MiVoice Office 400 – Security Guidelines

MiVoice Office 400 Security Guidelines 6.3

Version 1.0

March 2021

NOTICE

Contents

1 Introduction

1.1 Overview

This document provides an overview of the security mechanisms available to protect the MiVoice Office 400 solution from network threats and maintain user data privacy. This document will be of interest to personnel who are responsible for ensuring the secure deployment and the secure operation of the MiVoice Office 400.

Every organization should have a clearly defined IT security policy in place, defining goals, assets, trust levels, processes, incident handling procedures, and so on. The security mechanisms available in the MiVoice Office 400 solution should be covered by and configured according to this policy.

Security is an integral part of the MiVoice Office 400 system design; this document describes the MiVoice Office 400 security features and also provides recommendations on how the administrator should configure the security features to ensure a secure MiVoice Office 400 deployment.

The MiVoice Office 400 security features are enabled in the system by default, enabled during the installation/configuration phase of the system, or need to be enabled manually by the system admin when the MiVoice Office 400 system is initialized.

The MiVoice Office 400 security measures are mainly based on the following open standard technologies and access management mechanisms:

- TLS – Transport Layer Security (TLS 1.2) provides secure access to IP phones and secure signaling between IP phones and MiVoice Office 400 Service Nodes. The Transport Layer Security (TLS 1.2) provides secure web access to MiVoice Office 400 Service Nodes.
- SSH – Secure Shell (OpenSSH_8.2p1) provides secure console-based access to file system of the MiVoice Office 400 Small Medium Business Controller (SMBC) / Virtual Appliance (VA).
- SRTP – Secure Real-time Transport Protocol (SRTP) is used to protect the voice media streams between IP phones, and between IP phones and the MiVoice Office 400 with up to 128 bit AES encryption.
- Correct configuration of identity and access management policies to secure all end-user and administrator accounts, roles, permissions and password policies.

Other mechanisms that can be employed to protect the MiVoice Office 400 are based on the following:

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

An important security measure is to establish and maintain physical security. Only authorized personnel should have access to server locations because many data-exposure attacks can be mounted by having physical access to a host. Further, the IT data infrastructure should be designed with security in focus;

security mechanisms and protocols should be enabled, and all components of the whole system must be correctly configured, and maintained, and updated, as necessary.

2 About the MiVoice Office 400 Documentation Set

Documents for MiVoice Office 400 are available on the Mitel Document Center web site (https://www.mitel.com/document-center/business-phone-systems/mivoice-office-400) to anyone.

The following documents provide important information about the MiVoice Office 400:

- Mitel SMB Controller System Manual (syd-657)
- Mitel 470 System Manual (syd-0585)
- Mitel 415 and 430 System Manual (syd-0580)
- Virtual Appliance (VA) System Manual (syd-0590)
- System Functions and Features (syd-0570)
- SIP DECT Configuration Guide for MiVoice Office 400 (syd-0685)
- Mitel Open Interfaces Platform OIP (syd-0575)
- MiVoice Office 400 Application Card CPU2-S (syd-0620)
- MiVoice Office 400 Application Card CPU2-S Upgrade Guide (Windows 7 to Windows 10)
- MiVoice Office 400 Advanced Intelligent Network (AIN) System Manual (syd-0560)
- Mitel Standard Linux (MSL) Installation and Administration Guide
- Mitel SIP Teleworker via MBG on MiVoice Office 400
- MiVoice Border Gateway Installation and Maintenance Guide
- MiVoice Border Gateway Engineering Guidelines (syd-0675)
- MiVoice Office 400 Getting Started with Mitel 470 in Hospitality Environments (syd-0668)
- MiVoice Office Mobile Application
- MiVoice Office 400 Mitel OfficeSuite (eud-1684)
- Mitel CloudLink Gateway User Guide (https:/www.mitel.com/document-center/technology/cloudlink/all-releases/en/cloudlink-gateway-html)

The MiVoice Office 400 provides an integrated, web-based system configuration tool (WebAdmin) with a powerful online help.

The following documentation is related to deploying IP phones and can be found on the Mitel Document Center web site:

- Mitel IP Sets Engineering Guidelines
- SIP IP Phone Administrator Guide
- Network Engineering for IP Telephony
- *Ethernet Twisted Pair Cabling Plant, Power* and *Grounding Guidelines*

  Additional security related documentation can be found on Mitel's web site at: https://www.mitel.com/en-ca/document-center/security

3 Product Architecture

MiVoice Office 400 is a family of IP-based communications servers for professional use in companies and organizations operating as small and medium-sized businesses in all industries. The family consists of five systems with different expansion capacities. The systems can be expanded using cards, modules, and licenses.

