MiCollab

RELEASE 10.2

VERSION 1.0

SECURITY GUIDELINES

DECEMBER 2025

Mitel

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). 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.

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.

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.

Contents

Overview

This document will be of interest to personnel responsible for ensuring the secure deployment and operation of Mitel® MiCollab system(s).

Every organization must have a clearly defined IT security policy in place, defining goals, assets, trust levels, processes, incident handling procedure, and their other requirements. The security mechanisms available in MiCollab must be covered by and deployed according to this policy.

Security is an integral part of the Mitel MiCollab system design; this document describes the MiCollab security features and also provides recommendations as to how the Administrator should configure the security features to ensure a secure MiCollab deployment.

The MiCollab security features are enabled in the system by default, enabled during the installation/configuration phase of the systems, or must be enabled manually by the system Administrator.

The security measures available for MiCollab are mainly based on the following open standard technologies and access mechanisms:

- TLS—Transport Layer Security (TLS) 1.3 provides secure administration and signalling for a subset of interfaces. For more details, see the section TLS 1.3 Support for External Interfaces.
- SSH – Secure Shell (SSH)v2 provides secure, console-based access to the MiCollab administration and configuration tools.
- SRTP – Secure Real-time Transport Protocol (SRTP) is used to protect the voice media streams between IP phones and between IP phones and call managers.
- LDAPS– Secure LDAP is optionally used for connectivity to a customer's Active Directory server.
- OAuth2.0 (Open Authorization) may be used by voice mail to authenticate with other email applications such as Google Apps and Microsoft Office 365

Other mechanisms that can be employed to protect the MiCollab system are based on the following:

- A securely designed corporate Local Area Network (LAN) infrastructure.
- Configuration of internal and external public-facing routers and firewalls.

In addition to the security recommendations described in this document, there are a number of general security aspects that need to be covered and addressed by the System Administrator and/or the Information Technology (IT) security officer.

An important security measure is to establish and maintain physical security. Only authorized personnel should have access to server locations because many data-exposure attacks can be mounted by unauthorized physical access to a host. Further, the IT data infrastructure must be designed with security in mind, security mechanisms and protocols must be enabled, and all components of the whole system must be correctly configured, maintained, and updated as necessary.

The MiCollab Server is designed to be installed on a customer's secure Local Area Network (LAN).

 Note: The MiCollab Server must never be directly connected to the Internet. The MiCollab Server should always be isolated from the internet by MBG and a properly configured firewall.

About the MiCollab Documentation Set

Documents for MiCollab and other Mitel® products are available on the Mitel Documentation Center website (https://www.mitel.com/document-center). The documentation set consists of guides in PDF format and online help systems that you can view using an Internet browser. The following documents are the main source of information for the MiCollab platform:

- MiCollab Engineering Guidelines—provide information about the characteristics, requirements, configurations, capacities, and performance of the MiCollab solution.
- MiCollab Installation Guide—provides installation instructions for the MiCollab software and for the supported applications.
- MiCollab Platform Integration Guide—describes how to deploy MiCollab with Mitel communication platforms.
- Virtual Appliance Deployment Solutions Guide—provides engineering guidelines for deploying Mitel Virtual Appliances and applications in a VMware virtual infrastructure.
- MiCollab Administrator Online Help Systems—provide administration and programming procedures for the MiCollab applications.
- MiCollab General Information Guide.

Additional guides and help systems are available that contain instructions on how to configure and use the individual Mitel applications that are supported on MiCollab.

The complete documentation set is listed in the MiCollab Installation and Maintenance guide. To access the MiCollab product documentation set: MiCollab Server Technical Documentation.

The following document discusses security and toll fraud prevention:

- Security *Toll Fraud and Installation Checklist - EM004472*

The following documents, available in the Mitel Document Center, address network and product security:

- Mitel Technical Paper—Intrusion Detection and Prevention Systems
- Mitel Technical Paper—Securing Mitel Cloud Based Unified Communications

New for this Release

Single Sign-On (SSO) Support Using Keycloak

From MiCollab 10.2, administrators can configure Single Sign-On (SSO) for MiCollab using Keycloak as the identity broker. Keycloak enables secure, centralized authentication by integrating with multiple Identity Providers (IDPs) using either SAML 2.0 or OpenID Connect (OIDC) v1.0, improving enterprise authentication security.

This release also introduces:
- Multi-IDP support for federated authentication environments.
- IDP-initiated logout, ensuring session termination and token revocation across MiCollab clients.

Note: Due to the complexity of SSO environments and observations from field deployments, this capability is introduced as a Controlled Introduction. It is not intended for general deployment in this release. Activation requires prior approval from Mitel PLM and coordination with Mitel Technical Support.

System Architecture

Mitel® MiCollab is the brand name of Mitel's enterprise collaboration software and tools solution. MiCollab provides communication experiences that are consistent across all of a user's devices for real-time voice and video calling, individual and group chat, team collaboration, audio conferencing with web sharing, Outlook® and calendar integration, and many more collaboration features. It includes the following main components:

- MiCollab Clients (PC, Mac, Web, and Mobile devices)
    - Including softphone capabilities and desk phone control
- MiCollab Server
    - Single point of Provisioning for Users and Devices
    - Unified communication Application for features such as Chat, Presence notifications, Calendar Integration, and so on
    - Embedded Audio video Web conferencing solution or a cloud-based Mitel One / MiTeam Meetings integration
    - Unified Messaging (Advance UM) (AKA NuPoint)
    - Advanced Auto Attendant
    - Simplified Deployment
    - Mitel Border Gateway (MBG)
    - Licensing services

MiCollab can be deployed on industry-standard servers, in a virtualized computing environment (Hyper-V, VMware), or in the cloud in Microsoft Azure or Amazon Web services (AWS).

