A white paper from Mitel

MiCloud Flex as Deployed In iLand Infrastructure Security Whitepaper

1. Purpose

This whitepaper is intended for IT personnel, security personnel, Mitel accredited partners and Mitel personnel. Its purpose is to introduce the security aspects of the MiCloud Flex solution as deployed in iLand VMware infrastructure and the security aspects of the environments that MiCloud Flex is deployed within. This includes the controls put in place and the products and features that are made available to customers to meet their security objectives; the policies Mitel has established, as well as options available to administrators to ensure the secure operation of the MiCloud Flex as deployed in iLand VMware solution.

For customers interested in the security capabilities of the onsite deployed Mitel MiVoice Business Survivable Gateway the MiVoice Business Security Guidelines are available in the Mitel Documentation Center (https://www.mitel.com/document-center/business-phone-systems/mivoice-business/mivoice-business) and should be referred to.

2. Introduction

Mitel takes the business of security seriously by ensuring that the appropriate security measures are available for protecting the confidentiality, integrity, and availability of our customers systems and data. Mitel recognizes that security is a crucial aspect of the MiCloud Flex offering and so at Mitel, the latest technologies and security best practices are used to provide a secure service.

MiCloud Flex is a secure, hosted scalable Unified Communications and Collaboration (UCC) solution with a focus on high availability and dependability, allowing customers to run a wide range of Unified Communications applications.

The core telephony, collaboration and optional services operate in VMware. Each instance of the core services is deployed in its own virtual machine and on their own isolated Virtual LAN (VLAN). This means that each customer's instance is isolated from all of the other customer instances within the data center infrastructure.

A customer cannot contact another customer without routing through the Public Switched Telephone Network (PSTN), as customers are isolated from each other.

Mitel has created an infrastructure and architecture leveraging proven technologies onto which account administrators can layer and customize policies of their own, such as permitted user features and dialing rules.

Protecting the confidentiality, availability, and integrity of customer systems and data is of the utmost importance to Mitel. If your business has the same high standards, MiCloud Flex is the ideal solution for you.

3. Overview of MiCloud Flex

Unlike many other Unified Communications as a Service (UCaaS) offers which are strictly multi-tenanted solutions the MiCloud Flex solution is a hybrid solution utilizing both multi-instance and multi-tenant deployments.

Core telephony, collaboration and key optional services are deployed as multi-instance applications in the iLand provided VMware environment, providing the customer with their own isolated application instances - including Five "9s" availability for the core services.

Other optional services are deployed as highly available multi-tenanted solutions on Amazon Web Services (AWS) platform or Microsoft's Azure Cloud platform.

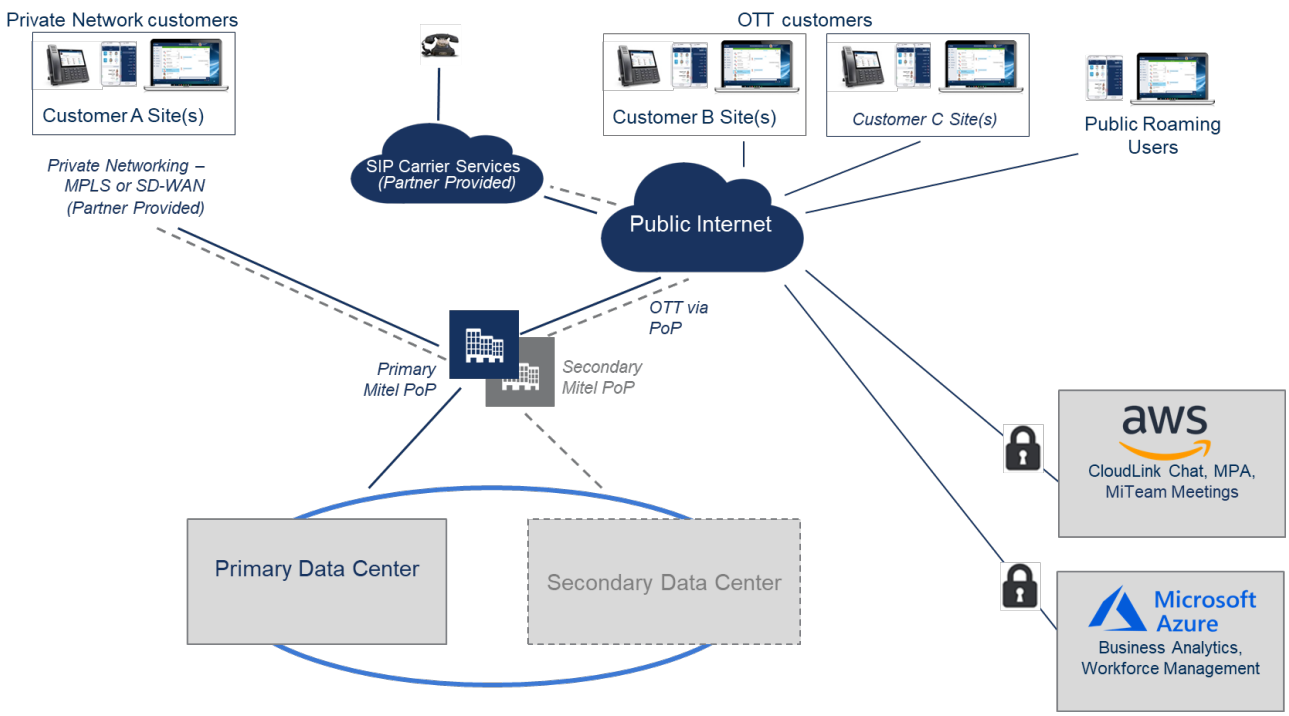
The figure below is a high-level architectural representation of MiCloud Flex solution showing where the various components reside.

As can be seen in the diagram, WAN connectivity, be it Over the Top (OTT), SD-WAN or MPLS terminates into Mitel's data centers. Customer's traffic is further secured, as noted previously, with each customer having their own VLANs isolating their traffic.

MiCloud Flex is available in multiple commercial models:

- **Retail** – sold, billed and serviced by Mitel. This model is available in the USA only and is only offered in exceptional circumstances.
- **Partner Delivered** – sold and billed by Mitel with service subcontracted to the customer's preferred channel partner. This model is available in the USA only.
- **Wholesale** - sold, billed and serviced by the customer's preferred channel partner and is available to all markets that MiCloud Flex is sold in.

The applications and security capabilities of the solution are the same with all selling models. However, audited compliance – specifically HIPAA and SOC 2 - is limited to the Retail model in the USA only. More detail is provided in section 5.