The MiVoice Office 400 family covers the growing demand for solutions in the area of unified communications, multimedia, and enhanced mobile services. It is an open system that supports global standards and is therefore easily integrated into any existing infrastructure. With its wide range of networking capabilities, the system is particularly well suited for companies that operate in several locations. Coverage can be extended to the smallest branch offices at low cost. MiVoice Office 400 communication systems support Voice over IP technology with all its benefits. The systems also operate just as easily with traditional digital or analogue phones and public telephone networks. With the integrated Media Gateways, any hybrid form of an IP-based, digital or analogue communication environment is possible. This enables customers to change their solution from traditional telephony to IP-based multimedia communication either in one step or gradually in several stages as preferred.

The MiVoice Office 400 product family includes the 415, 430, 470, SMBC and Virtual Appliance (VA) systems. Although these systems run on different hardware platforms, their functionality is essentially the same. Most of the interfaces are also available on all systems. Therefore, the statements in this document are valid for all systems of the product family. Exceptions are noted in the description of the individual interfaces

Product family:

- MiVoice Office 415/430: Embedded hardware-based call server
- MiVoice Office 470: Embedded hardware-based call server
- MiVoice Office 400 SMBC: Embedded hardware-based call server
- MiVoice Office 400 VA: Virtual Appliance (Mitel Standard Linux MSL)

3.1 Security Overview

The MiVoice Office 400 has been designed in accordance with Mitel's Secure Development Life Cycle (MiSDLC). For further details, see the section called Secure Development Life Cycle in this document. The MiVoice Office 400 has security features that address identity, authentication, encryption, and access and authorization.

MiVoice Office 400 also supports access and event logs and security certificates.

The MiVoice Office 400 security features are securely configured via the WebAdmin, a web-based, integrated system administration tool. The WebAdmin contains embedded help files with extensive search capabilities that will assist the admin with forms configuration. Transport Layer Security protocol

(TLS 1.2) is by default used to encrypt the data on the connection between the user's computer and the WebAdmin over TCP port 443 (HTTPS).

4 Securing the Operating System

4.1 Operating System Overview

- MiVoice Office 415/430 software is installed on Enea OSE® real-time embedded OS Version 5.8
- MiVoice Office 470 software is installed on Enea OSE® real-time embedded OS Version 5.8, extendable with plugin card (CPU-2, Windows 10 IoT Enterprise) for application server (for example, Mitel's Open Interfaces Platform - OIP)
- MiVoice Office 400 Virtual Appliance (VA) is installed on top of the Mitel Standard Linux OS 10.6.22.0 x86_64 (MSL, based on CentOS)
- Mitel's SMB Controller (SMBC): Embedded hardware-based communication server with Linux-based management software (Mitel Embedded Linux Distribution 1.2.5.9). MiVoice Office 400 software (RPM) can be installed. In addition, the applications OIP and CloudLink Gateway can be installed as extensions of the MiVoice Office 400.

As with all systems, the location of the solution should be physically secured from unauthorized access.

4.2 Operating System Related Network Controls

In their default initial state, the MiVoice Office 400 platforms' configuration provides only the minimum required access for setting up and configuring the system. The WebAdmin application that provides access to the system using a default username and password that the customer (admin) is forced to change upon first accessing the system.

Network access is reduced to the minimum and can be configured by the customer (admin):

- All unused IP ports are disabled
- Remote maintenance via SRM or ISDN is disabled
- FTP is disabled by default (needed for provisioning of Mitel SIP/IP terminals)
- SSH (OpenSSH 8.2p1) is disabled by default (MiVoice Office 400 VA / SMBC)
- TLS v1.2 by default
- Redirect WebAdmin to HTTPS by default
- Dynamic IP Blacklist for SIP (prevent Denial-Of-Service attacks)
- CSTA for First/Third-party CTI (for example, Mitel Dialer) is disabled

Note: The Monitor-Port (TCP/1818) was made switchable with Release 6.3. After a first start (factory reset) this port is closed and can be opened by the customer (admin) for maintenance purposes. FTP and TFTP are permanently activated for maintenance purposes and for Mitel SIP/IP terminals (provisioning).

Mitel strongly recommends that networking security procedures (such as Access Control Lists and Firewalling) be used to restrict access to only the devices that require these services.

5 Administration

5.1 Administration and Management Tools

The MiVoice Office 400 provides the customer with the following integral administration and management tools:

WebAdmin:

- Web-based, integrated configuration tool for configuring and monitoring a single system or an entire network of multiple MiVoice Office 400 systems (AIN - Advanced Intelligent Network)
- Expert or standard mode
- Access control with user accounts and predefined authorization profiles
- Special accesses for hospitality solutions
- Integrated online help and configuration assistant (wizard)
- Integrated in the communication server software package

Self Service Portal (SSP):

- Integrated web-based application for end-users (System User Interface, part of the WebAdmin), which allows personalized configuration of a telephone
- Functions key assignment and printing of labels
- Setting the idle text and language
- Setting the presence profiles, personal call routing, voice mail, forwarding, and so on.
- Setting up dial-in conference rooms
- Creating private phone book contacts
- Managing personal data such as email address, password, PIN, and so on.

