MiVoice Office 400

Mitel Open Interfaces Platform

Version OIP 8.9.1 (R6.3) System Manual

February 2022

Notice

Trademarks

Contents

About Mitel Open Interfaces Platform

Purpose and function

Mitel Open Interfaces Platform (OIP) is a Windows-based server application. It extends MiVoice Office 400 communication solutions in the fields of unified communications, operator applications, call centre applications, directory servers and automation and alarm system connection. You can, for instance, integrate additional sector-specific applications through the OIP interfaces and OIP connectors.

OIP can be deployed:

- on its own PC (Windows operating system)
- via the application server CPU2/CPU2-S. The application server CPU2/CPU2-S is a PC plug-in card for the Mitel 470 communication server and is pre-installed ex works with OIP and other extensions.
- as Virtual Appliance on VMware ESXi or Microsoft Hyper-V
- as a container application on the Mitel SMBC platform.

MiVoice Office 400 is an open, modular and comprehensive communication solution for business with multiple communication servers of varying performance levels and expansion capacity, a comprehensive telephone portfolio and a large number of expansions. These include an application server for unified communications and multimedia services, a cloud solution for mobile phone integration, an open interface for application developers and a wide range of expansion cards and modules.

The business communication solution with all its components is designed to cover the communication needs of companies and organisations in a comprehensive, user-friendly and maintenance-friendly way. The individual products and parts are coordinated and cannot be used for other purposes or replaced by outside products or parts (except to connect up other authorized networks, applications and phones to the interfaces certified for that purpose).

User Groups

The phones, soft phones and PC applications of the MiVoice Office 400 communication solution are particularly user-friendly in design and can be used by all end users without any specific product training.

Phones and PC applications for professional applications such as operator consoles and call centre applications do require personnel training.

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 is supplied complete with safety and product information, quick user's guides and user's guides.

These and all other user documents such as system manuals are available for download from the Document Center. 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 operation of the MiVoice Office 400 and communication solution and to inform and instruct your customers about all user-related aspects of the installed system.

- Make sure that 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 version of the MiVoice Office 400 used and that you have the latest editions.
- Always read the user documents first before you install, configure and put an MiVoice Office 400 communication system into operation.
- Ensure that all end users have access to the user's guides.

Conformity

Mitel hereby declares that the MiVoice Office 400 products

- conform to the basic requirements and other relevant stipulations of EMC (2014/30/EU) and LVD(2014/35/EU) directives.
- are manufactured in conformity with RoHS according to Directive 2011/65/EU.

You can find the product-specific information at www.mitel.com/regulatory-declarations.

Trademarks

Mitel® is a registered trademark of Mitel Networks Corporation.

All other trademarks, product names and logos are trademarks or registered trademarks of their respective proprietors.

The trademarks, service marks, logos and graphics (summarized under the term "trademarks") listed on Mitel websites or in Mitel publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (summarized under the term “Mitel”) and others. It is forbidden to use the trademarks without Mitel's prior express approval. For more information, contact our legal department at **legal@mitel.com.** A list of globally registered trademarks of Mitel Networks Corporation is available on this website: **http://www.mitel.com/trademarks.**

Use of Third-party Software

MiVoice Office 400 comprises, or is partially based on, third-party software products. The license information for these third-party products is given in the user's guide of the MiVoice Office 400 product in question.

Exclusion of Liability

(Not valid for Australia. See section *"Limited Warranty (Australia only)"*, on the limited warranty in Australia.)

All parts and components of the MiVoice Office 400 communication solution are manufactured in accordance with ISO 9001 quality guidelines. The relevant user information has been compiled with the utmost

care. The functions of the MiVoice Office 400 products have been tested and approved after comprehensive conformity tests. Nonetheless errors cannot be entirely excluded. The manufacturers shall not be liable for any direct or indirect damage that may be caused by incorrect handling, improper use, or any other faulty behavior. Potential areas of particular risk are signaled in the appropriate sections of the user information. Liability for loss of profit shall be excluded in any case.

The Environment

MiVoice Office 400 products are supplied in recycled corrugated cardboard packaging free from chlorine. Inside the cardboard packaging, the components are packed in a protective layer of polyethylene foam or polyethylene sheeting. The packaging is to be disposed of in accordance with statutory regulations.

MiVoice Office 400 products contains plastics based on pure ABS, aluminium-zinc coated or galvanized steel sheeting and circuits boards made from epoxy resin. These materials are to be disposed of in accordance with statutory regulations.

MiVoice Office 400 products should only be dismantled by unscrewing screw connections.

Safety Information

The following safety information applies to the MiVoice Office 400 communication solution and Mitel Open Interfaces Platform.

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. Take careful note of the hazard warnings in the user information.

Operating Safety

MiVoice Office 400 communication servers are operated on 115 VAC or 230 VAC mains power. Neither communication servers nor connected components (for example, phones) will function if the power supply 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 uninterrupted power supply. Up to a specific performance limit, a Mitel 470 communication server can also be operated redundantly using an auxiliary power supply. For more information, refer to your communication server's system manual.

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.

- During the installation follow the installation instructions for your MiVoice Office 400 product and observe to the letter the safety warnings they contain.

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

Data Protection

Protection of User Data

During operation the communication system records and stores user data (for example, call data, contacts, voice messages, and so on). Protect this data from unauthorized 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 only authorized persons have external 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 authorization profiles that are actually required.
- Instruct system assistants only to open remote maintenance access to the communication server for the duration of the necessary access.
- Instruct users with access authorizations to change their passwords regularly or 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 may 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 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 VPN encrypted connection paths.

About this Document

This document describes the technical scope of performance of the Mitel Open Interfaces Platform and supplements the OIP WebAdmin online help.

The document is meant for planners, installers and phone system managers. It requires in-depth knowledge of telephone systems, CTI, Microsoft Windows and relevant expertise in the area of application.

The system manual is available in Acrobat Reader format and can be printed off if necessary. You can navigate the PDF using the bookmarks, the table of contents, the cross-references and the index.

Referenced menu items and parameters on terminal displays and in the user interfaces of the configuration tools are italicised and marked in colour to help navigation.

Document information

- Document number: syd-0575
- Document version: 1.4
- Valid as of / based on: OIP R8.9.1.X (R6.3)
-
- For the latest documentation, see Document Center.

General Highlighting

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.

TIP: Additional information on the handling or alternative operation of equipment.

See also

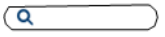
Reference to another section in the same document or to other documents.

Mitel Advanced Intelligent Network

Specific points to note in AIN.

References to the MiVoice Office 400 Configuration tool WebAdmin

References to WebAdmin views are recognised through the magnifier symbol with a navigation code.

=q9 is, for instance, a reference to the *License overview* view. To access this view directly, enter the navigation code in the WebAdmin search window  then press Enter.

You can find the navigation code of a view in the respective help page.

Safety highlighting

Special hazard alert messages with pictograms are used to signal areas of particular risk to people or equipment.

Hazard 	Failure to observe information identified in this way can put people and hardware at risk (electric shocks and short-circuits).
Caution 	Failure to observe information identified in this way can cause a module to malfunction.

Warning 	Failure to observe information identified in this way can lead to damage from electrostatic discharge.

Limited Warranty (Australia only)

The benefits under the Mitel Limited Warranty below are in addition to other rights and remedies to which you may be entitled under a law in relation to the products.

In addition to all rights and remedies to which you may be entitled under the Competition and Consumer Act 2010 (Commonwealth) and any other relevant legislation, Mitel warrants this product against defects and malfunctions in accordance with Mitel's authorized, written functional specification relating to such products during a one (1) year period from the date of original purchase ("Warranty Period"). If there is a defect or malfunction, Mitel shall, at its option, and as the exclusive remedy under this limited warranty, either repair or replace the product at no charge, if returned within the warranty period.

Exclusions

Mitel does not warranty its products to be compatible with the equipment of any particular telephone company. This warranty does not extend to damage to products resulting from improper installation or operation, alteration, accident, neglect, abuse, misuse, fire or natural causes such as storms or floods, after the product is in your possession. Mitel will not accept liability for any damages and/or long distance charges, which result from unauthorized and/or unlawful use.

To the extent permitted by law, Mitel shall not be liable for any incidental damages, including, but not limited to, loss, damage or expense directly or indirectly arising from your use of or inability to use this product, either separately or in combination with other equipment. This paragraph, however, is not intended to have the effect of excluding, restricting or modifying the application of all or any of the provisions of Part 5-4 of Schedule 2 to the Competition and Consumer Act 2010 (the ACL), the exercise of a right conferred by such a provision or any liability of Mitel in relation to a failure to comply with a guarantee that applies under Division 1 of Part 3-2 of the ACL to a supply of goods or services.

This express warranty sets forth the entire liability and obligations of Mitel with respect to breach of this express warranty and is in lieu of all other express or implied warranties other than those conferred by a law whose application cannot be excluded, restricted or modified. Our goods come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and for compensation for any other reasonably foreseeable loss or damage.

You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure.

Repair Notice

To the extent that the product contains user-generated data, you should be aware that repair of the goods may result in loss of the data. Goods presented for repair may be replaced by refurbished goods of the same type rather than being repaired. Refurbished parts may be used to repair the goods. If it is necessary to replace the product under this limited warranty, it may be replaced with a refurbished product of the same design and colour.

If it should become necessary to repair or replace a defective or malfunctioning product under this warranty, the provisions of this warranty shall apply to the repaired or re-placed product until the expiration of ninety (90) days from the date of pick up, or the date of shipment to you, of the repaired or replacement product, or until the end of the original warranty period, whichever is later. Proof of the original purchase date is to be provided with all products returned for warranty repairs.

Warranty Repair Services

Procedure: Should the product fail during the warranty period and you wish to make a claim under this express warranty, contact the Mitel authorized reseller who sold you this product (details as per the invoice) and present proof of purchase. You will be responsible for shipping charges, if any.

Limitation of liability for products not of a kind ordinarily acquired for personal, domestic or household use or consumption (for example, goods/services ordinarily supplied for business-use).

Limitation of liability

1. To the extent permitted by law and subject to clause 1.2 below, the liability of Mitel to you for any non-compliance with a statutory guarantee or loss or damage arising out of or in connection with the supply of goods or services (whether for tort (including negligence), statute, custom, law or on any other basis) is limited to:
   a. in the case of services:
      i) the resupply of the services; or
      ii) the payment of the cost of resupply; and
   b. in the case of goods:
      i) the replacement of the goods or the supply of equivalent goods; or
      ii) the repair of the goods; or
      iii) the payment of the cost of replacing the goods or of acquiring equivalent goods; or
      iv) the payment of the cost of having the goods repaired.
2. Clause 1.1 is not intended to have the effect of excluding, restricting or modifying:
   a. the application of all or any of the provisions of Part 5-4 of Schedule 2 to the Competition and Consumer Act 2010 (the ACL); or
   b. the exercise of a right conferred by such a provision; or
   c. any liability of Mitel in relation to a failure to comply with a guarantee that applies under Division 1 of Part 3-2 of the ACL to a supply of goods or services.

After Warranty Service

Mitel offers ongoing repair and support for this product. If you are not otherwise entitled to a remedy for a failure to comply with a guarantee that cannot be excluded under the Australian Consumer Law, this service provides repair or replacement of your Mitel product, at Mitel's option, for a fixed charge. You are responsible for all shipping charges. For further information and shipping instructions contact:

Manufacturer: Mitel South Pacific Pty Ltd ("Mitel") Level 1, 219 Castlereagh Street Sydney, NSW2000, Australia Phone: +61 2 9023 9500	**NOTE:** Repairs to this product may be made only by the manufacturer and its authorized agents, or by others who are legally authorized. Unauthorized repair will void this express warranty.

Mitel Open Interfaces Platform (OIP)

The wide-range of OIP functions significantly broadens the use of the communication server and offers a seamless connection of PC and telephony applications.

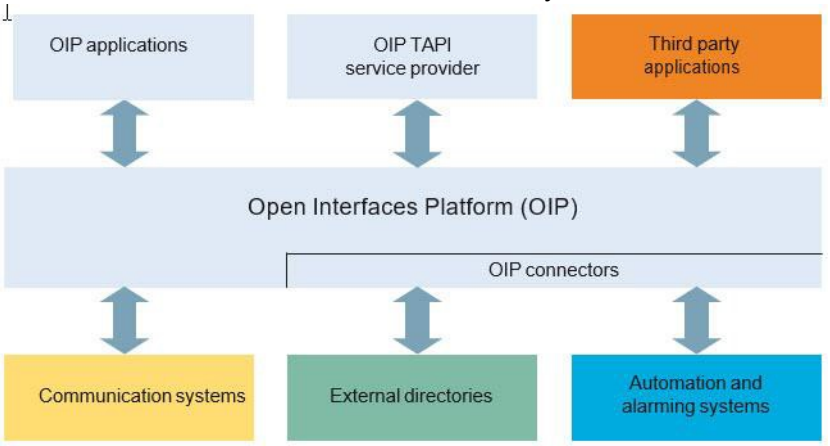
With the OIP-integrated applications you can implement more demanding Unified Communications solutions. OIP offers a versatile trunk group with sustainable extensions, together with operator applications and call center functions.

You can integrate, for instance, additional sector-specific applications via the OIP interfaces and OIP connectors.

OIP is also a directory server which, in addition to the directories of connected communication servers, integrates external directories into the communications landscape.

- OIP can be deployed:
- on a PC (Windows operating system)
- via the application server CPU2/CPU2-S.
- The application server CPU2/CPU2-S is a PC plug-in card for the Mitel 470 communication server and is pre-installed ex works with OIP and other extensions.
- as Virtual Appliance on VMware ESXi or Microsoft Hyper-V
- as a container application on the Mitel SMBC platform.

Figure 2.1: OIP as a link for communication systems, directories 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 organization 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 either as rich-client application together with a fixed, cordless phone or Softphone.

Areas of Operation

OIP as Directory Server

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

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

Moreover, Microsoft Exchange directories can be directly synchronized.

Unified Communications - OIP as Telephony Server

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

OIP as Operator Centre

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

OIP as Free Seating Server

OIP supports and expands the MiVoice Office 400 free seating function: A user logs on at a free seating workstation and the phone automatically takes over his call number and device configuration.

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 and 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 in an 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 optimize 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 Automation and Alarm System

External alarm systems and building automation equipment (for example, 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 their 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:

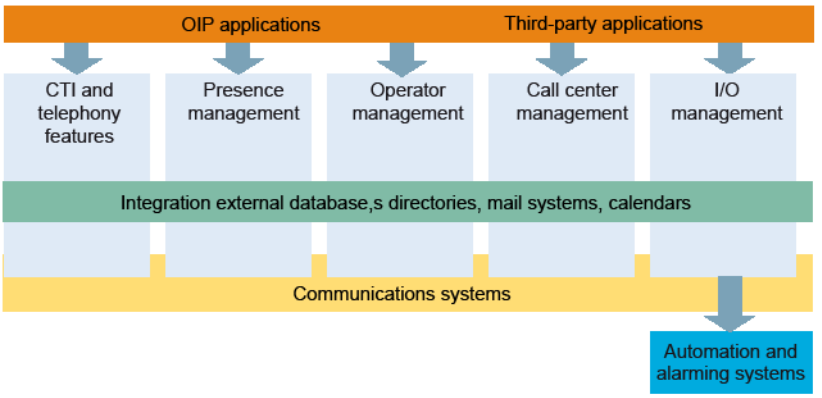
- Alarming equipment for maintenance personnel
- Monitoring of production processes
- Forwarding messages as e-mails
- Connection to building automation systems (KNX)

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.

Figure 2.2: Functions and interfaces



Features

Overview of available OIP features:

Table 2.1:Telephony functions/CTI (Sheet 1 of 2)

Features	MiVoice Office 400	Mitel OfficeSuite[1]	License[2]
Telephony functions/CTI for system phones:			
• Outgoing dialing	X	X	CTI Third-party Basic
• Call waiting	X	X	CTI Third-party Standard
• Rejecting a call during the ringing phase	X	X	CTI Third-party Standard
• Answer call	X	X	CTI Third-party Basic
• End call	X	X	CTI Third-party Basic
• Fetch call	X	X	CTI Third-party Basic
• Deflecting a call during the ringing phase (Call Deflection)	X	X	CTI Third-party Standard
• Calling line identification (CLIP)	X	X	CTI Third-party Basic
• Call forwardings: Unconditional (CFU), no response (CFNR), busy (CFB), do not disturb	X	X	CTI Third-party Standard
• Frequency dialing (DTMF)	X	X	CTI Third-party Basic
• Call charge information	X	X	CTI Third-party Basic

Table 2.1:Telephony functions/CTI (Continued) (Sheet 2 of 2)

Features	MiVoice Office 400	Mitel OfficeSuite[1]	License[2]
• Call transfer without prior notice	X	X	CTI Third-party Standard
• Call transfer	X	X	CTI Third-party Standard
• Hold	X	X	CTI Third-party Standard
• Conference	X	X	CTI Third-party Standard
• Brokering	X	X	CTI Third-party Standard
• Message to busy user	X	X	CTI Third-party Standard
• Park	X	X	CTI Third-party Standard
• Call back	X	X	CTI Third-party Standard
• Announcement to user	X		CTI Third-party Standard
• User-defined functions (macros/function commands)	X	X	CTI Third-party Standard
Telephony functions/CTI for analogue phones:			
• Outgoing dialing			CTI Third-party Basic

1. The Office Suite license contains all features and functions of the Basic CTI and Standard CTI license.
2. For more information about the licenses, refer to *"System limits and licensing"*.

Table 2.2:Presence profiles (Sheet 1 of 2)

Features	MiVoice Office 400	Mitel OfficeSuite[1]	License[2]
Presence profiles:			
• Create several presence profiles	X	X	Profiles Presence
• Set presence status	X	X	Profiles Presence
• Forwarding destinations (CFx) for internal calls		X	Profiles Presence
• Forwarding destinations (CFx) for external calls		X	Profiles Presence
• CFU (unconditional) forwarding destinations	X[3]	X	Profiles Presence

Table 2.2:Presence profiles (Continued) (Sheet 2 of 2)

Features	MiVoice Office 400	Mitel OfficeSuite[1]	License[2]
• CFB forwarding destinations (on busy)	X[c]	X	Profiles Presence
• CFNR forwarding destinations (on no answer)	X[c]	X	Profiles Presence
• Display profiles	X	X	Profiles Presence
• Voice mail profiles	X	X	Profiles Presence
• Notification profiles	X	X	Profiles Presence
• Display profiles	X	X	Profiles Presence
• Audio profiles	X	X	Profiles Presence
• Control via OIP calendar or external calendar (for example, Microsoft	X	X	Microsoft Exchange Connector/Profiles Presence

1. The Office Suite license contains all features and functions of the Basic CTI and Standard CTI license.
2. For more information about the licenses, refer to *"System limits and licensing"*.
3. Only a CFx type possible at the same time

Table 2.3:Call Centre and Work groups (Sheet 1 of 2)

Features	MiVoice Office 400	Mitel OfficeSuite[1]	License[2]
Mitel 400 Call Center:			
• Agent management (login and log out, pause, wrap-up)	X		Call Centre Agents
• Call routing (cyclic, linear, PBX cyclic, skill, CLIP, last agent)	X		Call Centre Base / Call Centre Groups
• Online and offline call centre statistic (export to Microsoft Excel), with graphic display	X		Call Centre Base / Call Centre Groups
• Expansion with the Mitel 400 CCS evaluation application	X		see "The OIP licenses"
• Emergency Routing	X		Call Centre Base / Call Centre Groups

Table 2.3:Call Centre and Work groups (Continued) (Sheet 2 of 2)

Features	MiVoice Office 400	Mitel OfficeSuite[1]	License[2]
• Business hours	X		Call Centre Base / Call Centre Groups
• Login and log out, pause, wrap-up	X		Call Centre Agents
• Call tickets	X		Call Centre Base / Call Centre Groups

1. The Office Suite license contains all features and functions of the Basic CTI and Standard CTI license.
2. For more information about the licenses, refer to *"System limits and licensing"*.

Table 2.4:OIP server and communication server link (Sheet 1 of 2)

Features	MiVoice Office 400	Mitel OfficeSuite[1]	License[2]
OIP server:			
• Configuration of system phones	X	X	CTI Third-party Basic
• Call lists (e-mail notification in the case of unanswered calls)	X	X	CTI Third-party Basic
• PUM - Personal User Mobility (multi-user workstation sharing)	X		CTI Third-party Basic
• Time synchronization with the communication server	X		CTI Third-party Basic
Presence Indicator:			
• Presence Indicator via all OIP users	X	X	CTI Third-party Basic / Office Suite
• Synchronization of the presence states with the communication server	X	X	-
• Synchronization of the presence states with Outlook using Micro-soft Exchange	X	X	Microsoft Exchange Connector
• Synchronization of the presence states with local Outlook using Mitel OfficeSuite		X	Local Outlook Connector

Table 2.4:OIP server and communication server link (Continued) (Sheet 2 of 2)

Features	MiVoice Office 400	Mitel OfficeSuite[1]	License[2]
• Absence message at caller with system phones	X		Microsoft Exchange Connector
User access control:			
• User management (licenses, access rights)	X		CTI Third Party Basic
• User group management	X		CTI Third Party Basic
Communications server link:			
• Connection to stand-alone systems	X		Connectionto <communication server> / CTI Connection to <communicationserver>
• Connection to QSIG-networked systems	X		
• Connection to an AIN	X		

1. The Office Suite license contains all features and functions of the Basic CTI and Standard CTI license.
2. For more information about the licenses, refer to *"System limits and licensing"*.

Table 2.5:Notification (Sheet 1 of 2)

Features	MiVoice Office 400	Mitel OfficeSuite[1]	License[2]
Notification of the following events:			
• Answered and unanswered calls	X	X	CTI Third-party Basic / Office Suite
• Voice mail messages from the standard voice mail system	X	X	CTI Third-party Basic / Office Suite
• Textmessages received	X	X	Profiles Presence
• E-mail message	X	X	Microsoft Exchange Connector
• Calendarevents	X	X	Microsoft Exchange Connector
• I/O Events:	X	X	Profiles Presence

Table 2.5:Notification (Continued) (Sheet 2 of 2)

Features	MiVoice Office 400	Mitel OfficeSuite[1]	License[2]
• Display on a phone (ATAS)	X	X	CTI Third-party Basic / Office Suite
• Textmessage	X	X	CTI Third-party Basic / Office Suite
• E-mailmessage	X	X	CTI Third-party Standard
• E-mail message with attached voice mail message of the standard voice mail system (wav or mp3)	X	X	CTI Third-party Standard
• Triggering of an I/O event	X	X	Profiles Presence
Notification: Other features			
• Allocation of filtering rules	X	X	Profiles Presence

1. The Office Suite license contains all features and functions of the Basic CTI and Standard CTI license.
2. For more information about the licenses, refer to *"System limits and licensing"*.

Table 2.6:OIP applications and OIP configuration

Features	MiVoice Office 400	Mitel OfficeSuite[1]	License[2]
OIP applications:			
• Mitel OfficeSuite: PC control and configuration application for hard phones connected to the system	X		Office Suite
• Operator applications MiVoice 1560 PC Operator			MiVoice 1560 / MiVoice 1560 IP
• Telephony, CTI, agent control via OIP WebAdmin	X		CTI Third-party Basic or CTI Third-party Standard
OIP configuration:			
• Configuration via OIP WebAdmin	X		No license required

1. The Office Suite license contains all features and functions of the Basic CTI and Standard CTI license.
2. For more information about the licenses, refer to *"System limits and licensing"*.

Table 2.7:Call logging

Features	MiVoice Office 400	Mitel OfficeSuite[1]	License[2]
Outgoing (OCL)	X		CTI Third-party Basic
Incoming (ICL)	X		CTI Third-party Basic
Individual charge counting (ICC)	X		CTI Third-party Basic
Cost centres	X		CTI Third-party Basic
Exchange line circuit counter	X		CTI Third-party Basic
Call charge display on system phones (throughout the network)	X		CTI Third-party Basic
Call data analysis	X		CTI Third-party Basic
Data export (in csv format)	X		CTI Third-party Basic

1. The Office Suite license contains all features and functions of the Basic CTI and Standard CTI license.
2. For more information about the licenses, refer to *"System limits and licensing"*.

Table 2.8:Directories and databases (Sheet 1 of 2)

Features	MiVoice Office 400	Mitel OfficeSuite[1]	License[2]
Connection and access:			CTI Third-party Basic
• Connecting OpenComdirectories			CTI Third-party Basic
• Local Microsoft Outlook connection		X	Local Outlook Connector
• Connection of Microsoft Exchange	X		Microsoft Exchange Connector
• Connection to LDAP directories	X		Phonebook Connector
• Access to the external phone-book directory TwixTel (CH)	X		Phonebook Connector
• Access to the Das Telefonbuch external phone-book directory (DE).	X		Phonebook Connector
• Access to the global address list of the Active Directory	X		Phonebook Connector
• Import/export of other directories		X	CTI Third Party Basic

Table 2.8:Directories and databases (Continued) (Sheet 2 of 2)

Features	MiVoice Office 400	Mitel OfficeSuite[1]	License[2]
Directory functions:			
• Search in directories with dialing by name	X		Phonebook Connector/ Microsoft Exchange Connector
• Search in directories with Quick-dial dialing by name	X		Phonebook Connector/ Microsoft Exchange Connector
• Name display	X	X	Phonebook Connector/ Microsoft Exchange Connector
• Synchronization of communication server directories– Microsoft B-Channels on PRI Cards directories	X	X	Microsoft Exchange Connector
Outlook connection via Microsoft Exchange or locally via Mitel OfficeSuite:			
• Data source for private contacts.	X		Microsoft Exchange Connector or Local Outlook Connector
• Integration of the public contact folders	X		Microsoft Exchange Connector or Local Outlook Connector
• Integration of the private calendar	X		Microsoft Exchange Connector or Local Outlook Connector
• Integration of e-mails	X		Microsoft Exchange Connector or Local Outlook Connector

1. The Office Suite license contains all features and functions of the Basic CTI and Standard CTI license.
2. For more information about the licenses, refer to *"System limits and licensing"*.

Table 2.9:OIP TAPI service provider (CTI)

Features	MiVoice Office 400	Mitel OfficeSuite[1]	License[2]
Microsoft TAPI 2.1	X		CTI Third-party Standard or CTI Third-party Standard
Telephony functions	X		CTI Third-party Standard or CTI Third-party Standard
Call centre functions	X		Call Centre Base / Call Centre Groups / Call Centre Agents / CTI Third-party Standard
Key telephone functions (see *"Key telephones, PC operator consoles and phones"*	X		CTI Third-party Standard
Operator console functions (see *"Key telephones, PC operator consoles and phones"*	X		CTI Third-party Standard

1. The Office Suite license contains all features and functions of the Basic CTI and Standard CTI license.
2. For more information about the licenses, refer to *"System limits and licensing"*.

Table 2.10:Automation and Alarm Systems

Features	MiVoice Office 400	License[1]
ATAS gateways with extended functional scope	X	ATAS Gateway2) / CTI Third-party Basic
DECT locating	X	ATASproGateway[2]
Evaluate and forward the communication server (for example, as e-mail)	X	ATASGateway[b]
Bidirection alarm interface (phone to external, external to phone)	X	ATASGateway[b]
KNX interface (European Installation Bus)	X	ATASGateway[b]
I/O system with extended system functions for customized adaptations	X	ATASGateway[b]

1. For more information about the licenses, refer to *"System limits and licensing"*.
2. For MiVoice Office 400 activate the ATAS Gateway and ATASpro Gateway licenses on the communication server. OIP then takes the licenses.

3) Only with a single radio unit

Table 2.11:Key telephones, PC operator consoles and phones

Features	MiVoice Office 400	License[1]
Key telephones:		
• Outgoing dialing from line keys	X	CTI Third-party Standard
• Answering calls on line keys	X	CTI Third-party Standard
Operator consoles and PC operator consoles:		
• Outgoing dialing from line keys	X	CTI Third-party Standard
• Answering incoming calls from a queue	X	CTI Third-party Standard
• Parking calls in the queue	X	CTI Third-party Standard
• Logging on, logging off, wrap-up, break	X	CTI Third-party Standard
• Operator groups	X	Call Centre Base/ Call Centre

1. For more information about the licenses, refer to *"System limits and licensing"*.

OIP server

In this chapter you will find all information on how to set up and put the OIP server into operation. Moreover, all central OIP services and features are described.

Planning Instructions

Signalling and Signalling Paths

The OIP server communicates with the communication server via Ethernet. OIP server and communication server exchange both time-critical signalling and control data and information data such as voice mail data. The OIP server itself does not process any real-time media data. The media stream flows directly between the communication server and the terminals, the OIP applications or the CTI applications of third-party manufacturers.

OIP applications and CTI applications also communicate with the OIP server via Ethernet.

OIP IP softphones are handled in the same way as IP system phones by the communication server:

- Voice transmission is effected via the VoIP channels.
- The media stream flows directly between IP softphone and communication server.
- The user data is stored in the communication server.

But unlike IP system phones the OIP server signals and controls the OIP IP softphones itself. The OIP server also handles the IP addressing of the IP softphones in the communication server, making manual configuration superfluous.

OIP Rich Client applications that are coupled with a system phone do not themselves process any media data, and the media stream flows between the coupled system phone and the communication server.

When an OIP server is operated in an Mitel Advanced Intelligent Network the OIP server communicates with the Master node only.

Compatible Communications Servers

The following communication servers can be connected to OIP R8.9.0.1:

- MiVoice Office 400 communication server as of Release R6.0

Networking is via the IP network.

PC Requirements

PC for OIP Server

The following requirements and limitations must be taken into consideration to guarantee safe and high-availability of the OIP server. Note that the system and performance limits of OIP also depend on the performance of the server PC (see *"System limits"*).

Table 3.1:OIP client PC requirements and limitations

Criterion	Requirement/recommendation
System specifications for operation with a client operating system	The minimum requirement is the requirement of the operating system used.
System specifications for operation with a server operating system	The minimum requirement is the requirement of the operating system used.
Supported operating systems	See Release Notes. Recommended for 50 or more users
Use of a server operating system	Permissible in principle. Applications with substantial RAM and computing power requirements should be operated on a different PC in order not to affect the performance of OIP.
Use of other applications on the same PC	Not recommended, to ensure OIP server availability and avoid compatibility problems
IIS installation on the same server	The minimum requirement is the requirement of the operating system used.
Real-time search for antivirus software	To be deactivated for the OIP directory

PC for OIP Clients

Make sure an OIP client PC meets with the following requirements.

Table 3.2:OIP client PC requirements and limitations

Criterion	Requirement/recommendation
System specifications	The minimum requirement is the requirement of the operating system used.
Supported operating systems	See Release Notes.
Use on a virtual client	Not allowed

For the installation of an IP-Softphone the PC has to be equipped with a headset or handset.

Compatible Operating Systems

Table 3.3:Compatibility with Operating Systems

Operating system X = supported	OIP server	Mitel OfficeSuite	MiVoice 1560 PC Operator	Mitel 400 CCS main services	Mitel 400 CCS supervisor client	OIP TAPI service provider	Exchange Driver
Windows 10[1]	X	X	X	X	X	X	
Citrix/ terminal server environment		X	X				
Windows Server 2012 R12	X	X	X	X	X	X	
Windows Server 2016	X	X	X	X	X	X	
Windows Server 2019	X	X	X	X	X	X	
VMWare ESXi 5.5	X						
VMWare ESXi 6.0	X						
VMWare ESXi 6.5	X						
VMWare ESXi 6.7	X						
Microsoft Hyper-V	X						
Microsoft Exchange Server 2013							X
Microsoft Exchange Server 2016							X
Microsoft Exchange Server 2019							X
Microsoft 365 for Business[2]							X

1. Home editions of windows are not supported
2. Microsoft 365 for Home is not supported

NOTE: The installation of the OIP server on a Windows Small Business Server is not supported.

Further PC Requirements

Installing Microsoft Security Updates

It is urgently recommend the installation of Microsoft security updates for all PCs on which Mitel applications are installed.

There is only a small risk of problems occurring after a PC is updated. Mitel cannot test the security updates in advance, just as it cannot test all possible hardware and software combinations. However, during operations and tests inside the company the applications are always deployed with the latest security updates, so that any problems can be rapidly detected.

Updating Java Runtime Environment (JRE) on Server and Client PCs

(Automatic) update of Java Runtime Environment (JRE) with CTI applications is not recommended on server PCs. Applications are optimised on specific JRE versions. Although it is possible for several JRE versions to run on the same PC, in reality, a JRE update often results in errors and, thus, to support cases. This is especially the case if new application components are installed or if already installed components are updated.

The CTI server applications provided by Mitel are normally always compatible with the latest JRE version available at the time of product release. The used JRE version is clearly defined. However, hitch-free operation with other JRE versions cannot be fully guaranteed. Therefore, it is advisable to use only the recommended JRE version without updating it.

You can update JRE on client PCs without worry.

Using Antivirus Software on Server PCs

Basically, the use of antivirus software on server PCs with CTI server applications is conflict-free and recommended. Nevertheless, the antivirus software must be configured in such a way that all data concerned by real-time processing is not scanned. For example, the operating MYSQL directory of the OIP server database must be excluded from OIP operations. The same exclusion applies, among others, to the Open Desk and Open Messsaging applications. We also recommend excluding from the scanned directory the call data and ACD statistics written by the application.

Using several antivirus programs from different manufacturers should not pose any problems.

IP Requirements

Note that a network environment must only be optimized a competent network technician.

Check the following points before installing the OIP server and integrating it into your IP network:

- The DNS is correctly configured.

Integrating OIP in the existing IP network requires additional bandwidth.

Communications between OIP Server and Communication Server

Communications between OIP server and the communication server take place

- when the OIP server is started,
- when the OIP server synchronizes with the communication server,
- during the runtime.

The required bandwidth depends on the following factors:

- The size of the communication server configuration during startup and synchronization
  - The number of internal users
  - The number of call distribution elements (CDE)
  - The entries in the abbreviated dialing list/PISN users
  - The entries in the private phone books
- The number of internal and external calls made (calls per hour)

The average network load during runtime can be influenced by the settings used for the various synchronization intervals. The synchronization intervals can be configured in the OIP Services.

Table 3.4:OIP server – PBX synchronization

Synchronization interval	OIP Service	Default setting
OIP server PBX configuration	PBX Manager	all 15 min
OIP server PBX abbreviated dialing directory	Public Directory Service	all 60 min
OIP server PBX private phone books	Private Directory Service	all 60 min

Communications between the OIP Server and the OIP Applications

For the communication between the OIP server and the OIP applications during the runtime, the bandwidth depends on the following factors:

- The number of internal and external calls made (calls per hour)
- The number of monitored users for each application (for example, Presence Indicator)
- Number of configuration modifications via OIP WebAdmin.

Communications between OIP server and Microsoft Exchange Server

For communications between OIP server and the Microsoft Exchange Server the bandwidth depends on the following factors:

- Number of abbreviated dialing list entries.
- The number of entries in the private phone books.
- The number of entries in the public contacts folder on the Microsoft Exchange Server.

- The number of entries in the private Microsoft Outlook address books.

The synchronization intervals between PBX, OIP Server and Microsoft Exchange Server are set in the OIP Services, see *Communication between OIP sever and Communication server"*.

Communications between IP-Softphone and PBX

To achieve a high voice quality when using IP Softphones, it is important to dimension and plan the IP network carefully with the same care as when planning IP Hardphones or an AIN system (MiVoice Office 400).

Connection via WAN Links

WAN connections should be implemented via virtual private networks (VPN) to protect the call data and due to the problems with firewalls (dynamic port allocations).

Firewall Management

When firewalls are used between communication sections of PBX, OIP server and OIP clients, some ports must be opened.

Firewall in front of the Communication Server

If the communication server is behind a firewall, the following ports must be opened incoming:

Table 3.5:MiVoice Office 400 IP ports:

Interface	TCP port
Configuration	1061/1062/1080[1]
OIP Name Server	1070
Telephony	1074
Alarming	1088
Ascotel OIP Information Link	1112

1. Ports for outputting event messages and call charge data can be configured in the communication server with WebAdmin. The values specified here are the default values of the PBX.

Firewall on the OIP Server

If the OIP server is protected by a firewall, the following ports must be opened incoming:

Table 3.6:IP Ports OIP Server

OIP server component	TCP port
OIP server	2809
OIP Web server	80[1]
PBX alarms	1062
Call charge data	1080
OIP database	3308

1. The port for the OIP web server can be defined when the OIP server is installed. The value specified here is the default value.

Network Bandwidth

When dimensioning the network bandwidth in LAN environments it is important to make sure that the LAN environments are implemented or adapted with switches instead of hubs.

WAN links in particular are critical during the dimensioning process.

Firewall on an OIP Client

If an OIP client (PC with an OIP application) is protected by a firewall, the following ports must be opened incoming:

Table 3.7:IP ports OIP applications, OIP TAPI service provider and OIP connectors (Sheet 1 of 2)

OIP application	TCP Ports
I/O Manager	Free port[1]
Mitel OfficeSuite	Free port
MiVoice 1560 PC Operator	Free port
OIP TAPI service provider	Free port
OIP VoIP media driver	60201 - 60300
OIP action server	60801 - 60900
OIP exchange driver	60001 - 60100
OIP ODBC/JDBC driver	63001 - 63010
OIP TwixTeldriver	60101 - 60110
OIPDasTelefonbuchdriver	60111 - 60120
OIP ISDN media driver	60901 - 60910

Table 3.7:IP ports OIP applications, OIP TAPI service provider and OIP connectors (Continued) (Sheet 2 of 2)

OIP application	TCP Ports
OIP ATASGateways	61001 - 61010
OIP KNX driver	60501 - 60600

1. A free port is searched for and occupied

System Limits and Licensing

The finely tuned licensing policy used for the OIP applications, OIP functions and OIP connections means that OIP's powerful functionality can be tailored precisely to requirements, and its costs optimized.

System Limits

The system limits of OIP depend on the PC used and the operating system. The following values are approximate and intended as a guideline. It is recommend that you contact Support if the system load exceeds one or more of the following values.

Table 3.8:OIP system limits

	Integrated	Basic	Standard	Complete configuration
OIP user	200	50	300	1'200
Calls per hour	1'000[1] and 500[2]	1'000	2'000	3'000
CTI clients	200[a]	50	300	1'200
Mitel OfficeSuite	200[a]	50	300	1'200
MiVoice 1560 PC Operator	5[a] and 3[b]	5	16	32
CTI agents/skills	50/501) and 20/502)	50/50	100/100	150/150
PC	Applications card (CPU2)[a] and Docker container[b]	Intel Dual Core 1.2 GHz, 1 GB RAM,	Intel Dual Core 2 GHz, 2 GB RAM,	Intel Quad Core 3 GHz, 4 GB RAM,
Operating system	Integrated	Client operating system	Server operating system	Server operating system

1. Mitel 470
2. SMBC

NOTE: The communication servers connected also influence the system limits: Smaller communication servers (for example, Mitel 415) or several communication servers lower the OIP system limits. You can offset this by using a more powerful PC.

Maximum number…	OIP	Remarks
CTI user Agents	1200 250	This is the maximum value of OIP. The maximum value during operation depends on the connected communication system.

Handling OIP Licenses

You can obtain OIP licenses directly via the license server or through your dealer. You will receive a license file which contains, in addition to the license key, a list of all activated OIP licenses. The OIP server reads the license code from the license file and manages the licenses independently of the communication server licenses.

To read the license information into OIP, proceed as follows:

If you have not yet installed OIP:

1. Copy the OIP license file to your PC.
2. Start the OIP installation and follow the instructions of the installation assistant.
3. At a certain stage of the installation process you will be prompted to indicate the storage location of the OIP license file.
4. Indicate the storage location of the OIP license file then continue with the installation.
5. The OIP license file is copied to the OIP basic directory. When OIP is started, the licence number is loaded and the available OIP licenses are activated.

If you have already installed OIP:

1. Store the OIP license file in your file system.
2. Load the OIP license file with OIP WebAdmin (*Licenses* view) on the OIP server and restart the OIP server.
3. Click *Upload* then, in the following dialogue, allow the OIP server to restart. The OIP server restarts with the new license information.

The OIP Licenses

Basic Operation

The basic operation of the OIP server requires a fully operational, permanently assigned communication server and an OIP license which enables the connection to the communication server. Any other communication server on the same OIP server requires an additional connection license.

The CTI connection license restricts the scope of functions to TSP applications.

Table 3.9:Communications server connection licenses

License	Description
Connection to <communication server>	License for operating one or more communication server with OIP. The systems are specified in the license file with their EID number (MiVoice Office 400). The license is valid only for the specified communication server systems.
CTI Connection to <communication server>	Same as Connection to *<communication server>* but restricted to TSP applications with OIP (CTI third party).
PBX Master	This is not a purchasable license: The communication server added first is declared as the PBX Master. The PBX Master must be permanently connected with OIP so that the other licensed communication servers remain enabled for operation with OIP. The OIP server checks the connection every 24 hours. If the communication server is not connected with the OIP server during two successive checks, all the connected communication servers are disconnected from the OIP server.

OIP Applications

The OIP applications are available on the OIP server and can be installed from it, providing the relevant licences have been acquired. The OIP application licences contain all the rights required to operate the application in its basic function.

The license of an OIP application enables all the OIP features required for its operation.

Table 3.10:Licenses for operator applications (Sheet 1 of 2)

License	Description
Office Suite	Mitel OfficeSuite user license

Table 3.10:Licenses for operator applications (Continued) (Sheet 2 of 2)

License	Description
MiVoice 1560	MiVoice 1560 user license
MiVoice 1560 IP	MiVoice 1560 IP user license

Connecting External Directories

The following licenses activate the access to various directories from third-party manufacturers.

Table 3.11:Licenses for connecting directories and specific third-party applications

License	Description
Phonebook Connector	License for connecting the following electronic directories to OIP: • "TwixTel", phone book for Switzerland • "Das Telefonbuch", phone book for Germany • Microsoft Active Directory as directory database. • LDAP databases as directory databases. You need a license for each directory type you want. Activating the license also activates the name server. This allows not only OIP but also the communication server access to the connected directories.
Microsoft Exchange Connector	License for connecting a Microsoft Exchange server to synchronize contacts, calendar entries, presence states to OIP, and for e-mail integration. Activating this license also activates the name server. This allows not only OIP but also the communication server access to the connected directories.
Local Outlook Connector	License for connecting a locally installed Outlook for synchronizing contacts, calendar entries, presence statuses on OIP and for the e-mail connection. The name server is not activated with this license. To allow the communication server direct access to the Outlook directory, you must also activate either the Microsoft Exchange Connector license or Phonebook Connector license. The communication server's access to the Outlook directory is required, for instance, to allow name dialing or the CLIP solution on a phone via the Outlook directory. **NOTE:** OIP applications, such as Mitel OfficeSuite or MiVoice 1560 PC Operator, have access to the Outlook directory without name server.

Call Centre - Operation

Activating the following licenses allows the OIP to be used as call centre.

Table 3.12:Call centre licenses

License	Description
Mitel CCS agent	This license allows a call centre agent to be monitored. The license is firmly attached to an agent. Therefore, you will need one license for each agent.
Mitel CCS supervisor	One supervisor client can be used with one of these licenses.
Mitel CCS wall board	One wall board view can be used with one of these licenses. To use the wall board view, the creation of online reports must be activated (*Mitel CCS online* license).

License	Description
Call Centre Base	Activates the call centre functions in OIP and the ACD queue.
Call Centre Groups	Each license allows an agent group to be set up (skill).
Call Centre Agents	This license activates a call centre agent. You need a license for each simultaneously active agent. Example: If 30 agents are working three shifts and a maximum of 8 agents are active in each shift, they need 8 licenses.

Activating the following licenses allows the Mitel 400 CCS application to be used.

Table 3.13:Mitel 400 CCS Licenses

License	Description
Mitel CCS offline	This license is part of the basic package. It activates the offline statistics function and is used to create offline reports.
Mitel CCS online	The online report creation function is activated with this license.

CTI Third-party Applications

Activating the following licenses allows CTI third-party applications to be deployed together with the OIP server.

Table 3.14:Third-party CTI licenses

License	Description
CTI Third-party Basic	Activates the connection to the TSP and the basic telephony features. Supports the telephony functions for a simple CTI application (for instance Office eDial, phone book CD).
CTI Third-party Standard	Activates the connection to the TSP, the basic telephony feature. Supports the necessary telephony functions of a standard CTI application.

These licenses are also required to operate third-party applications which communicate directly with the OIP server and not via TSP.

Presence Profiles

Activating the following licenses extends the OIP function with presence profiles.

Table 3.15:Licenses for OIP features

License	Description
Profiles Presence	Allows (the required number of) presence profiles to be set up.

KNX Connection

Activating the following licenses extends the OIP function with presence profiles.

Table 3.16:Licenses for KNX connection

License	Description
KNX Connection	Allows connection to a KNX system.

Alarm and Location Functions

Activating the following licenses extends the OIP function with alarm and localization functions.

License	Description

TASGateway	License for activating the alarm server function. This license is also required if an external alarm server is connected to the OIP server (activates the ATAS gateway).
ATASproGateway	Additional license for *ATAS Interface*. Releases the OIP DECT location feature and the personal protection function (safeguard).

Trial License

The trial license can only be activated for a limited period. It is used to acquaint oneself with the OIP server and its performance scope.

Table 3.17:Trial license

License	Description
Trial License, Office 1560x, CTI	The trial license enables all the OIP licenses for a period of 60 days (see *"The OIP licenses"*). It is used to test the OIP function.

License Transfer during Upgrade of Older OIP Versions

The OIP licenses as of OIP 7.6 do not have the same coverage scope as the OIP licences of earlier OIP versions. Moreover, license management has changed, because until OIP I7.5 OIP licenses were managed on the communication server. If you upgrade OIP to version I7.6 or higher, OIP continues to read out the licenses from the communication server and converts them. If you activate further licenses, you will receive a license file which contains both the new and transferred licenses. This way, all previously activated functions remain available after the upgrade.

Installation

OIP can be made available as the following variants:

- By installing a CPU2-S Application card for Mitel 470
- By installing OIP on an external MS Windows host
- By deploying OIP as Virtual Appliance on:
- VMWare ESCXi
- MS-HyperV
- By installing OIP as a container application on SMBC

CPU2/CPU2-S Application Card (Mitel 470 only)

Instead of installing OIP on your own server, you can also use a CPU2/CPU2-S application card (Mitel 470 only). OIP and selected additional applications are pre-installed and preconfigured on the application card. The higher level of integration simplifies both the commissioning and the maintenance.

For more details about installation card see *CPU2-S Application Card Installation Guide*.

Log in to OIP WebAdmin

To log in as OIP WebAdmin administrator, enter *cpu2-emmc* as username and use the password which was defined during the initial setup via MiVO400 Multimedia menu.

OIP on an External Microsoft Windows Host

Installation Scope

The following software components are installed during the OIP server installation:

- Microsoft .Net Framework
- MySQL database server
- Java Runtime Environment (JRE)
- Tomcat Web Server
- OIP server
- OIP installation components (optional)

MySQL database server

The MySQL database server is required for the OIP database. The MySQL database server is installed on Port 3308 instead of on the default port 3306. This means that the installation of the OIP server should be independent of an already installed MySQL database. Nonetheless if necessary, check before installing the OIP server that the port is not occupied by another instance of a MySQL database server.

As a matter of principle save a back-up of any existing MySQL databases before installing the OIP server.

The MySQL database server is installed in the directory *OIP Database<OIP-directory>\mysql*. The MySQL database server is started as a Windows service .

More detailed information on the MySQL database server can be found in the MySQL documentation at *http://www.mysql.com*.

Java Runtime Environment (JRE)

It is possible to install and run different versions of Java Virtual Machine on one PC. This ensures that programs already installed continue to run stably during the installation of OIP. If a Java Virtual Machine is already installed on the PC, a check is carried out to see whether it is suitable for the operation of OIP. If not, the supplied version is also installed.

OIP has migrated from Oracle JDK to AdoptOpen JDK.

OIP Installation Components

Experienced administrators, who already know prior to OIP installation which directories they wish to connect or which features they wish to use, can already start with it during the OIP installation. For this, during the installation and in the OIP installation components dialogue window, choose the components

you need. The following installation procedure will take you through the configuration of the selected components.

You can activate and configure the features and services only after the installation.

Table 3.18:OIP installation components (Sheet 1 of 2)

Components	Description
Synchronization of the OIP and PBX directories	OIP synchronizes the OIP directories with the directories of all the connected communication servers. Further information is available in *"Directories Synchronization"*.
OIP Name Server (Dial by name)	With the OIP Name Server it is possible to access the directories connected to the OIP server from the system phones. Further infor- mation is available in *"OIP name server"*.
Connection to a Microsoft Exchange Server	OIP supports the connection of a Microsoft Exchange server to synchronize directories (public contact folders as well as the personal Outlook address books), to access the users' calendars and their e- mail boxes. Depending on the version of the Microsoft Exchange Server the corresponding OIP Exchange driver needs to be installed. Further information is available in *"Microsoft Exchange Server directories"*.
Connection of external phone-book directories	OIP supports the connection of external phone-book directories. The corresponding OIP phone-book driver has to be installed on the phone-book directory server. Further information is available in *"Connectiing external phone-book directories"*.
Alarm logging	The event and alarm reports are stored in the OIP database.
Call logging	The communication server call data are stored in the OIP database. Further information is available in *"Call data"*.
Display Server (ATAS over OIP)	The Display Server is required for controlling the displays of the system phones (e.g. calendar reminders, RSS feeds) and for the alarming and messaging functionality.

Table 3.18:OIP installation components (Continued) (Sheet 2 of 2)

Components	Description
Connection of the Active Directory	OIP supports the connection of the Active Directory. Further information is available in *"Connecting Active Directory"*.
Connectionto LDAP directories	OIP supports the connection of an LDAP directory. Further information is available in *"Connecting LDAP directories"*.
Connection to an SMTP mail server	Connection of an external SMTP e-mail server for sending e-mails. Further information is available in *"E-mail connection via an SMTP mail server"*.
OIP test manager	The OIP Test Manager is used to create scripts to test the functionality of the OIP server (subject to the maintenance personnel).
Connection of KNX systems	Connection of KNX systems to the building services automation Further information is available in *"KNX connection"*.

Configuring the Communication Server

Preparing MiVoice Office 400 for the OIP connection

A user account and a user profile has to be set up for the OIP server before the OIP server is installed on the communication server.

1. Create a new user account for OIP server access in the communication server. Choose "OIP", for instance, as the user name.
2. Assign the user profile *OIP* to the user account that you have just created. The authorisation profile *OIP* is available in the default communication server installation. You can also open it yourself if necessary. Check that the authorisation profile's username is *OIP* and only assign the interface access *OIP*.
3. Save the new user account in the communication server.

OIP Server Installation

The OIP server can be installed on Windows Professional/Server operating systems, see *"Compatible operating systems"*.

To install the OIP server you must have local administrator rights on the server.

Installation Instructions

To install the OIP server, proceed as follows:

1. Have a valid license file *oip.lic* ready (see *"System limits and licensing"*).
2. Start installation by double-clicking on the installation file oipsetup.exe and follow the instructions of the installation wizard.
3. During the installation procedure you will be prompted to enter the communication server to be connected. Enter the communication server on which the OIP server is to be operated by clicking *Add communication server*. For access data use the OIP user account opened in the communication server (see *"Configuring the communication server"*). If you want to operate more than one communication server on this OIP server, insert the PBX master as the first communication server (see also *"Basic operation"*), followed by the others.
4. During the next installation procedure, you have the possibility to select OIP installation components (see *"OIP installation components"*). Change the default selection only as an experienced administrator. You can also make all the directory connections mentioned here after the installation and set up all the listed features after the installation.
5. In a next installation step, you can enter the license file (oip.lic).
6. Before the end of the installation you can decide whether the OIP Windows services should be started. Choose yes and complete installation. If you prefer to start the OIP Windows services manually, start with the Windows service *OIP Database*, followed by the Windows service *OIP WebConfig Server* and *OIP Web Server*. Finally, start the Windows service *OIP Server*.
7. End the installation procedure and read the OIP version instructions carefully. It may contain some information about your OIP version, which is only contained here.
8. Now log on via a browser to OIP WebAdmin to start configuring the OIP server (see next section).

Login to OIP WebAdmin

You can log in to OIP WebAdmin using the internal call number or OIP username. Enter as password the PIN or OIP password. The OIP password must first be saved in the user settings.

Before you can access OIP WebAdmin an appropriate license file has to be loaded into the system. This could be done during the installation (see above) or via the login screen (click on **License file**).

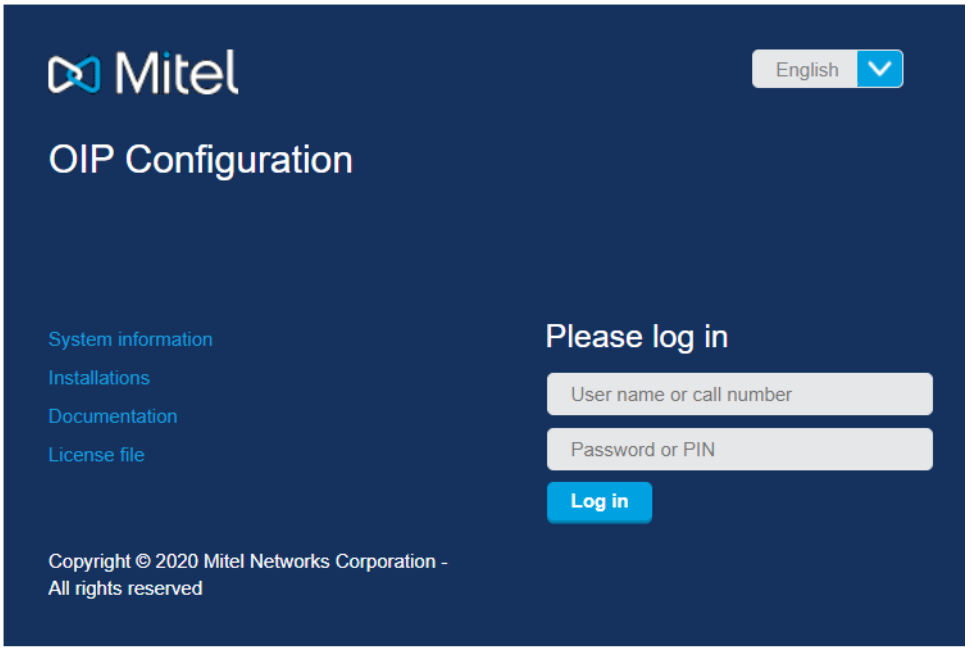
For your first access as administrator, use **oipadmin** as the username and **oipadmin** as the password. You will then be asked to change the password.

The available views depend on the user group to which the logged on user belongs.

