OFFICEMASTER SUITE 8 ADMINISTRATOR'S MANUAL

Ferrari electronic AG
Ruhlsdorfer Strasse 138
14513 Teltow

info@ferrari-electronic.de
Phone +49 3328 45590
Fax +49 3328 455960
https://ferrari-electronic.de

Table of contents

4. Getting started

5. Configuration programs

6. Base Configuration

7. Connector for Microsoft Exchange

8. OfficeMaster Suite call routing

9. Operation of the messaging server

10. Configuration of each Component

Legal information

version 1.5

March 1st, 2024 | Ferrari electronic AG

UNIFIED COMMUNICATIONS
© 2022-2024 Ferrari electronic AG
www.ferrari-electronic.de

OfficeMaster is a registered trademark of Ferrari electronic AG. All rights reserved. No part of this manual may be copied in any way without the written permission of Ferrari electronic AG. All trademarks mentioned in this manual are registered trademarks of the respective trademark owners. Changes to the software and manual are reserved, even without prior notice.

The information contained in this book has been compiled with the utmost care. Nevertheless, erroneous information cannot be entirely be excluded. Ferrari electronic AG is not liable for any errors and their consequences. Address hints and comments please to:

info@ferrari-electronic.de

This manual contains information about the OfficeMaster Suite 8 in all variants. The target audience are administrators who are using this solution and want to configure it.

Version history and imprint

Review	date	changes
1.5	1.4.2024	Chapter Operation, Section Administrators, extended for 8.1.0
1.4	13.9.2023	Chapter Operation, Section Firewall
1.3	13.7.2023	Chapter monitoring moved to Operation, extended for 8.0.1
1.2	19.4.2023	Chapter monitoring
1.1	1.2.2023	Updates and corrections
1.0	1.9.2022	Initial Release based on OfficeMaster Suite Release 8.0.0

Editor:

Ferrari electronic AG
Ruhlsdorfer Strasse 138
(DE) 14513 Teltow

Internet:

www.ferrari-electronic.de

Phone:

+49 3328 455 90

Fax:

+49 3328 455 960

E-mail:

info@ferrari-electronic.de

Authors:

C Helbing, M Riebe, B Mittelstedt, J Nimpadu, H Miersch, A Fechner, M Oberthür, R Fiedler

1. Introduction

1.1. Product evolution

The OfficeMaster Suite is an enhanced logical development of the communication classic *"ferrariFAX"* from Ferrari electronic.

With the product ***"ferrariFax"*** and the first intelligent fax card, Ferrari electronic detached the classic fax from fax machines as early as 1987 and integrated it into company networks.

In the years that followed, many **deep integrations** were created both in telephone systems (e.g. Avaya, Mitel, Auerswald), groupware (e.g. Microsoft Exchange or Lotus Notes) and in third-party systems (e.g. SAP, Microsoft 365).

With the announcement of the discontinuation of the ISDN telephone standard in 2016, Ferrari electronic AG already had the next technology available to communicate directly on the new SIP trunks. ***DirectSIP*** became an integral part of the ***OfficeMaster Suite*** and enabled for the first time - as a pure software solution - the legally compliant exchange of documents in IP networks.

As the next milestone, Ferrari electronic introduced ***"Next Generation Document Exchange - NGDX"*** in 2019, the next generation of document exchange. With ***NGDX***, the classic fax was freed from the last shackles of the "old" technology.

The classic fax became a digital document!

This document is no longer a 200dpi b/w image, but a **full color**, **searchable** and **archivable** PDF document that is **fast** (approx. 150 pages per minute), dual **encrypted** (both transport via TLS and the document) and **legally secure** via a qualified transmission report.

1.2. Office Master Suite 8

In version 8 of the ***OfficeMaster Suite***, the focus is on the one hand on robustness of the IP worlds and the integration of new and expanded communication channels into the existing infrastructure without changing the usual work processes or workflows. On the other hand, in the optimal preparation of received and sent documents for the new requirements of the digital working world.

The core features of OfficeMaster Suite 8 include:

- Extended web interface for connecting 3rd party systems, e.g. electronic mail letter (E-Postbrief in Germany)
- Integrated OCR (Optical Character Recognition) on incoming documents
- Sending X invoices on the Peppol network
- Integration with Microsoft Dynamics 365 CRM
- Document dispatch via cloud relay

1.2.1. Requirements

For detailed information on the requirements, please refer to the OfficeMaster Suite 8 data sheet. The following table provides an overview of the system requirements:

Parameters	**Value**
	Windows Server 2016/2019/2022
supported operating systems (server)	
supported operating systems (client)	Windows 10 and Windows 11
min. number of CPUs	2
min. main memory	8GB RAM
min. hard drive capacity	80GB SSD
Landline connection	SIP trunk or ISDN (OfficeMaster Gate)
Virtualization	ESX or Hyper-V

Depending on the scaling (>30 simultaneous fax channels), more CPUs and more RAM are required.

1.2.2. New functions

The following sections describe the essential functional enhancements that have been implemented in the OfficeMaster Suite Version 8.0.0.

Better support for cloud installations

Customers are increasingly installing the OfficeMaster Suite for cloud usages (mostly using the Azure Marketplace offer). In this scenario, a SIP trunk, Microsoft 365 (Azure AD, Exchange Online) and possibly a CRM are connected. The entire environment runs in the cloud.

To better support such use cases, a new browser-based configuration utility was created, a Web API connector was added, and improvements were made to AuthGateKeeper.

The configuration program can be accessed from https://{msgSrvHost}/cfg. The new configuration program does not support functionalities that do not make sense in a cloud environment (e.g. Notes, ISDN gateway search, SAP). There are functionalities in other areas (e.g. log analysis, dashboard) that go beyond the previous configuration program. Since the web-based configuration program cannot yet register apps in Azure AD, it is considered a technical preview. The documentation for Web API Connector can be found in https://{msgSrvHost}/webapi/v2/doc/ (the Web API component must be running).

Adaptation to changes in the IT landscape

The Exchange Online Connector has been completely redesigned to accommodate Microsoft's originally targeted September 30, 2022 shutdown of Exchange Web Services (EWS) app registration. The new Exchange Online Connector uses the Graph API with OAuth 2.0 authentication. Support for Windows Server 2022 and Office 2021 is provided with OfficeMaster 8.0.0 as well as support for Windows 11 clients.

Improvements for fax transmission

With the integration of Tesseract in addition to the B&L OCR engine, the OCR function is now available to all users of the OfficeMaster Suite without additional license costs. By default, if Tesseract is found on the system and the OCR functionality is switched on, all incoming documents will be provided with a text layer, allowing users to easily extract text (e.g. cut & paste).

An additional NGDX operating mode allows file transfer via a cloud relay operated by Ferrari electronic AG. The documents are broken down into pieces (shards), these are individually encrypted with a symmetric key and the key exchange with the recipient is encrypted again on the telephony route.

A line test function has been implemented. When a special number is called, an operating mode is adopted in which all modem operating modes are carried out and transmission errors are counted. As a result, the user receives a PDF file with an error report.

Sending faxes in geographically large VPNs with poor quality of service or high latency (round-trip time) is now possible if SIP2 and

the fipMediaServer are used. Thereby the media server should be placed close to the telephone connection/SIP trunk and the central messaging server will be able to control the fax workflow even over relatively “bad” connections. This allows SIP environments to increase the independence of the quality of the network from the OfficeMaster Gate-based solutions.

The robustness of the fax stack against carrier losses due to packet losses on VoIP routes has been increased.

New transmission paths

The E-POST letter and the X-Invoice were added as order types and their transmission is supported by new sending components.

In combination with the web API component, faxes, SMS, print jobs, letters and X invoices that can be sent from an ERP or CRM system. Various scenarios are implemented here after the release. The first will be the connection of fax, SMS, letter, X-invoice to a Dynamics 365 via the new web API connector of an OfficeMaster Suite from the Azure Marketplace.

Operational improvements

OfficeMaster Suite 8 includes the option of emptying (draining) the server. No new orders will be accepted, but orders that are already being processed will still be processed. On the one hand, this helps with maintenance work or with a server move. On the other hand, the server also goes into drain mode if (configurable) an important SIP trunk fails or the connection to a mail system (e.g. Exchange Online) is interrupted.

An SNMP plugin for the Windows SNMP service was created for server monitoring and the OfficeMaster Suite was expanded to include a large number of counters.

Each component configuration dialog has a contextual online help page.

Internal changes

The unique ID (UID) of the job files used to be 32 bits long. This could lead to collisions when job files were migrated from one messaging server to another (e.g. update, server move). In version 8, the UID was extended to 64 bits and a process for migrating from 32-bit UIDs to 64-bit UIDs was implemented.

The same library for regular expressions (PCRE2) is used everywhere in OfficeMaster Suite 8. From the user’s point of view, the same regular expression syntax is finally used everywhere. For backwards compatibility, some expressions are now modified on load.

In individual cases (redundant dispatch routes), the calculated job routing in previous versions could depend on the start order of the transmit components operated in parallel. Since this could vary from start to start (race), the routing was correct in these cases, but not deterministic. OfficeMaster Suite 8 solves this problem by being able to assign routing priorities. This allows deterministic routing to be established.

The OfficeMaster Suite 8.0.0 is built with Visual Studio 2022 and uses .Net Framework 6.

1.2.3. Removed or no longer supported features

ISDN interfaces on OfficeMaster Gates continue to work with OfficeMaster 8.0.0, but are no longer recommended for new configurations. The same applies to jcsim, whose use cases can be adopted by DirectSIP's loop mode of operation.

The old converter conv was already replaced by cmdconv in OfficeMaster 7; this time it was completely removed in version 8.0.0.

OfficeMaster Suite 8 supports three SMS sending methods:

- Landline SMS via DirectSIP (or omcums)
- GSM modem with LAN interface (AT commands via TCP) e.g. ConiuGo
- Provider SMS via SMPP

The other SMS variants (UCP, web interface, modem via UART, etc.) are either outdated or cannot be used in virtualized environments and are therefore no longer recommended. For updates from existing customers, however, the function will still be retained in OfficeMaster 8.0.0.

The OfficeMaster GateConfig, which is required to configure OfficeMaster Gates, is no longer part of the OfficeMaster Suite. Customers who still use ISDN can install them separately.

2. Overview

2.1. NGDX, Fax, Voicemail and SMS

The *OfficeMaster Suite* is a communication solution for use in heterogeneous computer networks. With the *OfficeMaster Suite* you can send and receive Documents and messages electronically as NGDX, Fax, SMS and E-mail attachments.

> NGDX, fax and SMS messages can be sent and received via ISDN or via IP networks (mixed environments are supported).

The voicemail solution integrated in the *OfficeMaster Suite* takes calls and sends an e-mail to the respective mailbox of the user with the recording as an attachment.

For all functions, special attention is paid to the integration of OfficeMaster into the existing environment.

> The *OfficeMaster Suite* provides special connectors for *Microsoft Exchange Server*, *Exchange Online / Microsoft 365*, *Notes/Domino Server* and *SAP*. It also serves customers without a mail system with an integrated web client for the users.

The following table compares the individual connectors of the *OfficeMaster Suite*. Features marked as optional can be extended by additional software licenses or hardware to extend the respective main product.

Table 2.1: OfficeMaster Suite product overview

General properties

	SMTP	**Exchange**	**Notes**	**SAP**	**Web\ Connector**
User Management	Proprietary, LDAP	Active Directory	Name and Address Book	SAP user base	Proprietary (SQL), using the AD users

Fax features

	SMTP	**Exchange**	**Notes**	**SAP (optional)**	**Web Connector**
Fax dispatch	mail client	Microsoft Outlook, OWA, mail client	Notes client	SAP frontend	Web Client
Fax Reception	mail client	Microsoft Outlook, OWA, mail client	Notes client	SAP frontend	Web Client
Bulk Fax	Anonymized circular fax and personalized serial fax	Anonymized circular fax and personalized serial fax	Anonymized circular fax and personalized serial fax	Depending on SAP application	Anonymized circular fax and personalized serial fax
Local Fax Printer Driver (Windows)	Calling Microsoft Outlook	Calling Microsoft Outlook	Calling Notes	-	Web client call
Fax retrieval	ISDN	ISDN	ISDN	ISDN	ISDN
Central conversion of file attachments	Yes	Yes	Yes	Yes	Yes
File-based job interface	Yes	Yes	Yes	Yes	Yes
Print-based job interface	Line Printer Daemon	Line Printer Daemon	Line Printer Daemon	Line Printer Daemon	Line Printer Daemon
Connection to network scanner	Yes	Yes	Yes	Yes	Yes
Character recognition (OCR)	Line Printer Daemon	optional	optional	optional	optional
Electronic fax signature	optional	optional	optional	optional	optional

	SMTP	Exchange	Notes	SAP (optional)	Web Connector
(mass signature)					

Short Messages/SMS

	SMTP	Exchange	Notes	SAP	Web Connector
Optional transmit/receive hardware	Landline SMS, SMS via SMPP	Landline SMS, SMS via SMPP	Landline SMS, SMS via SMPP	Landline SMS, SMS via SMPP	Landline SMS, SMS via SMPP
Sending and receiving SMS	mail client	MicrosoftOutlook	Notes client	SAP frontend	Outlook, Notes Client, Mail Client
interface for alerting/ monitoring	console program	console program	console program	console program	console program
Split more than 160 characters into multiple messages	Yes	Yes	Yes	Yes	Yes

email

	SMTP	Exchange	Notes	SAP	Web Connector
E-mail delivery	Network Printing (lpd)	Network Printing (lpd)	Network Printing (lpd)	SAP frontend	Network Printing (lpd)
E-mail receipt	-	-	-	SAP frontend	-
Automatic ZIPing of attachments	-	-	-	Yes	-
Electronic signing of attachments	optional	optional	optional	optional	optional

Voicemail

	SMTP	Exchange	Notes	SAP	Web Connector
Voicemail dispatch	Email	Email	Notes client	-	Web Client
Voicemail Query	PC and Telephone	PC and Telephone	PC and Telephone	-	PC and Telephone
Message Waiting Indication	Yes	Yes	Yes	-	Yes

2.1.1. IP and ISDN connection

OfficeMaster Suite is installed on a network computer running Microsoft Windows and provides users with fax, SMS and voicemail communication services. For this purpose, ISDN/IP interfaces are used from the existing telephone system or directly from a telephone service provider.

For the ISDN/IP connection, Ferrari electronic AG offers with OfficeMaster Gate offers a product range, which consists of professional ISDN/IP\ hardware in different configuration levels. SIP trunks and IP\ telephone systems will have a direct connection (DirectSIP) and therefore recommended without additional hardware or middleware.

Short messages are sent and received as standard fixed-network text messages via the available existing SIP trunks or ISDN connections. Since fixed line SMS from some providers via call-by-call is not supported, sending and receiving can also be done via an Internet service provider (via SMPP).

2.1.2. Integration with Microsoft Exchange Server 2013-2019

OfficeMaster Suite integrates with a special SMTP connector in *Microsoft Exchange Server 2013-2019*. All communication services are provided with a single connector recorded on any server within the Exchange organization can be operated. An installation of OfficeMaster Suite directly on the Exchange Server is under consideration additional installation steps possible. But mostly thanks of the virtualization possibilities are avoided.

The OfficeMaster Exchange Connector uses the *Active Directory Service Interface* (*ADSI*) to access the Active Directory to read stored user data. All relevant user parameters for fax, SMS and voicemail are maintained in the Exchange Management console. Already existing AD fields are used where possible to not need to extend the Active Directory schema.

Communication between Exchange and the connector takes place via the *Simple Mail Transfer Protocol* (*SMTP*), which is used worldwide as the basis for connecting independent mail clients to different mail servers. Sent and received e-mails as well as status messages are recorded transfer. For the personalized answering machine function the *Messaging Application Programming Interface* (*MAPI*) uses, which provides uniform access to mailboxes guaranteed. For Exchange 2013 - 2019 is used as an alternative to MAPI access to the *Exchange Web Services* (*EWS*) set.

> **Note!**
> Since both the Active Directory and the Exchange Server access via ADSI resp. MAPI and EWS resp. Graph is only granted if certain permissions are available when starting up OfficeMaster. Please take special care with the service account that needs to be set the use the connectors.

2.1.3. Integration with Notes/Domino

OfficeMaster Suite accesses the data stored in the Domino directory user data to all necessary information for fax, SMS and voicemail for the respective user or user group. To use advanced options, OfficeMaster reads information from defined Notes fields, whereby these can in turn be integrated into any masks.

Fax messages are received as Notes mail to the respective assigned mailbox. By converting to Notes mails are also Functions such as forwarding or retrieving mail-in databases supports. Outgoing faxes are managed centrally by the OfficeMaster Suite converted with the Notes client. In this way, all Notes documents can be sent by fax send without the need for user adjustments. Within Notes, faxes and SMS are treated like e-mails - under Use of all Notes\ mechanisms. So is an integration of Workflow applications can be implemented in the sending process.

A powerful answering machine is integrated into the computer network for the voice function of the *OfficeMaster Suite*. The prerequisite for the use of it is a telephone system, that redirects incoming calls to the voice server. Received voice messages are sent to the user in Lotus Notes as Notes mail with an audio file attached. The user can listen to the messages either by routing them to his phone, through sound card or Play PC speakers or listen to them remotely

2.1.4. Integration with various SMTP mail systems

The *OfficeMaster Suite* has the option of sending and receiving messages via SMTP. This means that every e-mail server can be addressed and provided the appropriate permissions, messages can be sent to different user mailboxes. One Integration into almost any mail system is therefore possible with OfficeMaster.

If a global directory service can also be accessed, the *OfficeMaster Suite* uses the user information stored there for the administration of the phone numbers.

Without access to external directory services, both user data and messages can be stored in the local user memory of the OfficeMaster Suite.

2.1.5. Integration into SAP R/3, S/4HANA or NetWeaver

Communication with SAP takes place via *SAPconnect*. This is the uniform communication interface of *SAP AG*. *SAP connect* is based on Remote Function Calls (RFC) over TCP/IP in LAN/WAN environments.

The *OfficeMaster Suite* receives the document to be sent via RFC with the associated recipient list and sends it using from OfficeMaster Gate as a fax or forward it to the e-mail address in-house email server. If the shipment has taken place, the status reported is assigned back to R/3, where he was assigned to the Business Workplace located transmission document.

In *SAP Version 4.7*, *SAPconnect* was extended to include SMTP as the transfer protocol between SAP and the communication partners. The send request is not sent via RFC, but via SMTP to *OfficeMaster*. *OfficeMaster* takes care of the dispatch and informs the SAP system via e-mail about the dispatch status. When starting up *OfficeMaster* it should be decided, depending on the installation, whether the RFC interface is to be used or the SMTP interface (the SMTP interface offers a smaller range of functions due to the concept).

OfficeMaster receives from R/3 for the central conversion of the Fax documents files in the formats

Printer Common Language (PCL), *Postscript* (PS) or *Portable Document Format* (PDF). These will be converted either with the internal PCL converter, with *Adobe Acrobat Reader* or with *Ghostscript* into a supported bitmap graphics format.

With *Connector for SAP*, buyers can send orders directly from *Materials Management* (MM), sellers can send offers from *Sales and Distribution Processing* (SD) and accountant notifications from *Financial Accounting* (FI) without having to print out the documents beforehand. Through the complete integration into SAP is the dispatch from almost every SAP application possible. The business documents are either sent as graphics by fax or as a PDF by email.

Received messages and status reports are stored in *SAP Business Workplace*. An Alarm from the *Alert Manager* (RZ20) can be automated when exceeding or falling below Thresholds.

2.1.6. Automatic document delivery via NGDX, fax and email

The fax and e-mail function of OfficeMaster can be quickly and easily be integrated via LPD network printing into an existing ERP or other application programs. For this purpose, a control

command is integrated once in the form used by the merchandise management or the application for the printout, which contains the NGDX-, fax number or the e-mail address of the recipient. The e-mail address of the recipient as it is stored in the master data of the application. After OfficeMaster has received the document by print, the control command is interpreted and send control command is interpreted and send job is sent.

Optionally, the document can be provided with an electronic signature before transmission. After the document has been sent, the sender receives the final status message by e-mail in his mailbox.

2.1.7. fax-on-demand server

Most fax machines offer two additional operating modes in addition to normal fax transmission:

- The targeted retrieval of documents that another fax subscriber has provided and
- the provision of documents for retrieval by another Attendees.

During fax polling, the fax number of the subscriber who is known to have provided a document for polling is dialed. This document is transmitted after the connection is established. With OfficeMaster, practically any number of documents can be made available for fax polling. Each of the documents can be reached under a different fax number.

> **Note!**
> The fax-on-demand server only works with OfficeMaster Gate.

2.1.8. Web Connector and Web Services

With the OfficeMaster WebServices, Ferrari electronic AG provides an Interface for your own applications to use the UM services of OfficeMaster Suite. It is possible to use both a programming environment and a programming language that standardized protocols XML, SOAP and WSDL. The WebServices are based on the same basis as the *OfficeMaster Suite* client. A separate connector may be required for this.

2.2. Architecture of the OfficeMaster Suite

OfficeMaster Suite consists of the *Messaging Server*, which is the basic technology of the products of Ferrari electronic. This basic technology impresses above all by modularity, load distribution, robustness, controllability, operating system independence and expandability. The messaging server is not a single program, but a comprehensive but simple system, consisting of a series of basic components, which ensure the basic process and operation. The basic components are supplemented with transmission / reception and Connector components according to the licenses acquired. Table 2.2 shows the currently available components.

All components communicate with the controller component (CTRL) via the network. To enable load balancing, components can be started multiple times if they are sufficiently licensed. The OfficeMaster Suite is configured via the supplied configuration program – *Messaging Server Configuration*.

The *Messaging Server Configuration* can be started on any computer running Microsoft Windows provided that the computers have network access and an IP connection to the Messaging Server.

OfficeMaster Suite supports aspects such as Reliability, scalability, regional distribution and virtualization in addition to its numerous Functionalities through the individual components.

These aspects are briefly described below. A detailed Explanation is beyond the scope of this manual. Further questions can be answer in www.ferrari-electronic.de by reading the available whitepapers or by consulting the technical product marketing of Ferrari electronic AG (hotline@ferrari-electronic.de).

Table 2.2: Overview of the components

Component Type	**Component Name**
Basic Components	Starter (START), Controller (CTRL), Unique ID Server (UID), Configuration Server (CFG), Distributed File System (SNFS), Converter (CONV), Message Control Outgoing (SPLIT) and Incoming (DIST), Undeliverable Messages (UNDLVRBL), LUA Interpreter (LUA), Base Converter (baseconv), Advanced OLE Converter (oleconv), Commandline Converter (cmdconv), Configurations Proxy (CFGPROXY), Gatekeeper (fgatekeeper)
Sender / receiver for fax and SMS	OfficeMaster Gate (OMCUMS), CAPI connection (JCISDN), DirectSIP (SIP)
Sender / receiver for email	E-mail sender (SMTPTX), e-mail recipient (SMTPRX)
Sender / Receiver for Voicemail	Voice Server (VOICE)
Connector for Microsoft Exchange	UMS connector (MSX2KGATE) and (FMSXBCSGATE)
Connector for Notes/Domino	Domino Fax/SMS and Voice Gateway (NOTESCONN)
Connectors for mail servers	Mail Gateway for Fax and SMS (MAILGW), Gateway for Voice (UNIVOICE)
Connectors for SAP	RFC connector (SAPCONN),(SAPCONNU), SMTP gateway (SAPSMTP)
Other Components	File interface (FILEGW), Web-API connector (webapi)
Components for Printing	Automatic printing (PRINTGW), network printing (LPD)

2.2.1. Reliability / high availability

A unified communications system is part of a complex embedded infrastructure from mail servers, communication controllers and telephone systems. For assessing the availability of these Infrastructure, the components must be considered individually and in their interaction. The OfficeMaster Suite has built-in monitoring routines that check if all required programs are running. If a program ended unexpectedly, it will be restarted accordingly.

There are installations where both the mail server and the computer on which the OfficeMaster Suite was installed are designed to be fail-safe and where the Telephone systems are set up as a fail-safe system network. In such concepts is either a corresponding number of SIP-Trunks routed to the OfficeMaster Suite, or one or more OfficeMasters Gate are connected to the telephone systems via ISDN/IP and via a network connection to the computer on which the Office Master Suite is running.

If OfficeMaster Suite or OfficeMaster Gate fail, they can no longer be addressed by the telephone system. The telephone system forwards all calls to another controller or server.

2.2.2. Scalability

OfficeMaster Suite consists of a larger number of components, too each of which owns a configuration set. The components communicate among themselves via a network protocol (based on TCP/IP), so that they can be installed on different computers.

The distribution on different computers (scalability) avoids Performance bottlenecks, can increase availability through redundant Structures or can include multiple locations in one installation.

2.2.3. Cross-site connection

Many companies and organizations are in more than one location active and have several national or international branches. As a rule, there is an EDP network for these locations, in which Employees from all locations can access central services and resources via an intranet.

For a unified communications system, it is desirable that its services are available at all available at all locations and that the know-how for its administration is only maintained at one central location. However, services such as voicemail and the exchange of documents are bound to the local telephone systems in the branch, and it is necessary to integrate these telephone systems into the central office to unify the communication system With OfficeMaster Gate is this possible in an elegant way.

In each branch OfficeMaster Gate or a remote fipMedia server is connected via ISDN/IP to the local telephone system (or the office), which is connected to the central OfficeMaster central

OfficeMaster Suite. The entire system including the OfficeMaster gates is managed centrally. All the stablished phone numbers will be retained for communication.

2.2.4. Security

The components of the OfficeMaster Suite communicate on the localhost address, so they cannot be reached from outside. The following components bind server ports (usually after manual configuration):

component	bound ports
IIS for WebUI	443, 80
authgatekeeper	3216
smtprx	587, 25
lpd	515
sip	5060+
rtp range	UDP 50000-50999

Table 2.3: component types

2.2.5. Job Processing

The OfficeMaster Suite processes jobs that were generated by connected IT systems. The controller plays the central role. It controls the communication with all components and also calculates the processing path of each job depending on image format and destination address.

A component can read jobs from its “in” directory if it receives the corresponding job from the controller. After processing (e.g. file conversion) a new job file is stored in the “out” folder and the job is passed back to the controller.

The individual component types behave differently in detail:

component type	Description
base component	Components required to control job processing, these have already been created
converter	Modifies the image files in a job
connectors	Connects the messaging server to an external IT system (Exchange, SAP, Notes, ...)

component type	Description
sendrec component	Sending / receiving component, sending or receiving via telecommunications
fofi component	File In/File Out component, used to integrate external processing steps (e.g. digital signature)

Table 2.4: component types

2.3. System Requirements

2.3.1. Communication interfaces

The messaging server is required to run OfficeMaster Suite Access to the (public) telephone network, e.g. via a telephone system or a SIP trunk (possibly behind an SBC). Most common is the connection SIP, in which documents, faxes and voicemails can be sent and received.

service	**Required communication interface**
NGDX, Fax, Landline SMS, Voicemail and Message Waiting Indication via VoIP	OfficeMaster Gate, SIP Trunk
SMS via Internet Service Provider	Internet access of the OfficeMaster Suite Server

Table 2.5: required communication interface

2.3.2. Server “hardware”, operating system and software

Please refer to the current server requirements data sheets.

3. What’s new in version 8

3.1. Graph API in Connector for Exchange Online

The Exchange Web Services (EWS) is an outdated protocol that is used since Exchange Server 2007. In August 2018, Microsoft announced that it would no longer make any further technical investments in EWS APIs for Exchange Online. The successor API recommended for use is Microsoft Graph. Microsoft had meanwhile announced that it would no longer be possible to register EWS apps in Azure AD from September 30, 2022. This shutdown of registration has now been postponed indefinitely into the future, but will occur in the foreseeable future.