Mitel 400 Hospitality Manager:

- Integrated web-based application (part of the WebAdmin) used to operate functions in the hospitality sector
- List view and floor-by-floor view of the rooms
- Functions such as check-in, check-out, group check-in, notification, wake-up call, retrieval of call charges, maintenance list, and so on.

These three different management tools are provided in order to meet the needs of technicians, administrators, and the telephony users themselves. Transport Layer Security protocol (TLS 1.2) is used to encrypt the data on the connection between the customer's computer and the MiVoice Office 400 management tools over TCP port 443 by using the HTTPS protocol.

5.2 Web Server Certificate

The MiVoice Office 400 by default creates a self-signed certificate for authentication of the MiVoice Office 400 to web browsers. However, self-signed certificates are inherently untrusted by the web

browser. This can be mitigated by installing the self-signed certificate on the local computer or bypassed by making an exception.

Mitel's recommendation is to install a certificate obtained from a Certificate Authority (CA) that the customer already owns (that is, an Enterprise Validated CA). The web browser will then trust the MiVoice Office 400 access. Note that certificates do expire and so the customer must be aware of the expiry date and renew them when needed

5.3 Administration Encryption

The WebAdmin is accessed through HTTPS on TCP port 443, which must be allowed through any data network local access control list or firewall. MiVoice Office 400 utilizes Transport Layer Security (TLS) version 1.2.

Note: By default, MiVoice Office 400 is initially configured to support only TLS 1.2 for the entire system (HTTPS, SIP TLS,…). If older SIP phones, for example, Mitel 6700 SIP series phones, are to be used, TLS 1.0 will also need to be activated in WebAdmin (compatibility mode).

The following encryption modules are available in the Cipher Suite of MiVoice Office 400 by default:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_RSA_WITH_SEED_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM

In the unlikely situation that requires a cipher to be removed, contact Mitel technical support.

5.4 Identity, Authentication, Profiles, and Password Policies

To ensure privacy and maintain system integrity, access to the MiVoice Office 400 is restricted by a login password to those users that can be correctly identified and authenticated. Users will be forced to change the factory default password to a password of their choosing.

The WebAdmin is used to create or change a user account. For maintenance purposes, the front panel of the MiVoice Office 470 offers the possibility to activate a time limited password-free access to the system. This function is possible only locally and therefore, requires physical access to the MiVoice Office 470 system. For details refer to the Mitel 470 System Manual (syd-0585).

Recommendation

It is recommended to restrict physical access to the MiVoice Office 470 system to authorized personnel.

Each user account must be linked with an authorization profile. Authorization profiles determine the users' access rights. A series of standard profiles are available. The admin can change and create new authorization profiles.

There are some predefined user accounts that are required for certain applications. These accounts cannot be deleted. For example, the predefined user account “amcc” is intended for operating a Mitel Mobile Client Controller, and the user account “blustar” and “bucs” are meant for BluStar. The predefined user accounts can be changed but cannot be deleted.

The password strength rules are fixed and cannot be changed.

Password rules:

- A password must consist of a minimum of 8 and a maximum of 255 characters
- Unlike the usernames, the passwords are case sensitive
- The password must contain at least one uppercase letter A - Z
- The password must contain at least one lowercase letter a - z
- The password must contain at least one digit 0 - 9
- The password must contain at least one of the following special characters:
  ?, /, <, >, -, +, *, #, =, full stop, comma or space
- German umlauts (for example, ä, ö, ü) and other diacritical characters (for example, é, à, â) are not permitted
- The default password “password” is not permitted
- The password must not be the same as the username
- It is not allowed to use the last 4 historic passwords

Recommendation

It is recommended that a strong password setting is used.

Note: The password never expires until the next change. If the password should be changed, the last 4 passwords must not be reused (password history).

Users logging in to the Self Service Portal (SSP) for the first time are required to change the default pin.

If the user (admin) logs in to the WebAdmin for the first time after installation, the user has to change the default password.

If a user fails a log in attempt, the event is recorded in the access log. The number of consecutive failed login attempts allowed is hardcoded at 15. If the log in fails 15 times the user’s IP is blocked for 10 minutes (to prevent Brute Force attacks). The blocking time is not configurable.

5.5 Access and Authorization

For privacy, all personal data processing is protected with role-based access and authorization controls, which include personal data processing by data subjects, administrators, technical support and machine

APIs. For system integrity and reliability, including the controls that protect privacy, all system data processing, and all access to databases, files, and operating systems, are protected with role-based access and authorization controls.

In the MiVoice Office 400 WebAdmin, there are two forms used to administer access and authorization: The *User Account* form and the *Authorization Profiles* form. A description of these two forms follows.

