Mitel MiCloud Flex

SECURITY OPERATIONS GUIDELINES

VERSION 1

MAY 2021

NOTICE

TRADEMARKS

Mitel MiCloud Flex
Security Operations Guidelines
Version 1
May 2021

Table of Contents

Purpose

This document will be of interest to Mitel Partners that are offering Mitel's MiCloud Flex Cloud services via the Wholesale or the Partner Delivered cloud services delivery models.

The information in this document is intended to assist Mitel's Partners with achieving security regulations compliance. This document identifies the areas where security compliances are required, and what is required for achieving and maintaining security compliance in the specific area.

This document identifies the security features and controls that are available on the various applications and products that comprise the MiCloud Flex solution. This document is not intended to be a solution level security guideline, for detailed information regarding application and product security features and controls, the Partner should refer to the security guidelines for the individual applications and products that comprise the MiCloud Flex solution.

Introduction

MiCloud Flex needs to meet a range of security compliance requirements for both the Wholesale and the Partner Delivered delivery models. To meet the compliance requirements requires that the security controls associated with the underlying applications are correctly configured when the solution is first deployed and that the configuration of the security controls is maintained during the operating life cycle of the solution.

Mitel is making MiCloud Flex available via the following delivery models:

- MiCloud Flex Wholesale
- MiCloud Flex Partner Delivered (US only)

Related Documentation

The following related documentation may be of interest to Mitel partners.

- MiCloud Flex Deployment Guide
- MiCloud Flex Engineering Guidelines
- MiCloud Flex Security Technical Paper

MiCloud Flex combines several different products into a hosted solution. The individual product related Engineering, Administrative and Security documentation may be found on Mitel’s web site.

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

What is new in this release

MiCloud Flex deployed on iLand data centres with a General Availability of May 2021 is the initial release product offering.

Overview of MiCloud Flex Delivery Models

The MiCloud Flex solution is offered through the following delivery models. Both models deliver the same MiCloud Flex solution to the customer, however the division of responsibilities between Mitel and the Partner changes depending on the delivery model.

MiCloud Flex Wholesale (Global)

The MiCloud Flex Wholesale offer from Mitel is available in various global markets. Under this market model:

- Mitel contracts with the Partner and the Partner contracts with the customer.
- The Partner bills and collects from customer and is responsible for including any taxes and regulatory fees.
- The Partner supplies the carrier services and the customer interconnect.
- The Partner is responsible for data collection, system configuration and user provisioning.
- The Partner is responsible for providing the customer with Level 1 and Level 2 technical support.
- Mitel is responsible for deploying the associated applications and tenants and providing Level 3 and Level 4 support to the Partner.

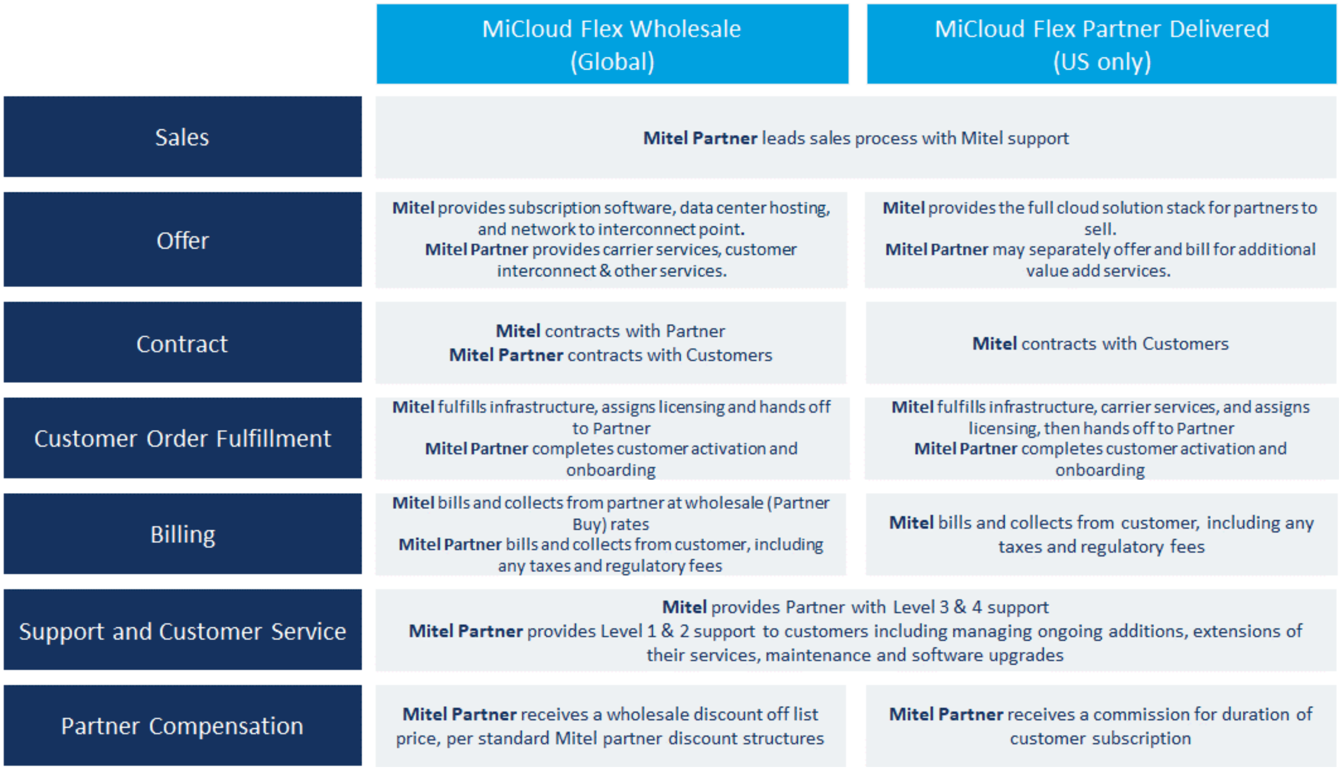
MiCloud Flex Partner Delivered (U.S. Only)

The MiCloud Flex Partner Delivered offer from Mitel is available only in the U.S. market. Under this market model:

- Mitel contracts with the customer.
- Mitel bills and collects from the customer, including any taxes and regulatory fees.
- Mitel supplies the carrier services and the customer interconnect.
- The Partner is responsible for system configuration and user provisioning.
- The Partner is responsible for providing the customer with Level 1 and Level 2 technical support.
- Mitel is responsible for deploying the associated applications and tenants and providing Level 3 and Level 4 support to the Partner.

MiCloud Flex Mitel/Partner Responsibility Matrix

The following chart shows the division of responsibilities between Mitel and the Partner for the two the delivery models.



	MiCloud Flex Wholesale (Global)	MiCloud Flex Partner Delivered (US only)
Sales	**Mitel Partner** leads sales process with Mitel support	
Offer	**Mitel** provides subscription software, data center hosting, and network to interconnect point. **Mitel Partner** provides carrier services, customer interconnect & other services.	**Mitel** provides the full cloud solution stack for partners to sell. **Mitel Partner** may separately offer and bill for additional value add services.
Contract	**Mitel** contracts with Partner **Mitel Partner** contracts with Customers	**Mitel** contracts with Customers
Customer Order Fulfillment	**Mitel** fulfills infrastructure, assigns licensing and hands off to Partner **Mitel Partner** completes customer activation and onboarding	**Mitel** fulfills infrastructure, carrier services, and assigns licensing, then hands off to Partner **Mitel Partner** completes customer activation and onboarding
Billing	**Mitel** bills and collects from partner at wholesale (Partner Buy) rates **Mitel Partner** bills and collects from customer, including any taxes and regulatory fees	**Mitel** bills and collects from customer, including any taxes and regulatory fees
Support and Customer Service	**Mitel** provides Partner with Level 3 & 4 support **Mitel Partner** provides Level 1 & 2 support to customers including managing ongoing additions, extensions of their services, maintenance and software upgrades	
Partner Compensation	**Mitel Partner** receives a wholesale discount off list price, per standard Mitel partner discount structures	**Mitel Partner** receives a commission for duration of customer subscription

Products Covered by this Document

The MiCloud Flex solution is comprised of several Mitel applications, Mitel products and a number of third-party business applications. The following products and applications are covered in this document.