Customers using the Connector for Exchange Online should migrate to the Graph API with version 8 before Microsoft discontinues support for EWS in Exchange Online.

3.1.1. What are the benefits of Microsoft Graph?

Security

Microsoft Graph has tighter security and governance policies using OAuth and granular scoping to restrict data access in a mailbox as opposed to the all-or-nothing access model in EWS.

Simplifications for developers

Microsoft Graph offers Graph Explorer to easily and quickly explore and test APIs, SDKs in various programming languages, and an active developer community.

Efficiency

Microsoft Graph APIs are REST based while EWS APIs are SOAP based. Benefits of using REST-based protocols include faster JSON serialization and reduced network usage.

3.1.2. What are the disadvantages of using Microsoft Graph?

Compared to EWS, some operations for searching for several maintained user addresses are missing. For example, it is no longer possible to determine a maintained fax address. Only SMTP addresses can be read out. This meant that the addressing procedures of the Exchange Online Connector had to be adjusted.

The granular assignment of rights makes it somewhat more difficult for administrators to determine and set the right set of rights

for their organization and the respective application.

3.2. Web API component

In previous versions, the file gateway (filegw) was often used for integration into various IT systems operated by customers. However, this approach can only be used in on-premise environments. As IT landscapes are increasingly hybrid and cloud usage is increasing, the Web-API component was developed. Here, the jobs are not transferred to the API via a job file in a directory, but as an HTTPS request. This allows documents to be sent and received by fax, SMS, e-mail, as an X invoice and to access printers.

There is an API for the integration, the documentation for which can be accessed at https://{msgSrvHost}/webapi/v2/doc/ (the web API component must be running for this). A test environment for e.g. Postman can be created automatically from the OpenAPI description.

One usage scenario for the Web API component is to be able to create Dynamics 365 flows for sending invoices by fax and letter or as an X invoice.

In the default configuration, the Web API component is linked to the localhost address and is addressed via the AuthGateKeeper (which acts as a reverse proxy here). Therefore, the AuthGatekeeper's certificate is also used for the TLS connection.

The setup of the Web-API component is shown again in the "Configuration of the individual components" chapter. This mainly involves generating API keys to authenticate access to the web API component.

3.3. E-POST component

The E-POST component allows letters to be sent via Deutsche Post's API. PDF files and address information are transferred here. In 8.0 this function is available via the Web-API component, in subsequent versions it should also be possible to generate these orders from the client (e.g. Outlook) via the appropriate connectors.

The use of the E-POST component requires registration with Deutsche Post. Corresponding access data is generated, which is required to configure the E-POST component.

There is a test operation to set it up. If this is active, the document is not printed and enveloped, but sent as a PDF file to an e-mail address specified in the test order. When connecting to an IT system, it is recommended to first use this test mode (which also does not cause any postage costs).

When connecting letter mail to CRM systems, for example, there is a risk of causing significant costs by selecting an unintentionally large number of recipients. Therefore there is a parameter to limit the maximum number of letters to be sent daily (quota).

The setup of the E-POST component is described in the chapter "Configuration of the individual components".

3.4. Component for sending electronic invoices (X invoice)

Peppol (Pan-European Public Procurement OnLine) is a project that standardizes public procurement procedures within the EU. Tendering, awarding and payment are supported. For the latter, electronic invoicing has been standardized as an X invoice.

The X-Invoice format is XML-based and standardized in Germany by the Coordination Office for IT Standards (KoSIT) on the basis of EN 16931-1. At the time of writing this document, v.2.2.0 was the current version.

From November 27, 2020, suppliers of the federal government are obliged to issue invoices in electronic form as part of public contracts. The federal states have their own regulations - while in some federal states an obligation for suppliers was decreed (e.g. in Bremen on November 27, 2020 or in Baden-Württemberg on January 1, 2022), other federal states did not initially stipulate any obligation for electronic invoicing.

The Peppol network is an association of Peppol providers who exchange electronic documents (including X invoices) with each other. A list of Peppol providers can be found here.

Addressing in the Peppol network is via the Peppol Participant Identifier (Peppol-Participant-ID). A distinction is made between sender ID and receiver ID. There are several methods of forming this unique address. The structure is always there

```
Prefix:AddressInformation
```

where prefix specifies the address type and the address information must be unique.

The public sector in Germany uses the routing ID to address the invoice recipient within the X-invoice. When handing over to the Peppol provider, however, the address is 0204:RouteID. The table shows a small selection of the possible addressing methods.

Peppol address prefix	Address Type	Peppol Participant ID	Audience
0204	Route ID	0204:Route ID	Invoice recipient federal/state/ municipal authorities/authorities
9930	VAT ID	9930:VAT ID	German companies
0088	Global Location Number	0088:GLN	Organizations with GL number

Table 3.1: Peppol addressing method (selection)

The first digits of the Leitweg ID roughly indicate where the invoice recipient is located in the federal structure of Germany:

- 01 Schleswig Holstein
- 02 Hamburg
- 03 Lower Saxony
- 04 Bremen
- 05 North Rhine-Westphalia
- 06 Hesse
- 07 Rhineland-Palatinate
- 08 Baden-Württemberg
- 09 Bavaria
- 10 Saarland
- 11 Berlin
- 12 Brandenburg
- 13 Mecklenburg-Western Pomerania
- 14 Saxons
- 15 Saxony-Anhalt
- 16 Thuringia
- 99 Federal Government
    - 991 - direct federal administration or a constitutional body and receives electronic invoices via the ZRE.
    - 992 - indirect federal administration or federal state and receives electronic invoices via the OZG-RE.
    - 993 - indirect federal administration and receives electronic invoices via its own solution (neither ZRE nor OZG-RE).

If the invoice recipient can be reached via ZRE (central invoice receipt portal) or OZG-RE (online access law-compliant invoice receipt platform) (route ID 991* or 992*), the Peppol web service of the federal government can be used. However, this does not forward any invoices to other recipients.

A Peppol provider must be selected for a universal connection. A suitable Peppol provider takes over the routing of the invoices to the correct Peppol access of the recipient.

> **Note!**
>
> The X invoice component has so far been tested with the federal government's Peppol web service. This means that compatibility tests with various (chargeable) Peppol providers are still missing. Therefore, no recommendation for a provider can be made at the moment.

It is planned to be able to use the X invoice component not only for sending but also for receiving X invoices in the future.

Instructions for setting up the X calculation component can be found in the chapter *Configuration of the individual components*.

3.5. Line test

With the conversion of the telephone network from circuit-switching to packet-switching, a new problem arose for fax communication: the influence of SBCs and media gateways on the audio signal. Echo cancellers, codec translation and audio healers mainly play a role in connection with packet loss. The functions can (often) be controlled by SDP parameters or switched off for fax communication. However, testing the line quality has always been difficult and was usually carried out by analyzing packet capture files (pcap).

To simplify the setup, the OfficeMaster Suite 8 now has the *Line test* function. It can be specified in the rules for processing incoming calls (inbound routing) that a phone number should be used for the line test. If this number is then called by another Direct SIP component, this connection is renegotiated into a line test. All you have to do is send a fax to this number. This can, for example, be commissioned with the fax test dialog that is new to the classic messaging server configuration program.

During the line test, the quality of the transmission is measured in both directions as the modem speed increases. At the end, the statistics are collected on the caller's side and a report is created. This report is sent to the person responsible as confirmation for the fax dispatch.

If all tests are 100% successful, there is a clear path between both participants - G.711 sample bytes are transmitted unchanged.

Ferrari electronic AG operates a remote station for the line test on +49 3328 455380.

3.6. Maintenance State / Drain Mode

Up to OfficeMaster Suite 7 there was the problem that when the messaging server service was stopped, jobs could still be being processed and then remained in the queue. With a restart (possibly also after an update) these were of course then processed. However, when the system was relocated or reinstalled, the jobs had to be transferred manually, which can sometimes involve considerable effort.

In OfficeMaster Suite 8 there is a maintenance status or drain mode. The messaging server is active in drain mode, but no longer accepts any orders. This means that the orders already in the system can be processed and the messaging server runs empty. Not accepting orders means:

- incoming calls are rejected (SIP error code Service Temporarily Unavailable),
- Exchange mailboxes are no longer queried, orders accumulate there.
- SMTPRX no longer accepts connections.
- ...

However, the outgoing function is not affected by this, outgoing calls can still be made and messages can be delivered to users or their mailboxes.

The maintenance state (drain mode) can be triggered manually in the messaging server configuration in the “Extras > Maintenance mode” menu. Then you should give the system time to process all orders. As soon as the job status is empty, the system can be stopped.

There is another use case for the maintenance status or drain mode. If failure redundancy is to be achieved through the parallel operation of two messaging servers (active/active with e.g. each with their own SIP trunks), it does not make sense to continue to forward jobs to this system if one SIP trunk fails. It can then be configured that the failure (alarm) of the SIP component automatically puts the messaging server into maintenance mode (drain mode). From this moment on, only orders are routed via the other system and no jobs accumulate in the failed system.

In normal operation with only one messaging server, the automatic drain mode can be helpful if you want the jobs to accumulate in front of the messaging server and not in its queue.

In the standard configuration, no maintenance state is automatically adopted.

3.7. Cloud Relay on NGDX transmission

With the OfficeMaster Suite Version 7, the NGDX procedures were published for the first time (NGDX - next generation document exchange). Version 8 now adds Cloud Relay as a new NGDX method. The key exchange (via telephone line) is separated from the file transfer (Internet) in order to achieve greater security and higher transfer speeds.

The process is as follows:

1. Sender/Telephony: call
2. Recipient/telephony: call acceptance, NSF CSI DIS
3. Sender/Telephony: checks receiver capabilities (ECM, BFT, IP)
4. Sender/IP: starts uploading, to that
    - Split documents into 256KB pieces (shards)
    - Generate and record AES key
    - Encrypt shards
    - Make a note of the download URL
5. Sender/Telephony: Fax retrieval of the recipient's X.509 certificate via T.434
6. Sender/Telephony: Certificate check
7. Sender/IP: Upload complete?
    - If not: Sender/Telephony: RNR
    - Otherwise: transmitter/ telephony: MCF
8. Sender/Telephony: Send T.434 stream, to do this
    - Encrypt JSON document with URLs and keys of the shards
    - Encrypt the AES key of the JSON document with RSA4096 (public key from the recipient's certificate).
9. Receiver/Telephony: Receive and extract T.434 stream
    - Extract URL list with private key AES Key and decrypt the list
10. Receiver/IP: Begin downloading shards
11. Receiver/Telephony: As long as the download persists, send RNR
12. Receiver/IP: decrypt shards, assemble documents, check hash
13. Recipient/Telephony: If hashes are correct, confirm documents (MCF)
14. Sender/Telephony: Create feedback for successful sending

Understanding the process is only necessary if you want to evaluate the security of the procedure yourself. The user does not notice anything about this process, for her it is a normal (albeit faster) document dispatch. In particular, users are not burdened with key management tasks.

The advantages of the cloud relay method are **higher security** and **higher transmission speed**. The security results from the fact that a different medium (telephony) is used for key exchange than for data exchange (IP). An attacker would have to listen to both media at the same time. Furthermore, the document transmission via HTTPS is transport-encrypted with TLS and the individual shards are each encrypted with their own AES256 keys.

The speed gain is significant. A 10 MB PDF file is transmitted in about 100 minutes via

fax modem (without using T.38 acceleration), with Cloud Relay in about 80 seconds (even without using T.38 acceleration).

A disadvantage of the cloud relay method is that the messaging server has to establish a client connection to the cloud relay server (to the Internet). Some messaging servers are operated without IP routing to the public network and cannot then use the method.

The cloud relay server is resolved via an SRV record (_ngdx._tls.ferrari-electronic.de) in the DNS domain ferrari-electronic. This also provides scalability and load balancing.

3.8. Browser-based configuration interface

The browser-based configuration interface was created for easier administration in cloud environments. This includes the subset of the functionality of the classic messaging server configuration program that is relevant for operation in cloud environments. Setting up ISDN, Notes and SAP is not included. The *Configuration programs* chapter explains how the configuration interface is opened in the browser.

> **Note!**
> At the time OfficeMaster Suite 8.0 was released, the web-based configuration interface was a technical preview. It is only available in English and does not yet allow apps to be registered in Azure AD. To register apps the use of the MS Exchange Online Connector installation wizard in the classic configuration program is recommended until further notice.

The advantages of the browser-based user interface are **operating system independence** and **simplification of setup** by eliminating the need to install a configuration program.

3.9. Tesseract OCR engine support

The OfficeMaster Suite has supported OCR for a long time, but this was associated with license costs due to the OCR engine used. In projects, however, it was also possible, for example, to recognize forms in order to be able to initiate automated processes. This paid OCR engine from B&L is still available for such projects.

With Tesseract, however, all users now have a license-free alternative. Tesseract was developed at Hewlett Packard between 1984 and 1994 for use with scanner products, but never shipped. The code was given to the University of Nevada, Las Vegas in 2005. The former developer was working at Google at the time. Upon request, the code was updated and placed under an Apache license by Google. Since 2006, the program has been further developed as the basis of Google Books (collection of retro-digitized books). Google uses Tesseract for text recognition on mobile devices, in videos and images.

When Tesseract is installed, OCR is used to add a text layer to the PDF documents of incoming faxes. This makes it possible for users to copy text from incoming documents via cut & paste or to initiate processes via text extraction (e.g. with PDFium) (e.g. via file gateway or Web-API).

The Tesseract Engine is not a product of Ferrari electronic AG. If there are problems with the quality of the recognition, there can be improvements through adjusted parameters when calling the OCR engine. From version 4, Tesseract supports both classic pattern recognition and a recognizer based on neural networks. The recognition is language dependent and supported by dictionaries. If the language is sometimes incorrectly recognized in mixed-language texts, the wrong dictionary is used. It therefore makes sense to contact Ferrari electronic support with an example file so that the problem can be analyzed and the parameters can be adjusted if necessary.

In the case of NGDX, it is assumed that the documents are synthetic PDFs and already contain text. However, if there are scanned documents, they may not be subjected to the OCR.

3.10. Remote fipMedia server

3.10.1. What do you need a remote fipMedia server for?

When using an OfficeMaster gate, this could be placed close to the telephone connection (e.g. in a branch) and controlled by a messaging server in a data center or, for example, from the central office. First, a file transfer took place in the OfficeMaster Gate, which then carried out the fax dispatch locally. The connection via VPN can have different quality of service. In particular, the latency or the round-trip delay sometimes exceeds 100ms, which means that the conditions for RTP transmission are poor.

The networks and VPNs have gotten better in recent years. However, there are still use cases where the quality of the VPNs is not sufficient to send RTP streams from a central messaging server to remote locations. Before OfficeMaster Suite 8, there was no good solution for this with DirectSIP; a physical or virtualized OfficeMaster Gate with ISDN controller components had to be used.

The remote fipMedia server brings the fax protocol stack from DirectSIP to an OfficeMaster Gate or a Windows system outside of the messaging server. The document transfer takes place via Websocket file transfer to the fipMedia server - network latency is not important for the fax transfer. The fax protocol is then run on a machine close to the telephone connection/SIP trunk and the RTP stream is terminated.

Who needs a remote fipMedia server? Most customers have simple installations with one or two (with redundancy) SIP trunks and a messaging server. These users do not benefit from the remote fipMedia server. But there are use cases that can only be solved in this way. On the one hand, there are customers whose locations are distributed over a large geographical area (international corporations) and are connected via VPN. A central messaging server with several SIP components should connect the SIP trunks on different continents, for example. On the other hand, there are customers who want to connect many locations with a central messaging server, but either the messaging server is not sufficiently scaled, the quality of service of the VPN (typically latency) is insufficient, or the bandwidth is too low for the RTP streams of all locations . In those cases, OfficeMaster Suite 8 can be used to calculate the media path of the fax transmission in the locations, but the SIP signaling, routing and IT connection are carried out centrally with a messaging server.

3.10.2. What steps are required for setup?

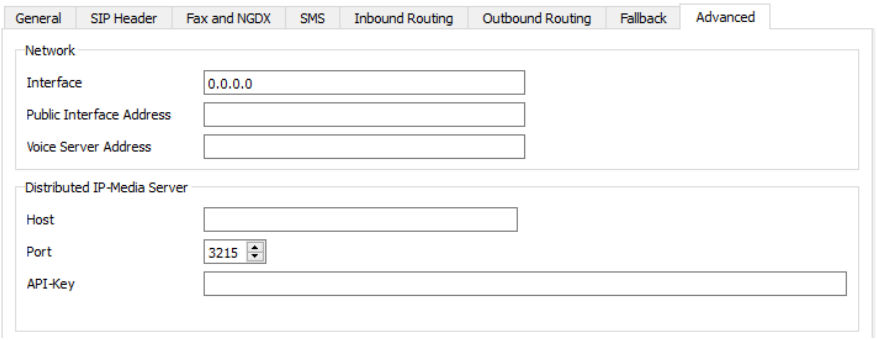
To set up a remote fipMedia server, you need a physical (OfficeMaster Gate Advanced) or virtual machine for each location. This can be installed with the OfficeMaster Gate Firmware 5.1 image.

The SBC function of the firmware can, but does not have to be used. The optional fipMedia server can be integrated into the firmware (TAR file to be installed). It also contains the Ferrari IP Media process for fax transmission.

After installation, an API key must be created. This is later entered in the messaging server and is used to authenticate the messaging server against the fipMedia server (not everyone is allowed to control fax operations). The API key can either be created via ssh and the command line tool *omgFmsApiKey* or set up with the *OfficeMaster Gate Config* for firmware 5.1 (older versions are not suitable) on a tab in the certificate management dialog.

```
omgFmsApiKey -user <any name>
omgFmsApiKey -list
```

As a next step, the name of the process to be executed in the Comptab must be changed for the SIP component that wants to use the remote fipMedia server (fsip to fsip2). The easiest way to do this is to edit the properties of the SIP component and change the name of the file to be executed (executable) to fsip2 (the component must be stopped for this). This also changes the configuration interface in the messaging server configuration and the host name of the fipMedia server and the API key can now also be stored on the “Advanced” tab. One fipMedia server can be configured for each SIP trunk or DirectSIP component.



Note!

If the remote fipMedia server is used, only fax communication (and landline SMS) improves. When using voice mail, the voice server must also be moved to the LAN close to the SIP trunk. With version 8.0, OfficeMaster Suite 8 does not yet support a remote voice server.

4. Getting started

The descriptions stored in this chapter will only name the necessary steps to be taken and will not go into configuration details. The configuration options for the individual components are described in detail below

The table below provides a brief overview of the required access rights for the respective connectors and their Installation.

Environment	**use case**	**Permission Type**
Exchange (local, AD)	Installation Account	local or organization administrator
Exchange (local, AD)	Service Account (simple, delivery)	local administrator, Public Folder Management
Exchange (local, AD)	Service Account (Full, Extract, Mark, Delete)	local administrator, public folder management, authenticated user
Exchange (hybrid, AD)	Installation Account	local or Microsoft 365 administrator
Exchange (hybrid, AD)	Service Account (simple, delivery)	local admin
Exchange (hybrid, AD)	Service Account (Full, Extract, Mark, Delete)	Local Administrator, (OfficeMaster Voice Access) Database Access
Exchange Online	Installation Account	local or Microsoft 365 administrator
Exchange Online	Service Account (simple, delivery)	Cloud Users
Exchange Online	Service Account (Full, Extract, Mark, Delete)	Cloud User, OfficeMaster Voice Access (new Management Role Assignment, created by setup wizard)
Notes	Installation Account	local admin
Notes	Service Account (Fax)	Notes ID without password, read permission on address book
Notes	Service Account (Voice)	Notes ID without password, read, write and delete permissions on mailboxes, read and write permissions on voice address book (possibly voice.nsf)

Environment	use case	Permission Type
WebConnector/ Client Gateway	Installation Account	local admin
WebConnector/ Client Gateway	Service Account	local administrator, if necessary read and write rights to the database of the external SQL server
SMTP/Mail Gateway	Installation Account	local admin
SMTP/Mail Gateway	Service Account	local system, if necessary LDAP reading rights, changing the VoicePIN requires additional writing rights
SAP	Installation	local administrator and CPIC user SAP-Con

4.1. Activation of the Products

To activate the delivered license key, start the Office Master configuration.

Login to the configuration interface requires username and Password, the first time you log in with the user “admin”, you must also change the password.

The initial password for the “admin” user is: OfficeMaster!

Then call up the license management via View > License status or via the license status.

Initially you don’t see any licenses in the overview, so go ahead first to Manage Licenses

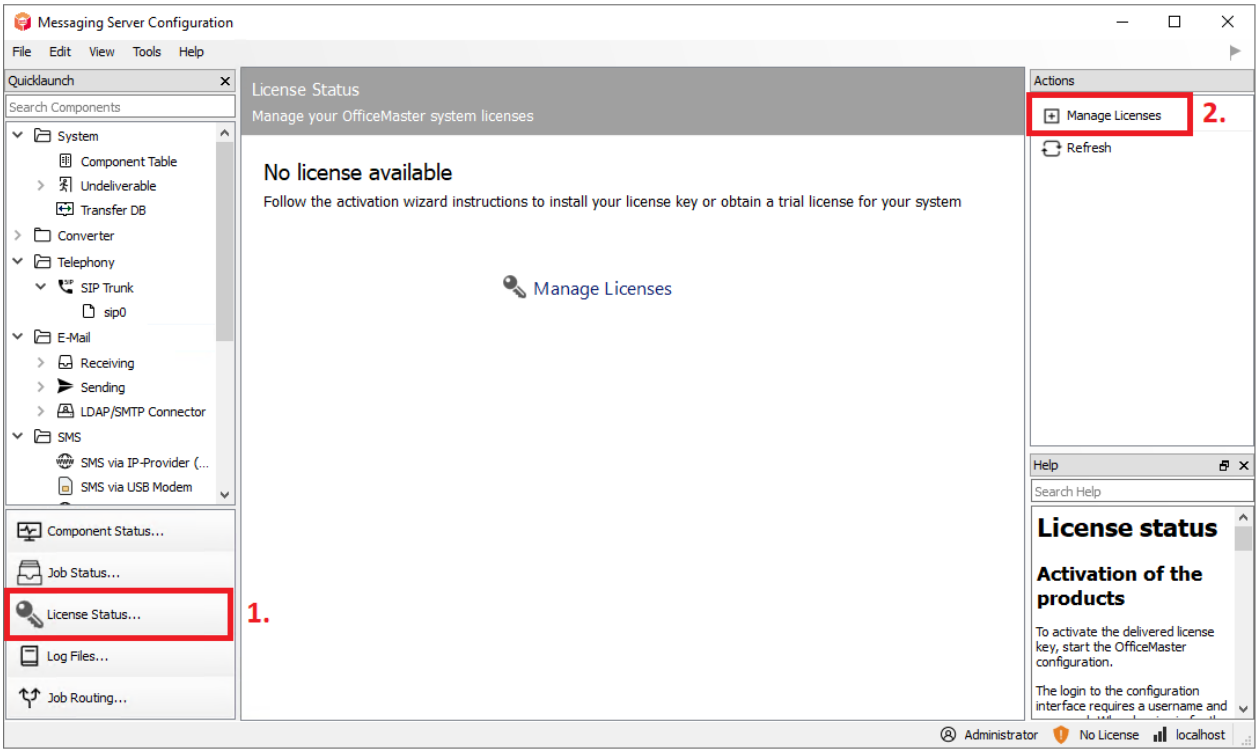


Figure 4.1: Starting the license dialog

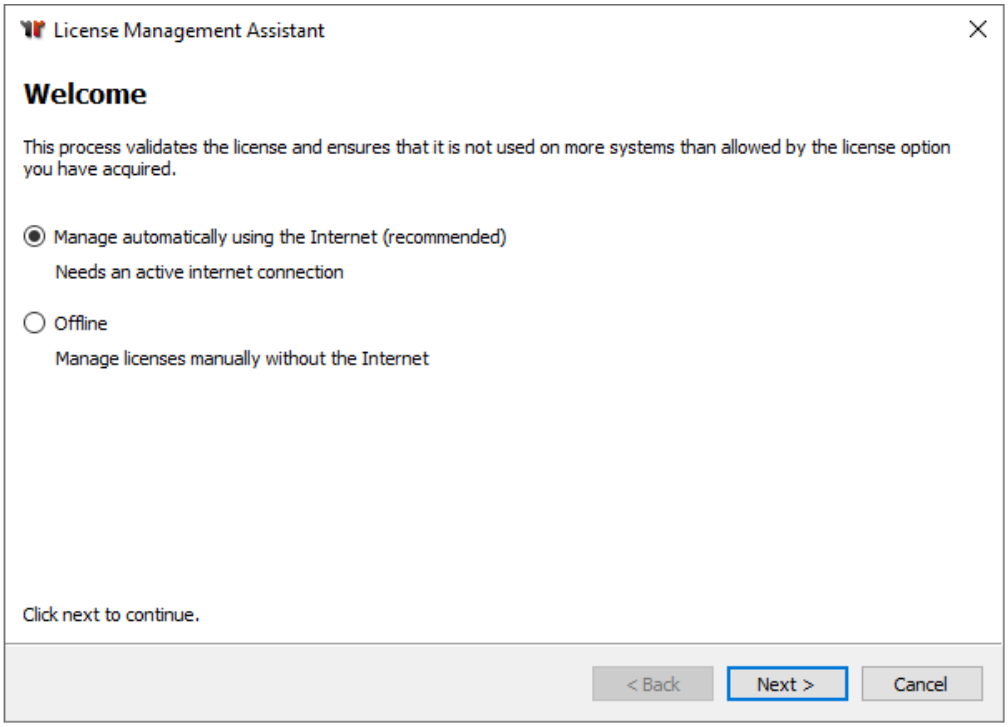


Figure 4.2: License Management Assistant

In the subsequent question, you decide how to activate the license. Online, or you log into the portal and load the generated licenses down.

Please enter your portal account now, or create a new one.

Once you have successfully logged in, you have the following activation options:

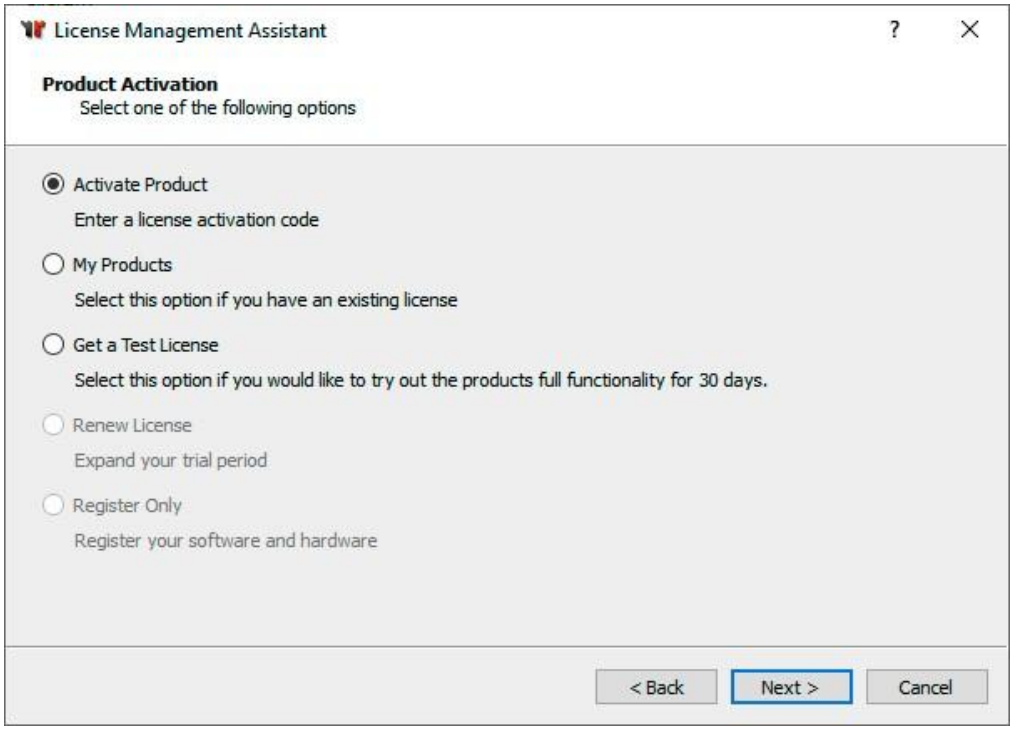


Figure 4.3: select type of license

For a fresh installation, use a trial license (A Trial License received) or activate your license key (Activate product).