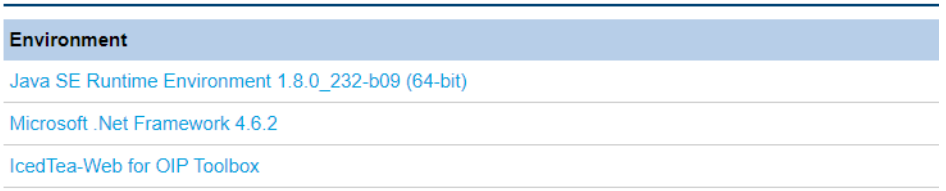
Java Runtime Environment (JRE) for the OIP Toolbox

In order to run the OIP Toolbox, you must install IcedTea-Web for OIP Toolbox. Follow the steps to install IcedTea-Web for OIP Toolbox:

1. From your browser, open the OIP Web application.

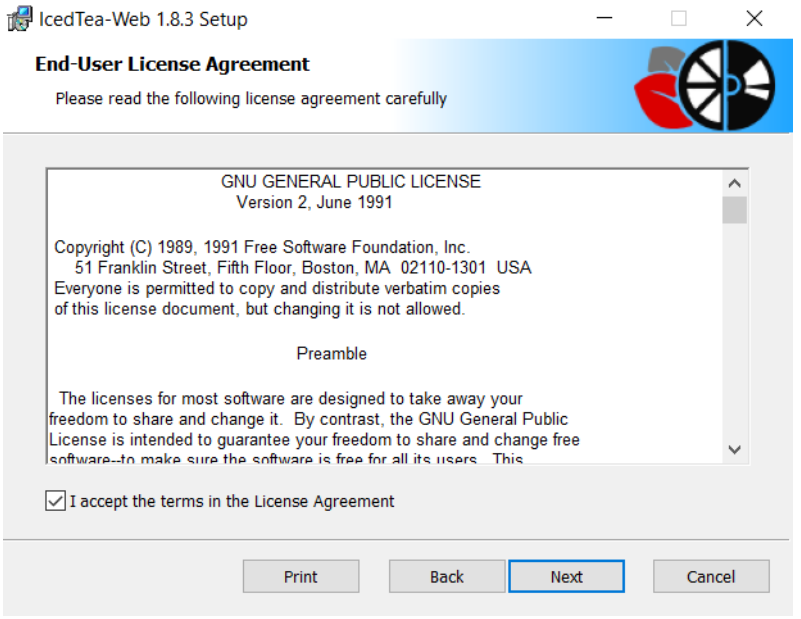


2. Click **Installations**. A new window OIPWebConfig :: Installations is displayed.

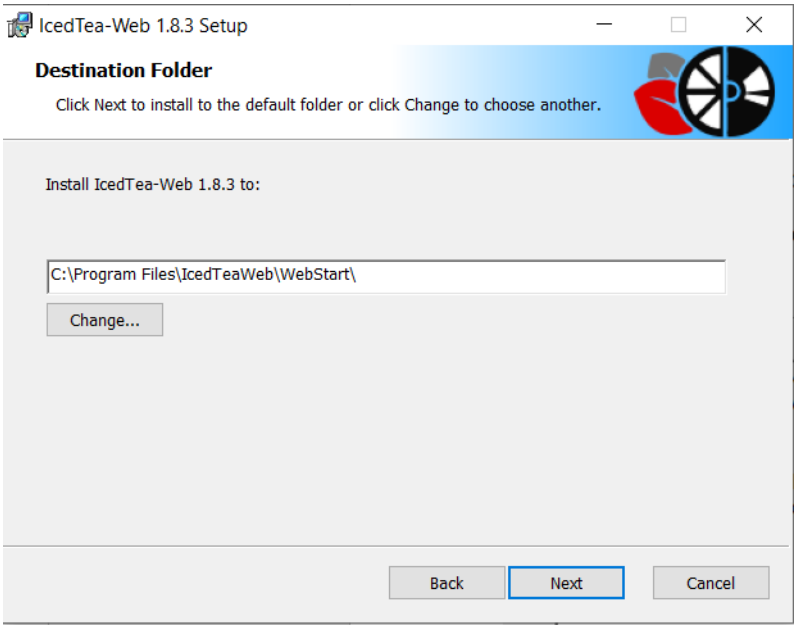


3. Click **IcedTea-Web for OIP Toolbox**. An installation setup is downloaded. Run the setup.

4. Click **Next**. End-User License Agreement wizard is displayed.



5. Select the check box **I accept the terms in the License Agreement** and click **Next**. Destination Folder wizard is displayed.



6. Click **Next**.
7. Click **Install** to install the IcedTea-Web.
8. Click **Finish**.

Uninstalling OIP Server

The OIP server is uninstalled using Control Panel \ Software in the Windows operating system.

The Java Runtime Environment (JRE) is not uninstalled as it may be required by other applications. If you no longer require JRE, you can uninstall it using *Control Panel* \ *Software*.

When uninstalling OIP and JRE completely, make sure you uninstall all the OIP applications and the OIP server first and then the JRE.

Deploying OIP as Virtual Appliance

OIP Virtual Appliance can be deployed on the following virtualization platforms:

- VMware ESXi
- Microsoft Hyper-V

Deploying on VMware

VMware Hardware requirements:

Following are the minimal requirements for the VMware installation:

- ESXi VMware vSphere 5.5, 6.0, 6.5 and 6.7
- Minimum 1 core (2 GHz) up to 4 cores (up to 3 GHz)

- Minimum 2 GB up to 4 GB memory
- 100 GB HDD space

For more information about supported server system see, VMware compatibility list. Follow the below steps to deploy OIP on VMware:

1. Open the vSphere Client / vSphere Web Client.
2. Select Deploy **OVF Template …** and browse for the **OIP8.X.X.X.ova** file which can be downloaded from the Mitel Software Download Center.
3. Enter a name for the virtual machine and select the installation folder.
4. Select **Thick Provision Lazy Zeroed** as virtual disk format.
5. (Optional) Select storage for the configuration and disk files.
6. Select the appropriate network, where the vm should be connected to.
7. Review the summary and click **Finish** to start the deployment process.

Deploying on Hyper-V

Hyper-V hardware requirements:

- Supported on Windows Server 2012R2, 2016 and 2019
- 1 vCPU reserved for the Virtual Appliance up to 4 vCPU
- Minimum 2.0 GHz (> 3 GHz to reach max. limits)
- 2 GB Memory minimum (Memory: Start-up RAM: 2048 MB) up to 4 GB 100 GB HDD space.

For Hyper-V server hardware and host OS requirements refer to Microsoft.com ©.

Follow the below steps to deploy OIP on Hyper-V:

1. Open the Hyper-V Manager.
2. Navigate to **Action** > **New** to create a new virtual machine.
3. Enter a name for the virtual machine.
4. Select **Generation 1**.
5. Assign at least 2048 MB memory (max 4096 MB).
6. Select the appropriate network, where the vm should be connected to.
7. Select **Use an existing virtual hard disk** and browse for the **OIP8.X.X.X.vhd** file which can be downloaded from the Mitel Software Download Center.
8. Review the summary and click **Finish** to start the deployment process.

Initial Configurations of OIP Virtual Appliance

On vSphere client / Hyper-V Manager select the virtual machine. Open a console and start the virtual machine.

The Mitel Standard Linux (MSL) operating system is booted. Follow the below initial steps:

1. Select your keyboard layout.
2. A menu to enter the Application record ID is displayed. Click **Next** to login into the Mitel Standard Linux.
3. Use the default username as admin and the default password as **msloip123** to login. A menu list is displayed.

NOTE: For older OIP VA deployments(that is before release 8.8.0.9), the default password is *password*.

4. Select point 2 **Configure this sever** and do the settings step by step:
    a. Set the “primary domain name” xxx.local (e.g. whateveryouwant.local)
    b. Set a system name (what you need to recognize the system)
    c. Set the “Local networking parameter” -> the desired IPaddress of the OIP Virtual Appliance and set the corresponding subnet mask.
    d. Set enable IPv6 protocol to No.
    e. Set the gateway IP address
    f. Set the DNS server address (this is mandatory here, ignore what is written on the screen)
    g. Set **Resolve** primary domain to **Corporate**.
5. At this point the operating system asks to reboot to take over the settings, click on **Yes**.
6. After the reboot you will be at the same place as above (Application record ID). Click **Next** and login again with the default credentials if you need to setup trusted networks.
7. Select point 8. **Manage trusted networks** and do the settings step by step:
8. Select **Add IPv4 trusted networks** to the gateway address of this virtual machine.

The configuration of your virtual operating system is now completed, you can exit the setup menu.

In case your time zone is different than Central European Time, you need to change the time zone of the virtual machine. You can do this using web-based configuration tool accessible via http://<server_address>:8080, where <server_address> is the address of the Virtual Appliance specified in previous steps. After opening the web-based configuration navigate to “Configuration / Date and Time” and adjust the time zone.

The next step is to configure the OIP Virtual Appliance.

Configuring the Communication Server

Preparing MiVoice Office 400 for the OIP connection.

A user account and a user profile has to be set up for the OIP server before the OIP server is connected to the communication server.

Create a new user account for OIP server access in the communication server. Choose

OIP, for instance, as the username.

Assign the user profile OIP to the user account that you have just created.

The authorization profile OIP is available in the default communication server installation. Save the new user account in the communication server.

Login to OIP WebAdmin

Before you can access OIP WebAdmin an appropriate license file has to be loaded into the system. On the login screen click **License file** to upload a license.

For your first access as administrator, the default OIP Webadmin username is *oipadmin*, the default password *oipadmin*. You will then be asked to change the password. The new password which you enter here has to follow the MSL password rules. A warning is prompted if the password is to weak.

The password entered for the *"oipadmin"* account is also used for the admin and root account on the underlying MSL.

To connect OIP to MiVO400 navigate to **Configuration** > **Server** > **Communication server**. Click the plus (+) icon and enter the relevant data.

A successful connection is established as soon as all MiVO400 user are automatically listed under **Configuration** > **Users** > **User list** > **Section**: Communication server users.

System Update

Existing OIP Virtual Appliance can be updated using the update package (zip file) available on download server. Use "Maintenance / System update" menu point in OIP WebAdmin to select the update package and perform the update.

To update to a newer MSL, save a backup of the oip-server and oip-client data (optional save pictures and other data), perform a new deployment of the .ova / .vhd file and restore the backups.

Migration of an existing OIP to OIP Virtual Appliance

Purchase of a new connection license is mandatory! Transfer of Master EID is possible by Mitel License Server Support (No automated OIP migration process but re-use of existing OIP feature licenses possible by request to Mitel License Server Support.)

Call Center Supervision (CCS)

Currently, it is mandatory that CCS is running on the same server as OIP. Since CCS is not a Linux application, this is not possible! Hence, CCS 2.0 is not compatible with OIP as Virtual Appliance

OIP on SMBC

MiVoice Office 400 Release 6.3 and later releases support integrating Open Interfaces Platform (OIP) as a container application on the SMBC platform along with MiVoice Office 400 and CloudLink Gateway. For earlier releases of MiVoice Office 400, OIP must be installed on a separate external server. Installing OIP

on a separate external server will continue to be supported for MiVoice Office 400 Release 6.3 and later releases.

It is mandatory, that SMBC is running with the Mitel Embedded Linux Distribution 1.2.5.10 (or higher) before OIP is installed on it.

System Limits

The following table contains the device/connection limits for this deployment.

Table 3.19:Summary of support for users, configuration, and call centre agents

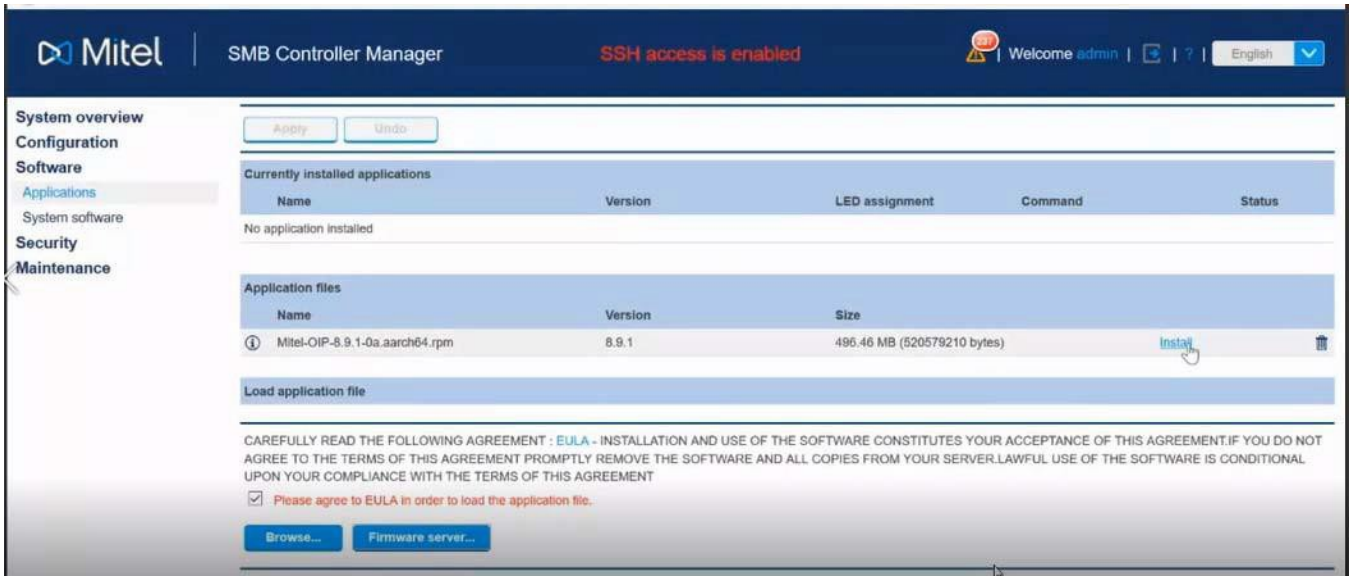
Specific properties	Maximum supported
OIP users	Up to 200 (including PBX users imported to OIP)
Calls per hour	• Up to 500 CPH on the ACD • Up to 1000 CPH on the SMBC including ACD calls (when OIP is installed on SMBC)
ACD	Up to 20 call centre agents / 50 skills
PC Operators	Up to three (1560 or 1560 IP)
External directory sources	Up to three
I/O Team Call	50 users
TAPI connectors	Up to 50 users
Mitel 470 or Virtual Appliance	Not Supported
Call manager	Supported (that must be running on the same hardware)
OfficeSuite and local Outlook connection	Up to 50 users
Software run on MiVoice Office 400 hardware	415-430, 470, SMB Controller, and Virtual Appliance
Interfaces supported/defined	Up to 10 (ethernet interfaces and subnets)

Installation Instructions

To install OIP on SMBC server, proceed as follows:

1. Log in to SMBC Controller Manager Web GUI.
2. On the left pane, navigate to **Software** > **Applications**.
3. Select the **Please agree to EULA in order to load the application file** check box.
4. Click **Firmware server**. A new window opens, displaying a list of available .rpms files for download.
5. Select the OIP .rpm file and click **Load**.

6. Under **Application files**, click **Install**. The OIP will be installed on the SMBC server.



After installing OIP on the SMBC server, the application will be available on <SMB- C_IP>:9443.

The next available LED group is F3/F4 or F5/F6 is assigned. The LED group assignments can be changed.

For information about configuring Mitel OfficeSuite for OIP on SMBC, refer **Mitel OfficeSuite (Rich Client)**.

For information about configuring MiVoice 1560 for OIP on SMBC, refer **Installing and Setting up the Operator Application**.

Configuring the communication server

Preparing MiVoice Office 400 for the OIP connection.

A user account and a user profile has to be set up for the OIP server before the OIP server is connected to the communication server.

Create a new user account for OIP server access in the communication server. Select

OIP, for instance, as the username.

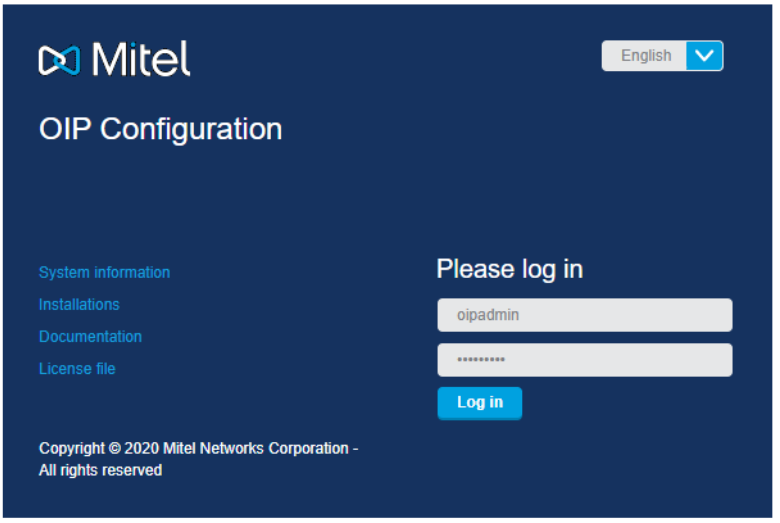
Assign the user profile “OIP” to the user account that you have just created.

The authorization profile OIP is available in the default communication server installation. Save the new user account in the communication server.

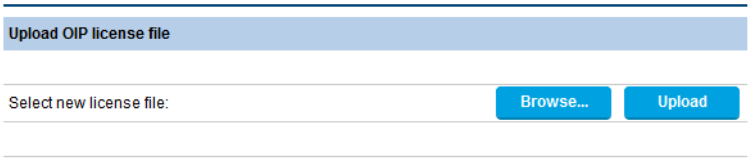
Uploading License and Login to OIP WebAdmin

After the installation, upload the license required to run the OIP application on the SMBC server. Proceed as follows:

1. Open the OIP WebAdmin login page available on *https://<SMBC-IP>:9443*. An alert is displayed **NO LICENSE FILE FOUND. PLEASE UPLOAD IT**.



2. Click **License file**. The Upload OIP license file window is displayed.



3. Click **Browse**.
4. Select the license file and click **Upload**.

For your first access as administrator, the OIP Webadmin username is **oipadmin**, and the default password **oipadmin**. You will then be asked to change the password.

To connect OIP to MiVO400 navigate to **Configuration** > **Server** > **Communication server**. Click the plus (+) icon and enter the relevant data.

A successful connection is established as soon as all MiVO400 user are automatically listed under **Configuration** > **Users** > **User list** > **Section: Communication server users**.

Mitel SMBC LED Indicators

There are nine LEDs on the Mitel SMBC's front panel to indicate system states. They are labeled PWR, F0 through F6, and SYS. Each system application can use two of the F1 through F6 LEDs. The assignment of the LEDs can be configured in the SMBC Manager. The LEDs used by OIP are referred to as LED-A and LED-B.

Table 3.20:LED A: The following table shows the status for OIP Container.

Container status	LED status color
Container down	Red
Container starting	Yellow
Container ready	Green

Table 3.21:LED B: The following table shows the status of the OIP server and the OIP web server:

Server status	LED status color
The OIP server and the OIP web server are both up and running	Green
Either the OIP server or the OIP web server is down	Red

Uninstalling OIP Server

To uninstall OIP on SMBC server, proceed as follows:

1. Log in to SMBC Controller Manager Web GUI.
2. On the left pane, navigate to **Software** > **Applications**.
3. Navigate to **Currently installed applications** section.
4. Select Uninstall from the drop-down list under **Command**, for **Mitel OIP**.

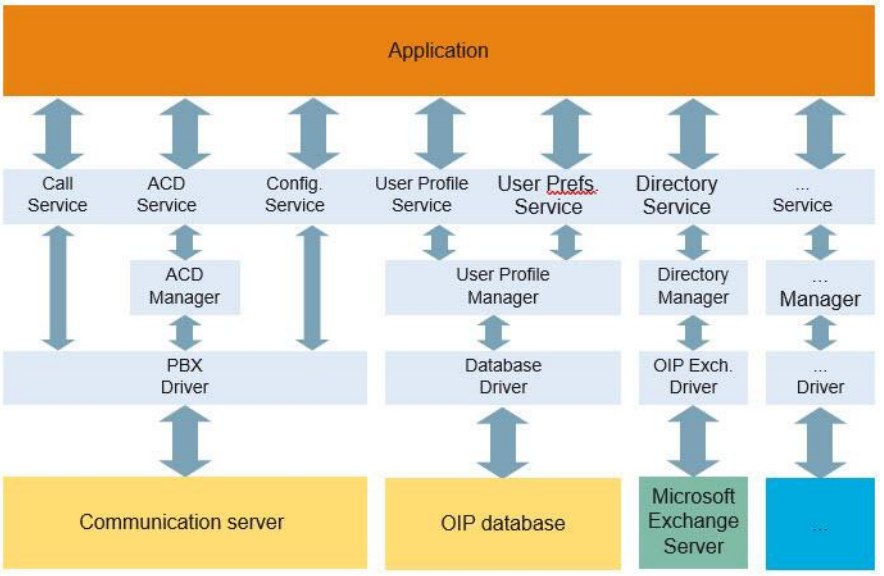
OIP Services

The core of the OIP server are the OIP services in which the individual functions are implemented. The OIP services are functionally dependent on three levels:

- The Driver level components are the OIP services which establish the communication between the connected communication servers and the OIP server. The various protocols for the OIP services of the Manager and Service levels are translated there. OIP applications cannot directly access these OIP services (internal OIP services).

- The Manager level contains the OIP services in which the logic of the individual functionalities of the OIP server is implemented. OIP applications cannot directly access these OIP services (internal OIP services). The Service level has the OIP services which provide the OIP applications with the individual functionalities of the OIP server. Access is controlled via the OIP user groups and the access rights assigned accordingly.

Figure 3.1: Organisation of the OIP services



The basic settings of the OIP services are chosen in such a way that the system can run without any intervention in the configuration.

The following describes the individual OIP services and the setting options. Any changes made should be carried out meticulously so that the system's functionality is not impaired.

The specific properties depend on the individual OIP services. Specific properties cannot be set for every OIP service.

During user group configuration, access rights can be configured to the allocated OIP Services. These access rights are inherited to the users assigned to the user group. If a user is assigned to several user groups within part identical OIP Services, the user always has the highest access right to the OIP Service which he has inherited through the user group.

The below table lists the possible access rights.

Table 3.22:OIP Services access rights (Sheet 1 of 2)

Access right	Description
admin	Full access to the corresponding OIP Service.
groupadmin	The access right allows the OIP Services of all users in the same user group to be started.
super user	The access right allows the OIP Services of all users to be started.

Table 3.22:OIP Services access rights (Continued) (Sheet 2 of 2)

Access right	Description
user	The access right allows only those OIP Services assigned to the user to be started.
guest	Reserved for expansions.
none	No access to the corresponding OIP Service.

Not all OIP Services make a distinction between the different access rights. If the the corresponding OIP service does not specify access rights, the OIP services can be started with the user access right.

Most changes to the settings in the OIP Services can be made while the server is running. If the OIP server has to be restarted, a message appears to prompt a restart of the OIP server.

An overview of the OIP services is given in the following table. Details and settings for the OIP services can be found in the following sections.

Table 3.23:OIP services (Sheet 1 of 8)

OIP Service	Description
Account Service	The Account Service is responsible for booking call charges to specific cost centres.
ACD Log Manager	ACD Log Manager (internal OIP service) is responsible for managing and generating ACD statistics.
ACD Log Service	ACD Log Service is responsible for the access to ACD statistics.
ACD Manager	ACD Manager (internal OIP service) is responsible for managing and configuring the ACD queue.
ACD Service	ACD Service is responsible for the access to ACD queue.
Active Directory Service	The Active Directory Service (internal OIP service) is responsible for managing the Active directories.
Agent Manager	The Agent Manager (internal OIP service) is responsible for the central management of the ACD agents.
Agent Service	Agent Service is responsible for the access to ACD agents.

Table 3.23:OIP services (Continued) (Sheet 2 of 8)

OIP Service	Description
Alarm Driver	You can use the Alarm Driver service to control communication server event and alarm reports on OIP and to store them in the OIP database. The event and alarm reports can be further processed with the I/O system or they can be used in external applications. A view or protocol file is not available.
Alarm Service	You can also use the Alarm Service service to store the communication server's user-specific reports and alarms in the OIP database. Requirement: The alarm log in the Alarm Driver service is enabled.
Alpha & Quick Dial Service	The Alpha & Quick Dial Service (internal OIP service) is responsible for the name resolution, which is sent to the communication server when dialing with names.
Buddy Manager	Buddy Manager (internal OIP service) is responsible for the central management of the user fields.
Buddy Service	The Buddy Service is responsible for accessing the presence indicator and for displaying the status information.
Calendar Manager	Calendar Manager is responsible for the central management of calendar entries.
Calendar Service	Calendar Service is responsible for accessing and controlling the calendar functionality.
Calendar Synchronization Service	The Calendar Synchronization Service (internal OIP service) is responsible for synchronizing the local Microsoft Outlook contacts with the Mitel OfficeSuite.
Call Logging Driver	You can use the Call Logging Driver service to control communication server call data on OIP and to store it in the OIP database.
Call Logging Manager	Call Logging Manager (internal OIP service) is responsible for managing the call data.

Table 3.23:OIP services (Continued) (Sheet 3 of 8)

OIP Service	Description
Call Logging Service	Call Logging Service is responsible for accessing and distributing charge data.
Call Service	Call Service is responsible for managing the telephony features.
Client Utility Service	Client Utility Service provides OIP-specific functions to applications.
CLIP Service	The CLIP Service (internal OIP service) is responsible for the number resolution of incoming calls in the configured directories.
Configuration Profile Manager	Configuration Profile Manager (internal OIP service) is responsible for managing the presence profiles.
Configuration Profile Service	Configuration Profile Service is responsible for accessing the presence profiles of the OIP users.
Configuration Service	Configuration Service is responsible for managing the OIP services.
DasTelefonbuch Directory Service	The DasTelefonbuch Directory Service (internal OIP service) is responsible for managing the external phone-book directories of “DasTelefonbuch Deutschland”.
Database Driver	The Database Driver (internal OIP service) is the interface adapter used for accessing the OIP database.
Directory Manager	Directory Manager is responsible for managing the directories.
Directory Service	Directory Service is responsible for the access to directories.
Display Manager	Display Manager (internal OIP service) is responsible for the management of the access to the system phones’ displays.
Display Service	Display Service is responsible for display control of the system phones.
Event Service	Event Service (internal OIP service) is responsible for distributing the events in the system.

Table 3.23:OIP services (Continued) (Sheet 4 of 8)

OIP Service	Description
Fax Manager	Fax Manager (internal OIP service) is responsible for managing the fax functionality.
Fax Service	Fax Service is responsible for the access to the fax functionality.
Feature Service	The Feature Service provides functions depending on the phone, the CTI license and the communication server type applications.
Flow Manager	Flow Manager (internal OIP service) is responsible for managing the call sequences.
Flow Service	Flow Service is responsible for the access to licenses.
Function Key Manager	Function Key Manager (internal OIP service) is responsible for managing the function keys.
Function Key Service	Function Key Service is responsible for the access to the function keys.
I/O Manager	I/O Manager is responsible for the central management of the I/O groups.
I/O Service	I/O Service is responsible for managing actors.
Jabber Driver	The Jabber Driver (internal OIP service) is the interface adapter used for accessing the external Jabber/XMPP Instant Messaging systems.
Journal Manager	Journal Manager (internal OIP service) is responsible for managing the journal entries.
Journal Service	Journal Service is responsible for managing and deflecting the call lists to the applications.
Key Configuration Service	Key Configuration Service is responsible for key configuration of the system phones.
LDAP Directory Service	LDAP Directory Service (internal OIP service) is responsible for managing the LDAP directories.
License Manager	License Manager (internal OIP service) is responsible for managing the licenses.
License Service	License Service is responsible for the access to licenses.

Table 3.23:OIP services (Continued) (Sheet 5 of 8)

OIP Service	Description
Line Service	Line Service is responsible for managing key telephone features.
Load Balancing Service	Load Balancing Service (internal OIP service) is responsible for the load distribution within the OIP Server Networks.
Location Manager	Location Manager (internal OIP service) is responsible for managing the cordless phone localisation.
Location Service	The Location Service is used to locate cordless phones on the covered premises.
Log Service	Log Service is responsible for the central management and recording of the log files.
Login Service	Login Service is responsible for managing the login to the OIP server.
Media Manager	Media Manager (internal OIP service) is responsible for managing the OIP Media Driver.
Message Manager	Message Manager (internal OIP service) is responsible for managing messages.
Message Service	Message Service is responsible for sending and receiving messages.
Naming Service	The Naming Service (internal OIP service) is responsible for the global management of services in OIP server network systems.
Notepad Service	Notepad Service is responsible for managing the note entries and redial lists.
Notification Manager	Notification Manager (internal OIP service) is responsible for managing the notifications.
Notification Service	Notification Service is responsible for accessing and distributing the notifications.
ODBC/JDBC Directory Service	The ODBC/JDBC Directory Service is responsible for managing connected ODBC or JDBC directories.
Operator Service	Operator Service is responsible for managing the operator queue.

Table 3.23:OIP services (Continued) (Sheet 6 of 8)

OIP Service	Description
PBX Driver Ascotel	PBX Driver Ascotel (internal OIP service) is the interface adapter used for accessing the communication server.
PBX Information Service	PBX Information Service provides information about the connected communication server; for example, the communication server name and users.
PBX Manager	PBX Manager (internal OIP service) is responsible for managing of the communication servers connected to the OIP server.
PBX Setup Manager	PBX Setup Manager (internal OIPservice) is responsible for the configuration of the communication servers connected to the OIP server.
PBX Setup Service	PBX Setup Service is responsible for managing the communication server configuration.
PISN Directory Service	PISN Directory Service (internal OIP service) is responsible for managing the PISN users.
Private Card Directory Service	The Private Card Directory Service (internal OIP service) is responsible for the central management of the communication server private phone book.
Private Directory Service	Private Directory Service (internal OIP service) is responsible for managing the private contacts.
Public Directory Service	Public Directory Service (internal OIP service) is responsible for managing the public contacts.
PUM Manager	PUM Manager (internal OIP service) is responsible for managing the Personal User Mobility function.
PUM Service	PUM Service is responsible for access to the Personal User Mobility data and configuration.
Registration Manager	Registration Manager (internal OIP service) is responsible for managing the registered applications.

Table 3.23:OIP services (Continued) (Sheet 7 of 8)

OIP Service	Description
Registration Service	Registration Service is responsible for registering applications.
Routing Manager	The Routing Manager (internal OIP service) is responsible for managing the call distribution in the communication server.
Routing Service	The Routing Service is responsible for accessing the call distribution in the communication server.
RSS Driver	The RSS Driver (internal OIP service) is the interface adapter used for accessing the RSS Feeds.
Security Service	The Security Service (internal OIP service) provides the encryption and decryption algorithms of security-relevant data for OIP Services.
Server Utility Service	Server Utility Service (internal OIP service) provides internal tools for OIP Services.
Service Manager	Service Manager (internal OIP service) is responsible for the local management of the Services on the OIP server.
Shortdial Directory Service	Shortdial Directory Service (internal OIPservice) is responsible for managing the communication server Abbreviated dialing.
SMTP Driver	The SMTP Driver (internal OIP service) is the interface adapter for sending e-mails and text messages (e-mail to text message).
Subscriber Directory	Subscriber Directory Service (internal OIP service) is responsible for managing the internal private contacts.
Subscriber Configuration Manager	Subscriber Configuration Manager (internal OIP service) is responsible for managing the user settings.
Subscriber Configuration Service	Subscriber Configuration Service is responsible for user and terminal settings.

Table 3.23:OIP services (Continued) (Sheet 8 of 8)

OIP Service	Description
System User Directory Service	System User Directory Service (internal OIP service) is responsible for managing all the registered users on the OIP server.
Test Manager	The Test Manager (internal OIP service) is responsible for the execution of OIP/communication server test orders.
Test Service	The Test Service is responsible for managing the OIP/ communication server test orders.
Time Service	Ticket Service is responsible for managing the call tickets.
Ticket Service	Time Service (internal OIP service) is responsible for managing time synchronization.
TwixTel Directory Service	The TwixTel Directory Service (internal OIP service) is responsible for managing the external phone-book directories TwixTel.
User Preferences Service	User Preferences Service is responsible for managing the user customized settings.
User Profile Manager	User Profile Manager (internal OIP service) is responsible for global OIP user management.
User Profile Service	User Profile Service is responsible for the access to OIP users.
User Service	User Service is responsible for controlling and monitoring applications.
Voice Mail Manager	Voice Mail Manager (internal OIP service) is responsible for managing the voice mails.
Voice Mail Service	Voice Mail Service is responsible for managing the mailboxes.
WEB Server Service	WEB Server Service (internal OIP service) is responsible for managing the Tomcat Web Server.

Account Service

The Account Service is responsible for booking call charges to specific cost centres.

ACD Log Manager

ACD Log Manager (internal OIP service) is responsible for managing and generating ACD statistics.

Table 3.24:ACD Log Manager Specific Properties (Sheet 1 of 2)

Specific properties	Description	Default setting /Settings
Call centre ID	Call centre ID	*OIP Call centre*
File format	Output format for the ACD statistic data.	*standard*
ACD statistic data file directory	Directory in which the ACD statistics are stored. The basic directory is the OIP installation directory.	*acdlog*
File name for the Call Centre calls data	File name for the Call Centre call statistics.	*acdcall-@DATE-@TIME.txt*
File name for the Call Centre status data	File name for the Call Centre status statistics.	*callcenter-@DATE-@TIME.txt*
Agent states data file name	File name for the agent status statistic file.	*agentstatus-@DATE-@TIME.txt*
Agent calls data file name	File name for the agent call statistic file.	*agentcall-@DATE-@TIME.txt*
Creation interval ACD statistic data files	Interval at which new ACD statistic data files are created.	1d 1m - each minute 1h - each hour 1d - each day
File name for the Call Centre calls data	File name for the Call Centre call statistics.	*acdcall-@DATE-@TIME.txt*
File name for the Call Centre status data	File name for the Call Centre status statistics.	*callcenter-@DATE-@TIME.txt*
Agent states data file name	File name for the agent status statistic file.	*agentstatus-@DATE-@TIME.txt*
Creation time ACD statistic data files	Time at which the ACD statistics files are created if the creation interval is configured to daily.	23:30
Call centre status data interval	Interval (in seconds) in which the Call Centre status data (snapshot) are created.	60

Table 3.24:ACD Log Manager Specific Properties (Continued) (Sheet 2 of 2)

Specific properties	Description	Default setting /Settings
Save ACD statistics in database	Number of days during which the ACD statistics entries are stored in the database.	30 0 – Database entries are not deleted
Save ACD statistic data file	Number of days during which the ACD statistic files are stored	30 0 – Files are not deleted

The ACD statistics are erased from the OIP database at the time listed in *"OIP database reorganization times"* see also *"Reorganize OIP database"*.

The OIP service ACD Log Manager is started only if the option ACD statistics logging was selected when the OIP server was installed.

ACD Log Service

ACD Log Service is responsible for the access to ACD statistics.

Table 3.25:ACD Log Service Access right

Access right	admin	group admin	superuser	user	guest	none
Retrieve statistics		A[1]			O[2]	
Delete statistics		A				
Highlight the statistics record as Retrieved.		A				

1. A – Statistics of all Skills
2. O – Statistics of Skills assigned to the agent

ACD Manager

ACD Manager (internal OIP service) is responsible for managing and configuring the ACD queue.

Table 3.26:ACD Manager Specific Properties (Sheet 1 of 2)

Specific properties	Description	Defaultsetting /Settings
Call deletion delay	Time interval (in seconds) in which the answered ACD calls are displayed in the Call Center Manager/Call monitoring.	15 0 - deactivated

Table 3.26:ACD Manager Specific Properties (Continued) (Sheet 2 of 2)

Specific properties	Description	Defaultsetting /Settings
CDE/DDIsynchronization interval	Time interval (in minutes) in which the CDE/DDI are synchronized with the communication server.	5 0 - deactivated

ACD Service

ACD Service is responsible for the access to ACD queue.

Table 3.27:ACD Service Access rights

Access right	admin	group admin	superuser	user	guest	none
Open ACD queue	X					
Create Skills	X					
Delete Skills	X					
Change Skills	X					
Create pause codes	X					
Delete pause codes	X					
Change pause codes	X					
Create Wrap-up codes	X					
Delete Wrap-up codes	X					
Modify Wrap-up codes	X					
Administer business hours	X					

Active Directory Service

The Active Directory Service (internal OIP service) is responsible for managing the Active directories.

Table 3.28:Active Directory Service Specific Properties (Sheet 1 of 3)

Specific properties	Description	Default setting /Settings
Active Directory server address	DNS name or IP address of the Active Directory server.	

Table 3.28:Active Directory Service Specific Properties (Continued) (Sheet 2 of 3)

Specific properties	Description	Default setting /Settings
Active Directory Port	Port of the Active Directory server	*LDAP*
User name	User authentication on the Active Directory server Sample inputs: CN=OIP AD Administrator, CN=Users, DC=mitel, DC=com or oip_ad_ad-**min@mitel.com**	LDAP, Global catalogue
Password	Password for the user authentication on the Active Directory server.	
Active Directory Base-DN	Active Directory root directory Sample inputs: CN=OIP AD Administrator, CN=Users, DC=mitel, DC=com	
Active Directory Search filter	Search filters enable you to define search crite- ria to confine the search request. Entered search filters overwrite the configuration of the LDAP object class. Sampleinputs:(&(objectCategory=person)(telephonenumber=*))	<Definition of LDAP filter according to RFC 2254>
Follow LDAP referrals	The search of objects in a distributed domain structure will be extended to the reference domaincontrollers.	*Disabled*
Number of call number digits	Number of phone number digits from back which are used to compare with the entries in the directory.	7

Table 3.28:Active Directory Service Specific Properties (Continued) (Sheet 3 of 3)

Specific properties	Description	Default setting /Settings
First data merging delay	The user data from the Active Directory can be merged in the OIP user directory if the Windows username is configured in the OIP user profile. • The first directory data merge will be delayed about the configured start time (in minutes) after a restart of the OIP server. The setting '0' disables the data merge.	0
Data merging interval	• The setting '0' disables the data merge.	0
Data merging time	• The user data will be merged at the configured time. The setting '00:00' disables the data merge.	00:00
Manual data merging	• If the manual user data merge is activated, the data merging can be executed manually in the OIP user directory in the Directory Manager.	*Disabled*

Technical information about Active Directory is available on the internet, on the Microsoft development page.

Agent Manager

The Agent Manager (internal OIP service) is responsible for the central management of the ACD agents.

Table 3.29:Agent Manager Specific Properties (Sheet 1 of 2)

Specific properties	Description	Default setting /Settings
Automatic agent login	All agents are logged in automatically when the OIP server starts up.	*Disabled*

Table 3.29:Agent Manager Specific Properties (Continued) (Sheet 2 of 2)

Specific properties	Description	Default setting /Settings
Start wrap-up time	If a call to the Call Centre is processed by several agents as a result of forwarding, you can set whether the wrap-up time should be started with the last agent or with all the agents.	*Last agent*

Agent Service

Agent Service is responsible for the access to ACD agents.

Table 3.30:Agent Service Access rights

Access right	admin	group admin	superuser	user	guest	none
Change Skills settings	A[1]	G[2]				
Create agent	A	G				
Remove agent	A	G				
Activate agent in a Skill	A	G	O[3]			
Deactivate agent in a Skill	A	G	O			
Log agent in	A	G				
Log agent out	A	G		O		
Start agent pause	A	G		O		
End agent pause	A	G		O		
End agent wrap-up time	A	G		O		

1. A – Management of all agents in all Skills
2. G – Management of all agents in assigned Skills
3. O – Management of own agent functionality

Alarm Driver

You can use the *Alarm Driver* service to control communication server event and alarm reports on OIP and to store them in the OIP database. The event and alarm reports can be further processed with the I/O system or they can be used in external applications. A view or protocol file is not available.

Here the settings for the destination of the event and alarm reports on OIP and the synchronization interval for checking this setting can be made with this communication server.

Table 3.31:Alarm Driver Specific Properties

Specific properties	Description	Default setting /Settings
IP port	IP port	1062
Save alarm entries in database	Storage duration (days) for the event and alarm reports in the OIP database	10 0 – Database entries are not deleted
Alarm logging	Store event and alarm reports in OIP.	*Disabled*
Synchronization interval	Synchronization interval (in minutes) in which the settings of the alarm destination are checked on the communication server.	60
Link timeout	Timeout (in seconds) after which the OIP server stops the connection to the communication server, once the last alarms have been sent by the communication server.	60
Maximumlinks	Maximum number of connections in parallel	10

The event and alarm reports are erased from the OIP database at the time listed in *"OIP database reorganization times"*

Alarm Service

You can also use the Alarm Service service to store the communication server's user-specific reports and alarms in the OIP database. Requirement: The alarm log in the Alarm Driver service is enabled.

Table 3.32:Alarm Service Specific Properties

Specific properties	Description	Default setting /Settings
User alarm	Show user alarms in the alarm list.	*Enabled*

Alpha & Quick Dial Service

The Alpha & Quick Dial Service (internal OIP service) is responsible for the name resolution, which is sent to the communication server when dialing with names.

Table 3.33:Alpha & Quick Dial Service Specific Properties (Sheet 1 of 3)

Specific properties	Description	Default setting /Settings
Root directories	Directories where the name resolution is searched.	*Public OIP directory / Private OIP directories/ OIPuser directory / PBX abbreviated dialing directory / Private PBX phonebook / PBX user directory /PISN user directory/ Active Directory / LDAP- directory /External phone book directories*
Extended directories	Expanded directories where the name resolution is searched. For the search in expanded directories the search prefix must be configured and made to precede the dialing by name.	*Public OIP directory / Private OIP directories/ OIPuser directory / PBX abbreviated dialing directory / Private PBX phonebook / PBX user directory /PISN user directory/ Active Directory / LDAP- directory /External phone book directories*
Search prefix	Search prefix which must be made to precede the dialing by name in expanded directories. Multiple entries must be separated by ";".	0;*
Search order	Search order in which the entries are searched in the directories.	First name; Last name; Company
Maximum cache entries	Maximum number of entries stored in cache.	30
Maximum cache time	Maximum amount of time (in minutes) during which the entries are stored in the cache.	5
Maximum search entries	Maximum number of search entries which are displayed in dialing by name.	30

Table 3.33:Alpha & Quick Dial Service Specific Properties (Continued) (Sheet 2 of 3)

Specific properties	Description	Default setting /Settings
Advanced name searching	Activated: Finds the character string at the beginning of each word in the contact entry. Example: The character string 'MAR' finds MARent Peter as well as Kessler MARtin (but not AnneMARie Lustig). Slows down the search. Disabled. Finds character strings only in the first word; in the example it would find only MARent Peter.	*Enabled*
Maximum name length	Maximum name length of the entries.	20
Business number extension	Extension added to the name of the business call number.	*BUS*
Business fax number extension	Extension added to the name of the business fax call number.	*NOTUSED*
Private number extension	Extension added to the name of the private call number.	*PRIV*
Private fax number extension	Extension added to the name of the private fax call number.	*NOTUSED*
Mobile number extension	Extension added to the name of the mobile number.	*GSM*
Pager number extension	Extension added to the name of the pager number.	*NOTUSED*
Main phone extension	Extension added to the name of the main phone number.	*NOTUSED*
List only default phone number	Lists only the default phone number.	*Disabled*
Display extension	The extension, which is added to the name of the number is displayed, if more than one number are assigned to the entry (disabled).	*Disabled*

Table 3.33:Alpha & Quick Dial Service Specific Properties (Continued) (Sheet 3 of 3)

Specific properties	Description	Default setting /Settings
Simultaneous search requests	Maximum number of simultaneous search requests.	100
Alpha Service	Activates or deactivates the Alpha & Quick Dial Service.	*Disabled*

Buddy Manager

Buddy Manager (internal OIP service) is responsible for the central management of the user fields.

Table 3.34:Buddy Manager Specific Properties

Specific properties	Description	Default setting /Settings
Absence timeout	Standard time (in minutes) after which automatic call forwarding should become active.	0
Permanent monitoring	Activates the permanent monitoring of subscribers, even if they are not logged in.	*Enabled*
Show calendar entries	Time (in seconds) in which an existing calendar entry of a called user, who did not answer the call, is displayed on the system phone.	0
Display existing calendar entry at status	Status of the calling subscriber, when an existing calendar entry of a called subscriber should be displayed.	*Free*

Buddy Service

The Buddy Service is responsible for accessing the presence indicator and for displaying the status information.

Table 3.35:Buddy Service Access rights (Sheet 1 of 2)

Access right	admin	group admin	superuser	user	guest	none
Administer absence messages	A[1]			O[2]		

Table 3.35:Buddy Service Access rights (Continued) (Sheet 2 of 2)

Access right	admin	group admin	superuser	user	guest	none
Monitor line	A		A	O		
Control line	A	G[3]				

1. A – All users
2. O – Own user
3. G – Agents in the same Skill

CLIP Service

The CLIP Service (internal OIP service) is responsible for the number resolution of incoming calls in the configured directories.

Table 3.36:CLIP Service Specific Properties

Specific properties	Description	Default setting Settings
Root directory	Directories where the number resolution is searched.	*Public OIP directory / Private OIP directories/ OIPuser directory / PBX abbreviated dialing directory / Private PBX phonebook / PBX user directory /PISN user directory/ Active Directory / LDAP- directory /External phone book directories*
Maximum cache entries	Maximum number of entries stored in cache.	30
Maximum cache time	Maximum amount of time (in minutes) during which the entries are stored in the cache.	2
Search results in directory order	Search results are displayed in directory order.	*Enabled*
Simultaneous search requests	Maximum number of simultaneous search requests.	100
CLIP Service	Activates or deactivates the CLIP Service.	*Enabled*

Calendar Manager

Calendar Manager is responsible for the central management of calendar entries.

Table 3.37:Calendar Manager Specific Properties

Specific properties	Description	Default setting /Settings
Save calendar entries in database	Number of days during which the calendar entries are stored in the database	10 0 – Database entries are not deleted
OIP Exchange driver address	DNS name or IP address of the OIP Exchange driver.	
Heartbeat OIP Exchange driver	Heart beat interval (in minutes) between the OIP server and the OIP Exchange driver.	1

The calendar entries are erased from the OIP database at the time listed in *"OIP database reorganization times"* see also *"Reorganize OIP database"*

Calendar Service

Calendar Service is responsible for accessing and controlling the calendar functionality.

Table 3.38:Calendar Service Access rights

Access right	admin	group admin	superuser	user	guest	none
Create calendar entry	A[1]		A	O[2]		
Delete calendar entry	A		A	O		
Change calendar entry	A		A	O		
View calendar entry	A		A	O		

1. A – Calendar entries of all users
2. O – Own calendar entries

Access rights concern the use of the calendar function via an OIP application or the connected application from a certified third-party manufacturer.

Calendar Synchronization Service

The Calendar Synchronization Service (internal OIP service) is responsible for synchronizing the local Microsoft Outlook contacts with the Mitel OfficeSuite.

Call Logging Driver

You can use the Call Logging Driver service to control communication server call data on OIP and to store it in the OIP database.

The call data are stored as text file for further use. They can also be processed with the I/O system. A view with the connection data is not available.

Here the settings for the destination of the call data on OIP and the synchronization interval for checking this setting can be made with this communication server.

Table 3.39:Call Logging Driver Specific Properties

Specific properties	Description	Default setting /Settings
Call logging	Store the communication server connection data in OIP.	*Disabled*
Synchronization interval	Synchronization interval (in minutes) in which the settings of the call data destination are checked on the communication server.	60
IP port	IP port	1080
Link timeout	Timeout (in seconds) after which the OIPserver stops the connection to the communication server, once the last call charge data have been sent by the communication server.	60
Maximum links	Maximum number of connections in parallel	10

Call Logging Manager

Call Logging Manager (internal OIP service) is responsible for managing the call data.

Table 3.40:Call Logging Manager Specific Properties (Sheet 1 of 2)

Specific properties	Description	Default setting /Settings
Save call data in database	Storage duration (days) for the call data in the OIP database	10 0 – Database entries are not deleted
Save call data files in file system	Storage duration (days) of the call datafile in the file system.	0 0 – Files are not deleted
Call data file extension	Text file extension with the call data	*tax*
Call data file directory	Directory in which the text files are stored with the call data.	*tax*
Create call data files	Number of days after which the call data is written from the database to the text file.	1 0 – No file written. 1 to 5, depending on the data volume
Data protection business calls	Number of phone number digits stored at the end of the call number for business calls.	0 0 to 7
Data protection private calls	Number of phone number digits stored at the end of the call number for private calls.	0 0 to 7
Merge call data tickets	Interconnected entries in the network are merged and stored as an entry in the database.	*Enabled*
Logging external calls	Store external outgoing call entries in the database.	*Enabled*
Logging internal calls	Store entries for internal calls and calls inside the network in the database.	*Disabled*
Logging incoming calls	Incoming CL tickets are logged.	*Enabled*
Logging outgoing calls	Outgoing CL tickets are logged.	*Enabled*
Show display text	Display duration (in seconds) of charge information on the system phone.	0

Table 3.40:Call Logging Manager Specific Properties (Continued) (Sheet 2 of 2)

Specific properties	Description	Default setting /Settings
Display text format	Format of the display text. The text can be adapted using variables, according to the following table.	
Gateway PBX call charges	Call charge information is shown on the system phone if the outgoing call is made via a gateway communication server. The ATASlicense is required to display call charges from the gateway communication server. see *"The OIP licenses"*	*Enabled*
Update journal entry	The corresponding journal entry will be updated Enabled with the call charge data.	Enabled
CLIP prefix	If the DDI does not correspond to the internal call number (e.g. DDI 32655xxxx, internal call number xxxx), "32655" has to be entered as the CLIP prefix so that the call data in the QSIG net- work can be assigned to the extension. Multiple entries must be separated by ";".	

Table 3.41:Display text variables (Sheet 1 of 2)

@SUBSCRIBERNAME	User name
@SUBSCRIBERNUMBER	Call number
@COSTCENTRE	Cost centre number
@STARTDATE	Date of start of connection
@STARTTIME	Time of start of connection
@TIMETOANSWER	Response time
@DURATION	Duration of connection
@TAXCHARGES	Call charges

Table 3.41:Display text variables (Continued) (Sheet 2 of 2)

@TAXPULSES	Metering pulses
@CALLERID1	Caller identification 1
@CALLERID2	Caller identification 2
@DESTINATIONNUMBER1	Destination number 1
@DESTINATIONNUMBER2	Destination number 2
@ORIGINSUBSCRIBER	call number from which the call is set up
@CURRENCY	Currency value

In the standard settings the following character sequence is displayed on the system phone as the display text:

Currency unit call charges/call duration sec.

The export file of call data is created at the configured interval at the time listed in *"Export data create times"* see also *"OIP Export data"*

The call data is erased from the OIP database at the time listed in *"OIP database reorganization times"* see also *"Reorganize OIP database"*

Call Logging Service

Call Logging Service is responsible for accessing and distributing charge data.

Table 3.42:Call Logging Service Access rights

Access right	admin	group admin	superuser	user	guest	none
Administer call data settings	X					
Retrieve call data			A[1]	O[2]		
Delete call data			A			
Highlight call data record as Retrieved.			A			
Resetting the charge counter			A			

1. A – Call data of all users
2. O – Own call data

Call Service

Call Service is responsible for managing the telephony features.

Table 3.43:Call Logging Manager Specific Properties

Specific properties	Description	Default setting Settings
Direct blind transfer	Calls can be transferred during call proceeding.	*Disabled*

Client Utility Service

Client Utility Service provides OIP-specific functions to applications.

Table 3.44:Client Utility Service Access rights

Access right	admin	group admin	superuser	user	guest	none
Start the OIP services		G[1]	A[2]	O[3]		
Start OIP services for users with monitoring rights on their line		X				
Start OIP services for users with control rights on their line	X					

1. G – User in the same user group
2. A – All users
3. O – OIP services assigned to the user

Configuration Profile Manager

Configuration Profile Manager (internal OIP service) is responsible for managing the presence profiles.

Configuration Profile Service

Configuration Profile Service is responsible for accessing the presence profiles of the OIP users.

Table 3.45:Configuration Profile Service Access rights (Sheet 1 of 2)

Access right	admin	group admin	superuser	user	guest	none
Read presence profile	A[1]	P[2]/O[3]	P/O	P/O	P/O	

Table 3.45:Configuration Profile Service Access rights (Continued) (Sheet 2 of 2)

Access right	admin	group admin	superuser	user	guest	none
Activate/deactivate presence profile	A	P/O	P/O	P/O		
Create presence profile	A		O			
Delete presence profile	A		O			
Modify presence profile	A		O			

1. A - All: Access right applies to the presence profiles of all users
2. P - Public: Access right applies to the public presence profiles
3. O - Own: Access right applies to the personal, private presence profiles

Configuration Service

Configuration Service is responsible for managing the OIP services.

DasTelefonbuch Directory Service

The DasTelefonbuch Directory Service (internal OIP service) is responsible for managing the external phone-book directories of “DasTelefonbuch Deutschland”.

Table 3.46:DasTelefonbuch Directory Service Specific Properties (Sheet 1 of 2)

Specific properties	Description	Default setting /Settings
Phone book server address	DNS name or IP address of the server on which the external phone-book directories are installed.	
Number of call number digits	Number of phone number digits from back which are used to compare with the entries in the directory.	0
Alias name order	Format of the alias name.	Last name - first name

Table 3.46:DasTelefonbuch Directory Service Specific Properties (Continued) (Sheet 2 of 2)

Specific properties	Description	Default setting /Settings
Use generated default alias	Generates a default alias (display name) for each contact defined in the ContactNameOrder setting.	*Enabled*
Data source	Display the used version of DasTelefonbuch Germany.	

Database Driver

The Database Driver (internal OIP service) is the interface adapter used for accessing the OIP database. This is where the settings for backing up the OIP database and the OIP configuration file are made.

Table 3.47:Database Driver Specific Properties (Sheet 1 of 2)

Specific properties	Description	Default setting /Settings
Database type	Database type	*rdbms*
Database path	Path to the database.	*jdbc:mysql://localhost/AXPDB*
Password	Password for database access.	
User	User for database access.	
Database driver	Database driver	*org.gjt.mm.mysql.Driver*
Communication channels	Number of communication channels possible in parallel	10
Maximum rows in database table	Maximum number of entries, which are returned with data base queries.	10000
Backup directory	Directory for the OIP data backup.	*backup*
Backup time	Directory for the OIP data backup.	*backup*
SaveOIPbackup files	Number of days the OIP backup files are stored in the file system.	5 0 – OIP backup files are not deleted
Database heartbeat	Heartbeat interval (in minutes) between the OIP server and the OIP database.	1

Table 3.47:Database Driver Specific Properties (Continued) (Sheet 2 of 2)

Specific properties	Description	Default setting /Settings
Deletion interval database table entries	Interval in which the database table entries will be deleted, if the configured maximum number of entries is exceeded.	1d 1m - each minute 1h - each hour 1d - each day
Deletion time database table entries	Time at which the database table entries will be deleted, if the deletion interval is set to daily.	03:45
Maximum number entries in database table (global)	Global setting for the maximum number of entries in each database table.	50000
Maximum number of entries in log database table	Setting for the maximum number of entries in the log database table.	50000
Database version	Database version	1

Backing up the OIP configuration is done once after starting the OIP Windows services after one hour. Thereafter the backup is carried out daily at the listed time, see also *"Backing up the OIP configuration"*

Directory Manager

Directory Manager is responsible for managing the directories.

Table 3.48:Directory Manager Specific Properties (Sheet 1 of 2)

Specific properties	Description	Default setting /Settings
Root directory	Directories where entries are searched.	*Public OIP* directory / *Private OIP directories* / *OIPuser directory* / *PBX abbreviated dialing directory* / *Private PBX phone book*/ *PBX user directory* / *PISN user directory* / *Active Directory* / *LDAP directory* / *External phone book directories*

Table 3.48:Directory Manager Specific Properties (Continued) (Sheet 2 of 2)

Specific properties	Description	Default setting /Settings
Refresh directory list	Time interval (in minutes) in which the availability of the configured directories are checked. The connection to directories which cannot be reached is then automatically restored as soon as these directories can be reached again.	

Directory Service

Directory Service is responsible for the access to directories.

Table 3.49:Directory Service Specific Properties

Specific properties	Description	Default setting /Settings
Root directory	Directories where entries are searched.	*Public OIP* directory / *Private OIP directories* / *OIPuser directory* / *PBX abbreviated dialing directory* / *Private PBX phone book*/ *PBX user directory* / *PISN user directory* / *Active Directory* / *LDAP directory* / *External phone book directories*

Table 3.50:Directory Service Access rights (Sheet 1 of 2)

Access right	admin	group admin	superuser	user	guest	none
PISNusers	R[1]	R	R	R	R	
Private PBX phone book directories	R/W[2]	R/W[3]	R/W[c]	R/W[c]		
Private OIP directories	R/W	R/W[c]	R/W[c]	R/W[c]		
Public OIP directories	R/W	R/W	R/W	R	R	
PBX abbreviated dialing directory	R/W	R/W	R/W	R	R	
PBX subscriber directory	R	R	R	R	R	

Table 3.50:Directory Service Access rights (Continued) (Sheet 2 of 2)

Access right	admin	group admin	superuser	user	guest	none
OIP subscriber directory	R/W	R/W	R/W	R/W[4]	R	
Active Directory	R	R	R	R	R	
LDAP directories	R	R	R	R	R	
External phone book directories	R	R	R	R	R	

1. Read rights to the directory
2. Read and write rights to all private directories
3. Read and write rights to one's own directory only
4. Write rights for own contact only

Display Manager

Display Manager (internal OIP service) is responsible for the management of the access to the system phones' displays.