- Mitel MiVoice 6900 Series of MiNET IP phones
- MiContact Center Business
- MiContact Center Outbound
- MiContact Center Speech
- MiVoice Border Gateway
- MiVoice Business
- MiVoice Business Survivable Gateway
- MiVoice Business Console
- MiCollab
- Open Integration Gateway
- Mitel Workforce Optimization Suite which includes Mitel Interaction Recording (ASC),

MiCloud Flex - Product Security Controls and Operational Policies

The following information is intended to assist the MiCloud Flex Partner and the MiCloud Flex customer with their regulatory security compliance initiatives, the following topics are covered:

- An overview of the operational procedures that the Mitel Flex Partner and Mitel Flex customer need to establish for their security compliance initiatives.
- The security controls available on each of the underlying MiCloud Flex products and applications.
- Recommendations on how the Administrator should set and configure the controls

Access Management

This section discusses the requirement for an Access Control Policy, the individual product access controls and how the controls should be configured to ensure that the access controls are securing the solution.

Access Control Policy - Recommendations

Advancements in how Unified Communications applications are delivered necessitates that the confidentiality and integrity of customer data must be protected so that only authorized users have access to specified data. Access control protects user data by reducing the risk of intentional and unintentional misuse, theft, alteration and destruction.

The partner should take the following recommendations into consideration when they are establishing their Access Control Policy.

To assist with meeting security compliance requirements the Partner should establish an Access Control Policy. The following recommendations and guidelines are provided to assist the Partner with establishing their own Access Control Policy.

The purpose of an Access Control Policy is to communicate Partner Management access control requirements and administrative activities regarding access to customer data.

The policy should apply to all users who have access to the Mitel customer's systems. Users include employees, contractors, consultants, temporary, and other workers employed or contracted by the Mitel Partner, including all personnel affiliated with third parties.

The Mitel partner should have an established centralized process for granting, changing, and revoking access to systems. Partner Management must approve access requests to customer data for all users that require access. Access requests for new access and changed access should require approval before access is granted.

All access authorizations should be documented, maintained and periodically reviewed to determine if appropriate. Access should be based on the employee's role and job responsibilities.

The Access Control Policy should be based on the fundamental principle of *"need to know"* when determining access privileges. A user’s access to data must be based on their role and limited to the minimum necessary required to complete their job responsibilities. Access authorizations should be maintained with the Mitel Partner Security Administrator or System Administrator.

A periodic review of access authorization lists should be conducted to determine the current authorizations are still appropriate by confirming with Partner Management. Inactive accounts must be monitored and removed when access is no longer necessary. Access control must be independently audited by those other than the user that granted access.

All changes to any access profile must be reviewed periodically. Emergency and temporary access authorizations must be documented, maintained, and then terminated immediately after the predetermined period has ended.

Partner Management is responsible for promptly reporting user changes to the appropriate department. User status changes include, but are not limited to, transfers, terminations, role change or system permission change. With these changes, the Partner Management Security Administrator and/or Human Resources must be notified immediately to begin the process of terminations (revocations) and changes.

Product Access Control

MiVoice Business and MiVoice Business Survivable Gateway

Administration Encryption

The MiVoice Business (MiVB) Management tools should only be accessed over a secured communication channel, to achieve this:

- The connection between the Administrator's computer and the MiVoice Business management tools should be encrypted using HTTPS TLS 1.2. For more information see the section of this document on TLS Encryption.
- The Administrator should install a certificate obtained from a Certificate Authority (CA) that the customer already owns (that is, an enterprise CA). The web browser will then trust the MiVoice Business access. Note that certificates do expire and so the customer must be aware of the expiry date and renew it when needed.

Identity and Authentication

The Administrator should use the System Security Management Form to configure the following Administrative access controls.

- Set/reset the password

Users logging into the System Administration Tool for the first time after installation are required to change the default password.

- Establish the password strength rules

The password strength rules should at a minimum have: 15 to 20 characters using at least two characters from each of the four character sets, that is: upper-case letters (A-Z), lower-case letters (a-z), numbers (0-9), and special characters (` ~ ! @ # $ % ^ & * ( ) - _ = +).

- Set the user session inactivity timer

The Administrator should determine a value that provides a good balance between security and usability.

- Set the password expiry interval

The Administrator should set the password expiry interval to the customer's IT department's existing password expiration polices.

- Enable/disable the Login Banner

It is recommended that a login banner is used. Actual text will come from the company's security policy.

- Set the Phone Administrator's Password

The Administrator should ensure that the Phone Administrator's Password is set so that access to advanced settings on the 69xx phones is secured by a passcode. The Administrator should ensure that the full ten characters be utilized, and simple pass codes such as 1111 or 1234 should not be used.

MiVoice Business to MiVoice Business Authentication

The Device Certificate is the certificate that is used to authenticate the identity of MiVoice Business systems interacting with each other, by default, the MiVB uses the Mitel legacy certificate.

- The Administrator should ensure that authentication between multiple MiVoice Business instances and MiVoice Business Gateways is properly configured.
- It is recommended that the Administrator replace the default Mitel legacy certificate with a self-signed certificate, a certificate signed by an enterprise or public Certificate Authority (CA) obtained through a Certificate Signing Request (CSR). Alternatively, you can also use the Web Server certificate from the Server Manager as a device certificate.

The Device Certificate form is accessed with the System Administration Tool.

Access and Authorization

- The Administrator should establish role-based access controls for controlling access to the MiVoice Business management interfaces.

This is accomplished via the User Authorization Profiles Form, the Administrator should use this form to create, modify, and delete user profiles which are required to access the following MiVoice Business management interfaces:

  - System Administration Tool
  - Group Administration Tool
  - Desktop Tool
  - Application (allows access to the MiXML management forms)

- The Administrator should use the Admin Policies Form to add, modify, and delete policies that are used to establish permissions for various user profiles. These permission policies dictate which System Administration Tool forms a user is allowed to access or modify.
- The Administrator should create a user authorization policy and establish MiVoice Business user authorization profiles that comply with the company policy and business requirements.

- Should temporary profiles be created to support maintenance and/or troubleshooting activities, the profiles should be deleted once the activities have completed.
- When a user leaves the employ of the company, the Administrator should delete all profiles associated with that user.

Application - Login Security

Mitel XML (MiXML) applications are used to access the MiVoice Business database, for example synchronizing programming data with MiContact Center Business.

- The Administrator should ensure that MiXML applications can securely access the MiVB database, to achieve this the Administrator to establish a User Authorization Profile as described below.

MiXML requires a user be set up in the User Authorization Profiles form and also requires a certificate to access to MiVoice Business systems. Accessing the system using MiXML generates events that are recorded in the Audit log system.
For additional information on securing MiXML accesses, refer to the System Administration Tool Help Files; in particular see the MiXML Applications form and the System Security Management form. Applications require a certificate as well as the credentials for a User Authorization Profile with Application access defined.

