

MiVoice Office 400

RELEASE 7.2

VERSION 1.0

SECURITY GUIDELINES

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means – electronic or mechanical – for any purpose without written permission from Mitel Networks Corporation.

Trademarks

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

For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

MiVoice Office 400
Security Guidelines
Release 7.2
Version 1.0
September 2025

Contents

1	Introduction	1
1.1	Overview	1
1.2	What is New in this Release	1
2	About the MiVoice Office 400 Documentation Set	2
3	Product Architecture.....	3
3.1	Security Overview	4
4	Securing the Operating System.....	4
4.1	Operating System Overview	4
4.2	Operating System Related Network Controls	5
5	Administration	6
5.1	Administration and Management Tools	6
5.2	Web Server Certificate	7
5.3	Administration Encryption	7
5.4	Identity, Authentication, Profiles, and Password Policies	7
5.5	Access and Authorization.....	9
5.5.1	User Account Form	9
5.5.2	Authorization Profiles Form	9
5.6	Audits, Logs, and Event Reporting	11
5.6.1	Access Logs.....	11
5.6.2	Event Reporting	12
5.7	Network Alarms—Monitoring and Supervision.....	12
5.7.1	SNMP.....	12
5.7.2	System Phones	13
5.7.3	E-mail (SMTP).....	13
5.7.4	PPP link (external destination).....	13
5.7.5	TCP/IP (local destination).....	13
5.7.6	Secure IP Remote Management Server (SRM)	13
6	Network Security	14
6.1	Network Access Security.....	14

6.1.1	SMBC with Multiple Network Interfaces (eth0, eth1, eth2, eth3).....	15
6.1.2	Network Components.....	15
6.2	IP Ports	16
6.3	Media Encryption—Secure Connections	19
6.3.1	Phone Streaming.....	19
6.3.2	Advanced Intelligent Network Media Streaming.....	19
7	Prevention of Toll Abuse.....	20
7.1	Mitigation of Telephony Denial of Service.....	20
7.1.1	LAN Quality of Service.....	21
8	Product Hardening for Security during Development	22
8.1	Secure Development Life Cycle.....	22
8.2	Miscellaneous Recommendations	22
8.2.1	System Security Options	22
8.3	Anti-Virus Protection.....	23
8.4	Securing Mitel Standard Linux	23
9	Product Security Information	24
9.1	Mitel Product Security Vulnerabilities	24
9.1.1	Security Risks of Wildcard Certificates.....	24
9.2	Mitel Product Security Publications.....	24
10	Disclaimer.....	25

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 must 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 administrator 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 1.2/1.3) provides secure access to IP phones and secure signaling between IP phones and MiVoice Office 400 Service Nodes. The Transport Layer Security (TLS 1.2/1.3) provides secure web access to MiVoice Office 400 Service Nodes. MiVoice Office 470 is only supporting TLS 1.2. SMBC and VA are supporting both.
- SSH – Secure Shell (OpenSSH_8.9p1-patched) 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.

1.2 What is New in this Release

With Release 7.2, Mitel provides the Mitel Embedded Linux 2.1.6.x for SMBC, which has received several security updates, e.g. the Openssl library 3.1.x. The release also includes a new Mitel Standard Linux 12.1 for the MiVoice Office 400 VA. This makes it possible to support TLS 1.3 in both products in the future.

NOTE 1: For technical reasons, an update of the Openssl library in the MiVoice Office 470 was omitted. Support for TLS 1.3 is therefore not possible.

NOTE 2: Upgrading the Mitel Embedded Linux from version 1.3.x.x or earlier to version 2.1.6.x is mandatory. It requires a special procedure, because the SMBC will execute a factory reset. Only the IPv4-Data will kept. We strongly recommend creating backups of all installed applications (MiVoice Office 400, OIP, CloudLink) before updating.

NOTE 3: The MiVoice Office 400 Virtual appliance R7.2 is based on a new Linux MSL 12.1 and is not backward compatible. Therefore, an Linux update by re-installing the OVA/VHD-File is mandatory. We strongly recommend creating backups.

NOTE 4: In parallel to the known SMBC hardware the new SMBC 8/38G was introduced. The MiVoice Office 400 and its applications can be installed on both hardware variants.

2 About the MiVoice Office 400 Documentation Set

Documents for the 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)
- 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>)
- Mitel One Web Application

The MiVoice Office 400 provides an integrated, web-based system configuration tool (WebAdmin) along 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 analog phones and public telephone networks. With the integrated Media Gateways, any hybrid form of an IP-based, digital, or analog 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 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 470: Embedded hardware-based call server
- MiVoice Office 400 SMBC/SMBC 8/38G: 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 [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 administrator with forms configuration. Transport Layer Security protocol (TLS 1.2/TLS1.3) is by default used to encrypt the data on the connection between the user's computer and the WebAdmin over TCP port 443 (HTTPS) and port 8443 (HTTPS) for the SMBC platform administration.