The recommended deployment for MiCollab is for the MiCollab Server to be installed on the customer's private network behind an MBG. The MBG's external network interfaces will be interfacing with the firewalled Internet connection for any web/telephony related communication.

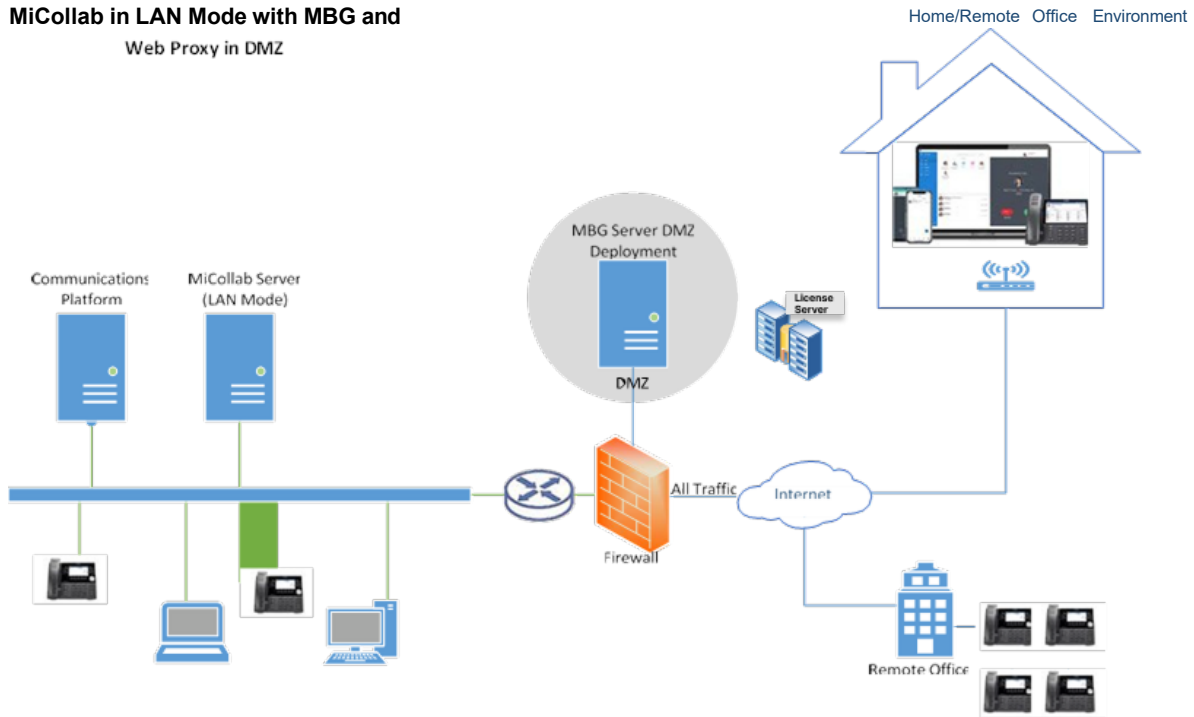MiCollab can be deployed in the following configurations:

- **MiCollab Server on the LAN with a separate MBG Server in the DMZ:**
    This configuration has MiCollab located in the Local Area Network (LAN) connected to a separate MBG server in the Demilitarized Zone (DMZ). Two variants of this configuration are supported:

    - **MiCollab with separate MBG Web Proxy in the DMZ** (2-Server) consists of a MiCollab on the corporate LAN with Web Proxy in an MBG server in the DMZ. Remote web browser users connect to the MiCollab Server through the Web Proxy.
    - **MiCollab with separate MBG / Teleworker/ Web Proxy in DMZ** (2-Server) consists of MiCollab on the corporate LAN with Teleworker and Web Proxy on a MBG server located in the DMZ. The Teleworker service is installed on both the MiCollab and the MBG systems. The Teleworker service in the MiVoice Border Gateway (MBG) is used to support the teleworkers in the DMZ. The Teleworker service in MiCollab is used only to remotely manage the Teleworker phones that are configured on the MBG server. The Web Proxy service is also installed in this configuration.

Note: The MiCollab Server must never be directly connected to the internet. The MiCollab Server should always be isolated from the internet by MBG and a properly configured firewall.

MiCollab in LAN Mode with MBG and
Web Proxy in DMZ

Home/Remote Office Environment

The following restrictions apply to MiCollab deployments:

- The majority of the applications included in MiCollab are designed to run on the LAN. For this reason, MiCollab is not supported in the DMZ.
- In configurations where multiple MiCollab Servers are deployed, each MiCollab server must be managed separately. A single point of management for multiple MiCollab Servers is not supported.
- The MBG Web Proxy is not supported directly on a MiCollab Server. MBG Web Proxy is supported only when it is installed on a separate MBG Server that is located in the DMZ. In this deployment, the Web Proxy on the MBG server allows clients on the internet to connect through the network firewall to a MiCollab system on the LAN.
- The MiCollab Server must never be directly connected to the Internet. The MiCollab Server should always be isolated from the Internet by MBG and a properly configured firewall.

Securing the Operating System

Operating System Overview

Mitel's MiCollab software is installed on top of the Mitel Standard Linux (MSL) operating system. Compared to other common operating systems, MSL provides a reduced attack surface. MSL is a 64-bit Linux distribution for Intel-based computers that is available for download from the Mitel Software Download Center and is based on the Rocky Linux 8.10 distribution with unnecessary packages removed, and certain services replaced. In addition, only Mitel applications are installed on the MSL server and installation of non-Mitel endorsed applications is not supported, which reduces chances of accidental installation of malware. MSL is also configured such that unnecessary IP ports are closed.