MiVoice Business Console

The MiVoice Business (MiVB) Console may only be accessed by users that have been authorised to access the Windows PC running the MiVoice Business Console.

- The Administrator should ensure that only authorized users have access to the MiVoice Business Console,
- The Administrators should ensure that authorized users require the use of username/password login combinations that are based on strong password mechanisms.

Mitel recommends using Microsoft Windows Authentication for added security measures leveraging the AD security rules; for example, account enable/disable, password rules, and login attempts.

- The Administrator should leverage Windows security capabilities to establish account lock out thresholds. For example: setting the login thresholds can be found at:

  https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold

- The Administrator should further limit access to the MiVoice Business Console over the network by using standard network security techniques such as VLANs, access control lists (ACLs), and firewalls.

IP Sets 6900

Authentication with Call Control

Mitel IP phones for use with MiCloud Flex use the MiNET protocol.

MiNET – an encrypted proprietary stimulus-based protocol. For a Mitel MiNET set to register with the MiVoice Business call control, the set type, PIN number and MAC address must be accepted by the MiVoice Business call control.

- This required information is entered by the administrator (it may be bulk entered too). After registration, the MiVoice Business call control has knowledge of the relationship between MAC Address, IP address, extension number and PIN Registration Number. This relationship of MAC/IP/Ext/PIN must be valid in order for the MiVoice Business call control to allow communications to proceed.

Network Access and Authentication (802.1X)

Mitel IP phones support the IEEE 802.1X authentication protocol. Depending on the model of phone, there will be support for EAP-MD5, PEAP and proxy logoff.

- It is recommended that the L2 switches used throughout the LAN support the IEEE 802.1X protocol and that this capability be enabled by the Administrator.

A device that connects to a L2 switch port that has IEEE 802.1X enabled needs to be authenticated as valid before full network connections will be allowed. Users authenticate with the L2 switch through the phone interface by entering a username and password. The username / password authentication combination used with 802.1X is entered into the IP set interface through the telephone keypad where it is stored in flash memory.

Dual Port Phones

A number of Mitel's IP phones are dual port, meaning that there are two Ethernet ports on the phone. One Ethernet port is used to connect to the LAN. The other Ethernet port can be used to connect a PC to the network via the phone's integral L2 switch; this capability is useful in environments where the phone and the PC need to share a single Ethernet connection.

The 69xx series of phones support IEEE 802.1X proxy logoff. This logoff feature will become enabled when 802.1X is enabled on the phone. With proxy logoff, when a PC is physically disconnected from the phone's PC Ethernet port, the phone's PC Ethernet port will be reset. Once the PC Ethernet port has been reset, if a PC is reconnected to the phone's PC port, the PC will have to re-authenticate before being allowed access to the network.
Alternatively, some networks may utilize MAC authentication to ensure only Mitel devices can access the voice VLAN.

If 802.1X is not available, MAC authentication may be an alternative solution that can be implemented.

MiVoice Business supports a Class of Service (CoS) option that can be used by the Administrator to disable the phone's PC Ethernet port on dual port phones, which in turn will bar access at the PC Ethernet port. The default condition is for all PC Ethernet ports to be enabled.

- If the phone's PC Ethernet ports are not being used for PC connectivity, then Administrator should disable PC Ethernet ports.

The phone's PC Ethernet port can be disabled by the Administrator by using the Class of Service (CoS) settings that are available through the MiVB management tool.

MiVoice Border Gateway

Administrator Access

Administrator access is secured by a username and password with strength validation, the password is stored as a secure hash. All access is encrypted using SSH version 2 or HTTPS (TLS), the use of TLS 1.2 can be enforced.

SSH is disabled by default and should remain so unless needed for troubleshooting. SSH access can be limited to a list of authorized networks or hosts. Repeated failed login attempts to SSH result in a temporary ban of further login attempts from this IP address.

Access to the administrator web interface by default is limited to the directly attached local network. Access may be extended to other specific networks and hosts.

There is no end-user (data subject) access to MiVoice Border Gateway. All personal data processing is limited to the local Administrator account.

Access to data files on disk requires Administrator (‘root’) access. Sensitive data within disk files is encrypted. Access to the system shell is disabled by default, Mitel recommends its use only for troubleshooting.

- The Administrator should enforce the use of TLS 1.2 to protect the transmission of the login credentials.
- The Administrator should ensure that a strong password is used.
- Except for troubleshooting purposes, the Administrator should ensure that SSH remains disabled.
- The Administrator should change the Administrator Access password as per the Access Control Policy

API Access

Applications may be individually authorized to connect through the Provisioning API or Secure Recording Connector. Provisioning API access is controlled by an OAuth enrollment mechanism for each application instance. Permissions may be assigned to each access token individually. Application access through the Provisioning API can be limited to specific subsets of the data by category, such as SIP trunks or MiNET devices. Access may be read-only or read-write per application.
The Remote Proxy Service may be used to authenticate a user with a target application such as MiVoice Business Contact Center or AWV.

Call recorders must enroll by submitting a Certificate Signing Request to a local Certificate Authority embedded in the product for this purpose. A unique certificate is issued to each call recorder and used for TLS authentication.

- The Administrator should limit access through the Provisioning API to only those applications that are required, and the Administrator should only provide Applications with the required permissions.
- Whenever possible, the Administrator should limit application access to read only.

MiContact Centre Business

Administration Encryption

The MiContact Center Business (MiCC-B) Management tools should only be accessed over a secured communication channel. To achieve this:

- The connection between the Administrator's computer and the MiContact Center Business management tools should be encrypted using HTTPS TLS 1.2. For more information see the section of this document on TLS Encryption.
- The Administrator must install a valid certificate assigned to port 443. If there are valid certificates in the server's local certificate store one of these may be assigned, otherwise a certificate signed by an enterprise of public Certificate Authority (CA) can be obtained through a Certificate Signing Request (CSR).

Identity and Authentication

The Windows Administrator account is used for managing the MiContact Center Business system. Set up a domain account with Server Administrator privileges on the server. Most of the MiCC services (including SQL) will run under this account. The account password should be set to never expire; if the password is changed, the installer will need to rerun to reconfigure all services.

Access and Authorization

Once the MiCC software is installed, log on to the administrator account using the default username "_admin" and password "_password". To change the password:

- In YourSite Explorer=>**Devices**=>**Employee** select Administrator.
- Under **General,** in the **Password** field, type in the new password (choose a strong password and save it).
- The Administrator should establish role-based access controls for controlling access to the MiContact Center Business management interfaces.
- The administrative account used to install MiCC Business must have the “dbcreator” role on the SQL server.

MiContact Centre Outbound

Administration Encryption

The MiContact Center Outbound Management tools should only be accessed over a secured communication channel. To achieve this:

- The connection between the Administrator's computer and the MiCC Outbound management tools should be encrypted using HTTPS TLS 1.2.
- Agent and Supervisor connections to the system should also be encrypted using HTTPS TLS 1.2.

Identity and Authentication

There are four administrative accounts which must be created during the installation of the MiCC Outbound platform. All these accounts must have full administrative rights on all the servers in the system. It is recommended that these accounts be Microsoft AD accounts, but if set up locally all must have the same password on each of the platform servers. In addition, corresponding accounts will be created on the SQL Database Server(s), and must have different rights to the databases. Strong passwords should be used on these accounts.

