A MITEL
PRODUCT
GUIDE

# MiVoice Office 400

## System Manual for Virtual Appliance

Release 7.0
July 2023

Mitel
Powering connections

# Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks™ Corporation (MITEL®).**The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

# Trademarks

The trademarks, service marks, logos and graphics (collectively “Trademarks”) appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website:http://www.mitel.com/trademarks.

# Contents

# Product and Safety Information 1

This chapter contains the following sections:



Here you will find information relating to safety, data protection and legal matters besides product and documentation information.

Please read through the product and safety information carefully.

## 1.1 About MiVoice Office 400

**Purpose and function**

MiVoice Office 400 is an open, modular and comprehensive communication solution for the business sector with several communication servers of different performance and expansion capacity, an extensive telephone portfolio and a multitude of expansions. They include an application server for unified communications and multimedia services, an FMC controller for mobile phone integration, an open interface for application developers, and a multitude of expansion cards and modules.

The business communication solution with all its components was developed to cover in full the communication requirements of businesses and organisations, in a way that is both user and maintenance-friendly. The individual products and components are coordinated and must not be used for other purposes or replaced by third-party products or components (unless it is to connect other approved networks, applications and terminals to the interfaces certified specially for that purpose).

**User groups**

The design of the phones, softphones and PC applications of the MiVoice Office 400 communication solution is particularly user-friendly, which means they can be operated by all end users without specific product training.

The phones and PC applications for professional applications, such as the operator console or call centre applications require training of the personnel.

Specialist knowledge of IT and telephony is assumed for the planning, installation, configuration, commissioning and maintenance. Regular attendance at product training courses is strongly recommended.

**User information**

MiVoice Office 400 products are supplied with the necessary safety/legal information and user documents. All user documents such as user guides and system manuals are available for download from the MiVoice

Office 400 document portal as individual documents or as documentation sets. Some user documents are accessible only via a partner login.

It is your responsibility as a specialist retailer to keep up to date with the scope of functions, the proper use and the operation of the MiVoice Office 400 communication solution and to inform and instruct your customers about all the user-related aspects of the installed system:

- Please make sure you have all the user documents required to install, configure and commission a MiVoice Office 400 communication system and to operate it efficiently and correctly.
- Make sure that the versions of the user documents comply with the software level of the MiVoice Office 400 products used and that you have the latest editions.
- Always read the user documents first before you install, configure and put a MiVoice Office 400 communication system into operation.
- Ensure that all end users have access to the user guides.

Download the MiVoice Office 400 documents from the Document Center

## 1.2 Safety Information

**Reference to hazards**

Hazard warnings are affixed whenever there is a risk that improper handling may put people at risk or cause damage to the MiVoice Office 400 product. Please take note of these warnings and follow them at all times. Please also take note in particular of hazard warnings contained in the user information.

**Warning**:

Warning indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.

**CAUTION**:

Caution indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury and/or damage to the equipment or property.

These symbols may appear on the product:

| | |
|---|---|
|  | The lightning flash with arrowhead symbol, within an equilateral triangle, is intended to alert the user to the presence of uninsulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock. |
|  | The exclamation point within an equilateral triangle is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the product |
|  | Indicates ESD components. Failure to observe information identified in this way can lead to damage caused by electrostatic discharge. |
|  | The ground symbol within a circle identifies the product to be connected to an external conductor. Connect this product to earth ground before you make any other connections to the equipment. |

**Operating safety**

MiVoice Office 400 communication servers are operated on 115/230 VAC mains power. Communication servers and all their components (e.g. telephones) will not operate when mains power fails. Interruptions in the power supply will cause the entire system to restart. A UPS system has to be connected up-circuit to ensure an uninterruptible power source.

When the communication server is started for the first time, all the configuration data is reset. You are advised to backup your configuration data on a regular basis as well as before and after any changes.

**Installation and operating instructions**

Before you begin with the installation of the MiVoice Office 400 communication server:

- Check that the delivery is complete and undamaged. Notify your supplier immediately of any defects; do not install or put into operation any components that may be defective.
- Check that you have all the relevant user documents at your disposal.
- Configure this product with only the assemblies specified and in the locations stated in the user documentation.
- During the installation follow the installation instructions for your MiVoice Office 400 product in the sequence that is given and observe to the safety warnings they contain.

**CAUTION**:

Failure to follow all instructions may result in improper equipment operation and/or risk of electrical shock.

- Install all wiring according to local, state, and federal electrical code requirements.
- Do not connect telecommunications cabling to the system, service the system, or operate the system with the grounding conductor disconnected.
- Ensure the AC receptacle is installed near the equipment and easily accessible.
- Use only Mitel approved power adapters.

Any servicing, expansion or repair work is to be carried out only by trained technical personnel with the appropriate qualifications.

## 1.3 Data protection

**Protection of user data**

During operation the communication system records and stores user data (e.g. call data, contacts, voice messages, etc.). Protect this data from unauthorised access by using restrictive access control:

- For remote management use SRM (Secure IP Remote Management) or set up the IP network in such a way that from the outside only authorised persons have access to the IP addresses of the MiVoice Office 400 products.
- Restrict the number of user accounts to the minimum necessary and assign to the user accounts only those authorisation profiles that are actually required.
- Instruct system assistants to open the remote maintenance access to the communication server only for the amount of time needed for access.
- Instruct users with access rights to change their passwords on a regular basis and keep them under lock and key.

**Protection against listening in and recording**

The MiVoice Office 400 communication solution comprises features which allow calls to be monitored or recorded without the call parties noticing. Inform your customers that these features can only be used in compliance with national data protection provisions.

Unencrypted phone calls made on the IP network can be recorded and played back by anyone with the right resources:

- Use encrypted voice transmission (Secure VoIP) whenever possible.
- For WAN links used for transmitting calls from IP or SIP phones, use as a matter of preference either the customer's own dedicated leased lines or with VPN encrypted connection paths.

## 1.4 About this document

This document contains information on the expansion stages, system capacity, installation, configuration, running and maintenance as well as the technical data of the MiVoice Office 400 communication servers. The system functions and features, the DECT planning and the possibilities for networking several systems into a private network (PISN) or a Mitel Advanced Intelligent Network (AIN) are not part of this Manual; they are described in separate documents.

**Note**:

In this document, it is presumed, that the Mitel SMB Controller is loaded with a MiVoice Office 400 application software. This assumption is always valid, even the expression Mitel SMB Controller, SMBC or communication server is used.

MiVoice Office 400 Virtual Appliance is a software-based, hardware-independent communication server. It is also Mitel Standard Linux (MSL) based, and runs on a virtual machine (VMware®). The expansion possibilities for the Virtual Appliance communication server include an FMC Controller for integrating mobile/external phones and an open interface for application developers.

The document is intended for planners, installers and system managers of phone equipment. Basic knowledge of phones, especially ISDN and IP technology, is required to understand the content.

The system manual is available in Acrobat Reader format and can be printed out if necessary. Navigation in PDF format is based on the bookmarks, table of contents, cross references and index. All these navigation aids are linked, i.e. a mouse click takes you directly to the corresponding places in the Manual. We have also ensured that the page numbering in the PDF navigation corresponds to the page numbering of the Manual, making it much easier to jump to a particular page.

Referenced menu entries and parameters appearing on terminal displays or on the user interfaces of the configuration tools are *highlighted* in italics and in colour for a clearer orientation.

**General Considerations**

Special symbols for additional information and document references.

**Note**:

Failure to observe information identified in this way can lead to equipment faults or malfunctions or affect the performance of the system.

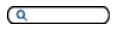
**See also**

Reference to other chapters within the document or to other documents.

**Mitel Advanced Intelligent Network**

Particularities that have to be observed in an AIN.

**References to the MiVoice Office 400 configuration tool WebAdmin**

If an equals sign is entered in the WebAdmin search window  , the view assigned to the code is directly displayed.

Example: *Licence overview* view

The corresponding navigation code is available on the help page of a view.

# System Overview 2

This chapter contains the following sections:



This chapter provides a brief overview of the Virtual Appliance communication server with its positioning within the MiVoice Office 400 series and the networking possibilities. It also features the system phones, the applications and the application interfaces. If you are setting up an communication system for the first time, it may be useful to set up a test system step by step on site. At the end of the chapter you find a useful getting started guide for this purpose.

## 2.1 Introduction

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 four systems with different expansion capacities. The systems can be expanded using cards, modules and licenses, and adapted to the specific requirements of companies.

The 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 even be extended to the smallest branch offices at low cost.

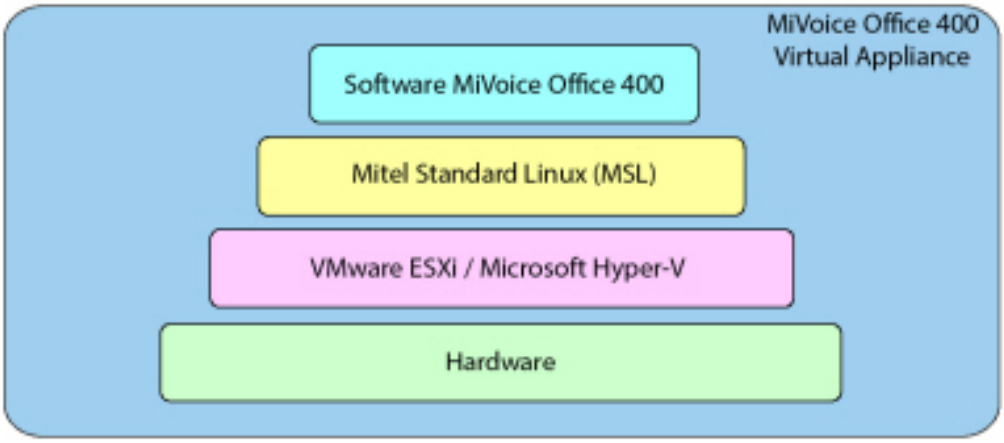
MiVoice Office 400 communication systems handle “Voice over IP” technology with all its benefits. What’s more, the systems operate just as easily with traditional digital or analogue phones and public networks.

With the integrated Media Gateways any hybrid forms of an IP-based and digital or analogue communication environment are also possible. This enables customers to make the switch from traditional telephony to IP-based multimedia communication either in just one step or, gradually, in several stages.

## 2.2 Communication server

MiVoice Office 400 Virtual Appliance is a software-based, hardware-independent communication server. It is also Mitel Standard Linux (MSL) based, and runs on a virtual machine ESXi (VMware)™ or Hyper-V (Microsoft).

Figure 1: MiVoice Office 400 Virtual Appliance




The integrated Mitel Media Server is responsible for switching the IP media channels. Analogue and digital interfaces are available via a networked, hardware-based Mitel 415, Mitel 430, Mitel SMBC or Mitel 470 satellite.

### 2.2.1 Positioning

Applications range from small businesses and branches to large companies at one or more locations. Up to 1200 users can be operated on the Virtual Appliance communication server (an approval by the Mitel Sales Engineering Team is required for configurations of more than 400 users). One licence is required for each user.

## 2.3 Networking Possibilities

MiVoice Office 400 communication servers at different company locations, even beyond national borders, can be linked together to form an enterprise-wide private communication network with a common numbering plan. The following networking types are possible:

**Mitel Advanced Intelligent Network (AIN)**

In an AIN several communication servers of the MiVoice Office 400 series can be connected up to form a homogeneous communication system. The single systems are connected with one another via the IP network, thereby forming the nodes of the overall AIN system One node acts as the Master and controls the other (satellite) nodes. All the features are then available at all the nodes.

No call charges are incurred as the internal voice traffic between locations is routed via the system's own data network. All the AIN nodes are configured and set up centrally via the Master.

If a node is isolated from the rest of the AIN by an interruption in the IP connection, it restarts with an emergency configuration after a set amount of time. The connections are then routed to the public network via local links, for example with ISDN or SIP connections, until contact with the AIN is restored.

For the Virtual Appliance communication server, AIN networking (Virtual Appliance as master) with at least one satellite is mandatory.

**SIP networking**

Networking based on the open global SIP protocol is the universal way of connecting several systems with one another via the private data network or the internet. MiVoice Office 400 communication platforms can be used to network up to 100 other Mitel systems or SIP-compatible third-party systems. All the main telephony features such as call number and name display, enquiry call, hold, brokering, call transfer and conference circuits are supported. The transmission of DTMF signals and the T.38 protocol for Fax over IP between the nodes is also possible.

## 2.4 Mitel system phones and clients

Mitel system phones stand out by virtue of their high level of user convenience and their attractive design. The broad range of products ensures there is a suitable model for every use.

**Table 1: Mitel system phones and clients**

| Product | Principal common features | Additional model-specific features |
|---|---|---|
|  <br>Mitel One (listed as Mitel One in the app store) | • Features of a desk phone include make and receive calls, blind call transfer, hold and make another call.<br>• Do Not Disturb (DND)<br>• Secure personal 1:1 and group chat<br>• Live status (presence) of users and extensions<br>• Dynamic call history<br>• Contact synchronization and management (business and personal).<br>• Simple admin controls. | |

**Table 2: Mitel 6900 SIP series SIP phones**

| Product | Principal common features | Additional model-specific features |
|---|---|---|
|  Mitel 6905 SIP Phone | • Connection for wall mounting<br>• Excellent voice quality due to Mitel Hi-Q™ wideband audio technology<br>• Data/voice encryption<br>• HD handset and speakerphone provide wideband audio quality | • Dual Ethernet ports, three programmable Personal Keys and a large 2.75" LCD display<br>• HD handset and speakerphone provide wideband audio quality<br>• Dual 10/100 Ethernet ports for PC and LAN |
|  Mitel 6910 SIP Phone | | • Dual Gigabit Ethernet ports for PC and LAN<br>• DHSG/EHS headset support<br>• Large 3.4" 128x48 pixel LCD display |

| Product | Principal common features | Additional model-specific features |
|---|---|---|
|  Mitel 6920 SIP Phone<br>  Mitel 6930 SIP Phone<br>  Mitel 6940 SIP Phone | • User-friendly registration, configuration and operation of system features through MiVoice Office 400 integration.<br>• XML browser compatible<br>• Automatic update of the terminal software<br>• Web-user interface<br>• Integrated 1 Gbit Ethernet switch for connecting a PC<br>• Hearing Aid Compatible (HAC) handset<br>• Headset port convertible to DHSG/EHS capable headset port<br>• Excellent voice quality due to Mitel Hi-Q™ wideband audio technology<br>• Full-duplex hands-free operation (speakerphone)<br>• Backlit display<br>• Up to 3 expansion key modules can be connected | Mitel 6920 SIP:<br>• Corded speech optimized handset<br>• MobileLink mobile device integration through optional USB Bluetooth Dongle<br>• Magnetic keyboard connector<br>• USB port 2.0 (100 mA)<br>• Can be used as auxiliary reception phone (reduced functionality) in hospitality environments<br><br>Mitel 6930 SIP:<br>• Corded speech optimized handset<br>• Support for optional cordless speech optimized handset<br>• Magnetic keyboard connector<br>• Can be used as auxiliary reception phone (reduced functionality) in hospitality environments |

| Product | Principal common features | Additional model-specific features |
|---|---|---|
| | • Wall mounting possible<br>• Power over Ethernet | Mitel 6930 SIP and Mitel 6940 SIP:<br>• Cordless speech optimized handset<br>• Mobile phone charging point<br>• MobileLink mobile device integration<br>• Bluetooth 4.1 interface<br>• USB port 2.0 (500 mA)<br>• Can be used as operator console<br>• Mitel 6940 SIP<br>• LCD touch display<br>• Can be used as reception phone in hospitality environments<br>General:<br>• Additional model-specific features include the resolution, the display type and size, and the number of configurable or fixed function keys. |
|  | | • LCD touch display<br>• Meeting centre enables access to the MiCollab Audio, Web, and Video conferencing |

**Table 3: Mitel 6800 SIP series SIP phones**

| Product | Principal common features | Additional model-specific features |
|---|---|---|
|  Mitel 6863 SIP Phone<br>  Mitel 6865 SIP Phone<br>  Mitel 6867 SIP Phone<br>  Mitel 6869 SIP Phone<br>  Mitel 6873 SIP Phone | • User-friendly registration, configuration and operation of system features through MiVoice Office 400 integration.<br>• XML browser compatible<br>• Automatic update of the terminal software<br>• Web-user interface<br>• Excellent voice quality due to Mitel Hi-Q™ wideband audio technology<br>• Full-duplex hands-free operation (speakerphone)<br>• Several configurable line keys<br>• Three-party conference possible locally on the phone<br>• Wall mounting possible<br>• Power over Ethernet | Mitel 6863 SIP:<br>• Integrated 10/100 Mbit Ethernet switch for connecting a PC<br><br>Mitel 6865 SIP, Mitel 6867 SIP, Mitel 6869 SIP and Mitel 6873 SIP:<br>• Integrated 1 Gbit Ethernet switch for connecting a PC<br>• Backlit display<br>• Expansion key modules can be connected<br>• Headset socket (DHSG standard)<br><br>Mitel 6867 SIP and Mitel 6869 SIP:<br>• Magnetic keyboard connector<br>• Can be used as auxiliary reception phone (reduced functionality) in hospitality environments |

| Product | Principal common features | Additional model-specific features |
|---|---|---|
| | | Mitel 6867 SIP, Mitel 6869 SIP and Mitel 6873 SIP:<br>• USB Interface<br>• Replaceable keyboard covers<br><br>Mitel 6869 SIP and Mitel 6873 SIP:<br>• Can be used as operator console<br><br>Mitel 6873 SIP:<br>• Bluetooth interface<br>• Can be used as reception phone in hospitality environments<br>• LCD touch display<br><br>General:<br>• Additional model-specific features include the resolution, the display type and size, and the number of configurable or fixed function keys. |
| The phones of the Mitel 6700 SIP series (Mitel 6730 SIP, Mitel 6731 SIP, Mitel 6735 SIP , Mitel 6737 SIP , Mitel 6739 SIP, Mitel 6753 SIP, Mitel 6755 SIP and Mitel 6757 SIP) are supported as before (not all system features can b e used). | | |

**Table 4: IP system phones (softphones) and clients**

| Product | Main features |
|---|---|
|  MiVoice 2380 Softphone | • Autonomous and powerful, IP-based PC system phone with intuitive user interface<br>• Can be used with headset or handset via PC audio interface, USB or Bluetooth<br>• Graphical user interface with mouse and keyboard operation<br>• Displayable expansion keypad for team keys, functions and phone numbers<br>• Displayable keypad<br>• Ring tones expandable using *.mp3, .mid and .wav* files<br>• Call contacts directly from Outlook<br>• All the system features can be used |
|  MiVoice 1560 PC Operator | • OIP client application for a professional PC operator console<br>• Can be used purely as an IP softphone (MiVoice 1560) or together with a system phone (MiVoice 1560)<br>• Graphical user interface with mouse and keyboard operation<br>• Can be used in an AIN as a network-wide PC operator console<br>• Call management with internal and external queues<br>• Presence indicator, presence profiles, phone book and journal<br>• Operator groups and agent control<br>• Line keys and calendar functions<br>• Possibility of synchronisation with a Microsoft Exchange server<br>• All the system features can be used |

| Product | Main features |
|---|---|
|  Mitel Office Suite | • OIP client application for PC-based call management<br>• Used in conjunction with a system phone<br>• Graphical user interface with mouse and keyboard operation<br>• Configuration of the coupled system phone<br>• Call manager with extensive functions and options<br>• Presence indicator of other users<br>• Configurable presence profiles<br>• Phone book with address books and personal contacts<br>• Journal with call lists, text messages and notes<br>• Workgroups (agent control)<br>• Possibility of synchronisation with a Microsoft Exchange server<br>• Possibility of displaying various additional windows<br>• All the system features can be used |

**Table 5: Digital system phones of the MiVoice 5300 family**

| Product | Principal common features | Additional model-specific features |
|---|---|---|
|  MiVoice 5361 Digital Phone<br>  MiVoice 5370 Digital Phone<br>  MiVoice 5380 Digital Phone | • Intuitive and user-friendly menu prompting with Foxkey and central navigation key<br>• All the system features can be used<br>• Automatic update of the phone software<br>• Connection via DSI interface<br>• Two phones can be connected per DSI interface<br>• Powered via DSI bus or power supply<br>• Wall mounting possible | MiVoice 5370/MiVoice 5380:<br>• Expansion key modules can be connected<br>• Headset socket with DHSG standard<br>MiVoice 5380:<br>• Backlit display<br>• Optional Bluetooth module<br>• Can be used as operator console when combined with expansion key module |

**Table 6: Cordless system phones of the Mitel 600 DECT family**

| Product | Principal common features | Additional model-specific features |
|---|---|---|
|  Mitel 612 DECT Phone  Mitel 622 DECT Phone  Mitel 632 DECT Phone  Mitel 650 DECT Phone | • Intuitive and user-friendly menu prompting with Foxkey and central navigation key<br>• Colour display<br>• All the system features can be used<br>• Automatic update of the phone software<br>• Backlit display and keyboard<br>• Headset socket<br>• Automatic handover and roaming<br>• Can be operated on both the DSI radio units SB-4+, SB-8, SB-8ANT and the SIP-DECT® radio units RFP L32 IP, RFP L34 IP and RFP L42 WLAN | Mitel 622 DECT/Mitel 632 DECT/ Mitel 650 DECT:<br>• 3 configurable side keys<br>• Vibra call<br>• Bluetooth interface<br>• USB Interface<br>• micro-SD card interface<br>• Power battery (optional)<br>Mitel 632 DECT:<br>• Complies with industry standard (IP65)<br>• With emergency button and sensor alarms, suitable for personal protection<br>Mitel 650 DECT:<br>• Supports the DECT standard CAT-iq (Cordless Advanced Technology – internet and quality) for high-quality broadband telephony (can be used with Mitel SIP-DECT only). |
| The Mitel 610 DECT, Mitel 620 DECT, Mitel 630 DECT, Office 135/135pro and Office 160pro/Safeguard/ATEX c ordless system phones are supported as before (not all system features can be used). | | |

**Table 7: Analogue Mitel phones**

| Product | Principal common features | Additional model-specific features |
|---|---|---|
|  Mitel 6710 Analogue Phone<br>  Mitel 6730 Analogue Phone | • Destination dialling keys<br>• Frequency dialling or pulse dialling<br>• Handsfree<br>• Adjustable volume (handset and loudspeaker)<br>• System features can be used via function codes<br>• Headset connection<br>• Wall mounting possible<br>• Functions controllable via communication server: Message display on/off, delete redial key memory.<br>• Ideally suited for hospitality and hotel environments | Mitel 6730 Analogue:<br>• Three-line display<br>• 100 phone book contacts<br>• 50 entries each on call list and redial list<br>• Number/name display for incoming calls<br>• Clock with wake-up function<br>• Functions controllable via communication server: Delete call lists and local phone book, set date, time and language. |
| The Aastra 1910 and Aastra 1930 analogue phones are still supported. | | |

## 2.5 Various phones, terminals and equipment

Thanks to the use of international standards other clients, terminals and phones, Mitel and third-party, can be connected and operated on the communication server:

- SIP-based phones

  With the integrated SIP protocol SIP-based phones (softphones, hardphones) - or via an SIP access point also WLAN and DECT phones - can be connected to the communication server. Besides the basic telephony functions, features such as call transfer, conference calls or CLIP/CLIR are also supported. Function codes can also be used to operate various system functions.
- Cordless phones

  Other DECT phones can be operated in GAP mode.
- Analogue terminals

  All terminals (phones, fax, modem, etc.) approved by the network operator can be connected on the analogue terminal interfaces. The communication system supports pulse and frequency dialling modes.
- ISDN terminals

  ISDN terminals that comply with the Euro ISDN standard can be connected to the BRI-S terminal interfaces. The communication system provides a series of ISDN features at the S bus.

- Mobile/external phones

  Mobile/external phones can also be integrated into the communication system. They can then be reached under an internal call number, and their status is monitored and displayed. Internal/external calls can be made via the integrated mobile/external phone; system functions can also be executed using function codes.

## 2.6 Solutions

- Alarming and Health care

  Thanks to the components Mitel Alarm Server, I/O-Gateway and the OpenCount application, flexible solutions are available for hospitals and old people's nursing homes. MiVoice Office 400 communication-server-integrated functions such as “Direct response” “Hotline alarm” or “PIN telephony” allow easy deployment of available features.
- Hospitality/Hotel

  The hospitality software package provides functions to implement a user-friendly accommodation and hotel solution in the range of 4 to 600 rooms. This solution is also ideally suited for the management of care homes and retirement homes. The functions are operated using the Mitel 6940 SIP, Mitel 6873 SIP, MiVoice 5380 reception phone or the web-based Mitel 400 Hospitality Manager application. Reduced hospitality functionality are also available on Mitel 6920 SIP, Mitel 6930 SIP, Mitel 6867 SIP and Mitel 6869 SIP phones. Connection to a Property Management System (PMS) via the communication server's Ethernet interface is also possible. The commercially available FIAS protocol is provided for this purpose.
- Mobility/Cloud application

  Mobility/Cloud solutions, especially Mitel One, enable employees to log on to the company network using their mobile phones/PC.

  Moreover, with Mitel SIP-DECT and Mitel 600 DECT series phones comprehensive solutions can be provided for wireless telephony on IP-based networks. In so doing, RFP radio units are directly connected to the LAN like a VoIP device.

## 2.7 Applications and application interfaces

A distinction is made among applications between Mitel-specific applications and certified applications supplied by third parties.

The Mitel application Mitel Open Interfaces Platform (OIP), as well as the certified third-party applications, are installed on a customer server. They communicate with the communication server via standardised interfaces (see Application interfaces).

Auxiliary applications for planning and the configuration and park management are available as a web application.