Additional measures can be taken to secure the MSL platform and the MiCollab application executing on the platform. These measures are based on well-known network security best practices.
In general, a platform that is both physically secure and installed in network that has been securely designed will have a low likelihood of being infected compared to a platform that lacks physical security and/or is installed in a network lacking security controls.

Use of Antivirus Software

While the use of antivirus software is widely accepted in the IT industry for use on servers, end-user mobile platforms and desktops, running antivirus software on a real-time computing platform can be problematic.

Because MiCollab is a real-time application, Mitel cannot guarantee that third-party antivirus software will not affect the performance of the application, and Mitel does not offer any endorsements of antivirus software vendors, or evaluations of particular antivirus products.

Should a customer require technical support from Mitel related to a system that has antivirus software installed, Mitel may require that the software be removed before Mitel can start troubleshooting the problem.

Software Patch Management Policy

It is necessary for the Administrator to ensure that the MiCollab systems are always updated and equipped with all critical patches to guarantee the highest level of security. Mitel has developed best practices for the management and installation of security patches released by the operating system vendors aiming to guarantee the highest level of security and the correct functioning of the system.

Operating System Related Network Controls

Mitel implements TLS 1.3 for administration and client signaling to defend against interception of usernames and passwords. Access to the management interface requires a username and password.

The underlying Linux OS (MSL) allows Administrators to be restricted to certain IP addresses or subnets, and to accept only secure-based web connections from permitted IP addresses.

Linux shell access is available only via SSH v2 (see Securing Operating System User Interfaces). SSH access also supports the IP address restrictions, ensuring that the platform rejects any non-authorized connections.

Network access is therefore reduced to the minimum and can be configured by the customer (Administrator) through MSL server-manager pages:

- Webserver interface supports TLS 1.2. TLS 1.3 is enabled by default for backward compatibility.

> **Note:** TLS 1.0 and 1.1 are no longer supported. It is recommended that the Administrator use TLS 1.2 or 1.3.

- Remote administrative access is disabled by default and must be specifically enabled through the Remote Access panel of the server manager.
- Port forwarding is disabled by default in server only (LAN mode).
- A default self-signed TLS certificate is provided with the MSL server at no additional cost. Customers may provide their own certificate.
    - Any customer supported TLS certificate can easily be configured.
- Unencrypted HTTP connections are not allowed but are redirected to an encrypted connection using HTTPS by default.

Securing Operating System User Interfaces

MiCollab provides SSH "Root (SSH only)" shell for maintenance and diagnostic purposes. It is disabled by default and if required, it must first be enabled by the Administrator to allow remote access to the command line and can be further restricted by source IP address. The SSH version used is SSHv2. The root shell allows access to the running OS and in initial default state, login/password credentials of root user are the same as those of the Administrator user.

The SSH access can be enabled/disabled via "server-manager > Security > Remote access > Secure Shell access". SSH ciphers enabled are:

- chacha20-poly1305
- aes128-ctr
- aes192-ctr
- aes256-ctr
- aes128-gcm
- aes256-gcm

Recommendation

Ensure "Remote access" is Disabled in the MiCollab Server when not needed. The default is Disabled (Off).

Administration

Administration and Management Tools

MiCollab provides secure administration access by using a TLS 1.3 encrypted Web User Interface that can be launched using the IP/FQDN of MiCollab followed by '/server-manager'. Administrator level privileges are required to log in to the management portal. Access to administration can be restricted at the source IP address level.

OS and Network Level Monitoring

- All security level aspects such as remote access, port forwarding, and web server certificate creation can be configured and monitored via 'Security' pages inside the 'Server-Manager' UI.
- Allow or Disallow for Trusted networks can be configured using the 'Network' tab under the Configuration settings of Server-Manager.

System Monitoring

For monitoring system performance, the underlying OS in MiCollab provides System Monitoring capabilities to monitor network traffic, free main and swap memory, and CPU Load avg.

- Viewing monitoring graphs can help analyze system performance.
- Frequency depicted by Graphs includes Daily, Weekly, Monthly, and Yearly.
- System monitoring is disabled by default.
- System monitoring access can be enabled for private and public networks.
- Support for audit logs is available.

Securing Client and Server Communication

An end-user who wants to make use of the collaboration services provided by the MiCollab Server needs to install the desktop or mobile MiCollab Client. Or alternatively, access the MiCollab Server via a Web browser.

For providing secure communications between Mitel Unified Communications applications on the LAN and remote clients connecting via the Internet, Web Proxy Services on the MBG are pre-configured to support the following MiCollab applications.

- MiCollab Client (Desktop, web, mobile)
- MiCollab Audio, Web and Video Conferencing
- MiCollab Client Deployment
- MiCollab Unified Messaging
- MiCollab Server Manager

Clients can be configured with a deployment email received on the user's corporate email account. An end-user can have one or more MiCollab Clients installed either as an app on their Android or iOS Mobile phone or as a Next Gen MiCollab Client application on their PC/Mac desktops. Web browsers can also be leveraged to launch the MiCollab application on desktops. How these various MiCollab Clients connect to MiCollab Server securely is described in the following steps:

- Assuming an Internet connected user, the MiCollab Client requests DNS resolution of the MiCollab Server FQDN, for example, micollab1.mitel.com.

- The DNS server the PC/smartphone is utilising for its internet connection will resolve the FQDN of the MiCollab Server to the IP address of the customer's corporate firewall.

- MiCollab Client connects to the corporate firewall.

- The corporate firewall routes the secure request to the MBG Web Proxy.

- The Web Proxy requests resolution for MiCollab1.mitel.com from the customer's Internal DNS server.

- The internal DNS server provides the IP address of the MiCollab1 Server.

- Web Proxy completes the connection to the MiCollab1 Server.

- The Web Proxy proxies the request to the MiCollab Server along with the full URL requested by the client (for example, MiCollab1.mitel.com/ucs/micollab/).