MiContact Center Speech

The MiContact Center Business integrates with Nuance Speech Suite for speech recognition and text-to-speech (i.e. voice prompts). Nuance Speech Suite is supported on both Windows and Linux, but is typically hosted on Windows for use with MiCC-B.

Administration Encryption

The MiContact Center Speech management tools should only be accessed over a secured communication channel. To achieve this:

- The connection between the Administrator's computer and the Nuance management tools should be encrypted using HTTPS TLS 1.2.
- Agent and Supervisor connections to the system should also be encrypted using HTTPS TLS 1.2.

Identity and Authentication

Both installation and system administration require Windows administrator privilege. Agents have user privilege. Accounts can be configured locally on each server, but it is recommended that AD be used, with strong passwords for all users.

MiCollab (Also includes NuPoint)

Administration Encryption

The MiCollab Management tools should only be accessed over a secured communication channel; to achieve this:

- The connection between the Administrator's computer and the MiCollab tools should be encrypted using HTTPS TLS 1.2.
- The Administrator should install a certificate obtained from a Certificate Authority (CA) that the customer already owns (that is, an enterprise CA). The web browser will then trust the MiCollab access. Note that certificates do expire and so the customer must be aware of the expiry date and renew it when needed.

Identity and Authentication

The MiCollab user database can be synchronized with a corporate database using LDAP, and can also be integrated with Active Directory Authentication. Strong passwords should be used on all accounts.

Flow-through Provisioning for MiVoice Business

Flow Through Provisioning uses System Data Synchronization (SDS) to synchronize updates

made between the MiCollab and MiVoice Business system databases.

To support reach through navigation from MiCollab server manager to the MiVoice Business system administration tool you must download the common Mitel Root Certificate from one of the MiVoice Business servers and import it into your browser as a 'Trusted Root Certification Authority'.

Open Integration Gateway (OIG)

Administration Access

Access to the Open Integration Gateway (OIG) is restricted to Administrator role access level, which requires Administrator login credentials (username and password). The password is subject to strength validation. There is no end-user access to OIG.

All personal data processing, system data processing, and all access to databases, files, and operating systems are protected with Administrative access and authorization controls. All access is encrypted using SSH version 2 or HTTPS (TLS). Use of TLS 1.2 can be enforced. Passwords are encrypted with AES and the password is stored as a secure hash.

- The Administrator should enforce the use of TLS 1.2 for Administrative access.

Access to the Administrator web interface by default is limited to the directly attached local network. Access may be extended to other specific networks and hosts.

SSH is disabled by default and should remain so unless needed for troubleshooting. SSH access can be limited to a list of authorized networks or hosts.

- The Administrator should ensure that access to the Administrator web interface is only extended to trusted networks and authorized hosts.
- The Administrator should ensure that SSH remains disabled.
- If SSH should be enabled for troubleshooting purposes

API Access

Third-party applications are individually authorized to connect to OIG with a 2-step process of identification and authorization check.

1. Each application needs to be registered as a standard or advanced application with Mitel Certificate Server (MCS) which is maintained by Mitel. Upon registration, it needs to be approved by Mitel.
2. Once approved, the application will be available under the list of "Available Applications" on the OIG Server. The Administrator needs to create a local password to the application before adding it as one of the Allowed Applications.

Only then can the application access the OIG server services by providing the local password. Hereafter, applications can access API services as well. A unique certificate is issued to OIG , and used for TLS authentication.

The Open Integration Gateway (OIG) Administrator web user interface (UI) provides a central location for configuring the Mitel OIG server and provides access to operational and configuration information.

- The Administrator must define a strong local password for each application that will connect to the OIG. This local password must be associated with the application when it is deployed (the application developer provides a means to do this). Each application must also supply the appropriate local password to the OIG when opening a communication session.
- The Administrator should verify that the OIG is correctly configured so that only authorized applications are enabled, that the application's passwords are set with an appropriate strength and that only authorized Google users are allowed access. The Administrator can check the OIG configuration from the main page of the OIG Administrator UI.

Remote OIG Applications

A MiVoice Border Gateway web proxy is required for any Mitel OIG application instances (users) that are deployed outside the enterprise.

- The Administrator should ensure that if required, a MiVoice Border Gateway web proxy is deployed and configured.

MSL Server Firewall Configuration

To allow the Mitel OIG to communicate with MiVoice Business controllers, the Mitel MSL server firewall must be configured to allow connections from each MiVoice Business IP address.

If Internet access is required:

1. The Mitel OIG must have access to the Internet.
2. The Mitel OIG server must be configured with a third-party CA certificate when using MiVoice Integrations.
3. The Mitel OIG must obtain licensing from the Mitel AMC server.
4. The Mitel OIG must communicate with the Mitel Certificate Server to obtain an Access Control List (ACL).
5. The ACL indicates what applications are authorized to use the Mitel OIG.

- The Administrator should ensure that the above requirements are met.

Mitel Workforce Optimization Mitel Interaction Recording (WFO MIR)

Mitel Workforce Optimization (WFO) is a suite of products to improve and integrate call handling and business processes. It is primarily targeted to Contact Centre deployments, but may be used outside of that arena. The Mitel Interaction Recording is a suite of products that provide Call Recording and Screen Recording capabilities. Speech analysis of the voice recording can optionally be included, and provides an ability to keyword spot or to provide full transcription of the conversations. The system is installed on Windows servers.

Administration Access

Secured, encrypted administration access using HTTPS to the Windows server is required to install the software on the server. The Windows server will have a self-signed certificate; a certificate from a valid CA should be installed on all the servers in the installation.

Identity and Authentication

The system must be installed by an Administrator of the system provider with root access on the Windows server. The system is installed initially as a single-tenant system, with one pre-defined tenant (“the customer”). Separate administration roles are created with default passwords for each of these accounts. On first login the password must be changed. Strong passwords are recommended.

Mitel Standard Linux

Mitel Standard Linux (MSL) is an operating system and server solution for single-site and branch-based enterprises. MSL provides a base for a suite of managed services and applications such as MiVoice Business, MiVoice Border Gateway and MiCollab.
MSL is a 64 bit Linux distribution for Intel based computers that is available for download from the Mitel Software Download Center. MSL is based upon the CentOS distribution.

Administration Access

Secured, encrypted administration access using HTTPS to the MSL server is limited to only configured hosts/networks during implementation. The Administrator password (or System password) is used to access the Server Manager web administration page and the server console as the "admin" user and the Linux shell as the "root" user.

- The Administrator should use a secure, non-trivial password that is at least eight characters in length.

Remote Management

Remote management allows hosts on the specifiedIPv4 remote network(s) to access the Server Manager of the MSL server. Remote management is disabled by default and must be enabled by the Administrator. This can be limited to an individual host level or a range of IP addresses using network IP address and subnet mask to enable remote management access.

- The Administrator should only enable remote management when it is required, and the Administrator should disable remote management as soon as remote management is not required.

Secure Shell Settings

Secure Shell (SSH) is disabled by default, but if desired can be enabled and be limited to specific networks and/ hosts who can access via SSHv2. Once enabled. SSH provides a secure, encrypted way to log in to the MSL server from a remote location.

- The Administrator should enable Secure Shell when it is required, and the Administrator should disable Secure Shell as soon as remote access is not required.

Password Rules

When first installing MSL there is no default password, meaning - there is no password established.

- The Administrator must establish a secure MSL password, to do so the Administrator should customize their own password complexity rules. Password complexity rules including non-alphanumeric requirements, minimum length, uppercase, lowercase and consecutive characters requirements as well as forbidden words to use as a password.