## 2.7.1 Mitel Applications

**Table 8: Mitel applications**

| Application | Main features |
|---|---|
| Mitel Dialer | • Simple first party CTI application<br>• Dial, answer, hang up<br>• Integration in Outlook, Lync 2013 and Office 365<br>• Search in directories<br>• Compatibility with MiVoice 5300, MiVoice 5300 IP, Mitel 6800/6900 SIP, Mitel 600 DECT series phones<br>• Installation via SSP or WebAdmin<br>• Click to call support (e.g. for Hospitality Manager) |
| Mitel Open Interfaces Platform (OIP) | • Application interface for deep integration of applications by Mitel or other manufacturers (see Application interfaces)<br>• Easy to manage through an integrated web-based application<br>• Integrates the MiVoice 1560 PC Operator and Mitel OfficeSuite applications<br>• Presence-controlled communication coupled with Outlook diary entries<br>• Integration of contact databases and directories (Outlook, Exchange, Active Directory, LDAP directories, phone book CD)<br>• Integration of building automation equipment and alarm systems<br>• Call centre functions with flexible routing algorithms, skill-based agent groups and emergency routing<br>• Unified messaging with notification whenever new voice messages are received via email (incl. message attachment)<br>• Partner program for integrating and certifying applications by other manufacturers<br>• Also available as OIP Virtual Appliance, for installation on a VMware server or HyperV. |

| Application | Main features |
|---|---|
| Mitel MiCollab | Comprehensive Unified Communications and Collaboration solution:<br>• Central software provided for industry standard servers or virtual environments<br>• Integration of Microsoft® Outlook®, IBM® Lotus Notes® Google®, Microsoft® Lync® etc.<br><br>UC clients for desktop, web and mobile applications:<br>• Comprehensive real-time presence information<br>• Dynamic call distribution<br>• Real collaboration with joint use of the desktop and documents<br>• Easy retrieval of voice messages<br>• Secure instant messaging (IM) and data transmission<br>• Audio, web and video conferences |
| Mitel 400 CCS | • Mitel 400 CCS is an additional application for the Mitel 400 Call Center, and provides statistics / reporting functions and agent monitoring (CCS = call centre supervision). The licensing of the application is made via OIP. |
| Mitel OpenCount | • MitelOpenCount is a software package used for the call logging management on the communication system. It consists for selected sectors of basic, comfort and premium solutions and is installed on an external server. |

| Application | Main features |
|---|---|
| Mitel BusinessCTI | • Powerful Unified Communications solution<br>• Presence management with calendar integration<br>• Instant Messaging (chat), video, SMS and e-mail functions<br>• Compatibility with the federation between Mitel Business CTI servers and/or Microsoft Lync and OCS<br>• Easy integration into CRM and ERP systems<br>• Compatible with other call managers<br>• Clients for PC (Windows, Mac) and mobile phones/tablets (Android/IOS) available<br>• Optional additional modules Mitel BusinessCTI Analytics |
| MiContact Center Business | • Contact Center on a location with up to 80 agents<br>• Progress reports<br>• Real-time monitoring<br>• Dynamic agents and wait loop control<br>• Screen pop<br>• Intelligent Messaging<br>• Multimedia compatibility |
| Mitel Border Gateway (MBG) | • Highly scalable solution which offers mobile and external workers secure and seamless access to the company's voice and data applications, regardless of their location. How to deploy such a solution refer to the document “Mitel SIP Teleworker via MBG on MiVoice Office 400”. |

| Application | Main features |
|---|---|
| Mitel Alarm Server | • Specially designed for use in hospitals and nursing homes, industries and businesses as well as public domains.<br>• Mitel Alarm Server monitors processes, activates the required services, sets off alarms based on predefined samples or notifies selected recipients via paging, e-mail, SMS or voice message.<br>• The alarm can be set off via a nurse call or fire-alarm system (ESPA interface), via a key predefined on the Mitel DECT or system phone, an alert button, web client, or by calling the alarm server (audio guide), or via e-mail (subject line analysis). |
| Mitel CloudLink Integration | Mitel CloudLink Integration is a solution that enables the communication server to connect to the CloudLink platform using CloudLink gateway that connects Mitel One. |
| | |

**Table 9: Planning and configuration applications**

| Application | Main features |
|---|---|
| Mitel CPQ | • Web-based planning application for Mitel communication platforms (CPQ = Configuring Planning Quoting)<br>• Uses project data to calculate the necessary communication server complete with terminals, interface cards, modules and licences<br>• Country-specific adaptations possible for accessories<br>• Stored price lists and configurable quote compilation<br>• No installation necessary |

| Application | Main features |
|---|---|
| WebAdmin | • Web-based configuration tool for configuring and monitoring a single system or an entire network (AIN)<br>• Access control with user accounts and predefined authorization profiles<br>• Special accesses for hospitality solutions<br>• Integrated online help and configuration assistant<br>• Integrated in the communication server software package |
| Mitel 400 Hospitality Manager | • Integrated web-based application used to operate functions in the hospitality sector<br>• List view and floor-by-floor view of the rooms<br>• Functions such as check-in, check-out, group check-in, notification, wake-up call, retrieval of call charges, maintenance list, etc. |
| Self Service Portal SSP) | Web-based application for end-users, which allows personalised configuration of a telephone:<br>• Functions key assignment and printing of labels<br>• Setting the idle text and language<br>• Setting the presence profiles, personal call routing, voice mail, forwarding, etc.<br>• Setting up dial-in conference rooms<br>• Creating private phone book contacts<br>• Managing personal data such as e-mail address, password, PIN, etc. |
| Secure IP Remote Management (SRM) | • Server-based solution for secure IP remote management<br>• No router and firewall configuration or VPN connection setup required<br>• Allows configuration via WebAdmin once the connection has been set up<br>• No installation necessary |

## 2.7.2 Application interfaces

The most important interface for own and third-party applications is the interface of the Mitel Open Interfaces Platform (OIP). This open interface allows the applications to be deeply integrated with

telephony. Third-party applications can also be integrated on MiVoice Office 400 series systems via different interfaces without OIP.

### 2.7.2.1 Mitel Open Interfaces Platform

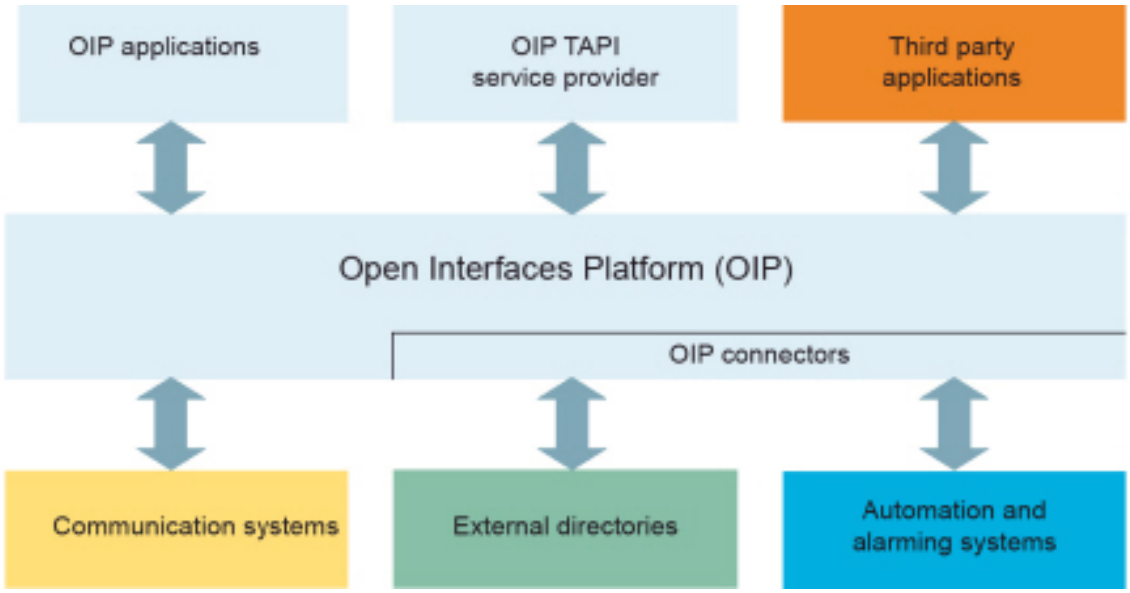



Figure 2: OIP as middleware between communications system, external data sources and applications

**OIP services**

The OIP services are the central components of OIP. They are used to control the system and make the OIP features and interfaces available. Thanks to the modular organisation and vast configuration possibilities, versatile and customer-specific solutions can be set up.

**OIP applications**

Sophisticated Softphones are available as OIP applications and are controlled as clients via OIP.

- Mitel OfficeSuite is a rich-client application, which significantly broadens the range of functions of the coupled fixed and cordless phones.
- MiVoice 1560 PC Operator is an operator application which can be used as rich-client application together with a fixed or cordless phone or alone as Softphone.

Possible OIP application fields are listed in the following sections:

**OIP as directory server**

Already available directories, databases and phone books are linked to OIP and made useful for name dialling and identification.

Integration is compatible with many standard databases such as Microsoft Exchange, Microsoft Outlook, Microsoft Active Directory, communication server directories, LDAP and ODBC directories and electronic phone books.

Moreover, Microsoft Exchange directories can be directly synchronised.

**Unified Communications - OIP as telephony server**

When OIP is used as telephony server, telephony integrates in a scalable manner into IT communication: Top-class Softphones, PC-operated fixed and cordless phones, presence-controlled call, voice mail control and calendar coupling via presence profiles, name dialling and call number identification via all linked company directories, synchronisation of Microsoft Exchange contacts, e-mail notifications, etc. facilitate daily communication.

**OIP as operator centre**

Several multi-functional operator applications can be organised with call centre functions in operator groups.

**OIP as call center**

The powerful Mitel 400 Call Center is an integral part of OIP and provides all the main features such as flexible routing algorithms (cyclical, linear, longest time available, CLIP-based, last agent), skill-based agent groups as well as an analysis of the call centre data (online and offline) with chart-based evaluation. In the event of a network interruption the emergency routing ensures the maximum availability of the system.

The agent functionality is available on all system phones including Softphones. This applies equally to home workstations and to all the users on a Mitel Advanced Intelligent Network. The one number user concept can also be set up for agents, which provides the staff of a Call Center with maximum mobility within the company.

The Mitel 400 Call Center is easy to manage and configure thanks to OIP WebAdmin. Various monitoring functions, simple statistical evaluations and work group control can be comfortably implemented using the administration interface.

Mitel 400 CCS is an extension of the Mitel 400 Call Center and offers several possibilities of statistically evaluating the call centre operation. Offline and online reports enable the call center operator to analyse and optimise call centre operations.

**OIP as application interface**

Certified third-party manufacturers can, for instance, integrate sector-specific applications into the MiVoice Office 400 communication environment.

**OIP as automaton and alarm system**

External alarm systems and building automation equipment (e.g. KNX) are easily monitored through the connection to the communication system. This allows information to be exchanged in a simple way between the systems. In this way the user can use his system phone for voice communications and for monitoring external systems.

The I/O service offers a wide range of features which allows very flexible uses and versatile applications. Some of its examples are listed below:

- Alarming equipment for maintenance personnel

- Monitoring of production processes
- Forwarding messages as e-mails
- Connection to building automation systems (KNX)

With the graphical interface (tree structure) events and the relevant actions are easily linked with one another.

**OIP in a networked environment**

An OIP server can also be used in an AIN. To do so, it will be linked to the Master. In addition, several communication systems can also be connected to an OIP server. It is then possible for instance to obtain network-wide call logging for all the systems, to display call charge information on the system phones or to display status in the presence indicator field of a PC operator console for all the users connected.

**See also:**

More information can be found in the Mitel Open Interfaces Platform system manual and in the OIP WebAdminOnline help.

### 2.7.2.2 Message and alarm systems

MiVoice Office 400 supports several message formats and message protocols for implementing messaging, monitoring and alarm systems.

**Internal messaging system for system phones**

The internal messaging system for system terminals allows users to exchange predefined or user-defined text messages between system phones. Text messages can also be sent to individual users or message groups.

The internal messaging system does not have an interface with which it can be addressed directly. However it can also be operated via OIP.

**External messaging, monitoring and alarm systems**

The powerful ATAS/ATASpro protocol is available via the communication server’s Ethernet interface for applications in the security and alarming sector. This protocol can be used to implement customised alarm applications. An alarm appears on the display of system phones, complete with the freely definable user functions that apply only to that alarm. In addition the duration of the tone as well as its volume and melody can be freely defined by the user for each alarm.

The Mitel Alarm Server is a flexible solution which can be used in all sectors to process and record alarms. It can be used, for instance, in old people's nursing homes and assisted-living homes, as well as in other different facilities such as hotels, industrial plants, shopping centres, schools or administrations. When used together with Mitel SIP-DECT it is even possible to dynamically determine the environment of the alarm solution using the location feature provided by the DECT system.

The cordless DECT phone Mitel 630 DECT is specially designed for applications in the security and alarming sector. Besides a special alarm button it also features a man-down alarm, a no-movement alarm and an escape alarm. Sensors inside the phone constantly check the handset’s position and motion. An

alarm is triggered if the phone remains in a virtually horizontal position or motionless for some time or if the handset is shaken violently.

### 2.7.2.3 CTI - Computer Telephony Integration

The Computer Telephony Integration (CTI) integrates telephony services in the company process. Besides conventional telephony features Mitel Open Interfaces Platform (OIP) offers many other convenient functions, which supports the employees with their daily work, for instance:

- Dialling by name for outgoing calls and CLIP display for incoming calls offers an added value by the integration of external directories and databases.
- Notification of Microsoft Outlook appointments on the system phones
- Presence-controlled communications with Busy Indicator
- Automatic Call Distribution
- Access to system configuration, what a maximum integration of different systems ensures

And of course the communication system supports also First and Third-Party CTI interfaces for commercial CTI applications based on the Microsoft TAPI 2.1 standard.

Terminal supervision/control on the communication server by third-party applications via the CSTA protocol is also supported.

#### 2.7.2.3.1 First-party CTI

A first-party CTI is the direct physical connection between a phone terminal and a telephony Client (workstation PC). Telephony functions and telephone states are controlled and monitored on the telephony Client. A first-party CTI solution is ideal for a small number of CTI workstations and is easily implemented.

MiVoice Office 400 supports First-Party CTI on all system phones via the Ethernet interface. For some applications, the First-Party TAPI Service Provider (AIF-TSP) is required. Other applications (e.g. Mitel Dialer) use the CSTA protocol.

Application example

- Dialling from a database (phone book CD, etc.)
- Caller identification (CLIP)
- Creating a call journal
- Mitel Dialer Mitel applications

#### 2.7.2.3.2 Third-party CTI

Third-party CTI is an user-friendly multi-station solution. In contrast to first-party CTI, third-party CTI controls and monitors several system phones (including cordless phones) via the central telephony server, which is connected with the communication server. In addition phones on ISDN and analogue interfaces can also be monitored. PC and phone allocation is handled by the telephony server.

The third-party CTI connection is effected via Ethernet using the Mitel Open Interfaces Platform (OIP). To this end the OIP is installed on the telephony server. Third-party connections via Ethernet with CSTA are also possible.

Application example

- Busy indicator
- Group functionality
- Networked CTI solution
- Automatic Call Distribution (ACD)

#### 2.7.2.4 ISDN interface

MiVoice Office 400 supports the ISDN protocols ETSI, DSS1 and QSIG.[1]Besides the possibility of networking various systems into a PISN (Private Integrated Services Network) via the ISDN interface, these protocols also provide various functions that can be used for connecting external applications (e.g. IVR systems, fax server, voice mail systems, unified messaging systems, DECT radio systems).

A gateway (Mitel 415, Mitel 430, Mitel SMBC, or Mitel 470) is required to use the ISDN interface.

#### 2.7.2.5 Configuration

The MiVoice Office 400 communication server is configured via the web-based WebAdmin application. Other components of the application include special accesses for hospitality and hotel solutions as well as a configuration wizard.

#### 2.7.2.6 System monitoring

The system status is monitored with event messages which can be sent to various internal or external destinations. Examples of message destinations are: system phones, events log WebAdmin), e-mail recipients, SRM servers, alarm servers (ATAS) or SNMP destination. Event messages are also accessible via the Mitel Open Interfaces Platform for application manufacturers.

#### 2.7.2.7 Call logging

The Call Logging Manager includes data acquisition for incoming traffic (ICL), outgoing traffic (OCL) and the counting of the acquired call charges according to a variety of criteria. The data can be retrieved via different interfaces and subsequently processed.

#### 2.7.2.8 Hospitality/Hotel

The MiVoice Office 400 communication servers offer you several possibilities to implement a hospitality and hotel solution, with different operation applications and interfaces. Configuration is done through WebAdmin. The Mitel 6940 SIP, Mitel 6873 SIP, MiVoice 5380 / 5380 IP reception phone or the web-based Mitel 400 Hospitality Manager application is available to operate the functions. Reduced hospitality functionality are also available on Mitel 6920 SIP, Mitel 6930 SIP, Mitel 6867 SIP and Mitel 6869 SIP phones. A connection to a Property Management System (PMS) via the communication server's Ethernet interface is also possible. The commercially available FIAS protocol is provided for this purpose.

[1] for USA and Canada on Mitel 470 other protocols are supported.

#### 2.7.2.9 Voice over IP

MiVoice Office 400 is a native VoIP solution. Apart from the possibility to operate IP system phones and SIP phones via the Ethernet interface, MiVoice Office 400 systems can also be networked over IP.

### 2.7.3 Connection options

MiVoice Office 400 Virtual Appliance is a software-based, hardware-independent communication server. It can also be operated in an AIN with one or more satellites. The Mitel 415/430, Mitel SMBC and Mitel 470 system manuals respectively contain a diagram of all interfaces with possible terminal equipment.

### 2.7.4 Getting started

If you are setting up an MiVoice Office 400 communication system for the first time, it may be useful to set up a test system step by step on site.

After working through the following chapters you can make internal calls between the different types of phones connected to the server. Furthermore you will have a perfect configuration platform to learn more about the system, its features and expansion possibilities.

#### 2.7.4.1 General requirements

You need a computer with internet access and credentials to login to Mitel MiAccess.

If you plan to address the communication server with a static IP address (recommended) you may obtain it from your IT administrator.

In order to allocate your IP and SIP phones to the communication server, DHCP service should be available in your subnet. (Your communication server has an integrated DHCP server as well, however it is switched off as per default.)

If you plan to set up a SIP trunk, you need a SIP account by a SIP provider of your choice.

You need a Windows OS computer with internet access and credentials to login to Mitel MiAccess.

MiVoice Office 400 Virtual Appliance is installed on a virtual machine of a professional server. For the minimum requirements for the virtual machine see chapter Installation.

To install the MiVoice Office 400 Virtual Appliance you need the IP address and the credentials of the virtual machine. You may obtain it from your IT administrator.

In order to allocate your IP and SIP phones to the communication server, DHCP service should be available in your subnet. (Your communication server has an integrated DHCP server as well, however it is switched off as per default.)

If you plan to set up a SIP trunk, you need a SIP account by a SIP provider of your choice.

For licensing reasons a communication server Virtual Appliance must either have a permanent internet access (to connect the Mitel licence server regularly) or must be operated as master in a Mitel Advanced

Intelligent Network (AIN) with at least one satellite. In the second case, and without a permanent internet connection, the satellite serves both as licensee (EID card), but also as gateway for analogue and digital terminals and interfaces. The satellite may be a Mitel 415, Mitel 430, a Mitel SMB Controller, or a Mitel 470. For these communication servers there are separate getting started descriptions available in the appropriate system manuals.

**Required accesses**

The URL's listed below refer to proprietary Mitel sites. You need a partner login to access them. If you do not have a Mitel partner login, ask your sales partner for more information.

**Table 10: Mitel sites you need access to:**

| SLno. | Title | |
|---|---|---|
| [1] | Document Center | https://www.mitel.com/document-center/business-phone-systems/mivoice-office-400 |
| [2] | Access to Mitel MiAccess (for *Mitel CPQ, Licences server; Services* and *Software Download Center*) | https://miaccess.mitel.com/ |

**Required tools**

- Torx screwdriver T10 and T20
- Phillips screwdriver size #1

## 2.7.4.2 Plan and order

Set up your MiVoice Office 400 project in Mitel CPQ first. As a result, you will obtain a list of needed components, a slot usage layout, a DSP configuration table and a licence overview.

Mitel CPQ is designed to support you with the different activities in the sales and ordering process. It is a web-based application for online usage. You can access the application through the Mitel MiAccess Portal [2].

## 2.7.4.3 Download documents, system software and tools

Before you start, download the documents and applications from the proprietary Mitel sites.

Proceed as follows to organize all downloads in a common folder:

1. Download the latest Virtual Appliance system software package (.exe) from [2] to the same target folder and double click the file.The system software (zip) and the release notes (pdf) will be extracted to the folder named *Mitel*.

2. The MiVoice Office 400 Virtual Appliance software and Mitel Standard Linux operating system are installed using an OVA file (for ESXi) or a VHD file (for Hyper-V). Download the latest Virtual Appliance package *(.ova or .vhd file)* from [2].

> **Note**:
>
> While the OVA file is only needed in the installation process, the VHD file represents a virtual hard disk and should be moved or downloaded directly to the final destination folder.

## 2.7.4.4 Installing MiVoice Office 400 Virtual Appliance

The MiVoice Office 400 Virtual Appliance software and Mitel Standard Linux operating system are installed using an OVA or a VHD file. A detailed installation description can be found here: Installing MiVoice Office 400 Virtual Appliance.

## 2.7.4.5 Commissioning

There are various methods of putting Virtual Appliance without or with a satellite into operation. Please follow the detailed descriptions in chapter Configuration.

## 2.7.4.6 Register and connect the phones

As you allocated phones to users in step 6 of the Setup wizard, the data instances for the phones have been automatically created. In this part of the procedure, for registering the phones, you pair the data instances with the physical phones.

> **Note**:
>
> Mitel SIP phones get their time and date from an NTP server. To ensure this, check the correct settings in *SMBC Manager* / *Configuration* / *Date and Time* .

**Register a Mitel SIP phone**

1. Go to *Terminals / Standard terminals* in WebAdmin and click the phone you want to register with the communication server.

   The automatically generated SIP credentials and registration credentials (*Registration user name* and *Registration password*) of the phone are displayed. You will need to provide the registration credentials later to register the phone.
2. Add one or more expansion key modules to the phone, if available.

3. Connect the phone to the IP network and to the power supply by using the optional power adapter. If your IP network supports PoE, no power adapter is required.
4. Restart the phone.

   The phone searches for the communication server. If more than one communication server is available, the phone lists them in the format lt;XXX–MAC address>.

5. Choose your communication server from the list, and when prompted, enter the *Registration user name* and the *Registration password*.

   The phone registers with the communication server. If a new phone software is available, the phone automatically updates and restarts.

**Connect the digital system phones MiVoice 5300**

1. Add one ore more expansion key module(s) to the phones.
2. Connect the phones to the DSI interfaces on the front panel. Connect the phones in the same order as you have set them up in the previous chapter and start with the lowest port number.
3. The phones are registered and allocated to their phone data instance in the communication server. If you keep the suggested order, the phone type matches with the configured terminal type. You can fix a terminal mismatch in the WebAdmin *terminal* view.

**Test your configuration**

Now you are able to make internal calls between the phones you connected to your communication server. Do some calling tests between the different phone types and check the audio. In the document center, you can find the user's guides to your phones.

## 2.7.4.7 Make further configurations

Congratulations, you have set up the communication server for self training purposes. Now you have a perfect configuration platform to learn more about the communication server, its features and expansion possibilities.

For further configurations, use the *WebAdmin configuration assistant* and the online help. For detailed information, see the user's guides and system manuals on Document Centre.

# Expansion Stages and System Capacity

3

This chapter contains the following sections:



This is transition session.

Since the Virtual Appliance communication server does not contain any hardware, the expansion possibilities are limited to licensed features and external equipment. The expansion of the connected satellites with interface cards and system modules is described in the Mitel 415/430, Mitel SMBC and Mitel 470 system manuals. However, the system capacity of Virtual Appliance differs from the other communication servers and is described here.

## 3.1 System capacity

The system capacity of Virtual Appliance is defined by the limits set in the software and the capacity of the integrated Mitel Media Server. The software limits can be partly expandable by licences.

### 3.1.1 Media resources

Media resources are used for complex signal processing functions. They provide functions for conference circuits, DTMF sender and receiver, compression of voice data, etc.

For Virtual Appliance, the media resources of the integrated Mitel Media Server are provided.

The Virtual Application implements DTMF transmitter and receiver functionalities exclusively as RFC4733 endpoints. Inband detection or transmission of DTMF tones is not supported within the Virtual Application.

**Functions of the integrated Mitel Media Server**

The table below gives an overview of the Mitel Media Server functions. The functions can all be of the same type or used as a mix. Some of these functions are subject to a licence.