Core Applications – Multi-instance

The core applications, telephony, voice and collaboration tools are all deployed as multi-instance solutions within the VMware infrastructure. The core components are:

1. MiVoice Business: Mitel's IP PBX / Call Control
2. MiCollab: Mitel's Unified communication and collaboration solution which includes:
   - MiCollab Audio, Web and Video (AWV) Collaboration
   - MiCollab Presence engine with calendar integration
   - MiCollab corporate instant messaging
   - And MiCollab (NuPoint) Unified Messaging that also includes a feature rich Auto Attendant known as Call Director.
3. MiVoice Border Gateway (MBG), a Mitel Internet facing edge device that acts as a Session Border Controller (SBC) for SIP trunks and phones, as well as for Mitel proprietary IP phones and applications.

The application layer and derived services are all developed by Mitel, including the IP Desk phones which provides for a seamless security architecture.

All of these applications can be securely accessed by the user through the MiCollab Client – Available as a desktop client, mobile device client (Android and Apple) and through a web browser. The MiCollab Client provides access to enterprise wide instant messaging, voicemail, presence management, display and control (including calendar integration), conferencing and collaboration, and optionally a softphone. All from one simple to use secure interface.

To these core components, other optional applications can be added, including:

Optional Applications – Multi-instance

The following optional applications are deployed as multi-instance solutions in the data center also in VMware with High Availability (HA):

- MiContact Center Business – A feature rich omnichannel contact center solution including an optional speech recognition module powered by Nuance.
- MiContact Center Outbound – comprehensive, integrated outbound campaign management suite that supports all modes of outbound dialing. Powered by Noetica.
- Open Integration Gateway – an Application Programing Interface (API) platform with pre-existing SFDC and Google integrations.
- Mitel Workforce Optimization suite which includes Mitel Interaction Recording, Mitel Quality Management, Mitel Speech Analytics and Mitel Workforce Management

Optional Applications – Multi-tenant

The following optional applications are deployed as multi-tenanted solutions:

- MiTeam Meetings – A cloud-based team instant messaging tool hosted on Amazon Web Services (AWS) utilized by MiCollab
- CloudLink Chat – A cloud-based team collaboration tool hosted on AWS utilized by MiCollab and optionally MiContact Center Business
- Mitel Business Analytics (Tollring) – A suite of cloud-based Business Analytics tools hosted on Microsoft's Azure
- Mitel Workforce Management powered by Teleopti/ Calabrio

Customer Access to MiCloud Flex

Access to MiCloud Flex is available through private connections, such as MPLS and SD-WAN (Mitel or customer provided) which add another layer of network security for the customer, or over the top (OTT) across the Internet. Mitel provided SD-WAN is available in the UK and USA.

NOTE: Not all features and services are available when connecting Over-The-Top. Please contact your local Mitel sales team.

3.1 Multi-Tenant vs. Multi-Instance

As noted in the Introduction and Overview sections, the MiCloud Flex in VMware solution is based on a multi-instance architecture with some non-core services hosted on other cloud platforms that MiCloud Flex interfaces with.

When cloud solutions are strictly multi-tenanted, it means that a single application is tenanted so that each customer has their own space within the application, but the application is a shared resource. Multi-tenanting allows the service provider to oversubscribe the solution, and therefore potentially reduce their own operating costs. These multi-tenanted solutions, by their definition of being tenanted, are not controlled by the customer, but by the service provider.

Additionally, with a multi-tenanted solution there is a possibility that a customer or several customers may consume resources excessively, potentially impacting not only their own ability but also other customer's ability to access resources during peak demand times.

In contrast to these pure multi-tenanted solutions, MiCloud Flex core services – telephony, collaboration and key optional services - are sized to meet the customer's requirements and are deployed as a multi-instance solution in VMWare.

This ensures that the MiCloud Flex core services are always adequately provisioned for peak performance and that customers have control over their MiCloud Flex software updates.

With MiCloud Flex being deployed in VMware the customer has their own secure isolated instances of core applications, this means that a customer does not have their ability to access their applications and resources impacted by other customers who may be performing their own updates.

With the exception of the data center's own scheduled infrastructure updates the customer can make their own MiCloud Flex update decisions and maintain as much control as they want. For example:

- Choose whether they want to perform an update, as the changes may or may not be applicable to their business.
- Choose when to schedule the update, so that they do not disrupt their business at a critical time.
- And as the core components of MiCloud Flex are not a multi-tenanted solution, if one customer requires an upgrade or downtime is required to resolve a problem, other customers are not affected.

This is of benefit to the customer, as MiCloud Flex allows the customer to:

- Have an OpEx based managed service Cloud solution
- Still maintain as much control of their infrastructure as they want to have and
- Decide for themselves whether to accept updates that may or may not be relevant to their business needs

4. Data Center – Key Features

The MiCloud Flex UC solution from Mitel is hosted in VMware infrastructure that is housed in Tier 3+ rated data centers around the globe.

The data center vendors utilized by Mitel include the following capabilities:

Data Center Certifications Include: ISO 27001, PCI DSS, SOC 1 Type 2 and SOC 2 Type 2, ENERGY STAR and LEED Gold

Data Center Connectivity

Diverse fiber points of entry

Redundant high-speed IP connectivity

Carrier-neutral access to over 100 networks and services

Data Center Power

Environment and power 100% uptime SLA, and six 9s (99.9999%) historical portfolio uptime

Two diverse DVP substations

Generators with N+1 redundancy

Fuel: 24 hours, on-site

High-efficiency UPS systems

UPS/PDU/RPP with N, N+1, 2N redundancy

Data Center Cooling

Variable speed Computer Room air handlers and ultrasonic humidification

Smart chillers with evaporative condensing units for air- and water-side economization

Water: Dual water sources backed by on-site wells

N+1 campus cooling towers and chiller plant

N+1 in-room AHU

Data Center Security

Key cards and biometric scanners

Double mantrap entries

Controlled site access Cameras

Perimeter and interior IP-DVR Security Officers

24x7x365 in-house staffed

Data Center Fire Protection

Dual-interlock pre-action dry-pipe sprinkler system

N+1 cooling system, dual-interlock, dry-pipe pre-action fire suppression system with VESDA

4.1 Data Center Physical Access

Physical access to the data center facilities where the production systems reside is restricted to only personnel authorized by Mitel, as required to perform their job function. There must be a very good reason for an individual to visit the facility since as most work can be carried out via Remote Hands request.

Should there be a need for authorized personnel to visit the facility, a ticketing system is used to arrange the visit. A record of the access request, justification, and approval are recorded by management, and access is granted by appropriate individuals. An audit record of all changes made by the individual during the access is logged. Once approval is received, a responsible member of the Infrastructure Team contacts the appropriate subservice organization to request access for the approved individual.

The individual visiting the facility needs to book access in advance and may be subject to screening to confirm identification. This may include biometric data as well as authentication paperwork and then they will be signed in through security.

4.2 Mitel Employee Policy

Mitel employee hiring, on-boarding and off-boarding policies require background checks, security policy acknowledgement, communicating updates to security policy, and non-disclosure agreements.