Administration Certificate

By default, MiCollab uses a self-signed certificate as a local certificate for encrypted communication between web servers and the web client using Transport Layer Security (TLS). However, self-signed certificates are inherently untrusted by the user's web browser(s). This issue can be mitigated by installing signed certificates from a third-party Certificate Authority (CA).

MiCollab provides options to use Let's Encrypt CA, which is a free, automated, option available to connect and get certificate with a single click) and open certificate Authority service.

Alternately, customers can obtain a Certificate of their own from their chosen Certificate Authority and install it on with the MiCollab Server.

Recommendation

- Mitel recommends installing a certificate obtained from a Certificate Authority (CA) that the customer already owns (that is, Enterprise CA). The MiCollab Clients will then trust the MiCollab Web server access. Note that certificates do expire and therefore, the customer must be aware of the expiry date and renew them when needed.

- Web certificates must be either in PEM format or in PKCS12/PFX format (.pfx or .p12 file).

Administration Tool Encryption

Administration access is through HTTPS on TCP port 443, which must be allowed through any data network local access control list or firewall.

The system can be configured to support TLS 1.2, and TLS 1.3 is enabled by default. It is recommended that the Administrator use either TLS 1.2 or TLS 1.3. To enable support for TLS 1.2, TLS 1.1 settings must first be disabled.

The following encryption modules are available for HTTPS in the Cipher Suite of MiCollab 10.2 by default for TLS 1.2:
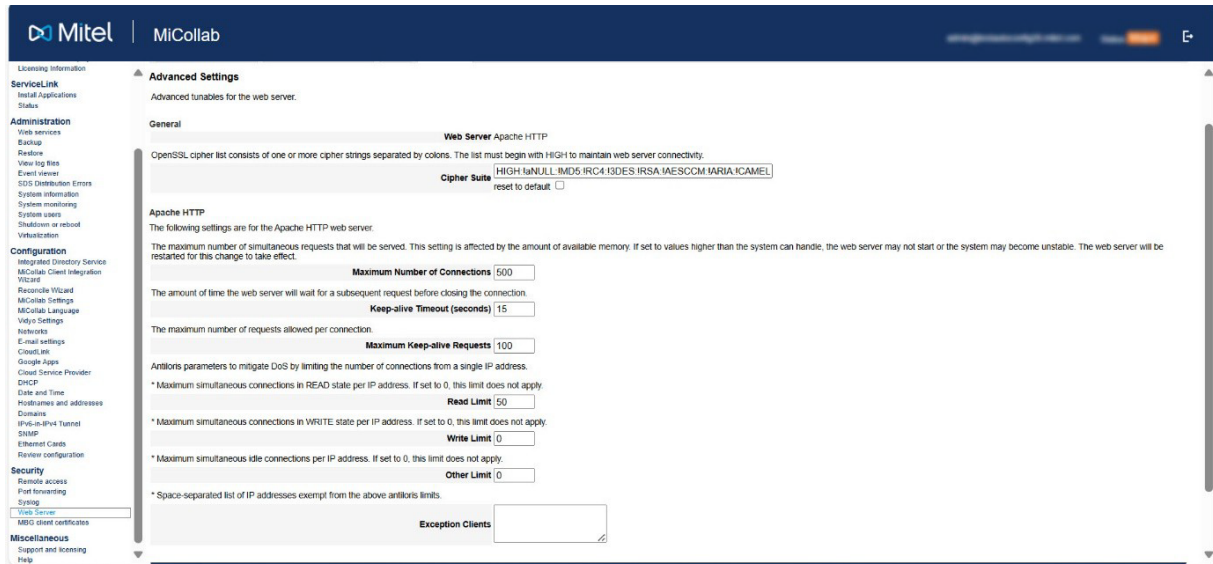
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- DHE-RSA-AES256-SHA
- DHE-RSA-CAMELLIA256-SHA
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA
- DHE-RSA-CAMELLIA128-SHA

Symmetric ciphers:

- AES, Camellia. Up to 256 bit.

The following encryption modules for TLS 1.3 are available in the Cipher Suite of MiCollab 10.1 and greater:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256

In the **Advanced Setting** page of the Web Server screen, the Cipher Suite setting is used to enter the cipher list that will be used by MiCollab. Settings for the Apache HTTP Web Server are provided in the **Advanced** tab; details of which are as follows:

- Maximum Number of Connections: The maximum number of simultaneous requests that will be served

- Keep-alive Timeout (seconds): The amount of time the web server will wait for a subsequent request before closing the connection.

- Maximum Keep-alive Requests: The maximum number of requests allowed per connection.

- Read Limit: Maximum simultaneous connections in READ state per IP address. If set to 0, this limit does not apply.

- Write Limit: Maximum simultaneous connections in WRITE state per IP address. If set to 0, this limit does not apply.

- Other Limit: Maximum simultaneous idle connections per IP address. If set to 0, this limit does not apply.

- Exception Clients: Space-separated list of IP addresses exempts from the above anti-Loris limits.

TLS 1.3 Support for External Interfaces

From MiCollab 10.1, support for TLS 1.3 has been introduced across multiple external interfaces, enhancing security and compliance with modern encryption standards. This applies to the following interfaces:
- From MiCollab server to
    - Microsoft Exchange Server (Office 365)
    - Google Calendar
    - Apple Push Server
    - Firebase Cloud Messaging (FCM) - formerly called Google Cloud Messaging (GCM)
    - External Directory
- From MiCollab Client (including the following types of MiCollab Clients (iOS Client, Android Client, PC Client, MAC Client, Web Client) to:
    - MiCollab Server

- NuPoint UM Server to:
    - Microsoft Exchange Server (Office 365)
    - Google Email
- NuPoint UM End User Web Portal to NuPoint UM Server

Identity and Authentication

To ensure privacy and maintain system integrity, access to MiCollab is restricted by a login password to those users that can be identified and authenticated.