You can activate multiple keys during activation. To do this, simply copy the sent keys into the Input box.

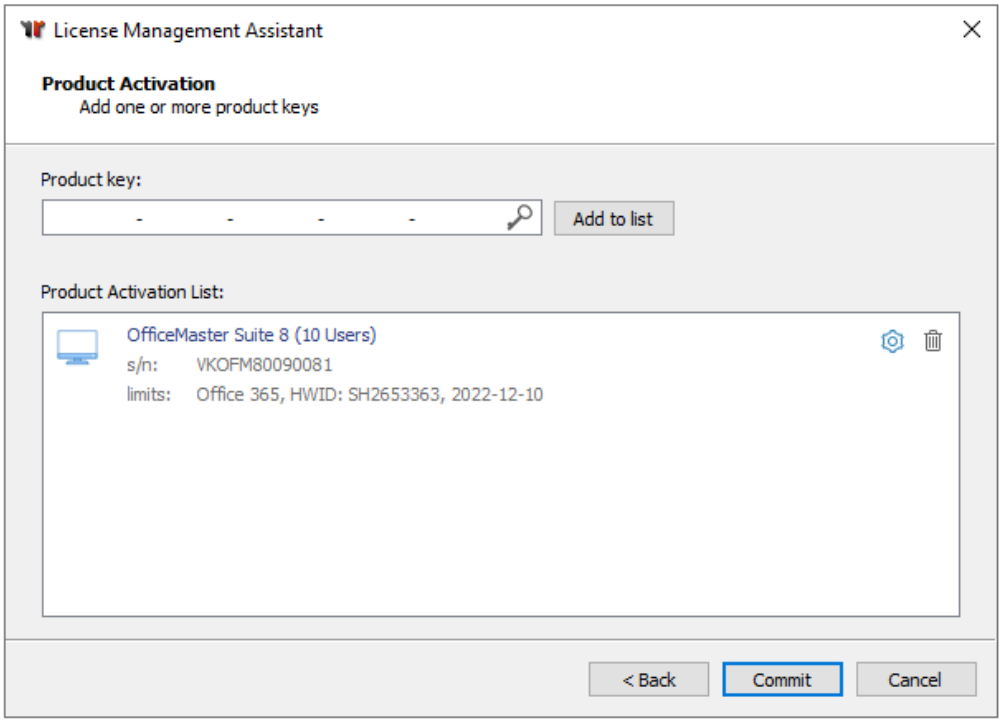


Figure 4.4: product activation

After you have imported the licenses, you will be returned directly to the now filled license overview.

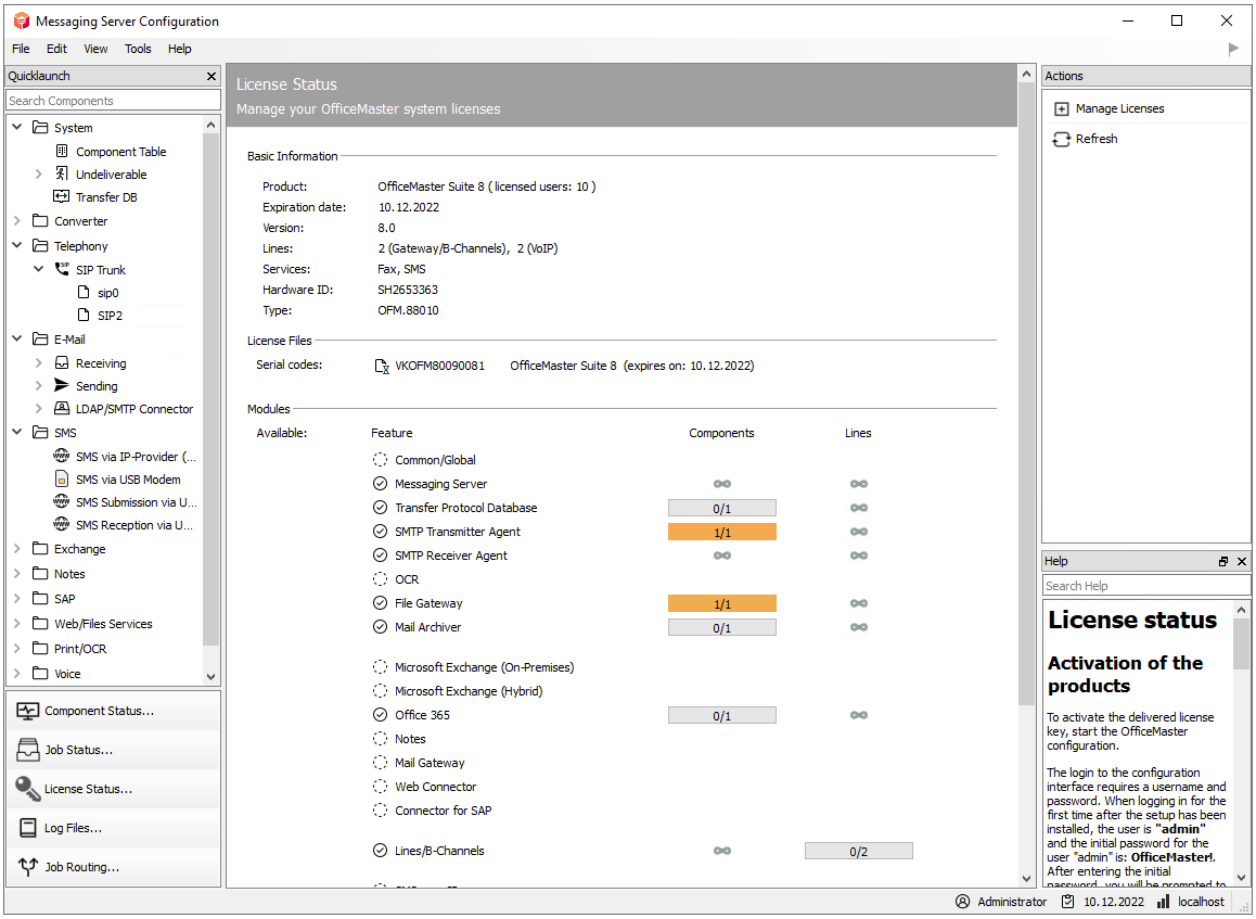


Figure 4.5: License overview

Note!

If you do not have direct access to the internet, the dialog allows you to save the created license information on a separate data carrier and transfer it from another computer. Please follow the specified steps in the license dialog
Portal page for license key activation: https://service.ferrari-electronic.de

4.2. Request a support number

4.2.1. Support with the installation and use of Ferrari electronic AG products

Since the commissioning and use of technically more demanding quality products in a complex environment of networks, operating systems, and telecommunications interfaces, Ferrari Electronic can help you if there are any start-up difficulties. Ferrari electronic with its support department provides an efficient support when problems arise. To help you as efficient as possible, we ask that you follow the instructions below:

1. The purchase of our products entitles you for a period of **one month** from the date of registration, to direct technical questions to our support department, which will respond with in a response time of 24 hours at most on normal working days (usually on the same day) either by writing (fax/e-mail) or by calling back.
2. After the end of the month is further support **chargeable**. You can choose either a 2-week limited support ticket or sign up for a one-year support contract with us.
3. To contact our support department you need a valid support number, we will provide you with this after the complete activation of your products. The condition for this is that your Account has to be verified accordingly in the service portal. The status of activation can be seen in the service portal and the configuration program.
    - You can reach the support department at:
        - Fax: +49 3328 455 962
        - Email: support@ferrari-electronic.de
    - To make it easier for you to describe your technical problem, we have prepared a support request form, which you can find in the service portal under *Technical Support*.

4.3. Quick start with Microsoft Exchange

An Exchange connector is set up using the following steps:

Note!
For the installation of the Exchange Connector use an account with the following rights:

- Domain administrator or authenticated user with the rights in the domain
- Exchange organization administrator (full)

This account is only needed temporarily for the installation and possibly for the configuration, but it is not the same as the Service Account.

4.3.1. Preparation

- The Connector component accesses the mailbox of the service account or the transfer mailbox. This leads to editing emails. To prevent and avoid the loss of important personal mailbox content the service account used should never be an existing personal user.
- Via the user administration or the Microsoft Exchange System Administration Console a user account is created, which is a member of the domain users. This account needs its own mailbox.
- The mailbox must not be suppressed in the global address list.
- The account gets full read permissions of the Exchange Organization through the membership in the group Public Folder Management.
- The account needs to be added to the local administrator's group in the computer where the installation took place.
- When using voicemail, the following additional permissions are required:
  - When using voicemail, the service account for the Exchange Connector must have write rights to the user object so that, for example, the PIN can be changed remotely.
  - For a remote query of the voice mailboxes via the Exchange Connector the read and write access to the corresponding mailboxes is necessary.

In Exchange 2013/2016/2019, the following command is used in the Exchange Management Shell to set access permissions to mailboxes:

```
new managementRoleAssignment “OfficeMasterVoiceAccess”-user
“Domain\Account”-Role ApplicationImpersonation
```

4.3.2. Installation

Install OfficeMaster Suite by running OfficeMaster Suite-8.x.y-z.exe.

4.3.3. Configuration

- Grant the service account full access to the directory %ProgramData%\ffums.
- Configure the SIP component to connect to a SIP trunk, an IP-TK or an SBC.
- Install the Microsoft Exchange Connector via the integrated installation wizard. During the installation deposit the service account.

4.3.4. Exchange Connector installation wizard

Receive Connector

It is recommended to create a receive connector, the corresponding option is preselected.

Note!
A receive connector is created with the following properties:

- Name: Connector for UMS (ExchangeServer-MessagingServer)
- Configuration of reception only via the specified port
- no anonymous authentication
- NTLM authentication is enabled
- Service account is activated specifically for this connector
- Communication to this connector is only from the IP address of the Messaging Servers allowed

Send Connector

A send connector is always created.

Note!
In addition, the following send connector is installed:

- Name: Connector for UMS (Exchange Server - Messaging Server)
- SMTP port 25
- No outgoing authentication enabled
- The sending server (local bridgehead) is the selected Exchange server

- Receiving server (smarthost) is the specified messaging server that houses the component of the connector

License Group

With the user-limited versions of the OfficeMaster Suite, a License group specified to manage authorized users will. By default, the license group is automatically in the container Users created in Active Directory. There can also be alternative groups be specified.

Service Account

The previously prepared account will appear in the service account input field entered in the component msx2kgate. The account will be specially authorized to access the connector.

Important decision on the type of installation of the configuration object!

Install base configuration object globally (recommended)

The global user settings are used as a template for all Users that are not administered directly. This Settings are stored in an object that is central replicated and made available across the organization. This Setting is the default for organizations with a single administrative group or only one routing group.

Install base configuration object domain wide

In larger organizations, the corresponding service account or the installation account of the domain does not have the right to store the global settings organization-wide. In this case, the settings can be written to the current domain object. All other sites should perform the installation form in this way as well. In each site (or domain) will be applyed different global settings.

4.3.5. Starting the Component

Finally, start the component msx2kgate of OfficeMaster Suite.

4.4. Quickstart with Exchange Online - Microsoft 365 (with on-premises AD, hybrid mode)

This is the correct mode if you want to read the messages while in the cloud, but still have a local Active Directory for the user management.

The hybrid installation assumes that user-specific values can be stored in Microsoft Active Directory. One of the the main purpose of this type of installation is the migration of a local Exchange installation to the Microsoft 365 cloud. The local Active Directory remains, which uses the existing schema extension of the Exchange organization. In the user objects are then, the required attribute fields (proxyAddresses, extensionAttribute15) available.

The connector requires an access to the Exchange Online server internet connection. Outgoing fax messages must be routed directly to the transfer mailbox without further processing such as signing.

4.4.1. Administrative account to set up

- Sign in to Microsoft 365 with an organization admin
- local domain user **Microsoft 365 service account**

This service account can be used as a

- “Shared Mailbox” (no license costs, but requires a password(!), our recommendation) or as
- normal user mailbox.

Other features of this account:

- Member of the domain users group
- local administrator of the installation computer
- The following authorizations are also required for Voicemail:
    - When using voicemail, the service account for the Exchange Connector needs write access to the user object, so that e.g. the PIN can be changed remotely.
    - For remote querying of the voice mailboxes via the Exchange connector are read and write access to the corresponding mailboxes necessary.
    - It should be removed from the Microsoft 365 password rotation

4.4.2. Microsoft 365 service transfer account (the service account may also be used here)

In this mailbox, the outgoing messages will be temporary buffered before the *OfficeMaster Suite* picks them up. For this, the size limit of this mailbox should be adjusted accordingly

Installation

- Install OfficeMaster Suite and insert a new component for Exchange Hybrid mode
- Now log in using the wizard and the one before described administrative account to the Microsoft 365 organization
- Message transfer: we recommend the service transfer mode
- Enter transfer domains: e.g. “fax.company.net”, “fax.local” (Separation with comma or semicolon) • Enter service account
- Select license group to manage authorized users (only for versions with user limit)
- Specification of the storage location for user data (AD or user mailbox)

4.5. Quickstart with Exchange Online - Microsoft 365 (Azure AD, online mode)

This connection to Microsoft 365 does not require Active Directory. The user-specific settings are saved directly in the mailbox of the corresponding user. The connector asks for these values when sending or receiving documents. With this connection, all unified messaging services that are supported are also available with a normal Exchange Connector.

The connector requires internet connection to access the Microsoft 365 server.Outgoing fax messages must be routed directly to the transfer mailbox without further processing such as signing.

4.5.1. Sign in to Microsoft 365 with an organization admin

A Microsoft 365 sign-in is performed during the installation. This login refers to an administrative account that contains the necessary rights to create, objects in the Microsoft 365 Exchange area (Organization Administrator).

4.5.2. Microsoft 365 service account to access address books

A separate service account or account is required to operate the connector, more precisely a mailbox is required. This mailbox should work as a normal user mailbox and needs to be created manually beforehand. The mailbox is used to access the public address book of the Microsoft 365 installation and it is store in the connector.

This service account can be used as a

- “Shared Mailbox” (without license costs, but requires a password(!), our recommendation) or as
- normal user mailbox.

Other features of this account are:

- For remote querying of the voice mailboxes via the Exchange connector are read and write access necessary for the corresponding mailboxes.
- It should be removed from the Microsoft 365 password rotation.

4.5.3. Microsoft 365 service transfer account (the service account may also be used here)

In this mailbox, the outgoing messages will be temporary buffered before the OfficeMaster Suite picks them up. For that it should be adjusted the size limit of this mailbox accordingly.

4.5.4. Installation

- Install the OfficeMaster Suite
- Insert a new component for online mode
- Now log in using the wizard and the one before described administrative account to the Microsoft 365 organization
- Message transfer: we recommend the service transfer mode
- enter transfer domains: e.g. “fax.company.net”, “fax.local” (Separation with comma or semicolon) • Enter service account
- Select license group to manage authorized users (only for versions with user limit)
- Specify the storage location for user data (AD or user mailbox)

4.6. Quick start with Notes

4.6.1. Preparation

- Create a service account and add it to the local Administrators on the operating system of the future fax server. Create a Notes user without a password.
- Furthermore, the Notes user ID requires unrestricted access to the Notes mailboxes of the users who want to retrieve voicemails via phone call. The reception of voicemails is also possible without this full access

  Note!
  Notes users ID cannot save password in name and address book. When registering the Notes user ID, the storage in the Name and address book should be deactivated.

- Create a “foreign domain” FAX in the Domino address book and let these point to the mail database of the created user.
- Install the Notes client in standalone mode and set it up. Enter it with the Notes ID you created.
- Install the programs required for conversion • Start installed programs using the service account.

User mailbox of the Notes user ID as transfer database

By default, the Notes Connector of the OfficeMaster Suite uses the User mailbox of the Notes user ID as transfer database. Thereby no special access permissions need to be configured. However, test faxes and SMS must always be sent from a workstation computer with its own user ID

Separate mailbox as transfer database

As an alternative to the user mailbox of the Notes user ID, a separate Mailbox can be created as a transfer database. This has to be done manually on the Domino server responsible for NOTESCONN. The default name of the separate mailbox is ffax.box.

Note!

To avoid permission conflicts, it's a good idea to create the mailbox with the Notes client from the OfficeMaster Messaging Server. To do this, select in Notes the menu sequence File > Database > New ENG: (File > Applications > New).

4.6.2. Installation

Then install the OfficeMaster Suite.

4.6.3. Configuration

- Grant the service account full access to the directory %ProgramData%\ffums.
- Configure the SIP/ISDN component OfficeMaster Gate Controller (omcums0) or the SIP Trunk (sip0).
- Configure the Notes Connector.

4.7. Quickstart with WebConnector

4.7.1. Preparation

- Create a service account and add it to the local Administrators on the operating system of the future fax server. The service account must later become the database administrator.
- Install the programs required for conversion, such as Libreoffice or Microsoft Office (without Outlook!).
- Start the installed programs with the service account.

4.7.2. Installation

Install OfficeMaster Suite.

4.7.3. Configuration

- Grant the service account full access to the directory %ProgramData%\ffums.
- Configure the SIP/ISDN component OfficeMaster Gate Controller (omcums0) or the SIP Trunk (sip0).
- Install a new component of type clientgw and select during the installation wizard, the desired data storage.
- New SQL Server instance; this is followed by an automatic installation process of a SQLServer 2014 Express.
- Selection of an existing SQL server in your environment.
- Enter the service account to be used.

4.8. Quickstart with SMTP mail server

4.8.1. Preparation

- Create a service account and add it to the local Administrators on the operating system of the future fax server.
- Install the programs required for conversion, such as LibreOffice or Microsoft Office.

4.8.2. Installation

- Start the installed programs with the service account.
- Install the OfficeMaster Suite.

4.8.3. Configuration

- Grant the service account full access to the directory %ProgramData%\ffums.
- Configure the SIP/ISDN component OfficeMaster Gate Controller (omcums0) or the SIP Trunk (sip0).
- Configure the pre-installed SMTP connector (mailgw0) that connects to the mail server and the user data storage.

4.9. Quick start with SAP

4.9.1. Preparation

- Create a service account and add it to the local administrators group on the operating system of the future fax.
- Install the programs required for conversion, such as LibreOffice or Microsoft Office.

4.9.2. Installation

Start the installed programs with the service account.

4.9.3. Configuration

- Grant the service account full access to the directory %ProgramData%\ffums.
- Configure the SIP/ISDN component OfficeMaster Gate Controller (omcums0) or the SIP Trunk (sip0).

Configuration in SAP

- CPIC User
- Node with associated RFC destination (in newer systems, the RFC destination can only be created in classic mode)
- Jobs

Configuration in OfficeMaster Suite

- Insert a SAP RFC or Unicode via the quick launch bar connector.
- Enter the data previously set up or specified in SAP:
    - R3 server
    - System number
    - Client
    - Program ID

5. Configuration programs

5.1. Overview

Various configuration interfaces can be used to set up the OfficeMaster Suite:

- the classic messaging server configuration program,
- the browser-based messaging server configuration interface,
- the MMC snap-in for the Exchange Server Management Console as well
- the OfficeMaster Gate Config for configuring SBCs and gateways.

The individual configuration tools are briefly introduced in the following sections.

5.2. Working with the classic messaging server configuration program

To start up OfficeMaster Messaging Server, *Messaging Server Configuration* – a program that runs on both the server as well as installed and used on administrative workstations can be.

The messaging server configuration opens as follows:

Start > Programs > OfficeMaster > Messaging Server Configuration

5.2.1. configuration interface

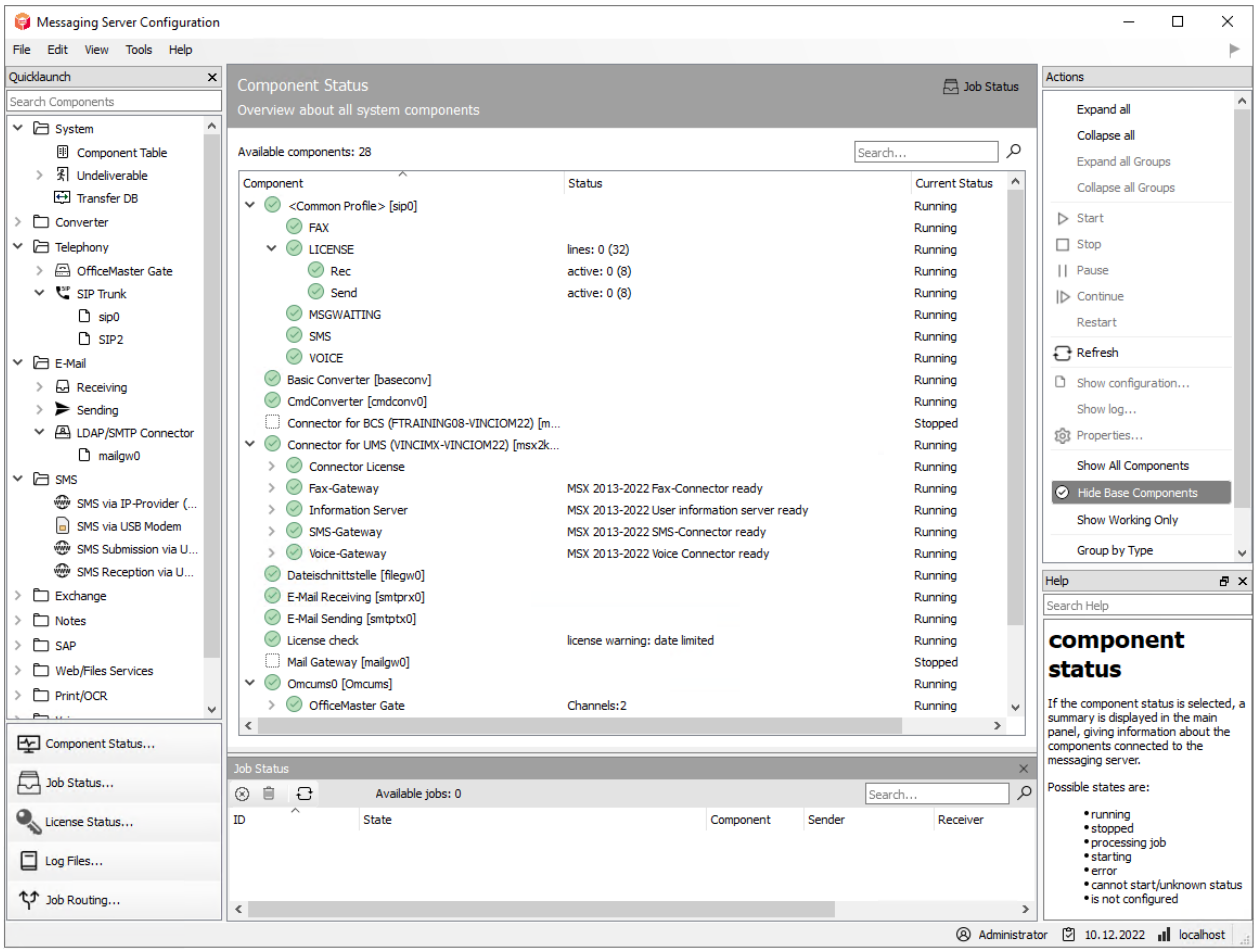


Figure 5.1: Distribution of the messaging servers

The messaging server configuration interface can be divided into the following Divide parts:

- Menu bar (top)
- Quick start (top left)
- Toolbar (bottom left)
- Peloton
- Action field (right)

Note!
The main field always shows the interface that is currently being viewed or edited. There is a special feature for the items component status and job status. These two can be displayed in parallel. For the above screenshot, choose one of the both fields and then click in the main field at the top right “Job Status” or “Component Status”. The first clicked window is always at the top of the display.

5.2.2. Create / delete components

Creating new components is possible in several ways:

1. Menu bar: New
2. Quick start: Component Table > New Component...
3. Quick Start Area: COMPONENT TYPE

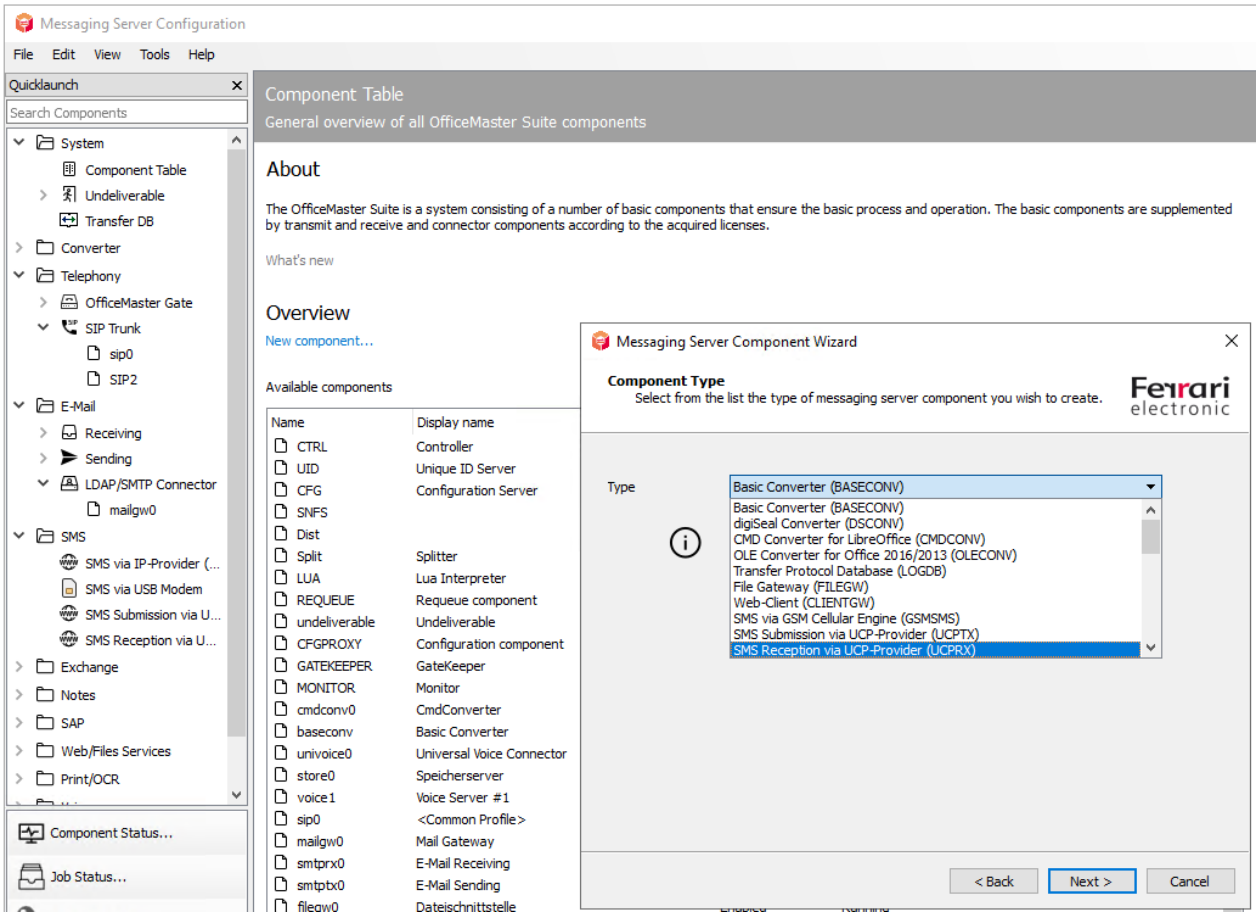


Figure 5.2: Creating a new component via the component table

With 1. and 2. a wizard is started, with the help of which the desired component is installed.