All Mitel employees are also required to pass an annual code of conduct training course that includes topics such as data privacy and security. Mitel employee off-boarding procedures ensure that all access to facilities and services are revoked immediately.

4.3 Remote Access

Mitel employee access to the MiCloud Flex environment is secured through use of a centralized directory for authentication and connectivity via secured protocols such as TLS 1.2 or better HTTPS connections.

For remote access, Mitel requires the use of VPN using two-factor authentication and any special access is reviewed and must be authorized. Access is limited to employees that require access to perform their role at Mitel.

Mitel employs technical access controls and internal policies to prohibit employees from arbitrarily accessing user files and to restrict access to metadata and other information about users' accounts. To protect end user privacy and security, only a small number of engineers responsible for developing Mitel's core services have access to the environment where user data is stored.

Access between networks is strictly limited to the minimum number of employees and services. For example, Firewall configuration is tightly controlled and limited to a small number of authorized administrators.

All employee access is promptly removed should an employee leave the company or change to a role that no longer requires access.

Customers should always verify their remote access policy with their provider and confirm adherence.

4.4 Data Storage

MiCloud Flex allows the customer to select the region where its content and services are hosted. After a selection is made, subject to any exceptions set out in MiCloud Services: Global Terms of Service, Mitel ensures that all MiCloud Flex data is stored within the designated region.

An exception to the foregoing is when the customer selects multiple regions to form an international deployment. With international deployments, general user information and content is shared across all regions within the customers dedicated environment.

A dual data center high-availability installation requires that systems are hosted in multiple data centers to maintain service levels should the primary lose service. When the primary data center is selected, a designated secondary data center is also defined. The hosted systems will share configuration data to ensure that a user can obtain service from either data center.

4.5 Partner Access Policy

Mitel Partner access is provided via Mitel Performance Analytics (MPA) management portal or alternatively via the iLand Cloud Console depending on the level of access required. In either scenario access is restricted only to the management interfaces of the underlying applications, for user and application configuration. Partners do not have access to any of the underlying infrastructure.

Partner access to a customer is only available after Mitel has instantiated and configured the underlying infrastructure, including the management portal.

Customers have access to only their own specific application portals (if provided) to allow configuration of certain features and functions, including administrator password resets, and user phone-key configuration and call direction, e.g. divert to voicemail.

Users do not have access to the underlying infrastructure.

Access roles within the applications provide user restriction access, such as allowing customer administration staff access, but restricting general users.

4.6 Data Sovereignty

The solution's core components are hosted in Tier 3+ data centers:

- Americas customers access services from data centers located in the USA (Reston Va. and Carrolton Tx.).
- UK customers access services from data centers located in the UK (London and Manchester)
- Australian customers access services from data centers located in Australia (Sydney and Melbourne).
- French customers access services from a primary data center located in Amsterdam, NL with Point of Presence (PoP) in Paris, France. The secondary DC option will be London, UK if required.
- Benelux customers access services from a primary data center located in Amsterdam, NL. The secondary DC option will be London, UK if required

The MiCloud Services – Global Terms of Service, supporting documents and other policy documents may be found at: https://www.mitel.com/legal/mitel-cloud-services-terms-and-conditions .

5.Compliance – A Shared Security Model

Mitel MiCloud Flex provides Unified Communications and Collaboration (UCC) services that can be configured to assist a customer with their security compliance considerations. As with any cloud-based solution the Security and Compliance needs are a shared responsibility.

With MiCloud Flex the shared responsibility is between the data center providers, the VMware infrastructure provider, Mitel, the channel partner / reseller (if applicable) and the customer.

MiCloud Flex computing environments are assessed and audited annually with certifications from accreditation bodies across geographies and verticals. In addition, the MiCloud Flex underlying infrastructure—including the physical and environmental security of its hardware and data centers, continuously undergoes assessments of its own.

By operating in an accredited environment, customers reduce the scope and cost of audits they need to perform, and customers can take advantage of those certifications and simply inherent those controls.

Data Center Security

The data center vendor(s) are responsible for the physical security of the data center. Section 4 describes several of the data center security and availability capabilities. With MiCloud Flex the actual data centers are provided by different vendors based upon geography and include CyrusOne, CoreSite and Equinix. The individual data centers' compliance requirements can be found by exploring each vendors' website.

VMware Infrastructure

MiCloud Flex is a hosted Unified communications solution hosted in VMware. Mitel has chosen to select the VMware infrastructure through iLand (www.iland.com). iLand provide to Mitel the underlying VMware infrastructure such as the host servers, storage area network (SAN), disaster recovery as a service (DRaaS) and virtual switching.

iLand is responsible for any security patches to the underlying virtualization infrastructure including hypervisors and redundancy applications (e.g. Zerto).

iLand's secure cloud holds multiple compliance certifications including ISO 27001, CJIS, PCI DSS and HIPAA. More detail about compliance capabilities of iLand can be found athttps://www.iland.com/services/compliance-services-2/ .

The MiCloud Flex solution uses optional additional cloud based platforms such as Amazon Web Services (AWS) and Microsoft Azure Cloud Services for hosting other MiCloud Flex solution components. Security compliance for these additional cloud platforms is discussed in the section *Other Cloud Based Services.*

Mitel Cloud Operations

Mitel provides the applications running the MiCloud Flex service and ensures that while the applications are in an unconfigured state (Partner Delivered and Wholesale) that a channel partner can be provided secure access to configure the service to the customer's requirements. Mitel is responsible for creating security patches for the applications.

Mitel data protection addendum and terms of service are available as follows:

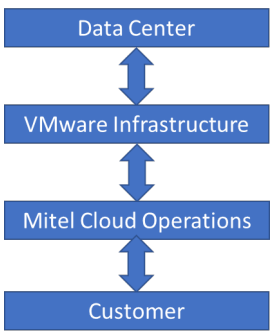
MiCloud Services – Global Terms of Service:https://www.mitel.com/legal/mitel-cloud-services-terms-and-conditions

Data Protection Agreement (DPA): https://www.mitel.com/legal/gdpr/dpa

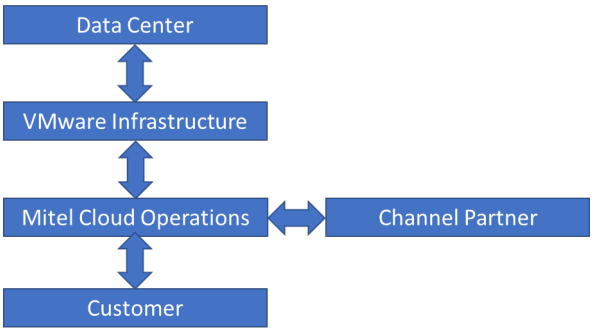
Mitel Application Privacy Policy:

https://www.mitel.com/en-ca/legal/mitel-application-privacy-policy/mitel-application-privacy-policy-en The sales and service model provided to the customer with MiCloud Flex has a direct relationship as to where compliance responsibilities will lie.