Display Service

Display Service is responsible for display control of the system phones.

Event Service

Event Service (internal OIP service) is responsible for distributing the events in the system.

Table 3.51:Event Service Specific Properties

Specific properties	Description	Default setting /Settings
Server address	DNS name or IP address of the server on which the Event Service is installed.	*localhost*
IP port	IP port of the Event Service.	2500

Fax Manager

Fax Manager (internal OIP service) is responsible for managing the fax functionality.

Table 3.52:Fax Manager Specific Properties

Specific properties	Description	Default setting /Settings
Maximum number of redials	Maximum number of last-number redials if the number is unobtainable.	3
Redial interval	Interval (in minutes) in which the fax is resend.	1

Fax Service

Fax Service is responsible for the access to the fax functionality.

Table 3.53:Fax Service Access rights

Access right	admin	group admin	superuser	user	guest	none
Create fax box	A[1]					
Delete fax box	A					
Modify fax-box settings	A					
Send/receiv efaxes	A			O[2]		

1. A – All users
2. O – Own fax box

Feature Service

The Feature Service provides functions depending on the phone, the CTI license and the communication server type applications.

Flow Manager

Flow Manager (internal OIP service) is responsible for managing the call sequences.

Flow Service

Flow Service is responsible for the access to licenses.

Table 3.54:Flow Service Access rights

Access right	admin	group admin	superuser	user	guest	none
Create call sequences	X					
Delete call sequences	X					
Modify call sequences	X					

Function Key Manager

Function Key Manager (internal OIP service) is responsible for managing the function keys.

Function Key Service

Function Key Service is responsible for the access to the function keys.

I/O Manager

I/O Manager is responsible for the central management of the I/O groups.

Table 3.55:I/O Manager Specific Properties

Specific properties	Description	Default setting /Settings
Serveraddress	DNS name or IP address of the server on which the driver for the OIP KNX Service is installed.	
Double-clickinterval	Time interval for double-click evaluation.	300
Long-clickinterval	Time interval for long-click evaluation.	500
Save action entries in database	Number of days during which the protocol entries are stored in the database.	10
Creating protocol log files	Number of days after which the logged actions are written from the database in the file.	

The export file of logged actions is created at the configured interval at the time listed in *"Export data create times"* see also *"OIP Export data"*.

The action entries are erased from the OIP database at the time listed in *"OIP database reorganization times"* see also *"Reorganize OIP database"*.

I/O Service

I/O Service is responsible for managing actors.

Jabber Driver

The Jabber Driver (internal OIP service) is the interface adapter used for accessing the external Jabber/XMPP Instant Messaging systems.

Journal Manager

Journal Manager (internal OIP service) is responsible for managing the journal entries.

Table 3.56:Journal Manager Specific Properties

Specific properties	Description	Default setting /Settings
Save journal entries in database	Number of days during whichthejournal entries are stored in the database	10 0 – Database entries are not deleted
Logging operator calls	Create journal entries for operator calls.	*Enabled*

The journal entries are erased from the OIP database at the time listed in *"OIP database reorganization times"* see also *"Reorganize OIP database"*.

Journal Service

Journal Service is responsible for managing and deflecting the call lists to the applications.

Key Configuration Service

Key Configuration Service is responsible for key configuration of the system phones.

Table 3.57:Key Configuration Service Access rights

Access right	admin	group admin	super user	user	guest	none
Manage system phone settings	A[1]		O[2]			
Manage keys on the system phone	A		O			
Manage locked keys on the system phone	A					

1. A – All system phones

2. O – Own system phone

LDAP Directory Service

LDAP Directory Service (internal OIP service) is responsible for managing the LDAP directories.

Table 3.58:LDAP Directory Service Specific Properties (Sheet 1 of 3)

Specific properties	Description	Default setting /Settings
LDAP server address	DNS name or IP address of the LDAP server.	
LDAP port	IP port of the LDAP server.	
Username	User authentication on the LDAP server.	Example: *CN=DirectoryManager*
Password	Password for user authentication on the LDAP server.	
LDAP base DN	LDAP base directory	
LDAP object class	LDAP object class	user / user / inetOrgPerson /organizationalPerson / person /contact
LDAP search filters	Search filters enable you to define search criteria to confine the search request. Entered search filters overwrite the configuration of the LDAP object class.	
Follow LDAP referrals	The search for objects in a distributed directory structure will be extended to the reference LDAP servers.	*Disabled*
First name		*DEFAULT-MAPPING*
Middle Names		*DEFAULT-MAPPING*
Last name		*DEFAULT-MAPPING*
Home address - Street		*DEFAULT-MAPPING*
Home address - Postal code		*DEFAULT-MAPPING*
Home address - City		*DEFAULT-MAPPING*
Home address - State		*DEFAULT-MAPPING*

Table 3.58:LDAP Directory Service Specific Properties (Continued) (Sheet 2 of 3)

Specific properties	Description	Default setting /Settings
Home address - Country		*DEFAULT-MAPPING*
Business address - Street		*DEFAULT-MAPPING*
Business address - Postal code		*DEFAULT-MAPPING*
Business address - City		*DEFAULT-MAPPING*
Business address - State		*DEFAULT-MAPPING*
Business address - Country		*DEFAULT-MAPPING*
Business call number		*DEFAULT-MAPPING*
Business fax number		*DEFAULT-MAPPING*
Private call number		*DEFAULT-MAPPING*
Private fax number		*DEFAULT-MAPPING*
Mobile phone		*DEFAULT-MAPPING*
Pager number		*DEFAULT-MAPPING*
Company number		*DEFAULT-MAPPING*
Alias		*DEFAULT-MAPPING*
Company		*DEFAULT-MAPPING*
Position		*DEFAULT-MAPPING*
E-mail		*DEFAULT-MAPPING*
Private e-mail		*DEFAULT-MAPPING*
E-mail mobile		*DEFAULT-MAPPING*
Webpage		*DEFAULT-MAPPING*
Manager's name		*DEFAULT-MAPPING*
Assistant's name		*DEFAULT-MAPPING*
Department		*DEFAULT-MAPPING*
User-defined 1		*DEFAULT-MAPPING*
User-defined 2		*DEFAULT-MAPPING*
User-defined 3		*DEFAULT-MAPPING*
User-defined 4		*DEFAULT-MAPPING*

Table 3.58:LDAP Directory Service Specific Properties (Continued) (Sheet 3 of 3)

Specific properties	Description	Default setting /Settings
User-defined 5		*DEFAULT-MAPPING*
Notes		*DEFAULT-MAPPING*
Number of call number digits	Number of phone number digits from back which are used to compare with the entries in the directory.	7

In the default setting, the attributes listed in *"Default allocation of LDAP attributes"* are used for DEFAULT MAPPING. Depending on the object class selected, the attributes of the subordinate object class are used.

Table 3.59:Default allocation of LDAP attributes (Sheet 1 of 3)

Specific properties	Attribute	Object class
First name	givenName	organizationalPerson/ contact/ user / inetOrgPerson
Middle Names	middleName	user / inetOrgPerson
Last name	sn	person / organizationalPerson / contact / user / inetOrgPerson
Home address - Street		
Home address - Postal code		
Home address - City		
Home address - State		
Home address - Country		
Business address - Street	streetAddress	organizationalPerson/ contact/ user / inetOrgPerson
Business address - Postal code	postalCode	organizationalPerson/ contact/ user / inetOrgPerson
Business address - City	l	organizationalPerson/ contact/ user / inetOrgPerson
Business address - State	st	organizationalPerson/ contact/ user / inetOrgPerson
Business address - Country	c	organizationalPerson/ contact/ user / inetOrgPerson

Table 3.59:Default allocation of LDAP attributes (Continued) (Sheet 2 of 3)

Specific properties	Attribute	Object class
Business call number	telephoneNumber	person / organizationalPerson / contact / user / inetOrgPerson
Business fax number	facsimileTelephoneNumber	organizationalPerson/ contact/ user / inetOrgPerson
Private call number	home Phone	user / inetOrgPerson
Private fax number		
Mobile phone	mobile	organizationalPerson/ contact/ user / inetOrgPerson
Pager number	pager	user / inetOrgPerson
Company number		
Alias	display Name	person / organizationalPerson / contact / user / inetOrgPerson
Company	company	organizationalPerson/ contact/ user / inetOrgPerson
Position	title	organizationalPerson/ contact/ user / inetOrgPerson
E-mail	mail	organizationalPerson/ contact/ user / inetOrgPerson
Private e-mail	mail	organizationalPerson/ contact/ user / inetOrgPerson
E-mail mobile	mail	organizationalPerson/ contact/ user / inetOrgPerson
Webpage	WWWHomePage manager	organizationalPerson/ contact/ user / inetOrgPerson
Manager's name		
Assistant's name		
Department	department	organizationalPerson
User-defined 1		contact
User-defined 2		user
User-defined 3		inetOrgPerson
User-defined 4		

Table 3.59:Default allocation of LDAP attributes (Continued) (Sheet 3 of 3)

Specific properties	Attribute	Object class
User-defined 5		user inetOrgPerson
Notes	notes	contact

License Manager

License Manager (internal OIP service) is responsible for managing the licenses.

Table 3.60:License Manager Specific Properties

Specific properties	Description	Defaultsetting /Settings
Licenses log file	Directory in which the log file for the licenses registered in the system are stored. The basic directory is the OIP installation directory.	.logs/license.txt

License Service

License Service is responsible for the access to licenses.

Line Service

Line Service is responsible for managing key telephone features.

Table 3.61:Line Service Specific Properties

Specific properties	Description	Default setting /Settings
Automatic parking of private calls	If during the call on the private line a call is answered on the line key, the private call is parked.	*Enabled*
Synchronization interval	Interval (in minutes) in which the line key configuration is synchronized with the communication server.	10

Table 3.62:Line Service Access rights

Access right	admin	group admin	superuser	user	guest	none
Create line key	X					
Clear line key	X					
Configure CDE	X					
Bar phone configuration	X					
Configure outgoing barring	X					
Configure terminating line	X					
Configure ring settings for line key	X			X		
Configure incoming / outgoing seizure	X			X		
Configure priority	X			X		
Configure call list	X			X		

Load Balancing Service

Load Balancing Service (internal OIP service) is responsible for the load distribution within the OIP Server Networks.

Location Manager

Location Manager (internal OIP service) is responsible for managing the cordless phone localisation.

Table 3.63:Location Manager Specific Properties

Specific properties	Description	Default setting/ Settings
Number of parallel search requests	Number of parallel requests for locating DECT handsets	10
Storage time	Time during which the requests for locating cordless phones are buffered	10s 1s – every second 1m - each minute

Location Service

The Location Service is used to locate cordless phones on the covered premises.

Log Service

Log Service is responsible for the central management and recording of the log files.

Table 3.64:Log Service Specific Properties

Specific properties	Description	Defaultsetting/ Settings
Days, log entries	Number of days during which the log entries are stored in the database	10 0 – Database entries are not deleted
Exception output destination	Output destination for the exception log entries.	Database / Screen / File / System
Output destination, error	Output destination for the error log entries.	Database / File
Output destination, warning	Output destination for the warning log entries.	Database / File
Output destination, security	Output destination for the security log entries.	Database / File
Output destination, information	Output destination for the information log entries.	*File*
Output destination, debug	Output destination for the debug log entries.	*File*
Log details	Level of detail for the log entries	*All*
Log file size	Maximum size of the log files (in bytes).	10000000 min. 1025
Log file days	Number of days during which the log files are stored in the file system	5
Log Memory	Interval (in seconds) in which the status of the used and allocated memory is written in the log file.	0 0 - deactivated >1 - activated

The log entries are erased from the OIP database at the time listed in *"OIP database reorganization times"* see also *"Reorganize OIP database"*.

Login Service

Login Service is responsible for managing the login to the OIP server.

Table 3.65:Login Service Specific Properties

Specific properties	Description	Default setting/ Settings
Automatic login	Enables or disables automatic login to the OIP server.	*Enabled*

Media Manager

Media Manager (internal OIP service) is responsible for managing the OIP Media Driver.

Table 3.66:Media Manager Specific Properties

Specific properties	Description	Default setting/ Settings
Server address	DNS name or IP address of the server on which the Media Service driver is installed.	
<Address>:60901@CAPI#<n>	<Address>: DNS name or IP address <n>=ISDN interface No.) The installed ISDN interfaces are displayed. Depending on which communication server the ISDN interfaces are connected, the communication server ID has to be specified. In the OIP Configuration Manage reach communication server ID can be determined via the menu item communication server network.	<Communicationserver ID>

Message Manager

Message Manager (internal OIP service) is responsible for managing messages.

Table 3.67:Message Manager Specific Properties (Sheet 1 of 2)

Specific properties	Description	Default settings /Settings
Save messages in database	Number of days during which the messages are stored in the database	10

Table 3.67:Message Manager Specific Properties (Continued) (Sheet 2 of 2)

Specific properties	Description	Default settings /Settings
Create journal entry	Creates for each incoming and outgoing mes- sage a journal entry.	0 – Database entries are not deleted
OIP Exchange driver address	DNS name or IP address of the OIP Exchange driver.	*Enabled*
Heartbeat OIP Exchange driver	Heartbeat interval (in minutes) between the OIP server and the driver for the Microsoft Exchange server.	1
E-mail sender address	Standard e-mail sender address used when sending e-mails. If you do not specify the domain (<sender> instead of <**sender@domain.xxx**>), the domain from the settings in the SMTP Driver or the e-mail domain of the Microsoft Exchange Server is used.	*OIP no reply*
Send messages to all	Messages which are sent to all the users of the communication server are sent to all users in the network which are connected to the OIP server.	*Enabled*

The message entries are erased from the OIP database at the time listed in *"OIP database reorganization times"* see also *"Reorganize OIP database"*.

Message Service

Message Service is responsible for sending and receiving messages.

Microsoft Exchange Driver Java WebServices

The OIP service Microsoft Exchange Driver Java WebServices is an integrated driver used to connect the Microsoft Exchange Server to OIP. It gives access to the domain users' public contact folders and mail-boxes (personal Outlook address book, calendar and e-mail folder). Alternatively, the external OIP Exchange driver can also be used. For new installations we recommend the use of the integrated driver.

Thanks to the access to the domain user's mailboxes, the contact entries of the personal Outlook address book can be synchronized with the private OIP directory. Moreover, existing calendar entries can be displayed in the presence display.

The presence status of Microsoft Outlook calendar entries is displayed in the OIP calendar by the OIP presence status.

Access to the e-mail folder is required to store voice mails as e-mail in the Inbox.

Table 3.68:Microsoft Exchange Driver Java WebServices

Parameter	Description
Microsoft Exchange Server version	• Microsoft Exchange Server 2013 for Microsoft Exchange Server 2013 and Office 365 • Microsoft Exchange Server 2013 SP1 for Microsoft Exchange Server 2013 SP1 and Office 365
Microsoft Exchange server address	DNS name or IP address of the Microsoft Exchange Server. If there are several Microsoft Exchange Servers on the network, the address of the server defined in the Client Access Server (CAS) role must be indicated. **NOTE:** Please leave this field empty in Office 365.
Domain	Domains assigned to the Microsoft Exchange Server, e.g. company.com. **NOTE:** Please leave this field empty in Office 365.
User name	User name of the OIP Exchange administrator. In Office 365 the OIP Exchange administrator's e-mail address is entered as user name.
Password	Password of the OIP Exchange administrator.
Notification interval	Interval within which the OIP Exchange driver checks the modifications on the Microsoft Exchange Server.

Naming Service

The Naming Service (internal OIP service) is responsible for the global management of services in OIP server network systems.

Table 3.69:Naming Service Specific Properties

Specific properties	Description	Default Settings
Time to live	Time to live, number of hops.	128
Multicast host IP address	Multicast host IP address	234.5.6.7
Multicast IP port	Multicast IP port.	9001
Heartbeat interval	Heartbeat interval (in milliseconds) with the clients.	300000
Garbage Collection	Clears the main memory.	*Enabled*

Notepad Service

Notepad Service is responsible for managing the note entries and redial lists.

Table 3.70:Notepad Service Specific Properties

Specific properties	Description	Default Settings
Number of note entries	Number of note entries.	20
Delete duplicated note entries	Deletes duplicated note entries.	*Enabled*
Number of redial list entries	Number of redial list entries.	20
Delete duplicated redial list entries	Deletes duplicated redial list entries.	*Enabled*

Notification Manager

Notification Manager (internal OIP service) is responsible for managing the notifications.

Notification Service

Notification Service is responsible for accessing and distributing the notifications.

ODBC/JDBC Directory Service

The ODBC/JDBC Directory Service is responsible for managing connected ODBC or JDBC directories.

Table 3.71:ODBC/JDBC Directory Service Specific Properties

Specific properties	Description	Default Settings
Phone book server address	DNS name or IP address of the server on which the OIP ODBC/JDBC Driver is installed.	
Number of call numbers	Number of phone number digits from back which are used to compare with the entries in the directory.	0
Alias name order	Format of the alias name	*Last name - First name*
Use generated default alias	Generates a default alias (display name) for each contact defined in the ContactNameOrder setting.	*Enabled*
Data source	Displays the source of the data	

Operator Service

Operator Service is responsible for managing the operator queue.

Table 3.72:Operator Service Specific Properties

Specific properties	Description	Default Settings
Automatic parking of private calls	If an operator call is answered during a call on the private line, the private call is parked.	*Enabled*

PBX Driver Ascotel

PBX Driver Ascotel (internal OIP service) is the interface adapter used for accessing the communication server.

Table 3.73:PBX Driver Ascotel Specific Properties (Sheet 1 of 2)

Specific properties	Description	Default Settings
IP port	IP port	1061
PBX authentication level	Authorization level with which the OIP server communicates with the communication server. This setting is no longer significant.	*Attendant*
OIP name server	The OIP Name Server is enabled.	*Enabled*
Display Server	Activates the ATAS messaging/alarming interface on the OIP server.	*Enabled*
Ascotel OIP Information Link	The Ascotel OIPInformation Link is activated on the OIP server.	*Enabled*
Number of parallel search requests	Number of parallel requests for locating cordless phones	10
Storage time	Time during which the requests for locating cordless phones are buffered	10s 1s – every second 1m - each minute
Maximum search entries	Maximum number of search entries which are displayed in dialing by name	30

Table 3.73:PBX Driver Ascotel Specific Properties (Continued) (Sheet 2 of 2)

Specific properties	Description	Default Settings
Maximum name length	Maximum name length of the entries.	20
Business number extension	Extension added to the name of the business call number.	*BUS*
Business fax number extension	Extension added to the name of the business fax call number.	*NOT USED*
Private number extension	Extension added to the name of the private call number.	*PRIV*
Private fax number extension	Extension added to the name of the private fax call number.	*NOTUSED*
Mobile number extension	Extension added to the name of the mobile number.	*GSM*
Pager number extension	Extension added to the name of the pager number.	*NOTUSED*
Main phone extension	Extension added to the name of the mainphone number.	*NOTUSED*
VoIPnumber extension	Extension added to the name of the VoIP number.	*NOTUSED*
Extension PBX internal number	Extension added to the name of the PBX internal number.	*NOTUSED*
List only default phone number	Lists only the default phone number.	*Disabled*
Display extension	The extension, which is added to the name of the number is displayed, if more than one number are assigned to the entry (disabled).	*Disabled*
Ignored journal entries	All journal entries beginning with the configured prefix are deleted from the journal. Example: If '*06' is configured, the following journal entries are deleted: '*061234*216789#'. Multiple entries must be separated by ";".	**33;#33;*47;#36;#46;*06*

Only the standard call number is synchronized in the standard setting. If all the call numbers of a contact are to be synchronized, you need to deactivate the Synchronize standard call number setting. A name extension for the various call number types should also be configured so that all the call numbers do not appear under one name in the communication server's private directory. For example, for the business call number under Synchronize business call number, enter the setting _B. Make sure the name extension you choose is not too long as the length of names is limited in the communication server. If a call number type is not to be synchronized, enter the setting NOSYNC.

PBX Information Service

PBX Information Service provides information about the connected communication server, e.g. the communication server name and users.

PBX Manager

PBX Manager (internal OIP service) is responsible for managing of the communication servers connected to the OIP server

Table 3.74:PBX Manager Specific Properties

Specific properties	Description	Default Settings
Synchronization interval	Synchronization interval with the communication server (in minutes).	15
Minimum length external numbers	All phone numbers which are equal to or longer than the configured length will be dialled as external number from the application (for example, Mitel OfficeSuite), i.e. the external access code will be added automatically. The setting '0' deactivates this function.	5

PBX Setup Manager

PBX Setup Manager (internal OIP service) is responsible for the configuration of the communication servers connected to the OIP server.

PBX Setup Service

PBX Setup Service is responsible for managing the communication server configuration.

Table 3.75:PBX Setup Service / PBX Setup Manager Access rights (Sheet 1 of 2)

Access right	admin	group admin	super user	user	guest	none
Manage date and time settings	X		X			

Table 3.75:PBX Setup Service / PBX Setup Manager Access rights (Continued) (Sheet 2 of 2)

Access right	admin	group admin	super user	user	guest	none
Administer time synchronization settings	X					
Execute time synchronization	X					

PISN Directory Service

PISN Directory Service (internal OIP service) is responsible for managing the PISN users.

Table 3.76:PISN Directory Service Specific Properties

Specific properties	Description	Default Settings
Synchronization interval	Synchronization interval with the communication server (in minutes).	30 0 – No synchronization
Name order	Format of the name entries in the communication server's PISN users directory.	*First name - last name*
Number of call number digits	Number of phone number digits from back which are used to compare with the entries in the directory.	7

PUM Manager

PUM Manager (internal OIP service) is responsible for managing the Personal User Mobility function.

PUM Service

PUM Service is responsible for access to the Personal User Mobility data and configuration.

Table 3.77:PUM Service Access rights (Sheet 1 of 2)

Access right	admin	group admin	supe ruser	user	guest	none
Create a PUM workstation	X					
Delete a PUM workstation	X					
Modify PUM workstation settings	X					

Table 3.77:PUM Service Access rights (Continued) (Sheet 2 of 2)

Access right	admin	group admin	supe ruser	user	guest	none
Create PUM users	X					
Delete PUM users	X					
Modify PUM users settings	X					

Private Card Directory Service

The Private Card Directory Service (internal OIP service) is responsible for the central management of the communication server private phone book.

Table 3.78:Private Card Directory Service Specific Properties

Specific properties	Description	Default Settings
Synchronization interval	Synchronization interval (in minutes) in which the private communication server directories are cached in the OIP database.	30 0 – No synchronization
Name order	Format of the name entries in the private communication server directories.	*First name - last name*
Number of call number digits	Number of phone number digits from back which are used to compare with the entries in the directory.	7

Private Directory Service

Private Directory Service (internal OIP service) is responsible for managing the private contacts.

The settings for synchronization with the private directories of the communication server and the private contacts in the OIP database or the private Outlook address books on the Microsoft Exchange Server can be made here.

Table 3.79:Private Directory Service Specific Properties (Sheet 1 of 3)

Specific properties	Description	Default Settings
OIP Exchange driver address	DNS name or IP address of the OIP Exchange driver.	

Table 3.79:Private Directory Service Specific Properties (Continued) (Sheet 2 of 3)

Specific properties	Description	Default Settings
Heartbeat OIP Exchange driver	Heart beat interval (in minutes) between the OIP server and the driver for the Microsoft Exchange server.	1
First synchronization delay	Start time (in minutes) after which the first synchronization begins after a restart of the OIP server.	5
PBX synchronization	Synchronizes private OIP directories with private communication server directories. The OIP directories are the master directories.	*OIP master*
Synchronization interval	Interval in which the private OIP directories are synchronized with the private communication server directories. If a Microsoft Exchange Server is connected the personal Outlook address books are also synchronized with the private OIP directories.	1d 1m - each minute 1h - each hour 1d - each day
Synchronization time	Time at which the private OIP directories are synchronized with the private communication server directories if the synchronization interval is set to daily. If a Microsoft Exchange Server is connected thepersonal Outlook address books are also synchronized with the private OIP directories.	01:30
Delete entries in external directories	Deleting entries in the communication server's private directories also deletes the entries in the OIP database or in the private Outlook address book (depending on the connection).	*Disabled*

Table 3.79:Private Directory Service Specific Properties (Continued) (Sheet 3 of 3)

Specific properties	Description	Default Settings
Name order	Format of the name entries in the private directories.	*Last name - first name*
Number of call number digits	Number of phone number digits from back which are used to compare with the entries in the directory.	7

Public Directory Service

Public Directory Service (internal OIP service) is responsible for managing the public contacts.

The settings for synchronization with the abbreviated dialing list on the one hand and the public contacts in the OIP database or the public contacts folder on the Microsoft Exchange Server on the other can be made here.

Table 3.80:Public Directory Service Specific Properties (Sheet 1 of 3)

Specific properties	Description	Default Settings
OIP Exchange driver address	DNS name or IP address of the OIP Exchange driver.	
Standard public contact folder	Public contact folder on the Microsoft Exchange Server in which new contacts are stored if they are not entered in Microsoft Outlook.	
Heartbeat OIP Exchange driver	Heart beat interval (in minutes) between the OIP server and the driver for the Microsoft Exchange server.	1
Synchronization, business call number	Extension added to the name of the business call number during synchronization with the abbreviated dialing list.	
Synchronization, business fax number	Extension added to the name of the business fax number during synchronization with the abbreviated dialing list.	*NOSYNC*

Table 3.80:Public Directory Service Specific Properties (Continued) (Sheet 2 of 3)

Specific properties	Description	Default Settings
Synchronization, private call number	Extension added to the name of the private call number during synchronization with the abbreviated dialing list.	*NOSYNC*
Synchronization, private fax number	Extension added to the name of the private fax number during synchronization with the abbreviated dialing list.	*NOSYNC*
Synchronization mobile phone	Extension added to the name of the Mobile number during synchronization with the abbreviated dialing list	*NOSYNC*
Synchronization pager	Extension added to the name of the Pager number during synchronization with the abbreviated dialing list.	*NOSYNC*
Synchronization company number	Extension added to the name of the main phone number during synchronization with the private card file.	*NOSYNC*
Default phone number	Call number type set by default during search, for instance, in call management.	*Business*
Synchronize defaultphone number	Synchronize only the default phone number.	*Enabled*
Maximum name length	Maximum name length of the abbreviated dialling entries in the communication server.	17
First synchronization delay	Start time (in minutes) after which the first synchronization begins after a restart of the OIP server.	10
PBX synchronization	Setting for synchronizing the public OIP directory with the abbreviated dialing list.	*Enabled*

Table 3.80:Public Directory Service Specific Properties (Continued) (Sheet 3 of 3)

Specific properties	Description	Default Settings
Synchronization interval	Interval in which the public OIP directory is synchronized with the abbreviated dialing list. If a Microsoft Exchange Server is connected the configured public contact folders are also synchronized with the public OIP directory.	1d 1m - each minute 1h - each hour 1d - each day
Synchronization time	Time at which the public OIP directory is synchronized with the abbreviated dialing list if the synchronization interval is set to daily. If a Microsoft Exchange Server is connected the configured public contact folders are also synchronized with the public OIP directory.	01:30
Delete entries in external directories	Deleting entries in the abbreviated dialing list also deletes the entries in the OIP database or in the public contacts folder on the Microsoft Exchange server (depending on the connection).	*Disabled*
Synchronize public contact folder	List of public contact folders on the Microsoft Exchange Server which are to be synchronized with the public OIP directory.	
Name order	Format of the name entries in the public directory.	*Last name - first name*
Number of call number digits	Number of phone number digits from back which are used to compare with the entries in the directory.	7
Display extension	The extension, which is added to the name of the number is displayed, if more than one number are assigned to the entry (disabled).	*Disabled*

Only the standard call number is synchronized in the standard setting. If all the call numbers of a contact are to be synchronized, you need to deactivate the Synchronize standard call number setting. A name extension for the various call number types should also be configured so that all the numbers do not appear under one name in the communication server's private directory. For example, for the business call number under Synchronize business call number, enter the setting _B. Make sure the name extension you choose is not too long as the length of names is limited in the communication server. If a call number type is not to be synchronized, enter the setting NOSYNC.

RSS Driver

The RSS Driver (internal OIP service) is the interface adapter used for accessing the RSS Feeds.

Registration Manager

Registration Manager (internal OIP service) is responsible for managing the registered applications.

Table 3.81:License Manager Specific Properties

Specific properties	Description	Default Settings
Registered applications log file	Directory in which the log file with the applications registered on the OIPserver is stored. The basic directory is the OIP installation directory.	.logs/registration.txt

Registration Service

Registration Service is responsible for registering applications.

Routing Manager

The Routing Manager (internal OIP service) is responsible for managing the call distribution in the communication server.

Routing Service

The Routing Service is responsible for accessing the call distribution in the communication server.

SMTP Driver

The SMTP Driver (internal OIP service) is the interface adapter for sending e-mails and text messages (e-mail to text message).

The settings for connecting to the external e-mail server are made here.

Table 3.82:SMTP Driver Specific Properties

Specific properties	Description	Default Settings
SMTP server address	DNS name or IP address of the SMTP mail server.	
IP port	IP port of the SMTP mail server.	25
User name	User name for authentication on the SMTP mail server.	
Password	Password for authentication on the SMTP mail server.	
SMS server address	DNS name or IP address of the alternative SMS mail server if not identical with the SMTP mail server.	
SMS Server IP Port	IP port of the alternative SMTP mail server.	
SMS Gateway Address	SMS gateway address which is added to the mobile number to form the e-mail address (...@example.com).	

Security Service

The Security Service (internal OIP service) provides the encryption and decryption algorithms of security-relevant data for OIP Services.

Server Utility Service

Server Utility Service (internal OIP service) provides internal tools for OIP Services.

Service Manager

Service Manager (internal OIP service) is responsible for the local management of the Services on the OIP server.

Table 3.83:Service Manager Specific Properties (Sheet 1 of 2)

Specific properties	Description	Default Settings
Maximum memory	Limiting the memory in the clients for OIP supporting applications (in megabytes)	128m

Table 3.83:Service Manager Specific Properties (Continued) (Sheet 2 of 2)

Specific properties	Description	Default Settings
Register OIP server on the client under the IP address.	Activated: The OIP server registers with the client under the IP address and not with the host name. OIP Restart the server to apply the set- ting.	Disabled

Shortdial Directory Service

Shortdial Directory Service (internal OIP service) is responsible for managing the communication server Abbreviated dialing.

The setting for the range of the common abbreviated dialing in the MiVoice Office 400 network can be made here.

Table 3.84:Shortdial Directory Service Specific Properties

Specific properties	Description	Default Settings
Synchronization interval	Synchronization interval (in minutes) in which the abbreviated dialing list is cached in the OIP database.	30 0 – No synchronization
Synchronization range	Range of shared abbreviated dialing numbers in the communication server	7000-7999
Name order	Format of the name entries in the communication server abbreviated dialing directory.	*Last name - first name*
Number of call number digits	Number of phone number digits from back which are used to compare with the entries in the directory.	7
Call number shown with name dialing	This setting lets you specify whether the abbreviated dialing number or the call number is displayed during a name search in the public communication server directory.	Abbreviate dialing no.(default value), Call number.

Subscriber Directory Service

Subscriber Directory Service (internal OIP service) is responsible for managing the internal private contacts.

Table 3.85:Subscriber Directory Service Specific Properties

Specific properties	Description	Default Settings
Name order	Format of the name entries in the communication server subscriber directory.	First name - last name
Number of call number digits	Number of phone number digits from back which are used to compare with the entries in the directory.	7

Subscriber Configuration Manager

Subscriber Configuration Manager (internal OIP service) is responsible for managing the user settings.

Subscriber Configuration Service

Subscriber Configuration Service is responsible for user and terminal settings.

System User Directory Service

System User Directory Service (internal OIP service) is responsible for managing all the registered users on the OIP server.

Specific properties	Description	Default Settings
Name order	Format of the name entries in the OIP user directory.	*First name - Last name*
Number of call number digits	Number of phone number digits from back which are used to compare with the entries in the directory.	7

TTS Manager

The TTS Manager (internal OIP service) is responsible for managing the TTS (Text-To- Speech) resources, synthesizing the speech files and providing the wav-files.

Table 3.86:TTS Manager Specific Properties

Specific properties	Description	Default Settings
Default speaker	List of installed language bundles.	
Installed language bundles	The default speaker is used if no other speaker was found.	

Test Manager

The Test Manager (internal OIP service) is responsible for the execution of OIP/communication server test orders.

Table 3.87:Test Manager Specific Properties

Specific properties	Description	Default Settings
Save test results in database	Number of days the test results are stored in the database.	10 0 – Database entries are not deleted

Test Service

The Test Service is responsible for managing the OIP/ communication server test orders.

Table 3.88:Test Service Specific Properties

Specific properties	Description	Default Settings
dummy		

Ticket Service

Ticket Service is responsible for managing the call tickets.

Specific properties	Description	Default Settings
Save ticket entries in database	Number of days during which the call tickets are stored in the database	10 0 – Database entries are not deleted

The call tickets are erased from the OIP database at the time listed in *"OIP database reorganization times"* see also *"Reorganize OIP database"*.

Time Service

Time Service (internal OIP service) is responsible for managing time synchronization.

Table 3.89:Time Service Specific Properties

Specific properties	Description	Default Settings
Timesynchronization	Activate or deactivate the time synchronization between the communication server and OIP server.	*Disabled*
Synchronization interval	Interval (in hours) in which the time synchronization is carried out.	24 1 to 24
Time synchronization from the OIP server	Activate or deactivate whether the OIP server is linked to the time synchronization.	*Disabled*
Synchronization command	Command for the time synchronization on the OIP server.	date dd.mm.yyyy; time hh:mm:ss

If no time master is configured in the communication server settings, the OIP server is automatically activated as time master.

TwixTel Directory Service

The TwixTel Directory Service (internal OIP service) is responsible for managing the external phone-book directories TwixTel.

Table 3.90:TwixTel Directory Service Specific Properties

Specific properties	Description	Default Settings
Phone book server address	DNS name or IP address of the server on which the external phone-book directories are installed.	
Number of call number digits	Number of phone number digits from back which are used to compare with the entries in the directory.	0

Specific properties	Description	Default Settings
Alias name order	Format of the alias name.	*Last name - first name*
Use generated default alias	Generates a default alias (display name) for each contact defined in the Contact Name Order setting.	*Enabled*
Data source	Display the used version of DasTelefonbuch Germany.	

User Preferences Service

User Preferences Service is responsible for managing the user customized settings.

User Profile Manager

User Profile Manager (internal OIP service) is responsible for global OIP user management.

Table 3.91:User Profile Manager Specific Properties

Specific properties	Description	Default Settings
Datasource username	The user name data source can be configured. The user name will be adapted in the OIP and internal user directory according to the setting.	Active Directory / OIP subscriber directory / PBX user directory

User Profile Service

User Profile Service is responsible for the access to OIP users.

User Service

User Service is responsible for controlling and monitoring applications.

Table 3.92:User Service Specific Properties

Specific properties	Description	Default Settings
Heartbeat interval	Heartbeat interval (in milliseconds) between OIP and application.	60000

Voice Mail Manager

Voice Mail Manager (internal OIP service) is responsible for managing the voice mails.

Table 3.93:Voice Mail Manager Specific Properties

Specific properties	Description	Default Settings
Save voice mails	Number of days the voice mails are stored	10

Specific properties	Description	Default Settings
Voice mail file type	Type (wav or mp3) of the voice mail file. Bit rate for mp3 voice mail file	
Bit rate for mp3 voice mail file	Bit rate for mp3 voice mail file	
Voice mail number PBX <communication server ID>	Voice mail number in the communication server	

Voice Mail Service

Voice Mail Service is responsible for managing the mailboxes.

WEB Server Service

WEB Server Service (internal OIP service) is responsible for managing the Tomcat Web Server.

The web server port can be changed here if the OIP server is started in console mode. If the port is changed, remember that the OIP server has to be restarted and all the OIP Clients re-installed or re-configured.

Specific properties	Description	Default Settings
IP port	IP port of the OIP Web server.	<defined during installation>
Root directory	Root directory of the OIP web server.	*axp*

OIP Export Data

The export data is created or deleted at the times listed in the following table. If so configured in the OIP services.

Table 3.94:Export data create times

Export data	OIP Service	Time
ACD statistics	ACD Log Manager	Configurable in ACD Log Manager
Call data	Call Logging Driver	23:45
I/O Data	I/O Manager	01:00:00 if configured daily

Call Centre Statistics Data

The Call centre statistics data are stored in four files on the OIP server if so selected during the user-defined installation of the OIP server.

- Call centre status data (callcenter-@DATE-@TIME.txt)
- Call centre call data (acdcall-@DATE-@TIME.txt)
- Agent status data (agentstatus-@DATE-@TIME.txt)
- Agent call data (agentcall-@DATE-@TIME.txt)

In the default settings, a new file is written daily to the directory <OIP-directory>\acd- log. The files are created in .txt format. The file names contain time variables so that the time stamp is added each time a new file is created. With fixed file names no new file is created before the existing file is deleted from the folder.

The Call centre statistics data can be provided in the OIP service ACD Log Manager.

Call Centre Status Data

A snapshot of the call centre is mapped in the call centre status data. The snapshot interval can be configured in the OIP Service ACD Log Manager.

Table 3.95:Designator for the Call Centre status data (Sheet 1 of 2)

Designator	Description
CallCenterID	Call centre ID The Call Centre ID can be set in the ACD Log Manager.
LogID SkillID	Unique log ID Skill ID
Date	Date of the snapshot.
Time	Time of the snapshot.
AgentsLoggedIn	Number of agents logged on.
AgentsReady	Number of agents whose status is Available.
AgentsRinging	Number of agents whose status is Ringing.

Table 3.95:Designator for the Call Centre status data (Continued) (Sheet 2 of 2)

Designator	Description
AgentsConnected	Number of agents whose status is Connected.
AgentsPause	Number of agents whose status is Pause.
AgentsWrapUp	Number of agents whose status is Wrap up.
CallsWaiting	Number of calls waiting in the ACD queue.

Call Centre Call Data

In the call centre calls data each incoming call to the call centre is listed in the ACD Queue.

Table 3.96:Designator for the call centre call data (Sheet 1 of 2)

Designator	Description
DisconnectTime	Time at which the call in the ACD Queue was completed.
DDI	DDI dialled by the caller.
CLIP	Caller CLIP.
SkillID	Skill ID of the called Skill.
CallStateBeforeIdle	Status of the call to the call centre before it switches to available.0 - unknown / 1 - available / 2 – call to ACD queue / 3 - connected / 4 – on hold/ 5 – call to agent
ExtWaitDuration	Caller ringing time in (in seconds) before the call centre call was answered.
ExtCopyDuration	Caller call duration (in seconds)
CallCenterID	Call centre ID The Call Centre ID can be set in the ACD Log Manager.
LogID	Clear protocol ID
Date	Date of the call to the call centre.
RingTime	Time at which the call in the ACD Queue is first signalled.
AgentConnectTime	Time at which the call is signalled to the first agent.

Table 3.96:Designator for the call centre call data (Continued) (Sheet 2 of 2)

Designator	Description
AgentRingTime	Time at which the call in the ACD Queue was answered. If Courtesy is activated, the call is considered answered when Courtesy starts up.
AnswerTime	Time at which the call was answered by the agent.

Agent States Data

The agent status data lists every change in agent status.

Table 3.97:Designator of the agent status data

Designator	Description
CallCenterID	Call centre ID The Call Centre ID can be set in the ACD Log Manager.
LogID	Clear protocol ID
UserID	Unique OIP user ID of the agent.
AgentCallLogID	Reference to the Log ID in the agent call data.
Date	Date
Time	Time
State	Agent status after status change
WrapupCode	0 – logged out / 1 – logged in / 2 - busy (call centre or private call) / 3 - pause / 4 – wrap-up / 5 - unknown
PauseCode	Wrap-up code - 0 if no wrap-up code is defined. Pause code - 0 if no pause code is defined.
SkillID	Skill ID assigned to the call.
ReadyAgents	Number of agents logged on and ready at the time of the agent status change.
LoginState	0 - Agent logged on during status change / 1 - Agent was logged on during status change / 2 - Agent logged out during status change / 3 - Agent was logged out during status change

Agent Calls Data

In the agent call data each incoming call centre call of the agents is listed.

Table 3.98:Designator of the agent call data

Designator	Description
CallCenterID	Call centre ID The Call Centre ID can be set in the ACD Log Manager.
LogID	Unique log ID
UserID	Unique OIP user ID.
AcdCallID	Unique call centre Call ID.
Date	Date
RingTime	Ringing time of the call on the ACD Queue.
AnswerTime	Time at which the call was answered.
DisconnectTime	Time at which the call was completed.
WrapupTime	Time at which the wrap-up time was completed.
WrapupCode	Wrap-up code - 0 if no wrap-up code is defined.
CallStateBeforeIdle	Status of the call to the call centre with the agent before change to available. 0 - available / 1 – dialing tone / 2 - dialing / 3 – ringing phase / 4 - proceeding / 5 - busy / 6 - connected / 7 - hold / 8 – on hold / 9 – incoming call / 10 – call deleted / 11 - conference / 12 - callback / 13 – reminder call / 14 – incoming announcement / 15 – outgoing announcement / 16 – function successfully completed / 17 – park / 18 - intrusion / 19 - unknown
SkillID	Skill ID assigned to the call.
DDI	DDI dialled by the caller.
CLIP	Caller CLIP.
RingDuration	Ringing time with the agent (in seconds)
ConvDuration	Duration of the call centre call (in seconds)
WrapupDuration	Duration of the wrap-up time of the call centre call (in seconds)

Call data

The call data is stored as a file on the OIP server if so selected during the user-defined installation of the OIP server.

In the default settings, a new file is written daily to the directory *<OIP-directory>tax*. The files are created in .csv format. The file name is taxdata-yyyy-mm-dd.tax, with yyyy-mm-dd representing year-month-day.

The Call Logging settings can be made in the OIP service Call Logging Driver.

The following table lists the designators of the call data records. The column Designator PC5 format lists the relevant data fields of the PC5 format. More details on the PC5 format can be found in the MiVoice Office 400 System Manuals.

Table 3.99:Designators of the call data records (Sheet 1 of 3)

Designator	Description	Designator PC5format
Ticket ID	Unique Ticket ID	
CS name	Name/ID of the communication server on which the user is created.	
Serial ID	While the serial number is unique for each communication server, it can be assigned several times within the network. If, in the OIP configuration in the OIP service, Call Logging Driver the option Update journal entry is activated, the call ID is added instead of the serial ID.	SERIALNO.
Sequence number	While the sequence number is unique for each communication server, it can be assigned several times within the network.	SEQ.NO.
Call number	Call number	No.
User ID	ID of the user on the OIP server.	
User name	User name	
Cost centre	Cost centre number	CC
Direction	Call direction: 0 - unknown / 1 - incoming / 2 - outgoing	SZ x
Call destination	Destination or source network: *0 - unknown / 1 - exchange / 2 - PISN*	SZ x

Table 3.99:Designators of the call data records (Continued) (Sheet 2 of 3)

Designator	Description	Designator PC5format
Call type	Network access type: 0 - unknown / 1 – network access, business, transferred / 2 – network access, business, subscriber dialled / 3 - incoming / 4 – incoming to ACD destination / 5 - PISN transit / 6 – network access with cost centre selection, transferred / 7 – network access with cost centre selection, subscriber dialled / 8 – network access, private, transferred/ 9 – network access, private, subscriber dialled	SZ y
Call handling	Call Handling Incoming calls: 0 - unknown/ 1 - transferred/ 2 – answered directly / 3 - unanswered / 4 - answered / 5 – transferred to network / 6 – data service call / 7 – rejected call Call Handling Outgoing Calls: 0 - unknown / 1 – normal call / 2 – transferred by CFU/CFNR/CD to network / 3 – transferred by internal user / 4 – data service call / 5 – booth call / 6 – room call	SZ z
Start date	Date of start of connection	DATE
Start time	Time of start of connection	TIME
Duration	Duration of connection	DURATION
Time to answer (TTA)	Call duration until the call was answered	TTA
Call charges	Call charges	CHARGE
Metering pulses	Metering pulses	METPUL
CS name interface	Home communication server	
Node	AIN node ID	
Interface card	Card on the home communication server	EXCH
Interface port	Port on the home communication server	EXCH
Channel group	Channel group on the home communication server	EXCH
Caller ID 1	Caller identification 1	ID1

Table 3.99:Designators of the call data records (Continued) (Sheet 3 of 3)

Designator	Description	Designator PC5format
Caller ID 2	Caller identification 2	ID2
Destination number 1	Destination number 1	DEST1
Destination number 2	Destination number 2	DEST2
Gateway CS	The communication server connected with the public exchange as a gateway.	
Gateway nodes	AIN nodes via which to access the network.	
Gateway interface card	Network card via which to access the network.	
Gateway port	Port via which to access the network.	
Gateway channel group no.	Channel group via which to access the network.	
Number of hops	Number of communication servers that sent call data records for the ticket.	
Origin CS	Communication server on which the call was made.	
Origin call number	Call number on which the call was made.	
Origin user name	User who made the call.	
CL data records	Number of individual call data records from which the ticket was cre- ated.	
Completed	Ticket state: *0 (false)- not completed / 1 (true) - completed*	
Confirmed	*0 (false)- not confirmed / 1 (true) - confirmed*	
Ticket date	Ticket issue date	
Ticket time	Ticket issue time	

I/O Data

The I/O Manager can be used to set for each configured action whether the action in question should be monitored. If monitoring is activated, a new file is written daily to the directory. *<OIP-directory>\iolog*. The files are created in .csv format. The file name is iolog-dd-mm-yyyy-hh-mm-ss, with <dd-mm-yyyy> representing day-month-year and <hh-mm-ss> for hour-minute-second.

The settings for creating the I/O data can be made in the OIP service I/O Manager. The following table lists the designators for the I/O data records.

Table 3.100:Designation for the I/O data records

Designator	Description
Date	Date on which the action was carried out.
Time	Time at which the action was carried out.
ActionId	Action ID of the action carried out.
DataType	Data type
DataSubType	Other data type if action is supported.
Data	Data sent with the action.

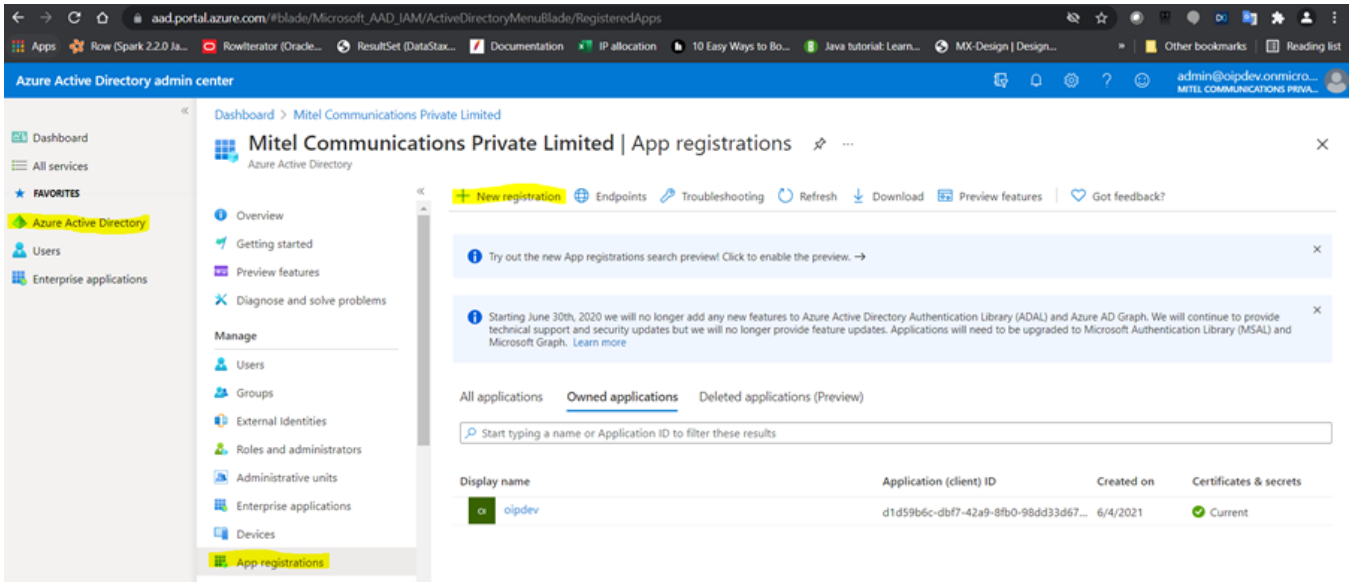
OAuth Token Authentication Procedure for Microsoft Exchange

This chapter describes the procedure to authenticate Microsoft Office 365 services by enabling OAuth token.

Register your application

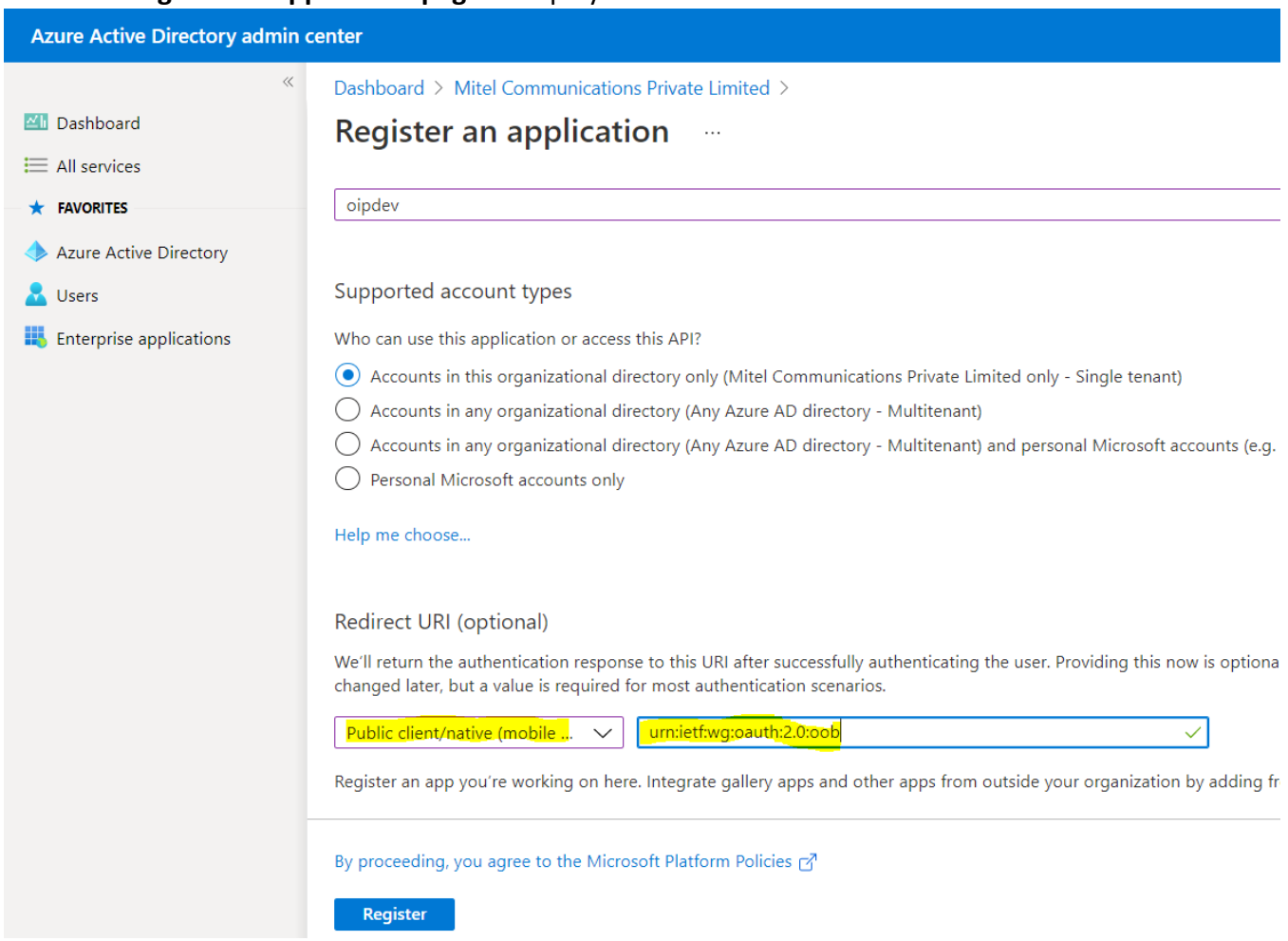
To receive the OAuth Token from Microsoft, the application must be registered in the Azure Active Directory. To use OAuth, an application must have an application ID issued by Azure Active Directory. In the following procedure, it is assumed that the application is a console application and you need to register your application as a public client with Azure Active Directory. You can register an application in the Azure Active Directory admin center or by using Microsoft Graph.

1. In the browser, navigate to the **Azure Active Directory** admin center Azure Active Directory admin center and log in using a personal account (also known as Microsoft Account) or work or school account.
2. Select **Azure Active Directory** in the left navigation panel, and then select **App registrations** under **Manage** as shown in the following image:



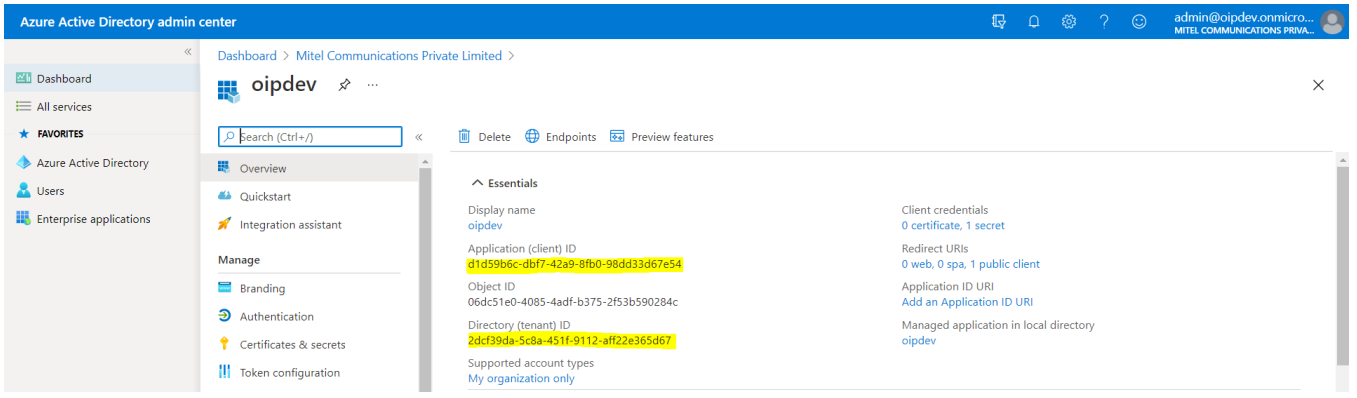
3. Select **New registration**.

The **Register an application page** is displayed.



4. On the **Register an application** page, enter the following:
   - Enter a name for your application.
   - Select **Supported account types** of your choice.
   - For **Redirect URI (optional)**, select **Public client (mobile & desktop)** from the drop-down list and set the value to `urn:ietf:wg:oauth:2.0:oob`.

5. Click **Register**. The **Application (client) ID** and **Directory (tenant) ID** are generated as shown in the following image. Copy the values and save them as you need the values later.