Preventative Controls

This section discusses the preventative controls provided by the individual products and applications and how the controls should be configured and used to ensure the secure operation of the MiCloud Flex solution.

Monitoring and Logging Policy - Recommendations

This section discusses the requirement for a Monitoring and Logging Policy and provides recommendations that the Partner should consider when creating their Monitoring and Logging Policy.

The Logging and Monitoring Policy should apply to all system logs, application logs and device logs on the MiCloud Flex solution. This policy should be followed by all Administrators who manage the solution.

The Administrator should identify and enable log events for every system and device to facilitate and support investigations and forensic analysis. These events should be retained and be readily available for immediate analysis and investigations. The Administrator should ensure that all systems that handle sensitive or confidential information (PCI cardholder data and HIPAA data including ePHI), and systems record events and retain audit-logging information sufficient to answer the following questions:

- What activity was performed?
  - Type of event
  - Severity of event
  - Security relevant event flag
  - Description
- Who performed the activity? (human or machine user)
  - Source address
  - User identity
- Where was the activity performed from?
  - Application identifier
  - Application address
  - Service name and protocol
  - Geolocation

  - Window/form/page/URL
  - Code location
- When was the activity performed?
  - Log date and time (international format)
  - Event date and time

The following is a minimum set of log events that should be enabled:

- All user authentication and authorization successes and failures
- Administrative account management events
- System administration activity events from applications, services, databases and operating systems
- Use of higher-risk functionality, such as, but not limited to the following:
  - Network connections
  - Add, change or remove user
  - Change user privilege
  - Assign user’s token
  - Add, change or delete token
  - Use of system Administrator privilege
  - Access to payment cardholder data
  - Use of data encrypting keys
  - Key changes
  - Creation and deletion of system-level objects
  - Data import and export including screen-based reports
  - Legal and other opt-ins

MiVoice Business and MiVoice Business Survivable Gateway

Logs in MiVoice Business are available for browsing via the System Administrator tool. There are separate log pages for Maintenance logs, Software logs, Audit logs, CESID logs and Data Distribution Update logs. In addition to being able to view the logs, the logs pages also support exporting the logs as CSV files. The scheduling capability of MiVB can also be used to export log files on a regularly scheduled basis.

Forwarding Logs to a Syslog Server

The MSPLogClient is a Linux-based utility that connects to MiVB and forwards logs to a syslog server. This utility is available from the Software Download Center on MiAccess. For MPLS-connected customers, the MSPLogClient can be installed on a Linux machine within the customer's own local area network.

Audit Trail Logs

Audit Trail Logs provide a historical record of changes made to the system from the System Administration Tool and various other user interfaces and applications.

- The Administrator should view the MiVoice Business Audit Trail logs as required by the Logging and Monitoring Policy.
- The Administrator should ensure that only authorized personnel are granted access to the Audit Trail Logs.
- The Administrator should ensure that the Audit Trail Logs are retained as per the Logging and Monitoring Policy.

SMDR Logs

Station Message Detail Recording (SMDR) is the Mitel name for Call Detail Recording (CDR) logs on the MiVoice Business platform.

- The administrator should use the SMDR options form to configure the details that will be recorded for internal calls, external calls and details related to location-based accounting.

Call accounting systems and other applications connect to the SMDR raw ASCII output on TCP port 1752.

- To restrict access to SMDR raw information the Administrator should create an Access Control List (ACL) on the Ethernet switch port that the MiVoice Business is connected to and allow only the permitted applications to connect on 1752.
- The Administrator should carefully review the SMDR options form and set the reporting controls as required. The application that is being used to collect SMDR information will have the recommended values.

Property Management System Logs - Occupancy Logs

- To restrict access to Property Management System Logs raw information, the Administrator should create an Access Control List (ACL) on the Ethernet switch port that the MiVoice Business is connected to and allow only the permitted applications to connect on 1753.

MiVoice Business Console

The MiVoice Business Console by default generate Error, Warning, and Info level logs for all log categories.

- The Administrator should use the Capture Logs form to ensure that log captures are configured with an appropriate logging interval, as required by the Logging and Monitoring Policy.

The Administrator can use the MSP Log Viewer to view console logs. Logs are stored in the following location:

C:\ProgramData\Mitel\MiVoice Business Console\Logview

- The Administrator should view the MiVB Console logs as required by the Logging and Monitoring Policy.

- The Administrator should ensure that the MiVB Console logs are retained as per the Logging and Monitoring Policy.

IP Sets 6900 MiNET

The 6900 MiNET sets create the following logs:

- Logs that are stored on the MiVB:
  - Personal contacts, which can be browsed by the user on the phone's User Interface.
  - The phone's IP call history, which can be browsed by the user on the phone's User Interface.
  - System Logs, which can be browsed by the user on the phone's User Interface.
- Logs that are stored on the phone:
  - Mobile contacts which can be browsed by the user on the phone's User Interface.
  - Mobile call history which can be browsed by the user on the phone's User Interface.
  - Name of paired Blue Tooth devices which can be browsed by the user on the phone's User Interface.
  - System diagnostic logs which can be browsed by the user on the phone's User Interface.

MiVoice Border Gateway

Partners are responsible for configuring and maintaining the applications that have been deployed by Mitel into the iLand environment. Part of this activity involves acting as the first level of support for their customers. In this role, Partners need access to application-level logs.

Audit Logs

Audit logs are supported to maintain an audit trail of all changes made by Administrator accounts and connected applications (through the Provisioning API), as well as all changes originating on other nodes of a MiVoice Border Gateway cluster are logged to the Audit Log.

The audit logs may be sent through syslog to a central site for aggregation and analysis. The audit log contains the IP address, administrator name or application token identifier, information on which objects were added/changed/removed, and the details of that operation. As such, the Audit Logs may contain personal end user information. These logs are captured under /var/log/mbgaudit.log. Audit logs can be viewed and downloaded under the View Log Files panel in MSL. The Audit Log can be accessed only by the Administrator unless it has been sent to another server by syslog.

- The Administrator should view the MiVoice Border Gateway logs as required by the Logging and Monitoring Policy.
- The Administrator should ensure that only authorized personnel are granted access to the Audit Logs, on either the MiVoice Border Gateway or on a server that has received the logs via syslog.
- The Administrator should ensure that the Audit logs are retained as per the Logging and Monitoring Policy.

Other Logs

Various MBG log files capture information regarding the behavior and performance of the software application. These are useful in troubleshooting, and optimizing application capabilities in different scenarios.
Some of the log files associated with MBG are tug.log, tugsec.log, tug-eventd.log, webrtc.log, mbgrest.log, tugvq.log and mbgui.log. Most of these logs are not intended for end users but can be retrieved for Product Support by using the Fetch Logs button or by generating an SOS report.

The MBG logs can be viewed and downloaded under the View Log Files panel in MSL.

- The Administrator should ensure that the MBG logs are retained as per the Logging and Monitoring Policy.
- The Administrator should view the MiVoice Border Gateway logs as required by the Logging and Monitoring Policy.

MiContact Centre Business

MiContact Centre Business is a Windows-based application running on virtualized Windows servers. Management of these applications is via a remote desktop connection connected via port forwarding through the MPA probe. Once connected via remote desktop, all management capabilities, including logging, are accessible in an identical manner to premise installations.

The following logs are collected, and stored by nightly scheduled maintenance.

- CDR records
- SQL transaction logs
- Other maintenance logs

Storage location, length of time stored, and reporting schedule are all configurable, and should be configured for compliance with the Logging and Monitoring policy.