5.5.1 User Account Form

Purpose

The *User Account* form is used by the system admin to create, modify, and delete additional user accounts:

- Username
- Password / Password confirmation
- Full name
- Description
- User account available
- Authorization profile
- FTP root directory
- File Access

5.5.2 Authorization Profiles Form

Purpose

The admin uses the *Authorization Profiles* form to perform the following tasks:

- Change default profiles
    - Administrator
    - Administrator (Standard mode only)
    - System manager
    - 1st party CTI user via LAN
    - 3rd party CTI user via LAN
    - Support
    - Hospitality administrator
    - Receptionist
    - BluStar Server
    - blustar
    - LDAP
    - OIP
    - Hospitality administrator
- Creating new profiles
    - Profile name
    - Description

- User access control
- Audio services
- OIP
- Office 45
- FTP
- Monitor
- CTI first party
- CTI third party
- ATAS
- Remote maintenance dial-up access
- System Search
- WebAdmin
- LDAP name service access

Recommendation

- It is recommended that the admin creates a user authorization profile. The admin should establish MiVoice Office 400 user authorization profiles that comply with the company policy and business requirements.
- The admin should create temporary authorization profiles to support maintenance and/or troubleshooting activities. The authorization profiles should be deleted once the activities have completed.
- When a user is no longer an employee of the company, the admin should delete all authorization profiles associated with that user.

5.6 Audits, Logs, and Event Reporting

Several audit trails and event and access logging capabilities are supported to maintain records of data processing activities and system accesses.

5.6.1 Access Logs

Purpose

The Access Logs form provides a historical record of access attempts and configuration changes from WebAdmin and various other user interfaces and applications.

- In general, login/logout attempts and any action from any user interface or application connected
- to MiVoice Office 400 that results in a change to the system database is logged.
- The last 20 access attempts, which were rejected due to incorrect login data, are listed in the Failed Access Log.
- The last 20 successful access attempts via a user account are also listed in the normal Access Log.
- Access logs are included in the system backup.

The user interfaces and applications audited for database changes and logins/logouts are as follows:

- WebAdmin (including Self Service Portal, Hospitality Manager)
- OIP
- CPU2
- Monitor
- LDAP
- FTP
- Remote Access via Secure IP Remote Management Server (SRM)
- Remote Access via ISDN (BRI)
- CTI first-party
- CTI third-party
- ATAS
- SIP Trunks (new feature “Multi-Gateways” on MiVoice Office 400 SMBC)

The user actions audited are:

- Logins and logouts, both successful and unsuccessful attempts
- Provisioning operations
- Maintenance operations

Note: The MiVoice Office 400 does not allow the admin to delete the access logs.

Recommendation

Refer to the MiVoice Office 400 WebAdmin Help file for the Access logs form for additional information about types of login/logouts that are audited and the log file size and location.

5.6.2 Event Reporting

Purpose

The MiVoice Office 400 generates an event message every time an event or error occurs. The event tables are used to specify how often an event message of a particular type may be generated by the system over a given period before the event message is sent to the allocated signal destinations.

Recommendation

Refer to the MiVoice Office 400 WebAdmin Help file for the Event logs form for additional information about types of event messages.

5.7 Network Alarms, Monitoring, Supervision

The MiVoice Office 400 supports system supervision with event notifications to multiple interfaces such as SNMP, System phones, E-mail, PPP link, SRM or Event log.

The MiVoice Office 400 generates an event message every time an event or error occurs. The event tables are used to specify how often an event message of a particular type may be generated by the system over a given period before the event message is sent to the allocated signal destinations.

5.7.1 SNMP

The SNMP interface is used to connect the MiVoice Office 400 to an SNMP Management System (for example, 3rd party) with the purpose of receiving alarm notifications in the form of SNMP TRAP requests provided by the MiVoice Office 400 and related terminals. The interface is based on the SNMPv1 standard specified by RFC1157.

The SNMP Protocol Data Unit "TRAP" is based on the default port "162" and it is sent from the MiVoice Office 400 to the remote Network Management System (NMS). The SNMP Protocol Data Unit "GET" is based on the default port "161" and it is sent from the NMS to the MiVoice Office 400.The Management Information Base (MIB) contains the Managed Objects (MOs) which are necessary to store the status or the representation of the "event" message in the MiVoice Office 400.

- SNMPv1
- Unencrypted via UDP/IP, Port 161 (GET) , Port 162 (TRAP)
- Messages are encoded according to ASN.1 data types defined in ITU standard X.208
- Community string is "public", and is not configurable
- Management Information Base (MIB) library version 1027.1.2.4

Supported commands are shown in the following table:

Request (RFC 1157)	**Supported by MiVoice Office 400**
GetRequest-PDU	Yes
GetNextRequest-PDU	No
GetResponse-PDU	Yes
SetRequest-PDU	No
Trap-PDU	
coldStart Trap	No
warmStart Trap	No
linkDown Trap	No
linkUp Trap	No
authenticationFailure Trap	No
egpNeighborLoss Trap	No
enterpriseSpecific Trap	Yes

5.7.2 System Phones

Event messages are sent to all system phones with displays and entered in the corresponding message group.

