

The open port list for Cloud Media Services is as follows:

- 5060 - UDP
- 5061 - TLS
- 7443 - TLS
- 16384-32768 UDP (RTP/SRTP)
- ICMP
- TCP/443, UDP/3478

The open port list for all cloud services with API CloudLink Gateways are as follows:

- Https/443
- Http/80: gets 301 redirect to 443 and https.

The web app uses URLs:

- *.mitel.io
- *.amazonaws.com

Web sockets used in the solution also require an entry in the allowed list for *.amazonaws.com for the following ports:

- MQTT/443
- MQTT/8883
- HTTPS/443
- HTTPS/8443

Product Hardening for Ensuring Security during Product Development

During the MiVoice Office Web Application development cycle all unnecessary diagnostic and debug software is removed from the released version of the software.

The software delivery process and change management policy are extensively automated through multiple Continuous Integration / Continuous Deployment (CI/CD) pipelines to allow deployment into development 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.

MiVoice Office Web Application undergoes Software Composition Analysis and Vulnerability scans at least once a year.

Security and privacy threats are constantly 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.

MiVoice Office Web Application Release 1.0 was developed in accordance with Mitel's Secure Development Life Cycle policy; this ensures the web application was designed with best practice safeguards to mitigate risks to confidentiality, integrity, availability of data contained within the web application, and to all data related to the functionality provided by the web application.

Mitel Product Security Policy

The Mitel Product Security Policy describes how Mitel assesses security risks, resolves confirmed security vulnerabilities, and how reporting of security vulnerabilities is provided. The Policy is available here: www.mitel.com/support/security-advisories/mitel-product-security-policy

Mitel Product Security Advisories are available here: 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.

Cloud app user: An app user licensed in CloudLink and belonging to a specific registered account.

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, usernames, or logins; and disabling or removing of unnecessary services.

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

MiSDLC: **Mitel 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 provides 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.

CloudLink Gateway: Mitel CloudLink Gateway solution that allows Mitel CloudLink Platform to communicate with Mitel PBX (communication system).