MiCollab user accounts can be authenticated:
1) Locally using the information in the MiCollab server
2) Via onsite Microsoft Active Directory using secure LDAP
3) Via Microsoft Entra ID using Mitel CloudLink SAML 2.0 connection.
4) Via Single Sign-On (SSO) with a local Identity Provider (IdP) using SAML 2.0 or OpenID Connect (OIDC) locally. Examples include with Microsoft AD FS or Microsoft Entra ID.

Users logging into the MiCollab system with local authorization for the first time are required to change the default password. The password strength and the user session inactivity timer are both configurable.

MiCollab System level/Administrative Users are authenticated locally.

Single Sign-On (SSO) allows MiCollab users to log in using the same set of credentials that they use for other cloud or on-premises applications.

Security Recommendations

Secure Password Recommendations

It is advised that an Organization Level Password Policy be adopted to incorporate the following recommendations.

Overview of password handling

For password handling and processing in MiCollab for system users, choose a password that contains a minimum of 10 characters including: uppercase and lowercase letters, numbers, and symbols.

For **System-level/Administrative Users**, password requirements can be customised under the **System Users option,** as shown in the following image.

For an end-user, Mitel recommends, wherever possible**,** leveraging MiCollab's integration with Microsoft Active Directory or another LDAP directory or CloudLink-based solution for authentication. With this in

place, an end-user can leverage accounts provided by the organization to perform Single Sign On (SSO) capabilities to log in to MiCollab Clients as well. Similarly, CloudLink platform can also be leveraged for authentication after the CloudLink Integration is performed. For CloudLink-based authentication, a CloudLink account can be linked to a Cloud Identity Provider (for example, Azure AD), which can provide Multi Factor Authentication (MFA) capability as well, which adds an extra layer of security.

If MiCollab end-user Authentication is managed within MiCollab, following is the recommended approach for password settings:

- Use a passphrase or a Password Generator. A passphrase is a group of words that means something to you but not discernable to anyone else. See the following image.

Secure Email Recommendations

Email is widely used across organizations, and MiCollab Server also sends various emails such as welcome emails and deployment emails for a new and existing user to share users details and facilitate logging in to MiCollab Clients. In most cases, emails are autogenerated by MiCollab Server. In case authentication of a user is managed through CloudLink, MiCollab acts only as the trigger to generate another email to 'Finish Building Account' for CloudLink, the Email is sent from CloudLink Servers only.

Some precautions, often overlooked, can eliminate unnecessary security risks:

- Ensure that the MiCollab Welcome Email received is from the administrator's account of your company. MiCollab Client Configuration Email must be from noreply@mitel.easydeploy.net.

- If organization users are authenticated using CloudLink, then ensure, before completing the account settings that the email received is from the CloudLink platform: no-reply@mitel.io.

- While configuring any external SMTP server in MiCollab and setting up the destination port for outbound SMTP, it is recommended to make use port 465 with SSL encryption port or 587 with TLS encryption port. Refer to the online Help for more details.

- To avoid DoS attacks, limit the number of connection and authentication errors that your systems will accept. Remove unwanted server functionality by disabling any unnecessary default settings. Have a dedicated mail server and move other services such as FTP to other

servers. Maintain the total, simultaneous, and maximum connections limits for your SMTP server.

- To protect your server from unauthorized access, implement authentication and access control mechanisms. For example, SMTP authentication requires users to provide a user name and password to be able to send mail from the server. Make sure access to your servers is on a need-to-have basis and is shared with limited people.

Secure MiCollab AWV Conferencing Recommendations

Each conference call account has two levels of Access code: Leader and Participant codes. All Invited Guests are provided with the participant Access code. They must enter the Access code when they join the conference.

The following are some security features to consider when creating conferences:

- Conferences can be created such that the Leader must be present for the other participants to join.

- All conferences must be password-protected. Passwords must be exchanged only through encrypted emails or other secure communication channels.

- Assign accounts to individual named users. It is easier to track such accounts in reports, and end-users are more likely to safeguard personalized details than those in a shared or generic account.

- Assign separate accounts to users even if they want to hold only a single conference call. There is typically no cost associated with this, and it can be done online or through customer service.

- Do not share a generic account within a department or group. Doing so is like sharing computer login or email credentials. There is an additional risk of two separate groups scheduling conflicting conference calls (occurring at the same time) or former employees still using the codes for access.

- Do not give out the conference Leader code to anyone else. This could enable anyone else to use your account whenever they want, without your knowledge.

- Try to minimize the number of participants in a conference call. The larger the number of people to whom conference details are passed, the greater the chance of them mistakenly falling into wrong hands. Moreover, it means more people could also keep dialing into calls in the future, even when they are no longer invited. It also makes it difficult to keep track of who is participating in the call at any given time.

- Do not set back-to-back conferences that use the same bridge details. Scheduling two separate meetings, with two separate groups of people, but over the same conference bridge and one right after the other, creates an opportunity for privacy issues. It would make it easy for participants from the first call to stay on the line too long, or for participants from the second call to dial in early – even if by mistake. Keep separate conference bridges for different conferences.

- Recording facility is available only for the Leader of the conference when properly authenticated by the system. Only that person must be responsible for sharing the recordings or recording links. The sharing must be done through encrypted emails or over-encrypted communication channels.

- Leaders must delete all chats associated with a conference, especially if the same conference bridge will be used for different groups.

- Limit the use of Reservation-less Conferences to limit unauthorized use of conference facilities. Limit the use of Callback to avoid tool fraud. People can often be slow to change Access codes and dial-in numbers. Anyone having access to an Access code and a dial-in number can join a conference call without permission. This can lead to the potential risk of

unscrupulous third-party eavesdropping on a call and harvesting sensitive information. The advanced security features described in the following section has more information about preempting this risk.