4 Securing the Operating System

4.1 Operating System Overview

- 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 12.1 12.1.12.0 x86_64 (MSL, based on Rocky 8).
- Mitel's SMB Controller (SMBC): Embedded hardware-based communication server with Linux-based management software (Mitel Embedded Linux Distribution 2.1.6.x, based on Yocto 4.0.29). 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 user name and password that the customer (administrator) is forced to change upon first accessing the system.

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

- All unused IP ports are disabled
- Remote maintenance via SRM or ISDN is disabled
- SSH (OpenSSH 8.9p1-patched) is disabled by default (MiVoice Office 400 VA / SMBC)
- TLS 1.3 only by default (MiVoice Office 470 is only supporting TLS 1.2)
- Redirect WebAdmin to HTTPS by default
- Dynamic IP Blocklist for SIP (prevent Denial-Of-Service attacks)
- CSTA for First/Third-party CTI (for example, Mitel Dialer) is disabled

NOTE: The Monitor port 1818/TCP on MiVoice Office 470 was made switchable with Release 6.3. After a first start (factory reset) this port is closed and can be opened by the customer (administrator) for maintenance purposes.

Changed as of Release 7.1:

- MiVoice Office 470 : Switching the Monitor port 1818/TCP on/off also automatically switches System Shell port 2323/TCP on/off. The FTP port 21/TCP is now really closed (IP server socket closed) when FTP is off.
- SMBC with Mitel Embedded Linux 1.3.1.2: The FTP port 21/TCP was made switchable. By default, this port is closed and can be opened by the customer (administrator).
- All: Most application ports (1061/TCP, 1070/TCP, 1074/TCP, 1088/TCP, 1112/TCP, 1116/TCP, 1130/TCP, 1131/TCP, 1132/TCP) was made switchable. For compatibility reasons, these ports remain open so that applications used by the customer, such as Mitel's Open Interfaces Platform OIP, continue to function. The customer (administrator) can close these ports.

As before, the TFTP port 69/UDP is permanently open. It is required for maintenance purposes and for SIP-DECT, 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 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 management tools are provided in order to meet the needs of technicians, administrators, and the telephony users themselves. Transport Layer Security protocol (TLS 1.3) 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 (for example, Chrome, Firefox, and Edge). 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 recommends installing a certificate (PKCS12 package or PEM) 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: Certificates do expire and 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 1.3.

NOTE: By default, MiVoice Office 400 is initially configured to support only TLS 1.3 for the entire system. 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 who 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 that physical access to the MiVoice Office 470 system be restricted to authorized personnel.

NOTE 1: As of SMBC version 2.1.6.0, the SMBC root user can be accessed by the SMBC admin user on the SSH command line by using the su-command. Therefore, the SMBC admin user must configure a strong root password during first install procedure. To enable a strong password, the SMBC's WebAdmin password rules have been expanded and include now the special characters:

?, /, <, >, -, +, *, #, =, !, ", \$, %, &, ', (,), :, ;, @, [,], ^, _ , ` , { , | , } , ~ , full stop, comma, or space

NOTE 2: As of SMBC version 2.1.6.0, Mitel has increased the number of configurable SMBC admin users to 5 (including the default SMBC admin).

Each MiVoice Office 400 user account must be linked with an authorization profile. Authorization profiles determine the users' access rights. A series of standard profiles are available. The administrator 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 user names, 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 user name
- It is not allowed to use the last 4 historic passwords

Recommendation: It is recommended that a strong password setting be 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).

As of Release 7.1, a password expiration time (to login to the WebAdmin) for user with admin rights can be configured. By default, this function is disabled.

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

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

If a user fails a login attempt, the event is recorded in the access log. The number of consecutive failed login attempts allowed is hardcoded at 15. If the login attempt fails 15 times, the user's IP address is blocked for 5 minutes. Furthermore, the user account itself is locked for 60 minutes (preventing brute force attacks). Both blocking times are not configurable.

5.5 Access and Authorization

For privacy, all personal data processing is protected with role-based access and authorization controls, which includes personal data processing by data subjects, administrators, technical support, and machines 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 system administrator uses the *User Account* form to create, modify, and delete additional user accounts:

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

5.5.2 Authorization Profiles Form

Purpose

The system administrator 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 administrator create a user authorization profile. The administrator should establish MiVoice Office 400 user authorization profiles that comply with their company policy and business requirements.
- The administrator 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 administrator 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 administrator 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 and Supervision

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

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, a third-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

MiVoice Office 400 support for commands is 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 1.3

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 the Port (default 443) for the SRM Server are configurable in the WebAdmin. The transport uses HTTPS as the protocol.