5.7.3 E-mail (SMTP)

Event messages are sent by email (configurable via WebAdmin) to configured recipient (authentication with CRAM-MD5 optional).

- SMTP PLAIN
- SMTP TLS 1.2

5.7.4 PPP link (external destination)

Event messages can be sent by opening a Point-to-Point communication channel (ISDN or analog external) to a terminal adapter or modem. Mitel recommends that the solution be configured so that the PPP channel is established only in an outbound direction to a known destination and that inbound connections are not used. Once the event message has been confirmed, the system clears the PPP link.

5.7.5 TCP/IP (local destination)

Event messages are sent to a specified IP address and TCP port (configurable via WebAdmin) via Ethernet as plain text.

5.7.6 Secure IP Remote Management Server (SRM)

Event messages can also be sent to the SRM server. Destination IP address and Port (default 443) of the SRM Server are configurable in the WebAdmin. The transport uses HTTPS as protocol.

6 Network Security

The MiVoice Office 400 and associated components communicate using the corporate network infrastructure.

6.1 Network Access Security

As with any network-attached device or application, the connection can potentially be accessed by unauthorized persons (“hackers”). If network access is not restricted, a bad actor can attempt to access the MiVoice Office 400 system and misuse it for their gain, for example, Toll Fraud. Unauthorized access can be from the outside (as from the WAN or from the Internet) when an access to the company’s data network has been permitted and also from an internal user. In both cases, the network access must be limited to only authorized personnel.

Note: MiVoice Office 400 systems are not designed to be connected directly to the Internet or a WAN. The MiVoice Office 400 must be deployed behind a reliable and secure firewall. Furthermore, a VPN is needed for AIN connections. For Teleworker and SIP trunks, the Mitel Boarder Gateway as a Session Boarder Controller can be used in addition to an existing firewall or replace it completely. Further information can be found in the document Mitel SIP Teleworker via MBG on MiVoice Office 400 (https://www.mitel.com/de-de/document-center) and MiVoice Border Gateway Engineering Guidelines (syd-0675) (https://www.mitel.com/de-de/document-center) available in the Mitel document center.

Recommendation

For the connection to a SIP provider, which does not deliver the connection via a secure VPN (for example, MPLS), and when no Session Boarder Controller is used, a firewall is recommended, which should be configured as follows:

- Block all incoming connection attempts in the direction to MiVoice Office 400

- Open specific ports
- SIP (Signaling) unencrypted: TCP Port 5060
- SIP (Signaling) encrypted: TCP Port 5061
- Media (Speech) RTP / SRTP UDP Ports 5004 – 5xxx
- Media (Speech) for Mitel IP System Devices UDP Port 30000
- Media (Speech) for Mitel SIP Devices UDP Port 3000

6.1.1 SMBC with multiple network interfaces (eth0, eth1, eth2, eth3)

In older releases of the SMBC platform software only one Ethernet interface (eth0) was supported. Installed applications such as the MiVoice Office 400, realized all network-based features (WebAdmin, VoIP, AIN, CTI, SIP Trunking, etc.) via this interface. With Release 6.3 of the MiVoice Office 400 a new feature called "Multi-Gateways for SIP Trunks" was implemented, which allows multiple SIP Trunks on different network interfaces and/or subnets. For this purpose, the SMBC platform software (Mitel Embedded Linux Distribution 1.2.5.9) was extended with the support of all physically existing 4 Ethernet interfaces (eth0, eth1,eth2,eth3).

With these multiple network interfaces, the SMBC acts partially as a router. This means that IP Forwarding has been activated between the interfaces and is therefore to be considered in a security assessment.

6.1.2 Network components

It is recommended that the Ethernet LAN switches used to provide IP phones with LAN connectivity be managed, enterprise-grade switches that include integrated access control measures. It is also recommended that the system administrator ensure that the switch access control measures are properly configured and maintained. IP Port information follows below.

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

6.2 IP Ports

The following table shows the TCP/UDP ports used by the MiVoice Office 400 to communicate with IP phones and other components of the MiVoice Office 400 solution.

Port (Range)	Service	Transport Protocol	Initial data sent ←from / →to peer	Link Type
20	FTP Data (MiVoice Office 400 as server)[1]	TCP	←	Node ← PC (SystemSearch EUL)
20	FTP Data (MiVoice Office 400 as server)[2]	TCP	→	Node → MiVoice 5300 IP
20	FTP Data (MiVoice Office 400 as client)	TCP	←	Node ← Localization Server
21	FTP Control (MiVoice Office 400 as server)[1]	TCP	←	Node ← PC (SystemSearch EUL)
21	FTP Control (MiVoice Office 400 as server)	TCP	←	Node ← MiVoice 5300 IP
21	FTP Control (MiVoice Office 400 as client)	TCP	→	Node → Localization Server
22[3 4 5]	Secure Shell	TCP	←	Node ← PC
23[1]	Telnet	TCP	←	Node ← PC
25[3]	SMTP client	TCP	→	Master/Standalone → SMTP Server
53	DNS server	UDP	→	Node → DNS Server
67	DHCP server	UDP	←	Master/Standalone ← any host
68[1]	DHCP client	UDP	→	Node → DHCP Server
69	TFTP server	UDP	←	Node ← PC
80	HTTP	TCP	←	Node ← PC (WebAdmin)
123	NTP client	UDP	→	Master/Standalone → NTP Server
161	SNMP	UDP	←	Node ← PC
162	SNMP TRAP	UDP	→	Node → PC