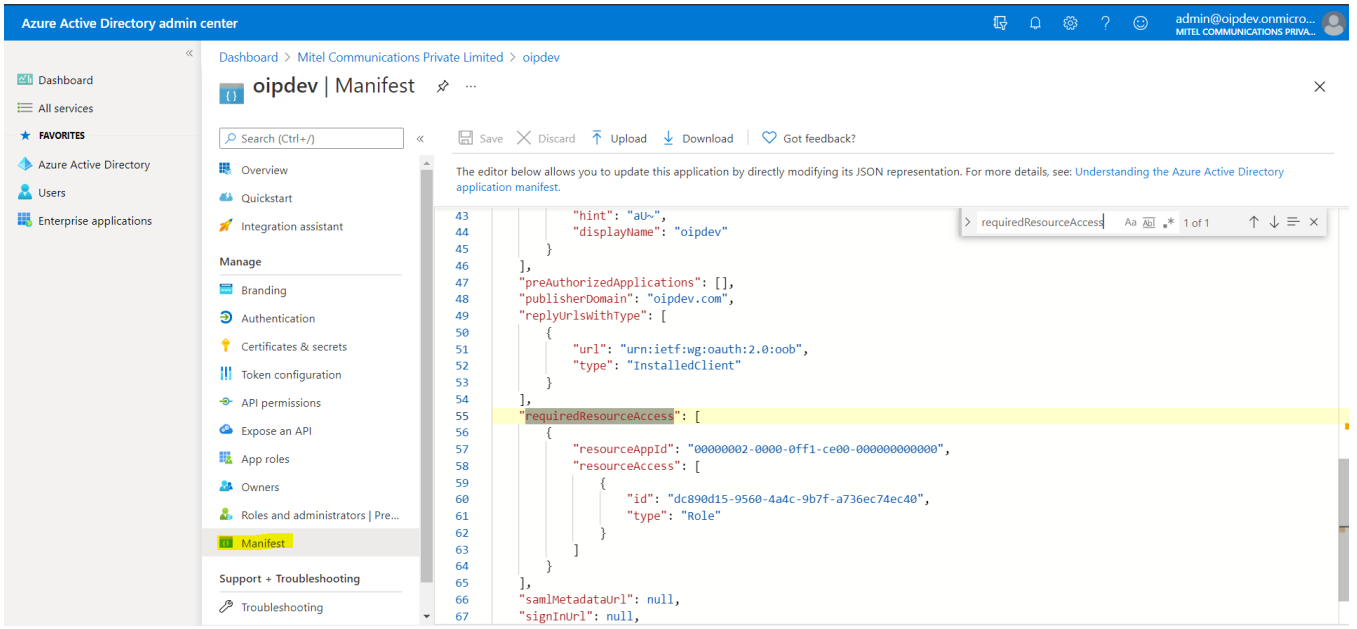


Configure for app-only authentication

This procedure must be completed to use application permissions.

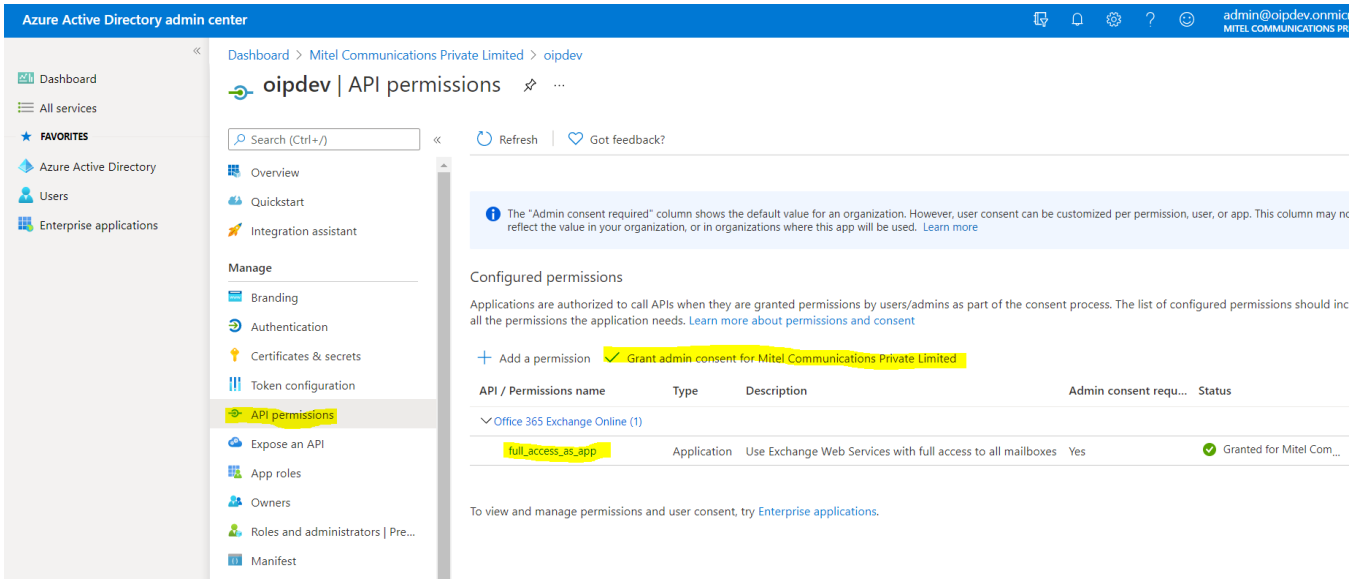
1. Select **Manifest** in the left navigation panel under **Manage**.
2. Locate the `requiredResourceAccess` property in the **Manifest** and add the following inside the square brackets ([]):

```
JSONCopy
{
"resourceAppId": "00000002-0000-0ff1-ce00-000000000000",
 "resourceAccess":
[
 {
 "id": "dc890d15-9560-4a4c-9b7f-a736ec74ec40",
 "type": "Role"
 }
]
}
```



3. Click **Save**.

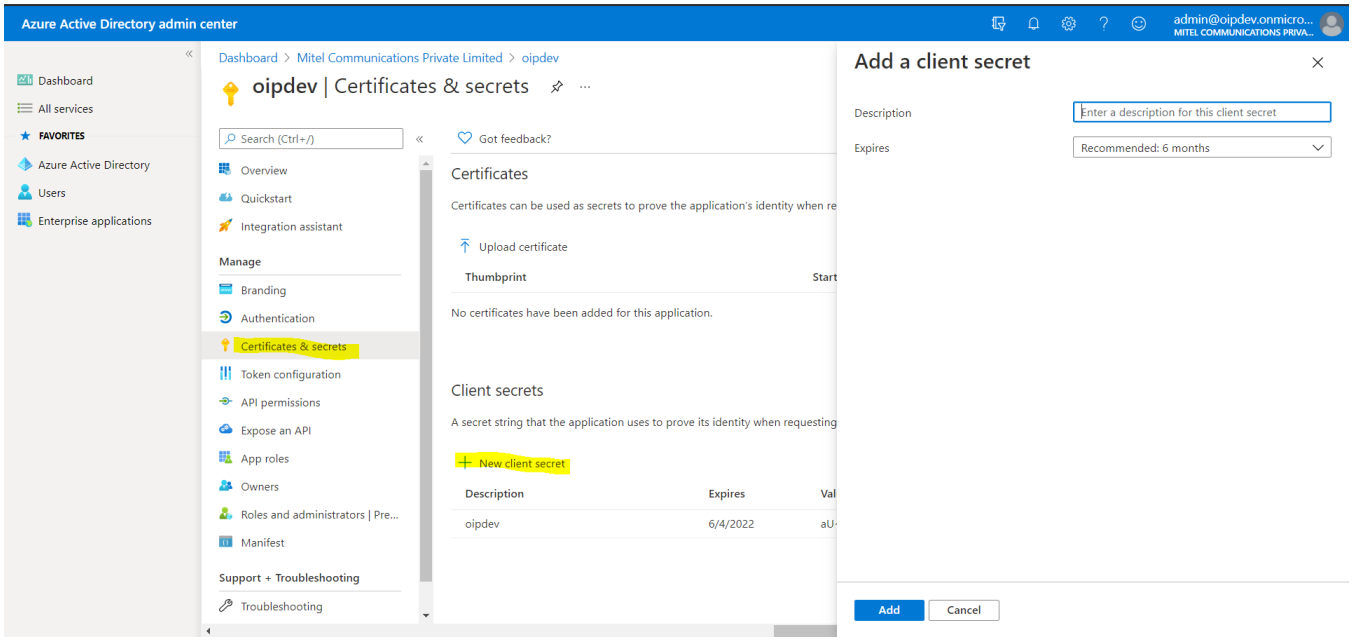
4. Select **API permissions** under **Manage**. Confirm that the **full_access_as_app** permission is granted as shown in the following image.



5. Select **Grant admin consent for org** and accept the consent dialog.

6. Select **Certificates & secrets** in the left navigation panel under **Manage**.

7. Select **New client secret**, enter a short description, and click **Add** as shown in the following image.



8. Copy the value of the **Secret ID** that you added client secret and save it as you will need it later.

NOTE: The value is visible only when you first create the client secret code. Make sure to copy it.

The following values are used for Microsoft Office 365 OAuth authentication in the OIP Exchange Configuration:

1. Application Client ID (Application (client) ID generated in step 5 of the **Register your application** procedure.
2. Application Tenant ID (Directory (tenant) ID generated in step 5 of the **Register your application** procedure.
3. Client secret code (Secret ID generated in the step 8 of the **Configure for app-only authentication** procedure.

Configure Microsoft Office 365 with OIP

1. To configure Microsoft Office 365 on OIP Web Admin, go to **Configuration** > **Exchange connection**.
2. Select Microsoft Exchange Office 365 from the **Microsoft Exchange version** drop-down list.
3. Enter values in the other fields.

   Make sure to enter the values of Application Client ID, Application Tenant ID, and Client secret code generated in the preceding procedures.

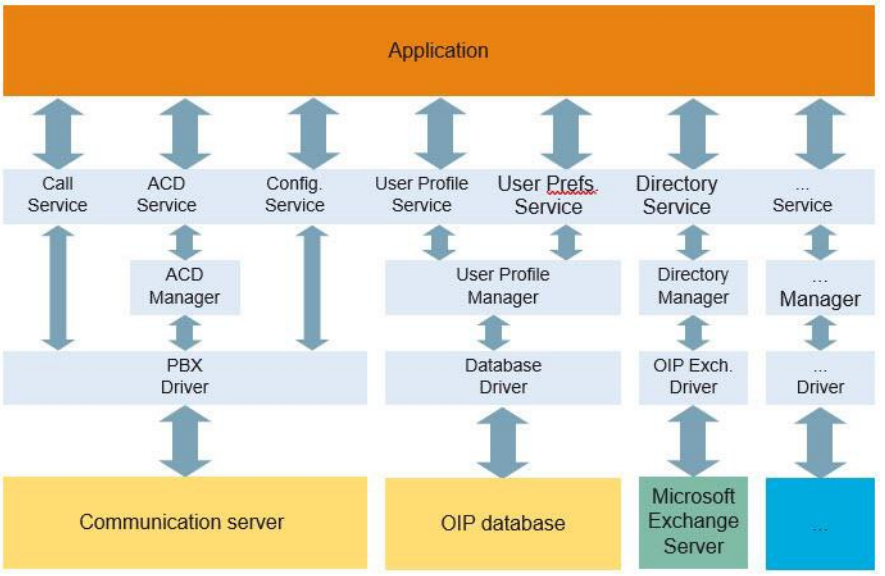
Directories

Attached directories can be used, for name dialing or name identification of incoming calls.

Apart from the directories of the attached communication server, you can also attach Microsoft Exchange, LDAP and ODBC directories and Microsoft Active Directory and commercial electronic phone books.

The following figure provides an overview of the various directories.

Figure 5.1: Overview of the directories



The OIP server has direct access to the communication server directories, OIPdirectories, Active Directory, LDAP directories and external telephone directories. The Microsoft Exchange directories are accessed indirectly via the OIP directories by being synchronized with one another.

The communication server, OIP and Microsoft Exchange directories have not just read rights but also write rights so that new contact entries can be created and existing entries edited. The OIP server only has read rights on LDAP directories and external telephone directories. You can configure users' access rights to the individual directories by assigning the users to user groups to which the OIP service Directory Service has been assigned.

Configuring the Directory Connection

No configuration is required on the communication server to connect a communication server to the OIP server. When several communication servers are connected, check that the abbreviated dialing on all communication servers are identically defined.

When external directories are connected, an appropriate OIP driver must be installed.

The OIP driver is installed, and the connection configured via OIP WebAdmin. You can find configuration and installation instructions in the OIP WebAdmin Online help.

Connecting Microsoft Exchange directories

By connecting Microsoft Exchange Server to OIP it is possible to access the following Microsoft Exchange directories:

- Public Contacts Folders
- Mailboxes of the domain user
  - Personal Outlook address book
  - Calender
  - E-mail folder

Thanks to the access to the domain user's mailboxes, the contact entries of the personal Outlook address book can be synchronized with the private OIP directory. Moreover, existing calendar entries can be displayed in the presence display.

The presence status of Microsoft Outlook calendar entries is displayed in the OIP calendar by the OIP presence status (see *"Presence status in the OIP"*)

Access to the e-mail folder is required to store voice mails as e-mail in the Inbox.

The settings for connecting a Microsoft Exchange Server can be made in the Configuration / Microsoft Exchange view.

The Microsoft Exchange Server can be connected either via the platform-independent integrated Microsoft Exchange driver or via the Windows-based external OIP Exchange driver.

Connecting Active Directory

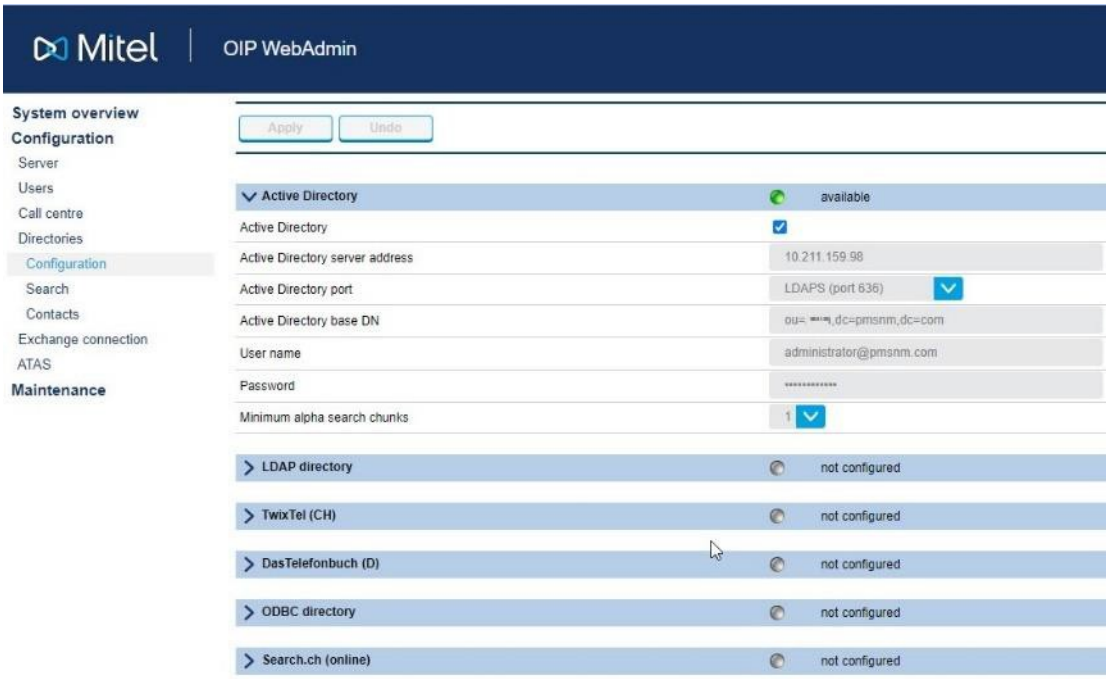
The Active Directory connection provides the possibility of connecting the Active Directory to the OIP server.

The Active Directory is accessed in read only mode, i.e. it is not possible to modify the data in the Active Directory.

The contact data is made available to the communication servers via the OIP Name Server, see *"OIP name server"*

Port 636 allows a secure connection from OIP to LDAPS and Active Directory. To connect to AD using secure LDAP follow the steps:

1. Log in to OIP WebAdmin.
2. Navigate to **Configuration** > **Directories** > **Configuration**



3. Expand Active Directory.
4. From the drop-down list of Active Directory port select LDAPS (port 636) and click **Apply**.

The LDAP Directory Service allows you to connect external LDAP directories to the OIP server. To access the LDAP directories, you need, while installing the OIP server, to select the option Connection of LDAP directories.

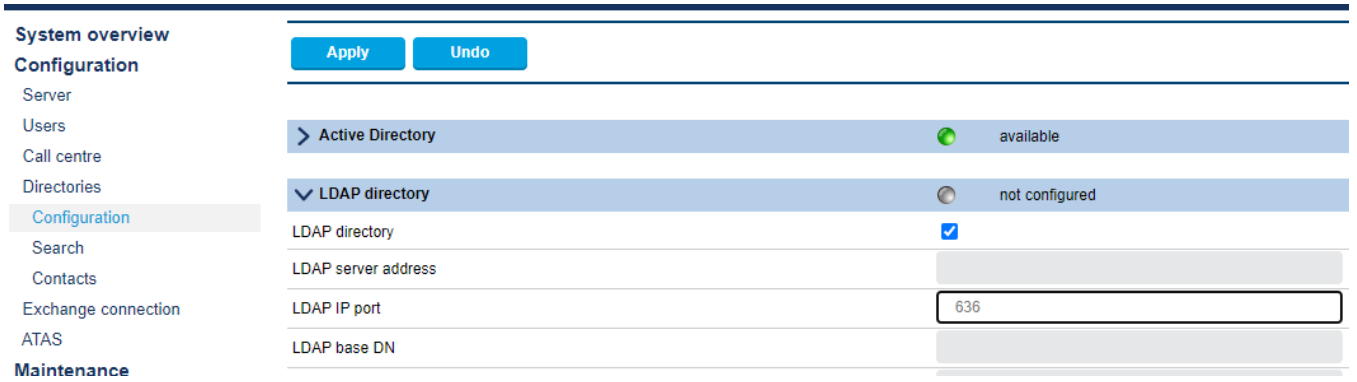
The LDAP directories are accessed in read mode, i.e. it is not possible to modify the data in the LDAP directory. One LDAP directory can be connected per OIP server.

The contact data is made available to the communication servers via the OIP Name Server, see *"OIP name server"*

The users can enter port 636 in the port field to have a secure connection from OIP to LDAPS and Active Directory.

To enter the LDAP IP port follow the steps:

1. Log in to OIP WebAdmin.
2. Navigate to **Configuration** > **Directories** > **Configuration**.
3. Expand **LDAP directory** and select the check box **LDAP directory**.



4. Enter 636 in **LDAP IP port** and click **Apply**.

NOTE: The FQDN of the Active Directory must be resolvable from the OIP server.

Connecting external phone-book directories

External telephone directory connection to OIP refers to phone book CDs or ODBC di- rectories, for instance, from spreadsheet applications.

To access the external phone-book directories, while installing the OIP server, you need to select the option Connection of external phone book directories (phone book CD).

The settings for connecting the phone book CD server in the OIP server can be made either when the OIP server is installed or later in the OIP service Phonebook Directory Service.

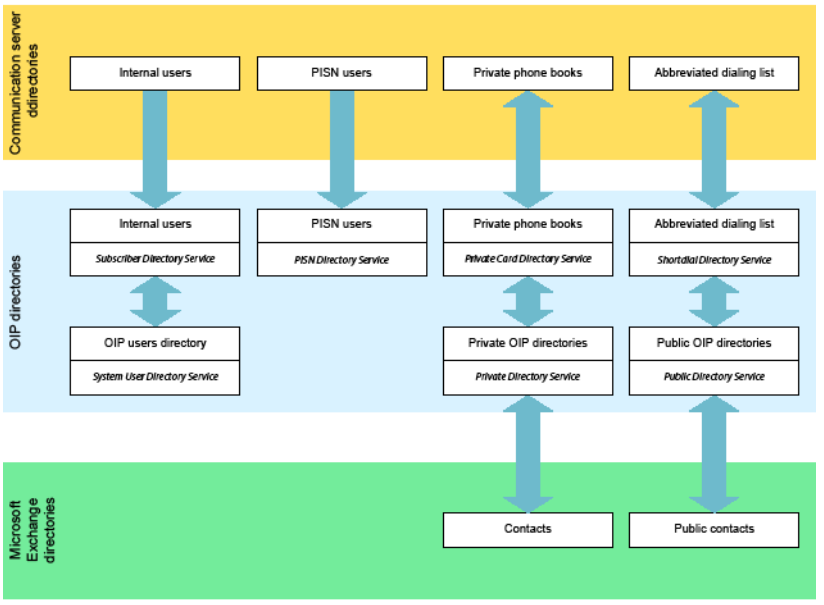
Not all phone-book CD manufacturers provide an interface on which the OIP server can access. As a result only those phone-book CDs that have an appropriate interface can be connected. External phone-book CDs are connected via a corresponding driver, which has to be installed on the PC on which the phone-book CD is placed in the CD-ROM drive or has been installed.

Directories Synchronization

The directories of the connected communication servers are synchronized with the OIP directories. If a Microsoft Exchange Server is connected, the Outlook directories are also synchronized with the OIP directories. Connected LDAP directories, external telephone directories and Active Directory are not synchronized.

The following figure shows the synchronization of the directories, and the relevant OIP services.

Figure 5.2: Directories Synchronization



Contact entries in the synchronized directories are managed via Mitel OfficeSuite, operator applications, OIP WebAdmin or via Microsoft Outlook. Synchronized directories of networked communication servers are managed via OIP WebAdmin.

Communications Server Directories

The communication server and OIP directories are synchronized via the communication server directories temporarily stored on the OIP server (see **Fig. 5.2**). The synchronization interval can be defined in the OIP services *Shortdial Directory Service*, *Private Card Directory Service* and *PISN Directory Service* through the *Synchronization interval* option. The default setting is 30 minutes. Within this interval, modifications in the communication server directories are imported and synchronized with the OIP directories. On the other hand, modifications in the OIP directories are directly reflected in the communication server directories.

The option *Synchronization of OIP and PBX directories* is activated in the default OIP server installation. During operation, you can activate, deactivate and configure synchronization via OIP WebAdmin in the Configuration / Server / General view.

The first synchronization after OIP server start takes place after a configurable start delay. For the synchronization of public directories, set the synchronization delay in the OIP service *Public Directory Service*. For the synchronization of private directories, set the synchronization delay in the OIP service *Private Directory Service* If multiple communication servers or a communication server network are connected, synchronization is carried out sequentially.

Check that the number of possible entries in the communication server directories is limited so that, under certain circumstances, not all the OIP directory contact entries can be synchronized in the communication server directories. You can increase the number of synchronized contacts if you are only synchronizing a certain number of call number types. You can make the settings in the OIP services *PBX Driver Ascotel* and *Public Directory Service*. Only the business call number is synchronized in the standard settings.

Public Directories

An OIP folder is created in the public OIP directory for synchronizing abbreviated dial- ling lists. The folder name can be changed if necessary. Contact entries in the public OIP directory including entries in the sub-folders are also synchronized in the abbreviated dialing list.

In a networked environment with several communication servers, the abbreviated dialling lists must be identically defined in all the networked communication servers.

Private directories

Contacts in the private communication server phone books are synchronized in the private OIP directory. Contact entries in the private OIP directories including entries in the sub-folders are also synchronized in the private communication server phone books.

Microsoft Exchange Server ectodirries

Synchronizing Public Contacts Folders

The public contact folders on the Microsoft Exchange Server can be synchronized with the public OIP directories. The Outlook contact folders to be synchronized can be configured in the OIP service *Public Directory Service* under the Synchronize public contact folder option. The folder structure of the public folders on the Microsoft Exchange Server is transferred to the public OIP directories.

To also synchronize a public Outlook contact folder on the Microsoft Exchange Server with the communication server abbreviated dialing list, enter the name of the public Outlook contact folder in the OIP service *Public Directory Service* in the Public default contact folder option. If it is located in a sub-folder, enter the corresponding path. Only a public Outlook contact folder can be synchronized with the communication server's abbreviated dialing lists.

Synchronizing private Outlook address books

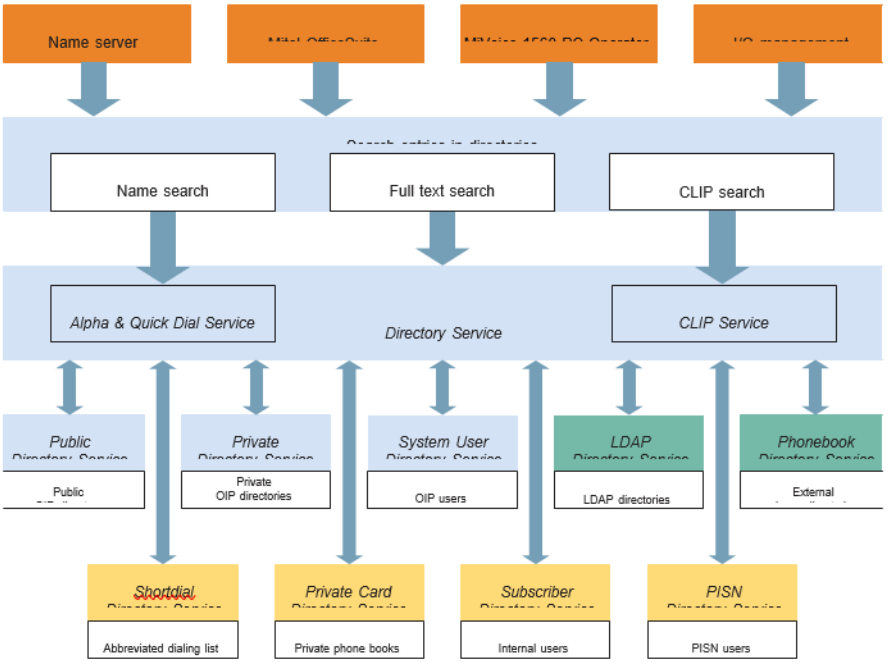
The private Outlook contacts, together with the sub-folders, are synchronized with the private OIP directories. The folder structure of the sub-folder is copied in the process.

Searching in directories

There are three different ways of searching through directories:

- With the Full-text search the string of search characters entered is searched for in all the contact data fields.
- With the Contact search the string of search characters entered is searched for in the name fields.
- With the CLIP search a contact corresponding to a known phone number is searched for.

Figure 5.3: Search in directories



All the search requests are sent to the OIP service *Directory Service*. With a full-text search the search request is forwarded directly to the configured directories. With the contact and CLIP search the search request is made via the OIP services *Alpha & Quick Dial Service* and *CLIP Service*. The sequence of the string of search characters (e.g. Name-First name) can be configured in the corresponding OIP services.

The search in OIP applications

OIP applications search in the directories which are globally entered in the OIP service *Directory Service*. The setting for the *OIP Name Server* is made accordingly in the OIP services *Alpha & Quick Dial Service* and *CLIP Service*. In the OIP applications the global setting can be restricted further for each user, where configurable.

OIP name server

The OIP name server gives the communication server access to the directories man- aged by OIP. This means that name searching when dialing from system phones is not limited to just the communication server directories; depending on the connection it can be complemented with external OIP directories, Microsoft Exchange directories, LDAP directories and external phone book directories.

Dialing by name

The directories covered by the name search and the sequence in which the directories are to be searched can be configured in the OIP service *Alpha & Quick Dial Service*. The user is shown all the possible entries that are found in the various directories.

Dialing by name can be carried out in two ways on the system phone to minimize the list of search results, e.g. for frequent internal name searches.

- A name dial search without search prefix only searches in the basic directories de- fined in the OIP service *Alpha & Quick Dial Service*. In the default setting those di- rectories are the OIP and communication server directories, depending on the installation.
- A name dial search with search prefix only searches in the extended directories defined in the OIP service *Alpha & Quick Dial Service*. The search prefix is also defined in the OIP service *Alpha & Quick Dial Service*.

If the OIP directories are synchronized with the communication server directories, while selecting the basic directories, check that name search is only allowed on one of the directories.

CLIP analysis

To evaluate the incoming call CLIPs, the directories configured in the OIP service is accessed *CLIP Service*. The user is shown the first match.

If the OIP directories are synchronized with the communication server directories, while selecting the basic directories, check that CLIP evaluation is only allowed on one of the directories.

The search sequence depends on the settings in the OIP service *CLIP Service*.

The OIP Name Server is automatically activated when the OIP server is started. No settings are required in the communication server.

OIP image server

Applications and phones which support contact images can obtain these from the OIP image server. The OIP image server can be synchronized with an image server in the cloud or via a connected Microsoft Exchange Server.

The image server downloads the images to a local directory on the OIP computer. Any image file in the cloud can be used as an image source. If Microsoft Exchange is connected, then the images in the public contacts are used as an additional source. The images are updated at the set intervals.

OIP that support contact images download the images directly from the OIP image server. The image size is adjusted automatically here.

The communication server can be connected to the OIP image server. As soon as the OIP image server is activated, OIP enters the address of the OIP image server in the communication server. Applications and phones on the communication server that support contact images also download the images from the OIP image server in this way. However, the image size is not adjusted here. The images should already have been stored with the appropriate dimensions and format.

OIP only enters the address of the OIP image server in the communication server when no other image server is configured there.

Table 5.1:Information about the OIP image server (Sheet 1 of 2)

Configuration element	Description
File path of the images	<OIP directory>\webapps\axp\images\contacts
Image format and size	PNG, 150 x 200 pixels

Table 5.1:Information about the OIP image server (Continued) (Sheet 2 of 2)

Configuration element	Description
Configuring the image server in the communication server	WebAdmin in expert mode, Configuration / IP network / Image server view

Presence profiles

Presence status in the OIP:

Presence states such as Available, Busy or Absent are specified states which provide information on the current presence and availability of an OIP user. A user's own presence status is indicated, for example, in the Mitel OfficeSuite phone window.

Presence profiles can be defined via the OIP applications.

Synchronization with communication server and Outlook

The OIP presence states are synchronized with the presence state in the communication server. If OIP is connected to a Microsoft Exchange Server or if Mitel OfficeSuite is connected to a local Outlook, OIP also synchronizes the presence states with Outlook if required. For this, two settings are available at the user level. The table below shows the synchronization responses based on these settings.

Table 6.1:Settings for synchronizing the presence states

A	B	Exchange/ localOutlook		OIP application (e. g. Mitel OfficeSuite)				Communication server
☐		Outlook	⟺	Calender	✗	OIPusers [1]	⟺	Internal users[2]
☑	☐	Outlook	⟺	Calender	⇨	OIP users	⟺	Internal users
☑	☑	Outlook	⟺	Calender	⟺	OIP users	⟺	Internal users
		Calendar-based				User-based		

1. e.g. display of the presence states in the Mitel OfficeSuite phone window or in the presence indicator
2. display of the presence states on the phone or to the calling party

Table 6.2:Legend explanation: (Sheet 1 of 2)

A	Outlook to communication server setting
B	Communication server to Outlook setting
⟺	Presence states are syncronised on both sides.
☐	Presence states are not syncronised.

Table 6.2:Legend explanation: (Continued) (Sheet 2 of 2)

⇨	Presence states are syncronised unilaterally from Calendar to user. Non-matching states are overwritten by the Calendar

The synchronization interface with Outlook is located between the user-based and the calendar-based presence states. This means that in non-synchronized operations the Calendar may indicate a different presence state to the one set with the user.

Example:

Configuration with Exchange connection; synchronization is deactivated. The user manages his appointments with Outlook and the Mitel OfficeSuite Calendar. The user has entered an appointment in Outlook and the presence status is Occupied (the term used in the Mitel OfficeSuite calender is Busy). This means the user's presence state is not coupled and may have a completely different value or be set differently.

Available presence states

OIP has more presence statuses than Outlook; some of the designations used are also different. The table below shows how the terms are assigned:

Table 6.3:Designation and assignment of presence states in Outlook, OIP / Mitel OfficeSuite and PBX

Outlook		OIP (notvisible)		Mitel OfficeSuite		Communication server
Absent	⇔	*Absent*	⇔	*Absent*	⇔	*Absent*
Absent	⇦	*Meeting*	⇔	*Meeting*	⇔	Meeting
Absent	⇦	*Unknown*	⇔	*Unknown*		Previous status is retained
Withreservations	⇔	*Available*	⇔	*Available*	⇔	*vailable*A
Busy / Occupied	⇔	*Busy*	⇔	*Busy*	⇔	*Busy*
Free	⇔	*Available*	⇔	*Available*	⇔	*Available*

Table 6.4:Legend (Sheet 1 of 2)

⇔	Presence states are exchanged (where syncronised).

Table 6.4:Legend (Continued) (Sheet 2 of 2)

	There is no equivalent in Outlook for the OIP presence states. The presence state entered is assigned instead(where syncronised).

Setting the presence states

The presence states can be set by different instances (manually on the Mitel Office- Suite or on the phone, using a synchronized calendar, by the OIP presence profiles or by the OIP I/O Manager). There are no priorities between the instances and an instance will in each case overwrite the current state.

Terminating a meeting prematurely

A user has the possibility of resetting the end time for an ongoing meeting appointment to the current time by switching the presence status on his phone manually to Available. This also applies to serial appointments, in which case only the end time of the current appointment is reset.

Example:

Configuration with Exchange connection; synchronization is activated. The user manages his appointments with Outlook and the Mitel OfficeSuite Calendar. A user returns sooner than expected from a meeting which in his calendar is scheduled to run until 10:30. His phone indicates the Busy presence status. At 10:04 he switches the state to Available. As a result the end time for the appointment entry in Outlook is set to 10:04.

Using presence profiles

You have two possibilities for working with presence profiles and therefore for influencing routing for example:

- With the presence profiles in the communication server you can store a CFU under each presence state, assign a personal call routing to each presence state and select the voice mail welcome text.
- The presence profiles in the communication server are activated and deactivated by the user-based presence state.
- With the help of license-based OIP presence profiles you can set up a comprehensive presence management that allows you not only to control the routing but also other actuators (such as lighting installations or actuating motors for operating blinds or windows). You can also compile adaptable and far-reaching notification rules.
- The OIP presence profiles have two interfaces for the presence states. OIP presence profiles can set the user-based presence state; they can also be activated and deactivated by the calendar-based presence status using the profile switch. Further information is available in *"Presence profiles"*

The presence profiles of the communication server and the OIP presence profiles are independent of other running features. Decide which ones you want to use and avoid using both. If both presence profiles are activated nonetheless, only the presence profile of the communication server is taken into account.

Nested and Private calendar entries

If there are nested calendar inputs in Outlook, OIP takes over the presence status ac- cording to the following order of priority: Absent, Tentative, Busy.

Calendar entries in Outlook with a Free presence status are used in the same way as other calendar entries. If a calendar entry in Outlook is also marked as Private, the subject text will not be displayed in the OIP calendar.

It is also possible to activate and deactivate presence profiles automatically based on the current pres- ence state.

Presence profiles can be assigned to all OIP users. However they work first and fore- most with OIP users with an assigned user as calls are never routed to an OIP user, but always to an user.

Defining and activating presence profiles

Presence profiles can be defined via the OIP applications.

No presence profiles are available in the standard configuration. For users to define and use presence profiles, you must activate the Presence Profile license.

Exactly one presence profile is always active for each user. If a profile is already active when a presence profile is activated, the active profile is deactivated.

There are several possibilities for activating a presence profile:

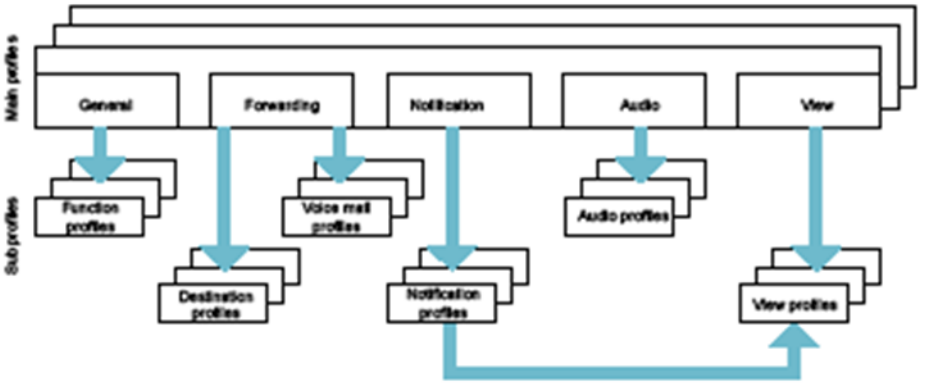
- The user activates the required presence profile manually via his OIP application or via OIP WebAdmin (User list, Active Presence profiles).
- The user manually activates the presence profile he wants, using a preconfigured key (Redkey func- tion) on his system phone.
- A presence profile is activated from the profile switch, depending on the presence status (see under **"Profile switch", Page 116**).

Activating a presence profile applies all the settings stored under that profile.

General profile features and sub-profiles

Function, notification, voice mail and display profiles are all subprofiles allocated to a presence profile.

Figure 6.1: Presence profiles and allocated subprofiles



General profile features

The General profile features contain information about the profile, regulates the profile availability, the presence status and the allocation of the function profiles which are activated when the profile is activated/deactivated.

Table 6.5:General profile features (Sheet 1 of 2)

Parameter	Description
Name	Profile title
Owner	Indicates the name of the OIP user who created the profile.
Profile availability	• A private profile is available only to its owner. • A public profile is available to all OIP users. • The template of a profile acts as a copy template when creating a profile. The template itself cannot be used directly as a profile and therefore cannot be activated.
Deactivation locked for profile switch	The profile can only be deactivated manually and not using the profile switch (see *"Profile switch"*).
Presencestatus	Sets the required presence state when the profile is activated.
Absencereason	Displayed in a precise indicator (e.g. on the Mitel OfficeSuite or an OIP operator application).
Message	Displayed in a precise indicator (e.g. on the Mitel OfficeSuite or an OIP operator application).

Table 6.5:General profile features (Continued) (Sheet 2 of 2)

Parameter	Description
City	Displayed in a precise indicator (e.g. on the Mitel OfficeSuite or an OIP operator application).
Functionprofiles	see *"Functions sub-profile"*
• *On profile activation*	The selected function profile is activated when the presence profile is activated.
• *On profile deactivation*	The selected function profile is activated when the presence profile is deactivated.

Functions sub-profile

A Functions sub-profile contains one or more predefined communication server functions. When the sub-profile is activated, the functions are either activated or deactivated in the sorting order. Some functions require a number of additional arguments for their execution.

Call forwarding sub-profile

A Call forwarding sub-profile contains call forwarding settings for each call forwarding type.

Table 6.6:Call forwarding sub-profile settings

Parameter	Description
Use call forwarding settings	This call forwarding is also activated/deactivated whenever the presence profile is activated/deactivated. If there is not check mark, the settings are ignored and the call forwarding is not activated/deactivated.
Internal calls	Activates the call forwarding configuration for internal calls.
External calls	Activates the call forwarding configuration for external calls.

Parameter	Description
Force settings of the profile	Prevents other instances from altering the call forwarding settings specified here as long as this presence profile is activated. Other instances include: User interaction via the system phone or a softphone, call forwarding destinations of the Presence Indicator, the Mitel OfficeSuite or a softphone, default call forwarding destinations defined in the communication server.
Call forwarding type	Selecting the call forwarding type.
Call number	Destination number for the call forwarding. You can only enter the destination number if a destination profile has not yet been assigned. The call number specified creates a destination profile which is assigned automatically.
Destinationprofile	Call forwarding to the destination stored in the destination profile (see *"Managing destinations"*).

Notification sub-profile

A Notification sub-profile records whether a certain event is to be notified, and if so, how. To this end, the various events are assigned information destinations. For example you can specify that an e-mail message is to be generated if a call goes unanswered.

Table 6.7:General notification sub-profile settings

Parameter	Description
Notificationprofile	Assigning a notification profile.
Force profile settings	Prevents other instances from altering the settings specified by the selected notification profile as long as this presence profile is activated. Other instances include: I/O events, settings in the Presence Indicator.
External calls	Activates the call forwarding configuration for external calls.

Managing events

You can create new notification event profiles or edit existing ones, provided the profile availability allows you to do so.

Table 6.8:Manage events (Notification sub-profile)

Parameter	Description
Name	Event name
Availability	Availability of the notification event profiles: • Private: Available only to its owner. • Public: Available to all OIP users. • System: Is created by an OIP service and cannot as a rule be mod- ified.
Event	Selecting the event type
Unansweredcalls:	The event is an unanswered call
• *from all call numbers*	The event is true for all unanswered calls
• *Call number*	The event is true for an unanswered call with the specified call number
Answeredcalls:	The event is an answered call
• *from all call numbers*	The event is true for all answered calls
• *Call number*	The event is true for an answered call with the call number specified
Textmessages:	
• *All text messages*	The event is a text message
• *to the current user*	The event is true for all text messages. The event is true for the current user.
Calender:	The event is a calendar entry
• *All calendar entries*	The event is true for all calendar entries.
• *Entry type*	The event is true for the selected type of calendar entry.
• *Presencestatus*	The event is true for the selected presence state
I/O event:	The event is an I/O event
• *All I/O events*	The event is true for any I/O event.
• *Parameter*	

Managing destinations

You can create new notification destination profiles or edit existing ones, providing the profile availability allows you to do so.

Table 6.9:Manage destinations (Notification sub-profile) (Sheet 1 of 2)

Parameter	Description
Name	Destination name
Availability	Availability of the notification destination profiles: • Private: Available only to its owner. • Public: Available to all OIP users. • System: Is created by an OIP service and cannot as a rule be mod- ified.
Visibility	The notification is made with the chosen information content.
Anruf:	The event is notified with a call:
• *to the current user*	• The destination for the call is the current user.
• *Call number*	• The call destination is the user whose call number is specified.
Fax:	The event is notified with a fax:
• *to the current user*	• The destination for the fax is the current user.
• *Call number*	• The destination for the fax is the user whose call number is speci- fied.
• *Priority*	• The indication on the terminal is made in accordance with the chosen priority. The priority settings are part of the display profile, see**"Presence profiles", Page 108.**
Textmessage:	The notification is made by means of a text message on the terminal:
• *to the current user*	• The destination for the text message is the current user.
• *Callnumber*	• The destination for the text message is the user whose call number is specified.

Table 6.9:Manage destinations (Notification sub-profile) (Continued) (Sheet 2 of 2)

Parameter	Description
MessageWaiting:	Notification on the terminal using the Message Waiting function:
• *to the current user*	• Message Waiting is activated on the terminal of the current user.
• *Callnumber*	• Message Waiting is activated on the terminal of the selected user.
Printer:	Notification by means of a hard-copy printout on a printer:
• *Printer name*	• The printout is made on the selected printer.

Audio sub-profile

A subject text sub-profile specifies the ring type on the terminal and the volume of the open-listening speaker and handset speaker.

Table 6.10:Audio sub-profile settings

Parameter	Description
Audio profile	Assigning an audio profile.

Display sub-profile

A Display sub-profile specifies how an event should be displayed on a terminal depending on its priority.

Table 6.11:General display sub-profile settings

Parameter	Description
Displayprofile	Assigning a display profile.
Force profile settings	Prevents other instances from altering the settings specified by the selected display profile as long as this presence profile is activated. Other instances include: I/O events, settings in the Presence Indicator.

Table 6.12:Display sub-profile settings

Parameter	Description
Name	Name of the display profile
Availability	Availability of display profiles: • Private: Available only to its owner. • Public: Available to all OIP users. • System: Is created by an OIP service and cannot as a rule be modified.
Priority:	Specify here the priority with which the display is to be made on the terminal.
• Signalling settings (Volume, Speed, Melody, Vibra, Ring time, Repeat time, LED, Beep)	You can specify your own signalling settings for each priority.

Profile switch

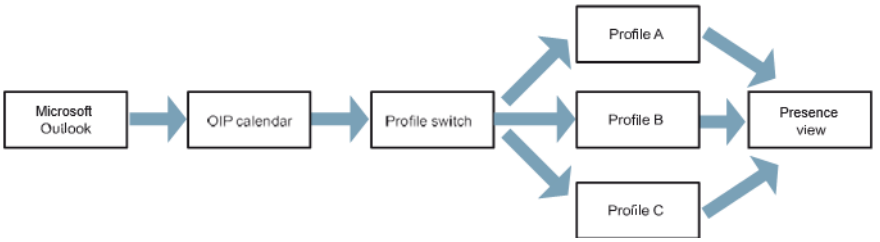
The profile switch is used to activate and deactivate presence profiles depending on the presence state of the OIP calendar. If the OIP calendar is connected to Microsoft Outlook, the presence profiles are switched depending on the Outlook presence state.

Example:

Microsoft Outlook sets the presence state to Busy based on the calendar entry. The profile switch deactivates the current profile and activates the presence profile assigned to the Busy presence status.

Each OIP user has one profile switch at his disposal.

Figure 6.2: Activating a profile based on the OIP calendar presence state



Setting up the profile switch

To set up the profile switch, proceed as follows.

1. Set up a presence profile for each presence status used, as indicated under "Defin**ing and activating presence profiles", Page 110.**
2. In the navigation tree right-click the OIP user and select Profile switch. The Profile switch window appears.
3. Assign one of the newly created profiles to each of the presence states.

4. Save the settings and close the Profile switch window.

Table 6.13:Settings for automatic profile activation

Parameter	Parameter value	Description
Presencestatus:		Presence state of the OIP calendar.
• *Avail-able/Meeting/Busy/Notav ailable/Absent*	<Profile>	The current presence state activates the assigned presence profile.
Applicationevent:		<..>
• *On login*	<..>	<..>
• *On logout*	<..>	<..>

Table 6.14:Linking of the presence states of different instances using the profile switch (Sheet 1 of 2)

Microsoft Exchange		OIPCalendar		Presence Profiles		Presence Indicator
Linking rules for the presence states of different instances:						
Exchangesta tus	⇔	Calendar Status	↙	Profile Status	⇨	Profile Status
Exchangesta tus	⇔	Calendar Status	↙	<blank>	⇨	Calendar Status
Linking rules for specific presence states:						
Free	⇔	Available	↙	Available	⇨	Available
Absent)	⇔	Unknown		<No profile can be switched with this sta- tus>		<Status profile of the cur-rently active profile>
Absent)	⇦	Meeting	↙	Meeting	⇨	Meeting
Booked	⇦	Busy	↙	Busy	⇨	Busy
Withreserva tions	⇔	Not available	↙	Not available	⇨	Not available

Table 6.14:Linking of the presence states of different instances using the profile switch (Continued) (Sheet 2 of 2)

Microsoft Exchange		OIPCalendar		Presence Profiles		Presence Indicator
Absent	⇔	Absent	⇜	Absent	⇨	Absent
Linking rules for specific subject texts:						
Exchangesubject	⇔	Calendarsubject	⇜	Profile subject	⇨	Profile subject
Exchangesubject	⇔	Calendarsubject	⇜	<blank>		Calendarsubject
Linking rules for specific location texts:						
Exchangelocation	⇔	Calendarlocation	⇜	Profile location	⇨	Profile location
Exchangelocation	⇔	Calendarlocation	⇜	<blank>		Calendarlocation

Table 6.15:Legend

⇔	The presence state of the OIP calendar is firmly coupled with the presence state of Microsoft Outlook, providing that Microsoft Outlook is syncronised.
⇦	There is no equivalent in Microsoft Exchange for the OIP calendar’s presence status. The presence status Absent is assigned during synchronisation.
⇜	The presence state of the OIP calendar determines the presence profile using the profile switch. A presence state is configured in the presence profile.
⇨	When a presence profile is activated, its presence state is forwarded to the presence indicator. It can however also be overwritten by a different instance (see also "Presence status in the OIP:", Page 108).

OIP Applications

Mitel OfficeSuite (Rich Client)

The Mitel OfficeSuite has a broad functional scope and covers a wide range of applications. As a personal cockpit it can be used not just as an added-features phone with direct access to external directories and groupware such as Microsoft Outlook. The user also has the possibility of using presence profiles to configure his personal and presence-related call routing and to obtain individual notifications of events he wishes to be kept informed of.

Installation Requirements

Microsoft .Net Framework must already be installed on the PC before the Mitel OfficeSuite can be installed. If applicable, the installation can be made from the OIP WebAdmin installation view.

To install the Mitel OfficeSuite, you have to have local administrator rights.

MiVoice 5300 series digital system phones and Mitel 600 DECT series DECT system phones can be used as media devices.

Installation Instructions

Start the installation via the OIP WebAdmin Installations view. To install Mitel Office- Suite, proceed as follows:

1. On the computer on which you wish to install Mitel OfficeSuite open a browser and log on to the OIP WebAdmin of your OIP server.
2. Navigate to the installation view and load the installation file on the PC, by clicking the *Mitel Office-Suite* installation link.
3. Start the downloaded setup file by double-clicking on it and follow the instructions given in the installation procedure.

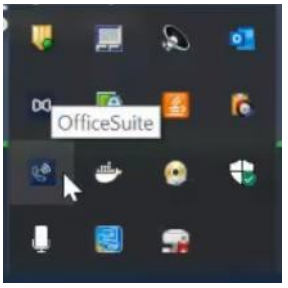
Mitel OfficeSuite is uninstalled using Control Panel \ Software in the Windows operating system.

Mitel OfficeSuite configure

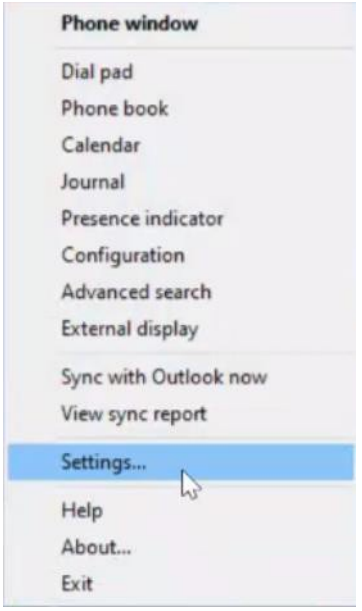
Once you have started the Mitel OfficeSuite you can carry out the configuration using the Mitel OfficeSuite icon in the info area of the taskbar. Open the context menu and click Settings.

For OIP on SMBC, you must configure the right port in the application. Follow the steps to configure the right port:

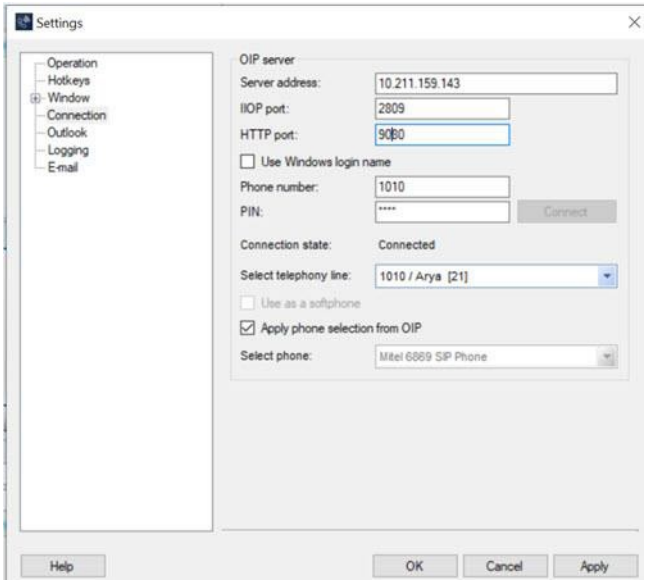
1. Open Mitel OfficeSuite application.
2. Right click OfficeSuite tray icon.



3. Click **Settings…** A new settings window opens.



4. Click **Application settings**. A new settings window opens.
5. Enter IP of the OIP server as the **Server address**.
6. Enter **9080** as the **HTTP port**.



7. Click **Apply** to save the setting.

Local Outlook connection

You can also synchronize Mitel OfficeSuite with a local Outlook installation. You will need a *Local Outlook Connector* license. This license enables the synchronization interface between Mitel OfficeSuite and Outlook. The OIP Name Server is not automatically activated in the process.

Without an active OIP Name server private Outlook contacts are directly synchronized with the communication server directory. The maximum number of contacts which can be managed that way depends on the communication server: 350 OIP contacts at most. With an active OIP Name server contacts are synchronized via the OIP directory and more contacts can be managed.

You can activate the OIP name server by activating a *Phonebook Connector* or a *Microsoft Exchange Connector* license.

OIP operator applications

The OIP application MiVoice 1560 PC Operator is a PC-based operator console. Two versions are available. The IP version (MiVoice 1560 IP) is a fully fledged IP softphone with integrated media, the other version operates as Rich Client together with a system phone.

General

Information on use and restrictions

OIP operator applications are available for MiVoice Office 400 communication systems only.

For each OIP operator application, one of the *MiVoice 1560*, *MiVoice 1560 IP* licenses must be available.

MiVoice 1560 PC Operator cannot be operated simultaneously on the same PC with an Mitel OfficeSuite CTI Rich Client or an MiVoice 2380 IP IP softphone.

Mitel SIP phones, digital MiVoice 5300 series system phones and Mitel 600 DECT series DECT system phones can be used as CTI Rich Client Version media devices (MiVoice 1560) (see *"Setting up a cordless phone as an operator console"*).

The system phone of an MiVoice 1560 CTI Rich Client used as a media device must not be configured as a key telephone. It must also not be configured as an operator phone in an operator group (see *"Working with operator groups"*).

Any PC on which the MiVoice 1560 IP softphone is to be operated must be equipped with media devices (e.g. a headset).

In an MiVoice Office 400 network one OIP PC operator console can be used across the network. The only requirement is that all the network's communication servers are connected to the same OIP server.

NOTE: Deactivate the screensaver on computers with an installed MiVoice 1560 PC Operator: The operation of an MiVoice 1560 PC Operator on a computer with an activated screensaver can lead to unexpected behaviour when displaying an incoming call.

Working with operator groups

You can group several OIP operator applications into operator groups. Operator groups have the following properties:

- In addition to the global operator number you can also specify a separate operator number for each operator group.
- Besides operator features members of operator groups also have a number of agent features at their disposal, e.g. log on, log off or break.

Information on how to set up operator groups can be found here: *"Setting up operator groups"*.

Configuring the Communication server

The configuration in the communication server specifies which users are to be set up as a PC operator console. You also specify whether an OIP operator application is used as an IP softphone or as a Rich Client.

Using an OIP operator application as a Rich Client

If set up as Rich Client, a system phone is used as a media device:

1. Open a user in WebAdmin and assign it the required phone.

   NOTE: The phone must be configured as an ordinary phone. It must not be configured as a key telephone. It must also not be configured as an operator phone in an operator group.

2. Assign the user the status of a PC operator console by setting PC operator console to Yes (WebAdmin: View User, Parameter group Multimedia).

   The user is now set up as a PC operator console and calls to the operator number will be routed through to that extension.

   You can carry out the assignment of the OIP operator application to the user later on when setting the application up on the computer.

3. Configure the user's other properties.

Using an OIP operator application as an IP softphone

In an IP softphone setup, the media is transmitted between communication server and computer via the IP network, and in the communication server the softphone is configured as an IP system phone. Proceed as follows:

1. Set up the necessary VoIP channels.
2. Open a user in the communication server and assign it an IP system phone of the type MiVoice 1560 IP.
3. Define an unobtainability destination for the user. Calls will then be routed to that destination whenever the softphone is not in operation.
4. Assign the user the status of a PC operator console by setting PC operator console to Yes (WebAdmin: View User, Parameter group Multimedia).

   The user is now set up as a PC operator console and calls to the operator number will be routed through to him.

   You can carry out the assignment of the OIP operator application to the user later on when setting the application up on the computer.
5. Configure the user's other properties.

Installing and Setting up the Operator Application

The installation is carried out regardless of whether you set up the operator application as a softphone or as a CTI Rich Client.

Installation Requirements

To be able to install an OIP operator application you must have local administrator rights.

You need to equip the computers on which the OIP operator application is to run as an IP softphone with the necessary media devices.