The following are advanced configurations and features that can be used before or during a conference call to enhance security:

- **Entry tone**: This plays a discreet tone when participants join, to let everyone know another participant has joined. The Leader can then ask who has joined.

- **Roll Call**: Participants are prompted to record their name as they enter the conference. For example, a text such as "Mary has entered the conference", identifies each participant distinctly. The number of participants present is also shown to the Leader.

- **Lock conference**: The Leader can lock the conference. The Leader can also hold or mute the conference at the group level or at the individual level.

- **Remove unauthorized participant**: The Leader can remove any unknown or unauthorized participant from the conference.

- **Conference approval**: A participant can join the conference only with the Leader's approval at runtime, even though the participant has the conference details for joining.

- **Host hang-up**: The Leader can end the conference for the entire group.

- **Conference starts only when the Leader joins**: The conference starts only after the Leader joins. Until then everyone will hear recorded music.

Network Access Security

It is recommended that the Ethernet LAN switches used to provide LAN connectivity be managed, enterprise-grade switches that include integrated access control measures. It is also recommended that the system Administrator ensure that the switch access control measures are properly configured and maintained.

Wireless networks must also employ access control measures and user authentication mechanisms with a minimum of WPA2 encryption and a separate SSID for voice applications. SSID to VLAN mapping is recommended.

Most businesses have a well-defined network structure that includes a secure internal network zone and an external untrusted network zone, often with intermediate security zones.

While the threat of attacks might seem daunting, the solution lies in implementing the dynamic and effective software and hardware security solutions available, as well as enforcing strategic security provisions to guard your enterprise against evolving attacks on the network.

- **Network Hardening** must be done for all devices by using strong password policies.

- **Maintain current patch levels**: Enterprises should implement adequate monitoring, ensure the timely deployment of patch releases, and keep systems up to date.

- **Limit physical access to network hardware**: Physical access to network hardware must be granted only to relevant and authorized personnel and all equipment must be stored in a restricted and controlled environment.

- **Implement advanced intrusion detection and prevention systems**: These systems must be a part of every enterprise VoIP network as they use stateful detection and prevention techniques in addition to deep packet scanning to guard against both zero-day and emerging threats.

- **Enforce security through authentication, authorization, and encryption**: Best practices include:
  - Configuring Ethernet switch ports to allow only known MAC addresses
  - Password protection by using cryptographic keys

Using VLANs to Assist with Security

To make eavesdropping attacks and Denial-of-Service attacks more difficult, or less effective, traffic on the LAN must be grouped according to traffic types and trust levels. This can be achieved by using Virtual LANs. VLANs can be used to segregate controller-to-controller signaling, controller-to-phone signaling, and voice traffic.

When VLANs are used to provide isolation between traffic types, it will make the solution more robust against virus-based and network flooding attacks. In particular, if Voice over Internet Protocol (VoIP) traffic is grouped into a single VLAN, and the nodes on this VLAN are strongly protected, a worm-based attack causing network overload that originated on a node located on another VLAN might only marginally affect the VoIP LAN.

When the traffic types have been segregated by VLAN, hosts or devices belonging to different VLANs can communicate only through a Layer 3 switch or router that connects the two VLANs. This means that broadcast traffic is blocked across VLANs, preventing broadcast storms from propagating network wide. Additionally, many modern routers offer Intrusion Detection/Prevention Systems (IDS/IPS), which are able to detect and/or block more advanced types of attacks.

Creating network trust zones for security purposes and the usage of Intrusion Detection and Prevention Systems (IDPS) are discussed in detail in the Mitel Technical Papers - *Intrusion Detection and Prevention Systems* and *Securing Mitel Cloud-Based Unified Communications*.

Develop a standard building of a secure desktop: Design a secure workstation configuration as the standard build of the company and make an image backup of the build and replicate it to the company desktops.

Make sure your network is locked down tightly. With good practices, policies, and procedures in place, your WAN and telecommunication services can be secured against the most common threats. Protect your network with a complete network security solution.

Audits and Logs

Log security events and review regularly: Logging and auditing functions are provided to record network connection, especially for unauthorized access attempts. The logs must be reviewed regularly. If a user fails to log in, the event is recorded in the maintenance log "/var/log/secure". For any services related failure the log file to refer is '/var/log/messages'.

The **Event Viewer** page of server-manager lists various events performed on the server. An Administrator can monitor this page to make sure there are no 'Critical' or 'High' severity level alarms being raised. The "Alarm Status" label on top of the page indicates the system alarm severity.

Secure Mobile Devices (Next Gen Client) Recommendations

The following list provides best practices for secure Next Gen Client handling:

- Use a password, passphrase, passcode, face ID, or fingerprint scanner on your mobile device. Set the lock feature to a few minutes.

- On all the clients except browser client, the logged in user details, including source code and local database, cannot be viewed. Recommendation is to make use of Next Gen Mobile and PC Clients.

- Install antivirus software on your device and update the antivirus software regularly.

- Use encryption to protect personal information on mobile devices.

- Leave your Bluetooth turned Off when not in use.

- Use remote tracking software on your smart phone, which enables you to locate, lock, and wipe if your smart phone is lost or stolen.

- Take note of your IMEI (International Mobile Equipment Identity) number. An IMEI is the 14-16-digit serial number that identifies your smart phone. If a device is reported stolen, the IMEI number can be used to render the device permanently unusable on most carrier networks, even if the SIM card is changed.

- Do not use your mobile phone as a place for storing your personal data, which is dangerous if the phone falls into the hands of strangers. It is advisable not to store important information such as credit card or bank card passwords in a mobile phone.