Installation variant 3. starts with the selection of whether a custom or a normal installation should be made. Select the user-defined variant for distributed installations.

The installation is completed with the subsequent dialog. The display name to be is the name with which the component overview is displayed.

5.2.3. Configure components

The components of the Messaging Server are divided into Configuration (Edit) and Properties.

Characteristics

Properties include all non-functional settings that are required for the operation of the component. This can be accessed in various ways:

- Selection of the component in the component status overview, with Right click and select *Properties*
- Select in the components table, then *Edit*

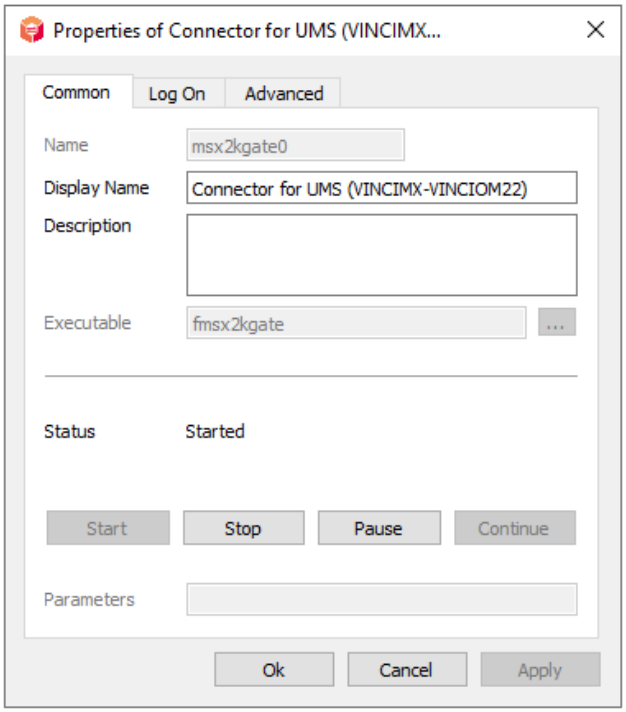


Figure 5.3: General settings of a component

The *General* tab will be displayed, when you open the properties of a component.

State

At this point the selected component can be started with *Start, Stop, Pause* and *Resume*.

Parameters

The entry of additional start parameters is under *Parameter* possible.

In some constellations it is necessary to start components under an account that is different from the system account. The corresponding entered account can be found under the *Login* tab.

To adjust logs for analysis purposes, use the *Advanced* tab.

Log Levels

The level of the log files is set accordingly here.

> Note!
> Some settings are only possible if the component has been stopped.

Stop Delay

Adjusting the response time of the component to the start and stop of the messaging server service.

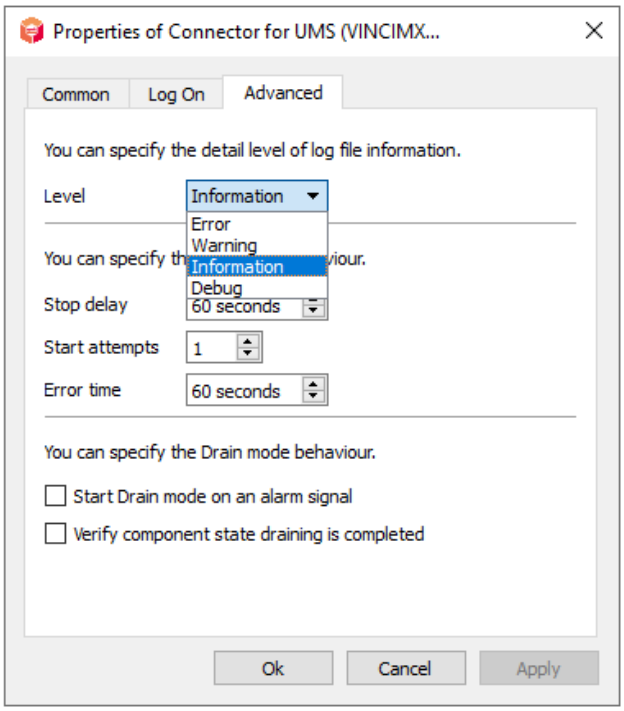


Figure 5.4: Component Debug Settings

Start attempts

Entry of attempts to restart the component if errors occurred beforehand.

Error time

Duration between the individual start attempts.

Configuration/Edit

The configuration of a component is displayed via:

- The menu bar of the messaging server configuration by selecting the Component (left click)
- Via component status and component selection, right click, Select *Edit*

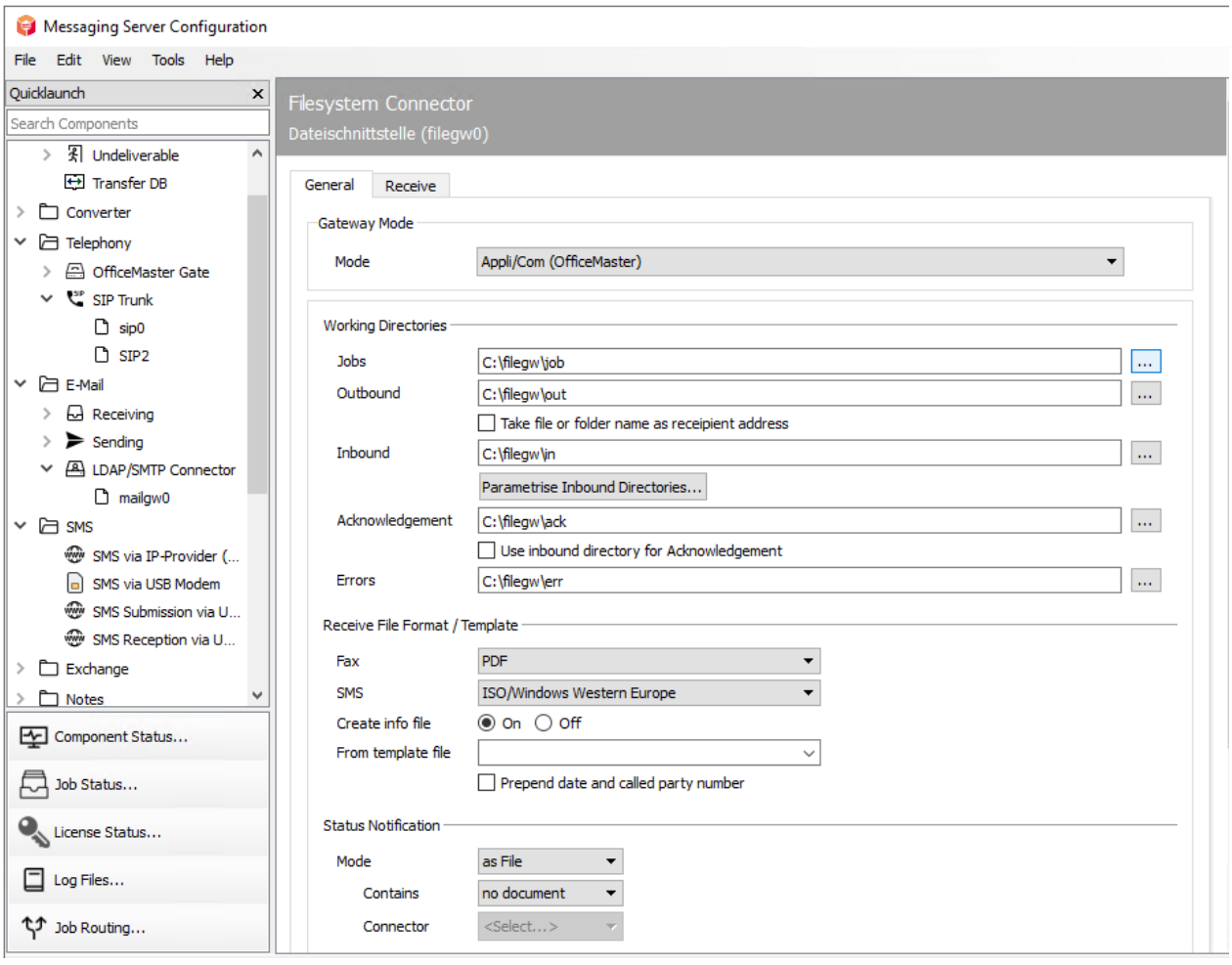


Figure 5.5: Selection of the component to be configured

The configuration steps to be carried out in each case are described in the corresponding chapters of this documentation.

5.2.4. Component Status

If the component status is selected, a summary is displayed in the main panel, giving information about the components connected to the messaging server.

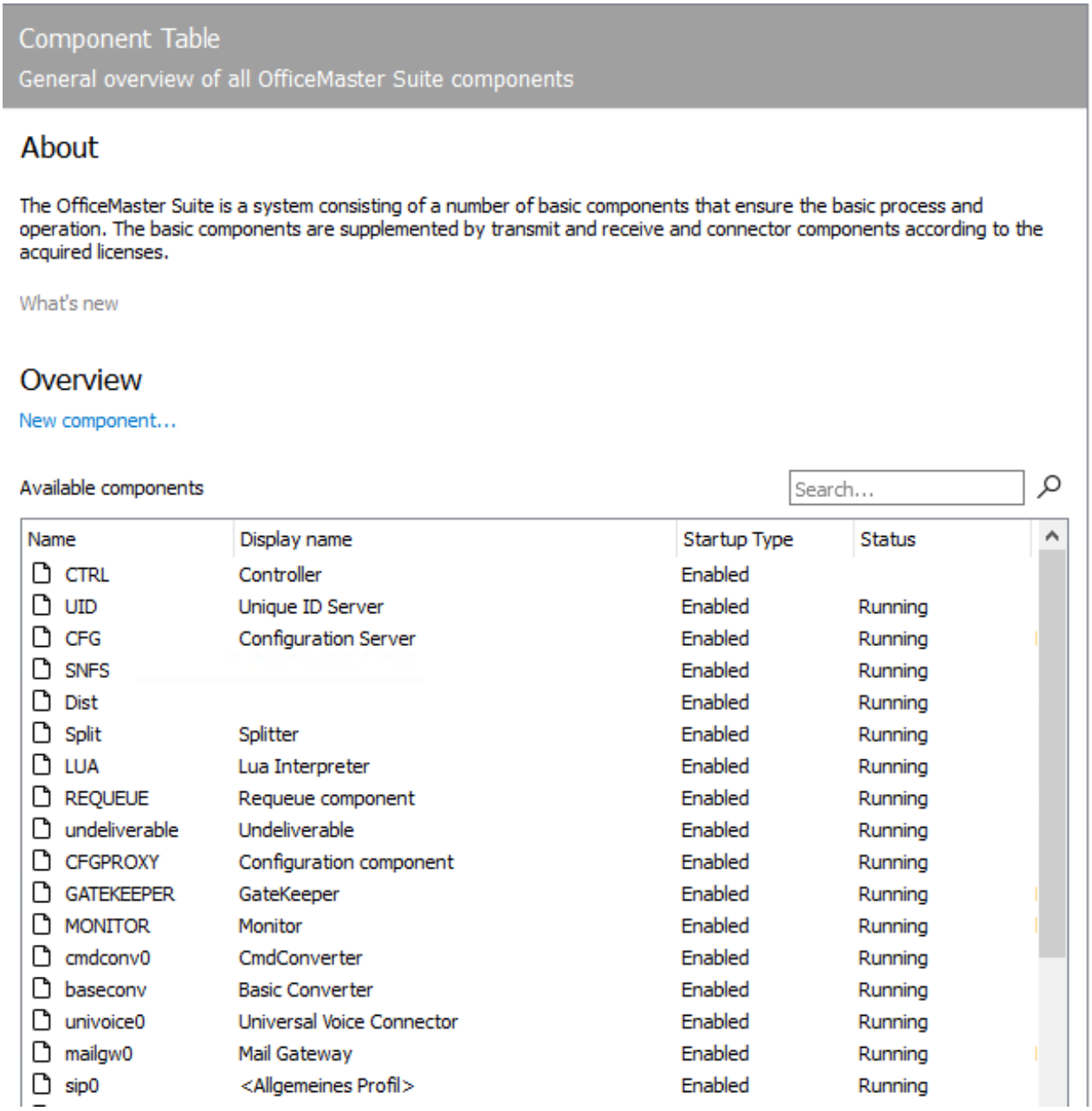
Possible states are:

- running
- stopped
- processing job
- starting
- error
- cannot start/unknown status
- is not configured

5.2.5. Component table

Components which have been configured, are displayed in the component table. The component name is the unique identifier of the component. The startup type indicates whether the component should be started automatically when the messaging server starts. The Status column shows the current status (e.g. running or stopped). Components deliver status messages when there are status changes. The Status Message column displays the latest of these messages.

If a component is selected by clicking in the corresponding line, it can be influenced (e.g. startet or stopped) by clicking on an icon in the *Actions* panel. System relevant components (e.g. CTRL, Starter) can’t be influenced by the context menu.



5.2.6. Job Status

The jobs that are currently being processed are displayed in the job status. These can be send or receive jobs. In addition to the component that is currently processing the job, the information on the *Job ID*, *Sender and recipient phone number* can also be read out here.

In addition, a job in the job status can be aborted or deleted.

> **Note!**
> With the **F3** key you get more information about the job (e.g. the documents that belong to the job). The information can then be useful when the job may not be processed further.

5.2.7. License status

Activation of the products

To activate the delivered license key, start the OfficeMaster configuration.

The login to the configuration interface requires a username and password. When logging in for the first time after the setup has been installed, the user is **“admin”** and the initial password for this user is: **OfficeMaster!**. After entering the initial password, you will be prompted to change the password.

Then call up the license management via *View* > *License - Status* or via *License Status*.

Initially you don’t have any licenses in the overview, so go to *Manage licenses* first.

Start the license dialog

In the subsequent question, you decide how to activate the license.

- **Automatic administration via the Internet:** Please enter your portal account now, or create a new one.

  Note!
  In case you need to create a new account, please fill in **all** fields.

Once you have successfully logged in, you have the following activation options:

Choose type of license:

For a new installation, use *Get a trial license* or activate your license keys that were sent to you via *Activate product*. You can activate multiple keys during activation. Simply copy the sent key into the input field. After you have imported the licenses, you return directly to the now filled license overview.

Under *My products* you will find the already activated licenses matching your hardware ID of the messaging server, which can be read “online”.

The hardware ID of the messaging server can be found under *Help* > *About* in the menu of the messaging server configuration

- **Offline:** If *Offline* is selected as an option, only licenses that have already been activated in the Service Portal can be imported.

License overview

Note!
If you do not have direct access to the Internet, the dialog allows you to save the license information you have created on a separate data medium and to transfer it from another computer. To do this, please follow the steps given in the license dialog.

Portal page for license key activation: https://service.ferrari-electronic.de

5.2.8. log files

The log files of the individual components (including those of the hidden components) can be viewed in the *Log files* area in the messaging server configuration.

Several files are created for each component, which differ in their file extension. For example, a log file from the current day of *msx2kgate0* is called ***msx2kgate0.0***. From yesterday it would be called ***msx2kgate0.1***. In the standard, a maximum of 5 log files are written per component.

Note!
The number of log files (days) to be written can be defined under Extras > System settings. The current day does not count here.

5.2.9. Job processing

This overview shows the routing rules of the messaging server in their entirety. The settings for this are made for each individual component.

Outgoing and incoming connections are displayed separately, since they are also separated in the ruleset and from the routing settings of the components.

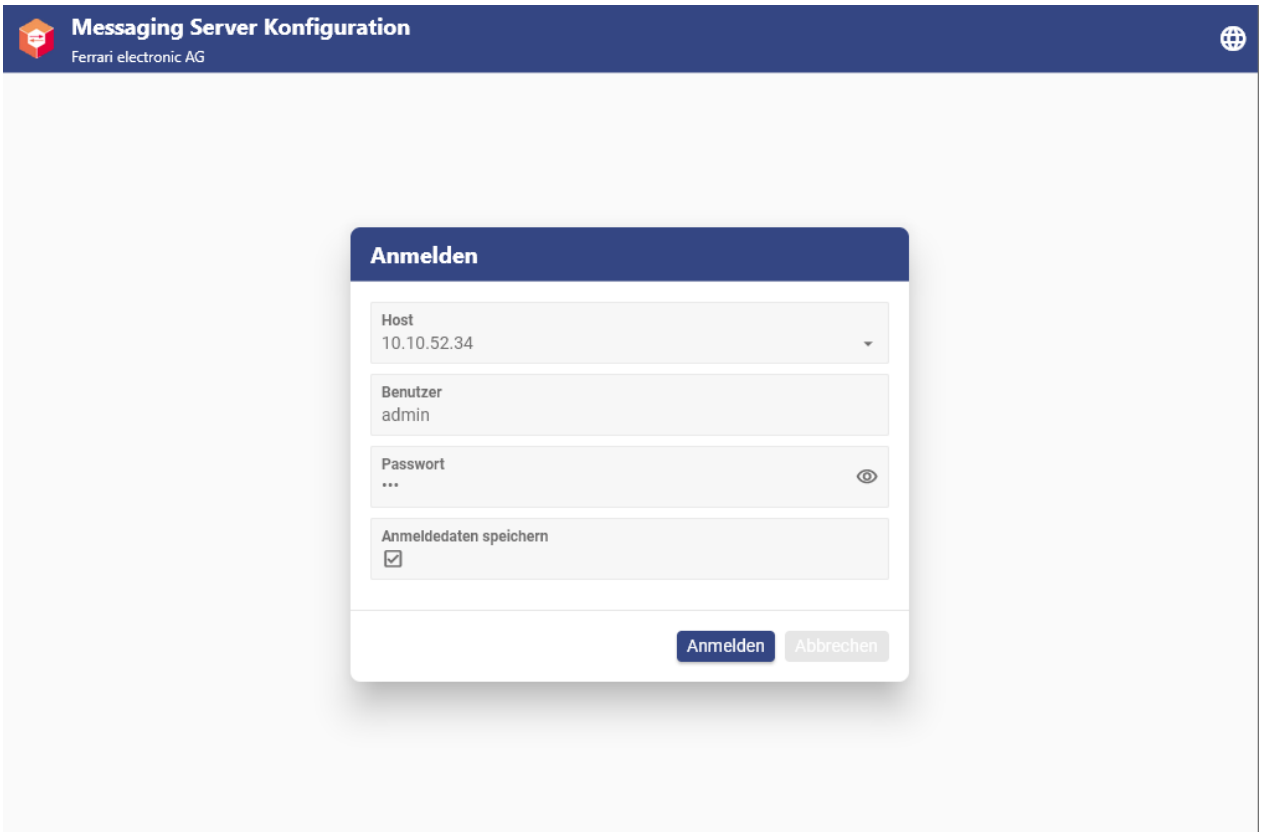
The various job types (FAX, SMS, VOICE, SMTP, EPOST, XRECH, ...) and file formats are also displayed.

The Recalculate job routing button can be used to rebuild the routing in the tables. This is necessary, for example, when components are stopped so that the jobs are not routed to these components in the case of orphaned entries and thus get stuck in the job status.

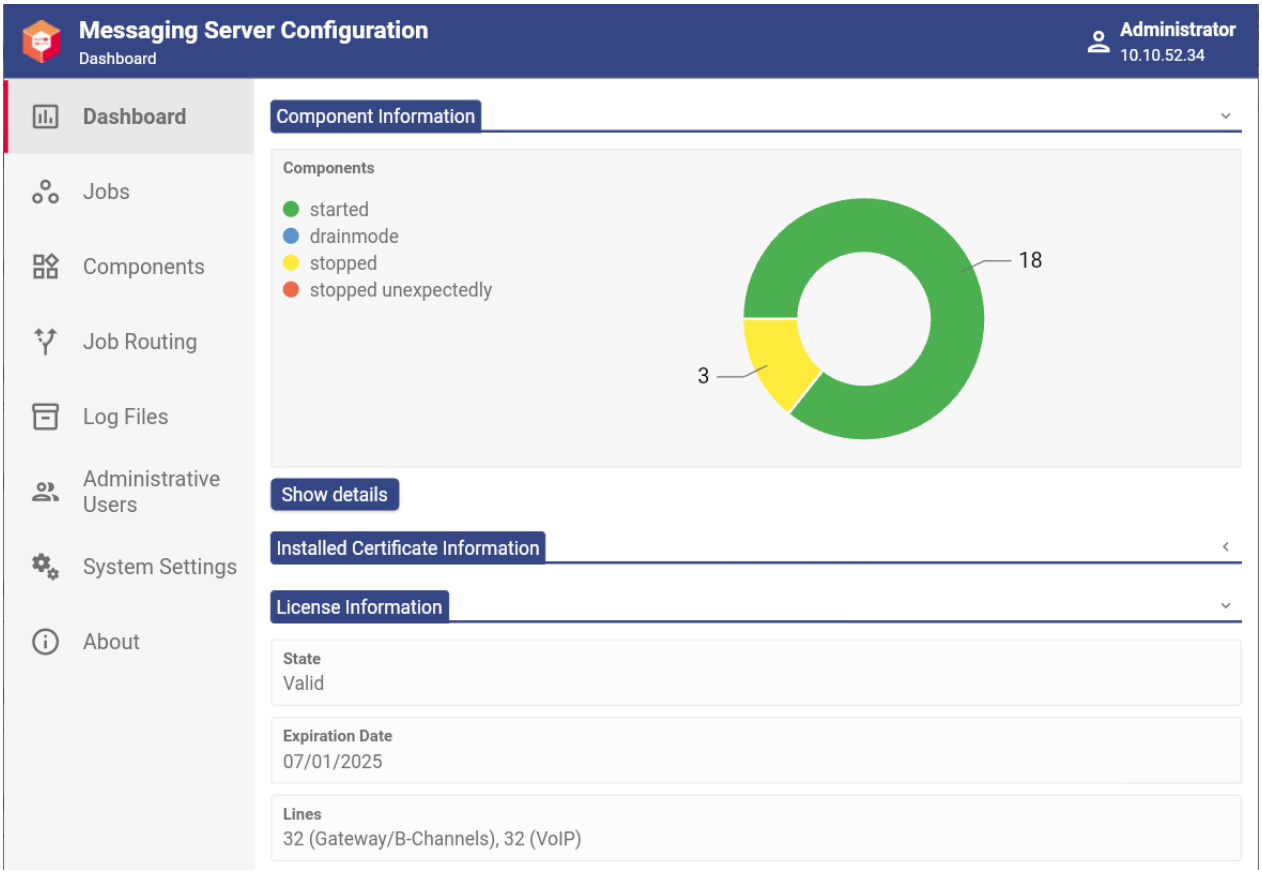
5.3. Browser-based configuration interface

To open the browser-based configuration interface, the address *https://messaging-server/cfg* can be entered in the browser (where *messaging-server* must be replaced with the name or address of the real server). The OfficeMaster Suite installs the WebServer role for the Client Gateway - an IIS which binds port 443 and redirects to https://messaging-server:3216/cfg. The AuthGateKeeper runs on port 3216 and delivers the frontend to the browser. The communication between frontend and backend is authenticated via the AuthGateKeeper.

After loading the frontend, the login dialog appears. The same access data apply here as for the classic messaging server configuration program.



The function of the browser-based configuration interface largely corresponds to the classic messaging server configuration program. Some components cannot be configured, but there is extended functionality in some areas (e.g. the dashboard).


Messaging Server Configuration
Dashboard
Administrator
10.10.52.34
Dashboard
Jobs
Components
Job Routing
Log Files
Administrative Users
System Settings
About
Component Information
Components
started
drainmode
stopped
stopped unexpectedly
18
3
Show details
Installed Certificate Information
License Information
State
Valid
Expiration Date
07/01/2025
Lines
32 (Gateway/B-Channels), 32 (VoIP)

5.4. OfficeMaster Exchange Administration

The Microsoft Management Console can be expanded using plugin DLLs (MMC snap-ins). In this way, functions were added to the Exchange Server Management Console, which contain the settings on the Exchange Server for the OfficeMaster Suite integration.

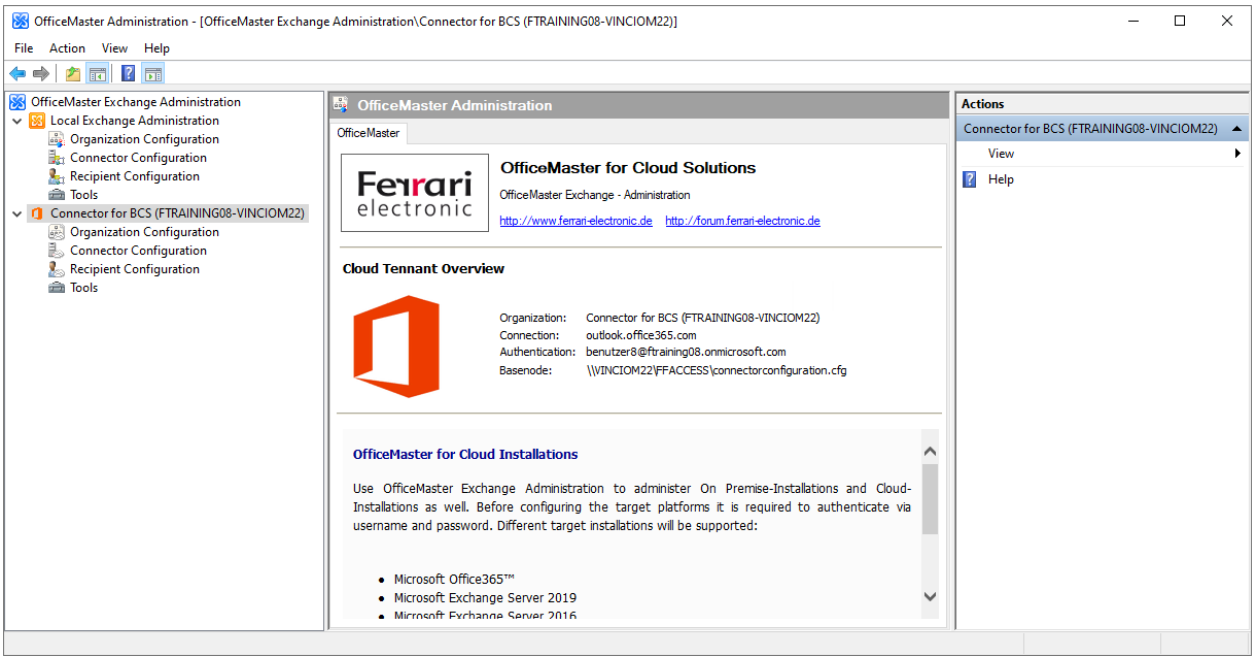


Figure 5.6: OfficeMaster Exchange Management

The use of the OfficeMaster Exchange administration is explained in detail in the *Connector for Microsoft Exchange* chapter.