**Table 11: Functions of the integrated Mitel Media Server**

| Max. number of simultaneous ... | Virtual Appliance |
|---|---|
| Total circuits for the functions three-party conference, six-party conference, intrusion and silent intrusion | 10 |

| Max. number of simultaneous ... | Virtual Appliance |
|---|---|
| switches in total for all audio services (voice mail, auto attendant, announcement service, music on hold, call recording, announcement with audio file, queue with announcement, conference bridge), for conferences, intrusion and silent intrusion, mobile and external phone integration as well as for each point-to-point connection (exchange to terminal, terminal to terminal). Two channels are required for DTP relay (indirect switching). | 250 [2] |
| Total number of switches for the functions Call waiting, DTMF sender and DTMF receiver | 400 |
| Dial tone receiver, busy tone receiver, call signal receiver, FSK sender and FSK receiver, CAS sender/receiver | [3] |

## 3.1.2 General system capacity

**Table 12: General system capacity**

| Max. number... | Virtual Appliance Individual systems or AIN with Virtual Appliance as Master |
|---|---|
| Nodes in a transparent network (AIN) | 50 |
| Nodes with SIP networking | 100 |
| Users[4] | 1200 (Configurations with more than 400 users must be approved by Mitel Sales Engineering Team) |
| Terminals per user[5] | 16 |

[2] For the number of switches per function (channels), see General system capacity.
[3] The resources are provided by the connected satellites.
[4] Each user requires a licence.
[5] Only 1 operator console, 1 MiVoice 2380 IP, 1 Mitel SIP-DECT, 2 DECT-cordless phones and 1 MiCollab client (3 MiCollab clients with MiCollab version 8.1) are possible for each user.

| Max. number... | Virtual Appliance Individual systems or AIN with Virtual Appliance as Master |
|---|---|
| Simultaneous connections | |
| • Without IP and without DECT (internal / external) | 250 |
| • IP – not IP (internal / external) | 250 |
| • IP – IP (internal) | 250 |
| • IP – IP via SIP access channels (external) | 240 |
| • DECT – not DECT (internal / external) | 250 |
| • DECT – DECT (internal) | 250 |
| VoIP voice channels G.711 / G.729 (Mitel Media Server)[6] | 250 / 50 |
| Audio channels, call recording | 8 per node[7] |
| Audio channels for voice mail | 16 pro node (max. 250) |
| Audio channels for voice mail and call recording, total | 16 pro node (max. 250) |
| Audio channels for auto attendant | 46 pro node (max. 250) |
| Total audio channels[8] | 46 pro node (max. 250) |
| Voice channels FoIP, T.38 (standard media switch) | on satellites only |

[6] Applies also to Secure VoIP modes
[7] For IP-IP connections maximum 8
[8] Audio channels can be used for voice mail, auto attendant, queue with announcement, call recording, announcement with audio file, or conference bridge. Announcement service and music on hold use their own resources.

| Max. number... | Virtual Appliance Individual systems or AIN with Virtual Appliance as Master |
|---|---|
| Voice channels FoIP, T.38 (IP media switch) | on satellites only |
| CAS transmitter/receiver for PRI-E1 network interfaces[9] | on satellites only |
| Configurable conference bridge | 60 |
| Active conferences | see Table 11: Functions of the integrated Mitel Media Server on page 34 |
| Trunk group | 506 |
| Trunk groups in route | 8 |
| Network interfaces per trunk group | 64 |
| Routes | 212[10] |
| B channel groups | 506 |
| SIP provider | 10 |
| SIP user account | 1200 |
| Direct dialling plans | 10 |
| Total DDI numbers[11] | 4000 |
| SmartDDI conversion rules per DDI plan | 100 |

[9] Of relevance only to certain countries such as Brazil
[10] 12 of them are masked (not configurable)
[11] In USA/Canada the abbreviation DID (Direct Inward Dial) is used instead of DDI (Direct Dialling In)

| Max. number... | Virtual Appliance Individual systems or AIN with Virtual Appliance as Master |
|---|---|
| SmartDDI conversion rules overall | 200 |
| Call distribution elements | 4000 |
| Queue with announcement | 16 |
| User groups | 99 |
| Members per trunk group "normal" | 16 |
| Members per trunk group "large" | 1200 |
| Abbreviated dialling numbers + PISN users | 4000 |
| Operator keys per phone on Mitel 6800/6900 SIP | 10[12] |
| Room keys on Mitel 6873 SIP (inclusive expansion keypad) | 200 |
| Line keys per key telephone (except Mitel 6800/6900 SIP) | 39 |
| Line keys per key telephone on Mitel 6800/6900 SIP | 2...12[13] |
| Line keys per CDE on Mitel 6800/6900 SIP | 16[14] |

[12] Only 6 on Mitel 6940 SIP Mitel 6873 SIP if phone is also used as reception phone.
[13] Depending on the phone type: Aastra 6730i/31i: 6 keys; Mitel 6735/37/39/53/55/57 SIP: 9 keys; Mitel 6863 SIP: 2 keys; Mitel 6865/67 SIP: 9 keys; Mitel 6869/73 SIP: 12 keys; Mitel 6900 SIP: 12 keys
[14] The value applies to CDE with destination KT line. With multiple destinations (User + KT or KT + UG) the value is reduced to 8.

| Max. number... | Virtual Appliance Individual systems or AIN with Virtual Appliance as Master |
|---|---|
| Total line keys on Mitel 6800/6900 SIP | see [15] |
| Switch groups | 50 |
| Positions per switch group | 3 |
| Hotline destinations | 20 |
| Emergency destinations | 50 |
| Internal emergency numbers | 10 |
| Internal emergency response teams | 50 |
| Members of internal emergency response teams | 20 |
| Public emergency numbers | 20 |
| Allocations of external call numbers to internal call numbers | 1500 |
| External digit barring | 16 |
| Internal digit barring | 16 |
| Barred list | 50 |

[15] Depending on the highest number of line keys, configured for the same line. The following pairs apply (line keys per line / total line keys): (16/48), (14/56), (12/72), (10/100), (8/160), (6/240), (4/320), (2/400).Example: The following line keys are configured on different Mitel SIP phones: 8 keys for line 1, 14 keys for line 2, 10 keys for line 3, 10 keys for line 4.

Highest number of keys per line: 14

total 56 line keys are allowed

Configured line keys: 8 + 14 + 10 + 10 = 4 -> OK

| Max. number... | Virtual Appliance Individual systems or AIN with Virtual Appliance as Master |
|---|---|
| Free list | 50 |
| Predefined text messages | 16 |
| Announcement / message groups | 50 |
| User per announcement / message group | 16 |
| Data service tables | 32 |
| User accounts for user access control | 25 |
| Authorization profiles for user accounts | 25 |
| Log entries per user account | 20 |
| First-party CTI users via LAN | 32 |
| First-party CTI users via Mitel Dialer | 1200 |
| Third-party CTI interfaces | 1 |
| Third-Party CTI interface (Basic, Standard) | 600 |
| Groups, Agents (OIP Call centre) | 150 |
| Agents (MiContact Center Business) | 80 |
| Mailboxes with Basic or Enterprise voice mail system | 1200 |
| Greetings per mailbox | 3 |

| Max. number... | Virtual Appliance Individual systems or AIN with Virtual Appliance as Master |
|---|---|
| Profiles per mailbox for auto attendant | 3 |
| Backup communication servers for Dual Homing | 50 |
| Primary communication servers for Dual Homing | 50 |
| Blacklist | 1 |
| Call number entries in the blacklist | 3000 |
| Number of CLIP based routing tables | 20 |
| Total call number entries in call distribution tables | 1000 |
| Call data memory internal (number of records)[16] | 1000 |
| Private contacts | 12000 |
| Call list entries for each of the 3 call lists per phone | 30 |
| Total call list entries | 60000 |
| Busy lamp field keys on Mitel SIP phones in total | 4000 |
| Busy lamp field keys per Mitel SIP phone | 50 |
| Same users on busy lamp field keys on Mitel SIP phones | 25 |
| Configured keys | 48000 |

[16] The call data memory is only used if the output destination is blocked (e.g. printer jam).

| Max. number... | Virtual Appliance Individual systems or AIN with Virtual Appliance as Master |
|---|---|
| Expansion key modules on DSI terminals | 400 |
| Expansion key modules on IP system phones | 400 |
| Expansion key modules on Mitel 6800/6900 SIP phones | 600 |
| Alpha keyboard Mitel K680 | 600 |
| Alpha keyboard (AKB) | 400 |

## 3.1.3 Terminals

**Table 13: Maximum number of terminals per system and interface**

| Interface | Terminal | Virtual Appliance Individual System | per AIN with Virtual Appliance as Master | per interface |
|---|---|---|---|---|
| Miscellaneous | Terminals (including virtual terminals and integrated mobile/ external phones) | 2400[17] | 2400[17] | |
| Miscellaneous | Terminals (excluding virtual terminals and integrated mobile/ external phones) | 2400[17] | 2400[17] | |
| Miscellaneous | Free seating pools | 2400 | 2400 | |
| DSI-AD2 | Terminals on DSI-AD2 interfaces (total) | – | 1200 | |

[17] Configurations with more than 800 end points must be approved by Mitel Sales Engineering Team.

| Interface | Terminal | Virtual Appliance Individual System | per AIN with Virtual Appliance as Master | per interface |
|---|---|---|---|---|
| DSI-AD2 | MiVoice 5360<br>MiVoice 5361<br>MiVoice 5370<br>MiVoice 5380 | – | 1200 | 2 |
| DSI-AD2 | MiVoice 5380<br>MiVoice 1560 | – | 32 | 2 |
| DSI-AD2 | SB-4+ radio unit | – | 255[18] | 1 |
| DSI-AD2 | SB-8/ SB-8ANT radio units | – | 255[18] | [19] |
| DECT | Mitel 610/612 DECT<br>Mitel 620/622 DECT<br>Mitel 630/632 DECT<br>Mitel 650 DECT<br>Office135<br>Office160<br>GAP terminals | – | 1200 | |
| LAN | Terminals on LAN interfaces (total) | 2400 | 2400 | |

[18] Maximum 64 radio units per location area if 4 location areas are defined, or maximum 128 radio units per location area if 2 location areas are defined.

[19] Operation on 2 DSI interfaces in each case

| Interface | Terminal | Virtual Appliance Individual System | per AIN with Virtual Appliance as Master | per interface |
|---|---|---|---|---|
| LAN | DHCP clients on the internal DHCP server | 3000 | 3000 | |
| LAN | MiVoice 2380 IP<br>MiVoice 5360 IP<br>MiVoice 5361 IP<br>MiVoice 5370 IP<br>MiVoice 5380 IP | 1200 | 1200 | |
| LAN | Mitel 6930 SIP<br>Mitel 6940 SIP<br>Mitel 6869 SIP<br>Mitel 6873 SIP | 4 | 4 | |
| | MiVoice 5380 IP<br>MiVoice 1560 | 32 | 32 | |
| LAN | Mitel 6940 SIP<br>Mitel 6873 SIP | 4 | 4 | |

| Interface | Terminal | Virtual Appliance Individual System | per AIN with Virtual Appliance as Master | per interface |
|---|---|---|---|---|
| LAN | Mitel 6920 SIP<br>Mitel 6930 SIP<br>Mitel 6940 SIP<br>Mitel 6863 SIP<br>Mitel 6865 SIP<br>Mitel 6867 SIP<br>Mitel 6869 SIP<br>Mitel 6873 SIP | 2400 | 2400 | |
| LAN | Mitel SIP-DECT Cordless phones | 2400 | 2400 | |
| LAN | Standard SIP terminals | 1200 | 1200 | |
| – | Virtual terminals | 1200 | 1200 | |
| – | Integrated mobile/ external phones | 1200 | 1200 | |
| BRI-S | Terminals on BRI-S interfaces (total) | – | 512 | 8[20] |

[20] Maximum of 2 simultaneous call connections.

| Interface | Terminal | Virtual Appliance Individual System | per AIN with Virtual Appliance as Master | per interface |
|---|---|---|---|---|
| BRI-S | Terminals as per ETSI standard<br>• ISDN terminals<br>• ISDN PC cards<br>• ISDN LAN routers<br>• ISDN Terminal Adapters | – | 512 | |
| FXS | Terminals on FXS interfaces (total) | – | 1200 | 1 |
| FXS | Analogue, nationally approved terminals<br>• Pulse dialling (PUL)<br>• Frequency dialling (DTMF)<br>• Radio units for cordless phones<br>• Door intercoms with DTMF control functions<br>• Group 3 fax machines[21]<br>• Answering machines<br>• Modems | – | 1200 | |
| FXS | External audio equipment with line output | – | 1 per node | |

[21] Transmission with the T.38 protocol is recommended for Fax over IP. The corresponding media resources need to be allocated.

| Interface | Terminal | Virtual Appliance Individual System | per AIN with Virtual Appliance as Master | per interface |
|---|---|---|---|---|
| FXS | External equipment can be switched via control outputs | – | 1200 | |
| FXS | External switches for controlling internal switch groups via control inputs | – | 1200 | |
| FXS | General bell | – | 1 per node | |

## 3.1.4 Terminal and network interfaces

**Table 14: Terminal and network interfaces**

| Max. number... | Virtual Appliance Individual systems | AIN with Virtual Appliance as Master |
|---|---|---|
| Ethernet interfaces | 1 | per node |
| Network interfaces, total (FXO, BRI-T, PRI, BRI-Sext.) | – | 288 |
| Terminal interfaces, total (DSI, FXS, BRI-S) | – | 1200 |
| DSI terminal interfaces | – | 1200 |
| Analogue terminal interfaces FXS | – | 1200 |
| BRI-S terminal interfaces | – | 224 |

| Max. number... | Virtual Appliance Individual systems | AIN with Virtual Appliance as Master |
|---|---|---|
| Analogue network interfaces FXO | – | 64 |
| Basic rate interfaces BRI-T | – | 256 |
| Basic accesses BRI-S ext. | – | 256 |
| Primary rate interfaces PRI | – | 32[22] |
| SIP access | 10 | 10 |
| SIP access channels[23] | 240 | 240 |

## 3.1.5 Software assurance

Software Assurance (SWA) is Mitel's comprehensive support offer which gives access to new software releases, support services and SRM remote access to the communication server.

The software assurance agreement has a fixed runtime and defines the number of authorised users on the communication system. You can see at a glance whether a valid (active) SWA is available for the communication server, via the SWA state in the WebAdmin title bar.

The SWA state is retrieved via an encrypted direct link on the licence server. If there is no connection to the licence server, the last known state is displayed

The number of users covered via SWA and the number of configured users requiring SWA can be seen in the *System information* view. SWA becomes invalid if the number of configured users exceeds the number of users covered via SWA.

## 3.1.6 Licences

Use of the call manager software requires a licence. The Mitel CPQ application automatically plans the necessary licences, which are then enabled on the communication server using a licence file.

The licence file contains all the enabled licences. When you purchase a new licence from your authorised dealer, you obtain a new licence file in return. Upload this file in WebAdmin in the *Licences* view.

[22] 10 B channels per PRI network interface can be used without licence
[23] Licences required

**Note**:

- A licence file is not transferable to another communication server.
- If you receive a voucher instead of a licence file, log on with your partner login at MiAccess https://miaccess.mitel.com/and generate the licence file yourself using the EID number. Detailed instructions about this can be found in the WebAdmin help on the *Licences* view.

### 3.1.6.1 Description of available licences

**Software**

- *Software Release*

  Updating to a new software release requires a licence. A valid software assurance (SWA) entitles you to upgrade the communication server to a new software level for a specific period., and to operate it with a specific number of users.

  A valid software assurance is the prerequisite for being able to acquire an update licence (*Software Release* licence) for a particular software version. Without a valid *Software Release* licence you can update the communication server to a new software level, but after four hours of operating time it will switch over to the restricted operating mode (see Restricted operating mode). The communication server will switch back to normal operation as soon as you upload a licence file that comprises the *Software Release* licence. You do not need to restart the communication server.

**Note**:

- The purchase of a new communication server also includes a software assurance for a specific period. Log on with your partner login to Mitel MiAccess https://miaccess.mitel.com/ and obtain a new licence file using the EID number and the voucher. The licence file issued as a result contains the appropriate *Software Release* licence (and any other licences you may have acquired). You can now activate the communication system with this licence file. Detailed instructions about this can be found in the WebAdmin help on the *Licences* view.
- **Mitel Advanced Intelligent Network**

  In an AIN, a valid *Software Release* licence must be available on the master only. Exception: For long-term offline mode, for operation with Secure VoIP and use as backup communication server, the satellite must also have a valid *Software Release* licence.

  - Behaviour of satellites in offline mode:

    Satellites with an incorrect release licence change over to restricted operating mode after thirty-six hours. Satellites without any release licence change over to restricted operating mode after four hours.

**User**

- *User*

  Virtual Appliance requires a *User* licence for each user in the system.

  Exception: A user without a terminal or with a virtual terminal only does not need a licence.
- *IP User* (licence bundle)

  With this licence bundle, an additional user is available who can assign 8 terminals of any type (exception: for a Mitel One, an extra terminal license is required) including the appropriate phone licences and video licences, if needed. This allows the user to change the phone type without changing the licensing
- With the following UCC licence bundles an additional user is available who can assign 8 terminals of any type including the appropriate phone licences and video licences for all phones, if needed. The licence bundles are explicitly assigned to a certain user:

  - *Entry UCC User*

    This licence bundle contains the licences described in the above section and activates MiCollab functions for the MiCollab role *UCC Entry*, and Mitel One feature for a user.
  - *Standard UCC User*

    This licence bundle contains the licences described in the above section and activates MiCollab functions for the MiCollab role *UCC Standard*, and Mitel One feature for a user.
  - *Premium UCC User*

    This licence bundle contains the licences described in the above section and activates MiCollab functions for the MiCollab role *UCC Premium,* and Mitel One feature for a user.

  With a specific number of UCC licence bundles, users with SIP terminal licences for using with MiCollab AWV are added.

  The formula is: **10 + [Standard UCC User] / 10 + [Premium UCC User] / 5**

  Example: Entry UCC User: 12, Standard UCC User: 22, Premium UCC User: 14

  Formula: 10 + 22 / 10 + 14 / 5 = 14 users with SIP terminals.

**Terminals**

- *MiVoice 2380 IP Softphones*

  An IP user license is required to operate the IP softphones MiVoice 2380 IP. The licences are needed to register the terminals on the system.
- *MiVoice 5300 IP Phones*

  An IP user license is required to operate the IP system phones MiVoice 5360 IP, MiVoice 5361 IP, MiVoice 5370 IP and MiVoice 5380 IP. The licences are needed to register the terminals on the system. If the required licences are missing, the relevant event message is output on the system.
- *Mitel SIP Terminals*

  To operate Mitel SIP terminals of the Mitel 6800/6900 SIP series, the user requires an IP user licence.

- *Mitel One*

  With this licence, a mobile phone with the Mitel One application can be integrated into the communication system together.
- *Dual Homing*

  In the event of failure of the primary communication server or an interruption in the IP connection to the primary communication server, SIP phones in the Mitel 6800/6900 SIP series can automatically register on a backup communication server. On the **backup communication server one licence** is required per phone. The licences are needed to register the clients on the system.
- *Mobile or External Phone Extension*

  This terminal type is used to integrate mobile phones or other external phones into the communication system. The user requires an IP user licence for this type of terminal.
- *SIP Terminals*

  An IP user licence is required to operate standard SIP terminals.
- *Video Terminals*

  To be able to use the video functionality of a standard SIP video terminal, an IP user licence is required.
- *Video Terminals*

  To be able to use the video functionality of a standard SIP video terminal you need to acquire a Video Terminals licence in addition to a *SIP Terminals* licence.

**Audio services**

- *Conference Bridge* (Dial-In conference)

  This licence is included in the MiVoice Office 400 SMBC Base kit - S bundle and allows the use of a conference bridge. The internal or external conference participants choose a specific call number and are connected with the conference after entering a PIN. One licence is required per system /AIN.
- *Number in Queue*

  This licence is included in the MiVoice Office 400 SMBC Base kit - S bundle and allows using the functionality of "Queue with announcement".
- *Auto Attendant*

  This licence is included in the MiVoice Office 400 SMBC Base kit - S bundle and allows the use of the auto attendant function.
- *Enterprise Voice Mail*

  The licence is included in the MiVoice Office 400 SMBC Base kit - S bundle.

**Note**:

Additional audio channels require additional *Audio Record amp; Play Channels* licences. An Auto Attendant licence is required to use the auto attendant function.

- *Audio Record and Play Channels*

  These licenses are included in the MiVoice Office 400 SMBC Base kit - S bundle. Audio channels are used for recording or playing back audio data for voice mail, auto attendant or call recording.

  **Mitel Advanced Intelligent Network**

  The media resources on each node must be available and allocated accordingly.

**Features**

- *Secure VoIP*

  This licence allows encrypted VoIP connections with the aid of SRTP (Secure Real-Time Transport Protocol) and/or encrypted SIP signalling data using TLS (Transport Layer Security).

  **Mitel Advanced Intelligent Network**

  **Note**:
  For legal reasons (Trade Control Compliance) in an AIN a Secure VoIP licence is required for both the Master and for each satellite.

- *Silent Intrusion*

  This licence is needed for the Silent intrusion feature, which is similar to the Intrusion feature. The difference is that the user intruded upon receives neither a visual nor an acoustic signal of the intrusion. The feature is used mainly in call centres. One licence is required per system /AIN.

**Resources**

- *Base licence Virtual Appliance*

  This basic licence is required for Virtual Appliance. For each user a *User* licence(see User licences) is required additionally. With this basic licence no other licences are needed for setting up a Mitel Advanced Intelligent Network (AIN).
- *VoIP Channels for Standard Media Switch*

  These licenses are included in the MiVoice Office SMBC Base kit - S bundle and enables the conversion of voice channels for VoIP-non-VoIP connections and is used for IP terminals, SIP terminals, SIP access channels or to operate a Mitel Advanced Intelligent Network. High voice data compression is possible with the G.729 VoIP channels.

- Theoretically there are no VoIP channels required in a pure VoIP environment (only IP/SIP phones on the system and connection to the public network via a SIP provider). However, as soon as voice mail functions, the announcement service or music on hold is used, VoIP channels are required as the use of these functions entails a conversion of the voice data.
- **Mitel Advanced Intelligent Network**

  The media resources on each node must be available and allocated accordingly.

**Networking**

- *B-Channels on PRI Cards*

  These licenses are included in the MiVoice Office SMBC Base kit - S bundle.
- *SIP Access Channels*

  The connection of the system to a SIP service provider or the networking of the systems via SIP requires one licence per channel. The MiVoice Office 400 SMBC Base kit - S bundle includes these SIP access channel licenses

**Note**:

**Mitel Advanced Intelligent Network:** The media resources on each node must be available and allocated accordingly.

### Private networking

- *QSIG Networking Channels*

  These licences are included in the MiVoice Office SMBC Base kit - S bundle and used to implement a private leased-line network with QSIG by enabling a specific number of simultaneously outgoing QSIG channels.

**Note**:

For Virtual Appliance this licence is only relevant to the QSIG networking of an AIN satellite.

### Applications

- *Advanced Messaging*

  Enables the SMPP protocol to be used for integrating an SMS server and 9d DECT and DT DECT cordless phones to be logged on as system phones). User-friendly messaging systems can then be implemented. One licence is required per system/AIN.
- *CTI First Party via LAN*

  This basic licence enables the CTI basic functions via Ethernet interface (e.g. for using a PC dial help) for a specific number of users (see General system capacity). It cannot be combined with CTI third-party licences.
- *CTI First Party via LAN*

  This licence is included in the MiVoice Office SMBC Base kit - S bundle and enables the CTI basic functions via Ethernet interface (e.g. for using a PC dial help) for a specific number of users (see General system capacity). It cannot be combined with CTI third-party licences.

- *Dialers*

  This licence allows you to use the Mitel Dialer CTI application. The number of licences determines the simultaneously active, user-assigned Mitel Dialer applications.
- *Hospitality Bundle SMBC / VA - S*

  This bundle allows you to use the Mitel 400 Hospitality Manager. The Mitel 400 Hospitality Manager is a web-based application for receptionists in the hospitality sector. One licence is required per system / AIN.

  This is used to connect the communication server to a hotel management system using the FIAS protocol.

**Interfaces**

- *ATAS Interface / ATASpro Interface*

  These licenses are included in the MiVoice Office 400 SMBC Base kit - S bundle and allows to connect external alarm and messaging sources via the Ethernet interface.

  ATAS Interface: Many commands available for messaging (displaying text and presenting softkeys on system phones), emergency number called alarm, safeguard basic with Redkey, charging bay monitoring etc.

  ATASpro Interface: Additional functions available like DECT localization, public emergency number called alarm, evacuation alarm, enhanced safeguard with alarm trigger, get rooms and room state.

> **Note**:
>
> If you use the Mitel Open Interfaces Platform, OIP takes the licences from the communication server. If you use the Mitel Open Interfaces Platform, OIP takes the licences from the communication server.

- *CSTA Sessions*

  This licence allows third-party applications to monitor/check a terminal on the communication server using the CSTA protocol. If a terminal is monitored or checked by several applications or instances, one licence is required for each monitoring/check.
- *Presence Sync. via SIMPLE and MSRP*

  SIMPLE (Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions) is a protocol for exchanging presence information, and is used between SIP endpoints (terminals, network interfaces and nodes). MSRP (Message Session Relay Protocol) is a protocol used for exchanging data between SIP clients (example for chats). These licenses are included in the MiVoice Office 400 SMBC Base kit - S bundle.

## 3.1.7 Restricted operating mode

Without a valid *Software Release* licence the communication server switches over to a restricted operating mode four hours after each restart. The restriction concerns the following aspects:

Restricted operating features:

- No call information for incoming calls and during the call connection.
- Dialling by name is deactivated.
- Functions cannot be invoked via the menu or function key (likewise no enquiry calls can be made).
- The team keys do not work.
- Functions codes are not carried out (except remote maintenance on/off).
- Dialling from PC and other CTI functions are not supported.

Restricted services and routing functions:

- Calls are not routed to integrated mobile/external phones.
- Call centre functions are out of service (no routing to ACD).
- Voice mail functions are out of service (no call routing to voice mail).
- The announcement service is out of service.

## 3.1.8 Temporary offline licences

If the connection to the master is interrupted in an AIN, the satellites restart in offline mode. The licences acquired on the master are no longer visible for the satellites in offline mode. To ensure autonomous VoIP and QSIG traffic temporarily, certain licences are enabled in the satellites concerned for the duration of offline operation or for a maximum of 36 hours (the licences are not visible in WebAdmin). The licence overview (Overview of licences) shows which licences are affected. To ensure longer offline operation, the necessary licences must also be acquired on the satellites.

## 3.1.9 Trial licences

Trial licences are available for some functions. This means that functions or features that require a licence can be used and tested, licence-free, for a period of 60 days. The trial licences are automatically enabled the first time a particular function is used and then listed in WebAdmin in the *Licences* view, complete with the date on which they expire. This procedure can only be used once for each function or feature. Thereafter you must acquire a licence. The licence overview shows which trial licences are available.

## 3.1.10 Virtual Appliance licences

You can obtain Virtual Appliance licences in two ways:

**Via the Virtual Appliance EID**

For this type of licensing, your Virtual Appliance communication server must have a permanent internet access. This is necessary as the licence server regularly checks whether a second communication server with the same EID (clone) does not exist. If this is the case, the event message *Possible clone of your system detected* is displayed. If the suspicion is confirmed, the communication server switches to restricted operating mode (see Restricted operating mode).

Restricted operating mode is also activated if the communication server remains unconnected to the licence server for a longer time (max. 72 hours), or if the licence is invalid.

**Note**:

If during normal operation Virtual Appliance loses contact with the licence server, a 72-hour timer is started. If the link is restored before the end of the 72 hours, the timer is not directly reset, but counts up until the 72 hours are reached again.

This licensing type can be used for an individual system or in an AIN. If a licence file of this type is loaded to the communication server, you will see the EID of Virtual Appliance in the *Licences* view and the status parameter *Online licence check* is activated.

**Licensing via the EID of a gateway satellite**

A satellite's EIM card serves as licensee for this licensing type. Therefore the satellite's EID (Gateway EID) must be entered on the licence server configuration. If a licence file of this type is loaded to the communication server, you will see the EID of Virtual Appliance and the Gateway EID in the *Licences* view and the status parameter *Online licence check* is deactivated.