Acquire all the necessary licenses and update the OIP license file. *oip.lic*.

Installation Instructions

Start the installation via the OIP WebAdmin Installations view. To install MiVoice 1560 PC Operator, proceed as follows:

1. On the computer on which you wish to install MiVoice 1560 PC Operator open a browser and log on to the OIP WebAdmin of your OIP server.
2. Navigate to the installation view and load the installation file on the PC, by clicking the *MiVoice 1560 PC Operator* installation link.

3. Start the downloaded setup file by double-clicking on it and follow the instructions given in the installation procedure.

MiVoice 1560 PC Operator is installed using *Control Panel* \ *Software* in the Windows operating system.

For OIP on SMBC, you must configure the right port in the application. Follow the steps to configure the right port:

1. Open MiVoice 1560 application.
2. Click Settings icon on the task bar. A new settings window opens.

3. Click **Connection**.
4. Enter **9080** as **HTTP port**.
5. Click **Apply** to save the setting.

Setting up an operator application

Proceed as follows to set up an operator application:

1. Start the OIP operator application. The login dialog box is displayed.
2. Enter the login and connection data as indicated in the following table then click *OK*.
3. The operator application opens and attempts to establish a connection with the user.
4. If the connection to the user fails, check the advanced settings (menu **Settings...**, view **Connection**) as indicated in the following table.
5. If you are operating the operator application as an IP softphone, indicate the in- stalled output devices next and select the audio files used for signalling calls or system messages. More detailed information can be found in the operator application's Online Help.
6. The operator application is now ready for operation. The online Help contains all the information you need to operate correctly.

Table 7.1:Login dialogue box and connection parameters (Sheet 1 of 2)

Parameter	Description
Server address	Enter here the host name or IP address of the OIP server.
Windows user name	The application automatically opens with the  Windows login data. Requirement: The user's name and password in the OIP configuration must match his Windows login data.
Call number	The user logs in using his call number and PIN. 
PIN	User's phone number

Table 7.1:Login dialogue box and connection parameters (Continued) (Sheet 2 of 2)

Parameter	Description
Save PIN	PIN of the user
Advancedconnection settings:	
• Connectionstatus	Indicates the current call connection status
• Select phone line	
• Use terminal selection from OIP	The phone assignment is carried out in accordance with the settings in OIP.
• Select terminal	The phone assignment is carried out manually using the following setting.

Setting up a cordless phone as an operator console

The user wants to be able to operate the PC operator console via his cordless phone too.

You have the possibility of setting up DECT system phones that are coupled with an operator application as an operator console. You will need the *ATAS Interface* license.

To set up the DECT system phone in twin mode as an operator phone, proceed as follows:

1. In the communication server, check whether the *ATAS Interface* license is activated.
2. Activate the OIP service *Display Driver* (*Services* view).
3. Add the user to the *OPERATORS* user group (*User groups* view).
4. Assign the user the DECT system phone (user's detail view, setting *Twinpartner*) and activate automatic terminal selection (setting *automatic terminal selection*).
5. On the DECT system phone, set the ringing time, repeat time and the audio properties of the ringing signal. Calls in the queue are not signalled individually. The ring settings refer to the queue as a whole. If for example you set a 10-second ringing time and a 60-second repeat time, the user is signalled every minute that there are still calls on the queue.

The DECT system phone is now configured as an operator console.

Setting up operator groups

An operator group is a call centre application with operator consoles.

Configuration steps on the Communication server

1. In the communication server create a call distribution element with the direct dialing number and the internal call number under which the new operator group is to be reached.
2. Select ACD as the CDE destination for all switch positions.

Configuration steps on the OIP server

An operator group is a skill in the call centre configuration and the assigned agents have an operator application.

1. Check whether an operator application has been set up for the users planned to serve as agents.
2. Assign all the users the default CTI license.
3. Start the call centre management and open a new skill with the name of the new operator group.
4. Configure the skill and add the users as agents.
5. For the agents enter the direct dialing number as the Alternative number for transferring to this operator group.

Configuration steps in the operator application

1. Start the operator application and click the Operator groups symbol.
2. Configure which operator calls (Own or All) are to be signalled.
3. Open the menu Settings/Configure Signalling ... and configure the colours to be used to display the operator calls.

All the information you need to operate the operator applications correctly can be found in the Online Helps.

Setting up redundant operator groups

To ensure that operator calls can be distributed in the operator group even in the event of an OIP server failure, the operator group needs to be replicated in the form of user groups in the communication server.

For this, open the operator group skill and select a user group from the dropdown menu in the Communication server section under Use emergency routing. The following configuration is made in the communication server:

- The user group is given the same name as the operator group.
- The agents of the operator group are added to the user group as members of the group.
- The agent statuses logged on/logged out in the operator group are assigned to the members in the user group.
- A new call distribution element with the call destination on the newly set up user group is created. It is given the name “ER - <Name of the operator group>”
- (ER = Emergency Routing).

- In the operator group's call distribution element, the newly created call distribution element is entered under CDE if no answer.

OIP TAPI service provider

The OIP TAPI service provider is connected to the OIP server via Ethernet. The OIP TAPI service provider can be installed on both application servers and on workstation PCs, see *"Application Examples"*.

Installation

Installation Requirements

To install the OIP TAPI Service provider, you have to have local administrator rights.

Installation Instructions

In a MiVoice Office 400 network, the OIP TAPI service provider must be installed only once. The OIP server handles the administration of the network communication servers and, depending on the configuration of the access rights, provides all the lines to OIP TAPI service providers. Alternatively you can also install the OIP TAPI service provider on each user PC.

The OIP TAPI service provider is started with the Windows Telephony service. The AgentProxySvc Windows service for the agent functionality is also installed along with the installation of the OIP TAPI service provider.

Start the installation via the OIP WebAdmin Installations view. To install Office eDial, proceed as follows:

1. On the computer on which you wish to install the OIP TAPI service provider open a browser and log on to the OIP WebAdmin of your OIP server.
2. Navigate to the installation view and load the installation file on the PC, by clicking the *OIP* TAPI service provider installation link.
3. Start the downloaded setup file by double-clicking it then follow the instructions given in the installation procedure.
4. Configure the OIP TAPI service provider (see the section *"Connection to the OIP Server"* then finish the installation.

The OIP TAPI service provider is uninstalled using Control Panel \ Software of the Windows operating system.

Connection to the OIP Server

To connect the OIP TAPI service provider to the OIP server, proceed as follows:

1. Enter the OIP server address if it is not already automatically entered during instal- lation. Make sure you specify the DNS name or the IP address of the OIP server as the OIP server address.
2. Click Connect with Server, to set up the connection with the OIP server.

3. Log on to the OIP server.
4. Logging on to the OIP server is done via the Windows user name, via a user name configured in the OIP server, or using the internal phone number with the terminal PIN, see *"Login to OIP WebAdmin"*.

Logging on with the Windows username is dynamic. This means that for different Windows user names one's own TSP user profile can be saved. Depending on which Windows username the PC is logged on, the corresponding TSP user profile is loaded.

Logging on via a username configured in the OIP server or using the internal phone number with the terminal PIN is a fixed setting. This means that the configured TSP user profile is always loaded independently of the Windows username.

Customized Settings

Available Lines

User-specific settings are made in the User profile tab:

1. Select the type of logon and enter the corresponding user data.
2. Click Read out lines to display the available lines.
3. If required, carry out any user-defined settings.
4. Save the configuration for the specified user in the TSP user profile by clicking Save.

If you want to save additional TSP user profiles for Windows users, repeat the steps above. This is necessary if you as the Administrator want, for example, the OIP TAPI Service provider to be available to Windows users who do not have local administrator rights.

The lines configured in the for the specified users are displayed in the logon data.

Listed next to the name and number of the lines are the terminal type and the access right to the line.

Table 7.2:Terminal types

Terminal type	Description
Digital/ *Mitel* SIP	The line is assigned to a system phone
<Systemphone>+	Set as agent
ISDN	The line is assigned an ISDN terminal
Analogue	The line is assigned an analogue terminal
Voicemail	The line is assigned an internal voice mail line
DECT GAP	The line is assigned a GAP-compatible DECT terminal

Table 7.3:Access rights to telephony lines

Access right	Description
Controlling	Full access rights to the line (controlling and monitoring)
Monitoring	Monitoring rights to the line only

Properties

At least one line has to be selected before you can modify the line settings. The Select all button can be used to select all the lines.

It is possible to configure the call number format to be displayed for incoming calls (CLIP) and connected calls (COLP).

The supported call number formats are listed in thefollowing table

Table 7.4:Call number formats

Setting	Description	Example
Keep exchangeaccess prefix	Exchange access prefix-phonenumber	0-004132655xxxx
Removeexchangeaccess prefix	Call number	004132655xxxx
Replaceexchangeaccess prefix	Exchange access prefix-phonenumber	9-004132655xxxx
Use canonical format	+Country code (area code) phone number	+41 (32) 655xxxx

There are two interaction options for calls to busy internal users. You can send a call waiting tone to a busy subscriber or you can intrude on a busy user. For both functions the user rights settings have to be configured in the communication server in each case. Microsoft TAPI does not support parallel use of these two functions. So, to call a busy internal user you can configure whether the call waiting function or the intrusion function is used.

If the user is an ACD-Agent of an external TAPI-ACD application, the Control of agent status changes on the terminal option can be used to hand over agent monitoring operation to the application. This means that each status modification made on the system phone must be confirmed by the external application.

General settings

The global settings apply to all saved TSP profiles.

Extended settings

The OIP TAPI service provider supports the use of key telephones. Whether and how the functionality is implemented depends on the CTI application. When the system phone is used, calls on the private line are disconnected when calls on the KT line are answered. You can configure that calls on the private line are automatically parked when a call is answered via the CTI application. As before, active calls on the KT line can be displayed as Connected (LINECALLSTATE_CONNECTED) or Idle (LINECALL-STATE_IDLE). Ask your application manufacturer which setting is correct for your CTI application.

The OIP TAPI service provider supports the use of Operator Consoles. Whether and how the functionality is implemented depends on the CTI application. When the system phone is used, active calls on the private line are disconnected when calls on the operator line are answered. You can configure that calls on the private line are automatically parked when a call is answered via the CTI application.

Parked calls can be signaled to the CTI application as idle or parked. This setting is dependent on the used CTI application. Ask your application manufacturer which setting is correct for your CTI application.

The signaling on the ACD queue can be set whenever the ACD functionalities of the OIP TAPI service provider are used. Ask your application manufacturer which setting is correct for your CTI application.

Debug Settings

The settings for the log files can be made here for maintenance purposes. In normal operation the debug mode should be deactivated as otherwise it affects the system's performance.

For debug output, the options Standard Debug Output and Log File must be activated. In the Log Directory field, specify the path to the log files (default setting c:\debug\).

Check that with this entry the directory is not automatically added. The folder itself has to be created separately, for example using Windows Explorer. You can also specify the maximum log file size and the number of days after which the log files are to be deleted automatically.

Two log files are created when the debug mode is activated:

- intf<mmddhhmm>.log
- tspa<mmddhhmm>.log

<mmddhhmm> stands for the month, day, hour and minute on which the log file was created.

Debug Level is used to specify the information to be logged. Normally all the options should be activated.

Automation and Alarm Systems

OIP offers the possibility of expanding the internal MiVoice Office 400 messaging and alarming interfaces into a comprehensive automation and alarm systems.

The various I/O applications are structured and configured in the I/O Manager. The I/O applications consist of one or more action trees in which the individual actions are logically linked with one another.

The OIP KNX driver is used to connect external KNX systems to OIP, see *"KNX connection"*

I/O system

The OIP I/O system is based on I/O actions. Each I/O action is a chip with inputs and outputs and a specific functional logic. Individual I/O actions can be interconnected and hierarchically linked.

The I/O actions work according to the IPO principle. They have an input part, a processing part and an output part. The logical processing of the incoming events is based on the defined actions. The results of the processing are sent on as results either to the subordinate actions or to addressed actions within the same action tree or in other action trees.

An input event may be, for instance, the character string of a redkey function configured on a system phone or a specific communication server event message. Further examples are calendar inputs which should be evaluated using some specific criteria in case of integration with a Microsoft Exchange Server or sensor data in a KNX environment.

Output events may be, for instance, a display on the system phone, an e-mail or file. In a KNX environment, output events may be directly transformed into in-house installation actions such as opening and closing blinds.

I/O Manager

The I/O Manager is used to create, modify and delete I/O actions of the OIP I/O system.

The I/O Manager is a Java application. You can open it via the *Toolbox* hyperlink on the top right side of the OIP WebAdmin user surface.

The configured actions are displayed in a tree structure on the left-hand side. To add a new action to the tree, select a higher-order action, open the context menu and click Add action. Select the new action and carry out the settings on the right-hand side.

The Details tab is used for specifying the settings of the respective action. Details about the actions types can be found in *"Automation and Alarm Systems"*.

Table 8.1:Actions details (Sheet 1 of 2)

Actions details	Description
Action ID	Unique ID assigned by the system
Action name	Action designation.

Table 8.1:Actions details (Continued) (Sheet 2 of 2)

Actions details	Description
Action type	Defined action type.
Monitoring	The actions carried out are logged and stored in the database.
Remark	Remarks relating to the action can be added here.
Data type	Each I/O action corresponds to one or more data types.
Datasubtype	Data types may contain subtypes.
Data	Current internal status of the I/O action. The Set value interface can be used to change the current internal status of the I/O action.

The *Parameter* tab is used to configure the parameter of the actions, see *"Automation and Alarm Systems"*.

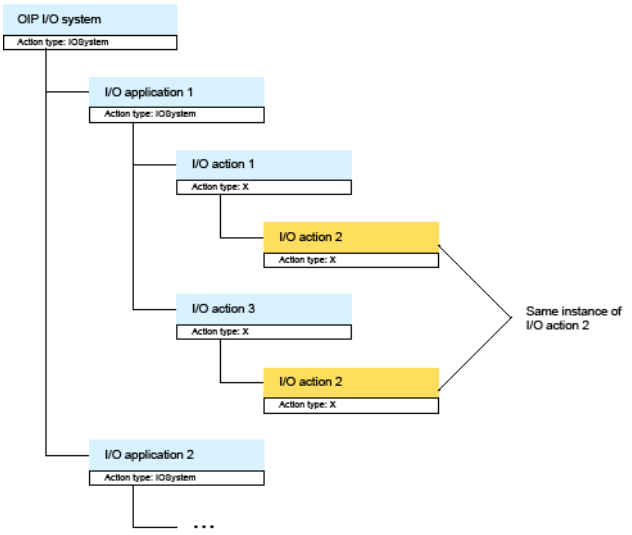
You will find a general block diagram of the action on the View tab. You can also replace this image with your own, specific image by changing the relevant image file in the image directory of the server.

To move the sequence of actions, select the action you want, open the shortcut menu and click Move Down or Move Up.

To delete an action, select the relevant action, open the context menu and click Remove action.

For a better overview and layout of the tree structure, you should start every I/O application with the action IO System under the output action. This ensures that the individual I/O applications are separated from each other and any unwanted interactions are avoided.

Figure 8.1: Layout of the I/O applications



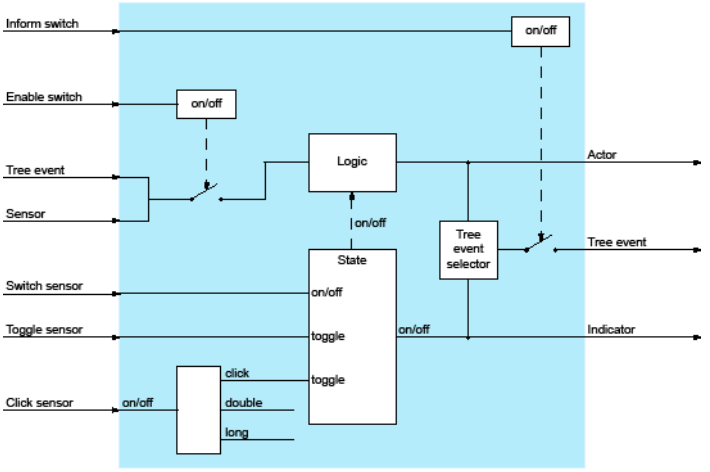
There may be several instances of one and the same action in the tree. Changes to the action need only be made once. To make another instance of the action available in the tree, select the action you want, press the <Strg>key and drag the action to the destination action you want, keeping the <Strg> key pressed down. When you delete, only the selected instance of the action is deleted.

I/O actions:

An I/O action is a logic module with various inputs and outputs. Events are processed on the inputs based on the implemented logic and configured parameters.

The following figure shows the general functional diagram of an I/O action.

Figure 8.2: Functional diagram of an I/O action



The meaning of the general inputs and outputs shown in the following figure and their parameters are identical in all the actions. They are listed in the following table. The action-specific inputs and outputs are described in the individual actions, see *"OIP I/O actions"*.

Table 8.2:General parameter of an I/O action (Sheet 1 of 3)

Parameter	Description
Owner	This parameter is not used at moment and should be left empty.
Treeevent	The Tree event is both an input and an output. The events are sent from one action to another in the action tree with the Tree event. The Tree event can send the state of the action (indicator), the result of the action (actor) or both.

Table 8.2:General parameter of an I/O action (Continued) (Sheet 2 of 3)

Parameter	Description
Tree event selector	The Tree event selector is a switch that defines which event is sent along the tree. The following settings are possible: • No event • Actor • Indicator • Actor and Indicator There is no entry corresponding to the No event setting.
Informswitch	The Inform switch is an input that operates as a switch. It switches the sending of the Tree event on or off. If the Inform switch receives a 0 (off) from the specified address, sending of the Tree event is switched off. If it receives a 1 (on), sending of the Tree event is switched on. If no address is specified, the sending of the Tree event is switched on.
Enable switch	The Enable switch is an input that operates as a switch. It switches processing of the Tree event and the Sensor on or off. If the Enable switch receives a 0 (off) from the specified address, processing of the Tree event and the Sensor is switched off. If it receives a 1 (on), processing of the Tree event and the Sensor is switched on. If no address is specified, processing of the Tree event and the Sensor is switched on.
Sensor	The Sensor is an input. It receives events with the specified address from other actions (e.g. form other action trees, from actions which are not directly above the receiving action or form external systems like KNX).
Switchsensor	The Switch sensor is an input that operates as a switch. If the Switch sensor receives a 0 (off) from the specified address, the status of the action is switched to 0 (off); if it receives a 1 (on), the status of the action is switched to 1 (on).

Table 8.2:General parameter of an I/O action (Continued) (Sheet 3 of 3)

Parameter	Description
Togglesensor	The Toggle sensor is an input that operates as a toggle switch. Irrespective of the value received from the specified address, the Toggle sensor toggles the state of the action (from 1 (on) to 0 (off) and vice versa).
Click sensor	The Click sensor is a special input for receiving multi-click events from KNX switches. The KNX switch muss send a 1 (on) if pressed and a 0 (off) if released.
Actor	The Actor is an output. It sends the result of the action to the specified address (e.g. to other action trees, to actions which are not directly below the sending action or to external systems like KNX).
Indicator	The Indicator is an output. It sends the status of the action to the specified address (e.g. to other action trees, to actions which are not directly below the sending action or to external systems like KNX).

I/O events

Data is exchanged between I/O actions or between I/O actions and sensors/actors with events. In KNX terminology, events are telegrams. I/O events are structured as follows:

Table 8.3:Constituent part of an event (Sheet 1 of 2)

Constituent part	Description
Address	The address can have a number of different formats see the *"Possible address formats"*In a tree structure, it is the action ID if no explicit address has been specified.
Data	This is the event's actual data. There are different types of data.
User ID	This is the OIP internal user ID. It is used if an event was successfully assigned to an OIP user (e.g. PBXUserCommand or PBXRedKey); if not, it is blank.

Table 8.3:Constituent part of an event (Continued) (Sheet 2 of 2)

Constituent part	Description
Monitoring	The I/O Manager can be used to set for each configured action whether the action in question should be monitored.

Addressing

Events can be sent and received via the tree structure or the direct addressing of an action.

No addresses need to be defined within the same action tree as the events are sent from the higher-level action to the subordinate action.

An address is required if events are to be sent to actions that are outside the action tree, that are not directly below the sending action or that are part of a KNX device. The same applies to receiving events.

The events sent by the actions consist of the following parts.

Table 8.4:Possible address formats (Sheet 1 of 2)

Address	Description
Freely selectable character string e.g. MYEVENT	Use the freely selectable character string to send events to actions that are not linked as subordinate actions.
Action ID	Each action has its own unique ID within the system. Use the action ID as the address if events are to be sent to a specific action. **NOTE:** Direct addressing of an action ID can result in hidden errors following a change. This address format should therefore only be used in exceptional cases.
Action type	The action type should be used if events are to be sent to a specific action type. In this case the events are sent to all the actions of the same type within the system. **NOTE:** Addressing an action type can result in hidden errors following a change. This address format should therefore only be used in exceptional cases.

Table 8.4:Possible address formats (Continued) (Sheet 2 of 2)

Address	Description
KNX group address e.g. KNX:5/3/8	Use this address format if the destination is a KNX device or multiple KNX devices. A KNX group address is like a line to which you can connect one or more KNX devices. The KNX group address can be a two-level or three-level address; three-level notation is now more common. The syntax is Ma/Mi/S, where Ma is the main group, Mi the middle group and S the subgroup. The value range of the group parts is as follows: Ma from 0 to 13, Mi from 0 to 7 and S from 0 to 255

Multiple entries of group addresses or user numbers are possible; they must be separated with ";".

The events can correspond to different types of data.

Table 8.5:Data types (Sheet 1 of 2)

Datatype	Description	DTP[1]	EIS[2]	Format	Range d=decimal/ b=binary
Switching	Switching	DPT 1	EIS 1	1 bit	(0.1)b
Dimming	Dimming (position/control/value)	DPT 3	EIS 2	1/4/8 bits	(1000...0111)b
Time	Time in the format hh:mm:ss:ms	DPT 10	EIS 3	3 bytes	
Date	Date in the format dd/mm/yyyy	DPT 11	EIS 4	2 bytes	
Value	2-byte floating point value	DPT 9	EIS 5	2 bytes	
Scaling	Relative value	DPT 5/6	EIS 6	1 byte	(0...255)d (0...100%)d (0...360°)d
DriveControl	Drive control	DPT 1	EIS 7	1 bit	(0.1)b
Priority	Force control	DPT 2	EIS 8	1/2 bit	

Table 8.5:Data types (Continued) (Sheet 2 of 2)

Datatype	Description	DTP[1]	EIS[2]	Format	Range d=decimal/ b=binary
Float	Positive or negative floating point value (IEEE 754)	DPT 14	EIS 9	4 bytes	
Counter16Bit	16-bit value	DPT 7/8	EIS 10	2 bytes	(-32768...+32767)d (0...65535)d
Counter32Bit	32-bit value	DPT 12/13	EIS 11	4 bytes	0..494967295 - 2147483648 .. 2147483647
Access	Access control	DPT 15	EIS 12	4 bytes	
Char	ASCII characters (A, B, 1, ä,etc.)	DPT 4	EIS 13	2 bytes	
Counter8Bit	8-bit value	DPT 5/6	EIS 14	1 byte	0 .. 255 -128 .. 127
String	String; can contain variables and separators	DPT 16	EIS 15	14 bytes	

1. Data point type
2. EIB Interworking Standard

The data types Char, Time, Date, Value, Scaling, Counter8Bit, Counter16Bit, Counter32Bit, Dimming, DriveControl, Priority and Access are of relevance only to the KNX extension.

If no user is specified for user-related actions (e.g. *PBXDisplay*, *PBXACDAgentState*, etc.), the event's user ID is used as default user.

In texts of the data type String, you can use variables that are then set with the corresponding value during runtime. The string data type is normally used if the result of the action (actor) is forwarded. How to use the variables correctly is detailed in each action. A list of available variables can be found here: in the following table.

A text of the data type String can be divided into a maximum of three substrings using separators. Only one separator or character combination is possible. The semicolon (;) is the standard separator. However, you can if required also use the following characters instead: a-Z, 0-9 and special characters such as ,-_:;#*. A space is not allowed and will automatically be replaced with the standard separator, the semicolon.

Table 8.6:Variables (Sheet 1 of 4)

Variable	Description
@ALARMNAME	PBX alarm name
@ALARMTYPE	PBX Alarm ID
@CALLSTATE	Call status output as value: 0 - Idle 1 - Ringing 2 - Busy 3 - Alerting 4 - Connected 5 - Conference Current date End date of the calendar entry End time of the calendar entry Address of the event
@CALLSTATENAM	Call state output as text, see description of values for the variable *@CALL- STATE*.
@DATE	Current date
@ENDDATE	End date of the calendar entry
@ENDTIME	End time of the calendar entry
@GROUP	Address of the event
@KEYID	Character string configured for the Redkey
@LF	Adds a line feed
@LOCATION	Location of the calendar entry
@MESSAGE	Message text
@NAME	Action name configured in the I/O Manager.
@NODEID	AIN node ID
@NODENAME	AIN node name
@PARAM1	PBX alarm parameter 1
@PARAM2	PBX alarm parameter 2
@PARAM3	PBX alarm parameter 3
@PARAMTITLE1	Title, PBX alarm parameter 1
@PARAMTITLE2	Title, PBX alarm parameter 2

Table 8.6:Variables (Continued) (Sheet 2 of 4)

Variable	Description
@PARAMTITLE3	Title, PBX alarm parameter 3
@PARAMTEXT	Data field of the event as text. With the string data type, it's the text; with the switching data type, it's on or off.
@PARAMVALUE	Data field of the event as value. With the string data type, it's the text; with the switching data type, it's 1 or 0
@PBXID	OIP PBX ID
PBXNAME	OIP PBX name
@PRESENCENAME	Presence state output as text, see description of values for the variable @PRESENCESTATE.
@PRESENCESTATE	Presence state output as value: 0 - Unknown 1 - Available 2 - Meeting 3 - Busy 4 - Not available 5 - Absent
@SENDERID	User ID of the sender of a message
@SENDERNAME	User name of the sender of a message
@SENDERNUMBER	User number of the sender of a message
@STARTDATE	Start date of the calendar entry
@STARTTIME	Start time of the calendar entry
@STATE	State of the action as value (0/1).
@STATENAME	State of the action as text (on/off).
@SUBJECT	Text in the subject line of a calendar entry or subject line of an e-mail.
@SUBSCRIBERID	User ID
@SUBSCRIBERNAME	User name
@SUBSCRIBERNUMBER	User number

Table 8.6:Variables (Continued) (Sheet 3 of 4)

Variable	Description
@SUBTYPETEXT	Data subtype output as text, see description of values for the variable @SUB- TYPEVALUE.
@SUBTYPEVALUE	Data subtype output as value: 0 - Unknown 1 - DimPosition 2 - DimControl 3 - DimValue 4 - CtrlMove 5 - CtrlStep 6 - PrioPosition 7- PrioControl 8 - CtrSigned 9 - CtrUnsigned
@TAB	Inserts a horizontal space
@TEXTPARAM1	First substring (from the start of the string to the first separator)
@TEXTPARAM2	Second substring (between the first and second separator)
@TEXTPARAM3	Third substring (from the second substring to the end of the string)
@TIME	Current time
@TYPETEXT	Data type output as text, see description of values for the variable *@TYPE- VALUE*.

Table 8.6:Variables (Continued) (Sheet 4 of 4)

Variable	Description
@TYPEVALUE	Data type output as value: 0 - Unknown 1 - Switching 2 - Dimming 3 - Time 4 - Date 5 - Value 6 - Scaling 7 - DriveControl 8 - Priority 9 - FloatValue 10 - CounterValue16Bit 11 - CounterValue32Bit 12 - Access 13 - Char 14 - CounterValue8Bit 15 - String

There are also special variables that contain certain functions or which can retrieve detailed information by means of identification.

Table 8.7:Special variables (Sheet 1 of 2)

Variable	Description
@EMPTY	Forwards a blank string.
@OFF	Corresponds to value 0.
@ON	Corresponds to value 1.
@PARTNERNAME	Caller's name, if known.
@PARTNERNUMBER	Caller's CLIP, if transmitted.

Table 8.7:Special variables (Continued) (Sheet 2 of 2)

Variable	Description
@PARTNERTYPE	Type of call in relation to the caller: 0 - Unknown 1 - internal 2 - external 3 - CDE 4 - CDE/DDI 5 - UG 6 - CFU 7 - CFNR 8 - CFB 9 - DND 10 - CFU Text 11 - CFU Pager 12 - CFNR Pager 13 - Follow Me 14 - deflected 15 - Pick up 16 - CFU first 17 - Call transferred 18 - Firm 19 - Dialled number 20 - Operator
@SUBSTRINGx	Contains the embedded substring from the higher-order string.

If a blank string is sent, for instance to clear a terminal display through an action of the type PBXDisplay, the variable *@EMPTY* must be used.

With the variables *@ON* and *@OFF*, it is possible to activate or deactivate an action using a string or to influence the status of an action. If, for example, the string "*@ON* 220" is sent to the action of the type *PBXPUMState*, user 220 is logged on to the terminal configured in the action.

If a substring of the string sent is to be used in a new string, the variable *@SUB- STRINGx* is used. Here x is replaced by a number from 1 to 10. In other words up to ten substrings can be transmitted. The substrings must be identified as follows in the original string: @<Substring>@. The start designator "@<" and the end designator "@>" are mandatory. *@SUBSTRING1* references the first substring in the original string, etc.

@PARTNERNUMBER, *@PARTNERNAME*, *@PARTNERTYPE* contain further information on telephone calls. They are used in actions that concern phone calls (e.g.

PBXCallState). With these variables the required partner information can be specified by adding a number.

With external calls three different information segments can be called up:

- *@PARTNERNUMBER1*: Caller CLIP

- *@PARTNERNUMBER2*: Called CDE/DDI
- *@PARTNERNUMBER3*: Redirect info

With internal calls two different information segments can be called up:

- *@PARTNERNUMBER1*: Caller CLIP
- *@PARTNERNUMBER2*: Redirect info

The same information can be accessed accordingly for the variables *@PARTNER- NAME* and *@PART-NERTYPE*.

OIP I/O actions

The following table gives an overview of the OIP I/O actions.

The availability of the actions on the various platforms is listed in columns [A] to [C]:

- MiVoice Office 400 = column [A]

Table 8.8:List of OIP I/O Actions (Sheet 1 of 2)

Symbol	Action	Description	[A]	License
	Area	The Area action is used to group different geographic areas (e.g. premises, buildings, storeys or individual rooms). The events entered are sent on to all the sub-actions. Events can also be forwarded recursively to specific types of sub-actions.	X	
	AstroCalendar	The AstroCalendar action calculates sunrise and sunset times for the configured location based on astronomic calculations	X	
	Blinker	The Blinker action activates or deactivates actions depending on the time interval.	X	
	CalendarEntry	The CalendarEntry action evaluates calendar entries according to the start and end time.	X	

Table 8.8:List of OIP I/O Actions (Continued) (Sheet 2 of 2)

Symbol	Action	Description	[A]	License
	CalendarNotification	The CalendarNotification action evaluates calendar reminders.	X	
	ConfigurationProfile	The ConfigurationProfileaction is bidirectional. It is used to activate predefined presence profiles and can be triggered by presence profiles.	X	
	ConfigurationProfileDisplay	The ConfigurationProfileDisplay action is used to display and select the set presence profiles on the system phones.	X	
	EmailMessage	The EmailMessage action sends an e-mail to a defined group of recipients.	X	

Table 8.9:List of OIP I/O Actions (Sheet 1 of 11)

Symbol	Action	Description	[A]	[B]	License
	EmailTrigger	The EmailTrigger action evaluates received e-mails according to their content.	X	X	
	Enabler	The Enabler action activates or deactivates the actions directly subordinated to this action, depending on the parameters supplied.	X	X	
	Execute	The Execute action starts an external application.	X	X	
	FileWriter	The FileWriter action writes the data received to the configured I/O export data file.	X	X	

Table 8.9:List of OIP I/O Actions (Continued) (Sheet 2 of 11)

Symbol	Action	Description	[A]	[B]	License
	Filter	The Filter action compares incoming events with the configured filter criteria. If they match up, the events are forwarded.	X	X	
	FloatingValue	The FloatingValue action sends floating point numbers in accordance with the IEEE754 standard with an accuracy of 4 bytes.	X	X	
	Heartbeat	The Heartbeat action periodically sends a switch-on message to the defined I/O group.	X	X	
	Initializer	The Initializer action is activated after the configured delay once the OIP server is started.	X	X	
	Inverter	The Inverter action inverts Boolean-type input signals (true ® false or false ® true).	X	X	
	IOSystem	The IOSystemaction is a placeholder for creating new node points for a clearer overview.	X	X	
	IP Text Listenser	The IP Text Listener action evaluates text strings that are sent to a specified IP address.			

Table 8.9:List of OIP I/O Actions (Continued) (Sheet 3 of 11)

Symbol	Action	Description	[A]	[B]	License
	JabberAccount	The JabberAccount action sets up a connection to an external Jabber/XMPP-compatible instant messaging account (e.g. Google Talk). The presence status in OIP (Absent, Meeting,...) is transmitted on the instant messaging status and vice versa. Chat messages can be received as system messages.	X	X	
	LogicAND	The LogicAND action checks input signals for "AND operation" and sends the output signals for activating and deactivating actions.	X	X	
	LogicNOT	The LogicNOT action checks input signals for "NOT operation" and sends the output signals for activating and deactivating actions.	X	X	
	LogicOR	The LogicOR action checks input signals for "OR operation" and sends the output signals for activating and deactivating actions.	X	X	
	LogicXOR	The LogicXOR action checks input signals for "EXCLUSIVE-OR operation" and sends the output signals for activating and deactivating actions.	X	X	

Table 8.9:List of OIP I/O Actions (Continued) (Sheet 4 of 11)

Symbol	Action	Description	[A]	[B]	License
	MessageWaitingIndication	Dieaction MessageWaitingIndication	X	X	
	Notification	Dieaction Notification	X	X	
	ParameterSetup	The ParameterSetup action allows the properties of actions directly subordinated to it to be adapted during runtime.	X	X	
	PBXACDAgentCall	The PBXACDAgentCall action is used to trigger an action based on the agent status.	X	X	
	PBXACDAgentSkill	The PBXACDAgentSkill action changes the status (activated, deactivated) of the agent for the configured skill. If the configured agent is activated or deactivated in a Skill, the status is forwarded accordingly.	X	-	
	PBXACDAgentState	The PBXACDAgentState action sets and evaluates the status of the OIP call centre agent. If the agent status received corresponds to the configured status, the corresponding events are forwarded. If an event is received, the agent status can be set for the configured user.	X	-	

Table 8.9:List of OIP I/O Actions (Continued) (Sheet 5 of 11)

Symbol	Action	Description	[A]	[B]	License
	PBXACDSkillCalls	The PBXACDSkillCalls action monitors the number of unansweredcalls in the ACD queue for the configured skill.	X	-	
	PBXACDSkillState	The PBXACDSkillState action changes the status (open, closed) for the configured skill. If the status of the configured (open, closed) is modified, the status is forwarded accordingly.	X	-	
	PBXActiveTerminal	The PBXActiveTerminal action is used to determine the currently active phone in a One Number or parallel switch configuration.	X	X	
	PBXAlarm	The PBXAlarmactionevaluates received PBX alarms in accordance with the parameters.	X	-	
	PBXApplication	The PBXApplication action is used to define a menu which can be displayed on a system phone using the PBXApplicationMenu action.	X	X	
	PBXApplicationMenu	The PBXApplicationMenuactionis used to call up a menu defined in the PBXApplication action and to display the menu on a system phone.	X	X	

Table 8.9:List of OIP I/O Actions (Continued) (Sheet 6 of 11)

Symbol	Action	Description	[A]	[B]	License
	PBXCallDeflect	The PBXCallDeflect action evaluates the incoming CLIP and forwards the call to the specified destination.	X	X	
	PBXCallRecording	The PBXCallRecording action is for starting and stopping the recording function of a user.	X	X	
	PBXCallState	The PBXCallState action evaluates the call status of the configured users.	X	X	
	PBXChargeContact	The PBXChargeContact action evaluates the charge contact of the configured DECT handsets.	X	X	ATAS
	PBXClipSetup	The PBXClipSetup action configures the outgoing CLIP number for the configured user	X	-	
	PBXControlOutput	The PBXControlOutput action evaluates the status of the control output (relay) and can also set it.			
	PBXDectSubscriber	The PBXDectSubscriber action evaluates the location data of a DECT handset in a configured area.	X	X	ATASpro[1]
	PBXDectSystemBase	The PBXDectSystemBase action is used to display a DECT radio unit connected to the communication server.	X	X	ATAS pro[a]
	PBXDestinationState	The PBXDestinationState action sets or evaluates the CFU state of an user.	X	X	

Table 8.9:List of OIP I/O Actions (Continued) (Sheet 7 of 11)

Symbol	Action	Description	[A]	[B]	License
	PBXDisplay	The PBXDisplay action controls the display of the system phone.	X	X	ATAS
	PBXDisplayOption	The PBXDisplayOption action is responsible for displaying and evaluating the foxkeys An action of the PBXDisplayOption action type is always a subordinate action of the PBXDisplay action type.	X	X	ATAS
	PBXGreeting	The PBXGreeting activates the configured greeting.	X	X	
	PBXMacro	The PBXMacro action sends PBX macros configured in the parameters.	X	X	
	PBXMessage	The PBXMessage action sends a message to the configured users.	X	X	
	PBXMessageIndication	The PBXMessageIndication actionresponds to MWI events from the communication servern(e.g. receipt or deletion of a voice mail).	X	X	
	PBXMessageToMail	The PBXMessageToMailaction evaluates text messages that are sent over the communication server text message system to forward them as e-mails or SMS.	X	X	

Table 8.9:List of OIP I/O Actions (Continued) (Sheet 8 of 11)

Symbol	Action	Description	[A]	[B]	License
	PBXMessageTrigger	The PBXMessageTriggeraction evaluatestext messages that are sent over the communication server text message system.	X	X	
	PBXNetworkMessage	The PBXNetworkMessage action sends messages to the QSIG network.	X	0	
	PBXPresenceKey	The PBXPresenceKeyaction indicates the presence status on a configured redkey.	X	0	
	PBXPresenceState	The PBXPresenceState action evaluates the presence status of the configured user. The presence status can also be set.	X	-	
PUM	PBXPUMState	The PBXPUMState action sets and evaluates the PUM status of the configured user.	X	-	ATAS
	PBXRedKey	ThePBXRedKeyactionevaluatesthereceived character string stored on a programmed red key, and sends Boolean-type output signals to the addressed actions.	X	X	
	PBXRedKeyLED	The PBXRedKeyLED action controls the LED for the configured redkey function on the system phone.	X	X	ATAS

Table 8.9:List of OIP I/O Actions (Continued) (Sheet 9 of 11)

Symbol	Action	Description	[A]	[B]	License
	PBXSubscriber	The PBXSubscriber action forwards the status (on/off) of a configured PBX user.. The status might be a particular call status or a new voicemail. The status can be used for the chart display.	X	X	
	PBXSwitchGroup	The PBXSwitchGroup action sets and evaluates the status of the switch position (day,night, weekend).	X	-	
	PBXTeamCall	The PBXTeamCall action allows the configuration of teams. All the team members see on the display of the system phone the calls made to the team members and can use the foxkey to fetch the calls.	X	X	ATAS
	PBXTeamKey	The PBXTeamKey action simulates a team key that is available in the QSIG network.	X	-	
	PBXTerminalEvent	The PBXTerminalEvent action evaluates safeguard alarms from the DECT cordless phones.	X	X	ATAS[a]
	PBXTimeCall	The PBXTimeCall action is used to generate a time alarm call in the case of one or moreusers.	X	X	
	PBXUserCommand[a]	The PBXUserCommand action evaluates alarms sent via the *77xxxx# function code.	X	-	

Table 8.9:List of OIP I/O Actions (Continued) (Sheet 10 of 11)

Symbol	Action	Description	[A]	[B]	License
	PBXUserGroup	The PBXUserGroup action sets and evaluates the status of the configured users in the user group.	X	X	
	PBXVoiceMa[a]	The PBXVoiceMail action responds to voice mails received by the configured user.	X	-	
	RandomSwitch	The RandomSwitch action activates or deactivates the status of any subordinated actions randomly in the configured time interval.	X	X	
	Routing	The Routing action is used to change the dynamic routing of calls in the Routing Manager.	X	X	
	RSSNews	The RSSNews action indicates messages in RSS file format on the display of the system phone.	X	X	ATAS
	ScalingValue	The ScalingValue action sends a configured floating point number to a configured I/O group.	X	X	
	Sequence	The Sequence action activates the subordinated actions in sequence.	X	X	
	SmallFloatValue	The SmallFloatValue action sends floating point numbers in accordance with the IEEE754 standard with an accuracy of 2 bytes.	X	X	
	State	The action State action indicates the status of the action.	X	X	

Table 8.9:List of OIP I/O Actions (Continued) (Sheet 11 of 11)

Symbol	Action	Description	[A]	[B]	License
	StringFilter	The StringFilter action compares messages received with the configured filter criteria. If they match, the configured text is forwarded.	X	X	
	StringTrigger	The StringTrigger action evaluates messages received according to their content.	X	X	
	StringValue	The StringValue action sends configured character strings to the corresponding actions.	X	X	
	Switching	The Switching action receives and sends events depending on the internal status of the action.	X	X	
	SwitchingValue	The SwitchingValue action sends Boolean type values if events are received.	X	X	
	Timeout	The Timeout action delays the sending of output signals.	X	X	
	TimerSwitch	The TimerSwitchaction is a timer switch that activates or deactivates the addressed actions at specific times.	X	X	
	WebPage	The WebPage action is used to display a website in the Mitel OfficeSuite of the user who is logged in. Application example: Webcam view of a door intercom	X	X	

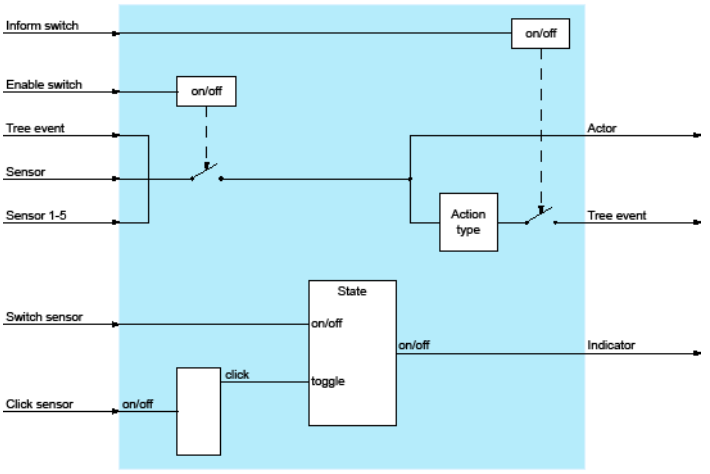
1. For OpenCom 1000 the license is ATAS Gateway pro

Area

The *Area* action is used to group different geographic areas (e.g. premises, buildings, storeys or individual rooms). The events entered are sent on to all the sub-actions.

Events can also be forwarded recursively to specific types of sub-actions.

Figure 8.3: I/O Action Area



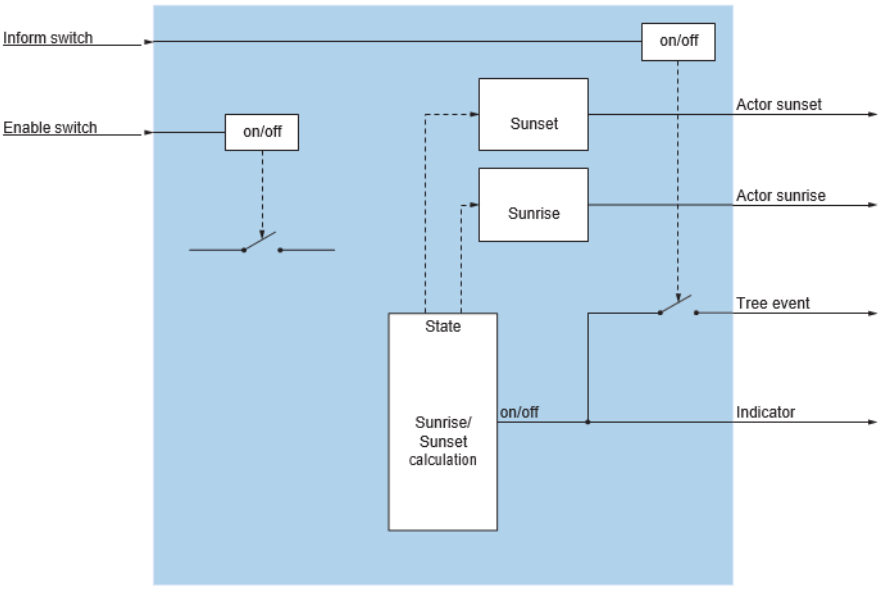
Example:

All the lights on a particular storey should be switched off using a configured Redkey on the system phone.

AstroCalendar

The *AstroCalendar* action calculates sunrise and sunset times for the configured location based on astronomic calculations

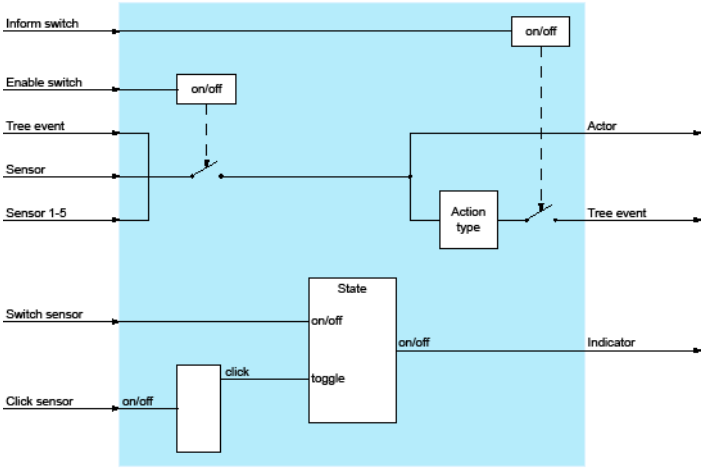
Figure 8.4: I/O Action AstroCalendar



Blinker

The *Blinker* action activates or deactivates actions depending on the time interval.

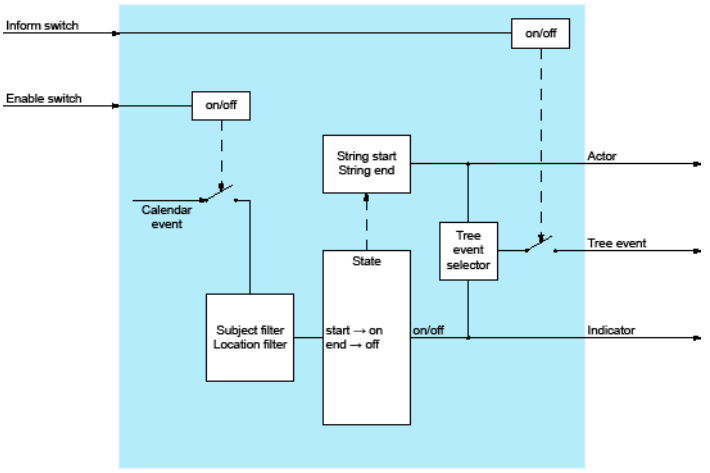
Figure 8.5: I/O Action Blinker



CalendarEntry

The *CalendarEntry* action evaluates calendar entries according to the start and end time.

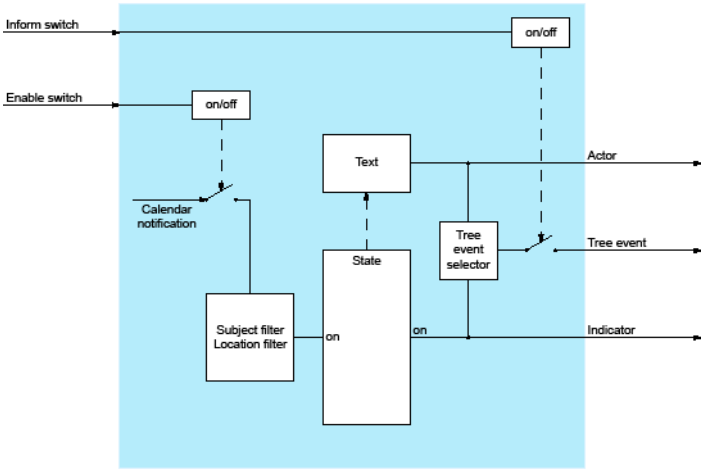
Figure 8.6: I/O Action CalendarEntry



CalendarNotification

The *CalendarNotification* action evaluates calendar reminders.

Figure 8.7: I/O Action CalendarNotification



Example:

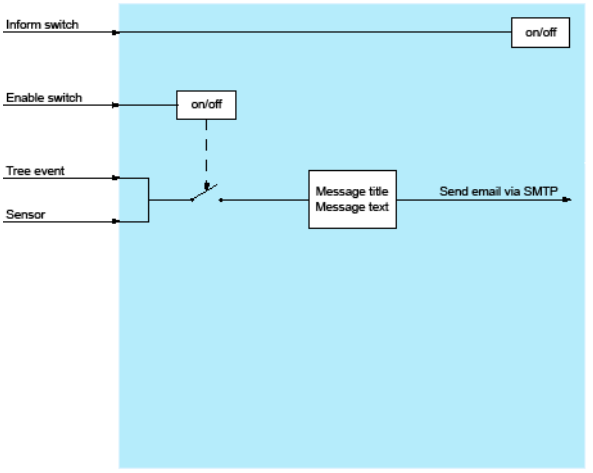
Using a specific calendar entry the system phone can automatically be forwarded to a configured destination and presence status set accordingly.

EmailMessage

The *EmailMessage* action sends an e-mail to a defined group of recipients.

For the *EmailMessage* action, the installation component *Connection to an SMTP mail server* must be selected and configured during installation of the OIP server.

Figure 8.8: I/O Action EmailMessage

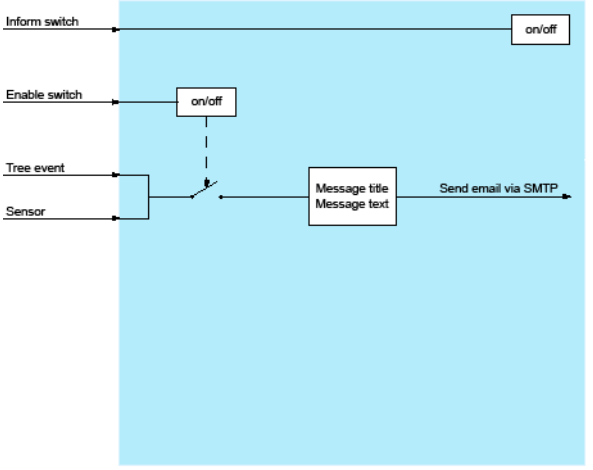


EmailTrigger

The *EmailTrigger* action evaluates received e-mails according to their content.

The analysis of received e-mails is available only with the connection to a Microsoft Exchange server the user's mailbox must also be configured in the user profile.

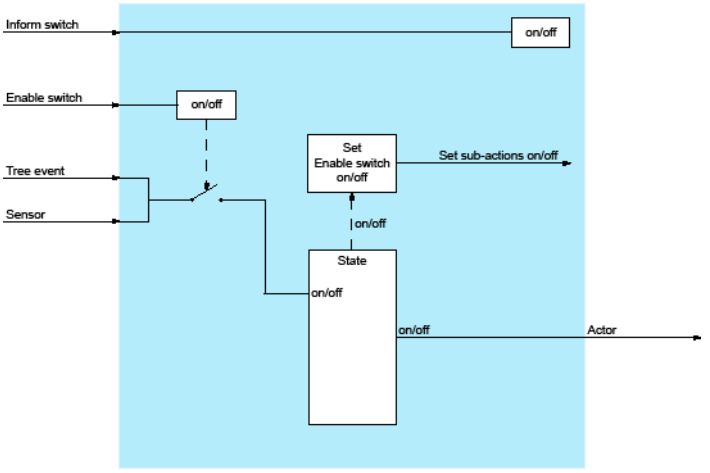
Figure 8.9: I/O Action EmailTrigger



Enabler

The *Enabler* action activates or deactivates the actions directly subordinated to this action, depending on the parameters supplied.

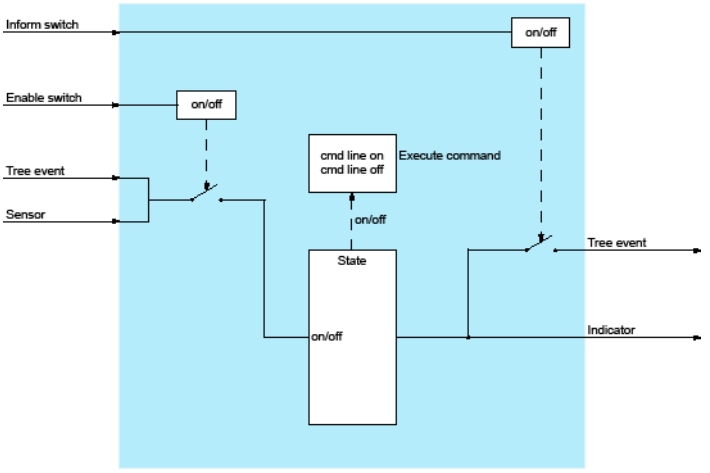
Figure 8.10: I/O Action Enabler



Execute

The *Execute* action starts an external application.

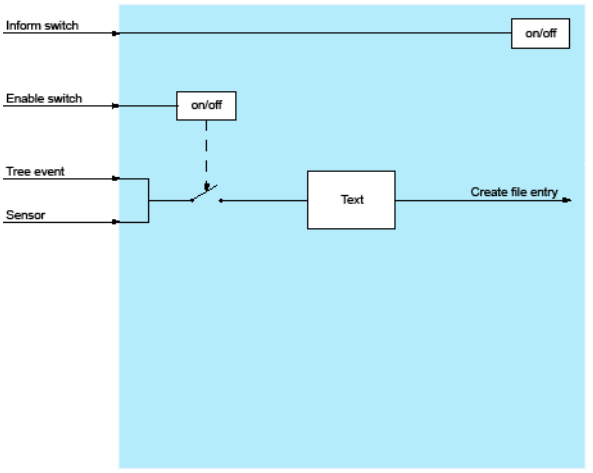
Figure 8.11: I/O Action Execute



FileWriter

The *FileWriter* action writes the data received to the configured I/O export data file.

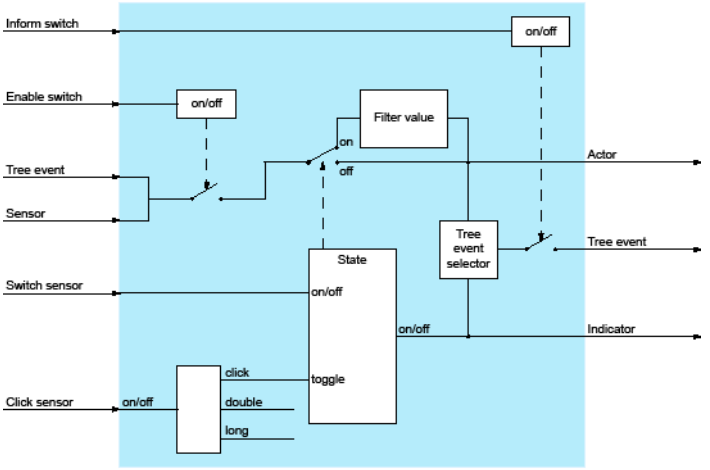
Figure 8.12: I/O Action FileWriter



Filter

The *Filter* action compares incoming events with the configured filter criteria. If they match up, the events are forwarded.