5.5. OfficeMaster Gate configuration program

With version 8, the OfficeMaster Gate configuration program was removed from the OfficeMaster Suite installation. For SIP connections of the OfficeMaster Suite, it is not absolutely necessary to use an SBC or a media gateway (OfficeMaster Gate). If a OfficeMaster Gate is used, the OfficeMasterr Gate configuration program can be installed. The installer is located in *https://ferrari-electronic.de* > Downloads. There select *Unified Communications* and *Software* and click *Search*. Then select *Setup: OfficeMaster Gate configuration*, download and install.

The use of the program is explained in the *Manual: OfficeMaster Gate Firmware 5.1* (or *Manual for OfficeMaster Gate* for the older firmware version 4).

6. Base Configuration

This chapter describes basic configuration steps and the creation of some important components. Other components can be created and configured in a similar way. The configuration options of all components are presented in the chapter *Configuration of the individual components*.

6.1. Certificate Management

Certificates are stored in various places in the OfficeMaster Suite used to secure communication. This is how you log in administrators with a secured login, which also certificates the server with the OfficeMaster Suite. With the installation, OfficeMaster generates a “self-signed” certificate so that the initial Configuration is possible. A certificate request (CSR) is also created, which can be signed by a certificate authority (CA) to create a trusted certificate. This means that the self-signed certificate can then be exchanged.

Additionally, computer certificates may be stored in the following needed locations:

- Receive email messages
- Connection to Microsoft Exchange
- Connection to SMS-IP provider
- SIP connection
- Voicemail configuration web page
- Website for the WebConnector

It is also possible to create a certificate for trustworthy and also to use encrypted communication via NGDX. However, it does not use computer certificates, but rather certificates based on phone numbers. Here, a self-signed certificate is initially created, and a certificate request (CSR) is generated. With the self-signed certificate encrypted, but not authenticated, communication is possible. Ferrari electronic AG can sign NGDX-CSR (after verifying the fax number details). The certificates are managed in the configuration via *Extras > Certificates...*

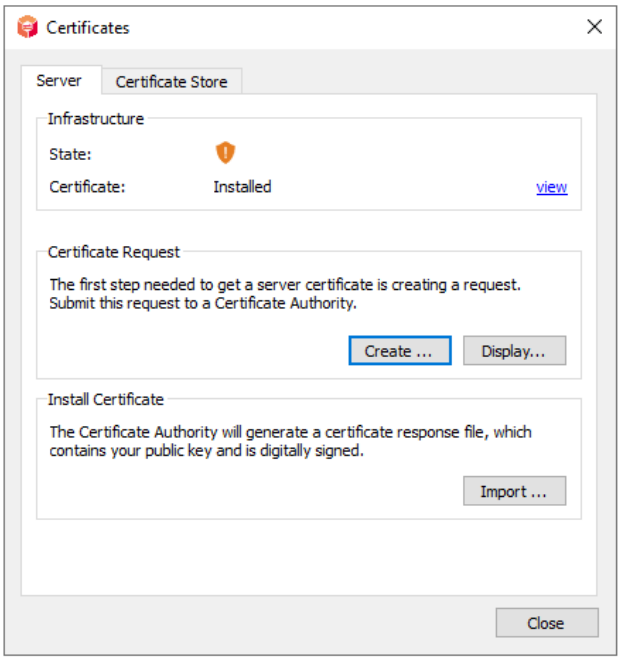


Figure 6.1: Certificate management

By clicking on the *Certificate storage* tab you can see the Self-signed certificates created during installation or later your own added.

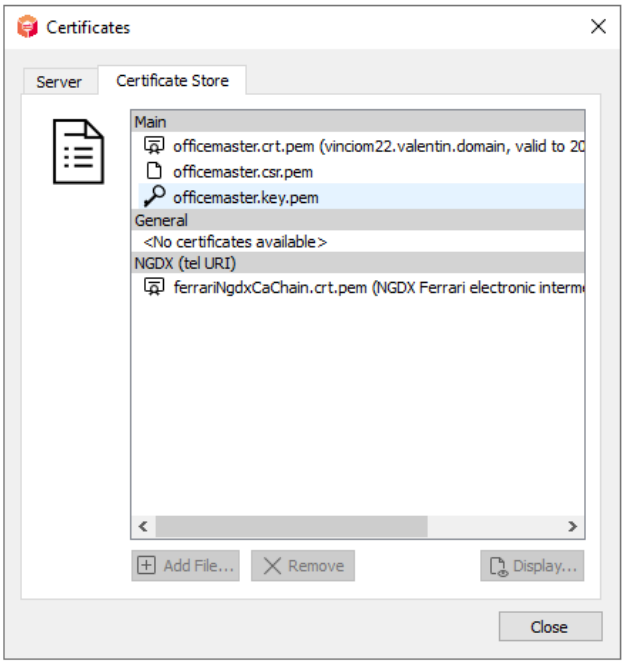


Figure 6.2: Certificate store

If the certification authority used is an Active Directory Domain Controller, the steps in the following section can be followed.

6.1.1. Generating a certificate with the certification authority of an Active Directory server

After installation, the OfficeMaster Suite generates a self-signed certificate when starting the AuthGateKeeper to ensure the initial communication of the configuration programs with the OfficeMaster Suite. In order to avoid warnings or error messages when accessing the website and to establish a secure connection between the individual components and the OfficeMaster Suite's AuthGateKeeper, your own signed certificates by a certification authority should be imported into the OfficeMaster Suite.

There are two basic procedures for importing certificates into the OfficeMaster suite:

- Generation of the private key with the OfficeMaster Suite and use of a certificate signing request (CSR). Generation of a certificate from the CSR by the certification authority and importing the certificate. The private key never leaves the machine, which is

advantageous from a security perspective. The private key must not be overstored with this method, as it is the only one that matches the certificate.

- Generation of private key and certificate by external tools (e.g. openssl) or the certification authority. With this procedure, both the private key and the certificate must be imported. Great care must be taken to ensure that the private key is not compromised when copying between machines.

The method described in these instructions utilizes the first approach, which is the simplest and most practical option when employing an Active Directory Domain Controller. However, the sequence of steps is also identical when using another certification authority (CA), with the exception that the certificate request is forwarded to a specific Certification Body, which then verifies the accuracy of the data in the certificate.

All subsequent steps require administrative authorizations on the OfficeMaster Suite server and partly in the Active Directory (certificate request).

Generate certificate request

The certificate request can be started via the messaging server configuration menu “Tools” -> “Certificates” -> “Create”.

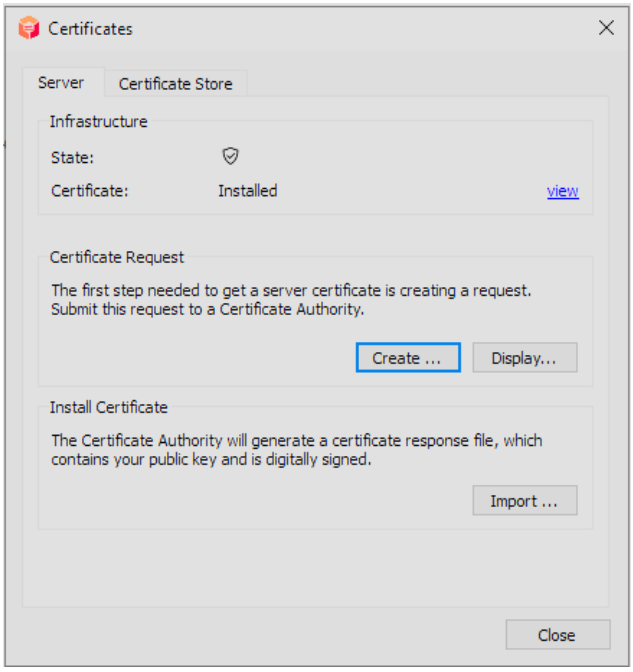


Figure 6.3: Certificate store

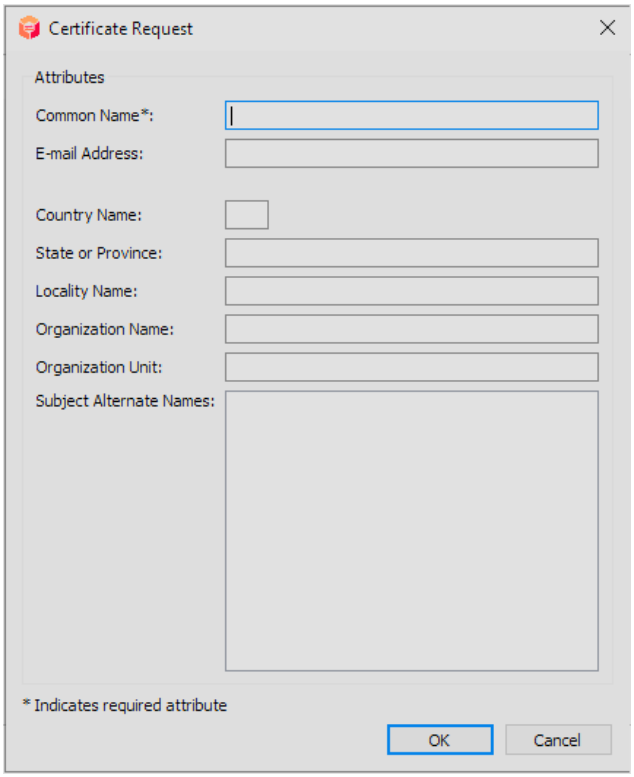


Figure 6.4: Certificate request dialog

The full name (fully qualified domain name, FQDN) of the local computer must be used as the common name (CN). The same applies to the alternative name fields (subject alternative names, SAN). In the example in the following image, **.test.local* is the name of the Active Directory domain. This must be adjusted according to the domain used.

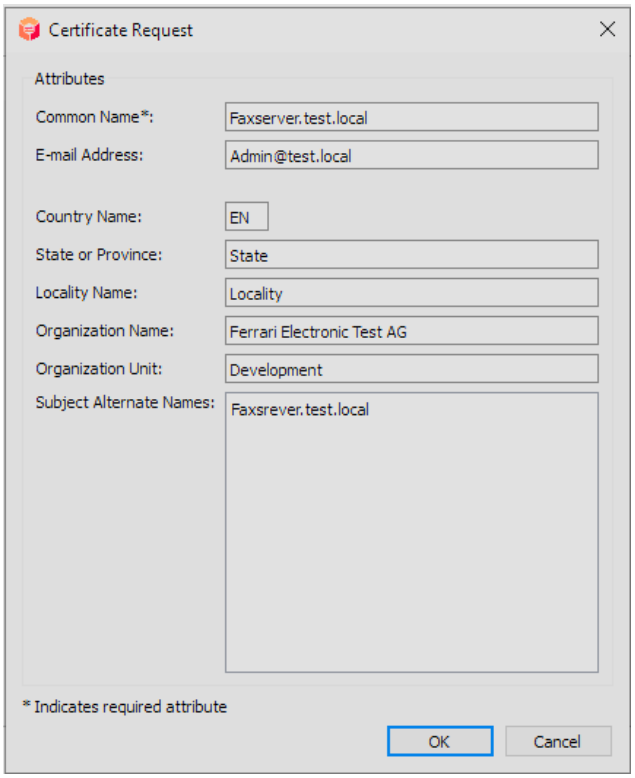


Figure 6.5: Example of a certificate request

After the certificate request has been created using the “OK” button, it can be accessed using “View”. Now the displayed content can be copied and saved as a certificate request file using Notepad (or another editor) (saving is optional, often the content can be copied directly into an input field of the certification authority).

Create certificate

The certificate request must then be passed to a certification authority (CA) so that it can create and sign a suitable certificate. The example below illustrates this using Active Directory Certificate Services. To do this, you must use a browser to access the address of the server that has the Active Directory Certificate Services role installed, e.g. https://servername/certsrv.

After successful authentication, the content of the previously generated certificate request can now be inserted via “Request a certificate” -> “advanced certificate request”. “Web Server” has proven to be suitable as a certificate template. The certificate can then be downloaded in Base64-encoded format (the formats **.p7b*/PKCS#7 and **.cer*/DER, which are also offered, are not suitable for the OfficeMaster Suite without conversion).

Import certificate into the OfficeMaster Suite

The certificate generated in this way can now be imported into the OfficeMaster Suite (Messaging Server Configuration->Extras->Certificates->Import):

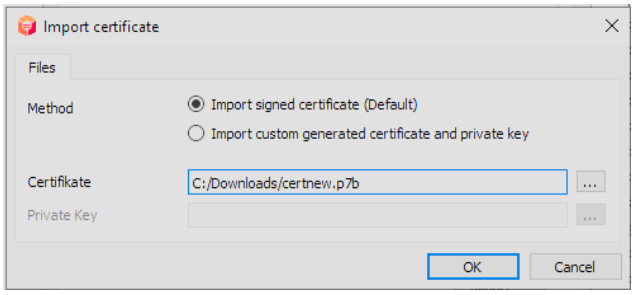


Figure 6.6: Import certificate

This ensures that when the TLS connection is established, the signature chain of the certificate can be checked and the connection is therefore authenticated.

> **Note:**
> The OfficeMaster Suite expects Base64 encoded PEM files.

When a new certificate is imported into the OfficeMaster Suite, AuthGateKeeper also creates a **.pfx* file. Like the PEM files, this is located in the PKI folder under %PROGRAMDATA% \FFUMS\fmsrv\data.

Import certificate into the Internet information server

If the web interface for voicemail or webfax (Clientgw) is also used, the certificate must also be imported into the Internet Information Server (IIS). To do this, the certificate must be available in the PKCS#12 file format as a **.pfx* file (including the private key). A **.pfx* file is automatically created by AuthGateKeeper when importing the PEM file.

This certificate (*.pfx file) must then be imported into the Internet Information Server on the OfficeMaster Suite server and configured as the standard certificate for https connections. To do this, start the IIS manager on the OfficeMaster Suite server and switch to the localhost address:

Figure 6.7: Internet Information Services Manager

By double-clicking on “Server Certificates” you can access the locally existing certificates. The default self-signed certificate “OfficeMaster.UmsSite” can be seen there. The previously created certificate (**.pfx* file) can be imported using “Import” in the action panel. During the import process, “Web Server” or “Web Hosting” should be selected as the certificate store instead of Personal.

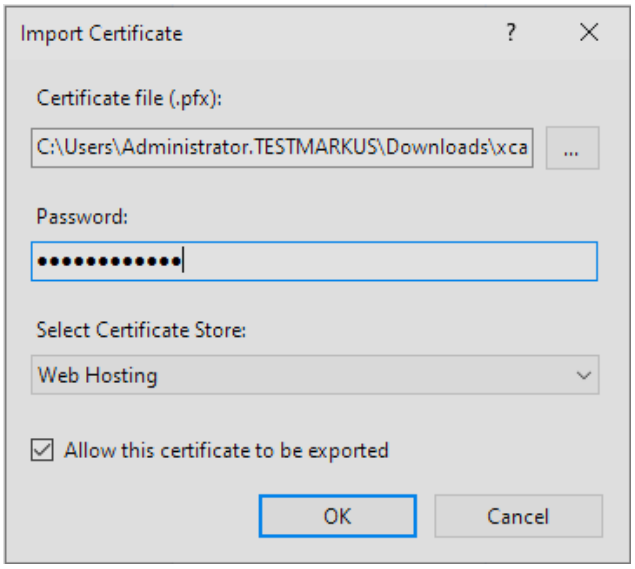


Figure 6.8: Certificate import dialog

After the certificate has been imported, it still needs to be defined as the standard for https access. To do this, click on the “Default Web Site” in the IIS Manager and select the previously imported certificate in the action panel via “Bindings”.

Figure 6.9: Dialog Edit Site Bindings

If necessary, all existing website connections should then be reset or restarted using “iisreset” from the command line. During this process, all locally hosted websites will be temporarily unavailable.

The correct installation of the certificate can be checked by visiting the website in a browser (https://FQDN of the computer/fax). If the existing lock is closed, the certificate was installed correctly:

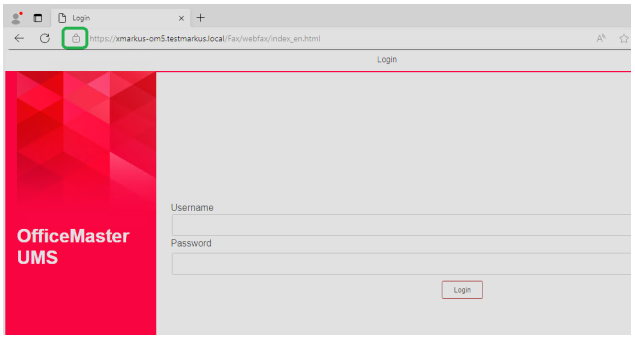


Figure 6.10: OfficeMaster UMS page with accepted certificate

Certificate file format conversion

ASN.1 (Abstract Syntax Notation One) is defined in the ITU standard X.680ff and is also used by the ISO. The ITU standards X.690ff define encoding rules for ASN.1 descriptions. Common ones are BER (basic encoding rules), PER (packed encoding rules), CER (canonical encoding rules) and DER (distinguished encoding rules). To put it simply, ASN.1 is a description language for data objects or structures and the encoding rules define how binary data streams are created.

PKCS (Public Key Cryptography Standards) are a series of standards that describe the encoding of cryptographic keys. PKCS#1 (RFC8017) is from/for RSA, PKCS#8 (RFC 5958) also supports other cryptographic methods. Both use ASN.1/DER to encode the keys.

The structure of public key certificates is defined in the ITU standard X.509 as an ASN.1 description. DER is commonly used for certificates and keys.

Different file formats are used for certificates, CSRs and keys. The following list provides a brief overview:

- PEM files: These are the most commonly used on the web because OpenSSL uses this format. They are Base64 files that encode certificates, certificate requirements or private or public keys in DER format as a text file. A text header or footer around a Base64 block shows whether it is a certificate, a certificate request or a private or public key (optionally encrypted with a password). Chaining these Base64 blocks together is also permitted, for example to be able to save a certificate chain.
- DER files: These are binary files which can contain all forms of certificates and keys in DER format. The file extension is **.der* or **.cer*. Its use is widespread in the Java environment.
- P7B files: These are Base64 files of certificates or certificate chains based on PKCS#7. Private keys are not included in P7B files. PKCS#7 forms the basis for S/MIME (RFC5652).
- PFX files: PFX files use PKCS#12 (RFC 7292) and contain both private key and certificate. This means that PFX files must be treated confidentially and can be protected with a password. PFX is a binary format used on Windows platforms (e.g. by the Internet Information Server).

Conversion of certificate files is currently not easily possible using Windows on-board resources. If you are familiar with external tools such as openssl, you are welcome to use this to convert certificate files. To simplify the conversion, reference is made to the third-party tool xca (http://hohnstaedt.de/xca).

> **Note:**
> Any software that reads the private key should be subject to a trust check beforehand. The private keys must be protected. Simply converting public keys or their certificates is usually not a problem.

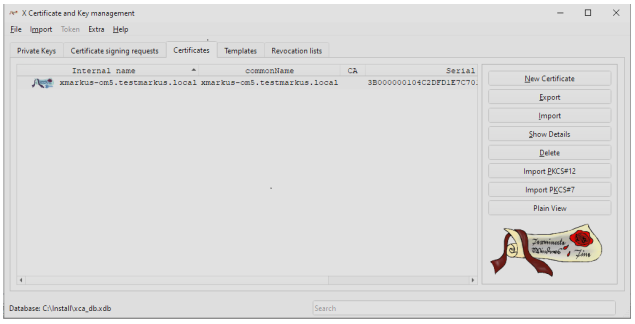


Figure 6.11: xca

After the software has been installed with standard settings on the OfficeMaster server, the first step is to create a new database (File->New Database). The previously created *.cer can then be imported via the “Certificates” -> “Import” tab:

In addition, the private key must be imported (“Private Key”> “Import”).

> **Info:**
> For security reasons, the private key should not be copied between machines, i.e. not leave the OfficeMaster server. That’s why in this example the xca software is also running on the OfficeMaster server.

By default, the private key of the OfficeMaster suite is available in the C:\ProgramData\FFUMS\fmsrv\data\pki\ directory as officemaster.key.pem in *.pem format. After successful import of the private key, the certificate can be exported via “Certificates”>“Export” as an encrypted PKCS#12 file in *.pfx format:

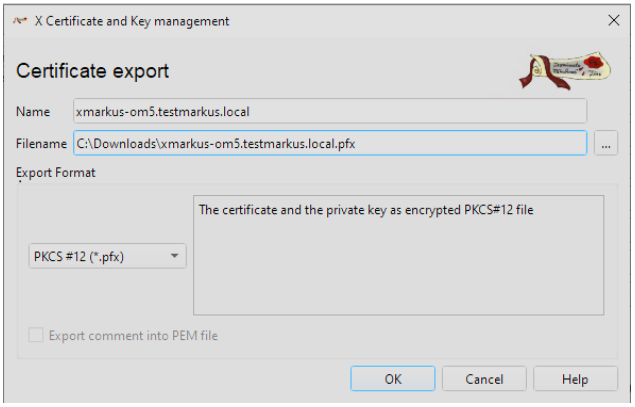


Figure 6.12: Certificate export

The conversion to PFX format shown in this example is carried out automatically by the OfficeMaster Suite when importing PEM files and is therefore not necessary in practice. Depending on the certification authority, however, different certificate formats can be delivered, which then have to be converted to PEM for the OfficeMaster Suite. In the standard process described above with a domain controller certification authority, no conversion is required.

6.2. DirectSIP

To connect to SIP trunks and IP telephone systems, you can use the Component SIP available. To configure, open the OfficeMaster Suite configuration and choose from the quick launch bar DirectSIP.

6.2.1. Create new component

On a newly installed system there are not yet created SIP components. To create a new component chooce *add component*. After that a installation wizard will show up.

After you have configured or adjust the default settings, such as *component name*, *Displayname* and *Server* , the special wizard for the SIP component will start.

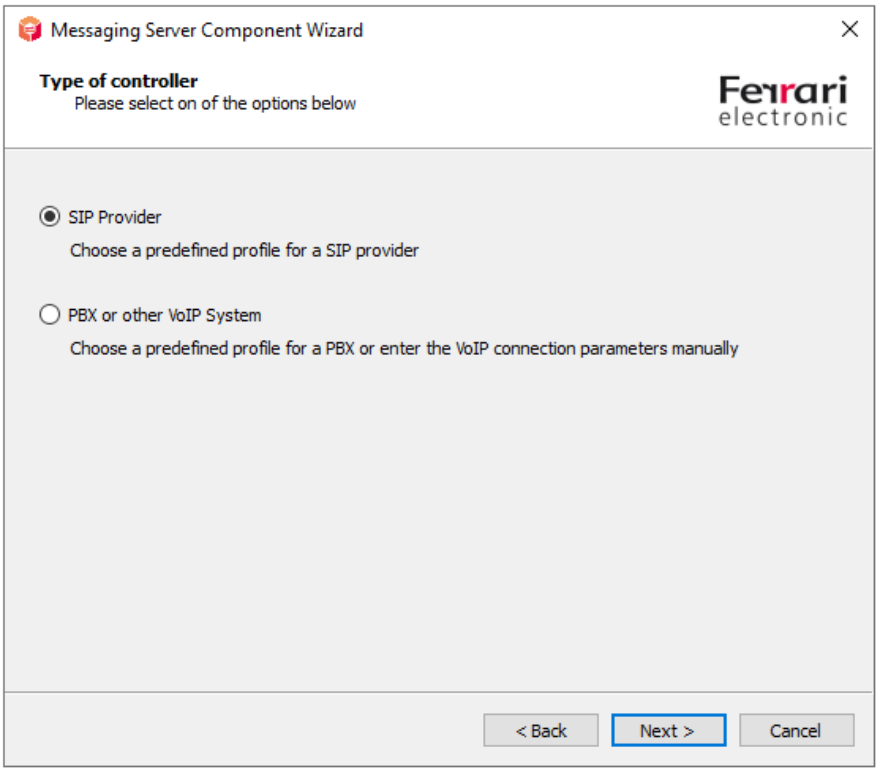


Figure 6.13: select type of connection

In the first step, select the type of connection to be used. This preselection forms the following dialog with the current predefined remote stations clearer.

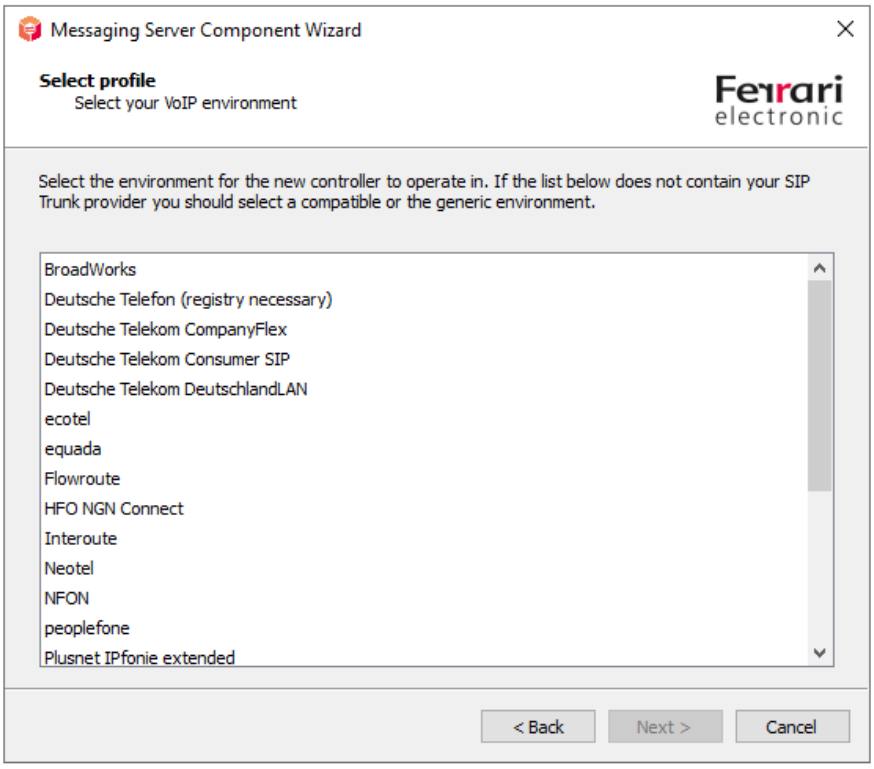


Figure 6.14: list of remote stations with template

The templates are constantly being expanded and updated accordingly. If the remote station you are using is not listed, select *General profile* and continue to follow the wizard.