If during normal operation the Master loses contact with the satellite with the gateway EID, a 72-hour timer is started. The satellite restarts in offline mode with the temporary offline licence (see Temporary offline licences). The Master Virtual Appliance continues to run for 72 hours in normal operating mode, except that, for instance, the satellite's gateway functions can no longer be used. After the 72 hours, the Virtual Appliance communication server switches to restricted operating mode (see Restricted operating mode).

**Note**:

If the link between the master and the satellite is restored before the end of the 72 hours, the timer is not directly reset, but counts up until the 72 hours are reached again.

This licensing type is only available in an AIN with Virtual Appliance as master.

**Overview of licences**

**Table 15: Overview of licences**

| Licence | Licensed attributes | Without licence | With licence | Licences for networking | Offline licence | Trial licence |
|---|---|---|---|---|---|---|
| **Software** | | | | | | |

| Licence | Licensed attributes | Without licence | With licence | Licences for networking | Offline licence | Trial licence |
|---|---|---|---|---|---|---|
| *Software Release* | Allows a particular software release to be operated | Restricted[24] | Unrestricted | In the AIN, only on the Master; otherwise per node. | – | – |
| **Users** | | | | | | |
| *User* | Allows user operation on Virtual Appliance. | Locked | 1, 20, 50, 100 or 200 additional users per licence. | In the AIN, only on the Master; otherwise per node. | yes | – |
| *IP User* | Licence bundle:<br><br>1 additional user<br><br>8 phone licences (any type except Mitel One)<br><br>8 phones per user only | 0 | 1 additional user per licence. | In the AIN, only on the Master; otherwise per node. | yes | – |

[24] 4 hours after the new software has been uploaded or after a restart operation, the communication server switches over to a restricted operating mode (see Restricted operating mode).

| Licence | Licensed attributes | Without licence | With licence | Licences for networking | Offline licence | Trial licence |
|---|---|---|---|---|---|---|
| *Entry UCC User* | Licence bundle:<br>• 1 additional user<br>• 8 phone licences (any one)<br>• 8 phones per user<br>• Video licence for all licensed phones.<br>• MiCollab role *UCC Entry.*<br>• 1 Mitel One client license per user | 0 | 1 additional user per licence. | In the AIN, only on the Master; otherwise per node. | yes | – |
| *Standard UCC User* | Licence bundle:<br>• 1 additional user<br>• 8 phone licences (any one)<br>• 8 phones per user<br>• Video licence for all licensed phones.<br>• MiCollab role *UCC Standard.*<br>• 1 Mitel One client license per user. | 0 | 1 additional user per licence. | In the AIN, only on the Master; otherwise per node. | yes | – |

| Licence | Licensed attributes | Without licence | With licence | Licences for networking | Offline licence | Trial licence |
|---|---|---|---|---|---|---|
| *Premium UCC User* | Licence bundle:<br>• 1 additional user<br>• 8 phone licences (any one)<br>• 8 phones per user<br>• Video licence for all licensed phones.<br>• MiCollab role *UCC Premium*<br>• 1 Mitel One Client licence per user | 0 | 1 additional user per licence. | In the AIN, only on the Master; otherwise per node. | yes | – |
| **Terminals** | | | | | | |
| *MiVoice 2380 IP Softphones* | Number of registered MiVoice 2380 IP IP softphones | 0 | Per licence 1 additional IP softphone | In the AIN, only on the Master; otherwise per node. | yes | yes |
| *MiVoice 5300 IP Phones*[25] | Number of registered , MiVoice 5360 IP, MiVoice 5361 IP, MiVoice 5370 IP and MiVoice 5380 IP IP system phones | 0 | 1, 20 or 50 additional IP system phones per licence | In the AIN, only on the Master; otherwise per node. | yes | yes |

[25] The licences can also be used if the *Mitel SIP Terminals* licences are missing.

| Licence | Licensed attributes | Without licence | With licence | Licences for networking | Offline licence | Trial licence |
|---|---|---|---|---|---|---|
| *Mitel SIP Terminals* | Number of registered phones of the Mitel 6800/6900 SIP series | 0 | 1, 20 or 50 additional Mitel SIP phone per licence | In the AIN, only on the Master; otherwise per node. | yes | yes |
| *Mitel 8000i Video Options* | Use of the video functionality of an Mitel SIP terminal | 0 | Additional licence for Mitel SIP Terminals. 1, 20 or 50 additional Mitel SIP terminals with video functionality per licence. | In the AIN, only on the Master; otherwise per node. | yes | yes |
| *Mitel Dialog 4200 Phones*[26] | Number of registered Dialog 4220, Dialog 4222 and Dialog 4223 digital phones | 0 | One additional phone per licence | In the AIN, only on the Master; otherwise per node. | yes | 3 |
| *MMC Extensions* | Number of mobile phones that can be registered with Mitel One client. | 0 | Per licence 1 additional mobile phone (with Mitel One) | In the AIN, only on the Master; otherwise per node. | – | – |
| *Dual Homing* | Number of registered Mitel 6800/6900 SIP phones on a backup communication server | 0 | Per licence 1, 20 or 50 additional phones | Always on the backup communication server | – | yes |

[26] Dialogue phones can be connected to Mitel 470 and Mitel SMBC only.

| Licence | Licensed attributes | Without licence | With licence | Licences for networking | Offline licence | Trial licence |
|---|---|---|---|---|---|---|
| *Mobile or External Phone Extensions* | Number of mobile/external phones that can be registered (without Mitel One) | 0 | One additional mobile/ external phone per licence (without Mitel One) | In the AIN, only on the Master; otherwise per node. | yes | yes |
| *SIP Terminals* | Number of registered standard SIP terminals | 0 | 1 additional standard SIP terminal per licence | In the AIN, only on the Master; otherwise per node. | yes | yes |
| *Video Terminals* | Use of the video functionality of a standard SIP terminal | 0 | Additional licence for SIP Terminals. 1 additional standard SIP terminal with video functionality per licence. | In the AIN, only on the Master; otherwise per node. | yes | yes |
| **Audio services** | | | | | | |
| *Conference Bridge (Dial-In Conference)* | Use of conference bridge | Locked | Enabled | In the AIN, only on the Master; otherwise per node. | – | yes |
| *Number in Queue* | Use of the function 'queue with announcement ' | Locked | Enabled | In the AIN, only on the Master; otherwise per node. | yes | yes |
| *Auto Attendant* | Use of the auto attendant function | Locked | Enabled | In the AIN, only on the Master; otherwise per node. | yes | yes |

| Licence | Licensed attributes | Without licence | With licence | Licences for networking | Offline licence | Trial licence |
|---|---|---|---|---|---|---|
| *Enterprise Voice Mail* | Voice compression, expanded voice memory capacity, and e-mail notification whenever new voice messages are received, forwarding of voice messages, call recording. | Locked | Enabled (including 2 audio channels for voice mail, Auto Attendant or call recording) | In the AIN, only on the Master; otherwise per node. | yes | 3 |
| *Audio Record amp; Play Channels* | Audio channels for recording or playing back audio data. | Locked | Per licence 1 additional audio channel for voice mail, Auto Attendant or call recording | In the AIN, only on the Master; otherwise per node. | – | – |
| **Features** | | | | | | |
| *Analogue Modem* | Use of the modem functionality on an Mitel 415/430. | Locked | Enabled | In the AIN, only on the Master; otherwise per node. | yes | yes |
| *Secure VoIP* | Encrypted VoIP connections using SRTP and TLS. | Non-encrypted trans-mission | Encrypted transmission | Per node | – | – |
| *Silent Intrusion* | Use of the Silent intrusion feature | Locked | Enabled | In the AIN, only on the Master; otherwise per node. | – | – |
| **Resources** | | | | | | |

| Licence | Licensed attributes | Without licence | With licence | Licences for networking | Offline licence | Trial licence |
|---|---|---|---|---|---|---|
| *Base licence Virtual Appliance*[27] | Allows the operation of Virtual Appliance. No additional licences needed for setting up a AIN. | Restricted[a] | Unrestricted (also in a AIN). | In the AIN, only on the Master; otherwise per node. | yes | – |
| *VoIP Channels for Standard Media Switch*[28] | VoIP functionality | 0 / 2 [29] | Per licence 1 additional VoIP channel | In the AIN, only on the Master; otherwise per node. | yes | yes |
| **Network** | | | | | | |
| *B-Channels on PRI Cards* | B channels that can be used simultaneously on the PRI interface | 10 | Per licence 1 additional B-channel | In the AIN, only on the Master; otherwise per node. | – | – |
| *SIP Access Channels* | Simultaneously usable channels to an SIP provider | 0 | Per licence 1 additional SIP access channel | In the AIN, only on the Master; otherwise per node. | yes | yes |
| **Private networking** | | | | | | |

27 This licence is not viewable in the licence overview in WebAdmin.

29 If VoIP mode is set to G.711, two G.711 VoIP channels per system can be used without a licence.

28 If Virtual Appliance is used as Master, the VoIP channels of the master node are made available without a licence from the integrated Mitel Media Server. However, for the satellites' VoIP channels, the licences must be purchased.

| Licence | Licensed attributes | Without licence | With licence | Licences for networking | Offline licence | Trial licence |
|---|---|---|---|---|---|---|
| QSIG Networking Channels[30] | QSIG channels | 0 | Per licence 4 or n QSIG channels (n limited by the system capacity) | Per node | yes | yes |
| **Applications** | | | | | | |
| *Advanced Messaging* | SMPP protocol for integration of an SMS server and registration of 9d cordless phones as system phones. (Includes licence SMPP) | Locked | Enabled | In the AIN, only on the Master; otherwise per node. | – | – |
| *CTI First Party via LAN* | First-party CTI clients with basic functions on Ethernet interface | 0 | Enabled for a specific number of users (see General system capacity | In the AIN, only on the Master; otherwise per node. | – | yes |
| *Dialers* | Number of simultaneously active, user-linked Mitel Dialer applications. | 0 | 1, 20 or 50 additional instances per licence | In the AIN, only on the Master; otherwise per node. | – | yes |
| *Hospitality Manager* | Use of Mitel 400 Hospitality Manager | Locked | Enabled | In the AIN, only on the Master; otherwise per node. | – | yes |

[30] For Virtual Appliance this licence is only relevant to the QSIG networking of an AIN satellite.

| Licence | Licensed attributes | Without licence | With licence | Licences for networking | Offline licence | Trial licence |
|---|---|---|---|---|---|---|
| *Hospitality PMS Interface* | Use of the PMS interface and therefore the FIAS protocol. | Locked | Enabled | In the AIN, only on the Master; otherwise per node. | – | yes |
| *Hospitality PMS Rooms* | Number of rooms when using the PMS interface. | 0 | 1, 20, 50 or 100 rooms per licence | In the AIN, only on the Master; otherwise per node. | – | 3 |
| *Mitel OpenCount Basic Package* | Basic licence: Prerequisite for all other OpenCount licences. Enables connection to the MiVoice Office 400 and the use of basic functions. | Locked | Enabled | In the AIN, only on the Master; otherwise per node. | yes | yes |
| *Mitel OpenCount Healthcare Branch Package* | Additional licence: Offers extra functions for care homes and retirement homes. | Locked | Enabled | In the AIN, only on the Master; otherwise per node. | yes | yes |
| *Mitel OpenCount Public Authorities Branch Package* | Additional licence: Offers extra functions for municipalities, communities and ministries. | Locked | Enabled | In the AIN, only on the Master; otherwise per node. | yes | yes |
| *Mitel OpenCount Functional Upgrade to Comfort* | Additional licence: Offers extra functions such as PIN telephony. | Locked | Enabled | In the AIN, only on the Master; otherwise per node. | yes | yes |

| Licence | Licensed attributes | Without licence | With licence | Licences for networking | Offline licence | Trial licence |
|---|---|---|---|---|---|---|
| *Mitel OpenCount Functional Upgrade to Premium* | Additional licence: Offers extra functions such as intermediate statements, invoicing etc. | Locked | Enabled | In the AIN, only on the Master; otherwise per node. | yes | yes |
| *Mitel OpenCount Users* | Additional licence: Enables a defined number of users to be monitored via OpenCount. | 0 | 1, 20 or 50 additional users per licence | In the AIN, only on the Master; otherwise per node. | yes | yes |
| **Interfaces** | | | | | | |
| *ATAS Interface* | Use of the ATAS interface | Locked | Enabled | In the AIN, only on the Master; otherwise per node. | – | yes |
| *ATASpro Interface* | Use of the ATASpro interface | Locked | Enabled | In the AIN, only on the Master; otherwise per node. | – | yes |
| *CSTA Sessions* | Number of monitored terminals via the CSTA protocol. | 0 | 1, 20, 50 or 100 CSTA sessions per licence | In the AIN, only on the Master; otherwise per node. | yes | yes |
| *Presence Sync. via SIMPLE and MSRP* | Number of users who can use one (or both) protocols for the third-party applications. | 0 | 1, 20 or 50 additional users per licence who may use both protocols. | In the AIN, only on the Master; otherwise per node. | yes | yes |

| Licence | Licensed attributes | Without licence | With licence | Licences for networking | Offline licence | Trial licence |
|---|---|---|---|---|---|---|
| *OAI Interface* | Use of the Open Application Interface | Locked | Enabled | In the AIN, only on the Master; otherwise per node. | – | yes |

All the licences are offered in separate licence packages. Depending on the sales channels the packages may differ from the licences in Overview of licences. The systems ship out unlicensed. Back-licensing is not provided for. However, resetting to the factory setting is possible.

**OIP licences**

OIP licences are managed by OIP itself. A detailed description of the OIP licences can be found in the System Manual Mitel Open Interfaces Platform.

# Installation 4

This chapter contains the following sections:

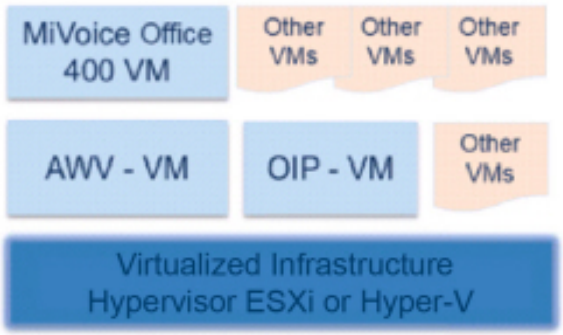


This chapter defines the conditions for installing Virtual Appliance and contains detailed installation instructions. A description of how to mount, power, equip and connect the Mitel 415/430, Mitel SMBC and Mitel 470 communication servers, and how to connect the interfaces, as well as their features, is given in the corresponding system manuals.

## 4.1 Introduction

The MiVoice Office 400 Virtual Appliance is provided as a preconfigured VMware compatible image (OVA file) or as virtual hard disc format (VHD file) and is installed on a virtual machine of a professional server. The server may also contain other virtual Mitel applications (e.g. OIP or MiCollab AWV) and third-party applications such as a mail server.

Figure 3: MiVoice Office 400 Virtual Appliance and other virtual applications




## 4.2 Abbreviations and definitions

**Table 16: Abbreviations and definitions**

| | | |
|---|---|---|
| VM | Virtual Machine | A virtual machine is the software implementation of a computer environment. It reflects the architecture of a real hardware PC. |

| | | |
|---|---|---|
| OVA | Open Virtualization Archive | Image file for installing MiVoice Office 400 Virtual Appliance, including Mitel Standard Linux operating system on a virtual machine. |
| VHD | Virtual Hard Disc | |
| MSL | Mitel Standard Linux | Operating system on which MiVoice Office 400 Virtual Appliance is running. |
| ESXi | Hypervisor developed from VMware | Abstracting layer between the hardware and one or more virtual machines. |
| Hyper-V | Hypervisor developed from Microsoft | Abstracting layer between the hardware and one or more virtual machines. |
| vSphere® Hypervisor | Installable ISO file containing the ESXi Hypervisor and vSphere client | |
| vSphere client | Configuration and management fool for ESXi | |

## 4.3 Minimum requirements for the virtual machine

**Supported platforms:**

VMware ESXi (refer to release notes for compatible versions) / Microsoft Hyper-V. Under VMware, virtual network card VMXNET3 is required.

The following table shows the recommendations for the vast majority of use cases - however, higher values may be required under special circumstances of load / traffic.

**Table 17: Minimum requirements for the virtual machine**

| Deployment type | Number of 2 GHz vCores | Amount of RAM | Disk size | Network |
|---|---|---|---|---|
| Virtual Appliance Standalone | 1 | 2 GB | 32 GB | 1 GB/s |

| Deployment type | Number of 2 GHz vCores | Amount of RAM | Disk size | Network |
|---|---|---|---|---|
| Virtual Appliance + CloudLink Gateway (standard) | 2 | 2 GB | 32 GB | 1 GB/s |
| Virtual Appliance + CloudLink Gateway (high performance) | 8 | 5 GB | 32 GB | 1 GB/s |

## 4.3.1 Installing MiVoice Office 400 Virtual Appliance

The MiVoice Office 400 Virtual Appliance software and Mitel Standard Linux operating system are installed using an OVA file (for ESXi) or a VHD file (for Hyper-V). The guide below contains the necessary steps to take in order to install MiVoice Office 400 Virtual Appliance.

**See also:**

You can find more information about Mitel Standard Linux in the Installation and Administration Guide "Mitel Standard Linux".

You can find more information on how to operate virtual applications in a virtual environment in the Solutions Guide "Virtual Appliance Deployment".

Both documents are available on in the technical document portal .

MiVoice Office 400 Virtual Appliance supports different virtualized infrastructures. Follow the steps in one of the following appropriate chapters:

- Installation in a vSphere virtualized infrastructure on page 70
- Installation in a Hyper-V virtualized infrastructure

### 4.3.1.1 Installation in a vSphere virtualized infrastructure

Installation prerequisites:

- ESXi VMware vSphere is pre-installed on an appropriate server and the registration data is known.

> **Note**:
>
> ESXi may only be installed by certified personnel on VMware compatible hardware. (see *http://www.vmware.com/resources/compatibility/search.php*)

- The OVA file used to install the virtual machine is available.

- The minimum requirements for the virtual machines are met (see Minimum requirements for the virtual machine on page 69).

**Install the vSphere client on a Windows PC**

1. In a browser window, enter the IP address of the server on which ESXi VMware vSphere is pre-installed.
   - The VMware ESXi website is displayed.
2. Click the *Download vSphere Client for Windows link then install the client.*


**Install the virtual machine using the OVA file**

**Note**:

If you had been deploying a Virtual Appliance communication server and wish to make a fresh installation with an OVA file, please take note of the following:

(Fresh installation resets all configuration data to the default values and deletes all audio data). First create a backup of the configuration and audio data (see Chapter Data backup).

1. Start the vSphere client and enter the ESXi server user name and password.
2. Click *File* / *Deploy OVF Template* then browse for the storage area and the OVA file (e. g.: *mlx_x50_pbx8834b1.ova*).
   - An information window displays the size of the packet and the required storage capacity on the hard disk.

3. Enter a name and the storage area for the virtual machine. By default, the OVA file name is proposed.
4. *Thick Provisioning Lazy Zeroed* is recommended as hard disk format. This setting reserves approx. 15 GB storage space on the hard disk for the virtual machine.
5. End the installation wizard and wait till the installation of the virtual machine with the Mitel Standard Linux operating system and the application for MiVoice Office 400 is completed.

**Starting the virtual machine**

1. Open a console via the menu or by clicking .
2. Start the virtual machine via the menu or by clicking .
3. After the start sequences, a window opens so you can enter an *Application record ID*. Skip this step by pressing *Next*.
4. In the login screen that opens, log on using the following default values:

   login: *admin*

   password: *mslmivo400*

**Note**:

- For older MiVoice Office 400 Virtual Appliance deployments (that is before release 7.0), the default password is password.
- The default WebAdmin password is used here as mslmivo400. Once you change the password in WebAdmin, you must henceforth use the new WebAdmin password here.
- Be careful if a new password contains some digits. When the console is active, the *Num lock* function of the digit block may be disabled and your password is not accepted. Therefore, it is better to use the digits via the normal keyboard and not via the digit block.
- If you see only a black window instead of the login, click inside the window and press *Enter*.

## 4.3.1.2 Installation in a Hyper-V virtualized infrastructure

Installation prerequisites:

- Hyper-V manager is available on an appropriate server.
- The VHD file (e.g. *mlx_x50_pbx8834b1.vhd*) used to install the virtual machine is available.
- The minimum requirements for the virtual machines are met (see Minimum requirements for the virtual machine on page 69).

**Create the virtual machine**

**Note**:

If you had been deploying a Virtual Appliance communication server and wish to make a fresh installation with an VHD file, please take note of the following:

(Fresh installation resets all configuration data to the default values and deletes all audio data). First create a backup of the configuration and audio data (see Chapter Data backup).

1. Start the Hyper-V manager on the server.
2. Create a new virtual machine, name it and click *Next*.
3. Keep the default setting for *Generation 1* and click *Next*.
4. Increase the assigned memory to 2048MB and click *Next*.
5. Select the appropriate network and click *Next*.
6. Select *Use an existing virtual hard disk*, browse for the mlx_50_...vhd file and click *Next*.
7. Check the summary of the new virtual machine and click *Finish*.

*Start the virtual machine*

1. Select the new virtual machine and click *Connect* (right mouse click)
   - The virtual machine connection window opens.
2. Start the virtual machine with *Start*.
3. After the start sequences, a window opens where you could enter a *Application record ID*. Skip this step by pressing *Next*.
4. In the login screen that opens, log on using the following default values:

   login: *admin*

   password: *mslmivo400*

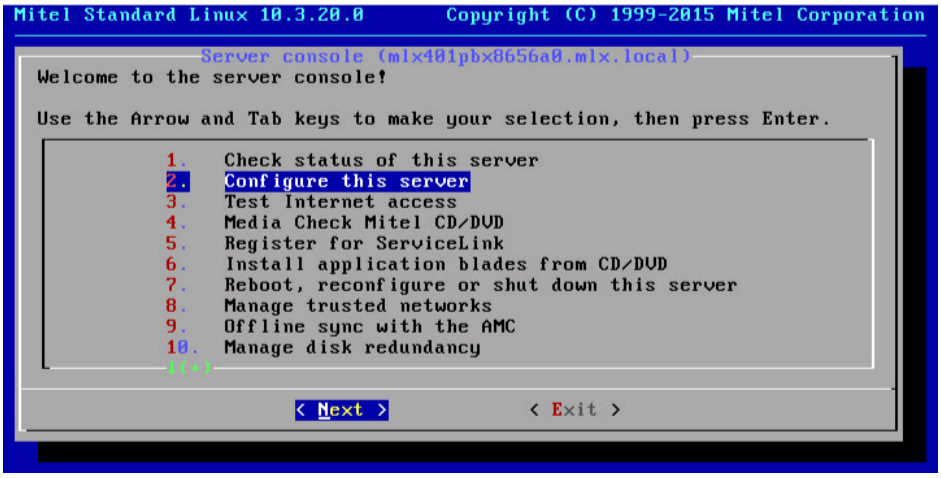
**Note**:

- For older MiVoice Office 400 Virtual Appliance deployments (that is before release 7.0), the default password is password.
- The default WebAdmin password is used here as mslmivo400. Once you change the password in WebAdmin, you must henceforth use the new WebAdmin password here.
- Be careful if a new password contains some digits. When the console is active, the *Num lock* function of the digit block may be disabled and your password is not accepted. Therefore, it is better to use the digits via the normal keyboard and not via the digit block.
- If you see only a black window instead of the login, click inside the window and press *Enter*.

# 4.3.1.3 Configuration of MSL (vSphere and Hyper-V)

**Configure the Mitel Standard Linux server**

The menu below is displayed after you have logged on successfully:




1. Use the arrow keys to select the entry *Configure this server*.

**Note**:

2. Enter a domain name for the server or use the default value *mlx.local*.
3. Enter a system name for the server or use the default value (e. g. *mlx41pbx8715a0*).
4. Overwrite the default IP address 192.168.104.13 with your communication server IP address.
5. Enter the subnet mask or use the default value 255.255.255.0.
6. Choose *IPv6 protocol = no* (default value).
7. Overwrite the default gateway IP address 192.168.104.1 with your gateway IP address.
8. Enter the DNS server IP address.
9. Select the DNS server you have just entered.
10. Restart the server with *Reboot Now*, to apply the settings.
11. Wait until the server starts up again. This is the case once the *Application record ID* entry window reappears. Click *Next* and log on again.

**Note**:

If you wish to change the IP address of your Virtual Appliance communication server later, you must do so via the console menu. Although the IP address is visible in WebAdmin, it cannot be changed.

**Activating a trusted network**

**Note**:

This step is only necessary if you wish to access this virtual machine and, thus, the Virtual Appliance communication server, from a PC located on another local area network.

1. After the server is restarted, and the login successfully implemented, select the entry *Manage trusted networks* with the arrow keys via the console menu.
2. To add a trusted network, select the entry *Add IPv4 trusted network*.
3. Enter the IP address area of the local area network, the subnet mask and the IP address of the router via which the added trusted network can be reached.
   - An information window then confirms the area of the local addresses added as trusted addresses.

**Access the Virtual Appliance communication server.**

Congratulations, the installation has now been completed. You can now, as usual, enter your Virtual Appliance communication server IP address in a browser window and see the entry page of WebAdmin for which the sales channel must first be chosen.

The necessary configuration steps for operating the Virtual Appliance communication server with or without satellites are described here Configuring with WebAdmin.

**Mitel Advanced Intelligent Network:**

In an AIN, the Virtual Appliance communication server must always be used as master. Satellites can be deployed as gateway for analogue and digital terminals and interfaces. Satellites may be of Mitel 415, Mitel 430 or Mitel 470 type. The installation of these communication servers, as well as the equipment of interface cards and system modules, is described in the Mitel 415/430 or Mitel 470 system manual.

# Configuration 5

This chapter contains the following sections:



This chapter describes the web-based configuration tool WebAdmin as well as some additional options.

With WebAdmin the installer configures and maintains the MiVoice Office 400 communication server and its auxiliary equipment, and is supported in the process by a set up and configuration assistant. WebAdmin offers different user interfaces for administrators, system assistants and end-users as well as a special application for accommodation and hotels. A context-sensitive online help provides valuable instructions on configuration, and step-by-step instructions.

The chapter ends with valuable information and instructions on how to configure your MiVoice Office 400 communication system.