- Activate the pin code request for mobile phone access. Choose a pin, which is unpredictable, and which is easy for you to remember.

- Change the PIN at regular intervals.

- Use devices running the latest supported Android version for optimal security and privacy protection.

- Regularly backup important data in the mobile phone or laptop.

Mitel has not verified any specific Mobile Device Management (MDM) application for the MiCollab Mobile client. MiCollab Mobile applications are available through the Apple Store and Google Play Store.

Secure Desk Phone/Softphone Recommendations

- With a desk phone, use a minimum of a 4-digit secure PIN to lock/unlock the phone.

- Avoid using obvious patterns (such as 0000,1111, or 1234) that can be easily guessed.

- When implementing VoIP on the corporate LAN, be sure to use SRTP if it is available. Also segregate VoIP traffic and data traffic into separate VLANs. If this cannot be done, consider installing a separate physical network.

- Always keep the desktop or mobile device antivirus software updated and have some good, secured firewall policies implemented.

- Network Administrators must enforce strong SIP passwords between UAC (User Agent Client) and UAS (User Agent Server).

- The relationship of /IP/Ext/PIN must be valid for softphones to allow communications to proceed. This prevents unauthorized sets being added to the system.

- Authorization of the unique identifier is typically done by the system Administrator. With MiVoice Business, the MiNet IP phone sends its MAC address as a unique identifier. Note that this identifier is sent in the encrypted MiNet call control stream and not as a layer 2 transmission, which can be easily spoofed.

- Do an integrity check on the application to ensure that software loaded is not corrupted.

- Ensure that VoIP applications have implemented Class of Restriction (CoR) properly to enable the customer to disallow the dialing of certain external telephone numbers or ranges of numbers (Call Barring). This is achieved by associating in software, each extension and trunk with a CoR, and providing specific barring plans for each CoR.

- User must log out from the browser client if it is on a shared or public PC.

Secure Voice Mail Recommendations

To secure voice mail, administrators and users should consider the following recommendations:

- When choosing new passwords, specify a voice mail password of at least 4-10 random digits. Do not choose obvious patterns, such as repeating digits (for example, 1111) or ordered (for example, 1234) numbers, years, or addresses.

- Have employees change their voicemail passwords on a regular basis. Organize scheduled password change dates for the company, if needed.

- Have employees check their recorded greetings on a regular basis, especially after holidays, to ensure they have not been tampered with. It is common for this type of hack to occur after weekends or holidays, when a hacker has a better chance of reaching voicemail boxes and will have a longer period before a changed voicemail message is noticed.

- If your business does not need to place calls internationally, consider disabling international calling capability entirely. If you do need the capability to make international calls, it is strongly recommended to use authorization codes as an extra protective measure–which entails dialing six extra digits for placing the call.

- Disable the pass-through feature so that calls cannot be made from your voice mail account.

- Remove the mailboxes of users who no longer work at your business. In general, always delete user accounts for users who are no longer working at your business.

- Block outgoing phone calls to premium-rate telephone numbers; for example, a 900 number or a 1-900 number.

- If you use the call forwarding feature, periodically run reports verifying valid call forwarding numbers.

Secure Chats Recommendations

Chats are useful when one needs quick response to important queries; but chats are often left unattended at the Client level as well as at the Server level once their purpose is over, which can lead to security risks. Chats may contain confidential information, therefore we must employ certain policies for chat history.

Although all chat history stored locally in the server is encrypted by default using Blowfish encryption, the following are some of the additional ways to make chat more secure.

Disable chat storage in server

Use the following commands to disable the MiCollab Client Service from storing chat history.

1. Edit the following file:

   /etc/e-smith/templates/opt/intertel/conf/sip_ims.ini/50Configuration

2. Change the entry of 'EnableFile=Yes' to 'EnableFile=no'.

3. Save and exit.

4. Enter the following line and then press enter:

   expand-template /opt/intertel/conf/sip_ims.ini

5. Restart MiCollab Client Service.
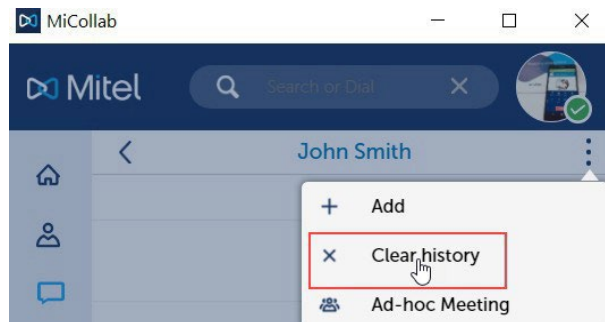
Delete existing chat history from server

Use the following procedure to delete existing chat history from MiCollab Client Service.

1. Stop the SIPIMS service from the MiCollab Client Service diagnostic page.

   o Go to the **MiCollab Client Service** configuration page and click the **Perform Server Diagnostics** under **Diagnostics**.

   o Locate **SIPIMS** and click **Stop**.

2. Move all files from the */opt/intertel/data/imarchive*directory.

   o You can move the files to /root by performing 'mv hab_ims_archive* /root' from /opt/intertel/data/imarchive directory.

   o You can do this with PuTTY, but if there are many files, you may want to use an application such as WinSCP.

   o You can also delete the files from the PuTTY command line if you do not want to keep the history.
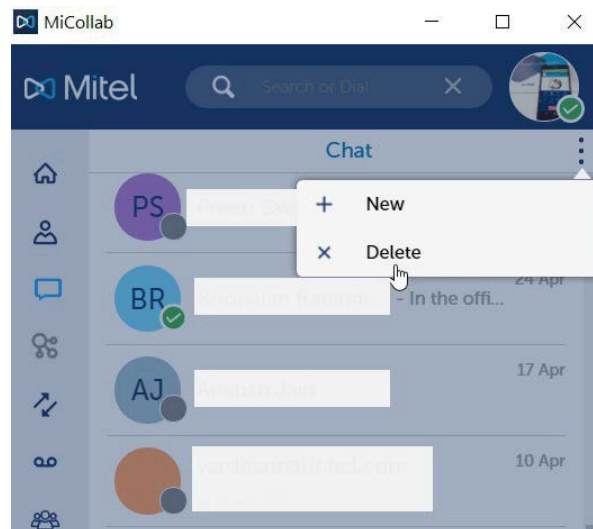
3. Restart MiCollab Client Service.