[1] Applies only for the MiVoice Office 415 / 430 / 470

[2] Applies only for the MiVoice Office 415 / 430 / 470 and is configurable (off / just IP phone / on) using the setting “FTP service”

[3] Configurable via MiVoice Office 400 configuration tool (WebAdmin).

[4] Applies only for the MiVoice Office 400 SMBC

[5] Applies only for the MiVoice Office 400 Virtual Appliance

389[3]	LDAP server	TCP	←	Node ← OMM Node ← MMCC
443[3]	HTTPS (Secure Transmission)	TCP	←	Node ← PC (WebAdmin)
443	SLS (HTTPS)	TCP	→	Node → SLS Server
465[3]	SMTPS	TCP	→	Node → SMTP Server
1061	OIP	TCP	←	Node ← OIP Server
1070	Name Server (atns)	TCP	←	Node ← OIP/TWP Server
1074	AIF-TSP (atpc3)	TCP	←	Node ← OIP/TWP Server
1088	ATAS Agent	TCP	←	Node ← PC
1112	MiVoice Office 400 Information Link (AIL)	TCP	←	Node ← OIP Server
1114	SC Configuration Monitor	TCP	←	Node ← PC
1116	TWP Link	TCP	↔	Node ↔ TWP Server
1130	Open Application Interface	TCP	←	Node ← PC
1131	Secure Open Application Interface	TCP	←	Node ← PC
1132	ATAS interface for Open Care Applications	TCP	←	Node ← PC
1136	SIP-DECT configuration monitor (AXI)	TCP	←	Node ← PC
2222	Secure Remote Management	TCP	→	Node → SRM Server
2855[4]	MSRP	TCP	←	Node ← PC
5004 - 5051[1] [2] 40000 - 40059[1] [4]	RTP on Standard Media Switch or UDPTL (Fax T.38)[5]	UDP	↔	Node ↔ Node Node ↔ Mitel IP-Term. Node ↔ SIP Phone/Trunk
5060[1]	SIP Service	UDP/TCP	→ ←	Master/Standalone ↔ SIP provider Master/Standalone ← SIP Phone
5061[1]	SIPS/TLS Service	TCP	→	Master/Standalone ↔ SIP provider Master/Standalone ← SIP Phone

[2] Applies only for the MiVoice Office 415 / 430 / 470 and is configurable (off / just IP phone / on) using the setting “FTP service”

[4] Configurable via MiVoice Office 400 configuration tool (WebAdmin).

[5] Applies only for the MiVoice Office 415 / 430 / 470

[6] Applies only for the MiVoice Office 400 Virtual Appliance

[7] Applies only for the MiVoice Office 400 SMBC

6830[1]	SX200 Voicemail Management	TCP	←	Master/Standalone ← PMS
7001[1]	CSTA	TCP	←	Node ← PC (CSTA Appl.)
7011[6]	Media Server (MSRV)	TCP		Node ← PC
8053	DNS client	UDP	→	Node → DNS Server
8065	IP Phones GW	TCP	→ ←	Master/Standalone ↔ IP Phones
8080[4]	HTTP	TCP	←	Node ← PC (WebAdmin)
8443[4]	HTTPS (Secure Transmission)	TCP	←	Node ← PC (WebAdmin)
8888[4]	Find My SMBC (HTTP)	TCP	↔	Node ↔ PC (smbcSearch)
15374[1]	SX200 Hotel Management	TCP	←	Master/Standalone ← PMS
18060[1]	IP-Phone Signaling	TCP/UDP	←	Node ← MiVoice 5300 IP
18061[1]	Secure IP-Phone Signaling	TCP	←	Node ← MiVoice 5300 IP
19790	Link Handler	TCP	↔	Master ↔ Satellite
33555[1]	SX200 Call Data Records	TCP	←	Master/Standalone ← Call accounting application
40000 - 40499[1] [6]	RTP on Media Server	UDP	↔	Node ↔ Node Node ↔ Mitel IP-Term. Node ↔ SIP Phone/Trunk
59901 - 60000[2] 37001-65535[3] 32768 - 60999[7]	Link Handler	TCP	↔	Master ↔ Satellite
64950 - 64999	NAT for PPP access	TCP	↔	Node → Node
	MONITORS			
1818[8]	Maintenance Monitor	TCP	←	Node ← PC
2323[9]	System shell	TCP	←	Node ← PC