MiContact Centre Outbound

The MiCC Outbound Platform generates a large number of logs for each of the Synthesys Application modules. Application logs are generally stored on the server for 7 days and archived for 30 days before being purged; however, this can be adjusted.

- The Administrator should ensure that the MiContact Center Outbound logs are retained as per the Logging and Monitoring Policy.
- The Administrator should view the MiContact Center Outbound logs as required by the Logging and Monitoring Policy.

MiContact Centre Speech

MiContact Center Speech records call logs, management activity logs, and diagnostic logs. All are available to Administrator level users.

- The Administrator should ensure that the MiContact Center Speech logs are retained as per the Logging and Monitoring Policy.
- The Administrator should view the MiContact Center Speech logs as required by the Logging and Monitoring Policy.

MiCollab (Also includes NuPoint)

MiCollab logs are available within the native MiCollab management interface via the View Log Files page. This page allows logs to be displayed including the ability to filter logs and highlight text within the logs. Additionally, the log files can be downloaded, including the ability to encrypt the download. In addition to log files, this page also allows diagnostic information to be downloaded.

MiCollab also has an Event viewer page that displays alarm events and an SDS Distribution Errors page for managing problems synchronizing data between MiCollab and MiVB.

OIG

The Open Integration Gateway (OIG) resides on the Mitel Standard Linux (MSL) operating system. The OIG uses MSL to generate software logs. The Administrator can either use the MSL Server command line and view the log files or use the MSL Server Manager to view the log files in a browser.

- The Administrator should view the OIG logs as required by the Logging and Monitoring Policy.
- The Administrator should ensure that only authorized personnel are granted access to the OIG logs.
- The Administrator should ensure that the OIG logs are retained as per the Logging and Monitoring Policy.

Workforce Optimization Mitel Interaction Recording (WFO MIR)

Work Force Optimization and Mitel Interactive Recorder are Windows-based applications running on virtualized Windows servers. Management of these applications is via a remote desktop connection connected via port forwarding through the MPA probe. Once connected via remote desktop, all management capabilities, including logging, are identical to the typical premise installations.

- The Administrator should ensure that the WFO MIR logs are retained as per the Logging and Monitoring Policy.
- The Administrator should view the WFO MIR logs as required by the Logging and Monitoring Policy.

Mitel Standard Linux

Administrative Access - Audit Trails

Administrative access audit trails are supported for installed applications to maintain records of data processing activities. Administrative access to the MSL server is logged, and all changes made via the Administrator accounts are logged to the Audit Log. The Audit Log can be accessed only by the Administrator unless it has been sent to another server by syslog to a central site for aggregation and analysis.

- The Administrator should monitor the MSL administrative access Audit Trail Logs as required by the Logging and Monitoring Policy.

- The Administrator should ensure that only authorized personnel are granted access to the Audit Trail Logs.
- The Administrator should ensure that the Audit Trail Logs are retained as per the Logging and Monitoring Policy.

Logging

MSL includes a syslog server for logging system event messages. When a system event occurs, such as a failed authentication attempt or login failure, the affected service generates a message which is recorded in a log file. The audit log contains the IP address, Administrator name or application token identifier, information on which objects were added/changed/removed, and the details of that operation.

- The Administrator should monitor the MSL Audit Trail Logs as required by the Logging and Monitoring Policy.
- The Administrator should ensure that the MSL Audit Trail logs are retained as per the Logging and Monitoring Policy.
- The Administrator should ensure that only authorized personnel are granted access to the Audit Trail Logs

Encryption for Data at Rest Policy - Recommendations

This section discusses the requirement for a Policy to address encryption of data at rest and provides recommendations that the Partner should consider when creating their Encryption for Data at Rest Policy.

Ideally, the Encryption for Data at Rest Policy should apply to all MiCloud Flex storage systems that contain customer data. At a minimum personally identifiable information, sensitive information, personal health information and personal financial information data should be encrypted while at rest.

The Administrator should identify all MiCloud Flex storage devices that require Encryption for Data at Rest and enable Encryption for Data at Rest on these storage devices.

Encryption for Data at Rest

Most of the individual systems that comprise the MiCloud Flex system do not natively encrypt the data stored on their drives. For customers who need additional security and privacy protection for their data, the Flex Advanced Security option for data at rest is available. With this option all data is encrypted at rest in the cloud storage array.

For further information about the Flex Advanced Security option, contact your Mitel Account Team or your Mitel Partner.

Mitel Standard Linux

MSL data at rest can be encrypted with the Flex Advanced Security option.

For availability reasons MiCloud Flex is designed so that the MSL server’s virtual hard drive is deployed on a Storage Area Network (SAN). As a result, MSL data at rest can be secured by segregating the MSL hard drive on a SAN and enabling encryption at the SAN.

- The Administrator should ensure that the MSL server's virtual hard drive is deployed on a Storage Area Network (SAN) that is encrypted at the SAN and/or virtual machine level.

Encryption of Sensitive Data Fields

The following applications provide native encryption of sensitive data fields.

MiVoice Business and MiVoice Business Survivable Gateway

Passwords are encrypted in the MiVoice Business data base.

Server Manager

Server Manager is a Web based administrative tool for Mitel Standard Linux (MSL), Server Manager is used with MiVoice Business and a subset of Server Manager is used with the MiVoice Business Gateway.

Server Manager obscures sensitive data that is stored on disk and in backup files such as the credentials that are used for accessing services.

MiVoice Business Console

The MiVoice Business Console encrypts passwords that are stored on the Console's PC.

- The Administrator should employ BitLocker (or a similar application) to ensure encryption of the local Windows desktop hard drive.

Postgres data is stored on a different PC/server than the MiVoice Business Console's PC. The data is not encrypted in the Postgres Server. Postgres stores the SQL data itself in binary files, not in plain text.

- The Administrator should review the article *How to Secure PostgreSQL: Security Hardening Best Practices & Tips*, and implement the recommended security measures.

The article, *How to Secure PostgreSQL: Security Hardening Best Practices & Tips* provides information on securing the PostgreSQL server, the article may be found here:

https://www.enterprisedb.com/blog/how-to-secure-postgresql-security-hardening-best-practices-checklist-tips-encryption-authentication-vulnerabilities

MiVoice Border Gateway

Access to data files on disk requires Administrator ('root') access and sensitive data stored on disk is encrypted.

Workforce Optimization Mitel Interaction Recording (WFO MIR)

WFO MIR has the ability to encrypt all recordings.

The Administrator should enable encryption for all recordings.

A validation process is available to check whether the encrypted data stream can be decrypted successfully. If the recording contains distorted audio signals a notification is issued. This works almost in real time; results are available shortly after the recording has started.

Mitel Standard Linux

Password information is hashed when it is stored on disk.

Data Backup Policy - Recommendations

This section discusses the requirement for a Policy to address data backup and provides recommendations that the Partner should consider when creating their Data Backup Policy.

The Data Backup Policy should apply to all MiCloud Flex storage systems that contain customer data and application data bases. The Data Backup Policy should define a schedule for full backups and incremental backups.

The Administrator should identify all MiCloud Flex storage devices that require coverage under the Data Backup Policy and ensure that backup schedules are strictly adhered to.

Data Backup

MiVoice Business and MiVoice Business Survivable Gateway

The Administrator must ensure that the MiVB is configured to perform regularly scheduled data base backups. To do so, the Administrator will need to login to the MiVoice Business System Administration Tool and use the External FTP Server Form to configure data base backups/restores, scheduled software downloads, and file transfers.