## 5.1 WebAdmin Configuration Tool

This web-based configuration tool is available for the online configuration of MiVoice Office 400 series communication servers. It offers a simple, user-friendly interface and an online help, and with its different authorization levels it is aimed at different user groups:

Figure 4: WebAdmin Configuration Tool


*Administrator* authorization level:

The Administrator has access to all the views and functions of the configuration tool (*Expert mode*). He can call up a set-up assistant, show a general configuration assistant and a special hospitality configuration assistant, and configure all system parameters. The administrator can switch back and forth between *Expert mode* and *Standard mode* at any time.

Authorization level *Administrator (Standard mode only)*:

In Standard mode the administrator has access to all the main views and functions of the configuration tool. He can call up a set-up assistant, show a general configuration assistant and configure the most needed system parameters.

*System assistant* authorization level:

The System Assistant only sees selected views of the configuration tool, and the scope of functions is limited.

*Hospitality-Administrator* authorization level:

The Hospitality Administrator features all the views required to set up the Mitel 400 Hospitality Manager and the reception menu of the Mitel 6940 SIP, Mitel 6873 SIP or MiVoice 5380 / 5380 IP and specify its default settings. A link can also be used to start the Mitel 400 Hospitality Manager (see Mitel 400 Hospitality Manager).

*Receptionist* authorization level:

This access starts the Mitel 400 Hospitality Manager directly (see Mitel 400 Hospitality Manager).

The WebAdmin is included in the file system of each communication server of the MiVoice Office 400 family and does not have to be installed separately.

Access:

To access the login page of WebAdmin, enter the communication server IP address in your browser. You can find the registration data of a new communication server in the chapter Default user account for initial access.

**Note**:

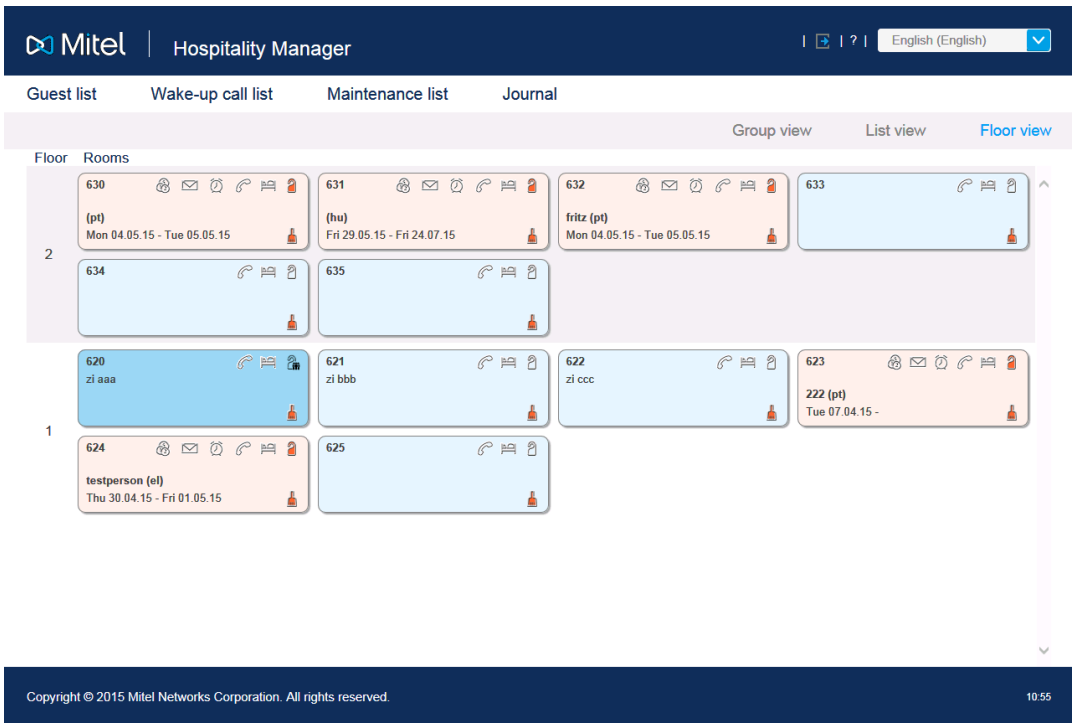
With the web-based administration two users are able to access the same communication server simultaneously (and no fewer than five users at the Receptionist authorization level). This can cause confusion if a configuration is being carried out in the same places.

## 5.1.1 Integrated and auxiliary applications

**Mitel 400 Hospitality Manager**

The Mitel 400 Hospitality Manager is a web-based application for receptionists in the hospitality sector. It provides a clear, at-a-glance list view or floor-by-floor view of the rooms and features functions such as check-in, check-out, notification, wake-up call, retrieval of call charges, maintenance list, etc.

Figure 5: Mitel 400 Hospitality Manager




Mitel 400 Hospitality Manager is integrated into WebAdmin and subject to a licence.

Access:

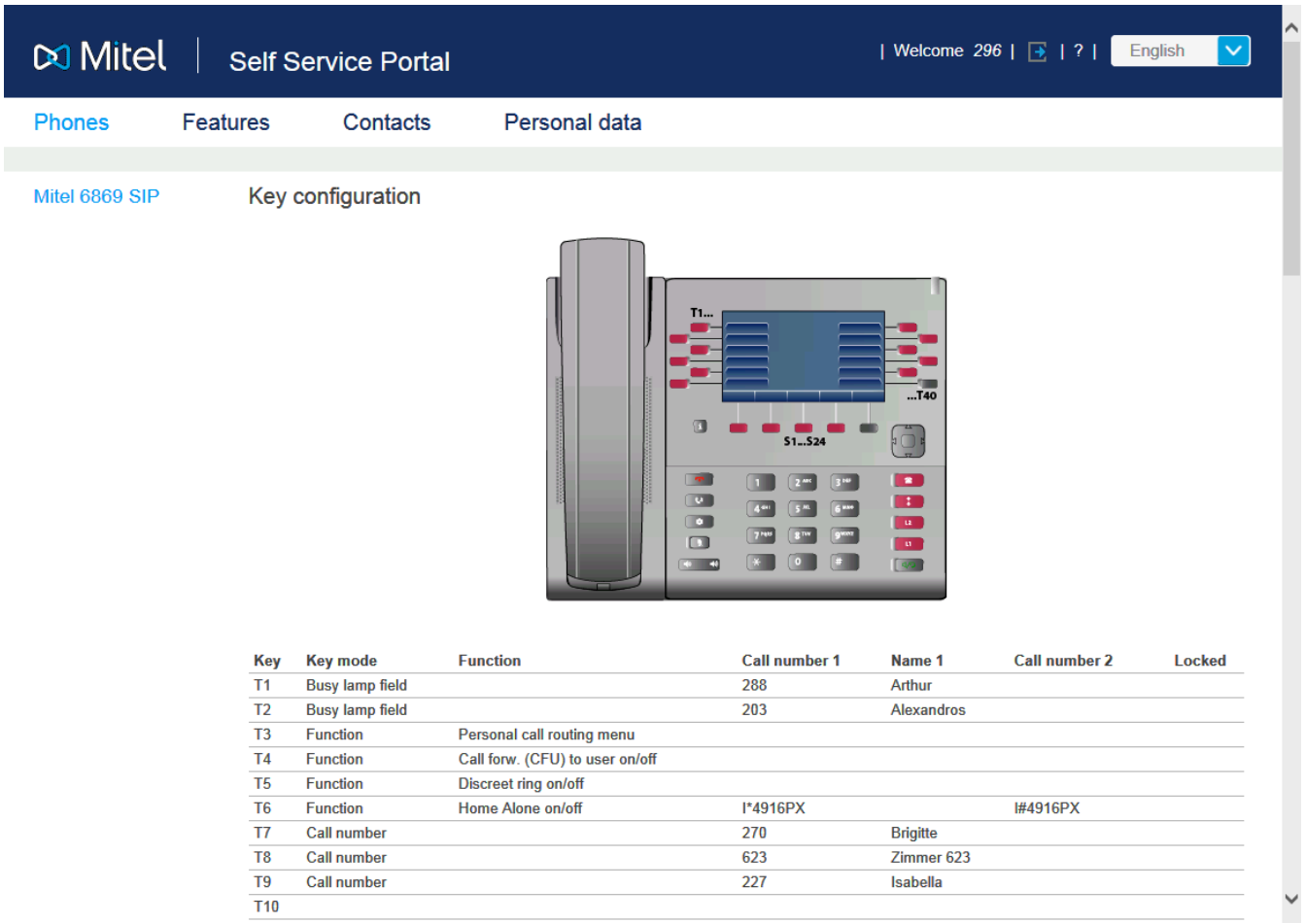
You have access to two types in Mitel 400 Hospitality Manager:

- Register on the WebAdmin registration page with the access data of a user account to which an authorisation profile with the WebAdmin authorisation level *Receptionist* has been assigned. This starts Mitel 400 Hospitality Manager directly.
- Register on the WebAdmin registration page with the access data of a user account to which an authorisation profile with the WebAdmin authorisation level *Hospitality administrator* has been assigned. Click the menu tree on the left side on the *Hospitality Manager* input.

**Self Service Portal**

With the Self Service Portal, users can configure and adjust personal phone settings, such as key configuration, labels, display language, directly and independently on the PC. Users also have access to their personal mail boxes; they can configure and control presence profiles, personal call routing and call transfers, and create or search for private phone book contacts.

Figure 6: Self Service Portal




| Key | Key mode | Function | Call number 1 | Name 1 | Call number 2 | Locked |
|---|---|---|---|---|---|---|
| T1 | Busy lamp field | | 288 | Arthur | | |
| T2 | Busy lamp field | | 203 | Alexandros | | |
| T3 | Function | Personal call routing menu | | | | |
| T4 | Function | Call forw. (CFU) to user on/off | | | | |
| T5 | Function | Discreet ring on/off | | | | |
| T6 | Function | Home Alone on/off | I*4916PX | | I#4916PX | |
| T7 | Call number | | 270 | Brigitte | | |
| T8 | Call number | | 623 | Zimmer 623 | | |
| T9 | Call number | | 227 | Isabella | | |
| T10 | | | | | | |

The Self Service Portal application is integrated into WebAdmin.

Access:You can access a user's Self Service Portal by entering any of the following combinations (registration data) on the WebAdmin registration page:

- Call number + PIN
- Windows user name + PIN
- Windows user name + password

The standard PIN "0000" is accepted, but must be changed during first login. You can choose any 2 to 10-digit number combination.

## 5.2 Access types with WebAdmin

There are the following possibilities to access the MiVoice Office 400 communication server with WebAdmin:

- In the LAN with an Ethernet cable (via a switch)
- Externally via SRM (secure IP remote management)

**Note**:

External access (ISDN/analogue) with a dial-up connection in a AIN via a Mitel 415/430, Mitel SMBC or Mitel 470 Satellite is only recommended on some conditions, for performance reasons.

**Accessing the communication server on the LAN**

If the communication server IP address is known, it can be entered directly in the address line of a web browser. WebAdmin is started after the access data is entered. The computer only needs to be located on the same LAN, but not necessarily on the same subnet.

**Accessing the communication server from outside**

For remote access to the communication server, we recommend SRM (Secure IP Remote Management) secure IP remote management. For this, you need to install an SRM agent on your computer with which you can set up a connection to the SRM server. Thereafter, the SRM server calls the communication server via PSTN and sends it the connection parameters. The communication server now sets up a secure connection to the SRM server which switches together them with the connection to the SRM agent.

**See also:**

You can find instructions on how to set up Secure IP Remote Management in the WebAdmin help on the *IP remote management (SRM)* view (=*mw*).

## 5.3 User access control

Access to the configuration is password-protected. Any user wanting to log in to a communication server is prompted for his user name and password (access data).

### 5.3.1 WebAdmin User accounts and authorization profiles

A user's authorizations are regulated by authorization profiles, which are assigned to the user accounts.

#### 5.3.1.1 User accounts

**Default user account for initial access**

When a new communication server is opened or after a first start, the default user account (*admin*) and several authorization profiles are created. The default user account is linked with the authorization profile *Administrator*. This authorization profile is assigned the administration rights for the *User access control* for *Audio services* and for WebAdmin at the Administrator authorisation level.

The required user accounts and authorization profiles can be set up using the default user account.

To access the default user account (*Default User Account*) enter the following:

**Table 18: Standard user account and standard password**

| | |
|---|---|
| User name | admin |
| Password | After first start, you are asked to enter and confirm a new password for the admin account. |

**Note**:

To prevent unauthorised access to the communication server, it is necessary to modify the default password during first access. For password selection and input, see Password syntax.

**Note**:

- To prevent unauthorised access to the communication server, it is necessary to modify the default password during first access. For password selection and input, see Password syntax.
- The password change is also applied to the login on the virtual machine for the configuration of the Mitel Standard Linux server (see Installing MiVoice Office 400 Virtual Appliance).

### Other predefined user accounts

Furthermore there are predefined user accounts for the Mitel Dialer for MiCollab, for OpenMobilityManager (OMM), and for CloudLink gateway.

You can see the predefined user accounts in the *User account* view.

**Note**:

The predefined user accounts cannot be deleted.

### Personal user accounts

Subject to the administration right for user access control, personal user accounts can be created in user access control and assigned some authorisation profiles. The following rules apply to user names selection and spelling:

- An user name must consist of a minimum of 1 and a maximum of 25 alphanumerical characters.
- Unlike the passwords, the user names are **not** case sensitive.
- The following special characters can be used: ?, /, lt;, >, -, +, *, #, =, full stop, comma and space.
- German umlauts (e.g. ä, ö, ü) and other diacritical characters (e.g. é, à, â) are not permitted.
- User names must be unique throughout the system.
- The user name and password must not be identical.

## 5.3.1.2 Authorization profiles

**Predefined authorization profiles**

The predefined authorization profiles are assigned administration rights and interface user rights. An overview of all predefined authorisation profiles with their administration and access rights is available in the WebAdmin help on the *Authorization profile* view.

**Personal authorisation profiles**

Subject to administration right for the administration right for user access control, no personal authorisation profiles can be protected and assigned the desired rights. A description of the various administration and access rights is available in the WebAdmin help on the *Authorisation profile* view.

**Note**:

Authorization profiles can only be viewed or created by *Administrators* in *Expert mode*.

## 5.3.1.3 Passwords

To ensure that the communication server can only be configured by authorized personnel, access to the configuration is password-protected.

### 5.3.1.3.1 Password syntax

The following rules apply to password selection and spelling:

- A password must consist of a minimum of 8 and a maximum of 255 characters.
- Unlike the 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:?, /, lt;, >, -, +, *, #, =, full stop, comma and space.
- German umlauts (e.g. ä, ö, ü) and other diacritical characters (e.g. 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.

#### 5.3.1.3.2 Change password

Any user who has been assigned an authorisation profile in which the *User access control* administration right is released is authorised to modify the passwords of all user accounts. It is therefore advisable to assign this administration right restrictively.

Users whose password has been changed are prompted to enter their newly assigned password the next time they log in. The same applies to users whose accounts have been newly created.

Users without the administration right *User access control* can only change their own password.

#### 5.3.1.3.3 Access with incorrect password

For user account, after a maximum of 15 unsuccessful logins, the account is disabled for 10 minutes. The account is automatically re-enabled after 10 minutes. The account does not require administrator to re-enable.

#### 5.3.1.3.4 Lost password

If another user has also been defined with the *User access control* administration right released, he can simply overwrite with a new password the password lost by another user. The next time he logs in, the corresponding user is prompted to change the password and enter the new one he has been assigned.

**Note**:

For security reasons, there is no password-free access for Virtual Appliance. Be careful with your passwords.

### 5.3.2 Automatic exit from the configuration

Access to the configuration is interrupted if no changes are made to a parameter value or the navigation system is not used during a specific timeout.

### 5.3.3 WebAdmin access log

An access log with 20 entries is drawn up for each user account so that the history of accesses to the configuration can be tracked. Denied access attempts using erroneous or incorrectly type passwords are also logged. The logs can be read by each user (authorization level) *Administrator* in *Expert mode* required).

**Retrieving the log data**

The system monitors all the accesses and failed access attempts and saves them in the file system of the communication server. These lists can be retrieved locally or remotely.

**CLIP verification**

If in the general maintenance settings of the parameter *CLIP required* is activated, remote maintenance is only possible if the retrieving party is using a CLIP. The CLIP number is also recorded by the access log.

**Entering the processes in the log**

Each access attempt generates an entry in the corresponding list.

In case of remote maintenance an entry will not be generated if remote maintenance is barred or if *CLIP required* is activated in the configuration and no CLIP is received.

## 5.4 WebAdmin remote access

With a remote maintenance access the user is authenticated using his user name and password. The user account must also be assigned an authorization profile in which the interface access *Remote maintenance dial-up access* is enabled. This also applies to SRM (Secure IP Remote Management), secure IP remote management.

### 5.4.1 Access enabled by local users

Remote maintenance access can be enabled in two ways:

- Using function codes (see Function code for remote maintenance access)
- With WebAdmin

It can be revoked again automatically or manually.

All enabling types have equal authorization status. This means that remote maintenance access can be enabled using a function code for example, and then barred again using the WebAdmin in general maintenance settings.

When remote maintenance access is activated, the event message *Remote maintenance* on is sent to all message destinations where the corresponding filter criteria in the assigned event table is set accordingly (see chapter Event tables).

If remote maintenance is released, this can be recognised in the WebAdmin title bar of the  symbol.

Remote maintenance access can be enabled or barred using the function codes both from the idle state and the talk state, e.g. after an enquiry.

The authorisation to activate or bar remote maintenance access using the function code is defined and granted to the user with the parameter *Remote maintenance access* in a permission set.

After a first start of the communication server, the authorizations of all users are restricted.

**Note**:

It is advisable not to keep the remote maintenance access permanently activated. This ensures that the communication server data cannot be manipulated from a remote location by unauthorized persons.

## 5.4.2 Function code for remote maintenance access

**Table 19: Function code for remote maintenance access**

| | |
|---|---|
| Enable/bar a one-off remote maintenance access | *754 / #754 |
| Enable/bar a permanent maintenance access | *753 / #753 |

When remote maintenance access is enabled using function code *754, access will automatically be barred again once the remote maintenance process has been completed. It is possible to bar remote maintenance manually using #754 before it is initiated.

Remote maintenance access can be enabled permanently using the function code *753. To bar access, the authorized user must enter the function code #753 manually.

The enabling or barring of remote maintenance access using the function code is signalled in each case by an acknowledgement tone.

Remote maintenance access can also be enabled or barred in WebAdmin, if the relevant authorization has been given.

**Note**:

In a QSIG network it is important to ensure that the authorization to change the remote maintenance access is also denied to unauthorized PISN users. Otherwise, a PISN user would be able to use an abbreviated dialling number defined for the destination PINX and containing the appropriate function code to change the remote maintenance access to the destination PINX.

**Mitel Advanced Intelligent Network:**

In an AIN the remote maintenance access of all the nodes depends on the setting in the Master. If remote maintenance access is enabled in the Master, both the AIN configuration and the offline configuration of the satellites are enabled.

Remote maintenance access via an external dial-up connection to the AIN is also protected and has to be explicitly enabled via the control panel on the front panel (Mitel 470) or via the control key (Mitel 415/430).

### 5.4.3 Function keys for remote maintenance access

On system phones the function code for enabling/barring remote maintenance access can be stored under a function key, provided the user has the appropriate authorization.

The relevant LED lights up if remote maintenance access is enabled once or permanently.

The relevant LED goes off as soon as remote maintenance access is denied again, either automatically or manually, using the function code or WebAdmin.

## 5.5 Configuring with WebAdmin

The configuration steps are based on the information determined during the planning and, where applicable, the installation.

Whenever possible, use the planning and ordering software Mitel CPQ, to set up your communication system. Mitel CPQ can be operated online after logging in at Mitel MiAccess https://miaccess.mitel.com/. Mitel CPQ not only calculates the required hardware – it also lists the required licences for the planned operation.

**See also:**

If you are setting up an MiVoice Office 400 communication system for the first time, read the chapter Getting started.

**Putting Virtual Appliance into operation**

There are various methods of putting Virtual Appliance without or with a satellite into operation. Below is a summary of a possible procedure for both cases.

### Operating without a satellite

Requirements:

- Your communication server Virtual Appliance has permanent internet access. This is required, because the communication server regularly sends messages to the Mitel licence server, to maintain the permission for the unrestricted operating mode.
- You have received a licence file and an EID for Virtual Appliance via Mitel MiAccess (https://miaccess.mitel.com/) with the help of the voucher.

Recommendation:

Download the latest MiVoice Office 400 software for Virtual Appliance from the *Software Download Center* in Mitel MiAccess (https://miaccess.mitel.com/) and store it.

For the operation, proceed as follows:

1. Enter the IP address of your Virtual Appliance communication server in a browser.
   - WebAdmin is opened in your web browser and shows the *Sales channel selector* view. The sales channel determines the country specific settings of the communication server and ensures the reliable operation with the local PSTN. Choosing the correct Sales channel is also important because it is mapped to the licence code.
2. Select your sales channel. If your country code is not listed, ask your Mitel representative, which sales channel you should select.
3. Click the *Next* button.
   - The *Software update* view is opened. We highly recommend updating the communication server to the latest software release.
4. Choose the *Manual software upload* entry in the drop down list and upload the system software which you have already saved to your hard disc.
   - During the software update (or if you chose not to update the software after you click the *Next* button) a first start is executed to set the sales channel and the country specific settings.
5. Click the *Next* button.
   - The *Upload audio guides* view is opened. The communications server uses spoken text for several purposes like voice mail, presence information or auto attendant. These texts are stored in audio files. You can download audio guide languages via the menu *Localize* in *System Search* and then upload them to the communication server in this view. You can skip this step, because the audio guides can be loaded later from a Mitel FTP-Server via the *Localization* view in WebAdmin much more comfortable.
6. Click the *Next* button.
   - The *First access* view is opened and you are asked to change the default password of the administrator account, to choose the *System language* and to enter a *Site name*.
7. Click the *Next* button.

   The WebAdmin *Setup wizard* is opened. Skip the setup wizard. You can call it up later at any time from WebAdmin.
8. You are asked to select the WebAdmin mode. Click on *Expert mode*.
9. Change to the *System overview* / *Licences* view.

10. Enter the *Equipment ID (EID)* of Virtual Appliance and upload the licence file.
    - The state of *Online licence check* checkbox should be ticked.
11. Enable the *NTP service* in the *System* / *General* view.
12. Change to the *System* / *Media resources* view. Make sure the media switch of the master Virtual Appliance is enabled and select the *VoIP mode*.
13. Restart the communication server in the *Maintenance* / *File management* / *System reset* view, to make the changes take effect.
14. Log on again and change to the *System* / *Media resources* view.
    - The state of the media switch has changed to *Operational*.
15. Now, carry out the configuration procedures to set up the numbering plan, the SIP providers, users, phones and DDIs[31]. For this you can call up the set-up wizard, the configuration wizard or use your own methods.

**Operating with a satellite**

If Virtual Appliance is operated with one or more satellites in a AIN you have two possibilities regarding licensing:

Variant 1: The EID of a satellite and the EID of Virtual Appliance is used to generate the licence. As long as the satellite and the master are connected, the unrestricted operation is ensured. This variant is especially useful, if no permanent internet access for Virtual Appliance can be ensured.

Variant 2: Only the EID of Virtual Appliance is used to generate the licence. This requires a permanent internet access of the communication server Virtual Appliance, because it regularly sends messages to the Mitel licence server in order to maintain the permission for the unrestricted operating mode.

Below the operating with variant 1 is described:

Requirements:

- The installation of the virtual machine has been completed; the Mitel Standard Linux server has been configured and you can access the Virtual Appliance communication server from your local area network (see Installing MiVoice Office 400 Virtual Appliance).
- You have successfully set up a communication server Mitel 415, Mitel 430, Mitel SMBC, or Mitel 470 as a satellite with a static IP address in the same range as the one of the communication server Virtual Appliance.
- You have received a licence file and an EID for Virtual Appliance via Mitel Connect (https://connect.mitel.com) with the help of vouchers and EID of the satellite (gateway EID).

Recommendation:

Download the latest MiVoice Office 400 software for Virtual Appliance from the *Software Download Center* in Mitel MiAccess (https://miaccess.mitel.com/) and store it. The master Virtual Appliance and the satellite must run with the same software release.

For the operation, proceed as follows:

[31] In USA/Canada the abbreviation DID (Direct Inward Dial) is used instead of DDI (Direct Dialling In).

1. Enter the IP address of your Virtual Appliance communication server in a browser.
   - WebAdmin is opened in your web browser and shows the *Sales channel selector* view. The sales channel determines the country specific settings of the communication server and ensures the reliable operation with the local PSTN. Choosing the correct *Sales channel* is also important because it is mapped to the licence code.
2. Select your sales channel. If your country code is not listed, ask your Mitel representative, which sales channel you should select.
3. Click the *Next* button.
   - The *Software update* view is opened. We highly recommend updating the communication server to the latest software release.
4. Choose the *Manual software upload* entry in the drop down list and upload the system software which you have already saved to your hard disc.
   - During the software update (or if you chose not to update the software after you click the *Next* button) a first start is executed to set the sales channel and the country specific settings.
5. Click the Next button.
   - The Upload audio guides view is opened. The communications server uses spoken text for several purposes like voice mail, presence information or auto attendant. These texts are stored in audio files. You can download audio guide languages via the menu Localize in System Search and then upload them to the communication server in this view. If your communication server has internet access, you can skip this step, because the audio guides can be loaded later from a Mitel FTP-Server via the *Localization* view in WebAdmin much more comfortable.
6. Click the *Next* button.
   - The *First access* view is opened and you are asked to change the default password of the administrator account, to choose the *System language* and to enter a Site name.
7. Click the *Next* button.

   The WebAdmin *Setup wizard* is opened. Skip the setup wizard. You can call it up later at any time from WebAdmin.
8. You are asked to select the WebAdmin mode. Click on *Expert mode*.
9. Change to the *System overview* / *Licences* view.
10. Enter the *Equipment ID (EID)* of Virtual Appliance, and upload the licence file.
    - The status of *Online licence check* checkbox should be unticked and the *Gateway EID* of the Satellite should be shown.
11. Enable the *NTP service* in the *System* / *General* view.
12. Change to the *Private networking* / *AIN* / *General* view, add a satellite then enter the Equipment ID and the gateway satellite *IP address*.
    - The satellite is being added.
13. In the same view, on the added satellite's line, click the *WebAdmin* button.
    - A new browser window opens.
14. Log on to the satellite and change to the same *Private networking* / *AIN* / *General* view. Select *AIN satellite* as *operating mode* and indicate the *Master IP address* of the Virtual Appliance communication server.
15. Restart the satellite directly in the popup window or in the *Maintenance* / *File management* / *System reset* view.