[2] Applies only for the MiVoice Office 415 / 430 / 470 and is configurable (off / just IP phone / on) using the setting “FTP service”

[4] Applies only for the MiVoice Office 400 SMBC

[6] Applies only for the MiVoice Office 400 Virtual Appliance

[7] Applies only for the MiVoice Office 400 SMBC

[8] Configurable via MiVoice Office 400 configuration tool (WebAdmin)

[9] Applies only for the MiVoice Office 415 / 430 / 470

Note: Additional system monitors are available on the following TCP ports, if the system configuration flag “Open all server/monitor ports” is activated. They occupy the following ports: 1056, 1060, 1062, 1065-1067, 1071, 1072, 1075-1078, 1081, 1083, 1085-1087, 1091, 1092, 1094, 1097-1101, 1103-1106, 1108-1111, 1113, 1114, 1116-1118, 1120-1123, 1126-1129, 1133, 1134, 1720

6.3 Media Encryption - Secure Connections

6.3.1 Phone Streaming

Media path security between IP phones or between an IP phone and a MiVoice Office 400 is accomplished with the Secure Real Time Protocol (SRTP), which is a standards-based protocol described by RFC 3711 using the 128-bit Advanced Encryption Standard (AES).

The MiVoice Office 400 specifies streaming connections using SRTP based on whether SRTP is enabled on the MiVoice Office 400 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. Further information can be found in the document *MiVoice Office 400 System Functions and Features* (syd-0570) (https://www.mitel.com/de-de/document-center).

6.3.2 Advanced Intelligent Network Media Streaming

Scalability of the MiVoice Office 400 solution is achieved by configuring multiple MiVoice Office 400 systems into clusters (AIN). Mitel provides encryption of the media path between multiple MiVoice Office 400 systems using SRTP. TLS 1.2 is used to encrypt the signaling path between multiple MiVoice Office 400 systems. For details, refer to the *MiVoice Office 400 Advanced Intelligent Network (AIN)* System Manual (syd-0560) available in the Mitel document center (https://www.mitel.com/de-de/document-center).

7 Prevention of Toll Abuse

Any communication system that has a combination of integrated auto attendant, Recorded Announcement Devices groups, an auto attendant or voice mail can be susceptible to toll abuse if not configured correctly. Therefore, it is important to assign appropriate telephone privileges and restrictions to devices. The use of Direct Inward System Access (DISA) is not recommended.

In addition, publicly accessible telephones should be denied toll access unless authorized through an attendant. The MiVoice Office 400 system provides comprehensive toll control as an integral part of the call control engine. The MiVoice Office 400 call control gives the admin the ability to restrict a user's access to trunk routes and/or specific external directory numbers.

The MiVoice Office 400 call control offers several call routing capabilities, which when used correctly, can substantially reduce the risk of toll abuse by disallowing the dialing of certain external telephone numbers or ranges of numbers (Call Barring).

7.1 Mitigation of Telephony Denial of Service

Areas that might be subject to Telephony Denial of Service (TDoS) within the system include:

- User end-devices and telephone extensions
- IP to TDM gateway
- Trunk interface to PSTN or SIP service provider

Most attacks for TDoS on the phones are targeted at the IP interface. Mitel phones include a micro-firewall, which applies rate limits to different protocols, including the voice streaming connections. Unexpected packets and packets over and above expected limits are throttled and rejected. For details, refer to the *Mitel IP Sets Engineering Guidelines* (https://www.mitel.com/de-de/document-center).

Note that non-Mitel phones connected to the system, such as third-party SIP devices, may not include this functionality.

The IP to TDM gateway provides the connections between the IP and TDM networks. The primary function is conversion of the voice streams between these networks. Streams with excessive packets are rejected.

UDP Ports for streaming are opened only as required and closed on call completion. Streaming to an unopened UDP port will result in that stream being dropped. Call setup rates are limited in line with the expected number of channels and calls through the gateway.

Primary connections to the PSTN or SIP service provider are via digital trunks or SIP trunks. Digital trunks are limited due to the number of physical channels that can be accessed at any time. The signaling channel and call handling can also be configured for rate limiting.

SIP trunks can handle many trunks and also high call rates. In order to ensure minimal impact due to TDoS, both the end-user system and the connections to the SIP Service Provider need to be balanced. This can be achieved by using a Session Border Controller, which serves as a SIP trunk proxy for the MiVoice Office 400.

The number of trunk connections on the end-user system is limited due to licensing and configuration settings. The service provider connections should be arranged to match the number of channels in a similar manner. Controllers and gateways can also be IP-networked to provide load distribution in situations where high traffic levels need to be handled, for example, call centers.