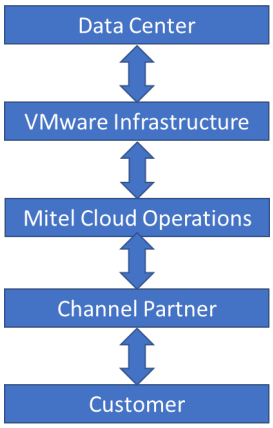
Retail (USA): with the MiCloud Flex Retail model (USA only) Mitel is responsible for the sales, service and billing of the customer. MiCloud Flex (USA) has been independently certified to comply with and meet HIPAA and SOC 2 regulation for both physical and technical requirements on multiple occasions.



Partner Delivered (USA): with the MiCloud Flex Partner Delivered model Mitel provides the sales and billing, however the implementation and service is provided by the customer's preferred channel partner. While MiCloud Flex has been audited to be HIPAA and SOC 2 compliant, for the compliance to be applicable to this model the Channel Partner must also have been independently audited and found to be meeting the same compliance levels as Mitel or better.



Wholesale (Global): with the MiCloud Flex Wholesale model Mitel's role is limited to creation of the applications. The implementation, configuration, selling, service, and billing is the responsibility of the Channel Partner. The Channel Partner is therefore responsible for any compliance of the solution with the end customer.



Channel Partner

The Channel Partner is responsible for the configuration and ongoing maintenance of the customer's applications (supported by Mitel as needed) in the Partner Delivered and Wholesale models, and for ensuring that they are configured to the customer's stated requirements including security settings that can be configured if not already enabled by default. The channel partner is responsible for applying security patches to the applications at a time that is acceptable to the customer. In the Retail model (USA) Mitel takes on this role.

Customer

It is the responsibility of the customer to ensure that any service that they purchase meets their compliance requirements. It is also the customer's responsibility to ensure that their implementation of the solution, working with their Channel Partner (Partner Delivered and Wholesale) or Mitel (Retail), is compliant to the particular level or standard and that all associated data is classified appropriately for that security compliance requirement. The MiCloud Flex applications security features and capabilities will assist customers with these needs.

6 Other Optional Cloud Based Services

The MiCloud Flex solution uses additional cloud-based platforms such as Amazon Web Services (AWS) and Microsoft Azure Cloud Services for providing Mitel customers with access to additional applications and services.

6.1 Amazon Web Services

Amazon Web Services (AWS) is used to host the Mitel CloudLink platform, the Mitel Performance Analytics management tool, the chat components of MiCollab and MiContact Center Business and MiTeam Meetings.

Amazon Web Services provides a highly reliable, scalable cloud infrastructure platform within the customer's geographic region. AWS services and data centers have multiple layers of operational and physical security and AWS is compliant with numerous industry-recognized security certifications and audits.

Connectivity to Amazon Web Services is via a secured channel over the Internet. For more information regarding AWS security refer to: https://aws.amazon.com/security/ . For more information regarding AWS security compliance refer to: https://aws.amazon.com/compliance/programs/

6.1.1 Mitel CloudLink

Mitel's CloudLink platform is built on the Amazon Web Services (AWS) cloud computing platform. The AWS platform provides CloudLink users with enterprise level high availability, stability, multi-layered security, and data protection.

The CloudLink platform is used to deliver the following applications and services.

MiTeam Meetings - A cloud-based team collaboration tool

CloudLink Chat - A cloud-based team collaboration tool utilized by MiCollab and optionally MiContact Center Business.

Additional services provided by the CloudLink platform include Identity and Access Management (IAM), chat, presence, notifications, workflow, media services, and Short Message Service (SMS).

European customers access the CloudLink services from AWS data centers located in Europe, Americas customers access the CloudLink services from AWS data centers located in the

Americas. These applications are discussed in further detail in the section *Application Security*.

6.1.2 Mitel Performance Analytics Management Tool

Mitel Performance Analytics (MPA) is a cloud-based management tool that is hosted on AWS. MPA is the administration tool that is accessible to the Mitel partner and the customer and supports two factor authentications for secured encrypted access.

MPA is used for performing MiCloud Flex system management, administration, configuration, data provisioning, voice quality monitoring, data synchronization, accounting, configuration of application interfaces and alarm and maintenance functions.

The MPA voice quality monitor can forewarn of any voice quality issues, which will allow the partner to take timely corrective actions.

When MPA is used to manage the MiCloud Flex components, the partner will use an OTT connection to the MPA server to manage the solution.

MPA consists of two components, the MPA server and the MPA probe. The MPA server is hosted on AWS infrastructure. The MPA probe is a software application that is deployed within the MiCloud Flex network on the customer's VLAN in the data center. The MPA probe communicates with the Mitel applications directly, these communications are fully contained within the customer's VLAN that the applications and probe are deployed within the data center. The MPA probe forwards status and events from the MiCloud Flex network and provides secure access to the application's native management

interfaces. The MPA probe performs some caching of status and events in the event of communication difficulties

between the probe and the MPA server. MPA, in conjunction with the probe, supports a secure Remote Access Service to the customer applications in the data center. MPA Remote Access provides several key advantages:

- There is generally no need to configure firewall rules at either end of the remote connection because MPA Remote Access uses outbound connections from the Probe employing standard TCP/IP protocols.
- No VPN server or client software is required, at either end of the remote connection.
- The MPA Remote Access service manages all of the security tokens required to establish a secure remote connection, avoiding the need to maintain multiple lists of VPN access credentials.
  The MPA communication links are secured using industry standard encryption and authentication mechanisms.
- System Authentication: MPA uses a 2048-bit security certificate and authenticates all connection requests.
- TLS: All TLS sessions to MPA are encrypted and authenticated using RSA-2048 for key exchange and AES 128 for encryption.
- SSH: All SSH sessions are encrypted and authenticated using RSA-1024 with a rotation for key exchange and AES 128 for encryption. Key Rotation is enabled and generates a new key for each session.

For more information on MPA security refer to the document Mitel Performance Analytics, found at: https://www.mitel.com/document-center/security/technical-papers

6.2 Microsoft Azure Cloud Services

MiCloud Flex customers are able to access Business Analytics and Workforce Management applications that are hosted on Microsoft Azure Cloud Services platform.

The Business Analytics and Workforce Management applications that are available, work in conjunction with Mitel's Unified Communications applications which gives customers the ability to optimize their business operations. Connectivity to the Azure platform from the customer's site is via a secured channel over the Internet. The Azure platform is designed with multilayered security controls which are applied to Azure data centers, infrastructure and operations. Azure is deployed in globally distributed data centers providing geographic resiliency and reliability. Azure is compliant with numerous industry recognized security certifications and audits. For more information related to Microsoft Azure Cloud Services, refer to: https://azure.microsoft.com/enca/overview/#security

6.2.1 MiCloud Business Analytics - Tollring

Tollring is the provider of Mitel's optional cloud-based Business Analytics. MiCloud Flex employs Tollring's Insight and Report Licensed Capabilities products.