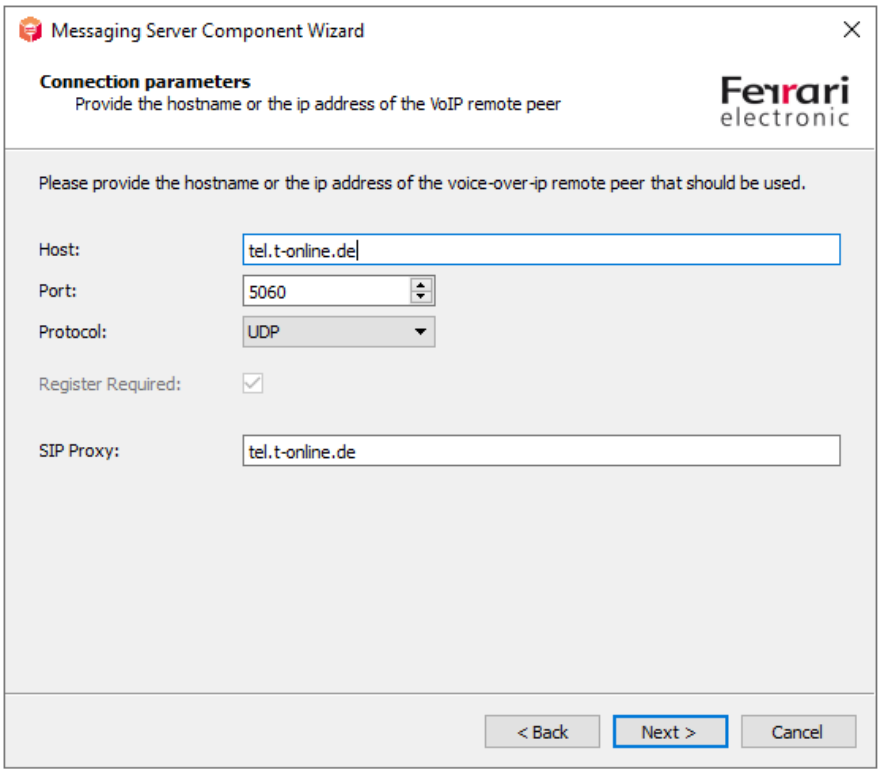


Figure 6.15: connection settings

Enter the connection information here, such as the IP address and port remote station.

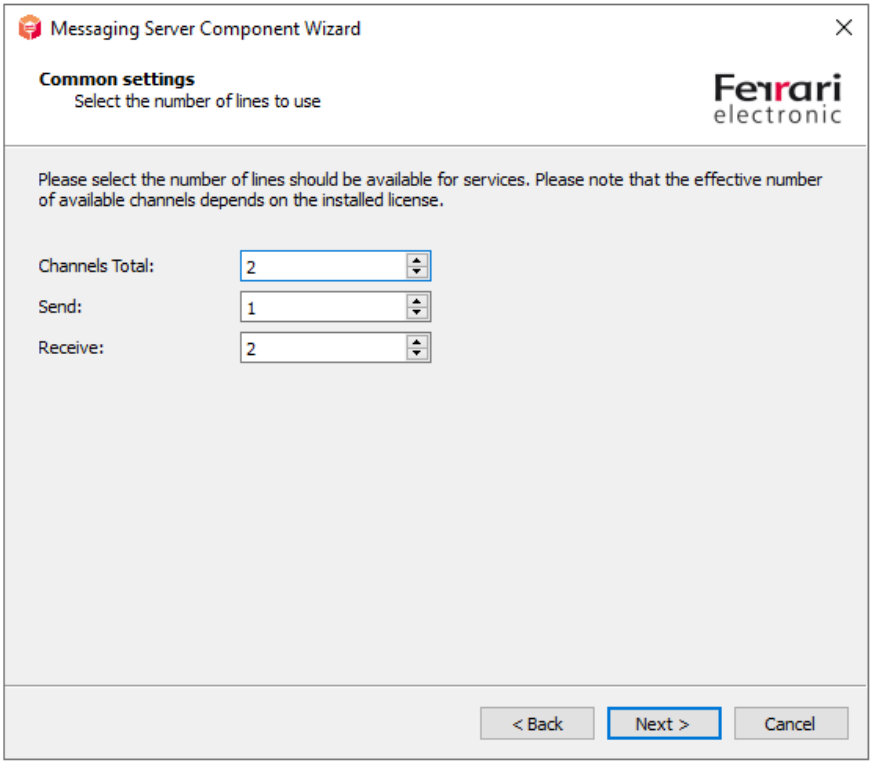


Figure 6.16: line configuration

Depending on the available licenses and the desired prioritization of incoming and outgoing messages, you can here configure the available lines.

Finally, when using the Fax function, enter the basic information for fax communication.

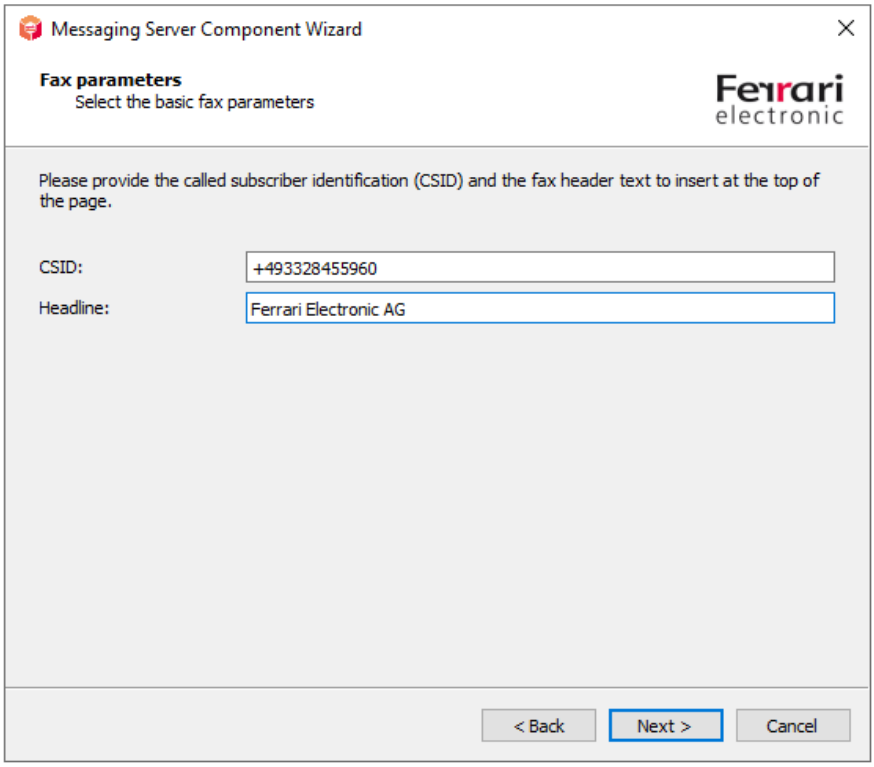


Figure 6.17: Fax settings

After going through the wizard, you will see the new created component (in this case sip2) in the overview of available SIP components.

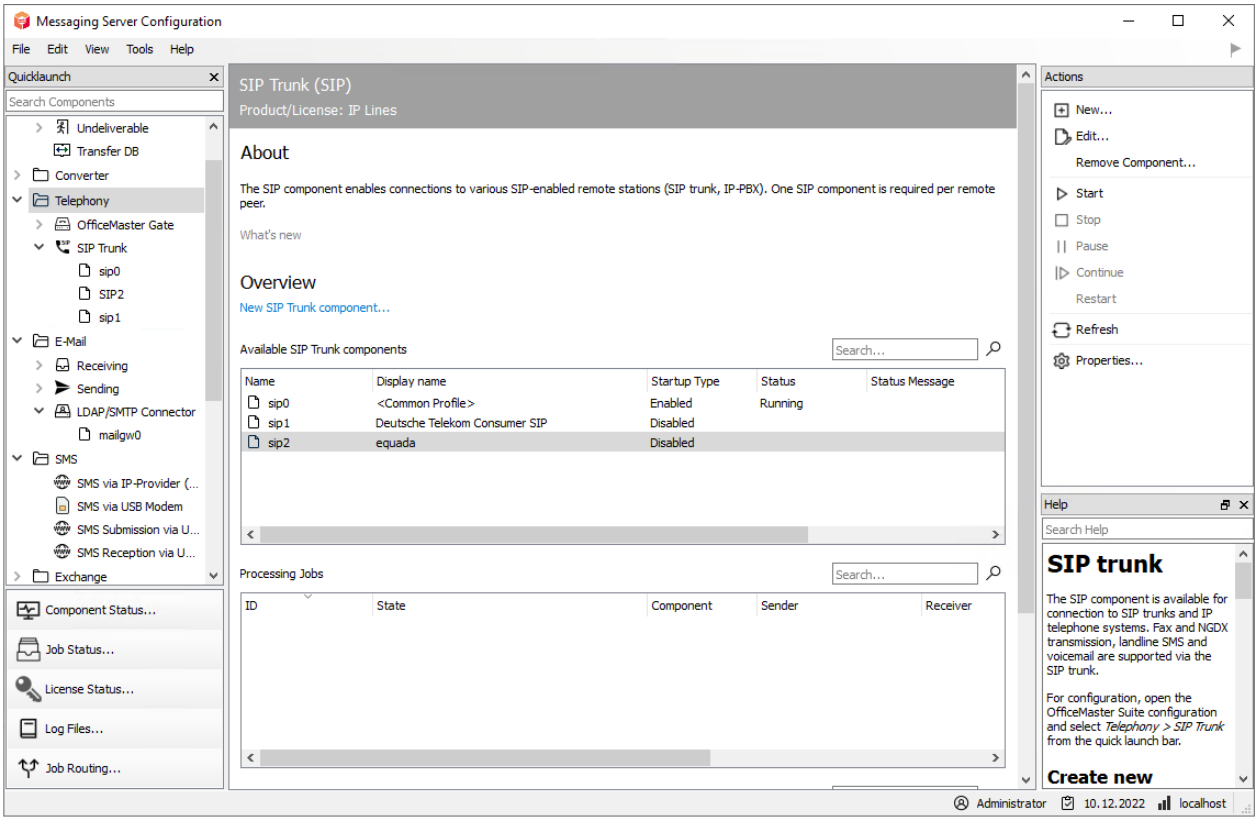


Figure 6.18: Newly created SIP component

The complete setting options for the connection can be reached by left-clicking on the component in the quick start bar or by right-clicking from the main field from the main field.

At this point, you can change further settings, e.g. for NGDX or the routing based on the dialed phone numbers.

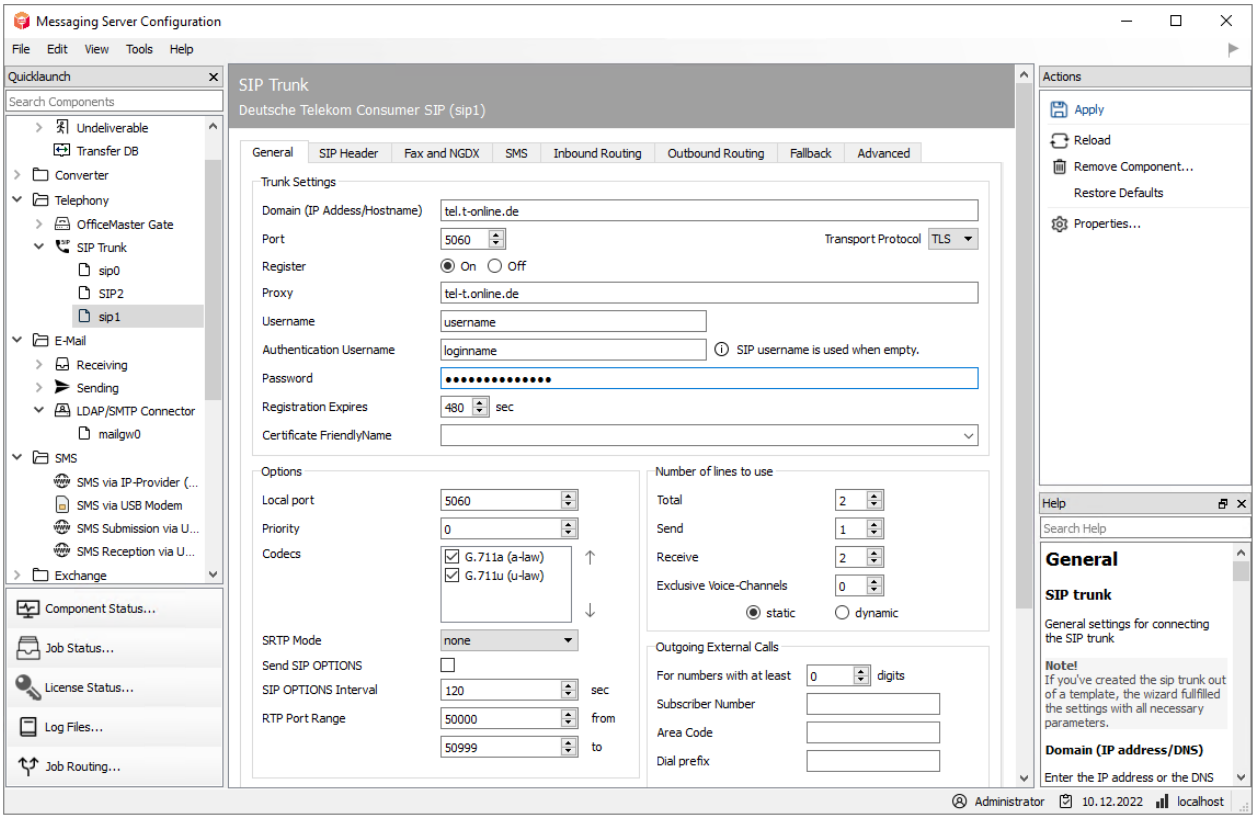


Figure 6.19: Complete configuration of the component

Note!

Have you had to make an adjustment for an existing profile, or a connection which is not yet listed? We would be pleased to receive your feedback and will be happy to add this for upcoming OfficeMaster Suite releases.

6.3. ISDN controller

The ISDN interface is controlled by the component *OMCUMS*.

> **Note!**
> The ISDN controller is only included to maintain backwards compatibility. For new setups, we recommend (where possible) using DirectSIP. The public ISDN connections have already been almost completely converted to SIP. However, ISDN still exists as an internal connection on private telephone systems.

To configure the OfficeMaster Gate, open the *OfficeMaster Suite Configuration* and then click on Edit > OfficeMaster Gate... and follow the menu sequence. A dialog will pop up and on the left side under *Name* all ISDN cards, virtual cards and already added OfficeMaster Gate names that were found by OMCUMS at the startup will be displayed.

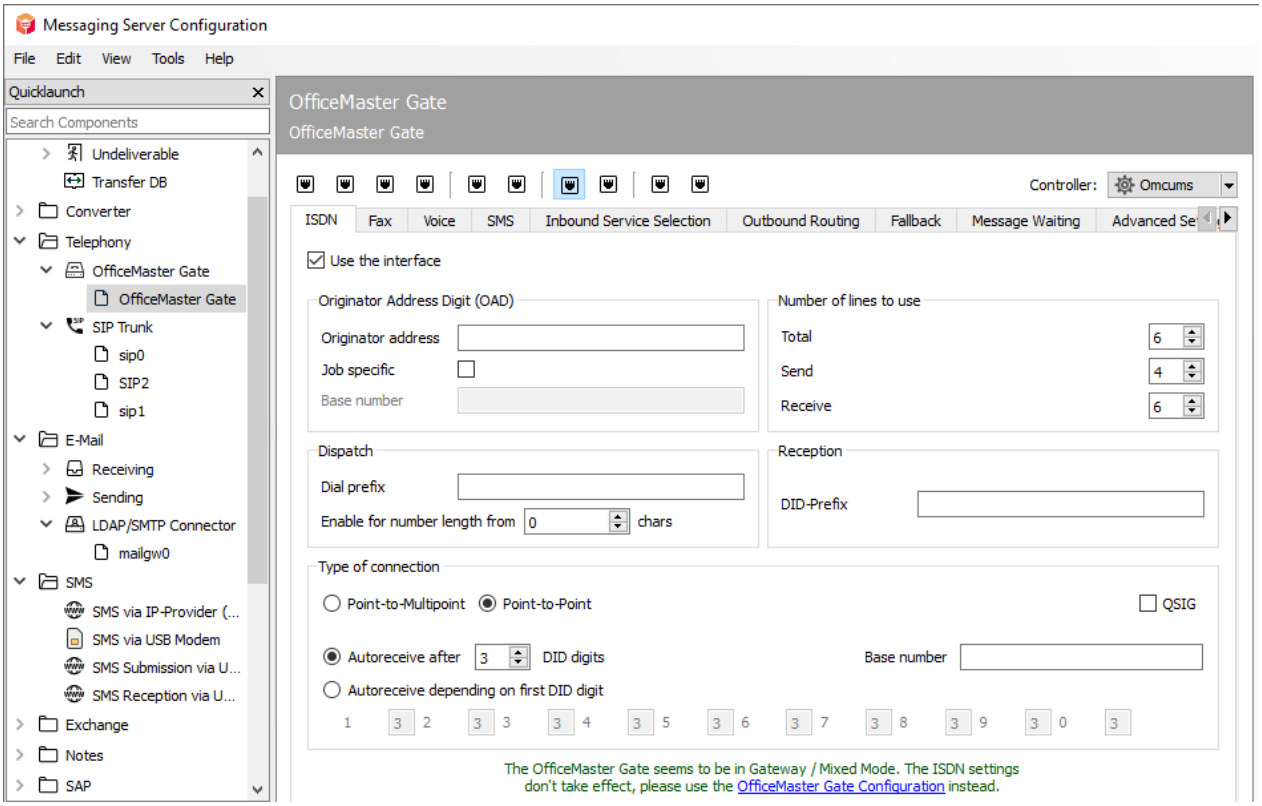


Figure 6.20: Hardware settings

At the top right, select the controller to which the listed gates and cards are assigned.

> **Note!**
> if it's about *CAPI* cards or *XCAPI*, the *JCISDN* component will be required.

If OfficeMaster Gate is connected to the network, it can be added to the OfficeMaster Suite. The available ISDN hardware is displayed in the left dialog box. OfficeMaster Gate carries the Prefix *omg* followed by the serial number. CAPI cards found are marked with the prefix *capi*. If necessary, the hardware used can also be given a suitable name subsequently. This is especially usefull in distributed installations. To do this, select the hardware and press *F2*. The configuration shown in the dialog box on the right always refers to the Hardware selected on the left.

If the *Use ISDN interface* check box is checked, the configuration tabs will be accessible. When the configuration is finished, press *OK* to save the settings and to apply them to the current operation of OMCUMS.

> **Note!**
> Before starting the initial configuration, the component OMCUMS should be stopped and should only be started after the settings have been accepted.

6.4. Voicemail server

With the extension for voicemail, the functions of the Voicemail server included in OfficeMaster Suite is unlocked. The general interrelationships are explained below.

Configurations on the voicemail server

In the quick launch bar, select the area for Voice or Voicemail to create and configure a component. After creating the component, you have extensive setting options, which are shown in detail in the chapter *Configuration of the individual components*.

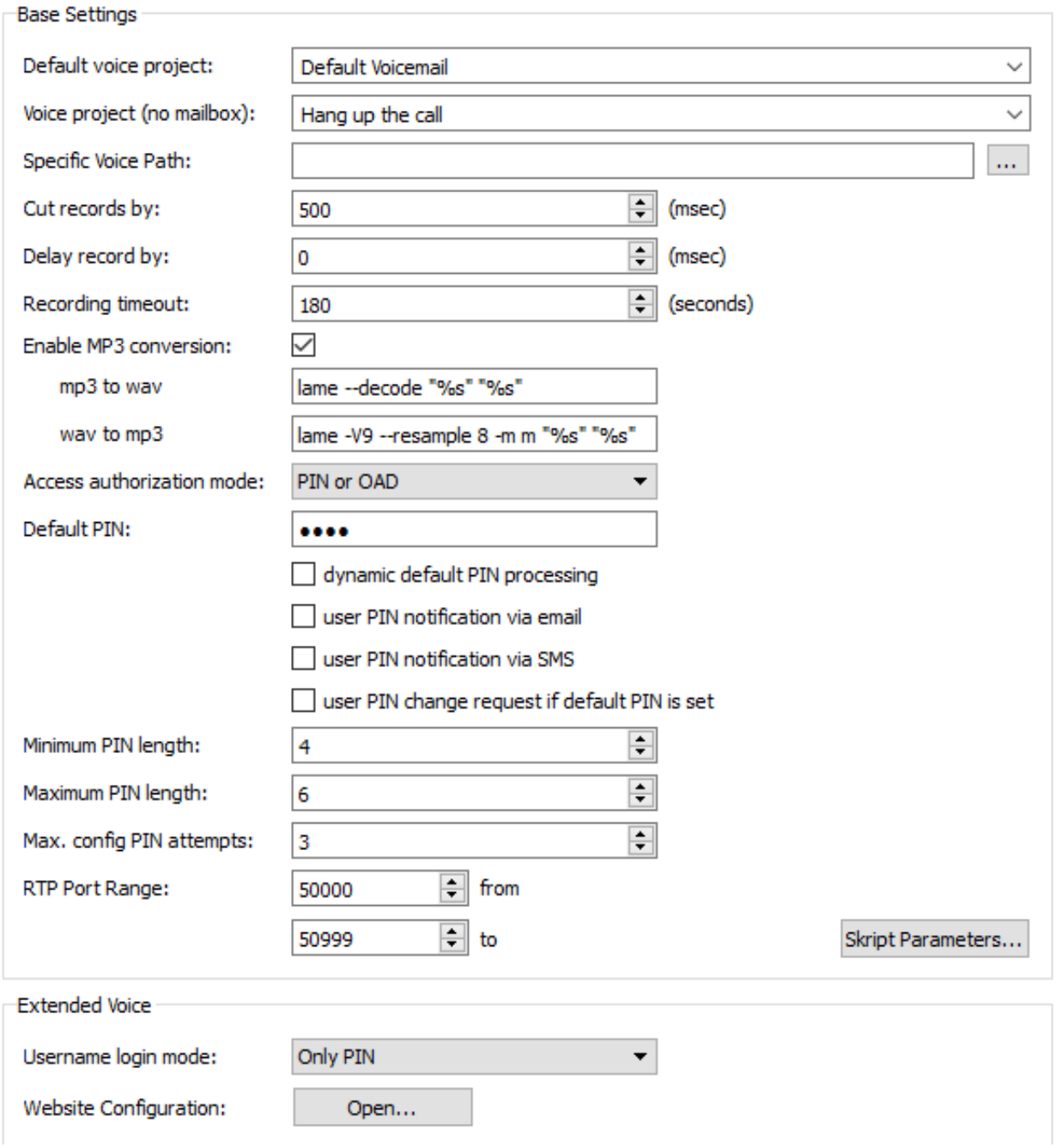


Figure 6.21: Configuration of voice server

6.4.1. Overall process of voice communication

Unlike faxes, voice calls must be decided directly when they are accepted, to which user the call should apply and which behavior should occur. When accepting the call, it must also be decided which project, which announcement and which language should be used. Accordingly, an incoming voice call is significantly more time-critical as a fax to which the entire IT infrastructure must be adapted.

Sequence of a voice call

- The call is established by a SIP trunk and thus the component SIP or an OfficeMaster Gate in the direction of the hardware controller of the messaging server.
- The hardware controller or the SIP component determine the voice connector associated with this call (e.g. *msx2kgate*) and the corresponding voice server (usually *voice0*). For this investigation all transmitted call number elements can be used (called/to, calling/from, redirected /diversion/history, etc.).
- The voice server establishes a UDP connection to the IPMedia process or OfficeMaster Gate and takes over the direct communication.

Note!
For the outgoing ones Connection from the voice server may have a corresponding rule in the Set up Windows Firewall. A clear sign of It is a firewall problem if, during test calls to fax numbers, the Fax signal can be heard, but not with calls to voice boxes corresponding standard announcement.

6.4.2. Projects included in the voice system

OfficeMaster provides several projects after the installation that can be used without major administrative effort that can provide various basic functions. This Projects are stored in ".. \data\voice" of the messaging server in the form of Subfolders created with description file and LUA script.

The voice system consists of several projects connected in series, between which are constantly switched. These projects are to be understood like individual states in a state graph. There are often multiple entry and exit points.

To keep things easily managable, not all projects are selectable as start-up projects. Which project is loadable is specified in the respective *.ini* file defined by the *loadable* flag.

Voicebox via Pilot ID

projectvoxdidcpn

The calling party number is set to the called party number, then the leap into the Extended Voicemail project takes place (*eVoice_projectStart*).

Extended voicemail

If *Extended Voicemail* is not available for licensing reasons, the system reverts to the *Standard Voicebox* described below. The individual projects perform the following tasks:

eVoice_projectStart

Entry point with setting the individual values for the variables.

eVoice_projectrecord

Recording a voice message.

eVoice_projectPlayAudio

If recording is deactivated for a period of time or a voice box, only the desired announcement is played and then the call is hung up.

eVoice_projectAnnouncementFromPhone

Recording of your own announcements controlled via the web interface.

eVoice_projectAnnouncementToPhone

Playback of your own announcements controlled via the web interface.

Recording function

projectrecordcall

When calling up this project, a short notice is given that the call is recorded and then the recording is started. After Termination of the call, a message will be send to the user with the corresponding recording.

For reasons of storage space, it is strongly recommended to enable audio conversion to .mp3!

Selection of the Voicebox to be called

projectvoxdid, projectdid

The caller is prompted to select which one to use by pressing a key Voicebox he wants to be connected.

“Recording Studio”

projectrecstudio

Recording an announcement, especially for creating announcements for IVRs. Creates an audio file in the valid file format for further use in the system.

IVR templates

Example of scripting your own IVR with the most important functions.

ivr xample_start

Entry point with timetable, public holidays, etc.

ivr xample_normal

The company is open, the caller has the choice of connecting to another subscriber or to leave a message.

ivr xample_closed

The company is closed, the caller gets an announcement played.

6.4.3. WebVoice

Users have the option of setting up their own voice mailbox via the web interface.

Base configuration

The basics for the interaction between voice server and the Components of the web services are controlled by the OfficeMaster Suite setup. Here, the *Internet Information Service* (*IIS*) is created and activated as a feature of the Windows Server.

The corresponding web pages for the IIS are available under %ProgramFiles% \FFUMS\fmsrv\Webservice.

To configure the web services, you would normally have to call various configuration files of the IIS but in OfficeMaster, with the tool FClientGwCfgPrg (callable via the configuration of the VOICE component), you can access these files in a simplified version.