7.1.1 LAN Quality of Service

For ensuring voice and video quality across a network, Mitel recommends that specific IEEE 802.1p settings be used to ensure that the networking equipment treats voice, video and signaling packets with higher priorities than other traffic at the Ethernet layer. In addition, traffic should be marked appropriately with the Differentiated Services Code Point (DSCP) for prioritization at layer 3.

Following these recommendations increases the possibility that voice, video and signaling packets will be more resistant to a DoS attack. For recommended settings, refer to *Mitel IP Sets Engineering Guidelines* (https://www.mitel.com/de-de/document-center) available in the Mitel Document Center.

8 Product Hardening for Security during Development

8.1 Secure Development Life Cycle

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

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

MiVoice Office 400 Release 6.2 was developed in accordance with Mitel's Secure Development Life Cycle policy. As a result, MiVoice Office 400 Release 6.2 has been designed with best-practice safeguards to mitigate risks to the confidentiality, integrity and/or availability of data contained within MiVoice Office 400 and to the data related to the functionality provided by MiVoice Office 400.

8.2 Miscellaneous Recommendations

8.2.1 System Security Options

The *System Maintenance General* form (see WebAdmin) is used to specify parameters that are used system-wide and contains a number of security related settings, which are described below.

- Remote Access – The default setting is "Not allowed”
- Remote Access – Clip required: The default setting is "Yes”
- Open all server/monitor ports: The default setting is "No”
- FTP service – The default setting is "FTP only for IP terminals”
- Compatibility mode for TLS v1.0 – The default setting is "No”
- Redirect WebAdmin to HTTPS - The default setting is "Yes”
- Save system data – Backup interval: The default setting is "1 hour”

The *IP Network Security General* form is used to specify parameters that are used system-wide and contains a number of security related settings, which are described below.

- DoS protection – Suspicious IP addresses are blocked for the amount of time: The default setting is 5 minutes
- DoS protection – Max SIP authentication failures: The default setting is 10
- DoS protection – Max SIP transactions per IP address: The default setting is 200
- VoIP encryption (SRTP) – The default setting is “No”
- TLS enable keep alive – The default setting is “Yes”

Recommendation

It is recommended:

- that the admin reviews all these options and set the controls as appropriate for their particular network.
- that the admin enables voice encryption and the use of SRTP.

8.3 Anti-Virus Protection

Applications such as MiVoice Office 400 VA must process data in real-time. Real-time applications require unfettered access to processor resources, memory systems, disk drive accesses, and network communications. When MiVoice Office 400 VA is deployed on proprietary hardware, industry-standard servers or virtual machines – as per Mitel's Standard Linux and Antivirus Software - Guidelines (see Mitel's Knowledge Management System 1W05) – 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. Because these real-time data processing applications execute on carefully sized computing platforms, the installation of antivirus software is not recommended.

8.4 Securing Mitel Standard Linux

Mitel's MiVoice Office 400 VA software is installed on top of the Mitel Standard Linux (MSL) operating system. Compared to more common operating systems, MSL provides a reduced attack surface. This reduced attack surface is the result of the following MSL characteristics:

- MSL does not support email
- MSL does not support internet Web browsing
- Users with write permissions are limited and access is strictly controlled
- Mitel has removed unnecessary files and packages from MSL
- Mitel has closed unnecessary IP Ports

Additional measures can be taken to secure the MSL platform and the MiVoice Office 400 VA application

executing on the platform. These measures are based on well-known network security best practices. Further details can be found in Mitel Standard Linux Security Technical Paper (https://www.mitel.com/en-ca/document-center/technology/mitel-standard-linux/110/en/mitel-standard-linux-security-technical-paper-v13). In general, a platform that is both physically secure and installed in network that has been securely designed will have a low likelihood of being infected compared to a platform that lacks physical security and/or is installed in a network lacking security controls.

9 Product Security Information

9.1 Mitel Product Security Vulnerabilities

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

Mitel's Product Security Policy is available at:
https://www.mitel.com/support/security-advisories/mitel-product-security-policy

9.1.1 Security Risks of Wildcard Certificates

If a wildcard character is used for creating any common name and host name of a certificate, there might arise a security concern that makes the certificate vulnerable. Therefore, to avoid a security risk:

- Common name should not have wildcard characters.
- Certificates should not contain any IP addresses in Common name and Host name.
- Common name and Host name should be properly qualified.

9.2 Mitel Product Security Publications

Mitel Product Security Publications are available at:
https://www.mitel.com/support/security-advisories

10 Disclaimer

THIS SOLUTIONS ENGINEERING DOCUMENT IS PROVIDED “AS IS” AND WITHOUT WARRANTY. IN NO EVENT WILL MITEL NETWORKS CORPORATION OR ITS AFFILIATES HAVE ANY LIABILITY WHATSOEVER ARISING FROM IN CONNECTION WITH THIS DOCUMENT. You acknowledge and agree that you are solely responsible to comply with any and all laws and regulations in association with your use of MiVoice Office 400 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.