Tollring applications are hosted on Microsoft Azure Cloud platform, and there are numerous Azure Cloud data centers that are globally distributed. The location of the Azure Cloud data center will be determined by where the customer is located and the customer's own requirements.

European customers will use the Azure data center in the Netherlands, there are also Azure data centers located in the U.S., the UK and Australia.

Tollring applications collect SMDR data from the MiVoice Business instance in MiCloud Flex, the data collected is then processed by Tollring to create online dashboards and reports detailing business communications usage and call statistics on a per user basis.

Access to Tollring technology resources is only permitted through secure connectivity and requires authentication. Tollring's password policy requires complexity, expiration and lockout.

Access to resources is restricted and closely monitored. Access is granted only for the period necessary to perform administrative or technical support tasks and is revoked after tasks are completed. All permissions are reviewed quarterly.

Tollring ensures that all data transmissions are encrypted using secure TLS cryptographic protocols and that data at rest is also encrypted.

Tollring is compliant with the ISO 27001 Information Security Standard and ISO 9001 Quality Management System. Tollring re-certifies those compliances annually. Tollring is compliant with and follows the General Data Protection Regulation (GDPR).

Further information about Tollring's company policies, security compliances, security practices and white papers may be found at: https://tollring.com/policies

6.2.2 Mitel Workforce Management

An important component of Mitel's Workforce Optimization (WFO) suite is Mitel Workforce Management (WFM) powered by Teleopti/Calabrio. Mitel's WFM solution integrates with MiContact Center Business and provides MiCloud customers with an enterprise caliber workforce management solution.

Mitel Workforce Management is hosted on Microsoft Azure Cloud platform which ensures a high level of availability. Customers are able to select AWS data centers in a geographic region that is appropriate for their requirements.

Mitel Workforce Management software and applications encrypt all customer data, while in use, transit and while at rest.

Teleopti/Calabrio has experience and knowledge related to helping customers understand how to meet the requirements of PCI, HIPAA, Sarbanes-Oxley, Frank-Dodd, or MiFID. Calabrio can provide contact center managers with tools to detect fraud, conduct investigations and mitigate specific security risks in a wide range of markets, including financial, retail, government and healthcare.
Teleopti/Calabrio has published a number of security documents that discuss PCI requirements, GDPR requirements, CCPA requirements and Cloud security, these documents are located at the following sites.

https://www.calabrio.com/resource-center/white-papers-reports/

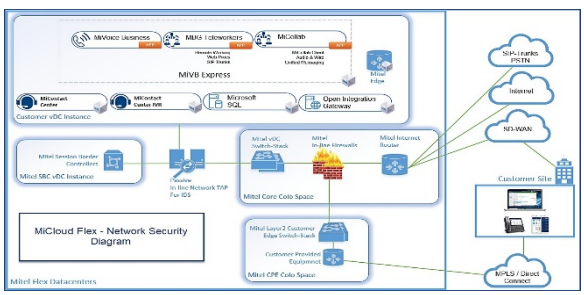
https://www.calabrio.com/resource-center/collateral/

7. Network Security and Connectivity

Mitel diligently maintains the security of the back-end network. Mitel identifies and mitigates risks via regular application, network, and other security testing and auditing by both internal security teams and third-party security specialists.

Mitel's network security and monitoring techniques are designed to provide multiple layers of protection and defense-in-depth strategies.

Mitel employs industry-standard protection techniques, including firewalls, network security monitoring, and customer ingress and egress intrusion detection systems to ensure only eligible traffic can reach the Mitel application infrastructure.



All MiCloud Flex applications are located in Tier3+ data center facilities. Connections from the customer site to the data centers can be made via an MPLS connection, SD-WAN or an Over-The-Top connection (OTT). Customer connections are logically isolated using different VLANS.

Mitel provided SIP carrier services are also terminated in the data center.

7.1 OTT Connectivity

Traffic originating from devices connected via the Internet such as OTT users and Teleworkers connect to the customer's MiVoice Border Gateway (MBG) across redundant Internet carrier circuits into the data center.

Before the traffic is granted access to the customer's VLAN in the data center, the traffic must be authenticated by the MiVoice Border Gateway, a Session Border Controller that is designed for Mitel solutions. Mitel devices further protect the traffic by encrypting signaling with TLS 1.2 and audio and video with SRTP 128-bit AES encryption.

7.2 Private WAN Connectivity

When using a private WAN to connect the customer site to the data center (e.g. MPLS or SD-WAN) the traffic must pass through a redundant firewall which ensures that only valid traffic is passed onto the customer's dedicated VLAN. Mitel devices further protect the traffic by encrypting signaling with TLS 1.2 and audio and video with SRTP 128-bit AES encryption.

7.3 Mixed Connectivity

MiCloud Flex also supports mixed connectivity, meaning that connections may be made over an MPLS connection and also an Over-The-Top Internet (OTT) connection so that users located at the customer's site and also remote workers can be connected simultaneously, however a user cannot be both an OTT user and an MPLS user from the same desktop.

7.4 SIP Trunk Connectivity

With MiCloud Flex SIP Trunks are provided through either the channel partner (Wholesale) or by Mitel (Retail and Partner Delivered) and in both cases are connected over a dedicated carrier link using a publicly routable IP address into the data center.

The SIP Trunk traffic is further authenticated by the MiVoice Border Gateway, a Mitel purpose-built Session Border Controller which supports SIP signaling encryption using TLS 1.2 and Secure Real Time Protocol (SRTP).

7.5 Customer Isolation

Customer isolation is an important security feature of MiCloud Flex. As noted elsewhere is this document, the core telephony and collaboration applications and key optional

services are deployed as multi-instance applications in the data center hosted environment.

Each customer's applications are installed in the customer's own dedicated virtual machines and VLAN within the data center, customers are isolated from each other and traffic cannot pass between different customers.

8. Application Security

The primary security concerns for IP Telephony, UC applications and networks can be summarized as follows:

Confidentiality: The need to protect transmissions, whether for voice-streaming, video streaming or data services, to prevent eavesdropping or interception of conversations, conferences, call control signaling or passwords and the confidentiality of data storage.

Integrity: The need to ensure that information is not modified by unauthorized users and to unequivocally prove a user or application is authorized to perform the task / function they are requesting, be it a voice call, video conference or a configuration change.

Availability: The need to ensure the operation of the solution at all times.