MiVoice Business Console

Console PC

User data and logs that contain user data are stored on the MiVB Console's PC.

- The Administrator should ensure that the MiVB Console's PC is backed up to a secure location as required by the Backup Policy.

PostgreSQL database

Call History records are stored on a customer configured and maintained PostgreSQL server.

- The Administrator should ensure that the PostgreSQL server is backed up to a secure location as required by the Backup Policy.

Additional Database Fields

Additional Database Fields (ADF) contains directory data and is stored on a customer configured and maintained ADF server.

- The Administrator should ensure that the ADF server is backed up to a secure location as required by the Backup Policy.

IP Sets 6900

The 6900 IP Sets store the following data on MiVB, and this data will be backed up when the MiVB data base backup is scheduled.

- Personal contacts
- IP call history
- System logs

MiContact Centre Business

MiContact Center Business allows specifying the location of folders for storing backup files, but only on local drives (not network drives). The database and telephone data can be backed up on command, and a .zip file is created containing an XML file with the entire configuration. This file can then be copied to a shared drive or an external location. The backup file is not encrypted, but if restored on any but the original system, all usernames and passwords will be blanked.

MiContact Centre Outbound

The SQL database should be backed up regularly. There is no provision to schedule this within the application, but it is possible to schedule it from Windows Task Scheduler.

Workforce Optimization Mitel Interaction Recording (WFO MIR)

During the installation of the provided PostgreSQL database of the MIR software, a

backup job is created for the PostgreSQL database which covers the last 5 days.

When using an external database, you will find information about backups in the manuals of the respective manufacturer.

MSL

MSL has two data backups that should be performed regularly, the VMWare backup and the Server Manager backup. Server Manager provides the UI for performing backups within MSL.

Detailed descriptions of the VMWare and Server Manager backups are as follows:

VMWare Backup

This refers to a backup of an existing instance of a VMWare-deployed application using the VMWare tools. This takes an image of the virtual hardware, software, storage, application databases, etc. and creates a new ova file that can be deployed in VMWare to create an exact copy of the previous deployment. This is ideal for disaster recovery cases where the desire is to be able to quickly re-create an existing deployment, but can also be used for the “golden database” use case where a pre-configured baseline image is created and used as the basis for new deployments.

Server Manager Backup

This is a backup, initiated through Server Manager, that captures the configuration of MSL as well as the applications installed on MSL. In the case of MiVB-ISS for example, this would include the MiVB database. In this case, a fresh install of MSL could be deployed (on a server or on VMWare as an ova) and then the Server Manager backup could be restored to re-create the previously backup up system, applications and all.

Antivirus/Malware Software

Windows Servers – Antivirus/Malware Software

The Flex Advanced Security option includes antivirus and anti-malware which can be set up to run on any of the Window servers that make up the Flex system.

The Flex Advanced Security option is available on all iLand data centers where Flex is deployed. For further information regarding the Flex Advanced Security option, contact Mitel Sales or the Mitel partner.

For management purposes, the Partner and the customer are provided with access to an Advanced Security Dashboard.

Some of the servers which may be processing and/or recording real-time streaming data recommend that antivirus software be disabled on the folders where this data is stored. This possibility can be discussed with the customer to arrive at a compromise between the risk of distorted audio and the risk of a breach through implanted code (which is not a high probability when streaming audio between phone devices).

Mitel Standard Linux – Antivirus/Malware Software

The following applications that process real time data are hosted on MSL:

- MiVoice Business
- MiVoice Border Gateway
- MiCollab (Including NuPoint)
- Open Integration Gateway (OIG)

Applications that process data in real-time require unfettered access to processor resources, memory systems, disk drive accesses and network communications. When Mitel applications are deployed on industry standard servers or virtual machines, as per the application’s engineering guidelines, the machine's resources will have been sized to ensure that the applications will have unrestricted and timely access to the resources that they require.

Since MSL is hosting real time application and these real-time data processing applications are executing on carefully sized computing platforms, the installation of antivirus software is not currently recommended, however as described below, Mitel has implemented measures to harden MSL.

MSL Hardening

Mitel has hardened the MSL operating system with the following techniques to minimize any vulnerabilities and reduce the potential attack surface of an MSL server.

- Unnecessary services and applications have been removed or disabled.
- Unnecessary IP Ports are closed.
- Wireless and Bluetooth networking services are not included.
- Email client and Web browser are not included.
- Remote control and access is disabled by default, with common unsecured services removed, e.g. Telnet.
- Directory services are disabled by default.
- Web Servers and services are only available to customer defined trusted networks and/or hosts. Access control is part of the implementation process and can only be updated by authorized Administrator.
- Software development tools and compilers are not provided.
- File and printer sharing services, NETBIOS, NFS, FTP, etc. are disabled or removed.
- SNMP is disabled by default. SNMPv3 and SNMPv2c are supported if enabled by an authorized Administrator.

Operating System user access and authentication have been restricted:

- Default accounts and non-interactive accounts are removed or disabled.
- There is no default password – it must be configured during installation.
- Remote access on external interfaces is disabled by default.
- Repeat failed access attempts are black-listed after 6 attempts within 10 minutes for 30 minutes, from Server Manager remote access (when enabled).
- Repeat failed access attempts are black-listed after 10 attempts from SSH remote access (when enabled.)
- SNMP is owned by root, not administrators.
- Login and Logout activity of users and root are logged.

Resource controls have been modified:

- MSL does not provide any world writable permissions.
- MSL does not provide any ‘no-owner’ files.
- Host based firewalls are enabled and configured.
- External interfaces do not report server type, nor release version.
- Only necessary IP ports are enabled by the OS so manual port intervention is not necessary.

Communications Security Policy - Recommendations

This section discusses the requirements for a Communications Security Policy and provides security recommendations that the Partner should consider when creating their Communications Security Policy.

The Administrator should identify all communications channels and ensure that they are properly secured with the highest-level encryption protocol available on the application.

The Administrator should ensure that all communications channels remain properly secured and that if any new channels are deployed, that they are also secured.

Communications Security

This following discusses the preventative controls provided by the individual products and applications and how the controls should be configured and used to ensure that the MiCloud Flex solution communications are properly secured.

MiVoice Business and MiVoice Business Survivable Gateway

Application Encryption

The System Security Management form is used to access the Application TLS Security Level Form.

These settings allow the Administrator to set the TLS security levels for the following applications: SIP communications, IP Sets, IP trunks, Trusted Applications, System Data Synchronization, MiTAI and Data Services.
Each application may be independently set to High, Low or Legacy, the default settings for all applications are High, which enables TLS 1.2.

- The Administrator should ensure that the TLS security levels be set to High, however in certain cases such as interfacing to an older system, it may be necessary to select Low or Legacy.

Media Streaming

MiVoice Business may be configured to encrypt all media streams (e.g. voice streams, video streams) with either Mitel SRTP or SRTP using AES 128 encryption.

- The Administrator should ensure that media streams are encrypted. To do so, the Administrator must use the MiVoice Business System Administration Tool to access the System Options Form.

IMAP Server

The Administrator should ensure that the transmission of usernames and passwords between NuPoint and the IMAP server is secured with TLS 1.2.

MiVoice Business WAN Security and Remote Access Security

Some MiVoice Business 3300 ICP appliances have a WAN interface port, the WAN interface is secured with an integral firewall that examines all packets attempting to access the internal network from the Internet.

Unless a packet is part of an existing connection or matches a specific TCP or UDP port programmed for forwarding, it is declared as unknown. All unknown packets are logged in System Diagnostics and then either dropped or rejected.