16. Wait until the satellite is running again. Then change to the WebAdmin configuration of the master Virtual Appliance, refresh the *Private networking* / *AIN* / *General* view and confirm the satellite.

    - Master and satellite are now networked.

17. Change to the *System* / *Media resources* view. Make sure the media switch of the master Virtual Appliance is enabled and select the *VoIP mode*. Enable the *Standard media switch* of the satellite, select the *VoIP mode* and allocate some audio channels to *VoIP*.
18. Restart the master Virtual Appliance in the *Maintenance* / *File management* / *System reset* view, to make the changes take effect.

    - The master Virtual Appliance and the satellite restart.

19. After master and satellite are running again, log on master Virtual Appliance and change to the *System* / *Media resources* view.

    - The state of the media switch of Virtual Appliance and the standard media switch has changed to *Operational*.

20. Now, carry out the configuration procedures to set up the numbering plan, the SIP providers, users, phones and DDIs[1]. For this you can call up the set-up wizard or configuration wizard, or even use your own methods.

**Setup wizard**

The WebAdmin setup wizard takes you step by step through the setup of a basic configuration and is suitable for initial communication server setup. The setup wizard is automatically called up when a new communication server is installed. Logging on as administrator in WebAdmin (expert or default mode) allows you to also start the setup wizard directly from the WebAdmin navigation tree.

The setup wizard comprises the following steps:

1. Activating licences
2. Viewing the IP addressing
3. Configuring media resources
4. Setting up the numbering plan
5. Setting up SIP providers
6. Setting up users, terminals and DDIs
7. Setting up the auto attendant

For each step you can display a help page or see it in the lower part of the window where it is already displayed. You can skip individual steps of the setup wizard or exit the setup wizard at any time in order to return to the WebAdmin start page.

**Configuration assistant**

The configuration assistant goes further than the setup wizard and helps you to configure a communication system in sequence, from scratch. Logging on as administrator in WebAdmin (expert or default mode) allows you to display the configuration assistant on the WebAdmin start page.

The configuration assistant comprises the following steps:

1. Viewing the IP addressing

2. Regulating access control
3. Checking licences
4. Configuring media resources
5. Setting date
6. Checking network interfaces
7. Setting up SIP providers and accounts
8. Specifying user permissions
9. Create users and DDI[1] numbers
10. Checking outgoing routing
11. Setting up the auto attendant
12. Setting up music on hold
13. Setting up an announcement service
14. Entering abbreviated dialling contacts
15. Saving configuration data

For each step, the upper half of the screen displays the configuration overview; the right-hand side contains notes and instructions about the step you have selected. The WebAdmin online help can be called up for further help.

You can skip individual configuration assistant steps or call up additional views of the WebAdmin navigation tree. To hide the configuration assistant again, untick the control box on the WebAdmin start page.

## 5.6 WebAdmin Configuration Notes

The sections below contain information that may be useful before, during or after a configuration with WebAdmin.

### 5.6.1 Licences

All the features (even those subject to licences) can be configured without a valid licence.

If you use a function or feature that requires a licence but do not actually have the relevant licence, a trial licence is acquired automatically; it is also shown in the overview of activated licences. With a trial licence you can now use the function or feature free of charge for 60 days. The trial licence's expiry date is indicated under *Status*. This procedure can only be used once for each function or feature. Thereafter you must acquire a licence. The licence overview (Virtual Appliance licences on page 55) shows which trial licences are available.

All licences are stored in a licence file, which you can obtain from your authorised dealer. Each licence file can only be used for one communication server. To licence several communication servers, you will obtain separate licence files to match the licence information of the individual communication server. If a communication system consists of several communication servers (e.g. in a AIN), normally only one licence file is required on the Master.

A new communication system must be activated first after commissioning. Otherwise, the communication server changes after 4 operating hours to limited operating mode.

Upload the licence file in the *Licences* view.

If you have received a voucher (or with the help of the *Equipment ID*), you can also obtain the licence file via Mitel MiAccess https://miaccess.mitel.com/ (partner login required). You can find instructions about this in WebAdmin help.

If you wish to use Virtual Appliance in an AIN, you can choose whether licensing will be carried out via *Equipment ID*. (see Virtual Appliance licences).

**See also:**

Licences

## 5.6.2 File management

The file management of the MiVoice Office 400 application is done via WebAdmin:

- *Localization*

  You can adapt the communication system to your country's specifications, with the help of localization. In this view language files can be manually or automatically loaded for Mitel 6800/6900 SIP phones via FTP server. Moreover, you can manually or automatically load the languages for the WebAdmin, Hospitality Manager and Self Service Portal user interface and online help, as well as an external numbering plan for the SIP connection via the FTP server.
- *File system state*

  In this view you can see the thematically structured file system's memory load. In an AIN the file systems for all nodes can be viewed.
- *File browser*

  With the file browser you have access to the communication server file system and create new folders as well as view, import, replace or delete files in the file system.

**Note**:

File management is only accessible for *Administrators* in *Expert mode*.

**See also:**

You can find detailed information about the functions in WebAdmin help for the corresponding view.

## 5.6.3 System reset

### 5.6.3.1 Restart

**Restart via WebAdmin**

A restart via WebAdmin is triggered in the maintenance settings with the *Restart* button in the *System reset* view.

A restart via WebAdmin reboots the MiVoice Office 400 application only. The configuration data is preserved.

**Note**:

- The restart is triggered immediately. All the active call and data connections are interrupted.
- With a restart via WebAdmin you only restart the Virtual Appliance communication server application. In some rare cases, it is necessary to also restart the corresponding virtual machines. Restarting the virtual machine also restarts the Virtual Appliance communication server application.

### Restarting the virtual machine

Should the virtual machine stop running (correctly) for whatever reason, it must be restarted. To do so proceed as follows:

**Note**:

Restarting the virtual machine also restarts the communication server. The restart is triggered immediately. All the active call and data connections are interrupted.

vSphere virtualization:

1. Start the vSphere client and enter the ESXi server user name and password.
2. Select your virtual machine from the list.
3. Choose via the menu *Restart guest* or click on .

- The virtual machine restarts, together with the communication server.
- After approx. two minutes, WebAdmin can again be used to access the Virtual Appliance communication server.

Hyper-V virtualization:

1. Start the Hyper-V manager on the server.
2. Select your virtual machine from the list.
3. Choose *Restart* via the menu.

- The virtual machine restarts, together with the communication server.
- After approx. two minutes, WebAdmin can again be used to access the Virtual Appliance communication server.

### 5.6.3.2 First start

A first start has the effect of resetting the MiVoice Office 400 communication server from scratch. The system-specific data such as the system ID, system type, sales channel, licence file, and software generation are preserved.

**Note**:

- A first start deletes all the configuration data already stored and replaces it with the default values of the sales channel. Therefore, back up your configuration data before a first start.
- The first start is triggered immediately. All the active call and data connections are interrupted.

**First start via WebAdmin**

A first start via WebAdmin is triggered in the maintenance settings with the *First start* button in the *System reset* view.

**First start via front panel**

**First start and reset sales channel via WebAdmin**

With the *First start and reset sales channel* button in the maintenance settings of the WebAdmin *System reset* view, you have the possibility not only to execute a first start but also to delete the sales channel. During the next start, you will be prompted for the sales channel and licence file. Note that the licence file is dependent on the sales channel. This means you can no longer use the existing licence file, if you choose another sales channel.

**Note**:

This function is only accessible for Administrators in Expert mode.

## 5.6.4 Data backup

With a configuration data backup all the MiVoice Office 400 configuration data of the communication server is stored in a compressed file in ZIP format. You can let the configuration data backup run automatically (*Auto backup*) or as required (*Manual backup*).

You can automatically copy the backup files to an FTP server or e-mail them.

With an audio data backup all the audio data of the communication server is backed up in a compressed file in ZIP format. The backup of the audio data can only be done manually.

You can find the automatic data backup and distribution service settings in the WebAdmin *Maintenance*/*Data backup* view where you can also test the configuration. Moreover, in this view, you can see the automatically and manually created backup files and also restore or delete them.

The configuration backup and the audio data backup are always stored in a encrypted format.

**Note**:

The backup may consist of several files. They are compiled by the communication server and compressed into a ZIP file. During the Restore process the ZIP file is extracted by the communication server itself. To ensure the restore process to run smoothly, make sure you do not modify the ZIP file. Never extract or modify a backup file yourself.

### 5.6.4.1 Auto backup

The automatic data backup function creates a backup of the MiVoice Office 400 configuration data at regular intervals and saves the backup files on the communication server's file management system.

The Auto Backup function creates a backup of the configuration data at daily, weekly and monthly intervals:

- Everyday at the set time a backup is created and stored in the *..\backup\day* directory.
- When the week changes, a copy of the backup is stored in the *..\backup\week* directory.
- When the month changes, a copy of the backup is stored in the *..\backup\month* directory.

The backup directories are located on the file system of the communication server and are directly accessible via the *File browser* or with an FTP connection.

A backup remains stored until the set storage time has expired; the *.zip file* is then deleted from the file system.

### 5.6.4.2 Distribution service

You can use the distribution service to automatically copy the backup files to an FTP server or e-mail them.

- The e-mail distribution service sends a copy of each backup file created to a preconfigured e-mail address.
- The FTP distribution service stores a copy of each backup file created on an FTP server.

### 5.6.4.3 Manual backup

Configuration and audio data must be stored separately and stored as *.zip* files on any data carrier you want. The configuration data is also backed up automatically as copy on the communication server file system.

Situations in which you have to create a manual backup:

- Before running a first-start of the communication server (a first start resets all the configuration data to their default values and deletes all audio data).
- Before making a new installation of the virtual machine (a new installation resets all configuration data to the default value and deletes all audio data).
- Before and after any major configuration changes.

#### 5.6.4.4 Restore backup

The available MiVoice Office 400 configuration data and audio data backup files can be restored at any time.

**Note**:

- Restoring a backup irretrievably overwrites the current configuration data or audio data.
- Restoring a backup also resets the users' presence status, the personal routing settings and any activated CFUs to the backup status.
- Some configuration changes only take effect after a restart. The communication server is restarted after the configuration data is restored.

**See also:**

The procedure for creating and restoring a backup is described in detail in the WebAdmin help in the *Data backup* view.

### 5.6.5 Importing and exporting configuration data

You have the possibility to edit various configuration data outside WebAdmin, or to import configuration data from other MiVoice Office 400 series communication systems. Here you can create, with the help of the export function, a specific Excel file hereinafter referred to as *Export file*. The export file contains several spreadsheets. Each sheet covers a specific configuration area. Subsequently, edit then re-import the export file. Only the data belonging to the view, on which you have activated the import function, will be imported. Example: The import function in the *Phone book* / *Public* view imports only the data from the export file located on the spreadsheet *Abbreviated dialling list*.

Exception: The export function in the *Backup* view imports the data in all spreadsheets.

You can find the export function in the following views:

- *Overview* (user data and key configuration of the terminals)
- *Abbreviated dialling numbers*
- *PISN user*
- *Time controlled functions*
- *Ext./Int. Allocation*
- *LCR*
- *Blacklist*

- *CLIP based routing*
- *Data backup*

> **Note**:
>
> You can activate the *Replace existing configuration* option with the import function. Activate this function only if you are setting up the communication server from scratch. This action deletes all previously configured user data and all user associated settings such as DDI numbers, CDE targets, user group entries, assigned phones, configured keys, etc.

### 5.6.6 Mitel 6800/6900 SIP phones

Prior to the registration, reset any phones that were already in operation back to the factory setting. For security reasons, delete the phone's MAC address in WebAdmin. This prevents problems during registration.

Use these procedures in the following cases:

- Assigning the phone to another user on the same system
- Transferring the phone to another system with the same software release
- Changing the software release to an earlier release
- Changing the communication server IP address

# Operation and Maintenance 6

This chapter contains the following sections:



This chapter describes maintaining the system and configuration data as well as updating the system software. Moreover, operations supervision is described with the event message concept.

## 6.1 Data Maintenance

### 6.1.1 File system of the communications server

The file system of the communication server comprises the system software, the software for system phones, the system and terminal configuration data, the audio data, system logs, data for WebAdmin, etc. With WebAdmin you have access to the file system via the menu item *File management*. You can see the file system memory load and then load audio data, languages for the user interface and online help, language files for Mitel 6800/6900 SIP phones as well as an external numbering plan for SIP connection. Moreover, with the file browser you have the possibility to view, upload, replace or delete the folders and files in the file system.

Functions for backing up and restoring configuration data and audio data are available in the WebAdmin *Maintenance* / *Data backup* view (see also Data backup).

Usually there is no need to access the MiVoice Office 400 file system directly as all needed functions are available in WebAdmin. For special cases you can access the MiVoice Office 400 file system also with a SSH session via the folder */home/mivo400*.

**Note**:

Modifying or deleting files on the file system can result in a system that is no longer able to run.

### 6.1.2 Updating configuration data

There are system-wide, user-related and terminal-related configuration data:

- System-wide configuration data can only be modified with WebAdmin.
- Terminal configuration data such as key assignments or ringing melodies can be modified either directly on the terminal, with Self Service Portal or with WebAdmin. With some system phones configuration is also possible using the web user interface or with the help of configuration files.

- User-related configuration data such as private contacts or CFUs is valid for all the terminals assigned to the user and can be configured using WebAdmin, partly via Self Service Portal, or directly on the terminal itself.

Access to the configuration data via WebAdmin is regulated by a User Access Control with user accounts, authorization profiles and authorization levels. More information can be found in the Chapter User access control.

## 6.2 Update Software

### 6.2.1 System software

**MiVoice Office 400 application software**

The MiVoice Office 400 application software is normally updated with WebAdmin. In some exceptional cases, it is necessary to reinstall the entire virtual machine via an OVA file or a VHF file (see page Installing MiVoice Office 400 Virtual Appliance on page 70).

**Note**:

Fresh installation with an OVA file or a VHF file resets all configuration data to the default values and deletes all audio data. First create a backup of the configuration and audio data (see Chapter Data backup).

**Firmware for system terminals**

The firmware for MiVoice 5300/MiVoice 5300 IP, Mitel 600 DECT phones, DECT phone Office 135/135pro, DECT radio units SB-4+/SB-8/SB-8ANT and WebAdmin is also available in the MiVoice Office 400 application software.

**Providing the MiVoice Office 400 system software and licence file**

The new MiVoice Office 400 system software and the relevant licence file are provided by your sales dealer. In most cases you will download the software from an internet site specified by your sales partner. You will also receive a voucher. With this you can generate the new licence file through the Mitel MiAccess internet portal https://miaccess.mitel.com/ and upload it to your communication system. You need a login to access Mitel MiAccess (user name and password).

**Load new MiVoice Office 400 system software with WebAdmin**

New MiVoice Office 400 system software can conveniently and safely be loaded on the communication server file system in the WebAdmin *Maintenance* / *System software* view. The activation point of the new software is selectable. (Exception: The activation time on the satellites AIN always depends on the master's demand).

In newly delivered systems it is possible to directly load new system software after choosing the sales channel.

**Note**:

- Most times a new licence file is also required for new system software. You can also install and start up the new software without specifying the licence file. However, once you have started to use the software you will need to enter the licence file within 4 hours; otherwise the communication server will switch over to the restricted operating mode. In this mode, only the basic functions of the communication server are available.
- Please read the chapter “Important hints and restrictions” in the release notes to the software to be loaded.

**See also:**

A detailed description of the software upload procedure with WebAdmin is available in the online help.

## 6.2.2 Firmware for corded system phones

The MiVoice Office 400 application software package contains the software for certain system phones (DSI and IP), which is updated in each case along with the application software. For other system phones (SIP) the firmware is located on a firmware server.

The MiVoice 5360 system phones do not have their own memory. All other system phones have a Flash memory.

**SIP system phones**

The firmware for Mitel 6800/6900 SIP phones and Mitel Dialer is preferably located on a firmware server. In the WebAdmin *Configuration* / *IP network* / *Firmware server* view Mitel FTP servers are already predefined. Various firmware releases are stored on this server, according to different communication server software releases. The predefined entry in WebAdmin is adjusted to each communication server release if necessary. You can also indicate the address of another firmware server.

Whenever the phones are started the phone firmware version is compared with the version on the firmware server. If the versions differ, the firmware is downloaded from the firmware server to the phones.

**DSI and IP system phones with Flash memory**

The flash memory contains the boot software and the application software. DSI phones also have an area with the interface software.

The firmware for the phones MiVoice 5370, MiVoice 5380 as well as for all MiVoice 5300 IP series phones is contained in the MiVoice Office 400 application software package. The firmware versions are compared when the phones are started. If the versions differ, the firmware is downloaded from the communication server to the phones. When updating the system software this can take several minutes for each DSI phone.

The expansion key modules MiVoice M530 and MiVoice M535 also have a flash chip containing firmware. The update mechanism is the same as the one described above. However a local power supply is always required (Power over Ethernet is also possible with IP terminals).

## 6.2.3 Firmware System MiVoice Office 400 DECT

**DECT radio units SB-4+, SB-8 and SB-8ANT**

The Flash memory on the radio units contains an area that cannot be modified. It is used for starting the radio unit and receiving the firmware for the radio unit.

The actual firmware for the radio unit is contained in the MiVoice Office 400 application software package. The loaded firmware is tested when the radio unit starts up. If the loaded firmware is not identical to the version in the system software, the firmware will be downloaded from the communication server on to the radio unit and stored in the Flash memory of the radio unit.

**Cordless DECT phones of the Mitel 600 DECT family**

The firmware for the Mitel 600 DECT cordless phones, is updated via radio (Air-Download). The update can be enabled or disabled individually for each cordless phone using the menu *System - Download server* on the cordless phones. If the cordless phone is logged on to several systems, this menu defines which system the firmware update is relevant to.

There is only one firmware for the cordless Mitel 600 DECT series phones. It is included in the MiVoice Office 400 application software package and stored in the file system of the communication server.

**DECT cordless phones Office 135 and Office 160**

The firmware for the Office 135 and Office 160 cordless phones, is updated via radio (Air-Download). This requires the cordless phone to be logged on to system A.

The memory in the cordless phones is a Flash memory. The Flash memory contains an area that cannot be modified. This area contains the cordless phone's boot software.

The firmware for the cordless phones is contained in the MiVoice Office 400 application software package. The loaded firmware is tested when the cordless phone starts up. If the loaded firmware is not identical to the version in the system software, the system will initiate an Air-Download. The firmware is loaded from the communication server onto the cordless phones via radio and stored in the Flash memory.

To be able to run an Air-Download, you need to ensure that the cordless phone contains a functional firmware.

The cordless phone remains fully functional during an Air-Download. The new loaded firmware is activated only once the Air-Download has been successfully completed. A restart is carried out on the cordless phone.

## 6.2.4 Firmware System Mitel SIP-DECT

With Mitel SIP-DECT and Mitel 600 DECT series phones comprehensive solutions can be provided for wireless telephony on IP-based networks. This requires RFP radio units that can be directly connected to other VoIP devices on the LAN. OpenMobilityManager (OMM) is installed on one of the RFP radio units

or on a PC, which constitutes the management interface for the Mitel SIP-DECT solution. Mitel 600 DECT phones have loaded a different firmware in an Mitel SIP-DECT system from the one in an MiVoice Office 400 DECT system.

The firmware for the RFP radio units and for the Mitel 600 DECT cordless phones is preferably located on a firmware server. Automatic firmware update is then possible. The WebAdmin *Configuration* / *System* / *DECT/SIP-DECT* / *SIP-DECT* view contains a global predefined Mitel FTP (Mitel 6700 SIP phones, Mitel Blustar clients and Mitel Dialer) / HTTPS (Mitel SIP 6800/6900 phones) server. Various firmware versions are stored on this server, according to different communication server software releases. The predefined entry in WebAdmin is adjusted to each communication server release if necessary. You can also indicate the address of another firmware server.

Firmware designations for Mitel SIP-DECT (examples):

aafon6xxd.dnld:

Firmware for Mitel 600 DECT cordless DECT phones.

iprfp3G.dnld:

iprfp4G.dnld

Firmware for OpenMobilityManager (OMM).

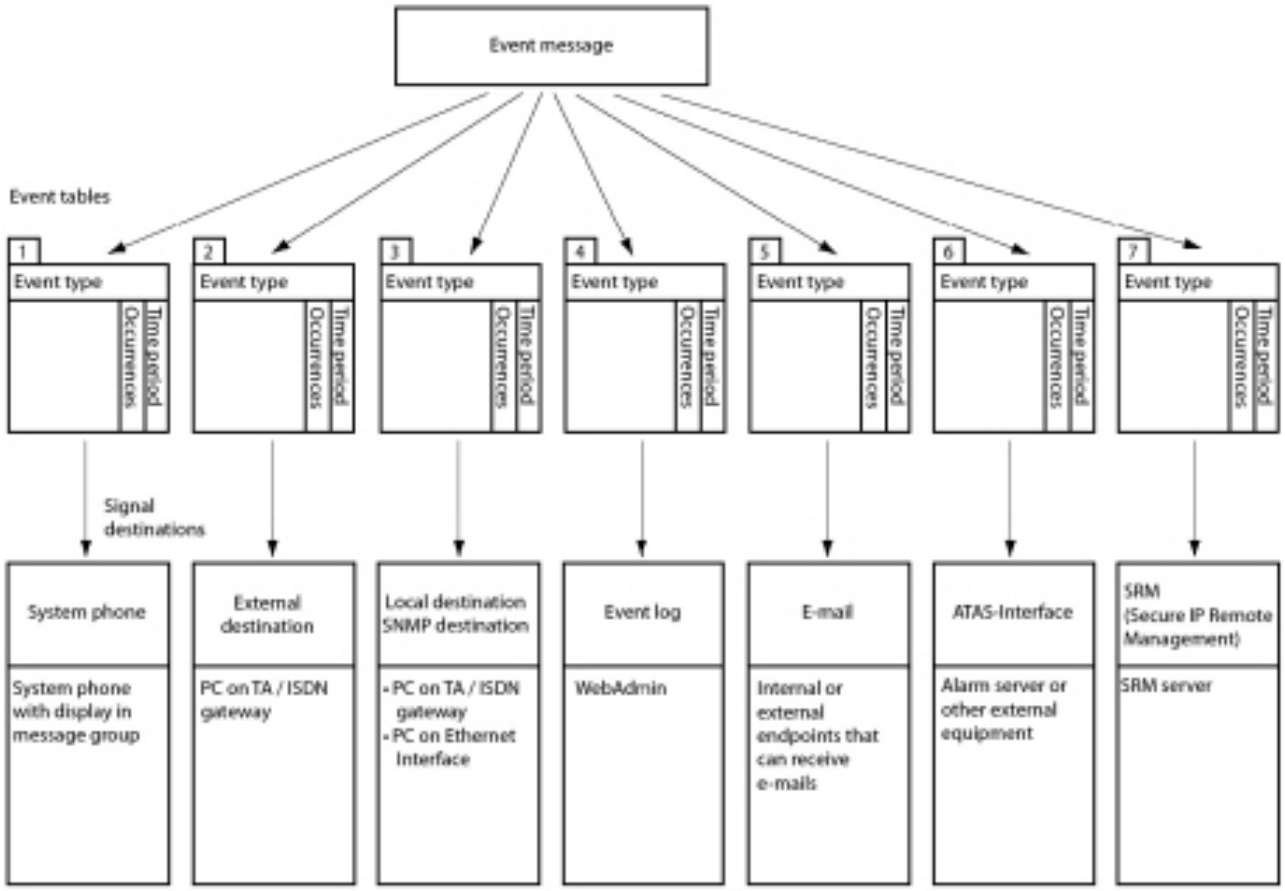
## 6.3 Operations supervision

### 6.3.1 Event message concept

The system 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.

There are 7 event tables that can be allocated to 8 signal destinations:

Figure 7: Distribution principle for an event message




## 6.3.1.1 Event types

Event messages have a certain severity level: *Normal* (blue), *Serious* (yellow) and *Critical* (red). Many event messages have both a negative impact (error occurred) and a positive impact (error corrected). Some event messages have no impact and, thus, no match. Severity level, positive or negative impact (if any) and the information, if there is a match or not, are indicated in the event table.

If an SRM server is indicated as signal destination, the event message severity level results in a change of system status. This can be seen in the SRM agent and is displayed with the corresponding colour (see also section SRM destination).