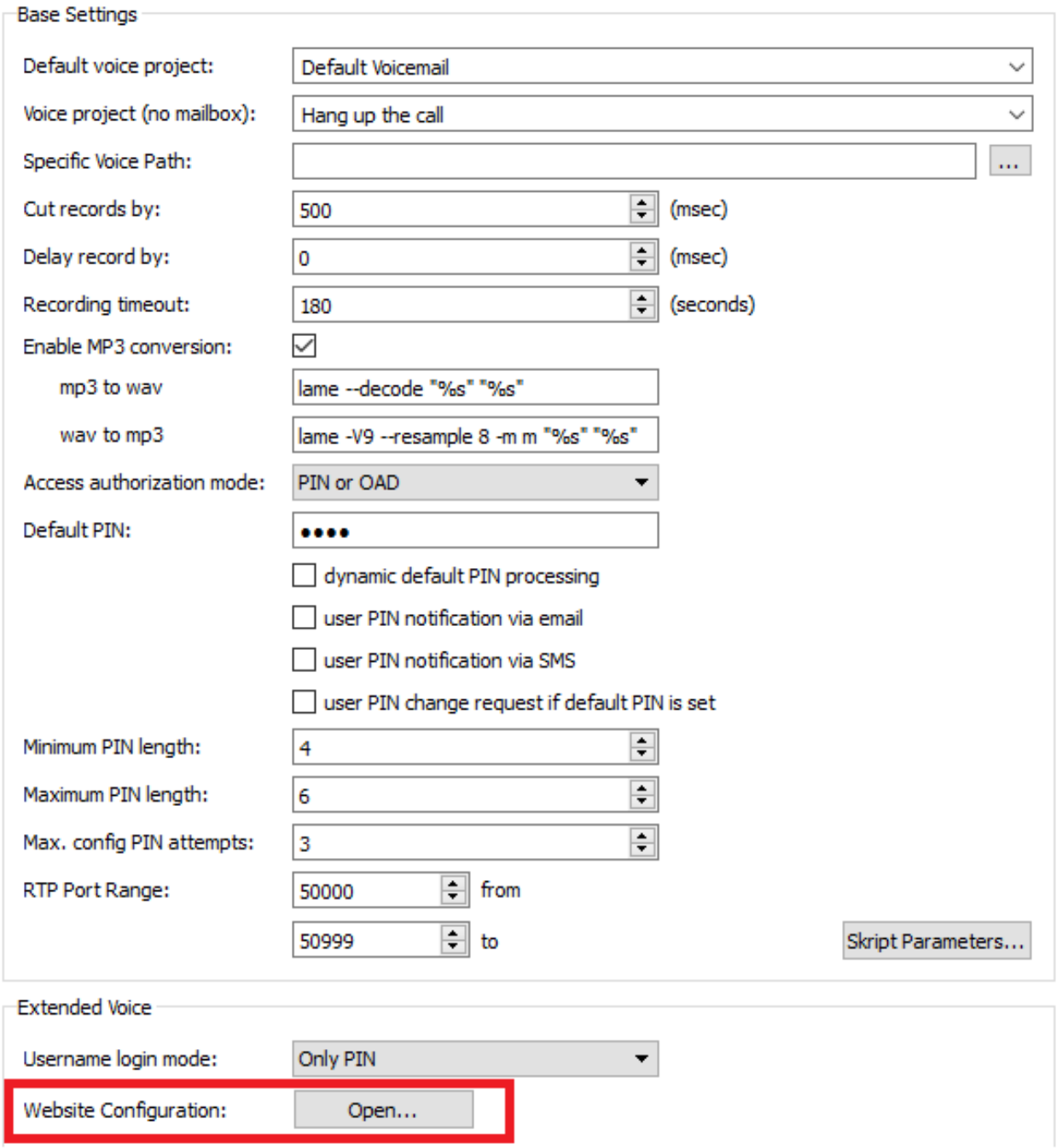


Figure 6.22: Start of the configuration program

Website address

The address of the website to be configured is entered here. Unless the default address after installation manually was changed on the IIS, this is either *http://SERVERNAME/ ums* or *http://SERVERNAME/fax*.

Configuration password

The access to the configuration is protected by the password “**OfficeMaster!**”.

After successful login to the server, the user will be able to configure the operating mode of the web page, the voice server and the corresponding connector for the user information.

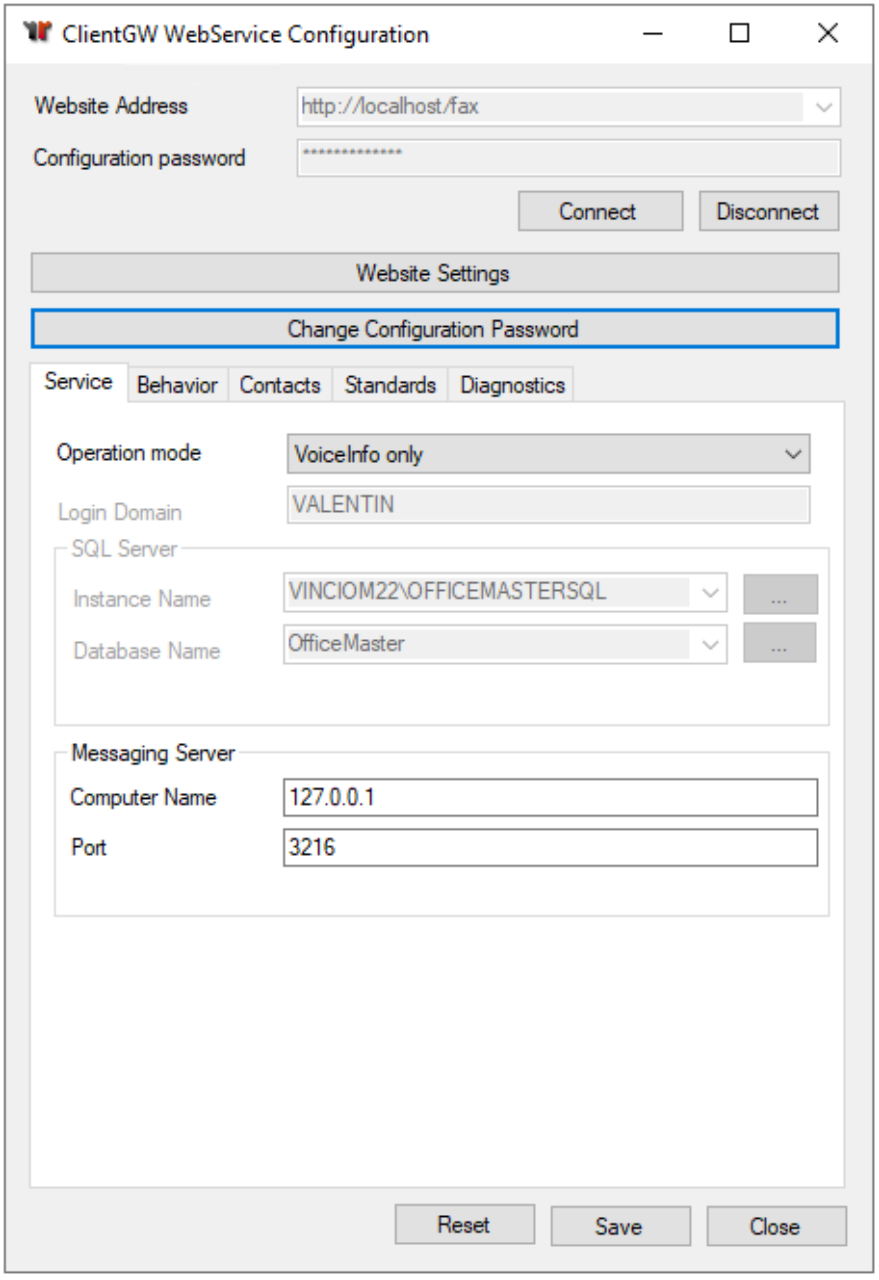


Figure 6.23: OfficeMaster client website setting

Operation mode

VoiceInfo only must be selected only for the main connector such as *Exchange*, *Notes* or the *SMTP* connector.

Login type (from OfficeMaster Suite 6.2)

Here you set the login variant of the users on the web front end.

- Username & Voice PIN
- Voicebox number & PIN
- Email address & Voice PIN

Voice component

Here is the used voice server component of the OfficeMaster stored. In the default case this is voice0 and does not need to be changed further.

Voice gateway

The voice server requires a component on which the user information can be requested and messages can be delivered. In Exchange environments this is usually *msx2kgate0*. In other environments this is *notesvoice0*, *univoice0* accordingly or *clientgw0*.

Change configuration password

It is recommended to change the default password so that no unauthorized access to the system can occur.

Permission levels

While setting up the Voice Server one must also define the authorization level of the user. Currently the following levels are available (with the permissions listed below):

without voice mail

If a user does not have a VOX number in their user data, it´s Voicemail will be automatically disabled.

without extended voice authorization

Once a user is assigned a VOX number, voicemail is activated and the standard project is used.

- Up to OfficeMaster 5.0.1 this is *projectVox,* from OfficeMaster 5.0.2 and so on is *eVoice_projectStart* used.
- *eVoice_projectStart* automatically falls back to *projectVox*, if the license condition is not met.
- *eVoice_projectStart* automatically falls back to *projectVox*, if no personal settings have been made yet.

extended voice user

A user's personal profile is initially created as soon as the user himself or the administrator wants to edit the profile for the first time. Through the intelligence of the website, a default profile is generated. This creates a subfolder on the messaging server based on the the VOX number from the user, which contains a profile description file.

The user can edit the following attributes:

- Load/edit/save own profile
- Language of automated announcements and telephone menu navigation
- PIN for remote inquiry
- Storage of the query-authorized phone numbers
- Change "*To my phone*" phone number
- Upload/record/rename/delete own announcements
- Assign action start points to individual days/time periods/weekdays
- Add announcements to action starting points
- Decide whether a message may be left for the action start points or only an announcement should be made

Administrator for extended voice profiles

The following points are selectable in addition to the normal voice user:

- Load/edit someone else's profile
- Change the Voice project
- Choose type of action start points between projects (subsequent selection of the target project) and voicemail

6.4.4. Audio files

The voice server works with file-level audio files. Here, the processing is project-based. If the audio file greeting.raw is called in the project *ivrExample_normal*, the system first looks in the subfolder *ivrExample_normal* for this file. If it is not found there, the system searches for it on a global level in the *Audio* folder.

This results in the possibility of both different files to maintain various sub-projects on one level, as well same-named files with different content in each projects to use.

6.5. Central conversion

One of the most important functions of the OfficeMaster Suite is the central conversion of the documents on the server. This involves converting documents that are to be sent by calling third-party software such as *Libre Office*, *Microsoft Word* or *Adobe Acrobat Reader*. This documents to be sent are converted into a graphic format, but also into PDFs (for NGDX).

If you have Libre Office installed on the server, the central converter will, after the successful installation of the OfficeMaster Suite, immediately be ready for use and does not need to be configured further.

If you want to use Microsoft Office instead of LibreOffice, you have to you set up an additional converter. We recommend the use of the OLE converter.

6.5.1. OLE converter when using Microsoft Office

The OLE converter described below uses the Conversion Microsoft Office. When *UAC* is on, it can (*[U]{.underline}ser [A]{.underline}ccess [C]{.underline}ontrol*) be used.

Creation of the OLE converter

In the quick launch bar of the Messaging Server Configuration, go to Converter > OLE Converter and then add a new component of this type.

Figure 6.24: Creating a new OLE converter

The creation of this new component is accompanied by a wizard, where the question for a service account takes place.

> Warning!
> This service account must be a local administrator!

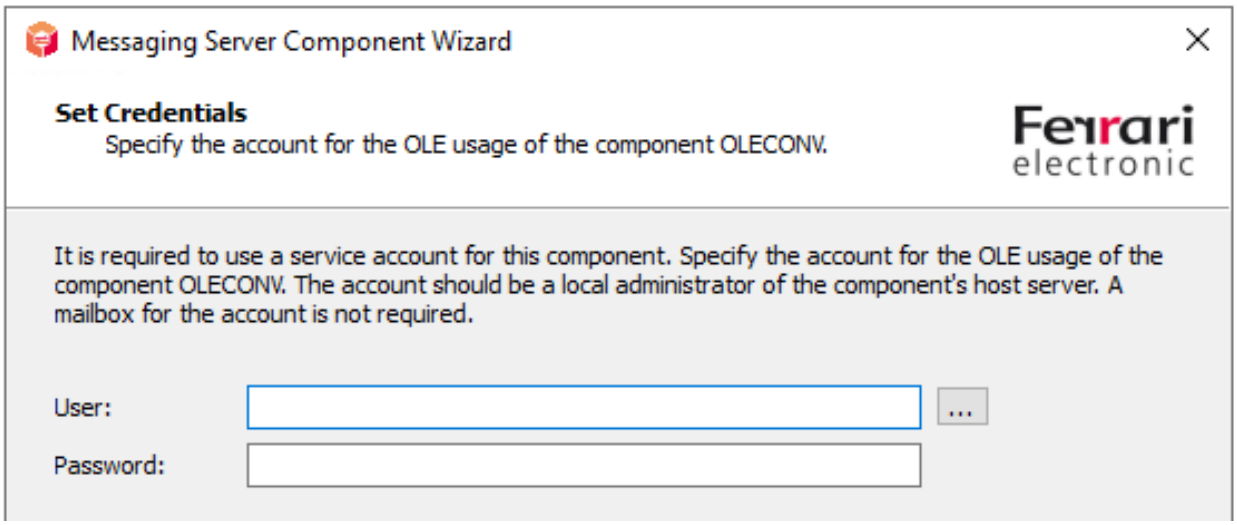


Figure 6.25: Entering the service account in the wizard for the OLE converter

The subsequent naming dialogs correspond to the standard wizard and can be implemented accordingly. After the OLE converter has been successfully created, the general configuration of the component will be available.

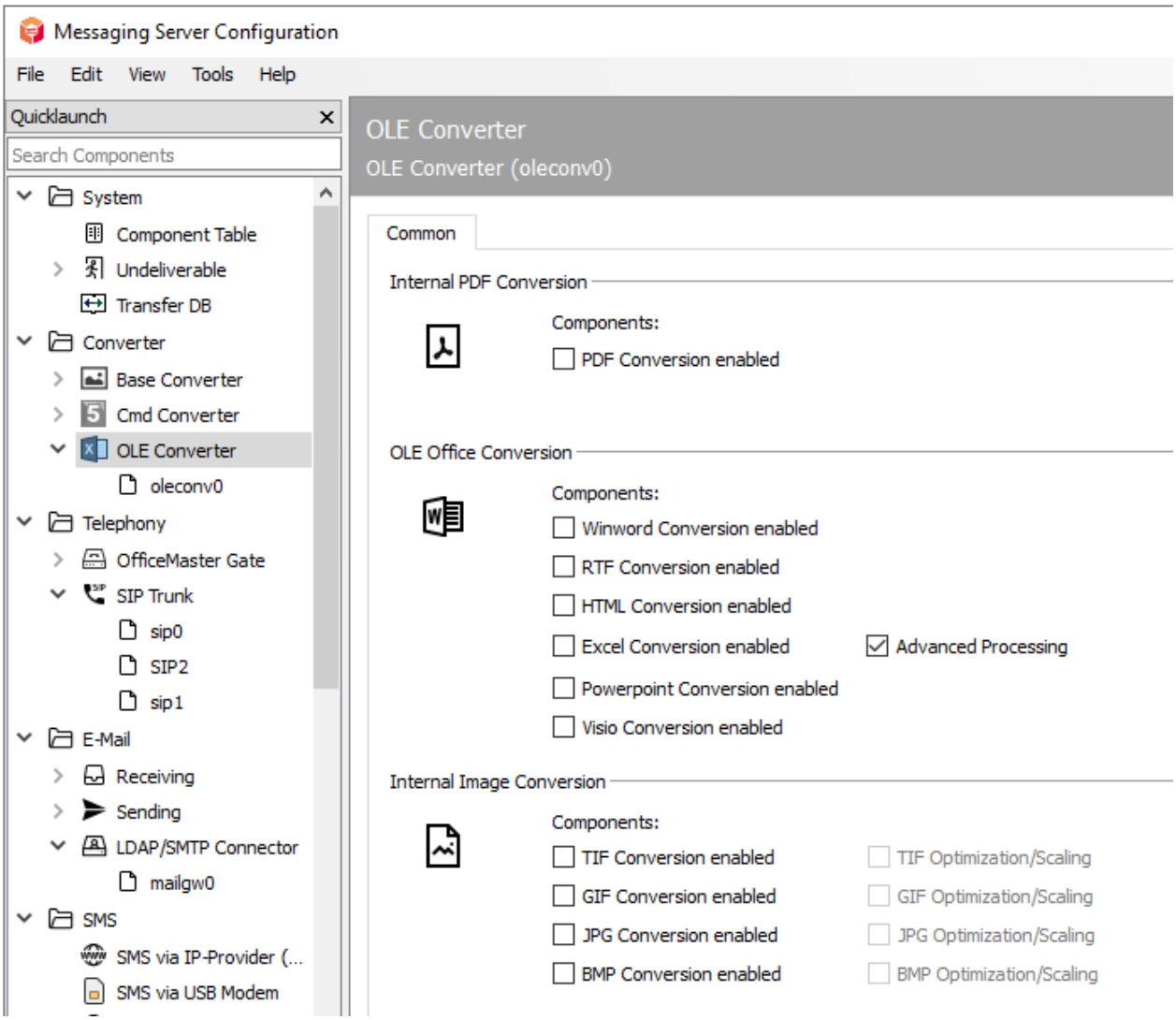


Figure 6.26: Configuration overview of the OLE converter for Microsoft Office and PDF

Internal PDF conversion

Enable PDF conversion

If the PDF convertion should be done by the OLE converter, the corresponding check mark must be set here.

OLE Office conversion

The document types for which the converter is to register are selected here. Only if the registration for a document type is carried out, the document can be converted by OLE converter into a graphic.

Internal image converter

If the converter is also to be used for graphic formats, click here to activate the appropriate format.

Deregistering the default converter for the desired formats

Enter in the configuration of the command line converter to deactivate the (undesirable) desired formats accordingly.

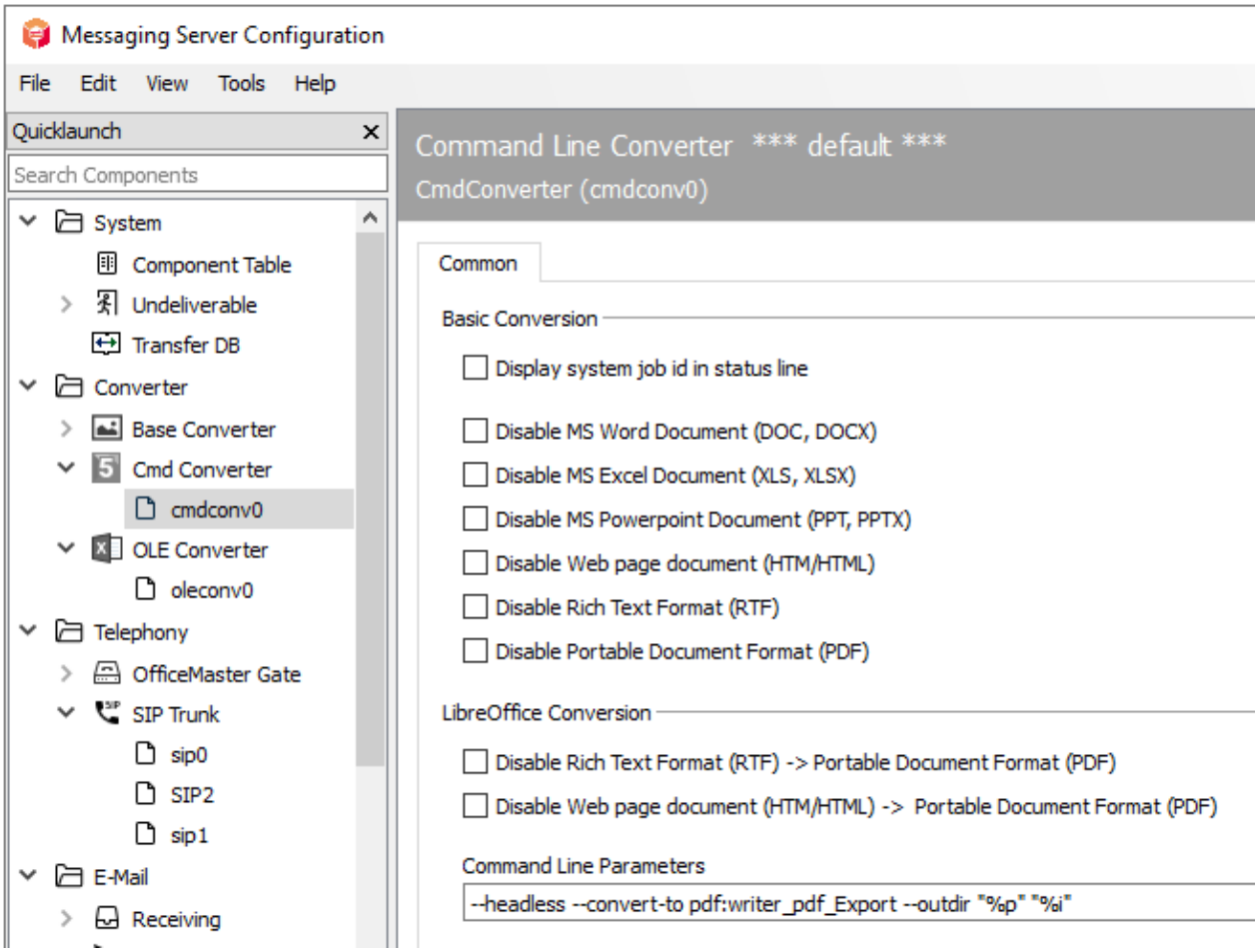


Figure 6.27: Disable formats in the command line converter

Then restart both converters to achieve correct job processing.

6.5.2. Base converter (BASECONV)

When installing the OfficeMaster Suite, a basic converter is also installed. This is responsible for converting incoming messages.

6.6. Automatic printing for received faxes

To print received faxes automatically on network printers, the messaging server has the *PRINTGW* component, to which receives call numbers can be assigned. In addition, PRINTGW can be assigned to print documents by other messaging server components, such as SAPCONN and Undeliverable (UNDLVRBL). To confgure such thing, go to the quick start bar under Print > Network Printer. First you need to create a new component and then you can configure it.

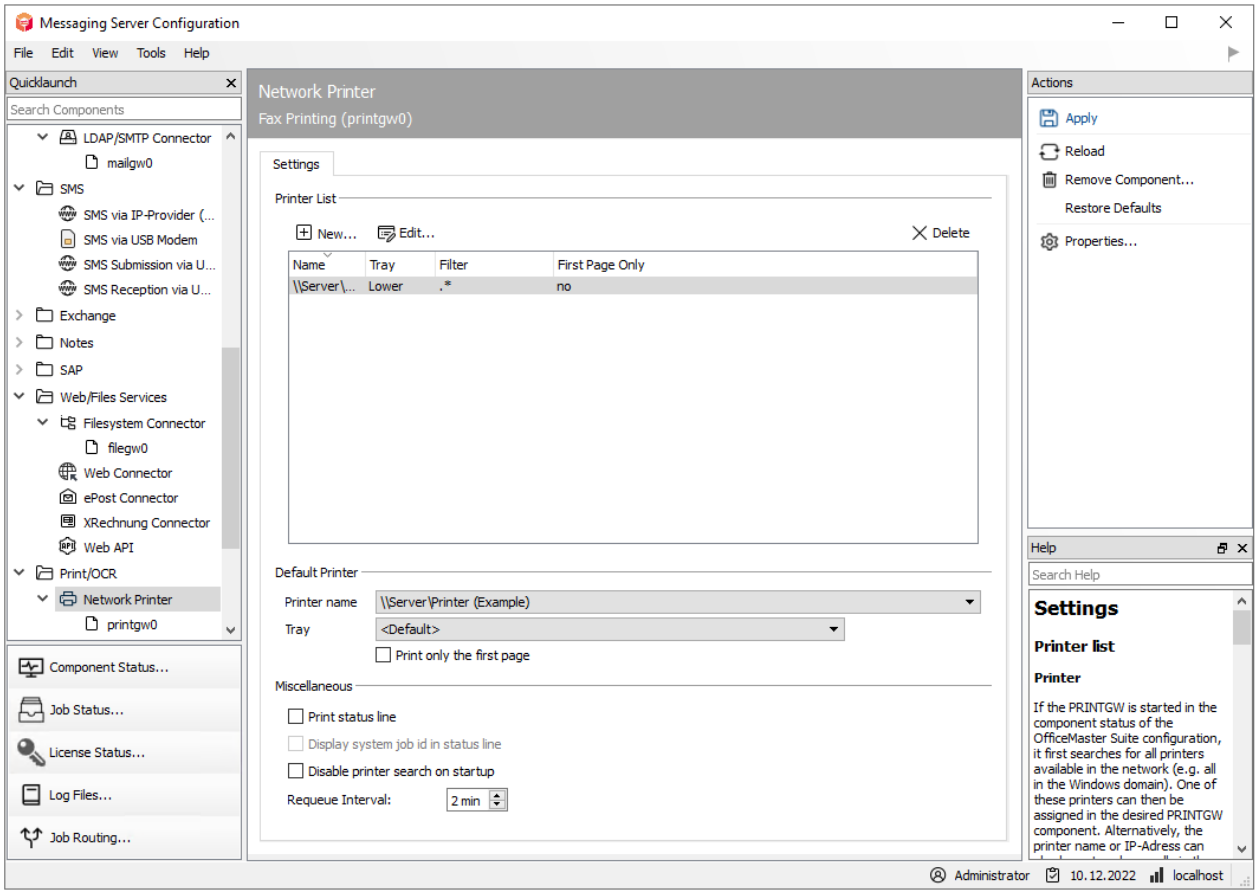


Figure 6.28: Add printer as output for messages

If the printing of received faxes is to take place on several printers distributed in the house, you can also use descriptive names like printgwSales or printgwFiBu, if each PRINTGW is to serve only one printer.

Host is usually the IP address or the resolved name of the OfficeMaster Suite Server.

6.7. Basic or system settings

The settings are divided into the following sub-items:

- General, next section
- Error handling, see call routing section for details
- International, see call routing section for details
- Drain mode, controlled shutdown or idling of the OfficeMaster Suite, details will follow.

6.7.1. General settings

Here you will find the setting options for the entire OfficeMaster Suite. These settings are cross-component.

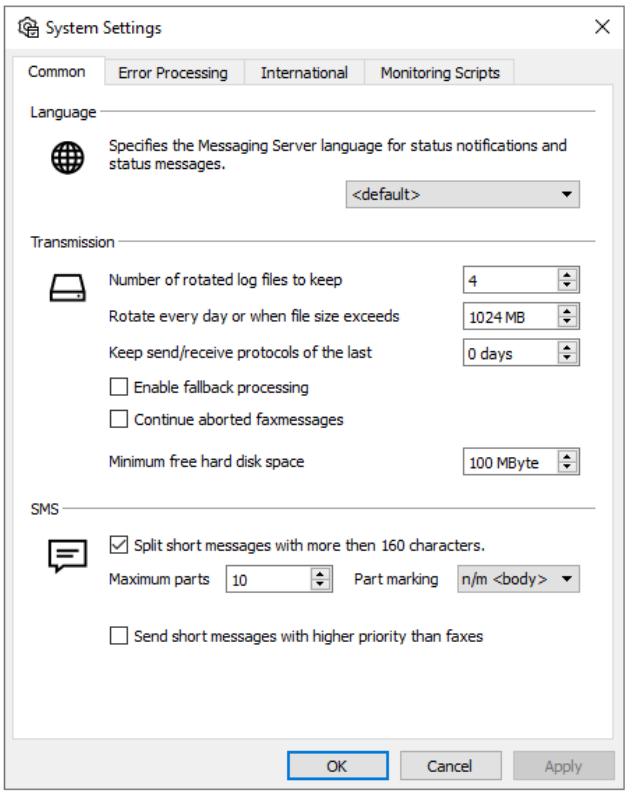


Figure 6.29: General system settings

Language

With this global language setting you set the language for status messages (to users and administrators).

Transmission

Store component log files for

In the delivery state, the log files are saved for 4 days and then overwritten. These are rotating log files.

Keep send/receive logs for

Leave the value at the default (***0 days***) if new created daily logs should never be deleted. However, to request the deletion of the logs in a specific time, please enter the time in days here.

Enable fallback mechanisms

The messaging server works internally according to defined routing rules. Each sending and receiving component registers for one certain type of orders. If the transfer of a job transfer is repeatedly faulty, the job will be transferred to another component that has another registered component for fallback routing.

Resume abandoned faxes

When using DirectSIP (fsip) it is possible to use this option. In this way, in the event of a fax transfer being aborted (outgoing), the aborted faxes are “forwarded/resent”. The normal send retries are taken into account in this case.

Minimum free disk space

If the minimum free memory capacity specified here is reached, the OfficeMaster Suite will no longer accept messages.

SMS

Here you can set whether short messages with more than 160 characters should to be split and the maximum number of set text messages for an order.

In addition, SMS can optionally be sent with a higher priority than faxes.

7. Connector for Microsoft Exchange

The Exchange Connector in its three forms is used by the majority of messaging server installations.