The integral firewall can also be programmed to allow Virtual Private Network (VPN) tunnels with PPTP and IPSec pass-through and also inbound connections with IP Port Forwarding.

- To secure the WAN interface port, the Administrator must use the MiVoice Business System Administration Tool to access the appropriate forms.
  - The Port Forward Table Form is used to configure the MiVoice Business's integral router.
  - The IP Routing Form is used to configure routing capabilities.
  - The Firewall Control Form is used to configure the integral Internet gateway.
  - The Remote Access (PPTP) Form is used to configure the internet gateway.

Note: The above-mentioned forms are applicable only to MiVoice Business 3300 ICP appliances that are equipped with a WAN interface.

MiVoice Business Console

Voice Streaming

By default, the MiVoice Business Console is configured to encrypt all IP voice call media streams with either Mitel SRTP using AES 128 encryption or SRTP using AES 128 encryption.

- The Administrator should ensure that all IP voice call media streams remain encrypted.

Voice Call Signaling

MiVoice Business Console by default is configured to encrypt all Call Signaling with Secure MiNET.

- The Administrator should ensure that all Call Signaling remains encrypted.

User Messaging

The MiVoice Business Console may be configured to register with the Mitel MiCollab for Instant Messaging and presence updates. This mechanism uses HTTP and SIP, both of which are unencrypted when connected directly to MiCollab. These mechanisms can be encrypted by connecting the MiVoice Business Console to a MiVoice Border Gateway.

- The Administrator should ensure that the MiVoice Business Console connects to a MiVoice Border Gateway.

Security Certificate

The console connects to the MiVoice Business system using a secure connection if the Enable TLS for IP Set Registration option is enabled in the ESM System Options form. When the console starts, it validates the TLS certificate provided by the MiVoice Business system against the console's certificate database.

- If the validation fails, the console displays a security error message and aborts the connection. To resolve this, the Administrator should run the MiVoice Business Console Configuration Wizard, verify whether the certificate provided matches the details in the ESM Device Certificate form, and add the required certificate to the console's certificate database.

MiVoice Border Gateway Secure Connection

To connect MiVoice Business Console operating in Teleworker mode to the MiCollab Client Server the Administrator should:

- Enable the MiVoice Border Gateway Secure Connection option if you want to connect to the MiCollab Client Server using secure connections (HTTPS on port 443 and SIP on port 6807) through MBG.

Or

- Disable the MiVoice Border Gateway Secure Connection if you want to connect directly to the MiCollab Client Server.

IP Sets 6900

Call Signaling Encryption

Two main protocols are supported and either of the protocols may be used to secure a signaling channel, they are:

- Secure MiNET, which is a Mitel standard
- TLS (Transport Layer Security), which is an open standard and the recommended protocol.

Mitel's Secure MiNET protocol uses the Advanced Encryption Standard (AES) to encrypt call control packets. Using secure MiNET ensures that call control signaling packets between the IP phones and the MiVB are protected from eavesdropping. Using secure MiNET also protects the call control engine from unauthorized control packets.

The TLS security protocol provides data encryption, server authentication message integrity, and optional client authentication for a TCP/IP connection. TLS will prevent unauthorized access to administrative functions. TLS encrypts all traffic on the link to prevent sniffing of usernames and passwords.

- The recommended protocol for securing the signaling channels is TLS, the Administrator should ensure that the TLS security levels be set to High.

To do so, the Administrator must access the System Security Management form which is in turn used to access the Application TLS Security Level Form.

Media Path Streaming

Media path security between IP phones or between an IP phone and a controller is accomplished with either the Secure Real Time Protocol (SRTP), which is a standards based protocol described by RFC 3711, or a Mitel variation of SRTP termed Mitel SRTP, both using the 128-bit Advanced Encryption Standard (AES). Mitel-SRTP uses the same encryption algorithm as SRTP.

- The Administrator must ensure that media path is secured between IP phones and between IP phones and the MiVB.

To enable encryption on the media path, the Administrator must use the MiVoice Business System Administration Tool to access the System Options Form. The MiVoice Business controller specifies streaming connections using SRTP or Mitel-SRTP based on whether SRTP is enabled on the MiVoice Business and the capabilities of the connection endpoints, including Mitel and third party phones. If SRTP is enabled and supported by both end points, SRTP is chosen; if not, Mitel SRTP is chosen.

MiVoice Border Gateway

Call Signaling

- The Administrator should ensure that MiNET call signaling is secured with TLS 1.2.
- The Administrator should turn off plaintext transports such as UDP or restrict this traffic to specific networks.

Voice Media

- To secure calls being processed by the MiVoice Border Gateway, the Administrator should enforce the use of SRTP on both the WAN and LAN ports of the MiVoice Border Gateway.

Web UI Access

- The Administrator should ensure that all access to internal web interfaces through the Remote Proxy Service use TLS 1.2.

API Access

Application access through the Provisioning API uses HTTPS (TLS) with high-grade cipher suites. Use of TLS 1.2 can be enforced.

Application access through the Secure Recording Connector is encrypted with TLS. Use of TLS 1.2 can be enforced.

Each application instance is authenticated with a unique certificate issued by the MiVoice Border Gateway Administrator.

- The Administrator should enforce the usage of TLS 1.2 for all Application accesses through the Provisioning API and the Secure Recording Connector.

MiContact Centre Business

Encryption - Secure Connections

All provisioning interfaces to the MiContact Centre Business system use secure channels.

- Channels that are not secured should be disabled by the Administrator.
- The Administrator should force the use of TLS 1.2 on all signaling channels.

Voice Media

To secure calls being processed by the MiVoice Contact Centre, the Administrator should enforce the use of SRTP on the LAN ports of from the MiVoice Border Gateway to the IVR servers.

Web UI Access

- The Administrator should ensure that all access to internal web interfaces through the Remote Proxy Service use TLS 1.2.

Open Integration Gateway (OIG)

All provisioning interfaces use secure channels.

- Channels that are not secured should be disabled by the Administrator.
- The Administrator should force the use of TLS 1.2.

The authentication mechanism for the MiVoice Integration for Google application attempting connection with the Open Integration Gateway server is controlled and maintained by the Open Integration Gateway Administrator. MiVoice Integration for Google must be added to the list of Allowed Applications by the Open Integration Gateway Administrator to the Open Integration Gateway server and configured with a local password to authenticate the application. Mitel Open Integration Gateway server must be configured to use a CA certificate when end users are using the MiVoice Integration for Google application.

Mitel Standard Linux

Data in Transit

Data in transit may be encrypted with different security levels - TLSv1.1, and TLSv1.2 only. TLS 1.0 is supported for backwards compatibility but is disabled by default.

- The Administrator should ensure that the most secure encryption level is employed.

Certificates

A default self-signed SSL certificate is provided with the MSL server. For enhanced security and ease of use, the Administrator may obtain a signed SSL certificate from a third-party Certificate Authority (CA). Two options are available:

  - Let's Encrypt is an automated, and open Certificate Authority, the acquired certificate is monitored and renewed automatically.
  - An alternative third-party Certificate Authority can issue an Extended Validation SSL certificate upon request, typically for a fee. Companies such as Entrust and GoDaddy provide such services.

- The Administrator should ensure that a signed SSL certificate from a third-party Certificate Authority is used.

Product Security Information

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/en-ca/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

Disclaimer

THIS SECURITY OPERTIONS 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 MiCloud Flex, MiVoice Business 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.