8.1 Mitel IP Phones with MiCloud Flex

MiCloud Flex supports the following Mitel IP Phones

- 6905, 6910, 6920, 6930, 6940, 6970.
- MiVoice Business Console
- 5304, 5312, 5324, 5320(e), 5330(e), 5340(e), 5360
- Wireless and DECT Phones including the RFP 12, 44, 45, 47, 48; 112 DECT; 612d, 622d and 623d
- MiCollab SIP Softphone including ACD hot desking

Please refer to the current engineering guidelines for the most up to date list of supported devices

8.1.1 Mitel Authentication: Known Devices and Users Only

With MiCloud Flex all IP Telephony devices and applications are reliant on the hosted call control engine for call establishment, tear down, transfer, etc. The MiCloud Flex call control must authenticate the device or application prior to providing it with service. Mitel phone authentication requires a unique association of device MAC addresses, Mitel set type and user-entered PIN registration numbers to successfully register with the call control engine. All communications are sent and received across a TLS encrypted channel.

Additionally, desktop phone software downloads are cryptographically protected.

SIP devices require a username and password combination. Mitel forces the use of strong username / password combinations which are sent and received across a TLS encrypted channel.

For sites where customers have controlled the access to their LANs with the IEEE 802.1X authentication protocol, Mitel also provides the option for IP phones to use 802.1X authentication.

Current models of Mitel IP phones support the IEEE 802.1X authentication protocol. Most phones support EAP-MD5, EAP-PEAP, and proxy logoff. The 6905, 6910, 6920, 6930, 6940 and 6970 also support EAP-TLS. Refer to the current Mitel IP Sets Engineering Guidelines for the most current information.

8.1.2 Call Signaling

To be able to make a call, a device must be authenticated and registered with the call control engine as described above.

Assuming the device has registered successfully, the call control engine then determines if a device is authorized to use a feature based on the device's Class of Service (CoS) or make a given call based upon its dialing privileges Class of Restriction (CoR).

This authentication decision to allow or bar a call or use a feature is invoked each time a user uses their device.

Signaling between MiCloud Flex and a Mitel IP phone uses a proprietary signaling protocol known as MiNET which is sent and received over a Transport Layer Security (TLS) encrypted channel. Secure MiNET is the default encryption method

MiCloud Flex also supports Mitel softphones which are SIP based, and Mitel approved standards-based SIP devices, all communications between the SIP device and MiCloud Flex are sent and received over a SIP TLS encrypted channel.

MiNET and SIP call signaling protocols are supported simultaneously from the same system.

8.1.3 The Media Path

With MiCloud Flex the encrypted voice and video IP media packets are routed over the optimum network path. That is packets do not 'hairpin' through the data center unnecessarily.

This results in reduced WAN bandwidth requirements and call latency is optimized and this results in improved call quality.

The MiCloud Flex call control engine simply provides the devices with the details needed to establish a

direct media path between one another and the media then takes the optimal path.

By default, with Mitel IP phones the media path encryption is accomplished with Secure Real Time Transport Protocol (SRTP) using 128-bit Advanced Encryption Standard (AES).

SRTP requires consistent end-to-end encrypted media negotiations; therefore, every component that negotiates SRTP with a SIP endpoint must comply with RFC 4568.

8.1.4 VMware Storage Encryption

The MiCloud Flex solution utilizes a Storage Area Network (SAN) which is encrypted providing encryption for data at rest using the Mitel Advanced Security option. An additional layer of security is available to customers by performing encryption of the individual virtual machines on top of the encrypted AES-256 XTS encrypted SAN.

8.2 MiCollab Client

The MiCollab Client application allows a user to securely collaborate with other users from their desktop. It gives users full access to their Mitel accounts and runs on Windows or Mac operating systems with presence management, unified messaging access, video chat, instant messaging, collaboration, and an optional softphone and is also available through web browser access. It allows users to access functionality through their browser across HTTPS / TLS connections without installing a client. The desktop client application is distributed by the administrator and users cannot connect without the express consent of the administrator.

Communications between the client and the MiCollab server are across HTTPS connections with Transport Layer Security (TLS) 1.2.

The same MiCollab user functionality is also available from a mobile device with the Mitel app available for iOS, Android, mobile devices, and tablets, allowing users to collaborate while on the go. Communications are across HTTPS connections with Transport Layer Security (TLS).

MiCollab Mobile Clients are distributed through the Google Play store and the Apple Store.

The optional softphone available for the desktop or mobile MiCollab clients has an encrypted call path (SRTP) and an encrypted call signaling path (SIP TLS).

Non-voice communications continue to use HTTPS / TLS. The desktop softphone is often used in combination with the MiContact Center Business application so that agents do not require a desk phone.

For MPLS connected systems, MiCollab client users authenticate with the MiCollab server typically via Active Directory (AD) integration (recommended) for single sign on, though local authentication is also supported, so that password and other security rules governed by the AD administrator can be utilized.

AD authentication requires that a private WAN connection is used to connected to the customer AD server. AD integration is not supported when using OTT connections.

For MiCollab connections split DNS I used to ensure that the FQDN is resolved correctly by both internal and external connected users.

8.2.1 MiTeam Meetings and CloudLink Chat

MiTeam Meetings

MiTeam Meetings is an optional CloudLink based multi-party video solution designed for MiCollab users who want to improve work efficiency and enhance workplace communication with seamless transitions between voice, video, and chat capabilities for a complete collaboration experience. 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

The MiTeam Meetings service is hosted on the Amazon Web Services (AWS) cloud computing platform using Amazon's Simple Storage Service (S3).

CloudLink Chat

CloudLink Chat is a Chat application that is enabled by the CloudLink Platform. Files and links in CloudLink Chat are not executed by the CloudLink Chat service and the Chat service does not access any content uploaded by the user.

CloudLink Chat runs on a serverless deployment using Amazon Web Services (AWS) S3 ElasticSearch foundation services to store data.

Data in Transit

Data in transit between a Mitel client (desktop, mobile, API, or web) and the hosted service is always encrypted via TLS 1.2 and Web Real-Time Communications (WebRTC) is protected by 256-bit or higher Advanced Encryption Standard (AES) encryption.

Mitel uses strong ciphers and supports perfect forward secrecy. Individual sessions are identified and re-verified with each transaction, using a unique token created at login.

Data at Rest

Server-Side Encryption (SSE) is used to encrypt the data stored at rest in Amazon S3. Amazon S3 ServerSide

Encryption employs strong multi-factor encryption. Each object is encrypted with a unique key. As an additional safeguard, this key itself is encrypted with a regularly rotated master key.

Security documentation for MiTeam Meetings and CloudLink Chat may be found at: https://www.mitel.com/document-center/security .

8.3 MiContact Center Business

Contact center agents use the browser accessed Mitel Ignite client for their contact center agent experience. Agents can authenticate with the MiContact Center Business server via Active Directory integration for single sign on (recommended) or through local authentication. Browser access uses HTTPS/TLS for communication between the agent's Ignite web client and the MiContact Center Business server. This functionality is available to OTT and SD-WAN/MPLS connected customers, with the exception of onsite AD integration which requires MPLS connectivity.