**Table 20: Event types, in alphabetical order**

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *ATAS: Connection established* | ATAS: connection (re) established | Date, time | critical (positive, with match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *ATAS: Connection lost* | ATAS: connection lost | Cause (0: Logoff, 1: missing cycle signal), date, time | critical (negative, with match) |
| *Card in service* | A card that was previously out of service is back in service again. | Number of the expansion slot, date, time | critical (positive, with match) |
| *Card out of service* | A card previously in operation has stopped functioning. | Number of the expansion slot, date, time | critical (negative, with match) |
| *Card reset* | A reset was carried out for one card | Number of the expansion slot, date, time | Serious (without match) |
| *Charge counter overflow* | Individual cumulative counter or cost centre counter overflow | Cause (0: User / 1: Cost centre / 2: Exchange line / 3: Room), number, date, time | Serious (without match) |
| *CL printer available again* | Printout on the system printer available once again | Date, time | Serious (positive, with match) |
| *CL printer blocked* | • No response from system printer for past 4 minutes<br>• Printer out of paper or switched off | Interface, interfaces/card number, port number, date, time | Serious (negative, with match) |
| *Compatible PMS application* | The external hotel management system (PMS application) is suitable for communicating with the communication server. | Date, time | critical (positive, with match) |
| *Configuration template available* | The missing configuration template for a Mitel SIP terminal is now available in the communication server file system. | Date, time | Serious (positive, with match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *Connection to IP remote management (SRM) failed* | IP remote management connection set up (SRM = Secure IP Remote Management) has failed.<br><br>Cause parameter:1: Connection attempt failed, 2: Authentication failed, 3: File upload rejected | Cause, date, time | Normal (negative, with match) |
| *Connection to IP remote management (SRM) restored* | IP remote management connection has been (SRM = Secure IP Remote Management) successfully restored. | Date, time | Normal (positive, with match) |
| *Connection to PMS system established* | A connection with a hotel management system (PMS system) has now been successfully established. | Date, time | critical (positive, with match) |
| *Connection to PMS system failed* | An unsuccessful attempt was made to establish a connection with a hotel management system (PMS system).Reason: 1: Call rejected, 2: Destination unobtainable, 3: Destination busy, 4: Connection timeout, 5: Wrong address, 6: Unknown error | Error, date, time | critical (negative, with match) |
| *CPU2 applications card Data communication out of service* | Data communications with the CPU2 applications card have been interrupted for an unusually long period of time (> 1 hour) due to an error (after a Windows update or for other reasons). | Date, time | critical (negative, with match) |
| *CPU2 applications card Data communications back in service* | Data communications with theCPU2 applications card have been restored. | Date, time | critical (positive, with match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *Creation instance on backup communication server failed* | The backup communication server was unable to create or modify a user or terminal instance with the received configuration data.<br><br>**Note**:<br>This event message is generated by the backup communication server. | Instance type (0: User, 1: terminal), user number or terminal ID, date, time | critical (negative, with match) |
| *Creation instance on backup communication server successful* | The backup communication server was able (following one or more previous failed attempts) to create or modify a user or terminal instance with the received configuration date.<br><br>**Note**:<br>This event message is generated by the backup communication server. | Instance type (0: User, 1: terminal), user number or terminal ID, date, time | critical (positive, with match) |
| *CSTA sessions within the licence limit again* | *CSTA Sessions* licences are now available again. | Number of licences, date, time | Serious (positive, with match) |
| *CTI first party Connection established* | The first-party link was (re-)established | User number, terminal ID, protocol type (0=ATPC3, 1=CSTA) date, time | critical (positive, with match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *CTI first party Connection lost* | The first-party link was interrupted because the cycle signal is missing. | User number, terminal ID, protocol type (0=ATPC3, 1=CSTA) date, time | critical (negative, with match) |
| *CTI third party: Connection established* | The third-party link was (re-)established | IP address, protocol type (0=ATPC3, 1=CSTA), date, time | critical (positive, with match) |
| *CTI third party: Connection lost* | The third-party link was interrupted | Cause (0=Logoff, 1= missing cycle signal), IP address, protocol type (0=ATPC3, 1=CSTA) date, time | critical (negative, with match) |
| *Definitive activation licence missing* | The initial temporary activation of the communication server for a certain duration (e.g. 90 days) was started. After this period, the communication server switches to restricted operating mode (see Restricted operating mode). | Date, time | critical (negative, with match) |
| *Definitive activation licence now present* | A licence file with a definitive activation licence was uploaded. | Date, time | critical (positive, with match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *Dual Homing back within the licence limit* | There are now enough licences available for registering SIP phones in the Mitel 6800/6900 SIP series on a backup communication server.<br><br>**Note**:<br>This event message is generated by the backup communication server. | Date, time | Serious (positive, with match) |
| *E-mail successfully sent* | The system has now successfully sent an e-mail.<br><br>Meaning of the parameter values in Meaning of the parameter values for the event message Send e-mail failed | Cause/ action=0000, e-mail client, additional information, date, time | critical (positive, with match) |
| *Emergency call ended* | The emergency call has been confirmed by a responsible person. | Date, time | critical (positive, with match) |
| *Emergency call started* | An emergency number out of the public emergency number list has been dialled.<br><br>**Note**:<br>If an emergency number of the internal numbering plan has been dialled, no event message will be generated. | Dialled number (the first 4 digits), user number, terminal ID (if user number ≠ 0) or trunk group ID (if user number = 0), date, time | critical (negative, with match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *ESME reachable* | The LAN connection between the SMSC and the ESME is now available | IP address, date, time | critical (positive, with match) |
| *ESME unreachable* | The LAN connection between the SMSC and the ESME is interrupted | IP address, date, time | critical (negative, with match) |
| *Ethernet activated again* | The overload on the Ethernet interface no longer exists. The interface has been reactivated. | Date, time | Normal (positive, with match) |
| *Ethernet deactivated due to high load* | The system has detected an overload on the Ethernet interface. The interface is temporarily deactivated. | Date, time | Normal (negative, with match) |
| *External auxiliary power supply failed* (Mitel 470 only) | The external auxiliary power supply to the communication server has failed. If the auxiliary power supply unit has been used for redundant operation, there are no short-term limitations. If the auxiliary power supply unit has been used to increase the power supply, the internal power supply unit overflow must be calculated. | Date, time | Serious (negative, with match) |
| *External auxiliary power supply in service* (Mitel 470 only) | The external auxiliary power supply to the communication server is working. | Date, time | Serious (positive, with match) |
| *External event message destination not reachable* | External signal destination not automatically reachable | Cause (0: Busy /1: Not available /2: (not used), 2: Barred /3: not defined), date, time | Serious (negative, with match) |
| *External event message destination reachable* | External signal destination is now reachable | Date, time | Serious (positive, with match) |
| | | | |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *Fan failure* (Mitel 470 only) | The fan is jammed or defective or the connection is no longer making contact.<br>• Parameter 1 = 0: No more fans in operation.<br>→ Risk of overheating: System shut down after 2 minutes.<br>→ Replace both fans.<br>• Parameter 1 = 1: Only one fan left in operation.<br>Parameter 2 = Defective fan number<br>→ System still running with only one fan.<br>→ Replace defective fan. | Parameter 1, parameter 2, date, time | critical (negative, with match) |
| | | | |
| *Fan in operation* (Mitel 470 only) | The fan is back in service again after a failure.<br>• Parameter = 0: A fan is back in service again.<br>• Parameter = 1: Second fan back in service again. | Parameter, date, time | critical (positive, with match) |
| *FIAS command buffer full* | The command buffer to the PMS interface is full. | Date, time | critical (negative, with match) |
| *FIAS interface usable again* | The command buffer to the PMS interface is back below the critical limit. | Date, time | critical (positive, with match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *Inactive radio unit port* | Radio unit not responding Reason: 0: Startup running, 1: Not registered, 2: Various nodes, 3: Port not permitted, 4: Local power supply, 5: Not connected, 6: Port reset, 7: Startup error, 8: Unknown error | Card number, port number, radio unit ID/reason, date, time | Serious (negative, with match) |
| *Incompatible PMS application* | The external hotel management system (PMS application) is not suitable for communicating with the communication server. | PMS SW version, PMS interface version, PMS interface driver version, date, time | critical (negative, with match) |
| | | | |
| *Insufficient bandwidth* | An user in an AIN is trying to set up a connection and the bandwidth currently available with the WAN link is insufficient. | Link ID, WAN link name, available bandwidth in Kbit/s, date, clock | Serious (without match) |
| *Internal event message destination not reachable* | Local output blocked or not available | Cause (0: Busy /1: Not available /2: (not used), 2: Barred /3: not defined), date, time | Serious (negative, with match) |
| *Internal event message destination reachable* | Local output available once again | Date, time | Serious (positive, with match) |
| *Internal power supply unit failed* (Mitel 470 only) | The internal power supply unit of the communication server has failed. If the auxiliary power supply unit has been used for redundant operation, there are no short-term limitations. If the auxiliary power supply unit has been used to increase the power supply, the external power supply unit overflow must be calculated. | Date, time | Serious (negative, with match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *Internal power supply unit in service* (Mitel 470 only) | The internal power supply unit of the communication server is in service. | Date, time | Serious (positive, with match) |
| *IP address added to the DoS black list* | A DoS attack has taken place beyond the maximum configured admissible registration attempts or transactions. The IP address concerned has been included in the black list and will remain blocked for a set period. | IP address, Cause (0: Registration / 1: Too many transactions / 2: No session / 3: modified message), date, time | Serious (negative, with match) |
| *IP address changed: Regenerate TLS certificates* | The IP address of the communication server has changed. The TLS certificates have to be regenerated. For terminals downcircuit from a NAT without ALG the public NAT gateway address has to be configured. | Date, time | Serious (without match) |
| *IP address removed from the DoS black list* | An IP address added previously due to a DoS (Denial of Service) attack was again removed from the black list and is no longer blocked. | IP address, date, time | Serious (positive, with match) |
| *IP phone: Connection lost* | An IP system phone is no longer connected to the communication server. | User number, terminal ID, date, time | Serious (negative, with match) |
| *IP phone: Connection re-established* | An IP system phone has re-established the connection to the communication server. | User number, terminal ID, date, time | Serious (positive, with match) |
| *IP system phone licence is now available* | A sufficient number of licences is now available again for MiVoice 5361 IP / 5370\ IP / 5380 IP. | Date, time | Serious (positive, with match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *Language file download failed* | The downloading of a language file via FTP server for an MitelSIP terminal has failed. | Parameter 1: FTP server address, Parameter 2: Language file type and name, date, time | Serious (negative, with match) |
| *Language file download successful* | The downloading of a language file via FTP server for an Mitel SIP terminal has been successfully completed. | Parameter 1: FTP server address, Parameter 2: Language file type and name, date, time | Serious (positive, with match) |
| *LCR on alternative network provider* | Automatic switch from primary network provider to secondary network provider using LCR function. | Provider ID, date, time | Normal (without match) |
| *Licence available for configured user* (Mitel 470 and Virtual Appliance only) | This event message is generated, if all configured users have a user licence (which was not the case before). | Date, time | Serious (positive, with match) |
| *Licence for integrated mobile/external phone available* | A sufficient number of licences is now available again for integrated mobile/external phones. | Date, time | Serious (positive, with match) |
| *Licence for PMS interface available* | The *Hospitality PMS Interface* licence or a sufficient number of *Hospitality PMS Rooms* licences are now available. | Date, time | Serious (positive, with match) |
| *Licence invalid, restricted operating mode 4 hours after restart* | The system software loaded requires a software release licence. Without this licence the system software's functionality is severely restricted 4 hours after the restart. | Date, time | Serious (without match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *Licence missing for configured user* (Mitel 470 and Virtual Appliance only) | This event message is generated, if one or more configured users have no user licence.<br><br>**Note**:<br>To avoid a flood of messages this event message is generated only once (the first time a user is created without a user licence) | Date, time | Serious (negative, with match) |
| *Licences for offline operations expired* | The maximum period of 36 hours for the temporary licence activation has expired. | Date, time | Critical (without match) |
| *Link to gateway satellite lost* (Virtual Appliance only) | The communication server has lost the link to the gateway satellite. Without this link, the communication server switches to restricted operating mode after xx hours. | Number of hours until restricted operating mode, date, time | critical (negative, with match) |
| *Link to gateway satellite restored* (Virtual Appliance only) | The communication server has been able to restore the link to the gateway satellite. | Date, time | critical (positive, with match) |
| *Link to the licence server (SLS) has failed* (Virtual Appliance only) | It has been impossible for a long time to set up a link to the licence server. The system switches to restricted mode after a variable timeout (max. 72 hours). | Date, time | critical (negative, with match) |
| *Link to the licence server (SLS) has restored* (Virtual Appliance only) | It has been possible to restore a link to the licence server. | Date, time | critical (positive, with match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *Local supply error on radio unit* | Local power supply of a SB-4+ / SB-8 / SB-8ANT radio unit failed or unavailable | Card number, port number, date, time | critical (negative, with match) |
| *Local supply on radio unit available* | Local power supply of a SB-4+ / SB-8 / SB-8ANT is now again available | Card number, port number, date, time | critical (positive, with match) |
| *Mains voltage failure* | Event message once mains power is restored<br>• Mains power has failed more frequently than entered in the trigger table | Date, time | Serious (without match) |
| *Malfunction* | A hardware or software error has occurred. The error ID can help Support to pinpoint the possible cause of the error. | Error ID, date, time | Serious (without match) |
| *MiCollab: Terminal limit has been reached* | A MiCollab terminal could not be linked to a user because a limit has been reached (reason).<br>reason = 0: Too much terminals per system<br>reason = 1: Too much terminal per user<br>reason = 2: Too much MiCollab clients per user | User number, reason, date, time | Serious (negative, with match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *MiCollab: Within the terminal limits again* | A MiCollab terminal could now be linked to a user because it is within a limit again (reason).<br><br>reason = 0: Terminals per system OK again<br><br>reason = 1: Terminal per user OK again<br><br>reason = 2: MiCollab clients per user OK again | User number, reason, date, time | Serious (positive, with match) |
| *Mitel Dialer within the licence limit again* | *Mitel Dialer* user licences are now available again. | Date, time | Serious (positive, with match) |
| *Mitel SIP terminals within the licence limit again* | *Mitel SIP Terminals* and *Mitel 8000i Video Options* licences are now available. | Parameter 1=1: Mitel SIP Terminals licence, Parameter 2=1: Mitel 8000i Video Options licence, date, time | Serious (positive, with match) |
| *Monitor event* | Monitor event | Monitor Type, Date, Time | Normal (without match) |
| *No configuration template* | A configuration template for a Mitel SIP terminal is missing in the communication server file system. Without the configuration template, no configuration file can be generated for this terminal type. | No configuration template, date, time | Serious (negative, with match) |
| *No DECT DSP channels available* | DECT channels on DSP-0x overloaded | Date, time | Normal (without match) |
| *No DTMF receiver available for integrated mobile/external phones* | A permanent DTMF receiver (for detection suffix dialling function codes) could not be assigned to an integrated mobile/external phone with enhanced functionality. | BCS Ref., date, time | Serious (without match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *No other system clone detected* (Virtual Appliance only) | The clone detection service on the licence server (SLS cloud) could not find any other clone (system with the same EID) for a long time (24 hours). | Date, time | critical (positive, with match) |
| *No response from network* | No answer to Call Setup on BRI-T/ PRI interface | Port number of the exchange line circuit, date, time | Normal (without match) |
| *No response from user* | No answer to incoming DDI call from user on S bus or DSI | DDI No., date, time | Normal (without match) |
| *Node: Connection lost* | A node is not connected to the Master for a certain amount of time (configurable). | Node number, date, time | critical (negative, with match) |
| *Node: Connection re-established* | A node is reconnected with the Master for a certain amount of time (configurable) after an interruption. | Node number, date, time | critical (positive, with match) |
| *Not enough licences for integrated mobile/ external phones* | The connection setup with an integrated mobile/external phone has failed because the number of configured mobile/external phones is greater than the number of licences available. All the integrated mobile/external phones remain blocked until a sufficient number of licences are available. | Number of licences, number of configured mobile/external phones, date, time | Serious (negative, with match) |
| *NTP: Time synchronisation failed* | Time synchronization via the NTP server (NTP = Network Time Protocol) has failed. | Date, time | Serious (negative, with match) |
| *NTP: Time synchronisation re-established* | Time synchronization via the NTP server (NTP = Network Time Protocol) has been restored. | Date, time | Serious (positive, with match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *Outgoing call rejected* | Call rejected by the network<br>• On any line: error code 34<br>• On required line group: error code 44 | Port number of the exchange line circuit, cause, date, time | Normal (without match) |
| | | | |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *Overheat* (Mitel 470 only) | The temperature inside the communication server is too high. Appropriate measures must be taken immediately to improve heat dissipation. Measures are automatically adopted, depending on where the overheating occurs:<br><br>FXO and FXS interface card:<br><br>• the ports are deactivated in groups of 4 ports.<br>• Once they have cooled down below a defined card-specific value, the ports are automatically reactivated group by group.<br><br>CPU2 applications card<br><br>• The card will be completely deactivated. Once it has cooled down below a defined value, the card is automatically reactivated.<br><br>Internal power supply unit PSU2U or call manager card CPU1:<br><br>• the communication server will be shut down completely.<br><br>**Note**:<br><br>• To revert the system from overheating, no more than 30% of the FXS ports should be active simultaneously per 32FXS card and no more than 50 FXS ports per system. | Card number, temperature, date, time | critical (negative, with match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| | • PRI, BRI and DSI cards do not have temperature sensors and are therefore never deactivated due to overheating. | | |
| *Overload detected on USB port (CPU2)* (Mitel 470 only) | A (current) overload was detected on one of the USB interfaces on the applications card (CPU2).<br><br>**Note**:<br>The maximum current input at the USB interfaces varies. | Date, time | Normal (without match) |
| *Port out of service* | A port previously in operation has stopped functioning. | Number of the slot, relevant port number, date, time | Serious (without match) |
| *Possible clone detected for your system* (Virtual Appliance only) | The clone detection service on the licence server (SLS cloud) has detected a possible clone (system with the same EID). | Date, time | critical (negative, with match) |
| *QSIG licence limit reached* | Maximum number of licensed outgoing connections with QSIG protocol exceeded | Route number, user number, date, time | Serious (without match) |
| *Radio unit port active* | The radio unit is responding again | Card number, port number, date, time | Serious (positive, with match) |
| *Register error* | • Card not fitted<br>• Card not logged on<br>• Card defective | Card number, date, time | Normal (without match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *Remote maintenance disabled* | Remote maintenance has been deactivated | Date, time | Normal (positive, with match) |
| *Remote maintenance enabled* | The remote maintenance has been activated (The report is output unfiltered on local destinations). | Date, time | Normal (negative, with match) |
| *Restart of applications card CPU2 executed* | The restart of applications card CPU2 was executed successfully. | Date, time | critical (positive, with match) |
| *Restart of applications card CPU2 required* | The system has detected that a manual restart of the applications card CPU2 is required (e. g. for a security update). | Date, time | critical (negative, with match) |
| *Restricted operating mode disabled* | Restricted mode could be disabled again. | Date, time | critical (positive, with match) |
| *Restricted operating mode enabled* (not valid for Virtual Appliance) | The communication server has switched to restricted mode. Cause: 0: No valid licence | Cause, date, time | critical (negative, with match) |
| *Restricted operating mode enabled* (Virtual Appliance only) | The communication server has switched to restricted mode. Cause: 0: No valid licence. 1: Link to gateway satellite lost. 2: Max. duration without link to licence server reached. 3: Your system clone confirmed. 4: Licence check mode mismatch in SLS and MiVo400. 5: Support mode enabled. | Cause, date, time | critical (negative, with match) |
| *Satellites missing after supervision time* | After an AIN update (Master and all satellites) some satellites no longer have a connection to the Master. | Total satellites missing, Satellites rolled back, Date, Time | Serious (without match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *Send e-mail failed* | The system was unable to send an e-mail because an error occurred.<br><br>Meaning of the parameter values in table below. | Cause/action, e-mail client, additional information, date, time | critical (negative, with match) |
| *SIMPLE/MSRP back within the licence limit* | There are now enough licences available for using the MSRP and/ or SIMPLE protocol for users. | Date, time | Serious (positive, with match) |
| *SIP account available* | The SIP account has successfully registered with the SIP provider. | Provider, account, date, time | critical (positive, with match) |
| *SIP account not available* | The SIP account cannot register with the SIP provider for a certain reason (0: Provider unobtainable / 1: no permission / 2: disallowed / 3: unknown). The event is triggered only if the parameter *Registration required* is configured to *Yes*. | Provider, account, date, time | critical (negative, with match) |
| *SMS gateway reachable* | External SMS gateway again reachable | Date, time | critical (positive, with match) |
| *SMS gateway unreachable* | External SMS gateway unobtainable by network provider or incorrectly configured | Date, time | critical (negative, with match) |
| *Software upgrade IP system phone failed* | The software update of an MiVoice 5361 IP / 5370 IP / 5380 IP has failed for the stated reason. | User number, terminal ID, reason, date, time | critical (negative, with match) |
| *Software upgrade IP system phone successful* | The software update of an MiVoice 5361 IP / 5370 IP / 5380 IP has now been successfully completed after unsuccessful attempt(s). | User number, terminal ID, date, time | critical (positive, with match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *Software upload* | During an upload in system status:<br>• Update running<br>• *Supervision running*<br>• *Normal operation* | Parameter 1:<br>• 0: "New communication server software loaded, starting...",<br>• 1: New communication server software crashed, roll-back performed<br>• 3: New communication server software started and running well<br>Date, time | Normal (without match) |
| *Standard SIP terminals within the licence limit again* | *SIP Terminals* and *Video Terminals* licences are now available. | Parameter 1=1: SIP *Terminals* licence, Parameter 2=1: *Video Terminals* licence, date, time | Serious (positive, with match) |
| *SX-200 call data record management system: Connection established* | The connection to the SX-200 call data record management system has been successfully established. | Date, time | critical (positive, with match) |
| *SX-200 call data record management system: Connection lost* | The connection to the SX-200 call data record management system has been lost. | Date, time | critical (negative, with match) |
| *SX-200 hotel management system: Connection established* | The connection to the SX-200 hotel management system has been successfully established. | Date, time | critical (positive, with match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *SX-200 hotel management system: Connection lost* | The connection to the SX-200 hotel management system has been lost. | Date, time | critical (negative, with match) |
| *SX-200 voice mail management system: Connection established* | The connection to the SX-200 voice mail management system has been successfully established. | Date, time | critical (positive, with match) |
| *SX-200 voice mail management system: Connection lost* | The connection to the SX-200 voice mail management system has been lost. | Date, time | critical (negative, with match) |
| *Synchronisation loss on trunk* | A BRI/PRI interface entered in the clock pool has lost the system clock | Port number, date, time | Serious (negative, with match) |
| *Synchronisation re-established* | Synchronization with the network has been restored on at least one BRI/PRI interface. | Date, time | Serious (positive, with match) |
| *Synchronisation with backup communication server failed* | The primary communication server was unable to transmit the configuration data to the backup communication server.<br><br>**Note**:<br>This event message is generated by the primary communication server. | Backup communication server ID, date, time | critical (negative, with match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *Synchronisation with backup communication server successful* | The primary communication server was able (following one or more previous failed attempts) to transmit the configuration data to the backup communication server.<br><br>**Note**:<br>This event message is generated by the primary communication server. | Backup communication server ID, date, time | critical (positive, with match) |
| *Synchronization on trunk re-established* | A BRI/PRI interface entered in the clock pool has been successfully resynchronized with the system clock. | Port number, date, time | Serious (positive, with match) |
| *System memory usage below the critical range again* | The memory usage in the file system for a specific purpose has again fallen below a defined (*Serious* severity level) or critical (*Critical* severity level) value.<br><br>Purpose (file type ID):0: File system, 1: Application, 2: Crash-Log, 3: Monitor-Log, 4: Announcement service, 5: Voice mail, 6: Music on hold, 7: Data backup, 8: Hospitality/ Accommodation, 9: User folder | File type ID, memory usage in %, date, time | Serious / Critical (positive, with match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *System memory usage over the critical range* | The memory usage in the file system for a specific purpose has exceeded a defined (*Serious* severity level) or critical (*Critical* severity level) value.<br><br>Purpose (file type ID):0: File system, 1: Application, 2: Crash-Log, 3: Monitor-Log, 4: Announcement service, 5: Voice mail, 6: Music on hold, 7: Data backup, 8: Hospitality/ Accommodation, 9: User folder | File type ID, memory usage in %, date, time | Serious / Critical (negative, with match) |
| *System overload* | Network access attempted when all lines are seized or the system is overloaded. | Route number, user number, date, time | Normal (without match) |
| *System phone in service again* | A system phone on the DSI bus is ready for operation again. | Card number, port number, user number, date, time | critical (positive, with match) |
| *System phone out of service* | A system phone on the DSI bus is defective or was disconnected. | Card number, port number, user number, date, time | critical (negative, with match) |
| *Temperature within normal range again* | Following overheating, the temperature inside the communication server is back in the normal operating range. | Card number, temperature, date, time | critical (positive, with match) |
| *Temporary activation expires on* | Reminder of the missing, definitive activation licence following connection set-up with the communication server. | Expiration date [DD.MM.YYYY], date, time | Serious (without match) |
| *Terminal power supply: Overload* (Mitel 470 only) | Rated output slightly exceeded for > 4 s. | Date, time | critical (negative, with match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *Terminal power supply: Shut-down (Mitel 470 only)* | Rated output clearly exceeded for 4 s | Date, time | critical (negative, with match) |
| *Terminal power supply: Switching back on* (Mitel 470 only) | The power supply to the terminals was switched back on after deactivation due to overflow. | Date, time | critical (positive, with match) |
| *Terminal power supply: Within normal range again* (Mitel 470 only) | The power supply to the terminals is back in the normal rated output range following a slight, preceding overflow. | Date, time | critical (positive, with match) |
| *Test event message* | The configuration of message destinations can be tested with this event message. | Date, time | Serious (without match) |
| *The communication server has been restarted* | The communication server was restarted manually or automatically due to an error. | Date, time | Critical (without match) |
| *The licence limit for CSTA sessions has been reached* | An application is unable to set up a CSTA session to monitor/check a terminal because there are too few *CSTA Sessions* licences available. | Max. number of licences, date, time | Serious (negative, with match) |
| *The licence limit for Dual Homing has been reached* | A SIP phone in the Mitel 6800/6900 SIP series has attempted to register on a backup communication server and not enough licences are available.<br><br>**Note**:<br>This event message is generated by the backup communication server. | Date, time | Serious (negative, with match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *The licence limit for Mitel Dialer has been reached* | Mitel Dialer could not be linked to a user because too few licences are available. | Total purchased licences, date, time | Serious (negative, with match) |
| *The licence limit for Mitel SIP terminals has been reached* | A Mitel SIP terminal is unable to register or use the video functionality because there are too few *Mitel SIP Terminals* or *Mitel 8000i Video Options* licences available. | Parameter 1=1: Missing *Mitel SIP Terminals* licence, Parameter 2=1: Missing *Mitel 8000i Video Options* licence, Parameter 3=3: Max. number of licences, date, time | Serious (negative, with match) |
| *The licence limit for SIMPLE/MSRP has been reached* | A third-party application wishes to use the MSRP and/or SIMPLE protocol for a user, but not enough licences are available. | Date, time | Serious (negative, with match) |
| *The licence limit for standard SIP terminals has been reached* | A standard SIP terminal is unable to register or use the video functionality because there are too few *SIP Terminals* or *Video Terminals* licences available. | Parameter 1=1: Missing *SIP Terminals* licence, Parameter 2=1: Missing *Video Terminals* licence, Parameter 3=3: Max. number of licences, date, time | Serious (negative, with match) |
| *TLS certificate expires soon* | A TLS certificate for a SIP node or SIP endpoint is about to expire (*Serious* severity level) or has just expired (*Critical* severity level) and needs to be renewed.If the endpoint type is = 0 (Mitel), then is parameter 2 = node ID.If the endpoint type is = 1 (3rd party), then the remaining parameter data contains the first eleven characters of the certificate name. | Type of endpoint (0: Mitel, 1: 3rd party), node ID or certificate name, date, time | Serious / Critical (without match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *TLS certificate update* failed | The update of the TLS certificate for an SIP node or SIP endpoint via FTP has failed and needs to be renewed manually.If the endpoint type is = 0 (Mitel), then is parameter 2 = node ID.If the endpoint type is = 1 (3rd party), then the remaining parameter data contains the first eleven characters of the certificate name. | Type of endpoint (0: Mitel, 1: 3rd party), node ID or certificate name, date, time | critical (negative, with match) |
| *TLS certificate update successful* | A TLS certificate for a SIP node or SIP endpoint was successfully renewed.If the endpoint type is = 0 (Mitel), then is parameter 2 = node ID.If the endpoint type is = 1 (3rd party), then the remaining parameter data contains the first eleven characters of the certificate name. | Type of endpoint (0: Mitel, 1: 3rd party), node ID or certificate name, date, time | critical (positive, with match) |
| *TLS certificate was generated: Upgrade non-Mitel endpoints now* | A TLS certificate has been generated. If generation is manual, the certificate must be imported manually into the Mitel SIP nodes. The certificate must always be imported manually on all non-Mitel nodes and non-Mitel endpoints. | Date, time | Normal (without match) |
| *TLS server certificate: Validation failed* | While a TLS connection is established the validation of the certificate of the TLS server failed. | Service, TCP port, reason, date, time | critical (negative, with match) |
| *TLS server certificate: Validation successful* | The validation of the certificate of the TLS server was successful. | Service, TCP port, date, time | critical (positive, with match) |
| *Too few FoIP channels* | Setting up a fax connection via T.38 failed because no FoIP channel is available. | Available FoIP channels on node | Serious (without match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *Too few licences for IP system phones* | A MiVoice\ 5361\ IP / 5370 IP / 5380 IP was unable to register because there are too few IP system phone licences. | Date, time | Serious (negative, with match) |
| *Too few licences for PMS interface* | Either the *Hospitality PMS Interface* licence is missing or the number of *Hospitality PMS Rooms* licences available is insufficient. | Number of licensed rooms, number of configured rooms, date, time | Serious (negative, with match) |
| *Too few VoIP channel licences* | Connection setup failed because the licence limit for simultaneously active VoIP channels has been reached. | No. of licensed VoIP channels, Date, Time | Serious (without match) |
| *Too few VoIP channels* | An user is trying to set up a connection that requires one or more VoIP channels which are currently not available. | Available VoIP channels on this node, date, time | Normal (without match) |
| *Too many errors with the same ID* | An unusual amount of errors (more than 50 per hour) with the same error ID have occurred. | Error ID, date, time | Normal (without match) |
| *Too many event messages* | Number of message types exceeds limit entered in the table on:<br>• "Synch. "Synch.loss on BRI/ PRI"<br>• "Outgoing Call Rejected"<br>• "No response from network" | Date, time | Normal (without match) |
| *Too much user data* | System capacity exceeded | Date, time | Critical (without match) |
| *Total synchronization loss* | Network synchronisation has failed on all BRI/PRI interfaces | Date, time | Serious (negative, with match) |