Figure 8.13: I/O Action Filter

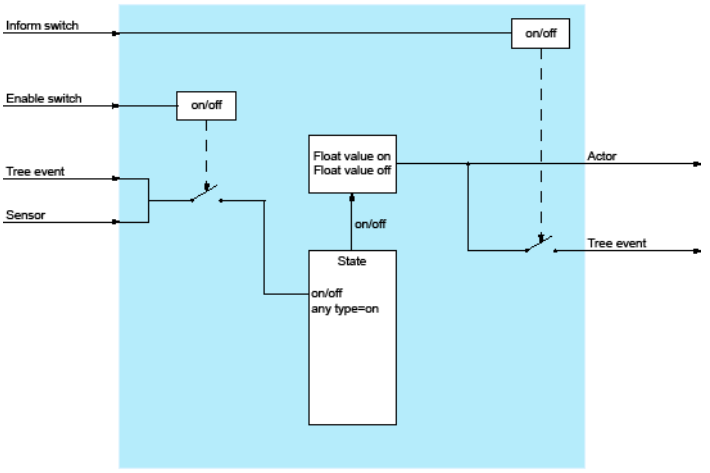


FloatingValue

0.01

The *FloatingValue* action sends floating point numbers in accordance with the IEEE754 standard with an accuracy of 4 bytes.

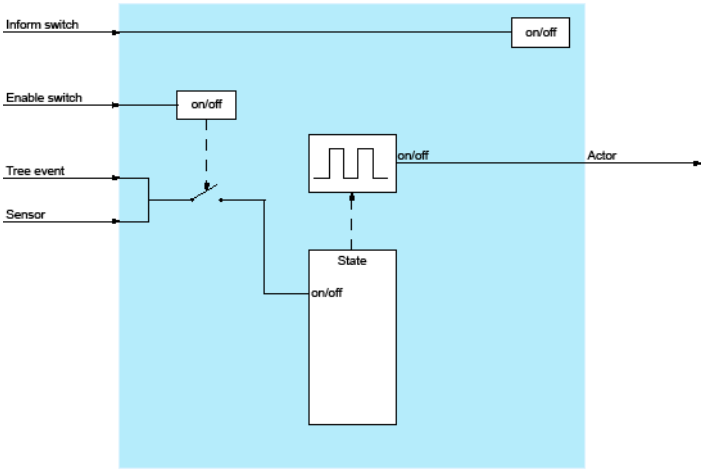
Figure 8.14: I/O Action FloatingValue



Heartbeat

The *Heartbeat* action periodically sends a switch-on message to the defined I/O group.

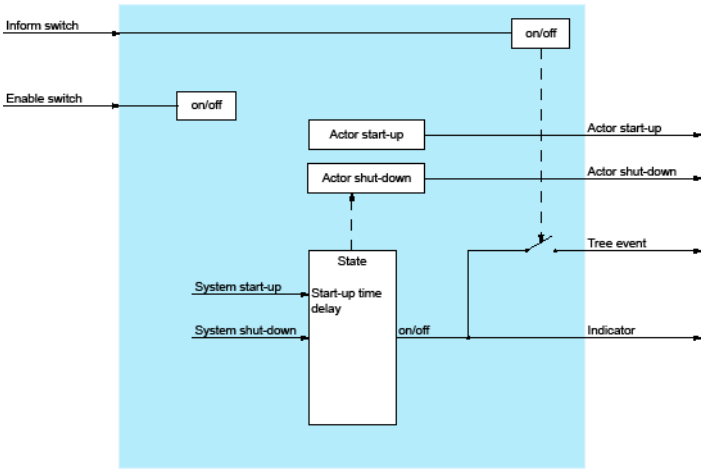
Figure 8.15: I/O Action Heartbeat



Initializer

The *Initializer* action is activated after the configured delay once the OIP server is started.

Figure 8.16: I/O Action Initializer



Inverter

The *Inverter* action inverts Boolean-type input signals (true -> false or false -> true).

IOSystem

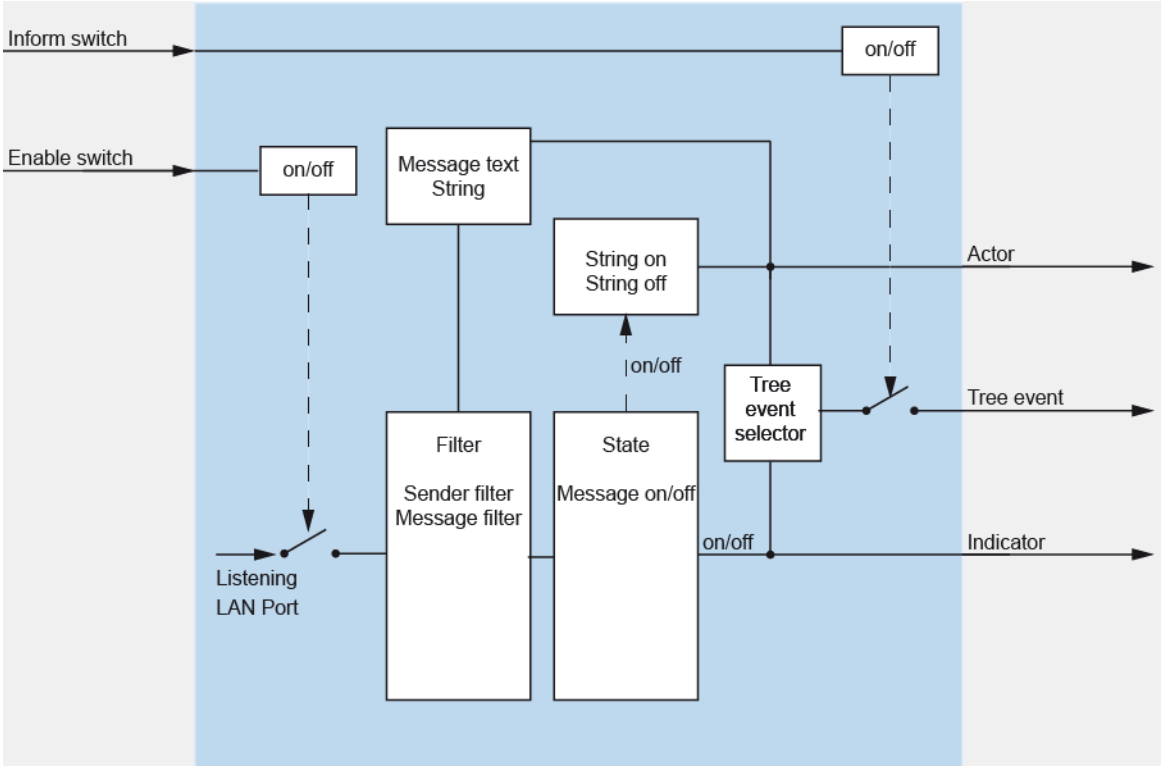
The *IOSystem* action is a placeholder for creating new node points for a clearer overview.

Events sent to the action via the tree structure or by addressing are not routed through by the action. This means that the action tree is interrupted at this point.

IP Text Listener

The *IP Text Listener* action evaluates text strings that are sent to a specified IP ad- dress.

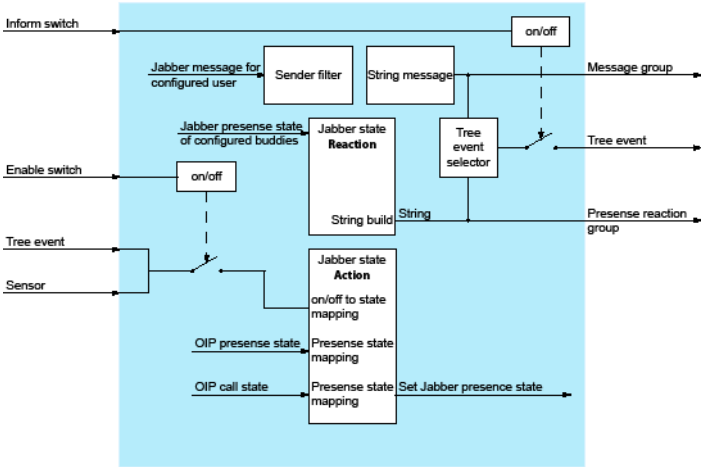
Figure 8.17: I/O Action IPTextListner



JabberAccount

The *JabberAccount* action sets up a connection to an external Jabber/XMPP-compatible instant messaging account (e.g. Google Talk). The presence status in OIP (Absent, Meeting, ...) is transmitted on the instant messaging status and vice versa. Chat messages can be received as system messages.

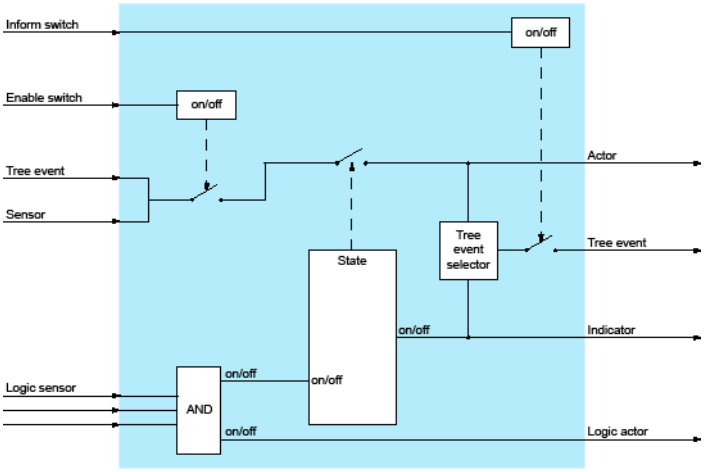
Figure 8.18: I/O Action JabberAccount



LogicAND

The *LogicAND* action checks input signals for "AND operation" and sends the output signals for activating and deactivating actions.

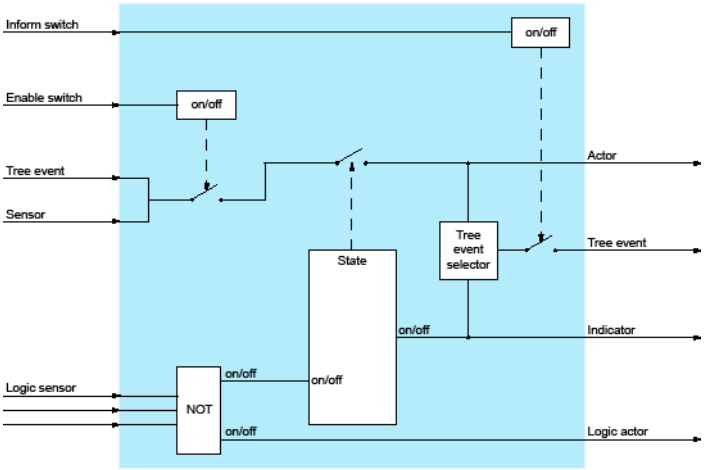
Figure 8.19: I/O Action LogicAND



LogicNOT

The *LogicNOT* action checks input signals for "NOT operation" and sends the output signals for activating and deactivating actions.

Figure 8.20: I/O Action LogicNOT

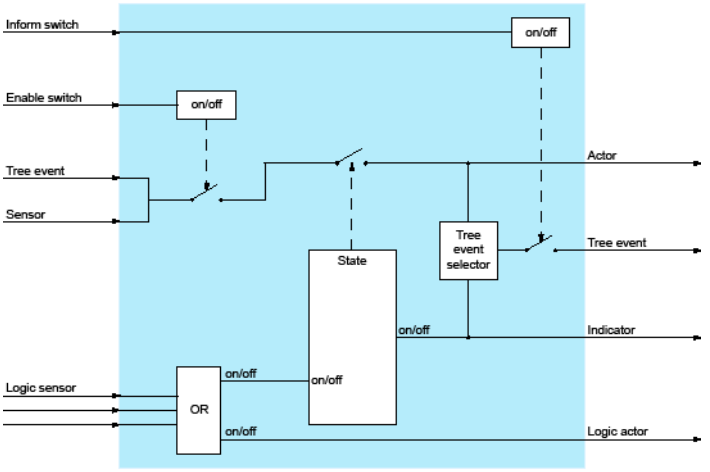


LogicOR

OR

The *LogicOR* action checks input signals for "OR operation" and sends the output signals for activating and deactivating actions.

Figure 8.21: I/O Action LogicOR

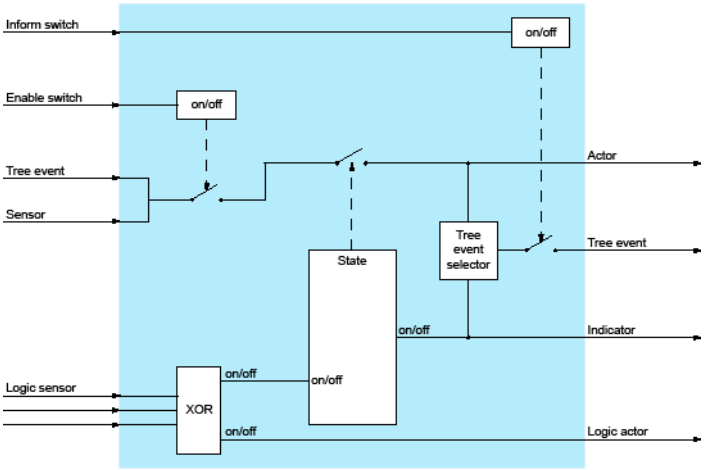


LogicXOR

X

The *LogicXOR* action checks input signals for "EXCLUSIVE-OR operation" and sends the output signals for activating and deactivating actions.

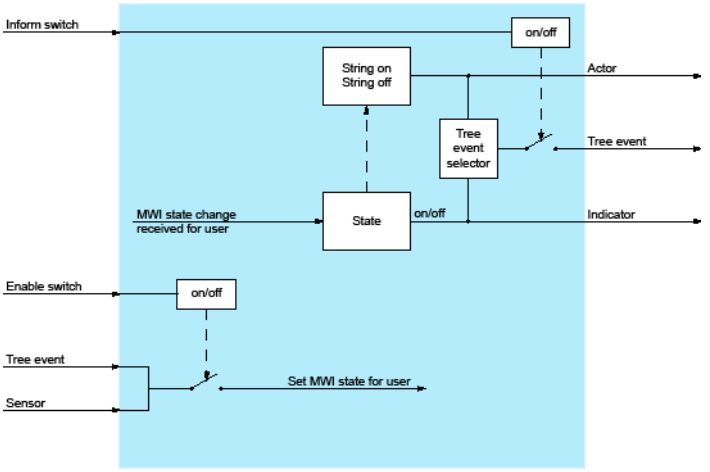
Figure 8.22: I/O Action LogicXOR



MessageWaitingIndication

The action *MessageWaitingIndication*

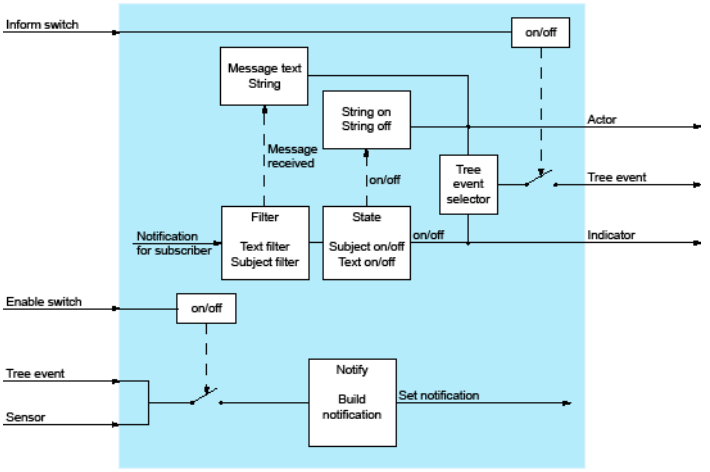
Figure 8.23: I/O Action MessageWaitingIndication



Notification

The action *Notification*

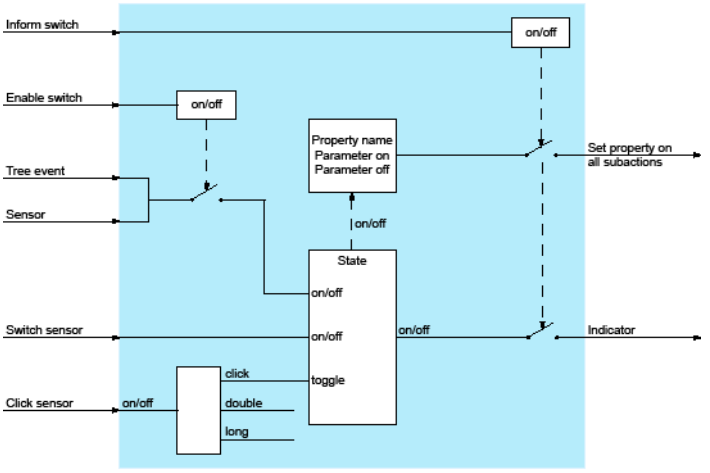
Figure 8.24: I/O Action Notification



ParameterSetup

The *ParameterSetup* action allows the properties of actions directly subordinated to it to be adapted during runtime.

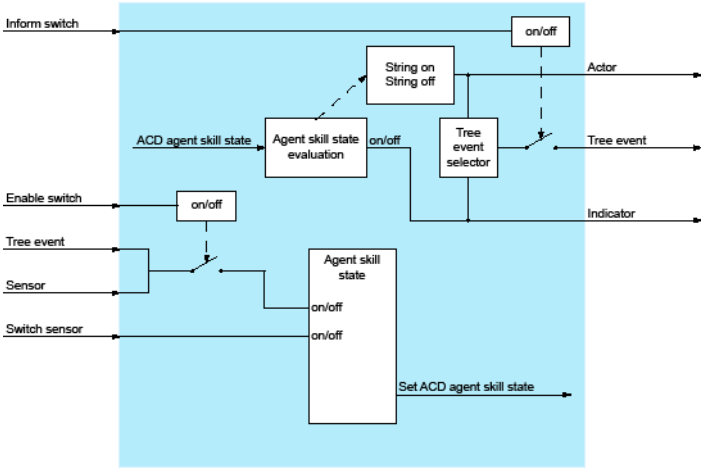
Figure 8.25: I/O Action ParameterSetup



PBXACDAgentSkill

The *PBXACDAgentSkill* action changes the status (activated, deactivated) of the agent for the configured skill. If the configured agent is activated or deactivated in a Skill, the status is forwarded accordingly.

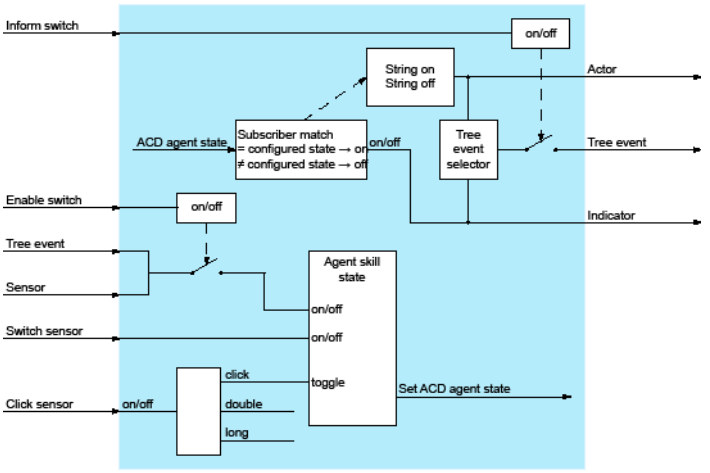
Figure 8.26: I/O Action PBXACDAgentSkill



PBXACDAgentState

The *PBXACDAgentState* action sets and evaluates the status of the OIP call centre agent. If the agent status received corresponds to the configured status, the corresponding events are forwarded. If an event is received, the agent status can be set for the configured user.

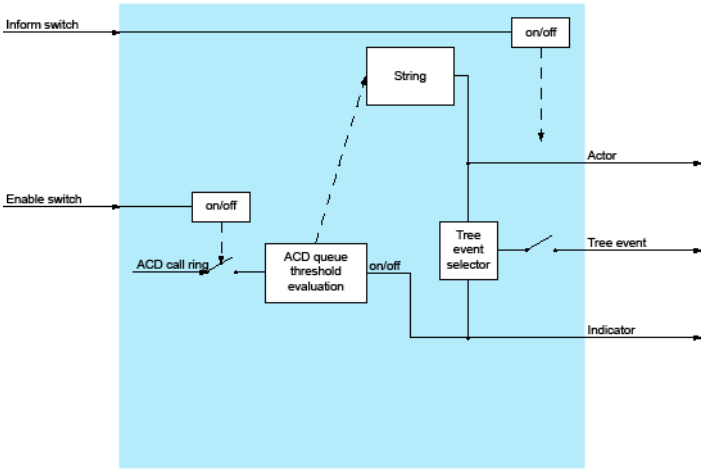
Figure 8.27: I/O Action PBXACDAgentState



PBXACDSkillCalls

The *PBXACDSkillCalls* action monitors the number of unanswered calls in the ACD queue for the configured skill.

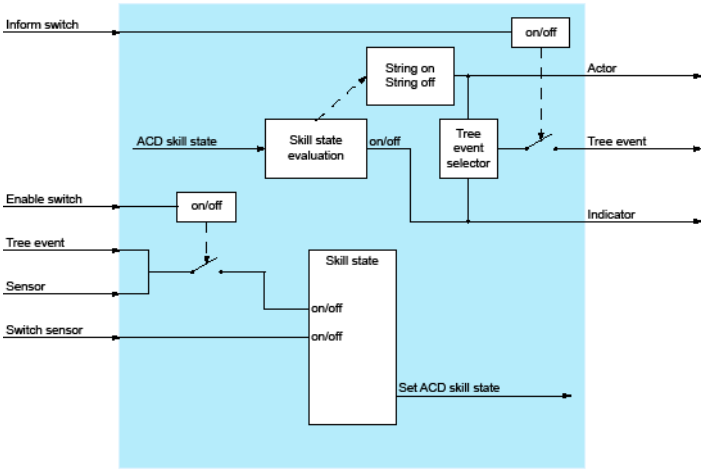
Figure 8.28: I/O Action PBXACDSkillCalls



PBXACDSkillState

The *PBXACDSkillState* action changes the status (open, closed) for the configured skill. If the status of the configured (open, closed) is modified, the status is forwarded accordingly.

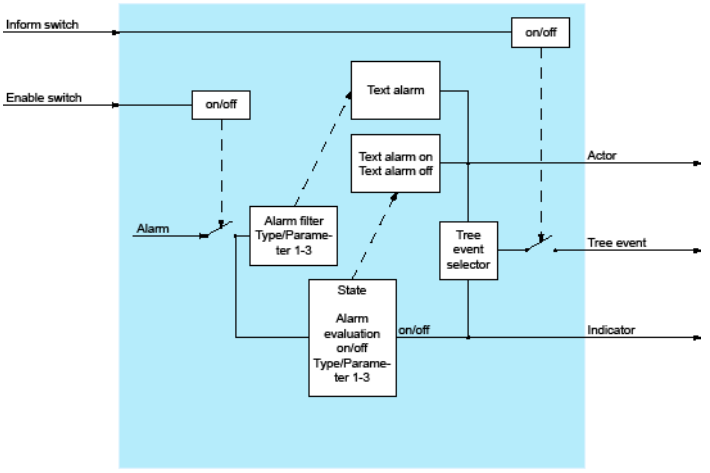
Figure 8.29: I/O Action PBXACDSkillState



PBXAlarm

The *PBXAlarm* action evaluates received PBX alarms in accordance with the parameters.

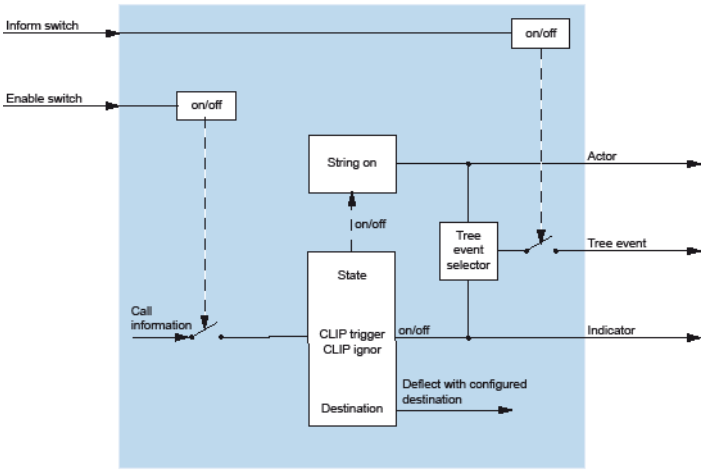
Figure 8.30: I/O Action PBXAlarm



PBXCallDeflect

The *PBXCallDeflect* action evaluates the incoming CLIP and forwards the call to the specified destination.

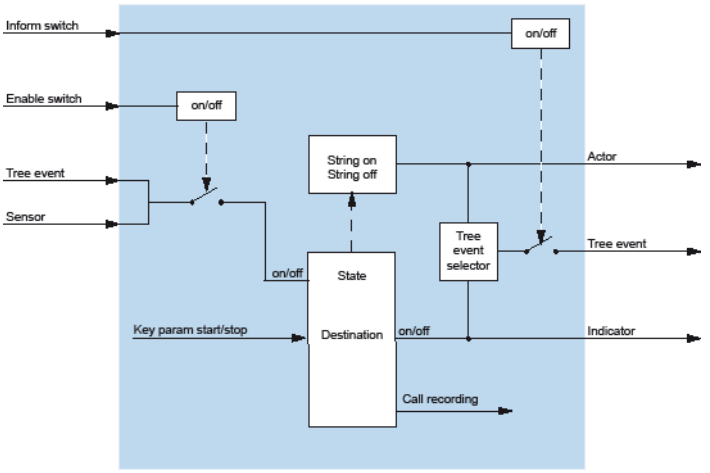
Figure 8.31: I/O Action PBXCallDeflect



PBXCallRecording

The *PBXCallRecording* action is for starting and stopping the recording function of a user.

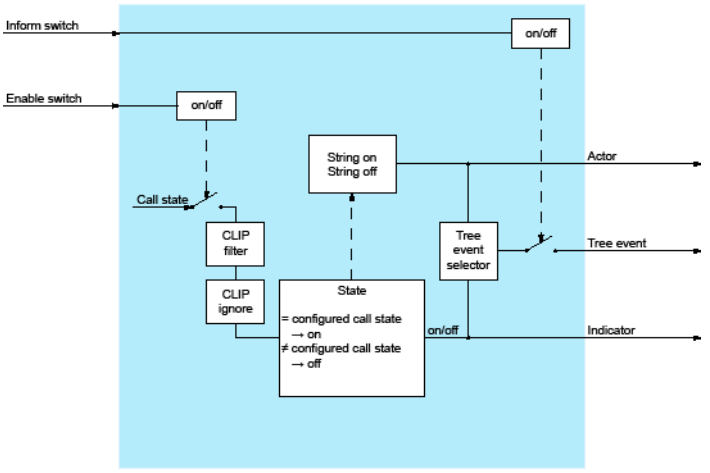
Figure 8.32: I/O Action PBXCallRecording



PBXCallState

The *PBXCallState* action evaluates the call status of the configured users.

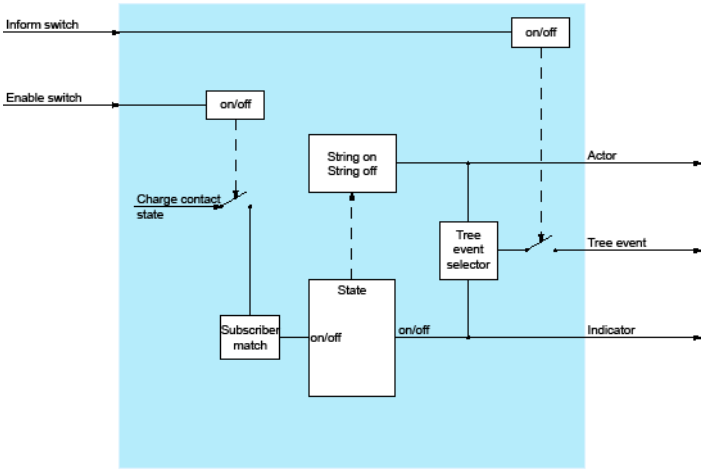
Figure 8.33: I/O Action PBXCallState



PBXChargeContact

The *PBXChargeContact* action evaluates the charge contact of the configured DECT handsets.

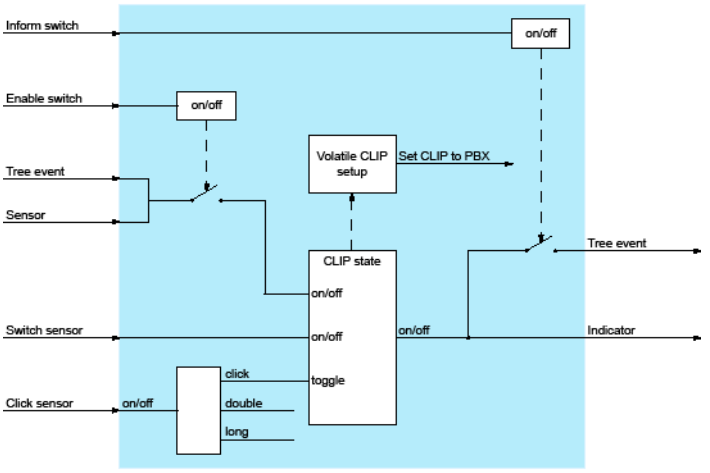
Figure 8.34: I/O Action PBXChargeContact



PBXClipSetup

The *PBXClipSetup* action configures the outgoing CLIP number for the configured user

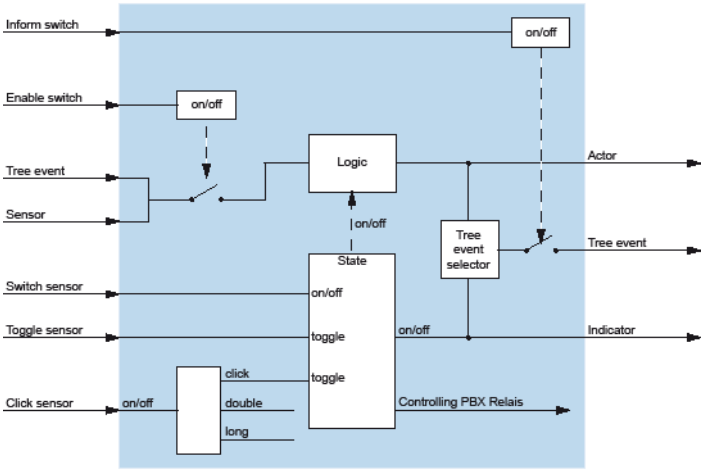
Figure 8.35: I/O Action PBXClipSetup



PBXControlOutput

The *PBXControlOutput* action evaluates the status of the control output (relay) and can also set it.

Figure 8.36: I/O Action PBXControlOutput

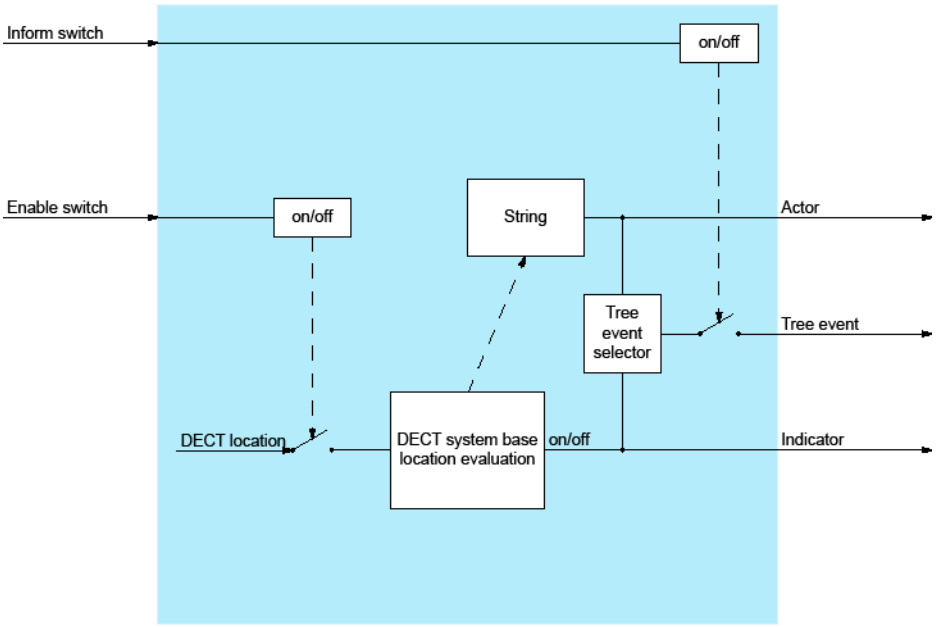


PBXDectSubscriber

The *PBXDectSubscriber* action evaluates the location data of a DECT handset in a configured area.

The PBXDectSubscriber action is available only if at least three DECT radio units are connected to the communication server.

Figure 8.37: I/O Action PBXDectSubscriber



In the interval configured in the action, the location of the DECT handset is calculated using the data from the three strongest DECT radio units. The availability of the DECT handset (e.g. DECT deactivated, outside the configured area, DECT in the charger) can also be determined and forwarded.

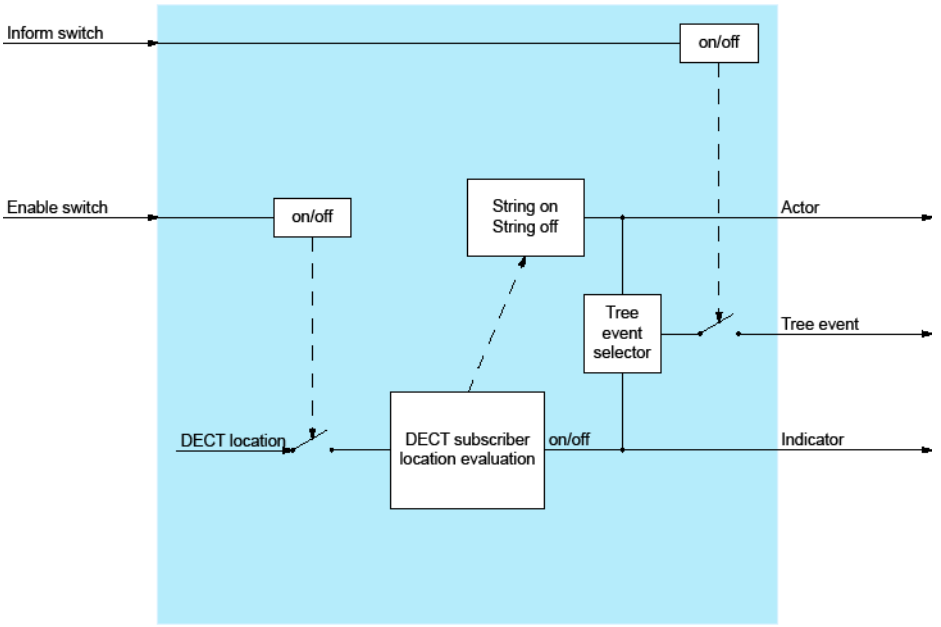
The PBXDectSubscriber action can be displayed in the chart view, see also **"DECT locating"**

PBXDectSystemBase

The *PBXDectSystemBase* action is used to display a DECT radio unit connected to the communication server.

The PBXDectSystemBase action is available only if at least three DECT radio units are connected to the communication server.

Figure 8.38: I/O Action PBXDectSystemBase



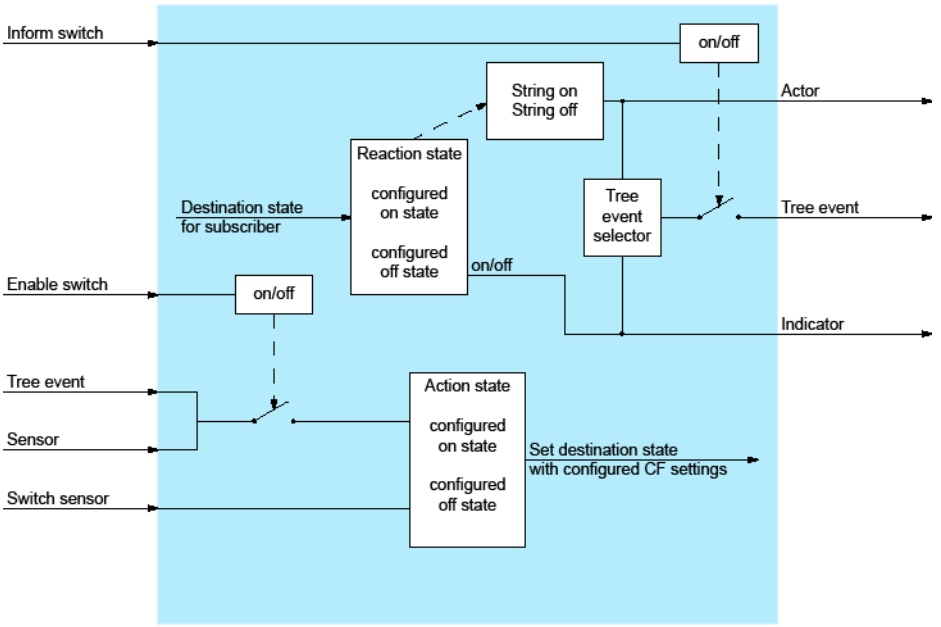
In conjunction with the DECT localization this action is shown or hidden if a configured DECT handset is located in the area of the DECT radio unit.

The PBXDectSystemBase action can be displayed in the chart view, see also **"DECT locating"**.

PBXDestinationState

The *PBXDestinationState* action sets or evaluates the CFU state of an user.

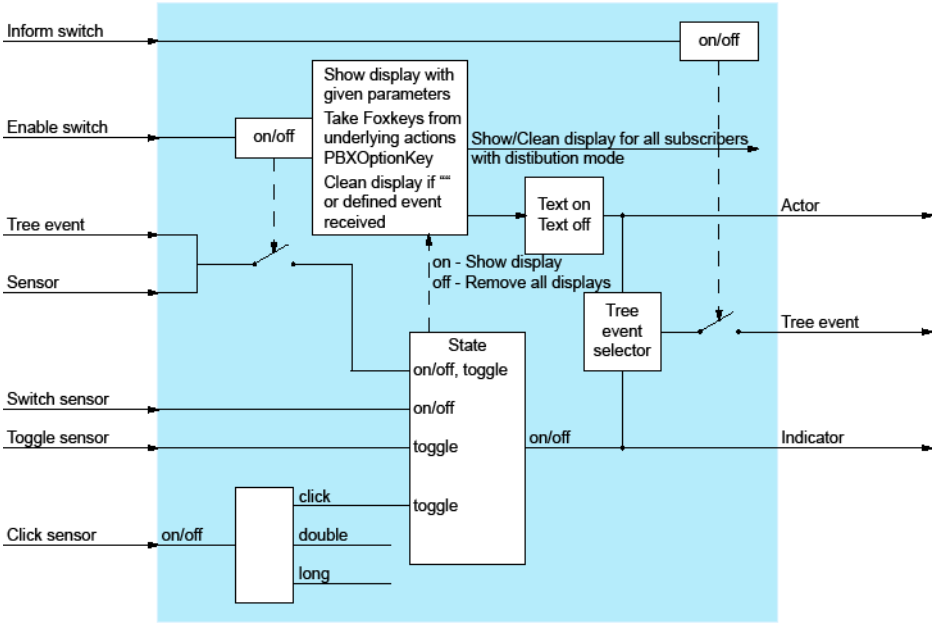
Figure 8.39: I/O Action PBXDestinationState



PBXDisplay

The *PBXDisplay* action controls the display of the system phone.

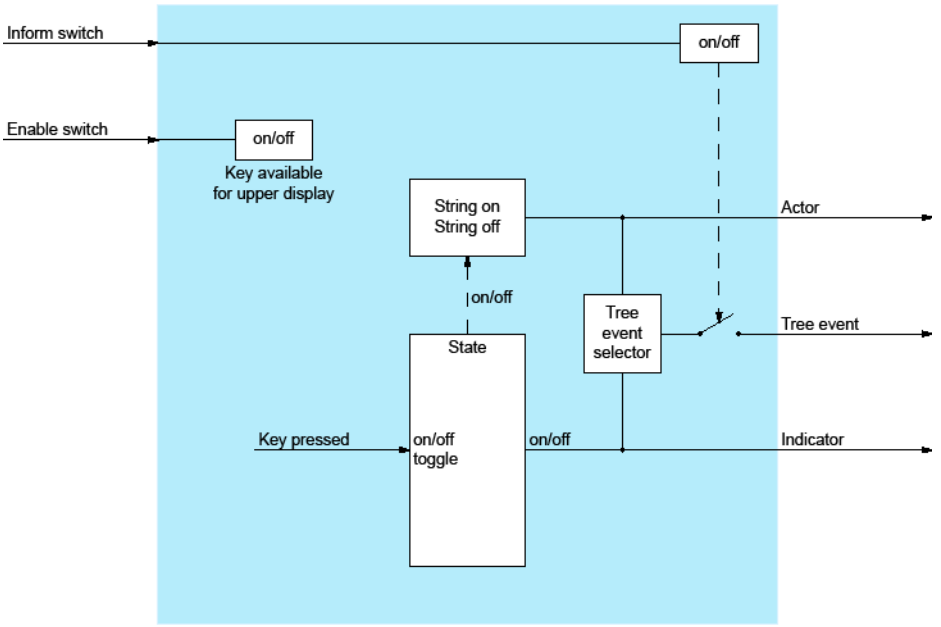
Figure 8.40: I/O Action PBXDisplay



PBXDisplayOption

The *PBXDisplayOption* action is responsible for displaying and evaluating the foxkeys An action of the PBXDisplayOption action type is always a subordinate action of the *PBXDisplay* action type.

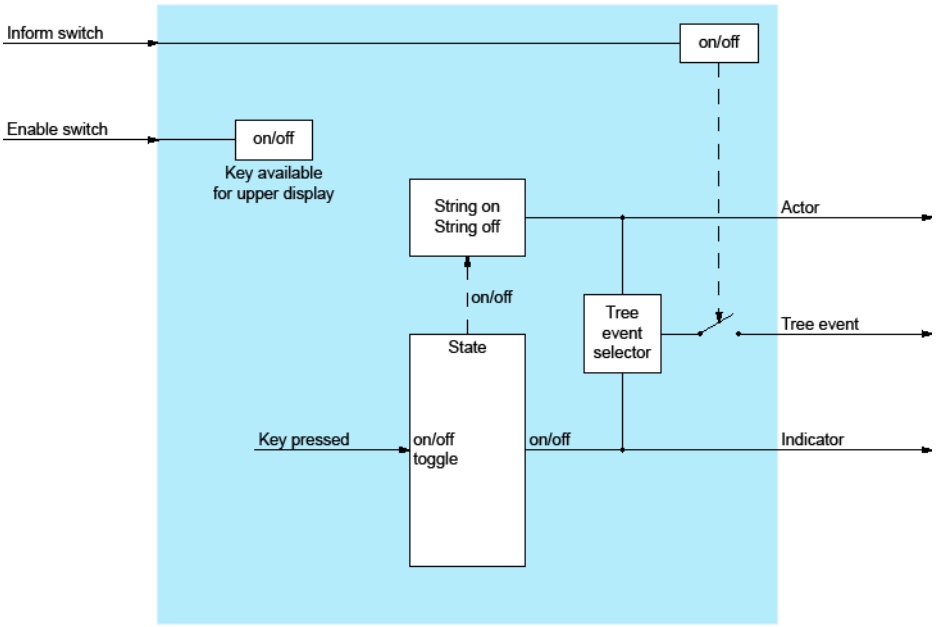
Figure 8.41: I/O Action PBXDisplayOption



PBXMacro

The *PBXMacro* action sends PBX macros configured in the parameters.

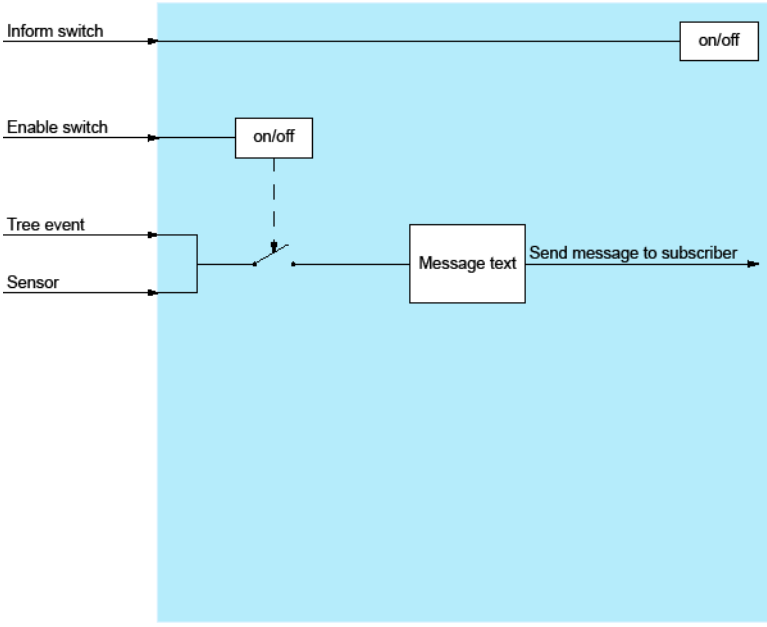
Figure 8.42: I/O Action PBXMacro



PBXMessage

The *PBXMessage* action sends a message to the configured users.

Figure 8.43: I/O Action PBXMessage

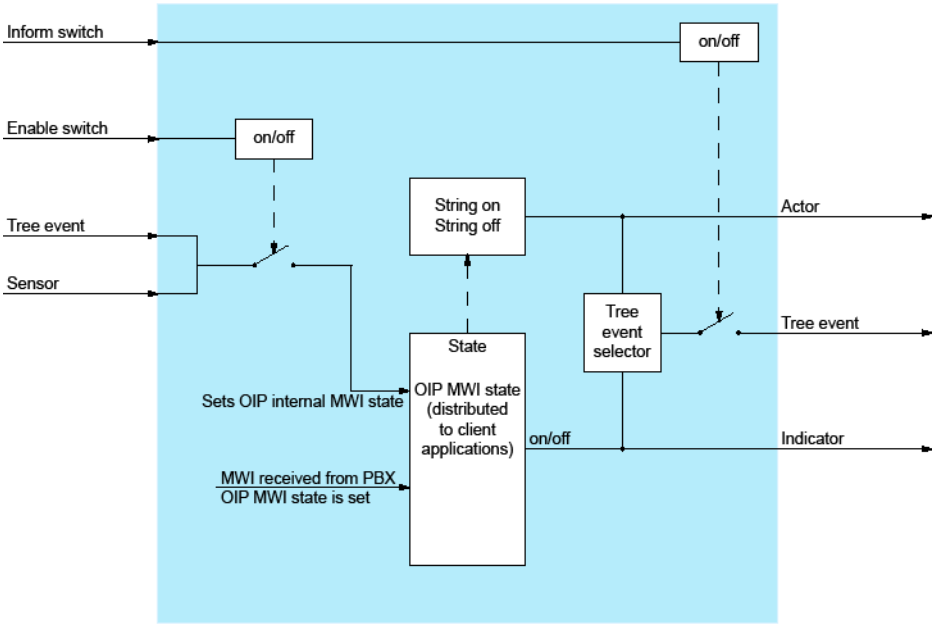


PBXMessageIndication

The *PBXMessageIndication* action responds to MWI events from the communication server (e.g. receipt or deletion of a voice mail).

The OIP internal MWI status can be set based on the events received and forwarded accordingly.

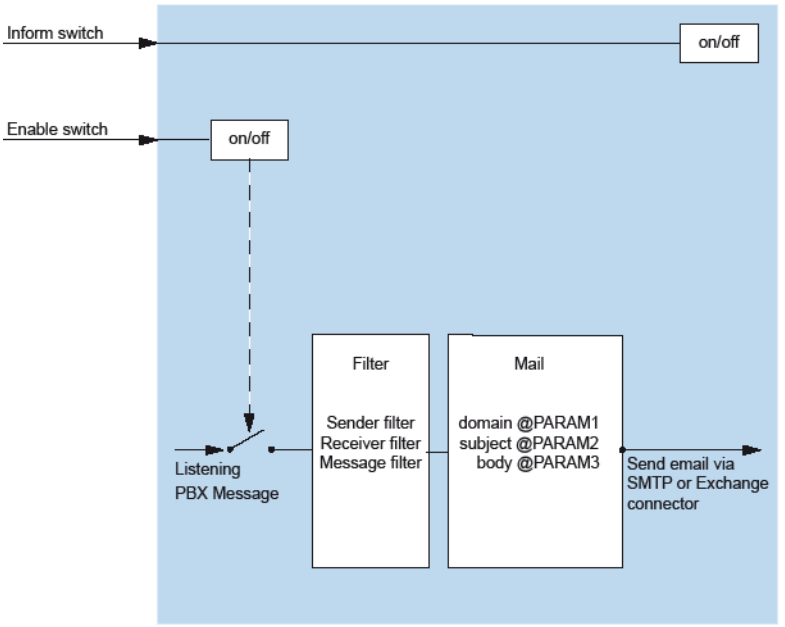
Figure 8.44: I/O Action PBXMessageIndication



PBXMessageToMail

The PBXMessageToMail action evaluates text messages that are sent over the communication server text message system to forward them as e-mails or SMS.

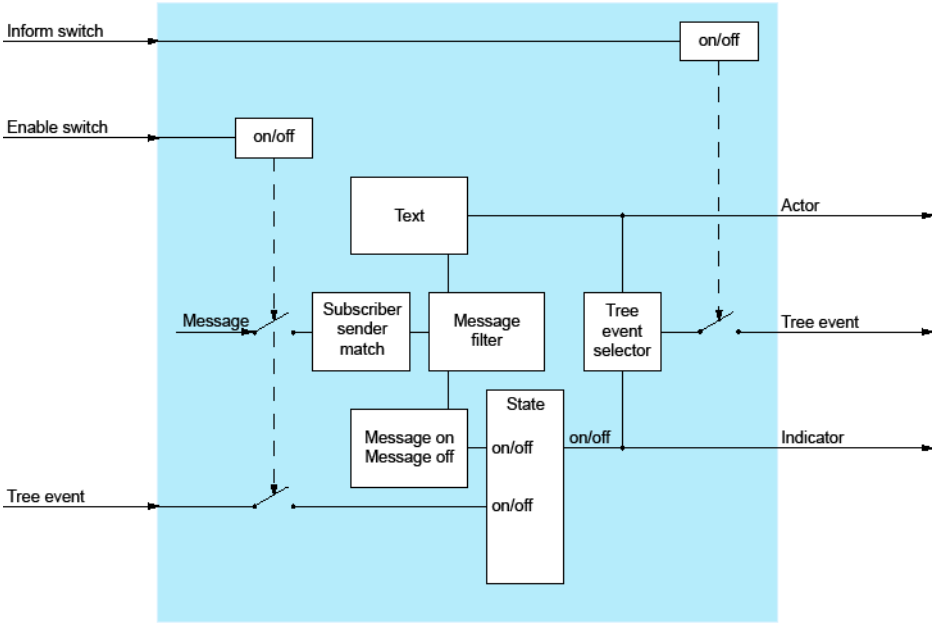
Figure 8.45: I/O Action PBXMessageToMail



PBXMessageTrigger

The *PBXMessageTrigger* action evaluates text messages that are sent over the communication server text message system.

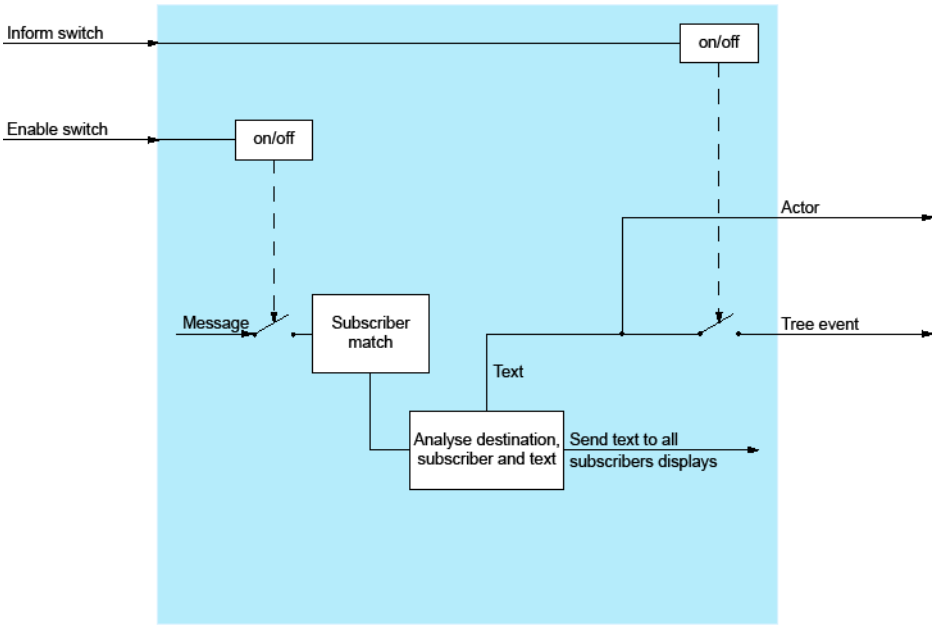
Figure 8.46: I/O Action PBXMessageTrigger



PBXNetworkMessage

The *PBXNetworkMessage* action sends messages to the QSIG network.

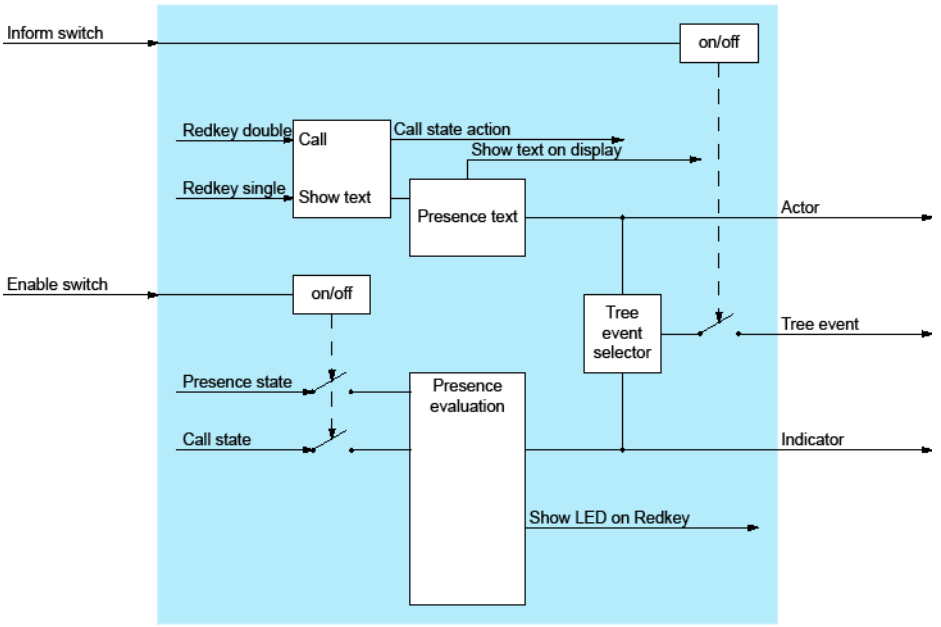
Figure 8.47: I/O Action PBXNetworkMessage



PBXPresenceKey

The *PBXPresenceKey* action indicates the presence status on a configured redkey.