8.3.1 Workforce Optimization - Mitel Interaction Recording (Call and screen recording)

Mitel offers advanced capabilities that can be leveraged by Cloud deployments that fall within the "Mitel Workforce Optimization" suite. As part of Mitel's Workforce Optimization (WFO) suite, Mitel has four applications that come from Mitel's OEM partner, ASC Technologies, including:

- Mitel Interaction Recording (Call and Screen Recording)
- Mitel Quality Management (Quality Management)
- Mitel Coaching and Learning (included in the Quality Management module)
- Mitel Speech Analytics (Transcription and Keyword spotting)

This release of MiCloud Flex provides the Mitel Interaction Recording solution as an option. Mitel Interaction Recording is the base to offer Mitel Quality Management, Mitel Speech Analytics and Mitel Coaching and Learning. Quality Management is required to offer Speech Analytics.

Mitel Interaction Recording and analytics products are in compliance with the highest security requirements and regulations such as MiFID II.

Mitel Interaction Recording is hosted in the customer's dedicated Virtual Machines hosted on their dedicated VLAN in their regional data center(s). Data center redundancy is available providing for a high level of service uptime..

Customers in sectors such as emergency services and financial services need to ensure that transactional recordings will be completely intact and permanent even in the event of a system failure. Mitel Interaction Recording's high level of availability ensures that these regulatory requirements pertaining to recording system availability can be met.

The recording and storage of customer transactions and conversations must be performed with the highest security protections in order to prevent access by unauthorized personnel.

Data encryption is a mandatory requirement. As such, data in transit is encrypted and the application is capable of recording all conversations in encrypted formats.

All system user and administrative activity and interactions are monitored and logged in detailed audit logs. These audit logs are kept, providing the customer with a full audit trail.

Documentation for Mitel Interaction Recording is available on Mitel's Document Center.

https://www.mitel.com/document-center

ASC Technologies' web site is located at:

https://asctechnologies.com/english/index.html

ASC Technologies compliance information related to fraud detection, MiFID II, FinVermV and GDPR can be found at the following location:

https://asctechnologies.com/english/compliance.html

8.4 Teleworker Capability

All of the Mitel IP phones, and a number of the applications offered by the MiCloud Flex solution are available to be connected to the Data Center over the Internet securely using the MiVoice Border Gateway (MBG) as the Internet facing Mitel application proxy and Session Border Controller.

This is also known as the Mitel Teleworker Service which securely connects remote IP phones, softphones and Mitel applications, such as collaboration and contact center tools to the data center providing full access to Mitel services all without the need for a VPN.

Voice communications are authenticated before being allowed access through the MBG where they are then further authenticated against the actual application.

UDP ports are opened and closed on call set up and tear down so that ports are not open without a valid call. Voice signaling is encrypted with TLS and media streams with SRTP.

Teleworker security is discussed further in the Mitel document Security and the Teleworker Whitepaper, which can be found at:

https://www.mitel.com/document-center/security/technical-papers

9 MiCloud Flex Availability

A communication and collaboration system must be reliable, and a key feature of MiCloud Flex . To that end, Mitel has developed the MiCloud Flex solution with multiple layers of redundancy and resiliency to guard against data loss and ensure availability.

The MiCloud Flex applications are installed in a Tier 3+ data center in a VMware cluster that is using a redundant Storage Area Network (SAN) and VMware High Availability for host server redundancy.

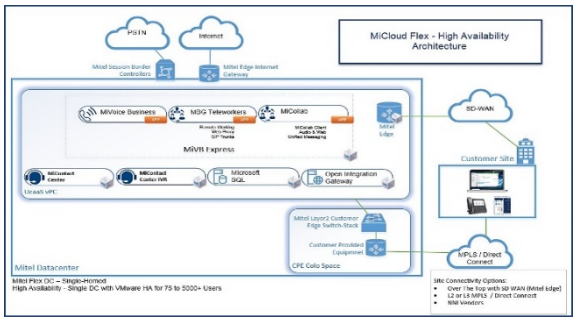
The customer has the choice of installing in:

• A single data center – Applications are protected by VMware High Availability,

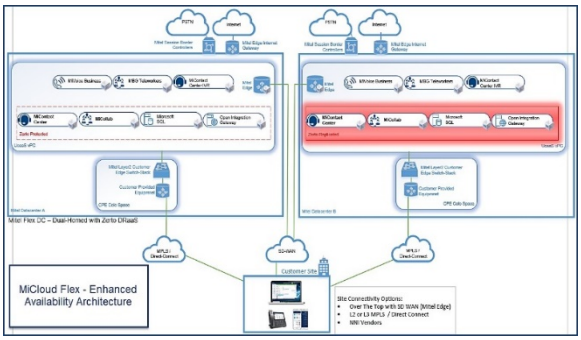
• A single data center with local survivability – Adds local application availability in the event of WAN communications being interrupted, or

• Dual data centers - Whereby using internal application resiliency and Zerto Disaster Recovery as a Service (DRaaS) a customer is protected from data center outages.

This flexibility in deployments allows customers to create the service level needed for their business. All variants include VMware High Availability and redundant SAN.



When installed in dual data centers, several of the Mitel applications, including the IP telephony, have built in application level resiliency whereby the applications (or end points) switch to the secondary data center in the event of a problem being detected.



For applications that do not have this level of inbuilt resiliency, Mitel also optionally provides the ability to have application replication between data centers using Zerto when using dual data centers.

Application resiliency and Zerto capabilities are in addition to the intrinsic VMware High Availability (HA) functionality.

The MiCloud Flex data center connectivity is available over several Wide Area Network (WAN) technologies including, over the top Internet (OTT), MPLS, NNI and SD-WAN. OTT users can be mixed with the other WAN connected technologies, allowing some users to be on net and others to be off net.

In addition, daily incremental and weekly full backups are performed on all customers' systems.

In order to improve the availability of the core services further, and to counter the threat of a large incident in one region impacting service availability, the MiCloud Flex solution is deployed in two different geographical regions in each country. The primary data center is located hundreds of miles from the secondary data center.

Deploying MiCloud Flex in two geographically different locations ensures that a system is always available, even if one of the data centers becomes unavailable.

When installed in dual data centers, several of the Mitel applications, including IP telephony, have built in application level resiliency whereby the applications (or end points) switch to the secondary data center in the event of a problem being detected.

Five '9's Availability for Core Applications

Deployment across different dual data centers and regions offers Five '9s' (99.999%) of service availability. This availability is offered across the core voice services. It does not apply to all of the applications.

The core voice services that are offered with Five '9s' of availability are:

- MiVoice Business - Call Control
- MiVoice Border Gateway – SBC Function
- Mitel Performance Analytics – Management
- MiContact Center IVR – Contact Center
- MiCollab Softphone – Calling Functionality
- Mitel IP Phones, MiNET and SIP
- Mitel approved 3rd Party SIP Phones

Availability of cloud hosted services is reliant on the connectivity to the data center and for customers wanting the best uptime the connectivity should have guaranteed service levels as well.