[32] The node is also always indicated in an AIN.

| Event message | Trigger condition | Details[32] | Severity |
|---|---|---|---|
| *Trial licence expired* | The duration for which a trial licence can be used for a specific feature has expired and there is no valid licence. | Licence ID, date, time | Serious (without match) |
| *USER EVENT MESSAGE* | With *77[nnnn] from a terminal | nnnn [0000...99999], user number, date, time | Serious (without match) |
| *User memory usage below the critical range again* | The memory usage in the file system for a specific user has again fallen below a defined (*Serious* severity level) or critical (*Critical* severity level) value. | User number, memory usage in %, date, time | Serious / Critical (positive, with match) |
| *User memory usage over the critical range* | The memory usage in the file system for a specific user has exceeded a defined (*Serious* severity level) or critical (*Critical* severity level) value. | User number, memory usage in %, date, time | Serious / Critical (negative, with match) |
| *Wake-up call failed* | The room wake-up call was not answered | Room No., date, time | Normal (negative, with match) |
| *Wake-up order confirmed* | The room wake-up call has now been answered | Room No., date, time | Normal (positive, with match) |

**Table 21: Meaning of the parameter values for the event message *Send e-mail failed***

| Value | Parameter 1 (XXYY) | | Parameter 2: | Parameter 3: |
|---|---|---|---|---|
| | Reason (XX) | Action (YY)[33] | E-mail client | Additional info depending on the e-mail client (XXYY) |
| 00 | Not defined | Not defined | Not defined | |

[32] The node is also always indicated in an AIN.
[33] Action carried out by the SMTP client at the point when the error occurred.

| Value | Parameter 1 (XXYY) | | Parameter 2: | Parameter 3: |
|---|---|---|---|---|
| | Reason (XX) | Action (YY)[33] | E-mail client | Additional info depending on the e-mail client (XXYY) |
| 01 | E-mail memory full | Connection set up to SMTP server | Voice mail | XX: Mailbox IDYY: Message ID |
| 02 | SMTP server access data invalid | Extended registration on SMTP server | Auto backup | |
| 03 | SMTP client cannot set up a connection to the server | Registration on SMTP server | Call recording | User number |
| 04 | Authentication failed | Transmission of e-mail address | Event message | |
| 05 | Continuous negative answer from SMTP server | Transmission of e-mail recipient address | Call logging for hospitality | |
| 06 | Temporary negative answer from SMTP server | Prepare data transmission | Configuration files | XX: User ID<br><br>YY: Terminal ID |
| 07 | No answer from SMTP server | Data transmission in progress | | |
| 08 | E-mail attachment not found | End data transmission | | |
| 09 | Invalid host, domain or IP address on the communication server | Prepare authentication (LOGIN) | | |

[33] Action carried out by the SMTP client at the point when the error occurred.

| Value | Parameter 1 (XXYY) | | Parameter 2: | Parameter 3: |
|---|---|---|---|---|
| | Reason (XX) | Action (YY)[33] | E-mail client | Additional info depending on the e-mail client (XXYY) |
| 10 | E-mail text too long (body) | User name authentication (LOGIN) | | |
| 11 | E-mail attachment too large | Password authentication (LOGIN) | | |
| 12 | Format of e-mail attachment not supported | Authentication (PLAIN) | | |
| 13 | No e-mail recipient address | Prepare encrypted authentication (CRAM-MD5) | | |
| 14 | Invalid e-mail recipient address | Encrypted authentication (CRAM-MD5) | | |
| 15 | Invalid e-mail sender address | Preparing to send next e-mail | | |

### 6.3.1.2 Event tables

Event tables list all the event messages the system is capable of generating (see Event types, in alphabetical order).

There are 7 event tables. After a first start, all event tables are assigned at least one destination. This assignment can be modified in the *Message destinations* view. Each event table can be configured individually. This means it is possible with a filter to decide which event message – if any – should be sent to a particular signal destination either immediately, with a delay or not at all.

- *No event:*

  This type of incoming event messages are **never** sent to the linked destination.

[33] Action carried out by the SMTP client at the point when the error occurred.

- *Every event:*

  This type of incoming event messages are **all** sent to the linked destination.
- *Custom:*

  With this setting, you can determine how often the event message may appear for each period, until they are sent to the linked destination.

  The *Frequency* of an event message may range between 2 and 20. The Period is indicated in hours, ranging between 1 and 672. The longest time *period* corresponds to 28 days or 4 weeks.

**Table 22: Example of event table**

| *Event type* | *Frequency* | *Time period* |
|---|---|---|
| *Total synchronization loss* | 10 | 1 |

In this example an event message is sent to the message destinations if there is a *Total synchronization loss* event message when the system generates the event message 10 times within 1 hour.

## 6.3.1.3 Signal destinations

After a first start, all event tables are exactly assigned to a message destination. (Exception: *Local destination* and *SNMP destination* use this event table.) You can assign event tables to several or no message destinations

The destinations are configured in the *Message destinations* view.

### 6.3.1.3.1 Signal destination system phone 1 and 2

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

- Destination system phone 1:
  - By default allocated to event table 1, which is preconfigured for common use.
  - Fix allocated to message group 16.
- Destination system phone 2:
  - By default allocated to event table 8, which is preconfigured for front desk terminals in hospitality environments.
  - Fix allocated to message group 15.

### 6.3.1.3.2 External signal destinations

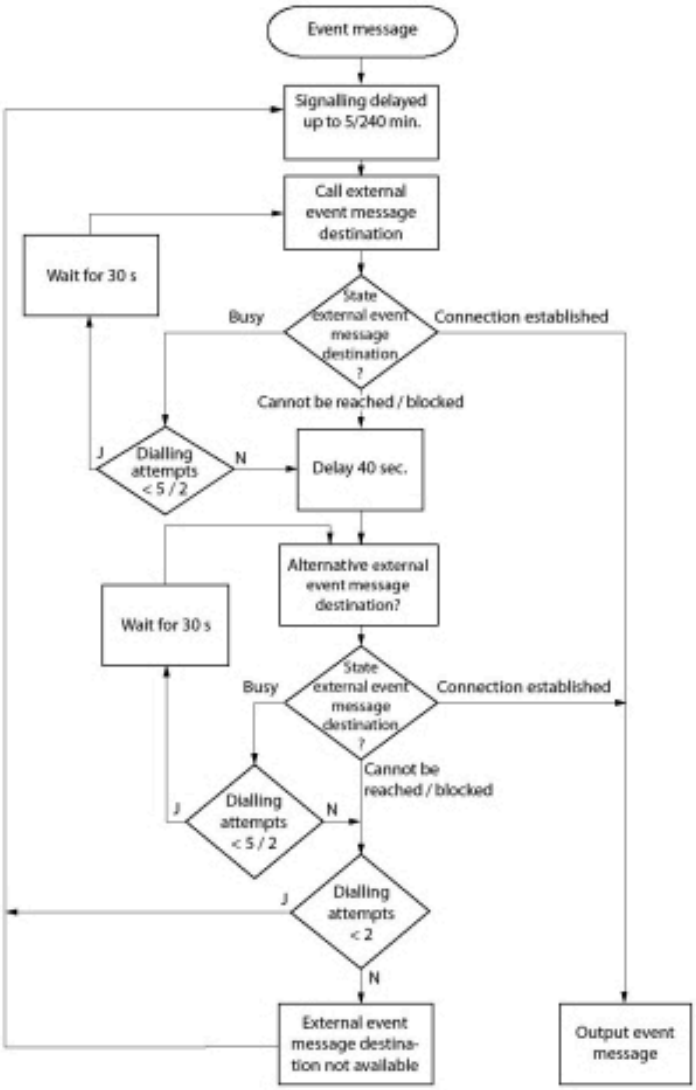
Depending on the event table allocated, event messages (normally Table 2) are sent to a specified external signal destination. Two external signal destinations can be specified:

- 1 primary external signal destination
- 1 alternative external signal destination

If the system issues an event message, the event message opens a PPP communication channel from the public network of the communication server to a terminal adapter or modem. Once the event message has been confirmed, the system clears down the PPP connection.

Signalling an event message to an external signal destination

Figure 8: Flowchart of the signalling of an event message to an external signal destination




The following principles govern the way event messages are signalled to an external signal destination:

- Individual event messages are not signalled if they occur at short intervals. The event messages are stored temporarily for 5 minutes and then sent together to the external signal destination.
- If over a period of one hour an attempt is made unsuccessfully to send the event messages to the external signal destination, the signalling period is extended from 5 minutes to 4 hours. As soon as the event messages are successfully output at the external signal destination, the time period is reset to 5 minutes.

- If over a period of 1 hour an attempt is made unsuccessfully to send an event message to an external signal destination, the number of dialling attempts is reduced from 5 to 2. As soon as an event message has been successfully sent, the number of dialling attempts is increased to 5 again.
- If the attempt to send an event message to an external signal destination was unsuccessful, the system will generate the event message *External event message destination missing*.

**Note**:

Event tables and signal destinations should be set in such a way that the event message *External event message destination missing* is signalled immediately to any signal destination still available.

## 6.3.1.3.3 Local signal destinations

Depending on the event table allocated, event messages (normally Table 3) are sent to a specified local signal destination.

PPP links:

Like with an external signal destination the event message opens a PPP communication channel from the communication server to a terminal adapter or modem. Once the event has been confirmed, the system clears down the PPP connection.

Ethernet link:

A PC connected either directly to the Ethernet interface or to the communication server via a LAN can be configured as the local signal destination.

**Note**:

- The local destination is linked with the same event table as the SNMP destination. Any changes to the link and/or filter criteria for the linked event table also apply to the SNMP destination.
- Event tables and signal destinations should be set in such a way that the event message *External event message destination missing* is signalled immediately to any signal destination still available.

### 6.3.1.3.3.1 SNMP destination

Depending on the event table allocated, event messages (normally Table 3) are sent to a specified SNMP destinations.

SNMP stands for "Simple Network Management Protocol" and is used by Network Management Systems (NMS).

If the Network Management System is to know the potential events of the communication system, the corresponding system components have to be defined in the form of configurable objects (Managed Objects: MO). These objects and the related event messages are stored in an object library referred to as the Management Information Base (MIB).

You will find the interface description and the different MIB versions on Mitel InfoChannel – Mitel Solution Alliance - API and Interface Information - MiVoice Office 400 - MiVoice Office 400 Network Management.

To access these documents, you have to be a member in Mitel Solution Alliance (MSA). If you are not a member yet, go to Mitel website and search for “Mitel Solution Alliance” where you can join. A membership on level MSA partner (MP) is sufficient.

5 SNMP destinations can be defined. Forwarding to the SNMP destinations can be activated and deactivated independently of the forwarding to the local and external signal destinations.

**Note**:

The SNMP destination is linked with the same event table as the local destination. Any changes to the link and/or filter criteria for the linked event table also apply to the local destination.

## 6.3.1.3.4 Signal destination event log

Normally, the signal destination event log is assigned to Event table 4. The filter on this event table is preconfigured for most event types in such a way that event messages are entered in the event log once they arrive.

If the signal destination event log is assigned a different event table or if event table 4 is reconfigured, the event messages are entered in the event log in accordance with the new event table or the new configuration.

The last 254 event messages are recorded in the *Event log*. *Active event messages* and the last 10 *Power failures* are recorded in separate logs.

If the maximum number of entries is exceeded, the oldest entry in each case is deleted.

If active event messages are available, they are indicated in WebAdmin on the left, with the  symbol.

## 6.3.1.3.5 E-mail signal destination

With the e-mail client integrated in the communication server, event messages can be sent to internal or external e-mail destinations. Normally, the signal destination *E-mail destination* is automatically assigned to event table 5. Up to 5 e-mail destinations can be defined, and e-mail notification can be activated or deactivated globally.

For the communication server to send the e-mails the access to the e-mail service provider's SMTP server must be configured in the *SMTP server* view.

## 6.3.1.3.6 Destination alarm server (ATAS)

Event messages can also be sent via the ATAS interface, for instance, to an alarm server. This may be an Mitel Alarm Server or a third-party alarm server. The use of the ATAS protocol is subject to a licence.

After a first-start of the communication server, the signal destination *Alarm server (ATAS)* is automatically allocated event table 6. The notification service via the ATAS interface to the alarm server can be globally switched on or off.

## 6.3.1.3.7 SRM destination

Event messages can also be sent to the SRM server. Depending on the severity level in the SRM agent, this changes the system status on the corresponding communication server line. The line colour changes at the same time. If the corresponding positive event message arrives later or if the event message is confirmed in WebAdmin, the status and colour are restored again. The following system statuses are defined:

- *Normal (Blue colour):*

  No active event messages with the severity level *Serious* or *Critical* is available.
- *Serious* (Yellow colour):

  At least one event message is available and needs to be closely examined. (Example: *Charge counter overflow*)
- *Critical* (Red colour)

  At least one event message is available and is hampering the system's function.(Example: *Fan failure*)

**Note**:

Not all negative event messages have a positive match. In this case, the event messages must be confirmed manually in WebAdmin.

Event messages, which are not *Serious* or *Critical*, are not sent to the SRM server. The severity of individual event messages is given in the Event types, in alphabetical order.

Example:

Power output: There are no serious or critical event messages. The communication server line in the SRM agent is blue and the system status is on *Normal*.

1. The event message *Charge counter overflow* reaches the SRM server.
   - The communication server's system status in the SRM agent changes to *Serious*, and the destinations turn yellow.
2. The event message *Fan failure* reaches the SRM server.
   - The communication server's system status in the SRM agent changes to *Critical*, and the destinations turn red.
3. The event message *Charge counter overflow* is confirmed in WebAdmin in the *Active event messages view*.
   - The system status of the communication server in the SRM agent remains on *Critical*, and the destinations on red, because there is still an event message with this severity.
4. The event message *Fan failure* reaches the SRM server.
   - The communication server's system status in the SRM agent changes to *Normal*, and the destinations turn red.

After a first-start of the communication server, the *SRM destination* is automatically allocated event table 7. The notification service to the SRM destination can be switched on or off.

On the SRM server the status modification per communication server must be allowed and configurations are also required in WebAdmin. You can find a configuration guide in WebAdmin help under the *Message destinations*.

#### 6.3.1.3.8 Testing the signal destination configuration

To test the configuration, a test event message can be separately initiated for each destination in the WebAdmin configuration (*Message destinations*view). The event message is signalled without any delay, directly at the selected signal destination.

If the communication server is connected via a modem or terminal adapter, the test event messages will be signalled only once the connection is cleared down.

## 6.3.2 Other aids

### 6.3.2.1 System logs

During operation or in the event of a malfunction the communication server stores the current operating data in the file system in the directory */home/mivo400/logs*.

You can open, view and back up these log files on any storage device, in WebAdmin in the *System logs* view.

### 6.3.2.2 File system state

In the *File system state* view you can see the thematically structured file system's memory load. In an AIN the file systems for all nodes can be viewed.

## 6.3.2.3 File browser

With the *File browser* you have access to the communication server file system and you can create new folders as well as view, import, replace or delete files in the file system.

All communication server folders and files are located in the directory */home/mivo400/*.

**Note**:

Be extremely careful while replacing or deleting files. The absence of files can hamper or even render impossible the working of the communication server.

# Annex 7

This chapter contains the following sections:



In this chapter you will find a list of functions and products not supported, licence information on third-party software products, and a table summary of related documents and online help.

## 7.1 Functions and terminals no longer supported

The MiVoice Office 400 series continues to support the terminals and functions of the Aastra IntelliGate series. Exceptions include the following terminals and functions:

- IP system phones Office 35IP, Office 70IP-b
- Cordless system phones Office 100, Office 130/130pro, Office 150, Office 150EEx, Office 155pro/155ATEX
- The Aastra 6751i phone is no longer supported as an Mitel SIP phone.
- IP system softphone Office 1600/1600IP
- DECT radio unit SB-4
- Pocket Adapter V.24
- X.25 in the D channel
- Ascotel® Mobility Interface (AMI) and DCT terminals
- Universal Terminal Interface (UTI)
- AMS Hotel manager and Hospitality Mode V1.0 (hotel functions)
- Operator application Office 1560/1560IP
- Aastra Management Suite (AMS) is replaced by the web-based configuration tool WebAdmin, the remote management SRM (Secure IP Remote Management) and the application System Search.
- The external remote control (ERC) cannot be set up with he system (Mobile or External Phone Extension).
- Only language package downloading is available for Virtual Appliance in System Search, Emergency Upload and the display of Virtual Appliance communication servers is not available.
- The CPU2 application card is no longer supported (only CPU2-S).
- The Telephony Web Portal (TWP) application is replaced with Mitel MiCollab Audio, Web and Video Conferencing.

## 7.2 Licensing information of third-party software products

**York Technologies Limited**
Copyright and License Information

You agree that all ownership and copyright of licensed icons remain the property of York Technologies Limited. You will be granted a non-exclusive license to display the graphical media royalty-free in any personal or commercial software applications, web design, presentations, and multimedia projects that you create and/or distribute. You may modify the icons and display the resulting derived artwork subject to the terms of this agreement. Where an application is to be distributed, the graphical media must be compiled into the application binary file or its associated data files, documentation files, or components. If you are creating software applications or websites on behalf of a client they must either purchase an additional license for the icons from York Technologies Limited or you may surrender and fully transfer your license to your client and notify us that you have done so. Except where stated above you may not license, sub-license, grant any rights, or otherwise make available for use the icons either in their original or modified state to any other party. You may not include the icons in any form of electronic template that allows other parties to distribute multiple copies of customised applications. You may not include the icons in form of obscene, pornographic, defamatory, immoral or illegal material.

TO THE EXTENT PERMITTED BY APPLICABLE LAW ICONS AND OTHER GRAPHICAL MEDIA ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. THE ENTIRE RISK ARISING OUT OF USE OR PERFORMANCE OF THE ICONS AND OTHER GRAPHICAL MEDIA REMAINS WITH YOU.

IN NO EVENT WILL YORK TECHNOLOGIES LIMITED BE LIABLE FOR ANY DAMAGES, INCLUDING LOSS OF DATA, LOST OPPORTUNITY OR PROFITS, COST OF COVER, OR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, DIRECT, OR INDIRECT DAMAGES ARISING FROM OR RELATING TO THE USE OF THE ICONS AND OTHER GRAPHICAL MEDIA, HOWEVER CAUSED ON ANY THEORY OF LIABILITY. THIS LIMITATION WILL APPLY EVEN YORK TECHNOLOGIES LIMITED HAS BEEN ADVISED OR GIVEN NOTICE OF THE POSSIBILITY OF SUCH DAMAGE. IN ANY CASE, YORK TECHNOLOGIES LIMITED'S ENTIRE LIABILITY UNDER ANY PROVISION OF THIS AGREEMENT SHALL BE LIMITED TO THE GREATER OF THE LICENSE/PURCHASE FEE PAID BY YOU FOR THE ICONS OR £1.00. NOTHING IN THESE TERMS AND CONDITIONS SHALL EXCLUDE OR LIMIT YORK TECHNOLOGIES LIMITED'S LIABILITY FOR DEATH OR PERSONAL INJURY CAUSED BY ITS NEGLIGENCE OR FRAUD OR ANY OTHER LIABILITY WHICH CANNOT BE EXCLUDED OR LIMITED UNDER APPLICABLE LAW.

This Agreement shall be subject to and construed and interpreted in accordance with English Law and shall be subject to the jurisdiction of the Courts of England. Any enquiries regarding this Agreement should be directed to York Technologies Limited, St Mary's Cottage, St Buryan, Penzance, UK, TR19 6DJ.

20 August 2007

Glyph Lab is a trading name of York Technologies Limited registered in England and Wales, No 3846468. Registered office St Marys Cottage, St Buryan, Penzance TR19 6DJ, UK.
Glyph Lab is a trademark of York Technologies Limited

## 7.3 Documents and online help systems with further information

**Table 23: Documents and online help systems with further information**

| Product | Document |
|---|---|
| Products of the MiVoice Office 400 family | System Manual Mitel 415/430 |
| | System Manual Mitel SMBC |
| | System Manual Mitel 470 |
| | System Manual System Functions and Features |
| | SIP Access User’s Guide (English) |
| | MiVoice Office 400 feature overview |
| Applications | System Manual Mitel Alarm Server |
| | Mitel Alarm Server User's Guide |
| | Installation Instructions Mitel OpenCount for MiVoice Office 400 |
| | Configuration Guide Mitel OpenCount for MiVoice Office 400 |
| | Installation and Administration Guide "Mitel Standard Linux" |
| | Solutions Guide "Virtual Appliance Deployment" |
| | Mitel SIP Teleworker via MBG on MiVoice Office 400 |

| Product | Document |
|---|---|
| SMBC Manager | Online Help |
| WebAdmin | Online Help |
| | Configuration assistant |
| | Setup wizard |
| Self Service Portal (SSP) | Online Help |
| Project planning application Mitel CPQ | Online Help |
| DECT | Planning DECT systems User’s Guide |
| Mitel SIP-DECT | User’s Guide for Mitel 600 SIP-DECT on MiVoice Office 400 |
| Basic/Enterprise voice mail system | User's Guide for MiVoice Office 400 voice mail system |
| | System Manual System Functions and Features |
| OIP | System Manual Mitel Open Interfaces Platform |
| | Online Help |
| | User's Guide Mitel OfficeSuite |
| | User's Guide for First Party TAPI Service Provider |
| Networking | System Manual for Mitel Advanced Intelligent Network (AIN) and IP system phones |

| Product | Document |
|---|---|
| | Private networking system manual |
| Mitel SIP phones on MiVoice Office 400 | Mitel 6730/31/53 SIP, Mitel 6735/37/55/57 SIP, Mitel 6739 SIP, Mitel 6863/65 SIP, Mitel 6867/69 SIP, Mitel 6873 SIP, Mitel 6920 SIP/Mitel 6930 SIP, Mitel 6940 SIP user's guide |
| Mitel SIP phones (platform-independent) | User's guide, short user's guide, installation instructions, administration instructions |
| IP system phones | Quick User's Guide MiVoice 5360 IP /MiVoice 5361 IP / MiVoice 5370 IP /MiVoice 5380 IP |
| | Operating Instructions for MiVoice 5360 IP / MiVoice 5361 IP / MiVoice 5370 IP / MiVoice 5380 IP / MiVoice 2380 IP |
| Digital system phones | Quick User's Guide Office 135/135pro / Office 160pro/Safeguard/ATEX / MiVoice 5360 / MiVoice 5361 / MiVoice 5370 / MiVoice 5380 / Mitel 610 DECT / Mitel 612 DECT / Mitel 620 DECT / Mitel 622 DECT / Mitel 630 DECT / Mitel 632 DECT / Mitel 650 DECT |
| | |
| | |
| | |
| | User's Guide Office 135/135pro / Office 160pro/ Safeguard/ATEX / MiVoice 5360 / MiVoice 5361/ MiVoice 5370/ MiVoice 5380 / MiVoice 5380 / Mitel 610 DECT / Mitel 612 DECT / Mitel 620 DECT / Mitel 622 DECT / Mitel 630 DECT / Mitel 632 DECT / Mitel 650 DECT |
| Analogue phones | Mitel 6710 Analogue / Mitel 6730 Analogueuser's guide |
| PC operator console | User's Guide MiVoice 1560 PC Operator |
| | Online Help |

Most of the documents are accessible at Document Center. Many documents in the above table are summarised per language.

More documents are available on the internet:

- Environmental information for communication server and system phones
- Declarations of conformity for communication server and system phones
- Labels for system phones and expansion key modules
- Safety instructions for system phones
- Application Notes
- Product information
- Leaflets
- Brochures
- Data sheets

Mitel
Powering connections

mitel.com