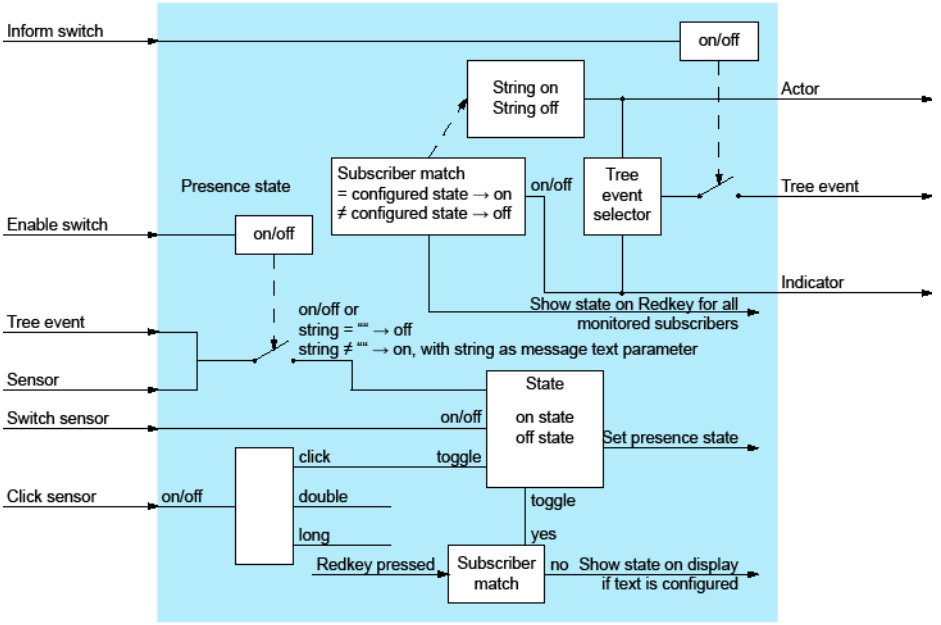
Figure 8.48: I/O Action PBXPresenceKey



PBXPresenceState

The *PBXPresenceState* action evaluates the presence status of the configured user. The presence status can also be set.

Figure 8.49: I/O Action PBXPresenceState

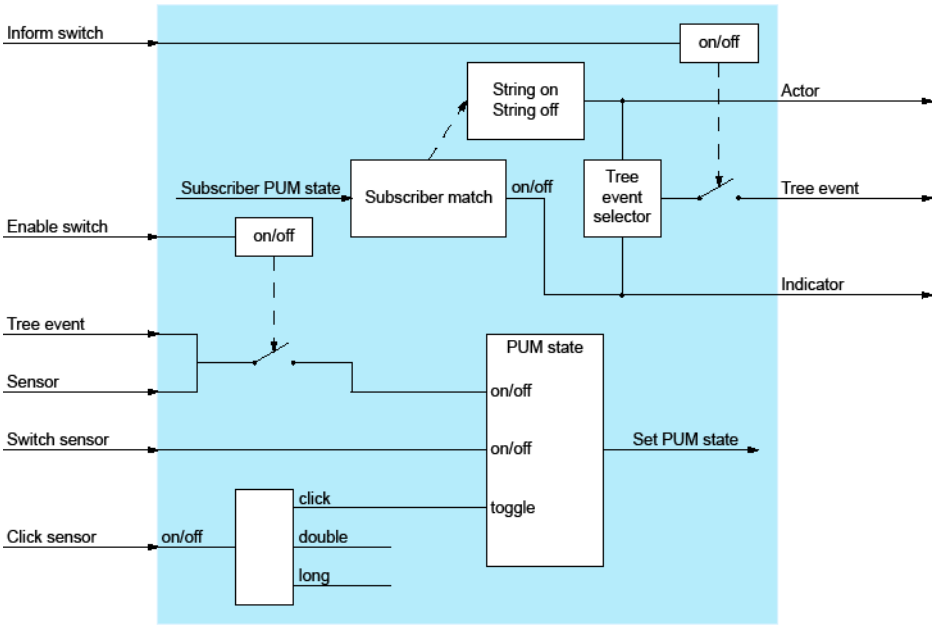


PBXPUMState

PUM

The *PBXPUMState* action sets and evaluates the PUM status of the configured user.

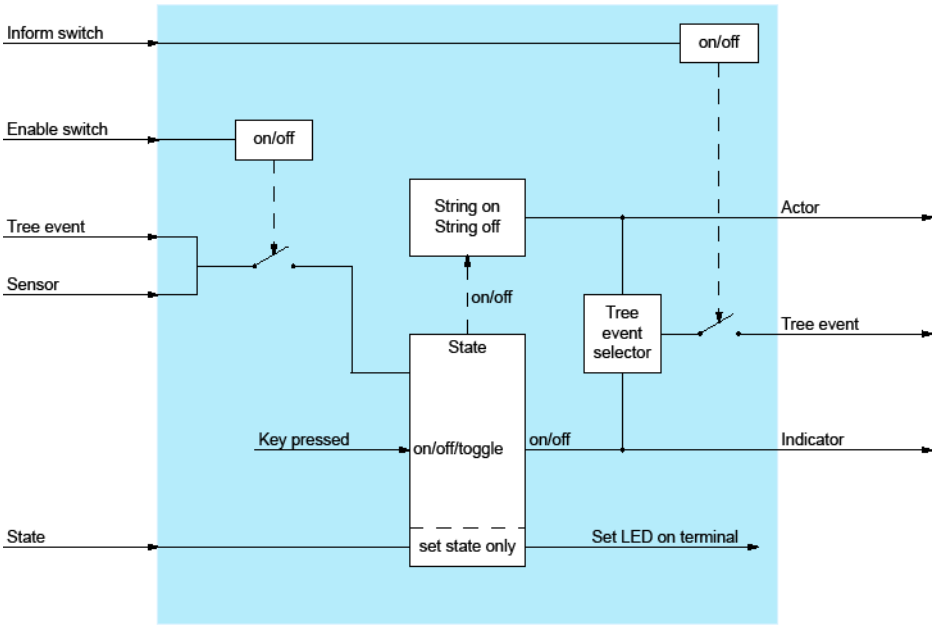
Figure 8.50: I/O Action PBXPUMState



PBXRedKey

The *PBXRedKey* action evaluates the received character string stored on a pro- grammed redkey, and sends Boolean-type output signals to the addressed actions.

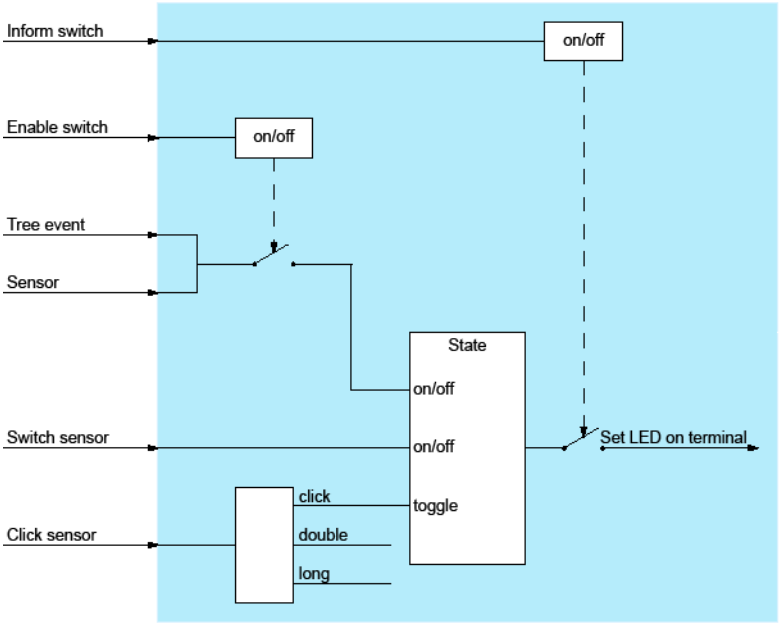
Figure 8.51: I/O Action PBXRedKey



PBXRedKeyLED

The *PBXRedKeyLED* action controls the LED for the configured redkey function on the system phone.

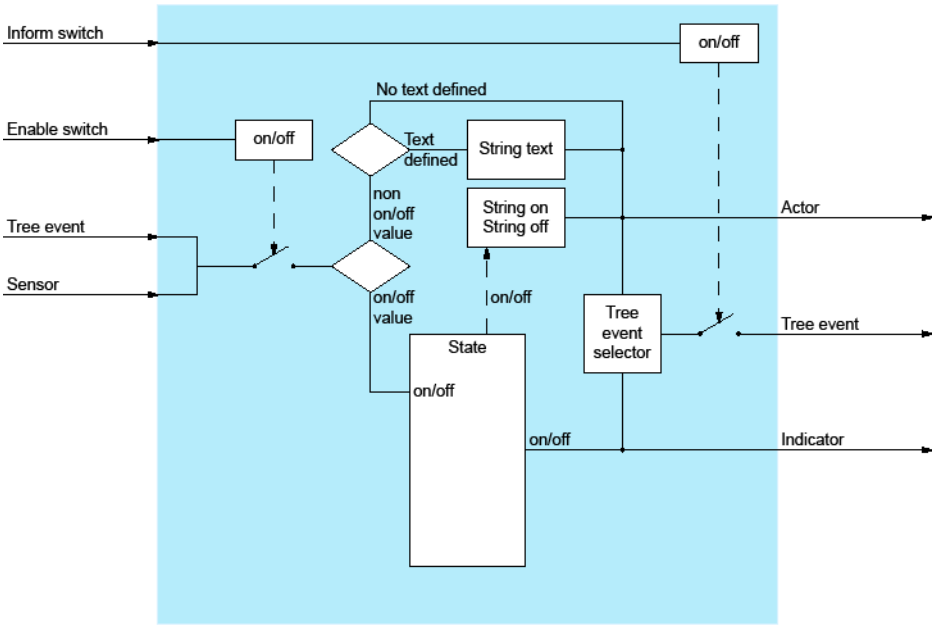
Figure 8.52: I/O Action PBXRedKeyLED



PBXSubscriber

The *PBXSubscriber* action forwards the status (on/off) of a configured PBX user. The status might be a particular call status or a new voice mail. The status can be used for the chart display.

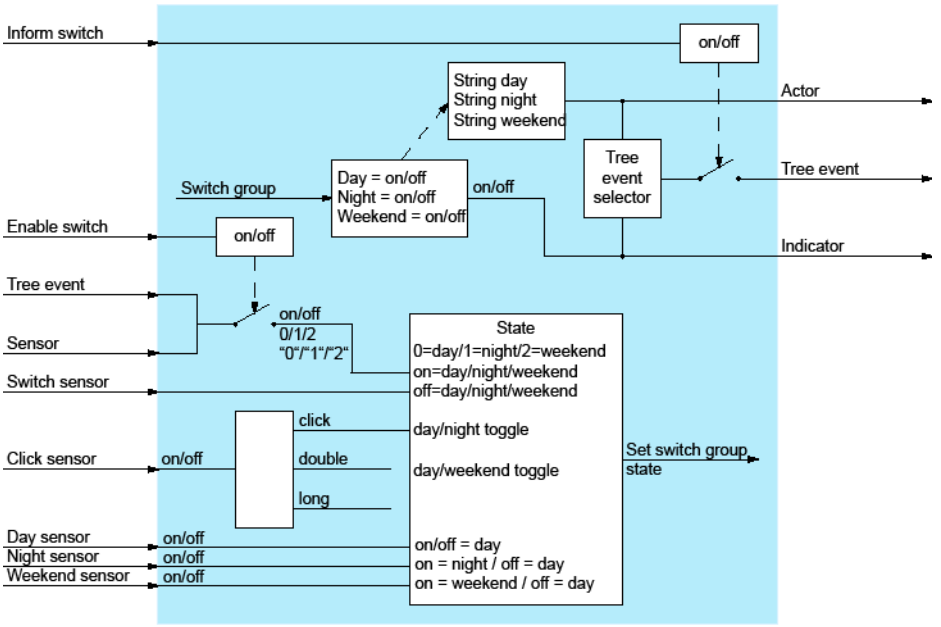
Figure 8.53: I/O Action PBXSubscriber



PBXSwitchGroup

The *PBXSwitchGroup* action sets and evaluates the status of the switch position (day, night, weekend).

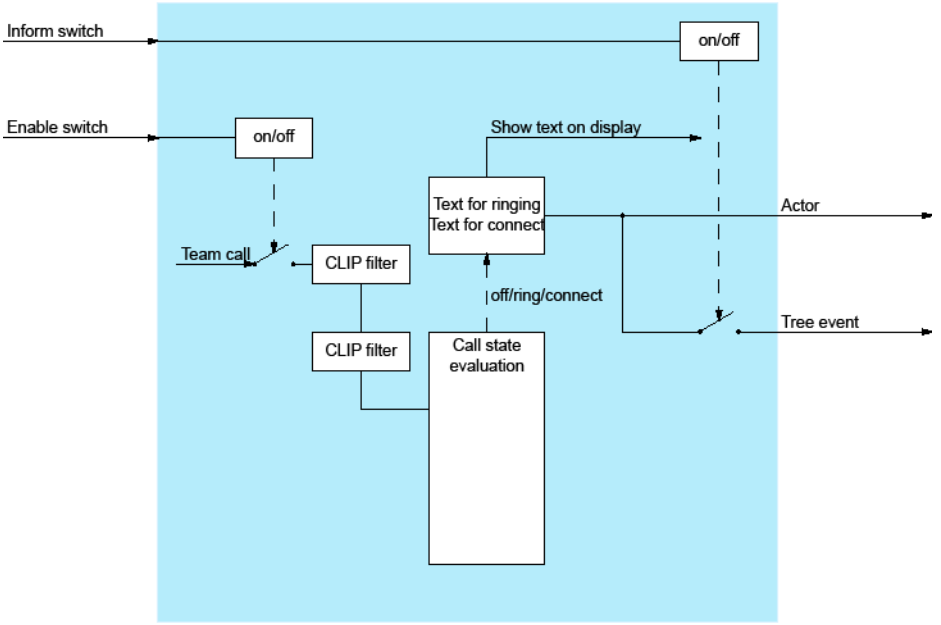
Figure 8.54: I/O Action PBXSwitchGroup



PBXTeamCall

The *PBXTeamCall* action allows the configuration of teams. All the team members see on the display of the system phone the calls made to the team members and can use the foxkey to fetch the calls.

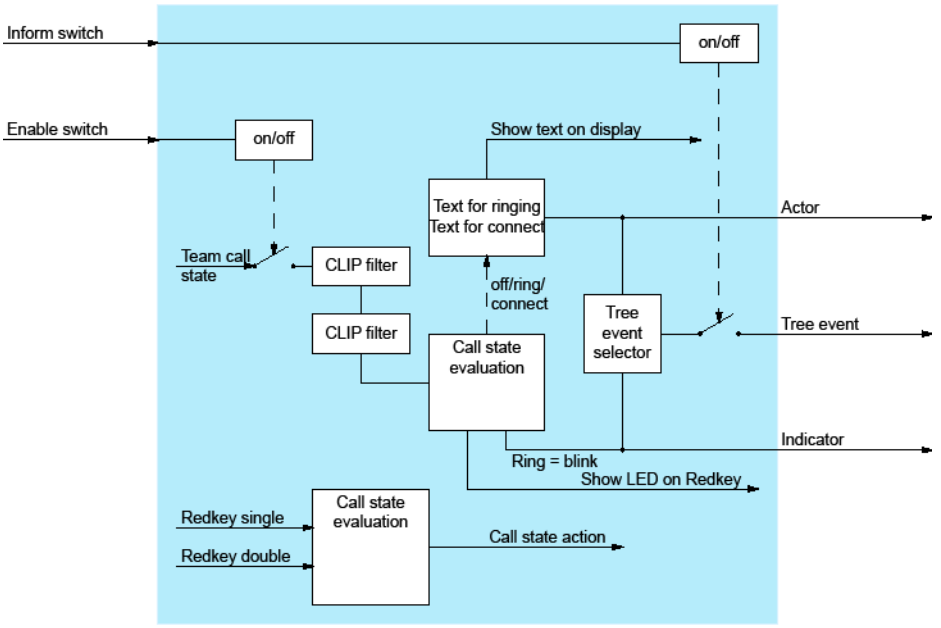
Figure 8.55: I/O Action PBXTeamCall



PBXTeamKey

The *PBXTeamKey* action simulates a team key that is available in the QSIG network.

Figure 8.56: I/O Action PBXTeamKey

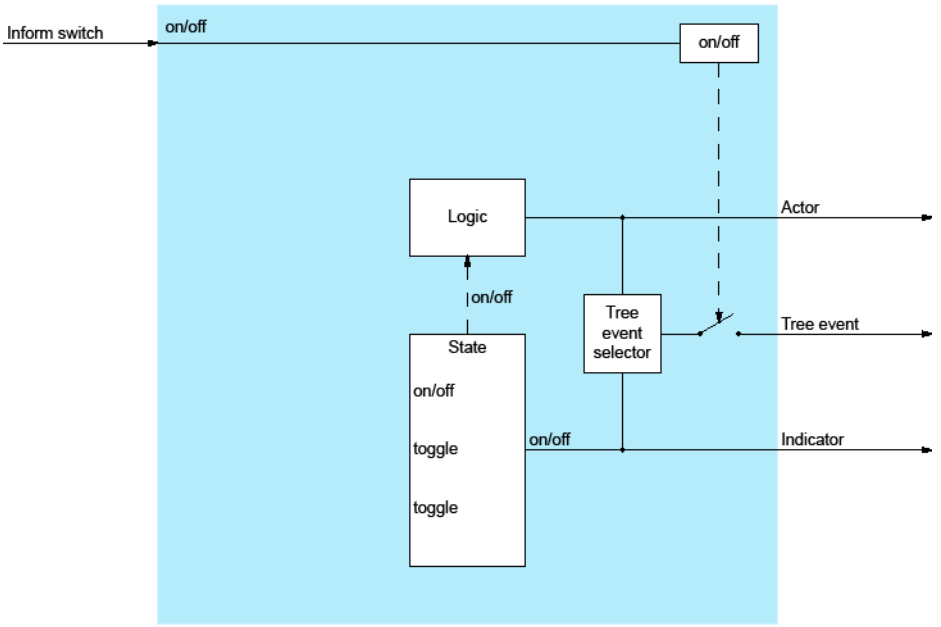


PBXTerminalEvent

The *PBXTerminalEvent* action evaluates safeguard alarms from the DECT cordless phones.

The following alarm criteria are recognised: redkey, man-down alarm, no-movement alarm, escape alarm, test alarm and room monitoring (Noise).requires an ATAS licence.

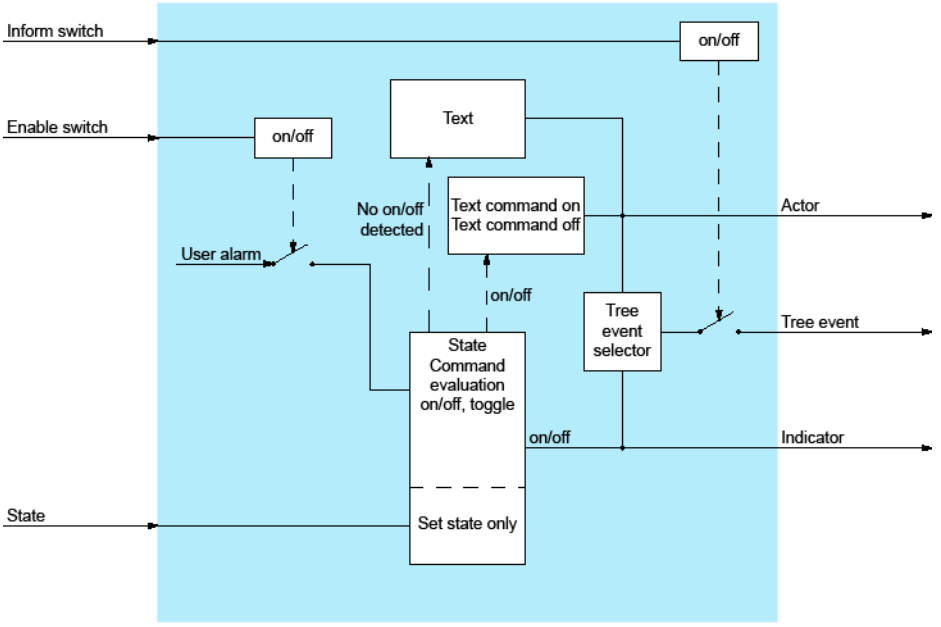
Figure 8.57: I/O Action PBXTerminalEvent



PBXUserCommand

The *PBXUserCommand* action evaluates alarms sent via the *77xxxx# function code.

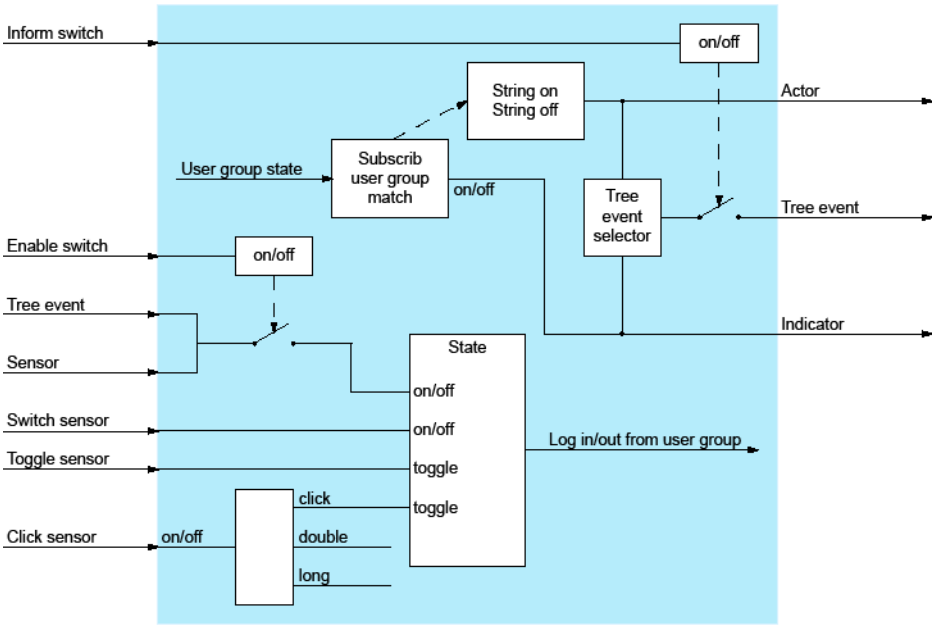
Figure 8.58: I/O Action PBXUserCommand



PBXUserGroup

The *PBXUserGroup* action sets and evaluates the status of the configured users in the user group.

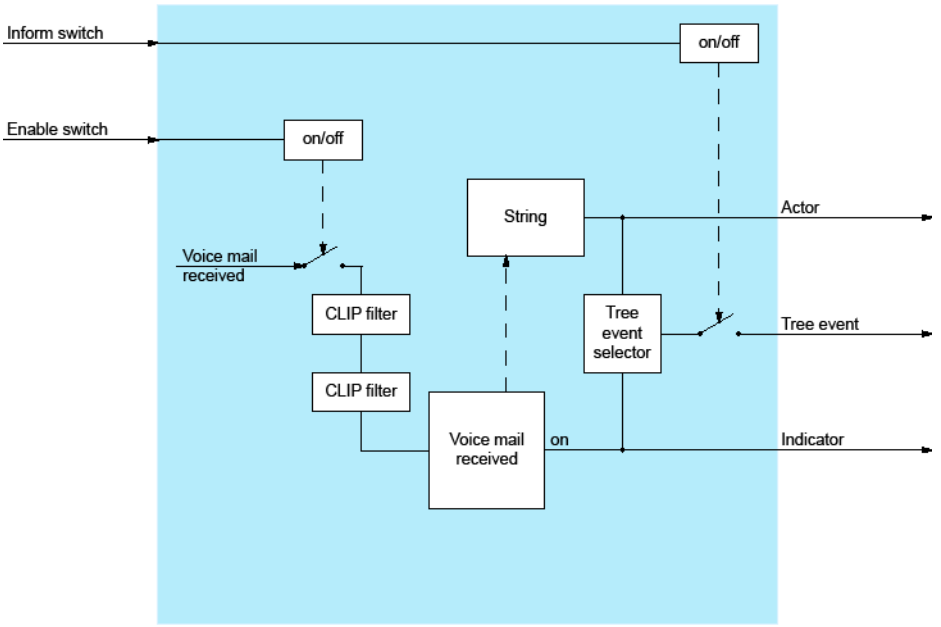
Figure 8.59: I/O Action PBXUserGroup



PBXVoiceMail

The *PBXVoiceMail* action responds to voice mails received by the configured user.

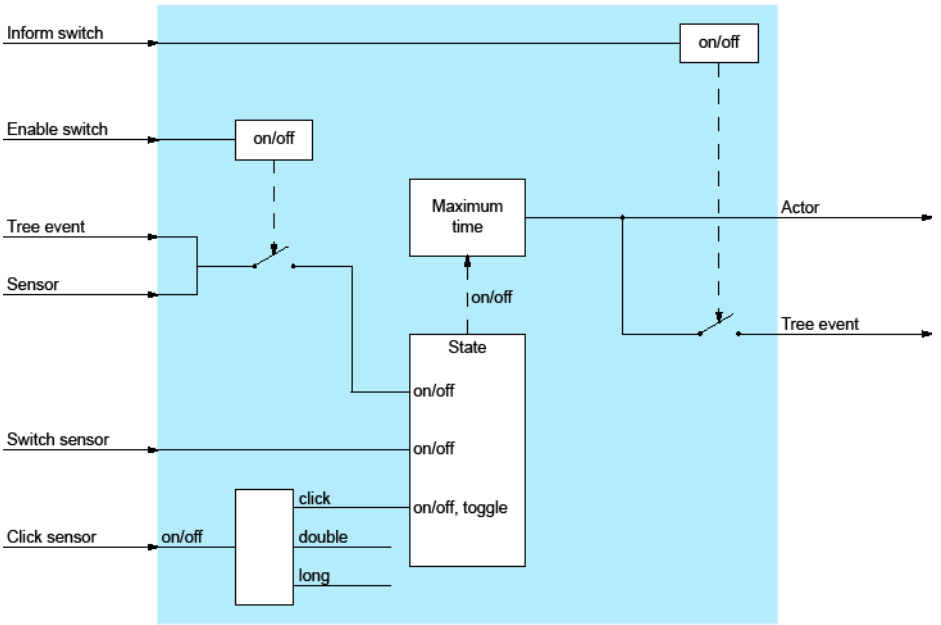
Figure 8.60: I/O Action PBXVoiceMail



RandomSwitch

The *RandomSwitch* action activates or deactivates the status of any subordinated actions randomly in the configured time interval.

Figure 8.61: I/O Action RandomSwitch



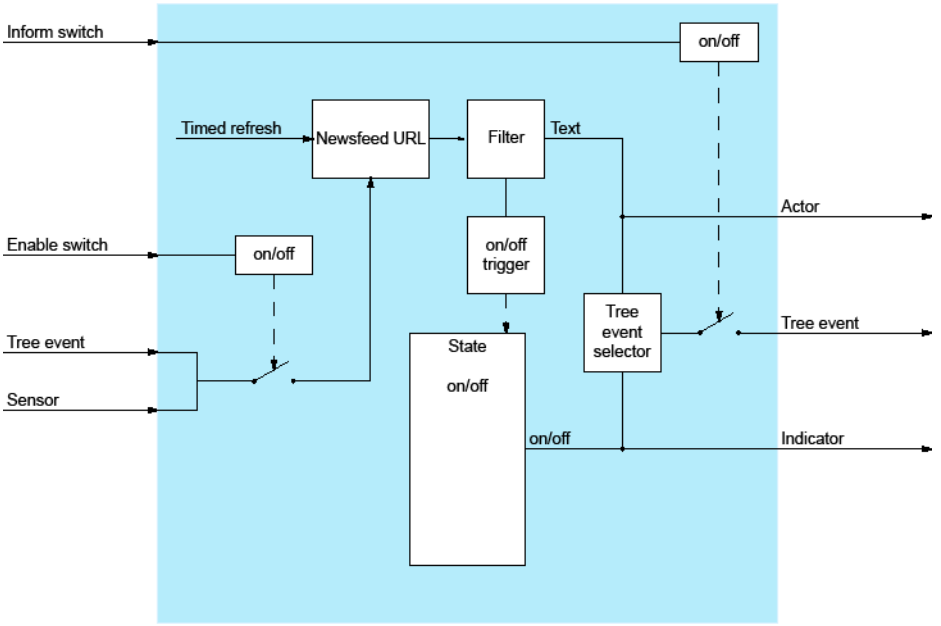
Example:

During an absence the lights in various rooms of a house are to be switched on and off again randomly.

RSSNews

The *RSSNews* action indicates messages in RSS file format on the display of the system phone.

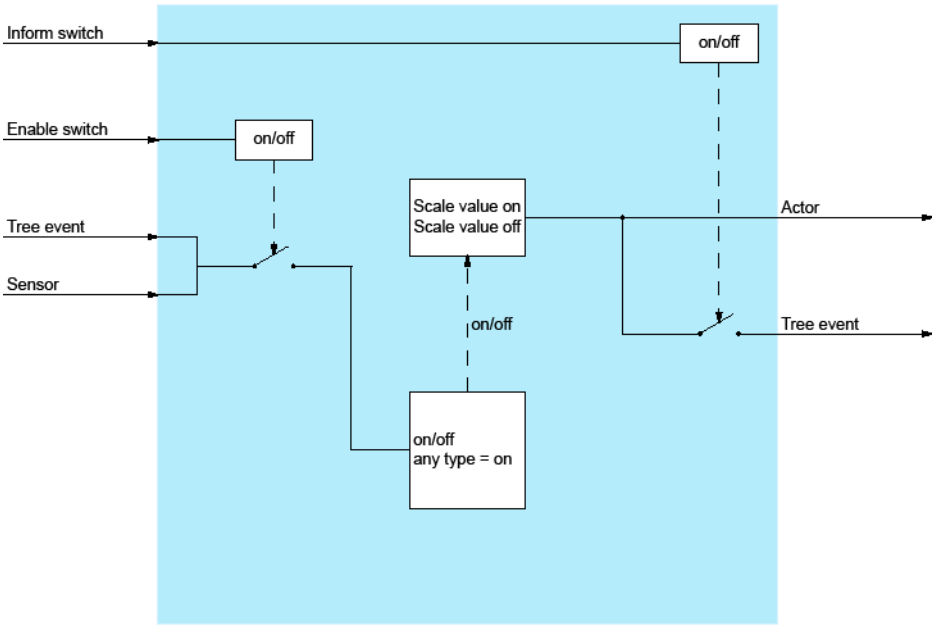
Figure 8.62: I/O Action RSSNews



ScalingValue

The *ScalingValue* action sends a configured floating point number to a configured I/O group.

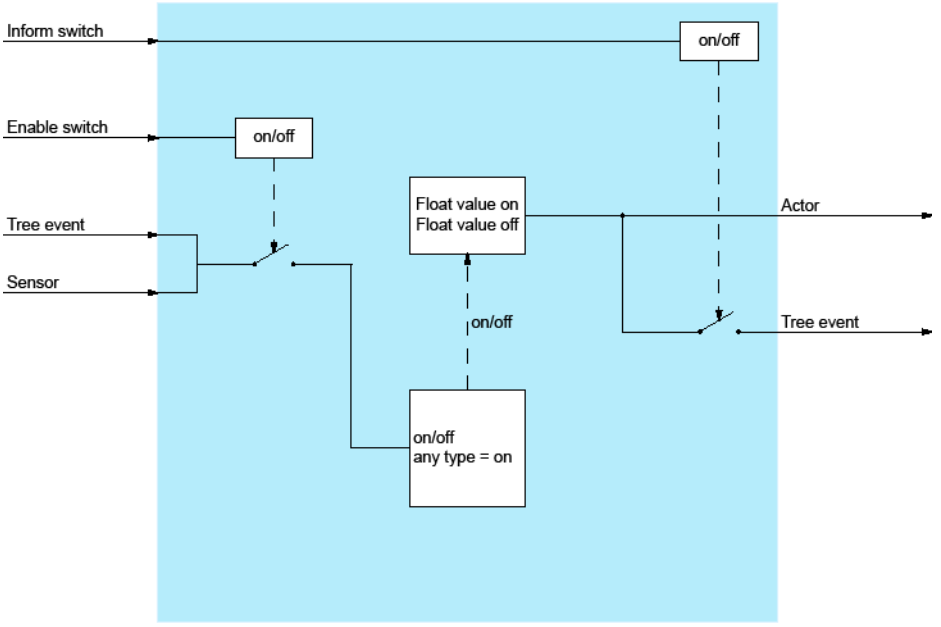
Figure 8.63: I/O Action ScalingValue



Sequence

The *Sequence* action activates the subordinated actions in sequence.

Figure 8.64: I/O Action Sequence

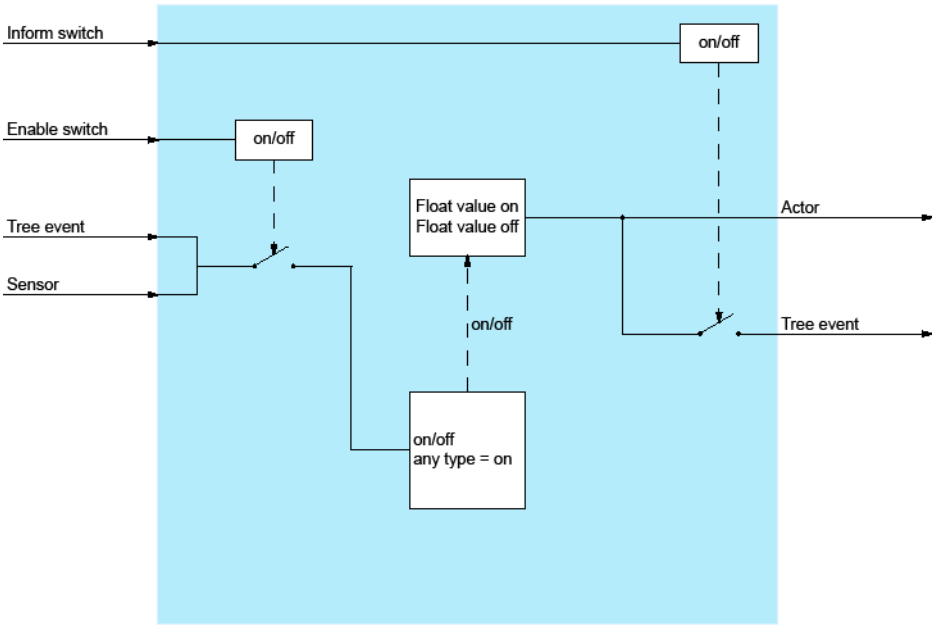


SmallFloatValue

0.1

The *SmallFloatValue* action sends floating point numbers in accordance with the IEEE754 standard with an accuracy of 2 bytes.

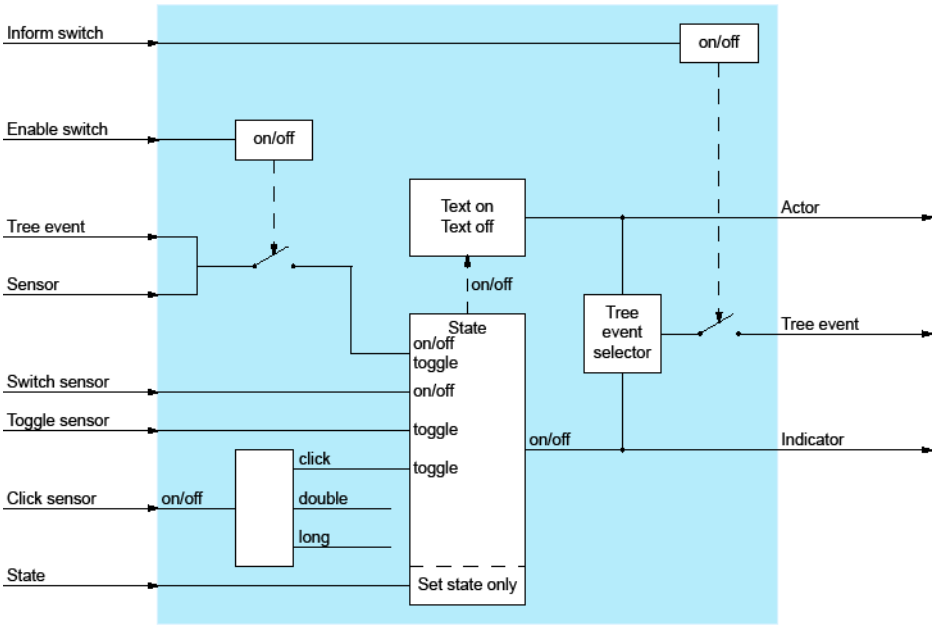
Figure 8.65: I/O Action SmallFloatValue



State

The action *State* action indicates the status of the action.

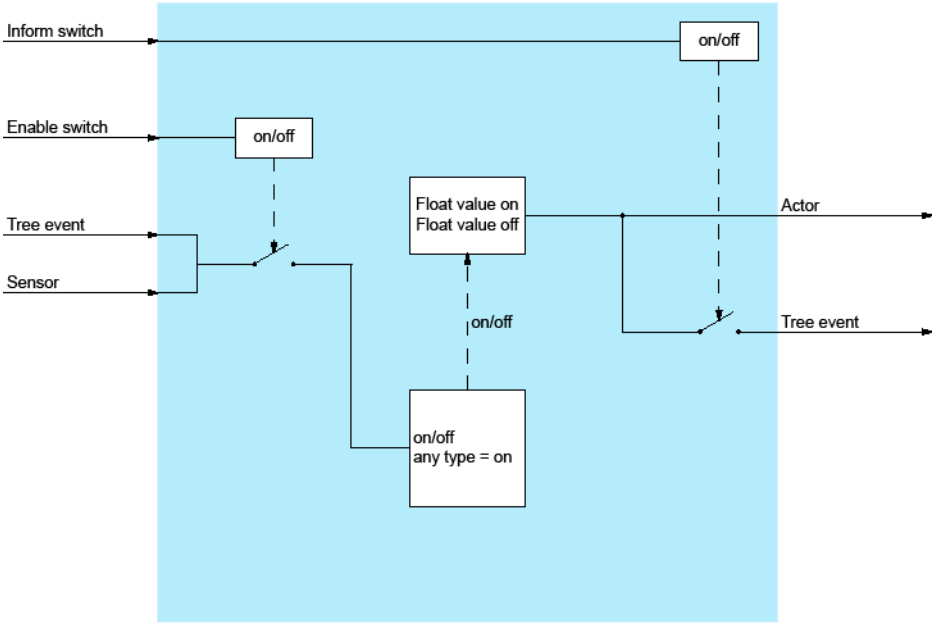
Figure 8.66: I/O Action State



StringFilter

The *StringFilter* action compares messages received with the configured filter criteria. If they match, the configured text is forwarded.

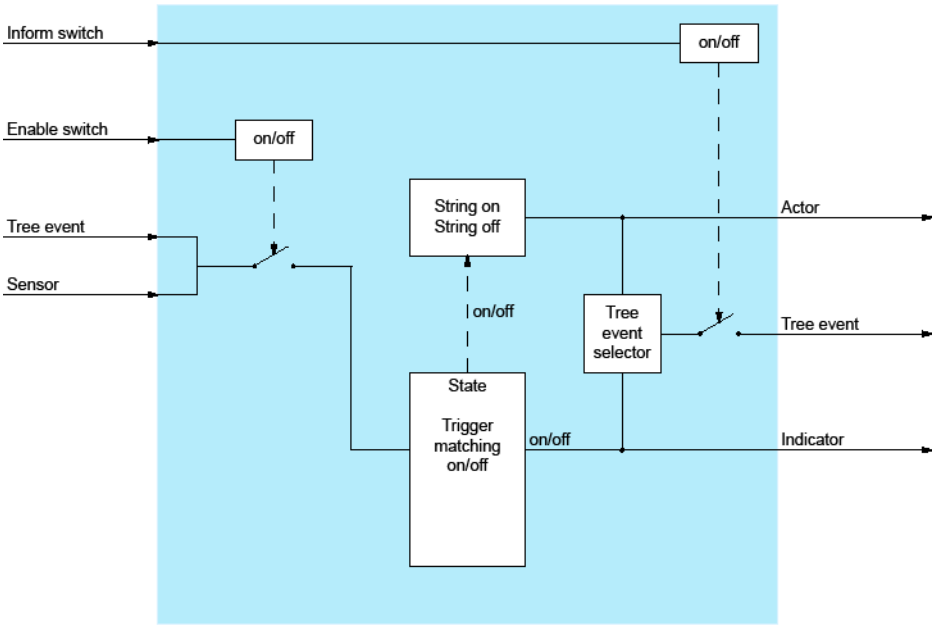
Figure 8.67: I/O Action StringFilter



StringTrigger

The *StringTrigger* action evaluates messages received according to their content.

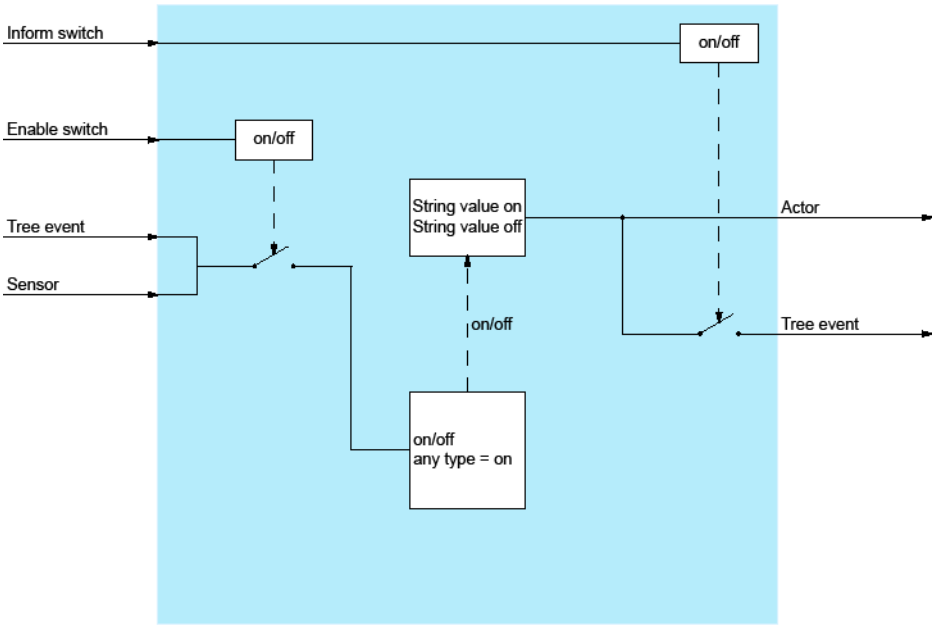
Figure 8.68: I/O Action StringTrigger



StringValue

The *StringValue* action sends configured character strings to the corresponding actions.

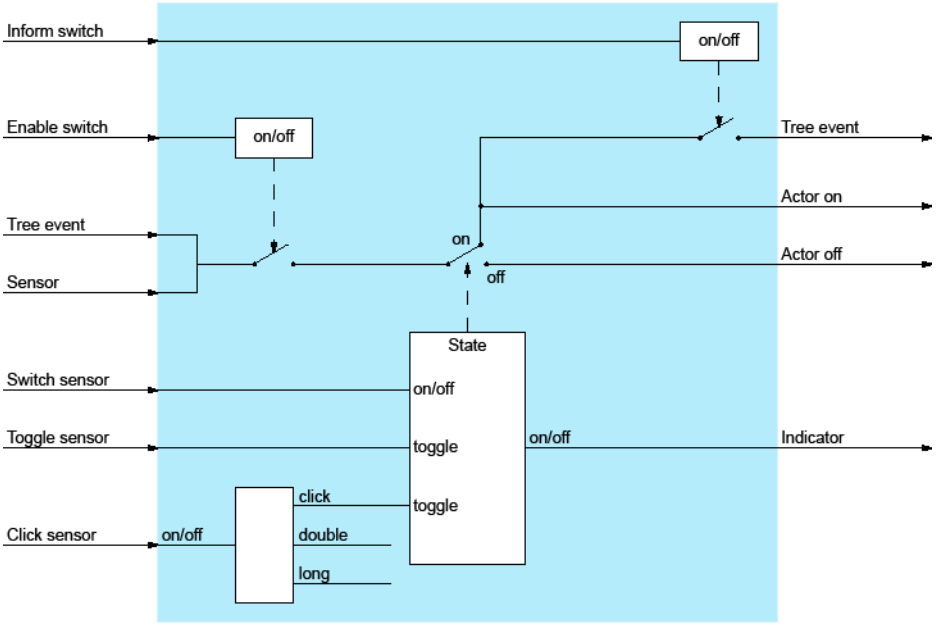
Figure 8.69: I/O Action StringValue



Switching

The *Switching* action receives and sends events depending on the internal status of the action.

Figure 8.70: I/O Action Switching

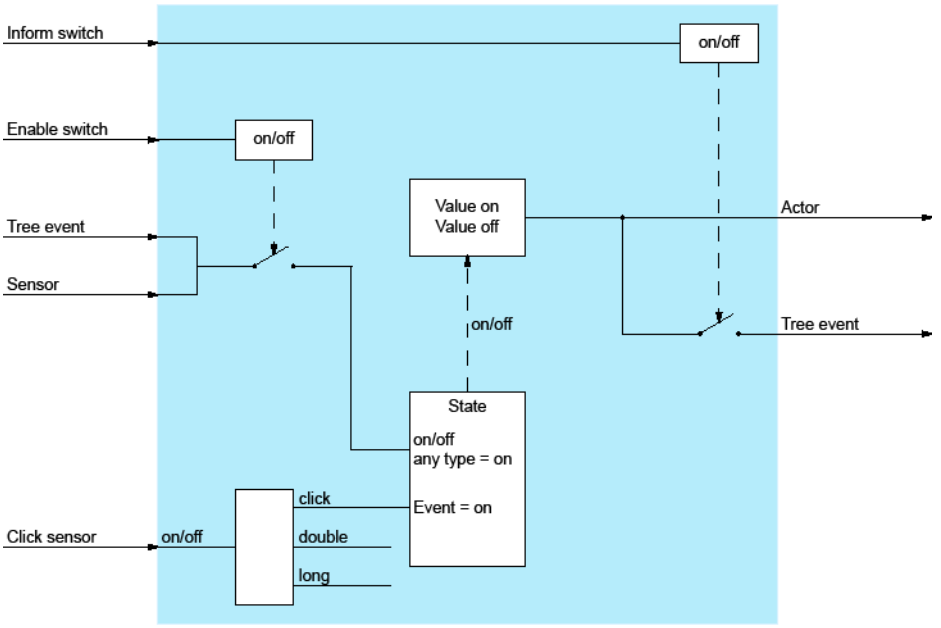


SwitchingValue

true

The *SwitchingValue* action sends Boolean-type values if events are received.

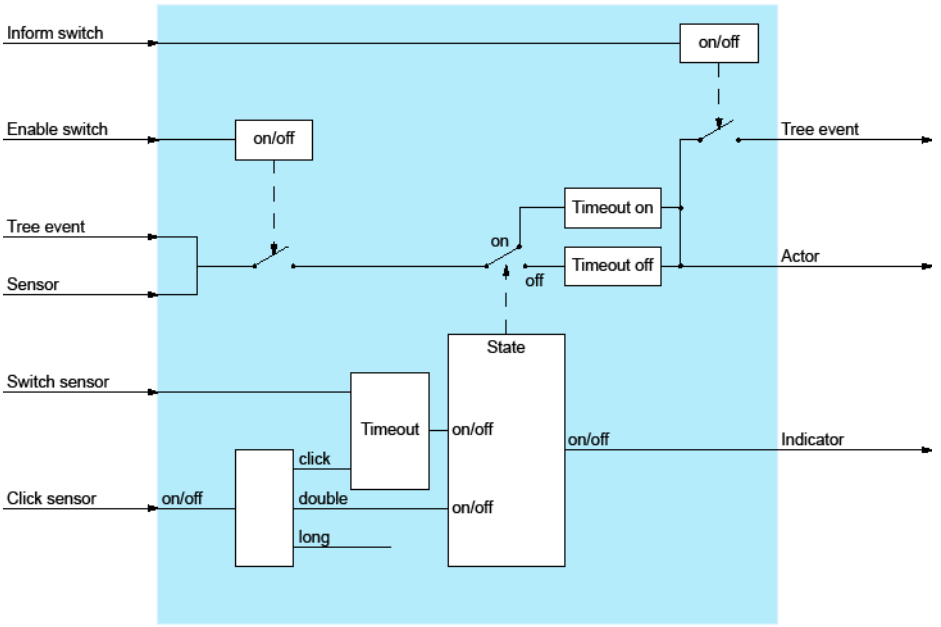
Figure 8.71: I/O Action SwitchingValue



Timeout

The *Timeout* action delays the sending of output signals.

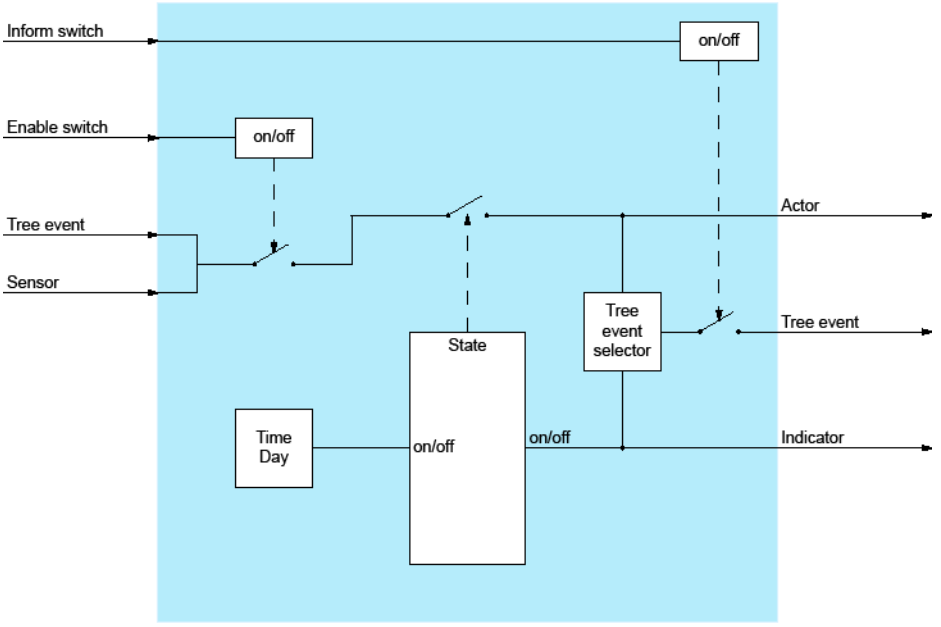
Figure 8.72: I/O Action Timeout



TimerSwitch

The *TimerSwitch* action is a timer switch that activates or deactivates the addressed actions at specific times.

Figure 8.73: I/O Action TimerSwitch



KNX connection

Building management systems integrate intelligent computer systems for controlling and monitoring electric building equipment. The connection is based on the European KNX standard (KNX=Konnex), which ensures that systems by different manufacturers are mutually compatible.

KNX is configured via I/O actions in the I/O manager. Specific KNX I/O actions are available. The names of KNX actions start with "KNX". Some actions can only be performed with these specific I/O actions (for example the I/O action *KNXLightControl*).

Control is via the KNX group addresses, for instance 1/7/2.

The licenses *KNX Connection*, *ATAS Gateway* (*ATASpro Gateway* for Opencom systems) and *CTI Third Party Basic* are required for KNX use.

KNX systems are connected to OIP via the OIP KNX driver, installed on the OIP server. The installation instructions are available in **"OIP KNX driver", Page 226.**

An overview of standardised DPT and EIS data types is available here: **Tab. 142.**

You will find further information about configuration in the description of individual I/O actions under OIP I/O actions and KNX I/O.

KNX I/O Actions

The following table lists an overview of the KNX I/O actions.

Table 8.10:List of KNX I/O Actions (Sheet 1 of 2)

	KNXAbsence	The KNXAbsence action monitors the status of the configured I/O group. The action is activated if the I/O group remains inactive during the configured time.
	KNXBell	The KNXBell action controls bell systems with short impulses if the action is activated.
	KNXBlindControl	The KNXBlindControl action controls the KNX blind actors.
	KNXBrightness	The KNXBrightness action evaluates the brightness values using the configuredvalues.
	KNXDimValue	The KNXDimValue action sends the settings for KNX dimmers.
	KNXHeatDevice	The KNXHeatDevice action controls heating systems for example.

Table 8.10:List of KNX I/O Actions (Continued) (Sheet 2 of 2)

	KNXHeatValve	The KNXHeatValve action controls KNX heating valves depending on the values received.
	KNXLevelControl	The KNXLevelControl action controls the water level.
	KNXLightControl	The KNXLightControl action controls KNX light actors.
	KNXPresence	The KNXPresence action controls PIR sensors.
	KNXPump	The KNXPump action controls external devices (e.g. pumps).
	KNXRainSensor	The KNXRainSensor action evaluates the rain status using I/O group events.
	KNXScene	The KNXScene action activates all configured actions and sub-actions.
	KNXSunblind	The KNXSunblind action is a control action for sun blinds.
	KNXTemperature	The KNXTemperature action evaluates the temperature received.
	KNXTextListener	The KNXTextListener action evaluates text strings that are sent from a groupaddress.
	KNXVentilator	The KNXVentilator action controls the on and off times of fans.
	KNXWatering	The KNXWatering action controls the automatic garden sprinkler system based on the data from the rainwater and humidity sensors, temperature and/or configured time intervals.
	KNXWindSpeed	The KNXWindSpeed action evaluates the wind speed.

KNXAbsence

The KNXAbsence action monitors the status of the configured I/O group. The action is activated if the I/O group remains inactive during the configured time.

KNXBell

The KNXBell action controls bell systems with short impulses if the action is activated.

KNXBlindControl

The KNXBlindControl action controls the KNX blind actors.

In scene mode, the telegrams received are forwarded to the subordinate I/O actions. Group addresses are therefore optional.

KNXBrightness

The KNXBrightness action evaluates the brightness values using the configured values.

KNXDimValue

The KNXDimValue action sends the settings for KNX dimmers.

KNXHeatDevice

The KNXHeatDevice action controls heating systems for example.

KNXHeatValve

The KNXHeatValve action controls KNX heating valves depending on the values received.

KNXLevelControl

The KNXLevelControl action controls the water level.

KNXLightControl

The KNXLightControl action controls KNX light actors. KNXLightControl supports switching, dimming, dim value and scene.

In scene mode, the telegrams received are forwarded to the subordinate I/O actions. Group addresses are therefore optional.

KNXPresence

The KNXPresence action controls PIR sensors.

KNXPump

The KNXPump action controls external devices (e.g. pumps).

KNXRainSensor

The KNXRainSensor action evaluates the rain status using I/O group events.

KNXScene

The KNXScene action activates all configured actions and sub-actions.

KNXSunblind

The KNXSunblind action is a control action for sun blinds.

KNXTemperature

The KNXTemperature action evaluates the temperature received.

KNXTextListener

The KNXTextListener action evaluates text strings that are sent from a group address.

If the text string consists of multiple substrings, you can use individual substrings (a maximum of three) as triggers with the @TEXTPARAMn variables. The substrings must be separated with a valid separator.

KNXVentilator

The KNXVentilator action controls the on and off times of fans.

KNXWatering

The KNXWatering action controls the automatic garden sprinkler system based on the data from the rain-water and humidity sensors, temperature and/or configured time intervals.

KNXWindSpeed

The KNXWindSpeed action evaluates the wind speed.

OIP KNX driver

KNX systems are connected to OIP via the OIP KNX driver, installed on the OIP server. The driver is installed via the installation view of OIP WebAdmin. You will require local administrator rights for installation.

The installation program required Java Runtime Environment (JRE). If JRE is not installed, also install JRE in the OIP WebAdmin installation view.

KNX connection can be set up via a V.24 or Ethernet connector.

Installation withV.24 connector

Start the installation via the OIP WebAdmin installation view. To install the OIP KNX driver, proceed as follows:

1. On the computer on which you wish to install the OIP KNX driver, open a browser and log on to the OIP WebAdmin of your OIP server.
2. Navigate to the installation view and load the installation file to the PC by clicking on the *OIP KNX driver* installation link.
3. Start the downloaded setup file by double-clicking it then follow the instructions given in the installation procedure.