6 Network Security

The components associated with MiVoice Office 400 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, to commit 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 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 Advanced Intelligent Network (AIN) connections. For Teleworker and SIP trunks, the Mitel Border Gateway (MBG) as a Session Border Controller can be used in addition to an existing firewall or replace it completely. More information is available 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/document-center/applications/mivoice-border-gateway/12.2/en/mivoice-border-gateway-engineering-guidelines>) 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), a Session Border Controller (SBC) or an MBG should be used to terminate the SIP trunks. If a firewall is deployed between the SBC/MBG and the Internet, the firewall 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 – 50xx
UDP Ports 40000 – 40499
- Media (Speech) for Mitel IP System Devices UDP Port 30000
- Media (Speech) for Mitel SIP Devices UDP Port 3000

NOTE: More details are provided in the [IP Ports](#) section in this document.

6.1.1 SMBC with Multiple Network Interfaces (eth0, eth1, eth2, eth3)

In the earlier 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, and so on) 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 (from Mitel Embedded Linux Distribution 1.2.5.9) was extended with the support of all physically existing 4 Ethernet interfaces (eth0, eth1, eth2, eth3).

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 is given in the next section.

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	Prot.	Port status (default)	Initial data sent ← from peer → to peer	Link Type
20 ¹²	FTP Data (Server)	TCP	closed	←	Node ← PC (SystemSearch EUL)
20 ¹²³	FTP Data (Server)	TCP	closed	→	Node → MiVoice 5300 IP
21 ²	FTP Control (Server)	TCP	open	←	Node ← PC (SystemSearch EUL)
21 ¹²	FTP Control (Server)	TCP	open	←	Node ← MiVoice 5300 IP
21 ³	FTP Control (Server)	TCP	closed	←	Node ← MiVoice 5300 IP
21 ²	FTP Control (Client)	TCP	closed	→	Node → Backup
22 ¹³	SSH	TCP	closed	←	Node ← PC
22 ⁴	SSH	TCP	open	←	Node ← PC
23 ²	Telnet	TCP	closed	←	Node ← PC
25 ¹	SMTP client	TCP	closed	→	Master/Standalone → SMTP Server
53	DNS server	UDP	open	→	Node ↔ DNS Server
67	DHCP server	UDP	closed	←	Master/Standalone ← any host
68 ²	DHCP client	UDP	closed	→	Node → DHCP Server
69	TFTP server	UDP	open	←	Node ← PC
80 ¹⁵	HTTP	TCP	open	←	Node ← PC (WebAdmin)
80 ²	HTTP	TCP	open	←	Node ← Localization Server
123	NTP client	UDP	closed	→	Master/Standalone → NTP Server
161	SNMP	UDP	closed	←	Node ← PC
162	SNMP TRAP	UDP	closed	→	Node → PC
389 ¹	LDAP server	TCP	closed	←	Node ← OMM, Node ← MMCC
443	HTTPS	TCP	open	←	Node ← PC (WebAdmin)
443 ³⁴	HTTPS	TCP	open	←	Node ← Localization Server
443	SLS (HTTPS)	TCP	open	→	Node → SLS Server
465 ¹	SMTPS	TCP	closed	→	Node → SMTP Server
1061	OIP	TCP	closed	←	Node ← OIP Server
1062	AIMS2(Comlib)	TCP	closed	←	Node ← PC
1070	Name Server (atns)	TCP	open	←	Node ← OIP/TWP Server
1074	AIF-TSP (atpc3)	TCP	open	←	Node ← OIP/TWP Server