Delete chats on MiCollab Client

From an end-user's perspective, you can **Clear history** within a chat conversation.

Also, you can delete an entire conversation.

Chat history and other settings are NOT deleted from PC if the application is uninstalled. This is done on purpose so that the chat history is not lost after a reinstall or upgrade.

In the Unified Communications PC Client 7.3 (legacy MiCollab Desktop Client), there is an option **Record Chat History**. If this option is not enabled, then Chat history is not stored on that PC.

Also, when deleting Client chat records, there is a subdirectory that requires manual cleanup. After the application is uninstalled, the Administrator must delete the following subdirectory:
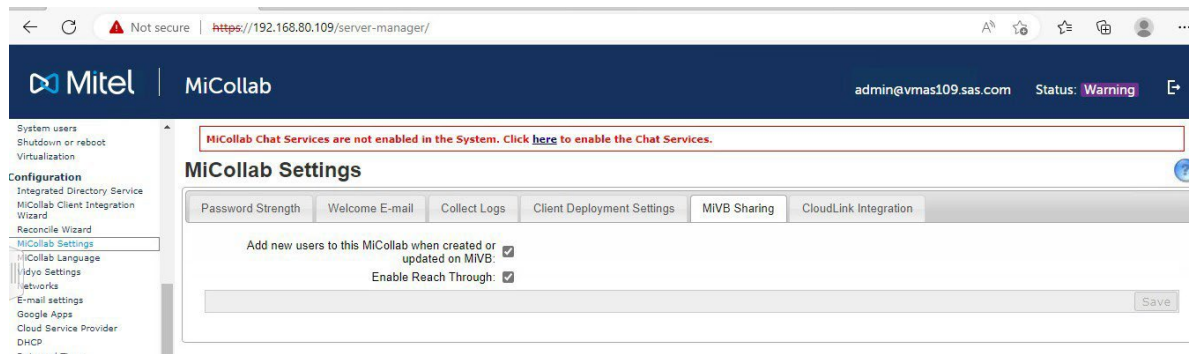
AppData\Roaming\Mitel Networks Corporation\MiCollab

Note: Customers using CloudLink-based chat must refer to the CloudLink Chat Security document at https://www.mitel.com/document-center/technology/cloudlink-security

Control of Users and Services Provisioning (USP) Single Sign on Reach Through to MiVoice Business from MiCollab

This feature provides a configurable option from CLI and/or UI (default off for new installs) and ensures that

- When this option is on, it means MiVoice Business pages will be accessible from MiCollab, same behavior that we see now.
- When this option if off, admin will not see links to open MiVoice Business ESM pages.
- The control should ONLY be available to the root administrator ("admin").
- Other administrators shall be able to use SSO reach through if enabled but cannot turn feature on/off.

Info Around Passwords Fields in MiCollab Database

Password Type	Encrypted [Yes/No]	Encryption Algorithm (if encrypted)	Hashing [Yes/No]	Hashing Algorithm (if hashed)	Encoded [Yes/No]	Encoding type (if encoded)	Plain Text [Yes/No]	Comments
MiVoice Business login password	Yes	SAFER K-64	No		No		No	
End User passwords (Local Authentication)	Yes	——	Yes	MD5	No		No	For Directory servers and CloudLink-based authentication no passwords are stored in DB
Voice mail PIN	No		No		No		Yes	
AD Connection Password (service account)	No		No		Yes	Base 64		
Advance UM user & super user credentials (Exchange server)	Yes	3DES	No		No		No	
SIP Phone PIN	No		No		No		Yes	
Network Element Password	No		No		No		Yes	
Advance UM Admin Password	Yes	3DES	No		No		No	
SIP Phone PIN	Yes	AES 256	No		No		No	
MBG SIP Password	Yes	AES 256/CBC	No		Yes	Base 64	No	Passwords are first encrypted and then b64 encoded

PBX SIP Password	Yes	AES 256/CBC	No		Yes	Base 64	No	Passwords are first encrypted and then b64 encoded

Secure Development Life Cycle

- Security and privacy threats are constantly being developed, and existing threats are always evolving. To combat such 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 into the design must be an integral part of the product design process itself.

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

- MiCollab was developed in accordance with Mitel's Secure Development Life Cycle policy; as a result, MiCollab has been designed with the best practice safeguards to mitigate risks to the confidentiality, integrity and/or availability of data contained within MiCollab, and to the data related to the functionality provided by MiCollab.

DISCLAIMER

THIS SOLUTIONS ENGINEERING DOCUMENT IS PROVIDED "AS IS" AND WITHOUT WARRANTY. IN NO EVENT WILL MITEL NETWORKS CORPORATION OR ITS AFFILIATES HAVE ANY LIABILITY WHATSOEVER
ARISING FROM IN CONNECTION WITH THIS DOCUMENT. You acknowledge and agree that you are solely responsible to comply with any and all laws and regulations in association with your use of MiCollab and/or other Mitel products and solutions including without limitation, laws and regulations related to call recording and data privacy. The information contained in this document is not, and should not be construed as, legal advice. Should further analysis or explanation of the subject matter be required, please contact an attorney.