Availability of Non-core Applications

The availability of non-core applications varies based on how the application is designed and also how the application is deployed. Resilient operation of noncore applications is identified in the following table.

Application	Primary	Secondary	Resilient	Primary Service outage outcomes
MiVoice Business Call Control	Yes	Yes	Yes	Voice Service switches to secondary controller
MiVoice Border Gateway	Yes	Yes	Yes	Voice Service switches to secondary gateway
MPA Management	Yes	Yes	Yes	Dual deployment allows access to both primary and secondary regions
MiContact Center Business	Yes			Available on recovery of primary service
MiContact Center IVR	Yes	Yes	Yes	Voice Services and call routing continue in service. The SIP SP must also be configured to route to both primary and secondary gateways
Call Recording & Playback	Yes	Yes		Call playback and access to the database will not be available. Available on recovery of primary service
Call Recorders	Yes	Yes	Yes	Call recordings are available on recovery of primary service
Screen Recorders	Yes	Yes	Yes	
MiCollab Softphone Call	Yes	Yes	Yes	Softphone will re-home to primary or secondary region. Calls can be made and received.
MiCollab Softphone Directory Calling	Yes			Directory lookup may be impaired for new searches. Cached information may still be used.
MiCollab Chat	Yes		Yes	MiCollab Chat redirects to use the CloudLink Chat on AWS. Once connection is established, connection is direct to CloudLink chat.
MiCollab Presence	Yes			MiCollab Presence information will become available on recovery of the primary service.
MiCollab AWV Collaboration	Yes			MiCollab Collaboration will become available on recovery of the primary service. MiCollab Collaboration using MiTeam and CloudLink will continue to be available
MiTeam Meetings	Yes		Yes	MiTeam meetings are provided via CloudLink MiTeam Meetings application. MiCollab is used primarily for management and initial configuration.
MiNET Phones	Yes	Yes	Yes	Service moves to secondary gateway or controller
3rd party SIP phones	Yes	Yes	Yes	For phones that support DNS-SRV, service switches to secondary gateway or controller

9. Management Features

MiCloud Flex is designed with multiple layers of protection, covering data transfer, encryption, network configuration, and application level controls, all distributed across a scalable, global, and secure infrastructure.

MiCloud Flex authorized users can access their data through robust access controls defined at deployment. With the MiCloud Flex multi-instance architecture delivering the service, customers are assured that information is not shared and is isolated to their environment, enhancing security.

9.1 Management Access Control

Mitel applications offer capabilities to define, enforce, and manage user access policies across MiCloud Flex. These include:

- Audit trails track application changes logging the date, time, changes made, and the user that performed the modification.
- Integration with the customers Active Directory or LDAP compliant identity broker for user authentication and provisioning is supported with MPLS connected systems.
- Password policies that force users to use strong passwords. Such policies can include password length and form.

9.2 Password Control

MiCloud Flex enforces password policies. Administrative accounts must be configured to comply with the following password constraints:

- Require at least one of each the following character elements:
    - Lower-case letter
    - Upper-case letter
    - Numeric Digit
    - 'Special' character enforcement e.g. !@££()*&^%$;:'\|"[]{}=+-_<>/?`~

10. Toll Fraud Management

Toll fraud is the action of an unauthorized use of a business' telephone system and carrier services. The primary purposes for this are to profit from a toll line and international revenue sharing fraud.

Mitel implements several controls to restrict user feature access and dialing rules. These include:

- Class of Service
- Class of Restriction
- Interconnect Restrict
- Account codes

These controls are used to define the available features, dialing restrictions, and interconnectivity of devices and trunks in predefined situations.

It is the partner's and/or the customer's responsibility to ensure that the feature access and dialing rules are correctly configured to protect the customer from toll fraud. Mitel can only provide recommendations.

Ensuring that dialing rules and restrictions on SIP trunks provided by SIP trunk providers are correctly configured is the responsibility of the partner.

10.1 International Dialing Restrictions

The default configuration for customers can be templated to deny access to dial all or specific international and premium rate numbers. Mitel recommends that calls to pay-per-call and pay-per minute services (potentially including directory assistance services) are templated, so they are blocked by default. Ensuring that dialing restrictions and Automatic Route Selection (ARS) are correctly configured is the responsibility of the entity responsible for system programing which differs depending upon the selling model but is ultimately guided by the customer's documented requirements.

11. Data Privacy

Guarding users' privacy and that of their business data is taken seriously at Mitel. Mitel works hard to protect user information from unauthorized access.

All data requests are scrutinized to make sure they comply with the law and Mitel is committed to giving users notice, as permitted by law when their accounts are identified in a law enforcement request.

Only data required to provide the UCC services is collected and processed.

11.1 GDPR

Respecting the privacy of our customers and partners has always been integral to the way Mitel operates.

As a data processor, Mitel provides a pre-signed Data Processing Addendum (DPA), which outlines how we process customer data when Mitel provides MiCloud Flex services. Mitel's DPA meets the requirements of GDPR Article 28.
https://www.mitel.com/legal/gdpr/dpa

11.2 Product Security Documentation

GDPR and data protection documentation for individual Mitel products and applications that are included in the MiCloud Flex solution can be found at:

https://www.mitel.com/document-center/security/personal-data-protection-and-privacy-controls Other MiCloud Flex security documentation can be found at

https://www.mitel.com/document-center/security/technical-papers

12. Summary

MiCloud Flex offers easy-to-use tools to help deliver enterprise class unified communications to its customers, without sacrificing the security that organizations require.

With a multi-layered approach that combines a robust back-end infrastructure with a customizable set of policies, we provide businesses a powerful solution that can be tailored to their unique needs.

To learn more about MiCloud Flex , contact Mitel or one of our approved partners at:

- Mitel: https://www.mitel.com/contact
- Partners: https://www.mitel.com/partners

13. Need to Know More?

Mitel has several whitepapers available that offer detailed descriptions of the security measures in place at Mitel.

Name	Description	Link
Mitel Secure Development Life Cycle	This paper provides an overview Mitel's Secure Development Life Cycle (MiSDLC), the customer benefits and the key aspects of MiSDLC. This paper also covers the key components of Mitel's Product Security Incident Response Process (PSIRT).	https://www.mitel.com/document-center/security
Mitel's Product Security Policy	The Product Security Policy discusses how Mitel assesses security risks, resolves confirmed security vulnerabilities, and how the reporting of security vulnerabilities is performed.	https://www.mitel.com/support/security-advisories/mitel-product-security-policy
Mitel Product Security Advisories	Product Security Advisories are published for moderate and high-risk security issues.	https://www.mitel.com/support/security-advisories

To find out more about MiCloud Flex Please visit:
www.mitel.com/products/business-phone-systems/cloud/micloud-flex