Port (Range)	Service	Prot.	Port status (default)	Initial data sent ← from peer → to peer	Link Type
1080 ¹	Call Logging	TCP	closed	↔	Node ↔ PC
1088	ATAS Agent	TCP	open	←	Node ← PC
1090	Short Message Service (SMSC)	UDP	open	←	Node ← PC
1112	MiVoice Office 400 Information Link (AIL)	TCP	open	←	Node ← OIP Server
1114	SC Configuration Monitor	TCP	closed	←	Node ← PC
1116	TWP Link	TCP	open	↔	Node ↔ TWP Server
1130	Open Application Interface (OAI)	TCP	open	←	Node ← PC
1131	Secure Open Application Interface (SecOAI)	TCP	open	←	Node ← PC
1132	ATAS interface for Open Care Applications	TCP	open	←	Node ← PC
1136	SIP-DECT configuration monitor (AXI)	TCP	closed	←	Node ← PC
2222	Secure Remote Management	TCP	closed	→	Node → SRM Server
2855 ¹	MSRP	TCP	open	←	Node ← PC
5004 - 50xx ¹²	RTP on Standard Media Switch or UDPTL (Fax T.38)	UDP	closed	↔	Node ↔ Node Node ↔ Mitel IP-Term. Node ↔ SIP Phone/Trunk
5060 ¹	SIP Service	UDP, TCP	open	→ ←	Master/Standalone ↔ SIP provider Master/Standalone ← SIP Phone
5061 ¹	SIPS/TLS Service	TCP	closed	→	Master/Standalone ↔ SIP provider Master/Standalone ← SIP Phone
6830 ¹	SX200 Voicemail Mgmt.	TCP	closed	←	Master/Standalone ← PMS
7001 ¹	CSTA	TCP	closed	←	Node ← PC (CSTA Appl.)
7011 ⁴	Media Server (MSRV)	TCP	open	←	Node ← PC
8053	DNS client	UDP	closed	→	Node → DNS Server
8065	IP Phones GW	TCP	open	→ ←	Master/Standalone ↔ IP Phones
8080 ³⁵	HTTP	TCP	open	←	Node ← PC (WebAdmin)
8443 ³⁴	HTTPS (Secure Transmission)	TCP	open	←	Node ← PC (WebAdmin)
8888 ³	Find My SMBC (HTTP)	TCP	open	↔	Node ↔ PC (smbcSearch)

Port (Range)	Service	Prot.	Port status (default)	Initial data sent ← from peer → to peer	Link Type
9080 ³	HTTP (OIP on SMBC)	TCP	open	←	Node ← PC (OIP WebGui)
9443 ³	HTTPS (OIP on SMBC)	TCP	open	←	Node ← PC (OIP WebGui)
15374	SX200 Hotel Management	TCP	closed	←	Master/Standalone ← PMS
18060	IP-Phone Signaling	TCP, UDP	open	←	Node ← MiVoice 5300 IP, MiVoice 2380
18061	Secure IP-Phone Signaling	TCP	closed	←	Node ← MiVoice 5300 IP
19790	AIN Link Handler Control	TCP	open	↔	Master ↔ Satellite
33555	SX200 Call Data Records	TCP	closed	←	Master/Standalone ← Call accounting application
40000 - 40059 ¹⁴	RTP on Standard Media Switch or UDPTL (Fax T.38)	UDP	closed	↔	Node ↔ Node Node ↔ Mitel IP-Term. Node ↔ SIP Phone/Trunk
40000 – 40499 ¹⁴	RTP on Media Server	UDP	closed	↔	Node ↔ Node Node ↔ Mitel IP-Term. Node ↔ SIP Phone/Trunk
59901 -60000 ² 37001-65535 ⁴ 32768 - 60999 ³	Link Handler	TCP	closed	↔	Master ↔ Satellite
64950 - 64999	NAT for PPP access	TCP	closed	↔	Node → Node
	MONITORS				
1818	Maintenance Monitor	TCP	closed	←	Node ← PC
2323	System shell	TCP	open	←	Node ← PC

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, 1065-1067, 1071, 1072, 1075-1078, 1081, 1083, 1085-1087, 1091, 1092, 1094, 1097-1101, 1103-1106, 1108-1111, 1113, 1117-1118, 1120-1123, 1126-1129, 1133, 1134, and 1720

Index legend:

- 1 Configurable via MiVoice Office 400 configuration tool (WebAdmin)
- 2 Applies only for MiVoice Office 470
- 3 Applies only for MiVoice Office 400 SMBC
- 4 Applies only for MiVoice Office 400 Virtual Appliance
- 5 Redirected to port 443 by default

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), a standards-based protocol that uses the 128-bit Advanced Encryption Standard (AES) as described by RFC 3711.

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 endpoints, SRTP is chosen. For more information, see 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 1.3 is used to encrypt the signaling path between multiple MiVoice Office 400 systems. For details, see 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 is 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 administrator 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. Several 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, and a list of Mitel phones that include a micro-firewall, refer to the *Mitel IP Sets Engineering Guidelines* (<https://www.mitel.com/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/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 (MiSDLC) 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 7.2 was developed in accordance with Mitel's Secure Development Life Cycle policy. As a result, MiVoice Office 400 Release 7.2 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 maintenance monitor port: The default setting is "No"
- Open all server/monitor ports: The default setting is "No"
- Open application ports: The default setting is "Yes"
- FTP service – The default setting is "FTP off"
- 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"
- Password expiration period (days) for WebAdmin – the default setting is "0 = off"

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 as follows:

- DoS protection – Suspicious IP addresses are blocked for the specified 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 administrator review all these options and set the controls as appropriate for their particular network.
- that the administrator enable 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) – 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 anti-virus 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 the 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/document-center/technology/mitel-standard-linux/all-releases/en/mitel-standard-linux-security-technical-paper-v14>).

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.