   NOTE: JRE must be installed for driver installation. If the installation procedure cannot be started, first install JRE. You will find a JRE installation link in the installation view of OIP WebAdmin.
4. Choose the interface type (BCU1 or BCU 2.1). Interface type transmission rates:
   - BCU1: 9600 kbit/s
   - BCU2.1: 19200 kbit/s.
5. Enter the COM port and the rate with which the KNX system is connected.
6. Finish the installation procedure.
7. The OIP KNX driver is started as a Windows service.
8. Open OIP WebAdmin and navigate to the Configuration / Server /Services / I/O Manager.
9. Under Server address, enter the IP address of the KNX server.

The OIP KNX driver is uninstalled using *Control Panel* \ *Software* in the Windows operating system.

Restoring the default values of the BCU component

To restore the default values of the BCU component, proceed as follows:

1. Power off the bus.
2. Short-circuit PIN5 and PIN6 with a bridge.
3. Press the PROG key and power on the bus at the same time.
4. Release the PROG key after 3 seconds.
5. Remove the bridge between PIN5 and PIN6. Then restart the OIP KNX driver in Windows service.

Installation with Ethernet connector

Before you begin with the installation, make sure you have the following information:

- DNS name or, if no DNS server, IP address of the OIP server.
- IP port of the OIP web server if it differs from the standard IP port.
- IP address of the KNX LAN module used

Start the installation via the OIP WebAdmin installation view. To install the OIP KNX driver, proceed as follows:

1. On the computer on which you wish to install the OIP KNX driver, open a browser and log on to the OIP WebAdmin of your OIP server.
2. Navigate to the installation view and load the installation file on the PC by clicking on the *OIP KNX driver* installation link.
3. Start the downloaded setup file by double-clicking it then follow the instructions given in the installation procedure.

   NOTE: JRE must be installed for driver installation. If the installation procedure cannot be started, first install JRE. You will find a JRE installation link in the installation view of OIP WebAdmin.
4. Choose the interface type NetVersion and enter the IP address of the KNX LAN module.
5. Finish the installation procedure.
6. The OIP KNX driver is started as a Windows service.
7. Check in the OIP server log whether the service has been installed and whether the KNX module is working.
8. Open OIP WebAdmin and navigate to the Configuration / Server /Services / I/O Manager.
9. Under Server address, enter the IP address of the KNX server.

The OIP KNX driver is uninstalled via the Windows control panel (*Programs and functions*) of the Windows operating system.

OIP ATAS Gateways

With the OIP ATAS Gateways it is possible to use the ATAS functionality of the OIP server (display server) and one or more external ATAS applications in parallel.

OIP Installing ATAS Gateways

To connect external ATAS applications, an OIP ATAS gateway must be installed for each application. OIP makes available a version of the OIP ATAS gateway for the network connection or serial connection.

- OIP ATAS Gateway TCP/IP
- OIP ATAS Gateway V.24

The following settings have to be made on the communication and the OIP server to be able to use the OIP ATAS Gateways.

1. Activate an ATAS Gateway license.

   NOTE: You can also activate the licenses in the communication server (recommended). OIP reads it out from the communication server then activates the Gateway.

2. Create a new OIP user for the ATAS administrator (e.g. atasadmin). Enter the access data and indicated (username and password).

   NOTE: For emergency operation, enter the access data set by the application in the communication server.

3. Assign the following user groups to the ATAS administrator:

   – *ATAS_ADMINISTRATORS*
   – *OIP_ADMINISTRATORS*
   – *OIP_USER*
   – *TAPI_ADMINISTRATORS* (only if CTI commands are used on the ATAS Gate- way).

4. Add the following lines in the Lines window:

   – Lines of all users seen as alarm targets.
   – Lines of all users which should otherwise be controlled via the application

5. Save the settings.

Installing OIP ATAS gateways

Installation Requirements:

- To install the driver, you must have local administrator rights.
- The web-based installation of the ATAS Gatewaydriver requires an installed Java Runtime Environment (JRE) on the PC. If necessary, this can be installed from the installation view of OIP WebAdmin.

You will need the following information during the installation procedure:

- DNS name or, if no DNS server, IP address of the OIP server.

- You need the IP port for the ATAS Gateway TCP/IP. IP port 1088 must be used if you also set the application for emergency operation.
- For ATAS Gateway V.24, you need the COM port and the communication parameters.

Start the installation via the OIP WebAdmin installation view. To install an OIP ATAS Gateways, proceed as follows:

1. On the computer on which you wish to install the OIP ATAS Gateways open a browser and log on to the OIP WebAdmin of your OIP server.
2. Activate ATAS (Configuration / ATAS view).
3. Navigate to the installation view and load the installation file of the desired ATAS Gateways on the PC, by clicking the installation link.
4. Start the downloaded setup file by double-clicking on it and follow the instructions given in the installation procedure.
5. For the priority of the messages sent from the external ATAS application enter a value between 1 and 8, since priorities 0 and 9 cannot be over or under-controlled. The OIP ATAS Gateway is started as a Windows service.

The OIP ATAS gateway is uninstalled over Control panel \ Software of the Windows operating system.

Start the installation via the OIP WebAdmin installation view.

Using OIP ATAS-Gateways

When you start a connection the external ATAS application must log on with the OIP server. To do so, enter the user data of the ATAS administrator you created.

Application Examples

Using OIP Server as Telephony Server

To use the OIPserver as a telephony server you do not need to specify any other set- tings on the OIP server as in the OIP default settings all the users are assigned their own telephony line with Controlling rights. Whenever Twin Comfort mode (MiVoice Office 400) is activated, the DECT line is also assigned control rights.

In each case the OIP users must be assigned the corresponding CTI license in the user profiles.

The OIP TAPI service provider has to be installed on the Client PC. Carry out the installation as indicated in *"OIP TAPI service provider"* As login information enter the Windows user name if it is configured on the OIP server in the user profiles. If not, log in using the internal call number and the PIN.

Access to other telephony lines has to be carried out in the user profile of the corresponding user.

Setting up the Mitel 400 Call Center

To set up the Mitel 400 Call Center carry out the following steps in sequence:

1. In the communication server create a call distribution element with the direct dialing number and the internal call number under which the ACD skill is to be reached.
2. Select ACD as the CDE destination for all switch positions.
3. Start the OIP WebAdmin application Call centre management to open a new skill and configure the agents.
4. In OIP WebAdmin create a Skill and configure the general skill settings.
5. In the skill settings in the section Communications server assign the skill to the previously created CDE element.
6. Add the agents to the skill.
7. To monitor the call centre operation, select a group administrator and assign him the ACD_SUPERVISOR user group.

The Mitel 400 Call Center has now been set up as basic call centre with a skill. Extend the configuration as needed. OIP-Softphones or OIP Rich-Client applications of the setup agents now have, for the call centre operation, extended operating elements and the group administrator can monitor the call centre operation in the OIP WebAdmin call centre views.

Extend the configuration as needed.

External TAPI Client Server applications

For external TAPI Client-Server applications the application server has to be provided with the necessary lines by the OIP server.

Proceed as follows to set up the OIP for an external TAPI client-server application:

1. Activate the necessary CTI licenses.
2. Assign the TAPI administrator (user tapiadmin) all necessary lines and give the Controlling access rights on all lines
3. Assign the corresponding CTI License to the lines you have added to the TAPI administrator. The TAPI administrator himself does not need any CTI license.
4. Install on the application server the OIP TAPI service provider in accordance with *"OIP TAPI service provider"*. To log on to the OIP server enter the user data of the TAPI administrator.
5. If the external TAPI client-server application has to be used as ACD application, set it as indicated in *"Setting up the Mitel 400 Call Center"*.
6. If the external ACD application is to take charge of agent status changes such as login and logout, in the OIP TAPI service provider in the line settings, the option Control of agent status changes on the terminal must be activated.

Citrix and terminal server environment

The OIP server can be integrated into a Citrix or terminal server environment. If so, the OIP server should not be installed on the terminal server for performance reasons.

To make telephone lines available via TAPI to terminal server users and applications, the OIP TAPI service provider has to be installed on the terminal server. To do so, carry out the steps described in the *"External TAPI Client Server applications"*.

For safety reasons you should also activate the Microsoft telephony server on the terminal server so that terminal server users do not have access to the lines provided by the OIP TAPI service provider. For the configuration of the Microsoft telephony server please refer to the documentation of the corresponding Windows server operating system.

E-Mail notification for voice mail

With OIP users can send their voice mail messages on the communication server as e- mail. Requirement: Their OIP administrator must have set up the OIP SMTP Client or Microsoft Exchange-Server for the e-mail connection.

As a user, proceed as follows:

1. Log on to OIP WebAdmin with your username or call number and PIN or password.
2. Navigate in the menu tree to the Configuration / User / Personal settings view.
3. In the Notifications section, activate the setting E-mail notification for voice mails.

The voice mail messages are attached to the notification e-mail as .wav file. If necessary, you can as administrator change the file type to MP3 in the service settings *Voice Mail Manager*.

As administrator, you can configure the e-mail sender address for notification e-mails in the service settings *Message Manager* (Default address: oip-noreplay.

E-mail connection via an SMTP mail server

1. Check in the list of services (Configuration / Server / Services view) whether the service SMTP driver is available. If it is not, start the OIP installation procedure and select the service in the OIP component selection.
2. Activate the OIP SMTP client (Configuration / Server / General view).
3. Enter the server address as well as the access data.
4. Check whether the e-mail addresses have been recorded at the users.

E-mail connection via a Microsoft Exchange Server

1. Check whether the Microsoft Exchange-Server is connected and whether the connection is working.
2. In the user settings enter the users' mailbox addresses.

DECT locating

DECT locating is used to locate handsets on the DECT system of a communication server. The signal strength of the various radio units can be called up on the device. It is important to note that there has to be at least three radio units. An external application uses the data to calculate the position and to display it. This position is for information purposes only and is not guaranteed to ensure personal safety.

The I/O Manager can be used to implement the example of DECT locating inside a building using visual means.

To do so proceed as follows:

1. The building's situation plan has to be available as an image file in gif format. The size of the image file should be adapted to the screen size and its resolution. Make sure the file name does not contain any spaces and is identical with the action name in the I/O Manager.
2. Copy the situation plan to the OIP server installation directory *...<OIP-Verzeichnis>\webapps\axp\images\io*.
3. Start the OIP I/O Manager application and add an action of the type IO system then give this I/O application the name DECT locating.
4. Under the I/O application add an action of the type Area then give it, for instance, the name Situation plan. The action name must be identical to the file name of the situation plan.
5. Add the DECT radio units that are to be integrated in DECT locating as follows: highlight your newly created action in the navigation tree, open the shortcut menu and select *Advanced* \ *DECT radio unit*. It is not necessary to perform settings at this point.

6. Under the I/O application add another action of the type IO system then name it, for instance, DECT terminal.
7. Highlight the action, open the shortcut menu and use Special \ Add DECT terminal
8. to add the DECT terminal to be included in DECT locating.
9. Add the DECT terminals that are to be integrated in DECT locating as follows: high- light the newly created action in the navigation tree, open the shortcut menu and select Advanced \ Add DECT terminals.
10. Define the monitoring signal interval of the DECT terminals added (setting Request interval). The shorter the monitoring interval is set, the greater the load on the DECT system.
11. To deactivate DECT locating: while the DECT terminal is in the charger, set the Handle charging bay setting to Yes (default value).
12. Highlight the action Situation plan then right-click the View tab. The situation plan should now be displayed. Use the mouse to drag the DECT radio units one by one into the situation plan and position them according to your location.
13. Next drag the DECT terminals one by one to your location in the situation plan. As soon as the system recognises the location of the DECT terminals, the DECT terminals are positioned accordingly. Alternatively you can also position the DECT terminals on the edge of the screen so that the situation plan only displays those DECT terminals that are not in the charging bay.

RSS News on system phones

RSS News (Really Simple Syndication) is used to retrieve information (news, weather, etc.) from web sites and display it on system phones.

1. Start the OIP application I/O Manager.
2. Add another action of the type IO system then name it, for instance, RSS news.
3. Under the I/O application add an action of the type RSS news then give it, for in- stance, the RSS provider's name.
4. In the Parameter tab configure the following parameters:
   - Refresh time
   - RSS location
   - Subscribers
   - Display time
   - Ring time

At the time interval configured under Refresh time OIP reads the provider’s RSS file and displays the newly added messages.

Maintenance and Troubleshooting

Reorganize OIP database

The OIP server reorganizes the database at set times. Depending on the configuration in the corresponding OIP services the older entries are then deleted. The following table lists the times at which the database reorganization of the individual OIP services takes place.

Table 10.1:OIP database reorganization times

Database entries	OIPService	Time
ACDstatistics	*ACD Log Manager*	02:17:00
Alarms	*Alarm Driver*	00:55
Calendarentries	*Calendar Manager*	01:00
Call data	*Call Logging Manager*	01:15
Actionsentries	*I/O Manager*	01:17
Journal entries	*Journal Manager*	01:55
OIP Log data	*Log Service*	00:50
Messageentries	*MessageManager*	00:35
Call tickets	*Ticket Service*	01:09

Maintenance of the OIP Server

Backing up the OIP configuration

The OIP database is automatically backed up once a day. In OIP WebAdmin in the Data backup view, you can manually create a backup file using the Create backup button. The backup consists of the following files, stored in the default directory *<OIP directory>\backup*\:

- *axpconfig* (xml)
- *axpdb* (sql)
- *clients* (zip) - contains a file each for MiVoice 1560 PC Operator and Mitel Office- Suite.

The backup copies are also compressed in the .zip file *oipBackup*. A copy of this .zip file is stored in the directory *<OIP directory>\webapps\axp\backup*.

By default, each backup is kept for 5 days. You can modify this duration in the OIP service *Database Driver*.

The times for automatic file backup are indicated in **Tab. 60.**.

If necessary, the storage location can also be changed in the OIP service *Database Driver*. If the backup files are to be stored on the network, the Windows Service *OIP Server* must be started under a user account that has access to these network resources. In this case, you need to specify the network path in the OIP service *Database Driver*.

Restore OIP Configuration

You can find information on how to restore the OIP configuration in the OIP WebAdmin online help.

Changes on the communication server

Changes to the communication server configuration are automatically adopted by the OIP server during the next synchronization with the communication server. The synchronization interval with the communication server can be set in the OIP service *PBX Manager*.

Changes to the following PBX settings could result in unintended data changes in the OIP database:

- IP address of the PBX
- Name of the PBX
- System ID

As long as the communication server's system ID remains the same, the OIP server handles the communication server as a known communication server. This means that the IP address and name of the communication server can be changed.

If the communication server's IP address and name remain the same and if only the communication server's system ID is changed, the OIP server also handles the communication server as a known communication server.

All other combinations will result in the OIP server handling the communication server as a different communication server and creating the PBX's users as new data records in the OIP database.

Changing the IP Address of the communication server

To change the IP address of the PBX, proceed as follows:

1. Change the IP address of the communication server and restart it.
2. Log on to the OIP server using the OIP Administrator (oipadmin).
3. Open the OIP configuration and in the PBX network menu select the communication server whose IP address you wish to change. You can change the IP address only after the communication server has been deactivated. After making the changes, re- activate the communication server and save the changes.
4. Exit and restart the Windows service *OIP Server*.

First Start of the PBX

If the communication server is being started for the first time, you should proceed as follows to avoid any data loss:

1. Exit the Windows service *OIP Server* on the OIP server.
2. Carry out the first-start of the communication server and the upload of the PBX configuration.
3. Start the Windows service *OIP Server* on the OIP server.

Hardware modifications on the communication server

It is possible to replace the hardware of a communication server or a license chip without changing the OIP configuration, provided the criteria under **"Changes on the communication server"** are met.

To modify the hardware on a communication server connected with OIP, proceed as follows:

- Exit the Windows service *OIP Server* on the OIP server.
- Make the changes on the communication server hardware.
- If necessary, update the communication server software and configuration.
- Start the OIP Windows service *OIP Server* on the OIP server.

Locating a malfunction

In the following chapters you will find the instructions on how to locate a malfunction.

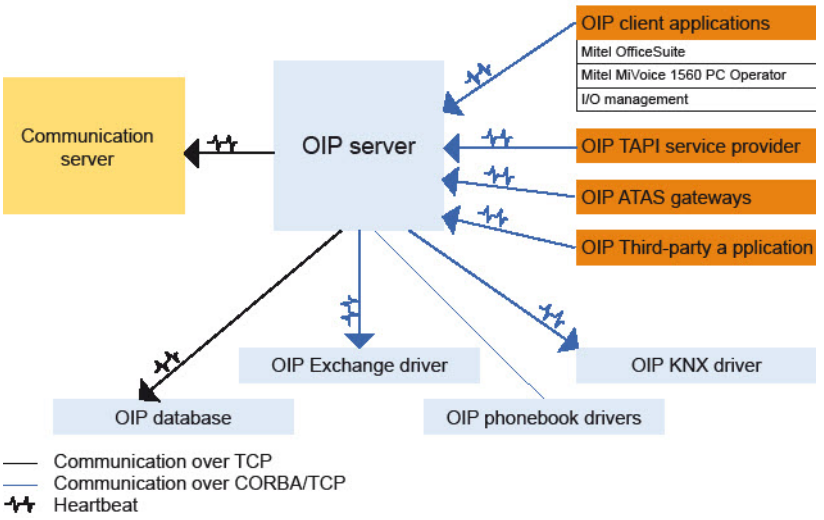
Overload

If the dimension and performance of the OIP server do not match the operational requirements, this may lead to malfunction. That is why utmost care has to be taken during planning to ensure that the infrastructure complies with the requirements.

Connection monitoring

The OIP server's communications with the communication server, the OIP database, the OIP applications and the OIP Connectors are monitored using Heartbeats, see the following figure.

Figure 10.1: Heartbeat between Client and Server



The heartbeat is sent by the Client periodically and checked on the server. If the Client cannot send a heartbeat, the Client automatically sets up the new connection1).

The OIP server can act either as a Client or as a server. With the following connections the OIP server is the Client and therefore sends the heartbeat to the:

- OIP server – communication server
- OIP server – OIP database
- OIP server – OIP Exchange Driver
- OIP server – OIP KNX driver

By contrast with the following connections the OIP server is the server, which means it receives the heartbeats from the:

- OIP applications – OIP server[1]
- OIP TAPI service provider – OIP server
- OIP ATAS Gateways – OIP server
- OIP third-party applications – OIP server

Connection interruptions can occur on the TCP layer or on the CORBA layer. In the event of interruptions on the TCP layer (e.g. network cable disconnected), the connections between Client and server are cleared down immediately. By contrast short-term interruptions of up to 10s are caught at the CORBA layer whenever possible.

The OIP services started by the Clients on the OIP server are automatically terminated by the OIP server after a connection interruption due to the missing heartbeat.

Connection interruptions in which the OIP server is the Client are entered in the log file

<OIPServer-jjjj-mm-dd_hh-mm-ss.log>. Connection interruptions in which the OIP server is the server are entered in the log file of the corresponding Client.

1. The operator applications must be restarted.

A alarm can be configured on the communication server so that it generates an alarm in the event of a connection interruption between the OIP server and the communication server. The following alarm messages can be configured:

- ACD server out of service
- ATAS: connection lost/established
- CTI third party: connection lost/established

For an overview of the log files of the OIP components during the runtime please refer to *"Backing up log files"*.

OIP server performance

The following factors can cause the OIP server to perform below par:

Slow OIP databases

OIP is a real-time application that relies on fast, high-level availability on the part of the database. The number of entries in the individual tables of the database, in which data matches are carried out even during the runtime, increases the CPU load on the OIP database service and the performance of the OIP server can be diminished as a result.

Use the Windows Task Manager to check the CPU load of the OIP database service. Only a permanent load of more than 30% should be considered as critical.

In this case check the amount of time the following data is stored in the database:

- Call centre statistics data
- Call journals (logs)
- Call data
- Log data

In this case change the amount of time the data is stored in the database. The Call Centre statistics data and the call data can be accessed via the stored files. If the data is still required in database form, you should duplicate the OIP database in an offline database. More details can be found on the MySQL web pages (http://www.mysql.com).

Insufficient memory

In the system information view under Memory usage you can see the current OIP server memory usage. If the average storage space used is above 200 MB, the PC should have a main memory of at least 1 GB.

Unsuccessful connection setup attempts

If the OIP server regularly tries without success to set up a connection with the OIP Connector drivers, this limits the OIP server performance. Check the OIP server's main log file <OIPServer-jjjj-mm-dd_hh-mm-ss.log> to see whether there are any entries about this behaviour (see also *"Connection monitoring"*).

Too many activated OIP services

Deactivate all OIP services you need.

For an overview of the log files of the OIP components during the runtime please refer to *"Backing up log files"*.

Backing up log files

For an analysis of the malfunction you should save the relevant log files and send them to your support organisation along with an exact description of the fault as a .zip file.

Malfunction during Installation

Any error during installation is recorded in the following log files.

OIP server

From the OIP server installation directory, save the log files with the file extension **.log*.

OIP applications

From the installation directory of the OIP application, save the log files with the file extension **.log*.

OIP TAPI service provider

Save the log files of the Windows event display.

If the malfunction occurs during configuration, see *"Malfunction during the runtime"*, Section *"OIP TAPI service provider"*.

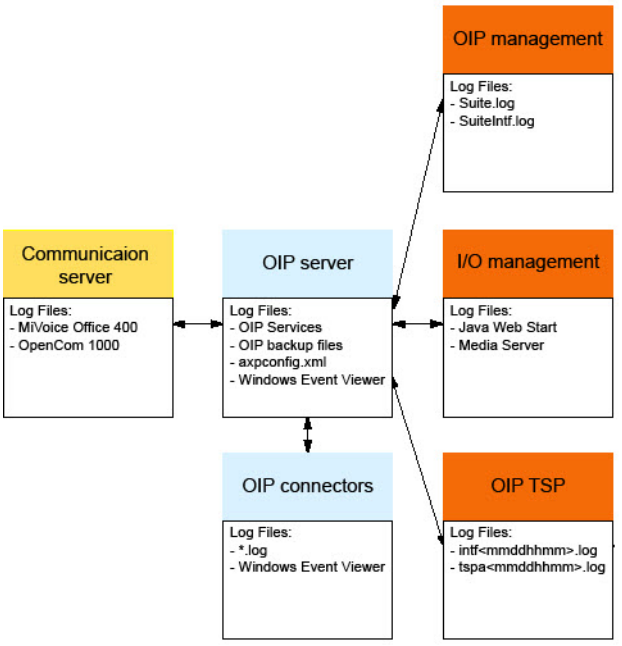
OIP Connectors

From the installation directory of the driver of the OIP Connector, save the log files with the file extension **.log*.

Malfunction during the runtime

Any malfunction during the runtime is recorded in the corresponding log file. The following figure gives an overview of where the various log files are created.

Figure 10.2: Log file overview



MiVoice Office 400

Table 10.2:MiVoice Office 400log files

Log file	Remarks
MiVoice Office 400 log files:	
• *I-bus*	Switch on the Benni Monitor
• *ATPC3*	
• *Error logs*	

OIP server

On the OIP server there are two levels of log files. The upper level comprises the log files that log the general status of the OIP server. They include the log files listed in the following table.

Table 10.3:Level 1 Log files (Sheet 1 of 2)

Log file	Description
OIPServer-yyyy-mm-dd_hh-mm-ss.log	Log file of the OIP server
OIPWebServer-yyyy-mm-dd_hh-mm-ss.log	Log file of the OIP web server
AXP-Logfile-yyyy-mm-dd_hh-mm-ss.log	Log file of the OIP server with detailed information

Table 10.3:Level 1 Log files (Continued) (Sheet 2 of 2)

Log file	Description
axpusers.log	Log file of the OIP users configured in the OIP server

The second level comprises the log files of the individual OIP services. These log files are created or filled with log entries only if the corresponding OIP service has been set to debug. The following table lists the OIP services and the relevant log files.

Table 10.4:Level 2 Log files (Sheet 1 of 7)

OIPService	Log file
Account Service	AccountService_<OIPuserID>_yyyy-mm-dd_hh-mm-ss_0.log
ACD Log Manager	ACDLogManager_yyyy-mm-dd_hh-mm-ss_0.log
ACD Log Service	ACDLogService_yyyy-mm-dd_hh-mm-ss_0.log
ACDManager	ACDManager_yyyy-mm-dd_hh-mm-ss_0.log
ACDService	ACDService_<OIP user ID>_yyyy-mm-dd_hh-mm-ss_0.log
Active Directory Service	ActiveDirectoryService_yyyy-mm-dd_hh-mm-ss_0.log
Agent Manager	AgentManager_yyyy-mm-dd_hh-mm-ss_0.log
Agent Service	AgentService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Alarm Driver	AlarmReceiver_yyyy-mm-dd_hh-mm-ss_0.log TCP-IN-<PBX IP-address>-ON-1062.log
Alarm Service	AlarmService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Alpha & Quick Dial Service	AlphaService_yyyy-mm-dd_hh-mm-ss_0.log
Buddy Manager	BuddyManager_yyyy-mm-dd_hh-mm-ss_0.log
Buddy Service	BuddyService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Calendar Manager	CalendarManager_yyyy-mm-dd_hh-mm-ss_0.log
Calendar Service	CalendarService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
<Default ¬¹ Font>Calendar Synchro nization Service	CalendarService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Call Logging Driver	TaxReceiver_yyyy-mm-dd_hh-mm-ss_0.log TCP-IN-<PBX IP-address>-ON-1080.log
Call Logging Manager	TaxManager_yyyy-mm-dd_hh-mm-ss_0.log
Call Logging Service	TaxService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log

Table 10.4:Level 2 Log files (Continued) (Sheet 2 of 7)

OIPService	Log file
Call Service	CallService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Client Utility Service	UtilsService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
CLIPService	CLIPService_yyyy-mm-dd_hh-mm-ss_0.log
Configuration Profile Manager	ConfigProfileManager_yyyy-mm-dd_hh-mm-ss_0.log
Configuration Profile Service	ConfigProfileService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
ConfigurationService	ConfigurationService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
DasTelefonbuch Directory Service	ThePhoneDirectoryService_yyyy-mm-dd_hh-mm-ss_0.log
Database Driver	DatabaseDriver_yyyy-mm-dd_hh-mm-ss_0.log
Directory Manager	DirectoryManager_yyyy-mm-dd_hh-mm-ss_0.log
Directory Service	DirectoryService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Display Manager	DisplayManager_yyyy-mm-dd_hh-mm-ss_0.log
Display Service	DisplayService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Event Service	EventService_yyyy-mm-dd_hh-mm-ss_0.log
Fax Manager	FaxManager_yyyy-mm-dd_hh-mm-ss_0.log
Fax Service	FaxService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Feature Service	FeatureService_yyyy-mm-dd_hh-mm-ss_0.log
Flow Manager	FlowManager_yyyy-mm-dd_hh-mm-ss_0.log
Flow Service	FlowService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Function Key Manager	FunctionKeyManager_yyyy-mm-dd_hh-mm-ss_0.log

Table 10.4:Level 2 Log files (Continued) (Sheet 3 of 7)

OIPService	Log file
Function Key Service	FunctionKeyService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
I/O Manager	IO-Manager_yyyy-mm-dd_hh-mm-ss_0.log
I/O Service	IO-Service-<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Jabber Driver	JabberDriver_yyyy-mm-dd_hh-mm-ss_0.log
Journal Manager	JournalManager_yyyy-mm-dd_hh-mm-ss_0.log
Journal Service	JournalService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Key Configuration Service	KeyService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
LDAP Directory Service	LDAPDirectoryService_yyyy-mm-dd_hh-mm-ss_0.log
License Manager	LicenseManager_yyyy-mm-dd_hh-mm-ss_0.log
License Service	LicenseService_yyyy-mm-dd_hh-mm-ss_0.log
Line Service	LineService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Load Balancing Service	LoadBalancingService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Location Manager	LocationManager_yyyy-mm-dd_hh-mm-ss_0.log
Location Service	LocationService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Log Service	Log_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Login Service	SystemLogin_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Media Manager	MediaManager_yyyy-mm-dd_hh-mm-ss_0.log
MessageManager	MessageManager_yyyy-mm-dd_hh-mm-ss_0.log
Message Service	MessageService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log

Table 10.4:Level 2 Log files (Continued) (Sheet 4 of 7)

OIPService	Log file
Naming Service	DistributedNameService_yyyy-mm-dd_hh-mm-ss_0.log
Notepad Service	NotepadService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Notification Manager	NotificationManager_yyyy-mm-dd_hh-mm-ss_0.log
Notification Service	NotificationService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
ODBC/JDBCDirectory Service	JDBCDirectoryService_yyyy-mm-dd_hh-mm-ss_0.log
Operator Service	OperatorService<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
PBX Driver Ascotel	ASNMP-<PBX IP-address>_yyyy-mm-dd_hh-mm-ss_0.log ATNS-<PBX IP-address>_yyyy-mm-dd_hh-mm-ss_0.log ATNSDriver-<PBX IP-address>_yyyy-mm-dd_hh-mm-ss_0.log CTIDriverAscotel-<PBX IP-Adress>_yyyy-mm-dd_hh-mm-ss_0.log DisplayDriver_yyyy-mm-dd_hh-mm-ss_0.log PBXConfigDriver-<PBX IP address>_yyyy-mm-dd_hh-mm-ss_0.log PBXDriverAFP-<PBXIPaddress>_yyyy-mm-dd_hh-mm-ss_0.log PBXDriverAscotel-<PBXIPaddress>_yyyy-mm-dd_hh-mm-ss_0.log PBXDriverInfolink-<PBX IP address>_yyyy-mm-dd_hh-mm-ss_0.log TCP-OUT-<PBXIPaddress>-1061_yyyy-mm-dd_hh-mm-ss_0.log TCP-OUT-<PBXIPaddress>-1070_yyyy-mm-dd_hh-mm-ss_0.log TCP-OUT-<PBXIPaddress>-1074_yyyy-mm-dd_hh-mm-ss_0.log TCP-OUT-<PBXIPaddress>-1088_yyyy-mm-dd_hh-mm-ss_0.log

Table 10.4:Level 2 Log files (Continued) (Sheet 5 of 7)

OIPService	Log file
PBX Driver OpenCom 1000	ANETProvider-<PBX IP-Address>_yyyy-mm-dd_hh-mm-ss_0.log ANVZDriver-<PBX IP-Address>_yyyy-mm-dd_hh-mm-ss_0.log CI-Provider-<PBX IP-Address>_yyyy-mm-dd_hh-mm-ss_0.log CTIDriver-<PBX IP-Address>_yyyy-mm-dd_hh-mm-ss_0.log OC1000DisplayDriver-<PBX IP-Address>_yyyy-mm-dd_hh-mm-ss_0.log PBXConfigDriver-<PBX IP address>_yyyy-mm-dd_hh-mm-ss_0.log TAMI-Provider-<PBX IP-Address>_yyyy-mm-dd_hh-mm-ss_0.log TCP-OUT-<PBX IP address>-8092_yyyy-mm-dd_hh-mm-ss_0.log TCP-OUT-<PBX IP address>-8095_yyyy-mm-dd_hh-mm-ss_0.log TCP-OUT-<PBX IP-Address>-880x_yyyy-mm-dd_hh-mm-ss_0.log
PBX Information Service	PBXInfoService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
PBX Manager	PBXManager_yyyy-mm-dd_hh-mm-ss_0.log
PBX Setup Manager	PBXSetupManager_<OIP-user ID>_yyyy-mm-dd_hh-mm-ss_0.log
PBX Setup Service	PBXSetupService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
PISN Directory Service	PISNSubscriberDirectoryService_yyyy-mm-dd_hh-mm-ss_0.log
Private Card Directory Service	PhoneCardDirectoryService_yyyy-mm-dd_hh-mm-ss_0.log
Private Directory Service	PrivateDirectory_yyyy-mm-dd_hh-mm-ss_0.log
Public Directory Service	PublicDirectory_yyyy-mm-dd_hh-mm-ss_0.log
PUMManager	PUMManager_yyyy-mm-dd_hh-mm-ss_0.log
PUMService	PUMService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log

Table 10.4:Level 2 Log files (Continued) (Sheet 6 of 7)

OIPService	Log file
RegistrationManager	RegistrationManager_yyyy-mm-dd_hh-mm-ss_0.log
Registration Service	RegistrationService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Routing Manager	RoutingManager_yyyy-mm-dd_hh-mm-ss_0.log
Routing Service	RoutingService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
RSS Driver	RSSDriver_yyyy-mm-dd_hh-mm-ss_0.log
Security Service	SecurityService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Server Utility Service	UtilityService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Service Manager	axpservices-yyyy-mm-dd_hh-mm-ss.log
Shortdial Directory Service	ShortDialDirectoryService_yyyy-mm-dd_hh-mm-ss_0.log
SMTPDriver	SMTPDriver_yyyy-mm-dd_hh-mm-ss_0.log
Subscriber Configuration Manager	SubscriberConfigManager_yyyy-mm-dd_hh-mm-ss_0.log
Subscriber Configuration Service	SubscriberConfig_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Subscriber Directory Service	SubscriberDirectoryService_yyyy-mm-dd_hh-mm-ss_0.log
System User Directory Service	SystemUserDirectoryService_yyyy-mm-dd_hh-mm-ss_0.log
Test Manager	TestManger_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Test Service	TestService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Ticket Service	TicketService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Time Service	TimeService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log

Table 10.4:Level 2 Log files (Continued) (Sheet 7 of 7)

OIPService	Log file
TTS Manager	TTSManager_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
TwixTel Directory Service	TwixTelDirectoryService_yyyy-mm-dd_hh-mm-ss_0.log
User Preferences Service	UserPreferences_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
User Profile Manager	UserProfileManager_yyyy-mm-dd_hh-mm-ss_0.log
User Profile Service	UserProfileService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
User Service	UserServices-<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Voice Mail Manager	VoiceMailManager_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Voice Mail Service	VoiceMailService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
WEB Server Service	Output on console if the OIP server is started in console mode.

1. Activate the debug mode for all OIP services. The log level should be set to debug. Please note that activating the debug mode restricts the runtime behaviour of the OIP server.
2. From the installation directory of the OIP server, save the entire *logs* directory.
3. From the installation directory of the OIP server, save the entire *backup* directory.
4. From the OIP server installation directory, save the OIP configuration file *axpcon- fig.xml*.
5. Save the log files of the Windows event display.

Mitel OfficeSuite

1. Activate debug mode.
2. Backup the log files Suite.log and SuiteIntf.log from the following directory: *c:\Us- ers\<User name>\AppData\Local\Mitel\Suite\Log*

MiVoice 1560 PC Operator

1. Activate debug mode.
2. Back up the log files Mitel1560.log and Mitel1560_Intf.log from the directory *c:\User\<User name>\AppData\Local\Mitel\Mitel1560\Log*.

Java-based OIP applications

1. Delete the temporary internet files in the Java Control Panel (Control Panel\Java). Deleting the Temporary Internet Files deletes all downloaded applications; the next time you start up the OIP application, the application files will again be downloaded.
2. From the Java Control Panel activate debugging from the Advanced tab.
3. Reproduce the malfunction.
4. From the user profile directory ...\Sun\Java\Deployment\log, save the log file javaws*.log.

Operator applications

1. Activate debug mode.
2. From the user profile directory ...\Documents and Settings\All Users\Application Data\Mitel, save the entire Logs directory.

Media Server

The Media Server is installed with an OIP softphone: From the user profile directory save the log file media.log.

Office eDial

1. Activate debug mode.
2. From the installation directory save the log files:
   - adialer.log
   - atapilib.log

OIP TAPI service provider

1. Activate the debug mode of the OIP TAPI service provider.
2. Restart the Windows Telephony Service.
3. Save the configured Log directory.
   - intf<mmddhhmm>.log
   - tspa<mmddhhmm>.log

If an error occurs, the event messages in the following table may be displayed when connecting with the OIP server and when reading out the lines.

Table 10.5:Event messages

Event message	Cause/solution
No lines configured for the user.	Use the OIP server to check whether the user has been assigned lines.
List of available lines cannot be loaded.	• Use the OIP server to check whether the user has been assigned the necessary access rights. • Check whether the OIP server is running fault-free. Restart the OIP server if necessary.
OIP server software is not compatible.	Check the OIP version notes to see whether the version of the OIPTAPI service provider is compatible with the OIP server.
Log in to OIP server failed. Please check your user name and password.	• Use the OIP server to check whether the user name is correct. • Use the internal phone number and terminal PIN for the login; check whether the terminal PIN has been changed.
Log in to OIP server failed. Please check the server address.	Check whether the correct address of the OIP server has been entered. If you have no success with the DNS name, re-try the connection setup with the OIP server IP address. If this attempt also fails, contact your OIP Administrator.
Initialisation of the CORBAinterfacefailed. Installation aborted.	The connection to the OIP server cannot be set up. Contact your OIP Administrator.
Connection disconnected by the user.	You have disconnected the connection setup to the OIP server.

OIP Exchange drivers for Microsoft Exchange Server 2007 and 2010

If you did not activate the debug mode after installing the OIP Exchange driver, start the configuration via the Start menu entry.

Reproduce the malfunction and save the log files: Windows XP:

c:\Documents and Settings\All Users\Application Data\Mitel\Oip\MsxDrv\Log

Windows Server 2008/2008 R2 and Windows 7/Vista:

c:\ProgramData\Mitel\Oip\MsxDrv\Log

1. On the PC on which the OIP Exchange driver is installed, save the log files from the following directories:
   – Windows XP:
     c:\Document and Settings\All Users\ApplicationData\Mitel\Oip\MsxDrv\Log
   – Windows Server 2008/2008 R2 and Windows 7/Vista:
     c:\ProgramData\Mitel\Oip\MsxDrv\Log
2. On Microsoft Exchange Server, save the Windows event display log files.

OIP Exchange drivers for Microsoft Exchange Server 2003 & 2007

To activate debug mode, first end the Windows service OIP Exchange Service on the Microsoft Exchange Server and then proceed as follows.

1. From the installation directory of the *OIP Exchange driver*, open the configuration file msexchangedriverconfig.oip using a text editor.
2. Change the entry oip.exchangeconnector.debug=0 to oip.exchangeconnector.debug=1 and save the change.
3. Start the Windows service *OIP Exchange Service*.

   Reproduce the malfunction and save the following log files:
4. On Microsoft Exchange Server, from the installation directory save the log files:
   – delprivate.log
   – delpublic.log
   – regprivate.log
   – regpublic.log
   – regresult.txt
5. On Microsoft Exchange Server, save the Windows event display log files.

OIP phone book driver (phone book CDs)

The information listed here refers to the following OIP phone book drivers:

- OIP TwixTel driver (CH)
- OIP Phone Book Drivers (D)

To activate the debug mode first exit the Windows System Service of the corresponding OIP phone book driver and proceed as described here.

1. From the installation directory of the OIP phone book driver open the configuration file ...config.OIP with a text editor.
2. In the paragraph [Config], change the entry DebugLevel=0 to DebugLevel=1 and save the change.
3. Start the Windows service of the corresponding OIP phone book driver.

Reproduce the malfunction and save the following log files:

1. On the PC on which the OIP phone book driver is installed, save the log file "...driver.log" from the installation directory.
2. On the PC on which the driver of the OIP phone book is installed, save the log files of the Windows event display.

OIP phone book driver (ODBC/JDBC)

The information listed here refers to the OIP phone book driver OIP ODBC/JDBC driver.

The debug mode is activated while the OIP ODBC/JDBC driver is being installed.

1. On the PC on which the OIP ODBC/JDBC driver is installed, save the entire *logs* directory from the installation directory.
2. On the PC on which the driver of the OIP ODBC/JDBC is installed, save the log files of the Windows event display.

OIP ATAS-Gateways

The debug mode is activated while the OIP ATAS-Gateway is being installed.

1. On the PC on which the OIP ATAS gateway is installed, save the entire *logs* directory from the installation directory.
2. On the PC on which the driver of the OIP phone book is installed, save the log files of the Windows event display.

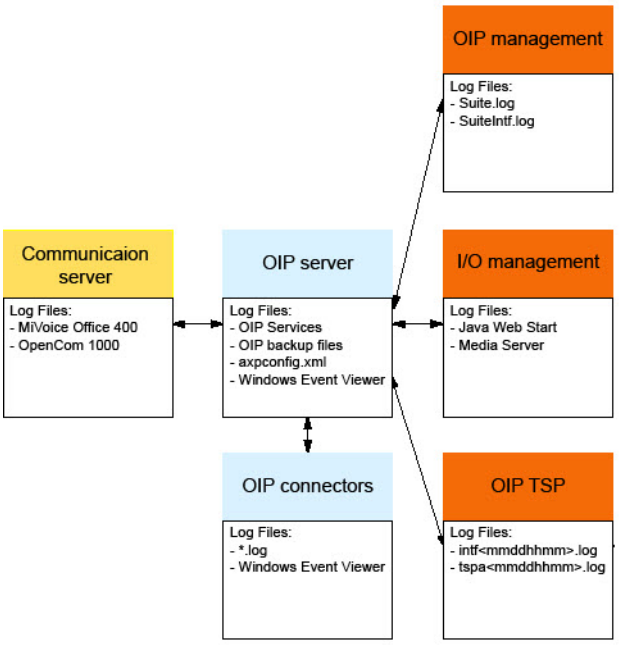
OIP KNX driver

The debug mode is activated while the OIP KNX driver is being installed.

1. On the PC on which the OIP KNX driver is installed, save the entire *logs* directory from the installation directory.

On the PC on which the driver of the OIP KNX is installed, save the log files of the Windows event display

Figure 10.3: Log file overview



MiVoice Office 400

Table 10.6:MiVoice Office 400 log files

Log file	Remarks
MiVoice Office 400 log files:	
• *I-bus* • *ATPC3* • *Error logs*	Switch on the Benni Monitor

OIP server

On the OIP server there are two levels of log files. The upper level comprises the log files that log the general status of the OIP server. They include the log files listed in the following table.

Table 10.7:Level 1 Log files (Sheet 1 of 2)

Log file	Description
OIPServer-yyyy-mm-dd_hh-mm-ss.log	Log file of the OIP server
OIPWebServer-yyyy-mm-dd_hh-mm-ss.log	Log file of the OIP web server
AXP-Logfile-yyyy-mm-dd_hh-mm-ss.log	Log file of the OIP server with detailed information

Table 10.7:Level 1 Log files (Continued) (Sheet 2 of 2)

Log file	Description
axpusers.log	Log file of the OIP users configured in the OIP server

The second level comprises the log files of the individual OIP services. These log files are created or filled with log entries only if the corresponding OIP service has been set to debug. The following table lists the OIP services and the relevant log files.

Table 10.8:Level 2 Log files (Sheet 1 of 7)

OIPService	Log file
Account Service	AccountService_<OIPuserID>_yyyy-mm-dd_hh-mm-ss_0.log
ACD Log Manager	ACDLogManager_yyyy-mm-dd_hh-mm-ss_0.log
ACD Log Service	ACDLogService_yyyy-mm-dd_hh-mm-ss_0.log
ACDManager	ACDManager_yyyy-mm-dd_hh-mm-ss_0.log
ACDService	ACDService_<OIP user ID>_yyyy-mm-dd_hh-mm-ss_0.log
Active Directory Service	ActiveDirectoryService_yyyy-mm-dd_hh-mm-ss_0.log
Agent Manager	AgentManager_yyyy-mm-dd_hh-mm-ss_0.log
Agent Service	AgentService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Alarm Driver	AlarmReceiver_yyyy-mm-dd_hh-mm-ss_0.log TCP-IN-<PBX IP-address>-ON-1062.log
Alarm Service	AlarmService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Alpha & Quick Dial Service	AlphaService_yyyy-mm-dd_hh-mm-ss_0.log
Buddy Manager	BuddyManager_yyyy-mm-dd_hh-mm-ss_0.log
Buddy Service	BuddyService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Calendar Manager	CalendarManager_yyyy-mm-dd_hh-mm-ss_0.log
Calendar Service	CalendarService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
<Default ¬¹ Font>Calendar Synchro nization Service	CalendarService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Call Logging Driver	TaxReceiver_yyyy-mm-dd_hh-mm-ss_0.log TCP-IN-<PBX IP-address>-ON-1080.log
Call Logging Manager	TaxManager_yyyy-mm-dd_hh-mm-ss_0.log
Call Logging Service	TaxService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log

Table 10.8:Level 2 Log files (Continued) (Sheet 2 of 7)

OIPService	Log file
Call Service	CallService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Client Utility Service	UtilsService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
CLIPService	CLIPService_yyyy-mm-dd_hh-mm-ss_0.log
Configuration Profile Manager	ConfigProfileManager_yyyy-mm-dd_hh-mm-ss_0.log
Configuration Profile Service	ConfigProfileService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
ConfigurationService	ConfigurationService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
DasTelefonbuch Directory Service	ThePhoneDirectoryService_yyyy-mm-dd_hh-mm-ss_0.log
Database Driver	DatabaseDriver_yyyy-mm-dd_hh-mm-ss_0.log
Directory Manager	DirectoryManager_yyyy-mm-dd_hh-mm-ss_0.log
Directory Service	DirectoryService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Display Manager	DisplayManager_yyyy-mm-dd_hh-mm-ss_0.log
Display Service	DisplayService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Event Service	EventService_yyyy-mm-dd_hh-mm-ss_0.log
Fax Manager	FaxManager_yyyy-mm-dd_hh-mm-ss_0.log
Fax Service	FaxService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Feature Service	FeatureService_yyyy-mm-dd_hh-mm-ss_0.log
Flow Manager	FlowManager_yyyy-mm-dd_hh-mm-ss_0.log
Flow Service	FlowService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Function Key Manager	FunctionKeyManager_yyyy-mm-dd_hh-mm-ss_0.log

Table 10.8:Level 2 Log files (Continued) (Sheet 3 of 7)

OIPService	Log file
Function Key Service	FunctionKeyService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
I/O Manager	IO-Manager_yyyy-mm-dd_hh-mm-ss_0.log
I/O Service	IO-Service-<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Jabber Driver	JabberDriver_yyyy-mm-dd_hh-mm-ss_0.log
Journal Manager	JournalManager_yyyy-mm-dd_hh-mm-ss_0.log
Journal Service	JournalService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Key Configuration Service	KeyService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
LDAP Directory Service	LDAPDirectoryService_yyyy-mm-dd_hh-mm-ss_0.log
License Manager	LicenseManager_yyyy-mm-dd_hh-mm-ss_0.log
License Service	LicenseService_yyyy-mm-dd_hh-mm-ss_0.log
Line Service	LineService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Load Balancing Service	LoadBalancingService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Location Manager	LocationManager_yyyy-mm-dd_hh-mm-ss_0.log
Location Service	LocationService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Log Service	Log_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Login Service	SystemLogin_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Media Manager	MediaManager_yyyy-mm-dd_hh-mm-ss_0.log
MessageManager	MessageManager_yyyy-mm-dd_hh-mm-ss_0.log
Message Service	MessageService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log

Table 10.8:Level 2 Log files (Continued) (Sheet 4 of 7)

OIPService	Log file
Naming Service	DistributedNameService_yyyy-mm-dd_hh-mm-ss_0.log
Notepad Service	NotepadService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Notification Manager	NotificationManager_yyyy-mm-dd_hh-mm-ss_0.log
Notification Service	NotificationService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
ODBC/JDBCDirectory Service	JDBCDirectoryService_yyyy-mm-dd_hh-mm-ss_0.log
Operator Service	OperatorService<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
PBX Driver Ascotel	ASNMP-<PBX IP-address>_yyyy-mm-dd_hh-mm-ss_0.log ATNS-<PBX IP-address>_yyyy-mm-dd_hh-mm-ss_0.log ATNSDriver-<PBX IP-address>_yyyy-mm-dd_hh-mm-ss_0.log CTIDriverAscotel-<PBX IP-Adress>_yyyy-mm-dd_hh-mm-ss_0.log DisplayDriver_yyyy-mm-dd_hh-mm-ss_0.log PBXConfigDriver-<PBX IP address>_yyyy-mm-dd_hh-mm-ss_0.log PBXDriverAFP-<PBXIPaddress>_yyyy-mm-dd_hh-mm-ss_0.log PBXDriverAscotel-<PBXIPaddress>_yyyy-mm-dd_hh-mm-ss_0.log PBXDriverInfolink-<PBX IP address>_yyyy-mm-dd_hh-mm-ss_0.log TCP-OUT-<PBXIPaddress>-1061_yyyy-mm-dd_hh-mm-ss_0.log TCP-OUT-<PBXIPaddress>-1070_yyyy-mm-dd_hh-mm-ss_0.log TCP-OUT-<PBXIPaddress>-1074_yyyy-mm-dd_hh-mm-ss_0.log TCP-OUT-<PBXIPaddress>-1088_yyyy-mm-dd_hh-mm-ss_0.log
PBX Information Service	PBXInfoService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log

Table 10.8:Level 2 Log files (Continued) (Sheet 5 of 7)

OIPService	Log file
PBX Manager	PBXManager_yyyy-mm-dd_hh-mm-ss_0.log
PBX Setup Manager	PBXSetupManager_<OIP-user ID>_yyyy-mm-dd_hh-mm-ss_0.log
PBX Setup Service	PBXSetupService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
PISN Directory Service	PISNSubscriberDirectoryService_yyyy-mm-dd_hh-mm-ss_0.log
Private Card Directory Service	PhoneCardDirectoryService_yyyy-mm-dd_hh-mm-ss_0.log
Private Directory Service	PrivateDirectory_yyyy-mm-dd_hh-mm-ss_0.log
Public Directory Service	PublicDirectory_yyyy-mm-dd_hh-mm-ss_0.log
PUMManager	PUMManager_yyyy-mm-dd_hh-mm-ss_0.log
PUMService	PUMService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
RegistrationManager	RegistrationManager_yyyy-mm-dd_hh-mm-ss_0.log
Registration Service	RegistrationService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Routing Manager	RoutingManager_yyyy-mm-dd_hh-mm-ss_0.log
Routing Service	RoutingService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
RSS Driver	RSSDriver_yyyy-mm-dd_hh-mm-ss_0.log
Security Service	SecurityService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Server Utility Service	UtilityService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Service Manager	axpservices-yyyy-mm-dd_hh-mm-ss.log
Shortdial Directory Service	ShortDialDirectoryService_yyyy-mm-dd_hh-mm-ss_0.log
SMTPDriver	SMTPDriver_yyyy-mm-dd_hh-mm-ss_0.log

Table 10.8:Level 2 Log files (Continued) (Sheet 6 of 7)

OIPService	Log file
Subscriber Configuration Manager	SubscriberConfigManager_yyyy-mm-dd_hh-mm-ss_0.log
Subscriber Configuration Service	SubscriberConfig_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Subscriber Directory Service	SubscriberDirectoryService_yyyy-mm-dd_hh-mm-ss_0.log
System User Directory Service	SystemUserDirectoryService_yyyy-mm-dd_hh-mm-ss_0.log
Test Manager	TestManger_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Test Service	TestService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Ticket Service	TicketService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Time Service	TimeService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
TTS Manager	TTSManager_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
TwixTel Directory Service	TwixTelDirectoryService_yyyy-mm-dd_hh-mm-ss_0.log
User Preferences Service	UserPreferences_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
User Profile Manager	UserProfileManager_yyyy-mm-dd_hh-mm-ss_0.log
User Profile Service	UserProfileService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
User Service	UserServices-<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Voice Mail Manager	VoiceMailManager_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log
Voice Mail Service	VoiceMailService_<OIP-user-ID>_yyyy-mm-dd_hh-mm-ss_0.log

Table 10.8:Level 2 Log files (Continued) (Sheet 7 of 7)

OIPService	Log file
WEB Server Service	Output on console if the OIP server is started in console mode.

1. Activate the debug mode for all OIP services. The log level should be set to debug. Please note that activating the debug mode restricts the runtime behaviour of the OIP server.
2. From the installation directory of the OIP server, save the entire *logs* directory.
3. From the installation directory of the OIP server, save the entire *backup* directory.
4. From the OIP server installation directory, save the OIP configuration file *axpcon- fig.xml*.
5. Save the log files of the Windows event display.

Mitel OfficeSuite

1. Activate debug mode.
2. Backup the log files Suite.log and SuiteIntf.log from the following directory: *c:\Users\<User name>\AppData\Local\Mitel\Suite\Log*

MiVoice 1560 PC Operator

1. Activate debug mode.
2. Back up the log files Mitel1560.log and Mitel1560_Intf.log from the directory *c:\User\<User name>\AppData\Local\Mitel\Mitel1560\Log*.

Java-based OIP applications

1. Delete the temporary internet files in the Java Control Panel (Control Panel\Java). Deleting the Temporary Internet Files deletes all downloaded applications; the next time you start up the OIP application, the application files will again be downloaded.
2. From the Java Control Panel activate debugging from the Advanced tab.
3. Reproduce the malfunction.
4. From the user profile directory ...\Sun\Java\Deployment\log, save the log file javaws*.log.

Operator applications

1. Activate debug mode.
2. From the user profile directory ...\Documents and Settings\All Users\Application Data\Mitel, save the entire Logs directory.

Media Server

The Media Server is installed with an OIP softphone: From the user profile directory save the log file media.log.

OIP TAPI service provider

1. Activate the debug mode of the OIP TAPI service provider.
2. Restart the Windows Telephony Service.
3. Save the configured Log directory.
   - intf<mmddhhmm>.log
   - tspa<mmddhhmm>.log

If an error occurs, the event messages in the following table may be displayed when connecting with the OIP server and when reading out the lines.

Table 10.9:Event messages (Sheet 1 of 2)

Event message	Cause/solution
No lines configured for the user.	Use the OIP server to check whether the user has been assigned lines.
List of available lines cannot be loaded.	• Use the OIP server to check whether the user has been assigned the necessary access rights. • Check whether the OIP server is running fault-free. Restart the OIP server if necessary.
OIP server software is not compatible.	Check the OIP version notes to see whether the version of the OIPTAPI service provider is compatible with the OIP server.
Log in to OIP server failed. Please check your username and password.	• Use the OIP server to check whether the username is correct. • Use the internal phone number and terminal PIN for the login; check whether the terminal PIN has been changed.
Log in to OIP server failed. Please check the server address.	Check whether the correct address of the OIP server has been entered. If you have no success with the DNS name, re-try the connection setup with the OIP server IP address. If this attempt also fails, contact your OIP Administrator.

Table 10.9:Event messages (Continued) (Sheet 2 of 2)

Event message	Cause/solution
Initialisation of the CORBAinterfacefailed. Installation aborted.	The connection to the OIP server cannot be set up. Contact your OIP Administrator.
Connection disconnected by the user.	You have disconnected the connection setup to the OIP server.

OIP phone book driver (phone book CDs)

The information listed here refers to the following OIP phone book drivers:

- OIP TwixTel driver (CH)
- OIP Phone Book Drivers (D)

To activate the debug mode first exit the Windows System Service of the corresponding OIP phone book driver and proceed as described here.

1. From the installation directory of the OIP phone book driver open the configuration file ...config.OIP with a text editor.
2. In the paragraph [Config], change the entry DebugLevel=0 to DebugLevel=1 and save the change.
3. Start the Windows service of the corresponding OIP phone book driver.

Reproduce the malfunction and save the following log files:

1. On the PC on which the OIP phone book driver is installed, save the log file "...driver.log" from the installation directory.
2. On the PC on which the driver of the OIP phone book is installed, save the log files of the Windows event display.

OIP phone book driver (ODBC/JDBC)

The information listed here refers to the OIP phone book driver OIP ODBC/JDBC driver.

The debug mode is activated while the OIP ODBC/JDBC driver is being installed.

1. On the PC on which the OIP ODBC/JDBC driver is installed, save the entire *logs* directory from the installation directory.
2. On the PC on which the driver of the OIP ODBC/JDBC is installed, save the log files of the Windows event display.

OIP ATAS-Gateways

The debug mode is activated while the OIP ATAS-Gateway is being installed.

1. On the PC on which the OIP ATAS gateway is installed, save the entire *logs* directory from the installation directory.
2. On the PC on which the driver of the OIP phone book is installed, save the log files of the Windows event display.

OIP KNX driver

The debug mode is activated while the OIP KNX driver is being installed.

1. On the PC on which the OIP KNX driver is installed, save the entire *logs* directory from the installation directory.
2. On the PC on which the driver of the OIP KNX is installed, save the log files of the Windows event display.