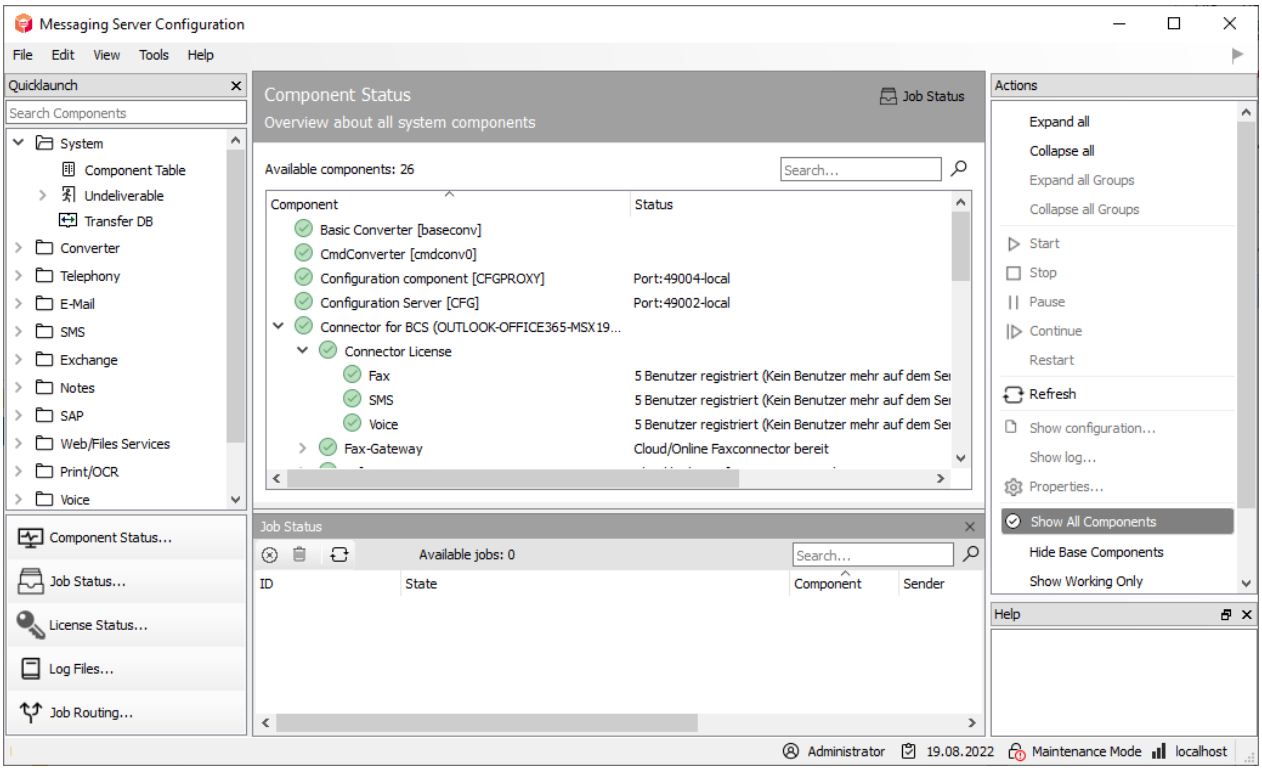


Figure 7.1: Configuration of the Exchange Connector

This documentation describes the installation and configuration of the connector for Microsoft 365 on the Version 8.0 of the OfficeMaster Server.

7.1. General

7.1.1. What is the OfficeMaster Connector for Microsoft 365?

Since OfficeMaster 4.0, an additional Exchange connector for online services has been offered. This connector is a further development of the proven Exchange connector **msx2kgate**.

msxbcsgate (**M**icro**s**oft E**x**change **B**usiness **C**ommunication **S**ervices **Gate**way)

The development of the new connector pursued the following goals:

- Compatibility with previous versions
- Possibility to use an existing Active Directory
- Can also be used in on-premise and hybrid scenarios
- No storage of connector configurations in Active Directory
- Use of the known and proven administration tools
- Bidirectional support of the Exchange Server transmission format (TNEF)

Advantages:

- Easy installation
- No lower permissions required in the Exchange organization
- Can be used for Microsoft 365 (Full Featured)
- No use of MAPI for mailbox access
- Use of existing user configuration in Active Directory for on-premise and hybrid installations

Particularities:

- SMTP transfer connectors must be created manually for on-premise installations

7.1.2. Areas of application

The product is an Exchange Connector for fax, SMS and voice mail services. It can connect all installation forms of Exchange Server-based messaging environments.

- Connection to Microsoft 365
- Connection to Microsoft 365 / Exchange 2019 On-Premise Hybrid
- Connection to Microsoft Exchange Server 2013 On-Premise
- Connection to Microsoft Exchange Server 2016 On-Premise

7.1.3. Differences to older previous versions

The previous versions of OfficeMaster Revisions 4 and 5 always required an existing local Active Directory. The connection of these connectors does not support voice mailboxes. These shortcomings have been eliminated from version 6 onwards.

7.1.4. Differences to the pure Exchange Connector MSX2KGATE

The Online Connector **msxbcsgate** has the following differences to the Exchange Connector **msx2kgate**:

- The **msx2kgate** traditionally requires a Microsoft Active Directory with an intact Exchange Server organization.
- The Online Connector **msxbcsgate** always stores its configuration data in a data file. No node is created in an Active Directory. Therefore the Connector does not necessarily require an Active Directory.
- The Online Connector **msxbcsgate** can support the individual user configuration by saving the values in the Active Directory in a way that is compatible with **msx2kgate**. However, this is only a compatibility for migration environments. The **msxbcsgate** supports the storage of individual data directly in the Microsoft 365. Therefore, the connector does not necessarily require an Active Directory here either.
- The online connector **msxbcsgate** supports mail transfer via a transfer mailbox (service transfer mode). This can avoid the outbound SMTP transfer over the Internet.
- The Online Connector is optimized to communicate directly with Microsoft's Mailprotection endpoint.
- The **msxbcsgate** installation wizard supports direct communication with Microsoft 365.

7.1.5. General requirements

To use the connector for Microsoft 365, an OfficeMaster installation is required. Ideally, ISDN hardware or VoIP access points should be correctly installed. This means that ideally there should be a correct hardware connection.

Prerequisites:

- Microsoft Windows Server 2012 (32Bit or 64Bit) or higher
- Microsoft Windows 8 (32Bit or 64Bit) or higher
- Microsoft .Net Framework 4.5 Client Profile

7.1.6. Modern authentication and communication with Exchange Online/Azure AD

Secure authentication forms the basis for the installation and administration of the components in Microsoft 365. In this case, the concept of “modern authentication” refers to manual login via the web, usually with OAuth 2.0 mechanisms, possibly with multi-factor authentication, in order to ensure secure interactive login.

Applications/programs that access interfaces of Microsoft 365 (Azure AD, etc.) via the Internet must also support this “modern authentication”. Older programs designed for on-premises Exchange Servers can be used to communicate with the interfaces that use basic authentication. However, since this is less secure, support for this basic authentication in the cloud will be gradually switched off (MC375736).

The configuration of modern authentication was available for the first time in July 2020 in the Azure AD portal under the item “Modern Authentication”:

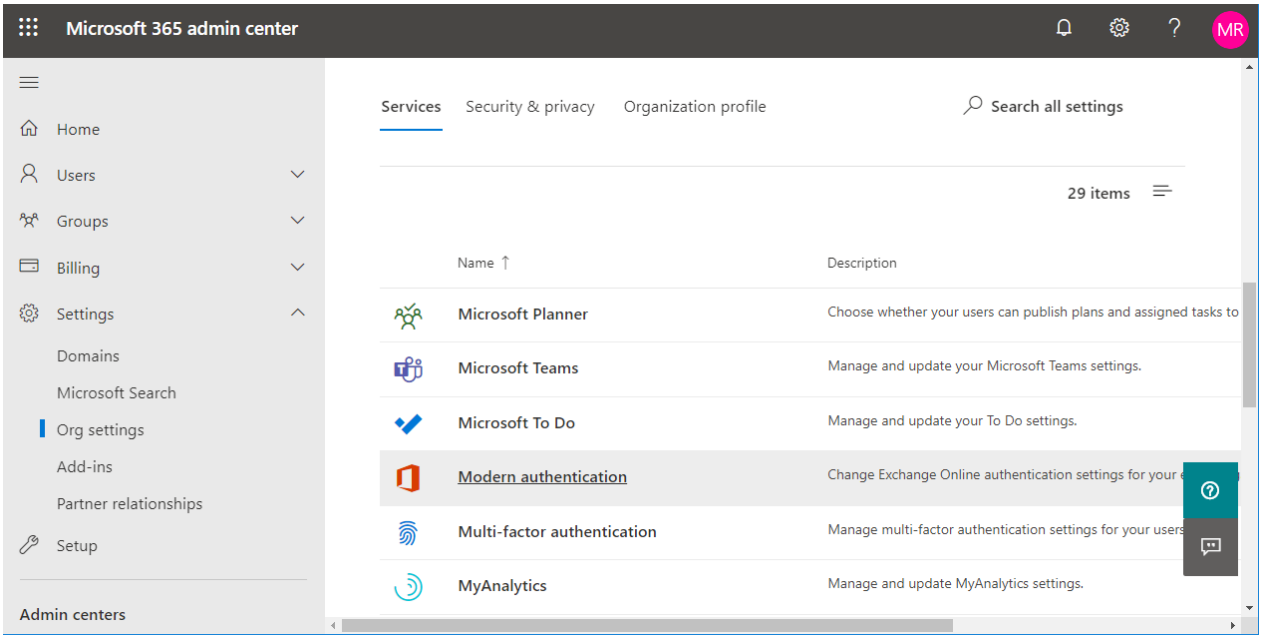


Figure 7.2: Organization Configuration - Modern Authentication

Up to version 7, the OfficeMaster BCS connector communicated exclusively with Microsoft 365 Exchange Online via the Exchange Web Services. This was changed from version 8.0, as Microsoft will no longer support the creation of applications for the Exchange Web Services in the future (MC296195).

As of version 8.0, OfficeMaster will no longer create applications in Azure AD that are based on Exchange Web Services (EWS). As an alternative, OfficeMaster will create an application based on the Microsoft Graph interface.

This way is the official interface that Microsoft mandates and supports for mail-based applications.

7.1.7. Existing installations

With a pure update to OfficeMaster Version 8, the form of communication between the connectors will not change automatically. The pure update only updates the program components. The cloud installation remains as it was before the installation.

Hybrid Installations

- As long as communication based on Exchange Web Services is technically possible in the cloud, a connector can communicate with Exchange Online.
- If EWS communication is no longer possible, the connector should be overinstalled and the communication (see Point 5) changed.

Native installations without local AD

- As long as communication based on Exchange Web Services is technically possible in the cloud, a connector can communicate with Exchange Online. Then nothing changes.
- If EWS communication is no longer possible, the connector should be overinstalled and the communication changed.

However, the addressing of the fax addresses will then change.

> **Notice about native installations!**
>
> When changing the communication to the Microsoft Graph interface, the addresses must be changed. Pure FAX, SMS or VOX address types will then no longer be recognized or supported!

7.1.8. New installations

In the course of future-proof communication to the services of the cloud, access to Exchange Online should take place with the Microsoft Graph interface. A downgrade to the EWS interface is not possible. The installation is largely automated. The degree of manual intervention can be chosen to be minimal during installation.

7.2. Connection to Microsoft 365 Exchange Online

7.2.1. General information

Microsoft Active Directory is not required for the pure connection to a Microsoft 365 service. The connector only requires an existing internet connection to access the Microsoft 365 server.

Since the connection to Microsoft 365 does not require Active Directory, the user-specific settings can be saved directly in the corresponding user's Azure AD (native). However, in a hybrid scenario, on-premises AD can also be used. This is the preferred installation variant (hybrid). All Unified Messaging services that are also available with a normal Exchange Connector are supported with this connection.

The installation wizard carries out all important installation steps in the cloud automatically. Technically, however, it is also possible to carry out these individual steps using the Microsoft 365 administration console or Exchange Onlineoffice365 PowerShell.

7.2.2. Installation requirements

Sign in to Microsoft 365 with an Organization Administrator account

An internet connection is required to install the connector. A Microsoft 365 sign-in is performed during the installation. This login refers to an administrative account that contains the necessary rights to create objects in the Microsoft 365 Exchange area (organization administrator).

> **Note!**
>
> The installation account is not a service account. This is primarily an administrative registration for the installation. This account must never be used as a service account.

Microsoft 365 service transfer account

The Microsoft 365 connector distinguishes between two transmission modes:

1. Service transfer mode

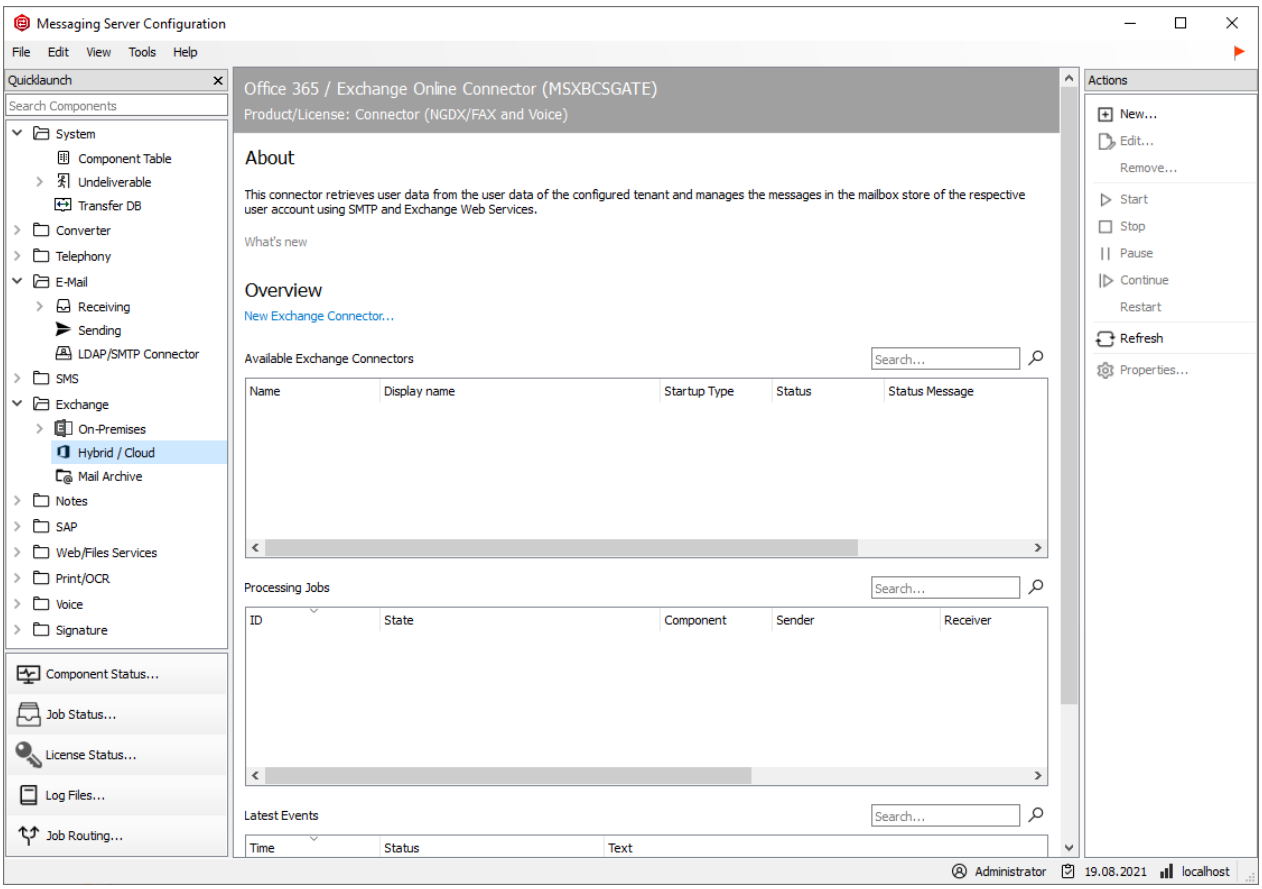
2. Internet transmission mode

   With the service transfer mode, outgoing messages are not sent to the OfficeMaster Server via the Internet, but are redirected to an internal Microsoft 365 mailbox. This saves time-consuming administration of the SMTP route to the OfficeMaster Server (MX record, provider, etc.)

   The Internet transmission mode is the classic transmission type of outgoing messages to the OfficeMaster Server via the Internet. A unique fax and SMS domain is selected (e.g. fax.domain.de, sms.domain.de), which is then linked to an Internet provider with a MX record that points to the **public Internet address of the OfficeMaster Servers** or an existing frontend server.

In general, a transfer mailbox must always be created, which temporarily buffers the outgoing messages before the OfficeMaster Server picks them up. For this purpose, the size limit of this mailbox should be adjusted accordingly in order to be able to handle any bulk faxes.

7.2.3. Installation



The connector is installed in the properties of the component administration for the Exchange/ Online services.

The installation wizard for BCS connectors will be open, when you want to add a new connector or change the current connector.

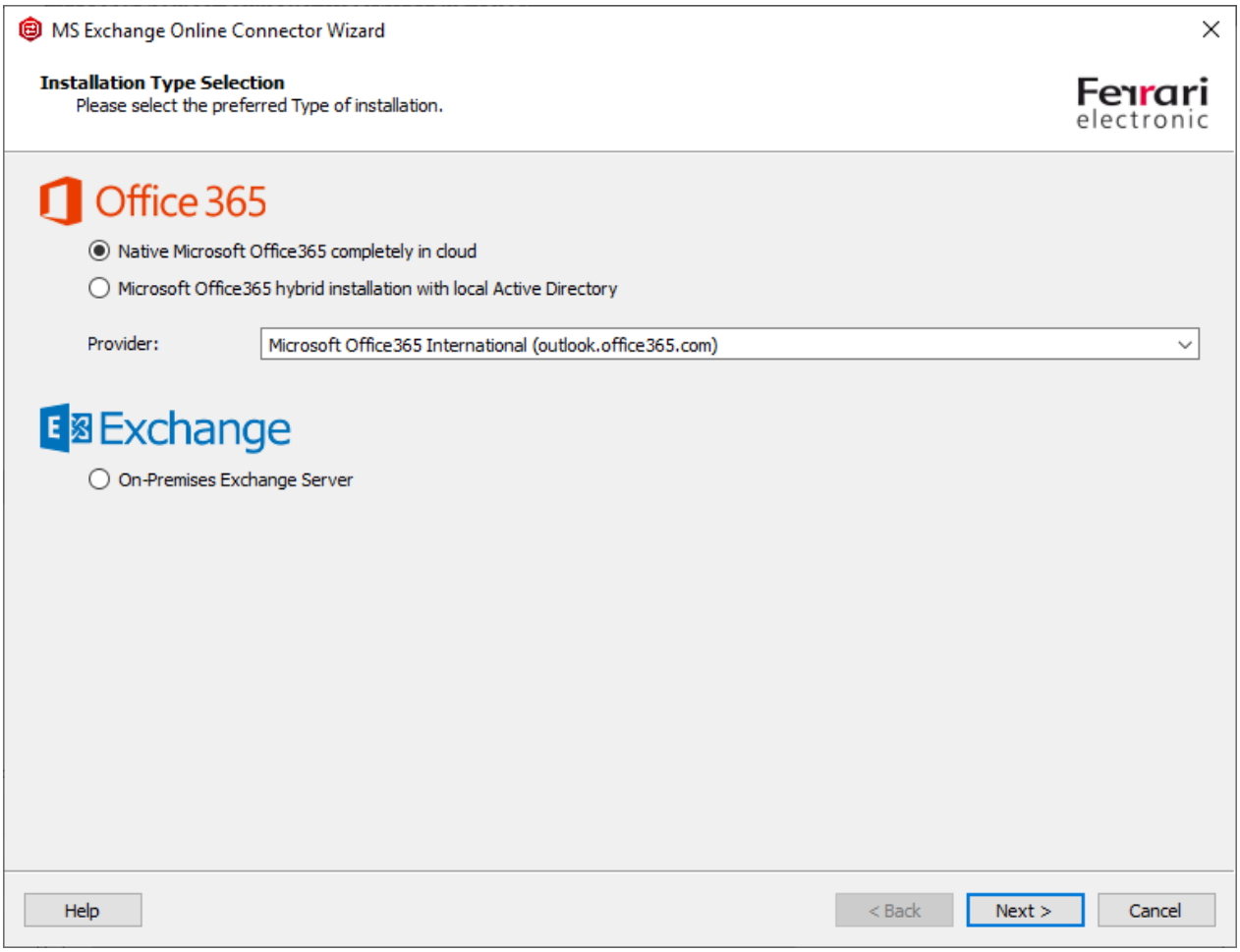


Figure 7.3: Organization Configuration - Modern Authentication

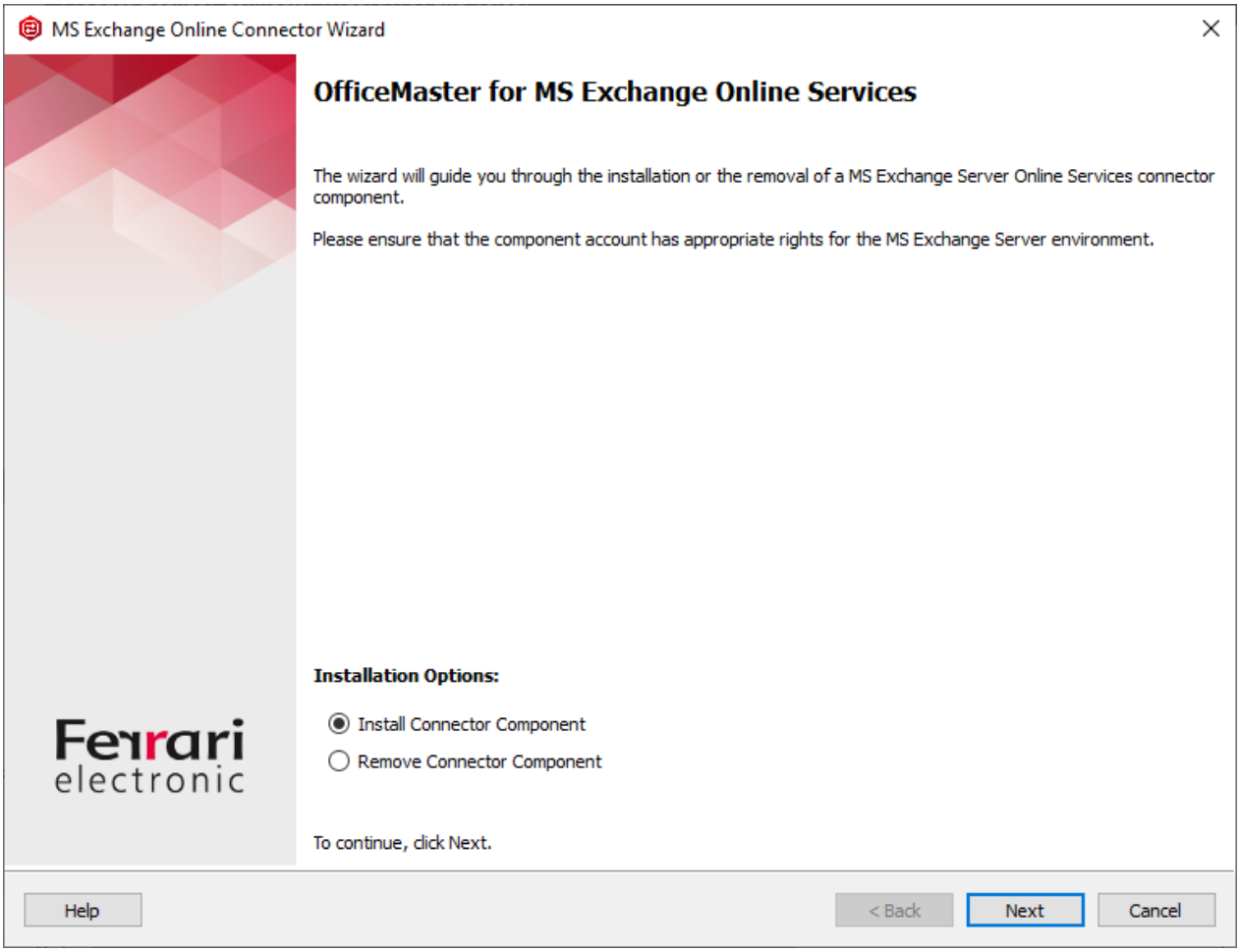


Figure 7.4: Installation wizard selection dialog

The figure above shows the selection dialog of the installation wizard. If the Microsoft 365 installations is selected, a login to the Microsoft 365 cloud is then made. Cloud login supports multi-factor authentication.

Note!

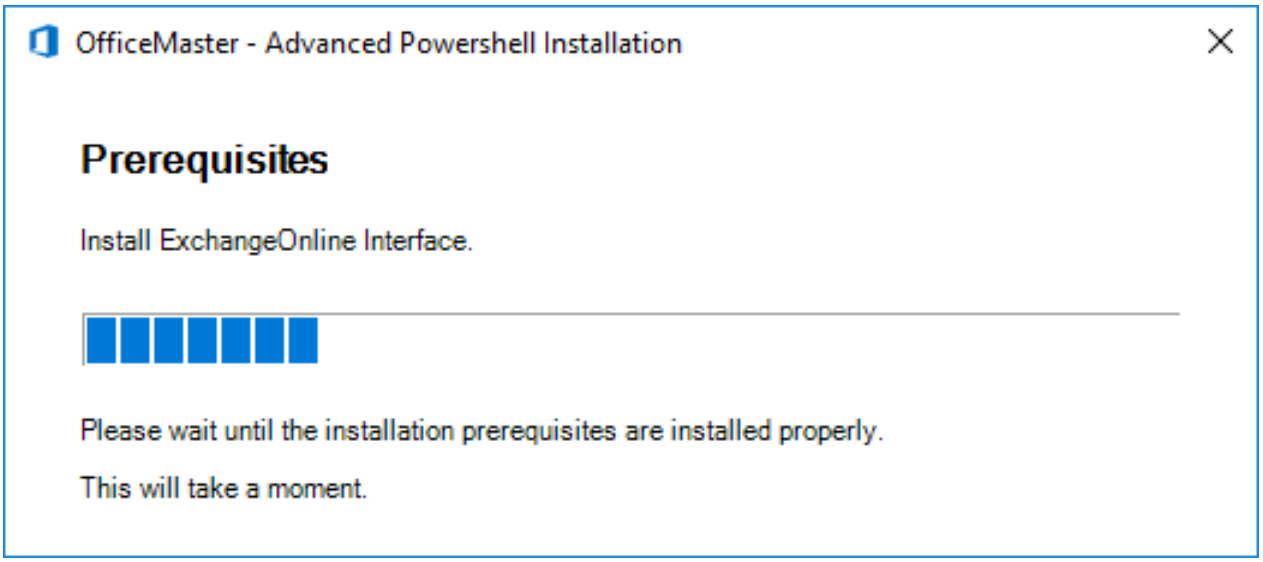
This registration is carried out internally via a remote powershell. Certain requirements must be met for this:

- Presence of Microsoft Powershell at least version 5.0
- Enhanced security mode for Internet Explorer **MUST** be disabled. The Powershell modules work with an internal browser module for the login dialogs, which cannot work correctly without JavaScript execution and access to the cloud login endpoints.

Note!

If this login to the cloud is done for the first time by the installing account, modules may have to be installed later. This can take a moment. A dialog indicates

the post-installation. After closing this dialog, the display of the login window can also be delayed by around 30 seconds.

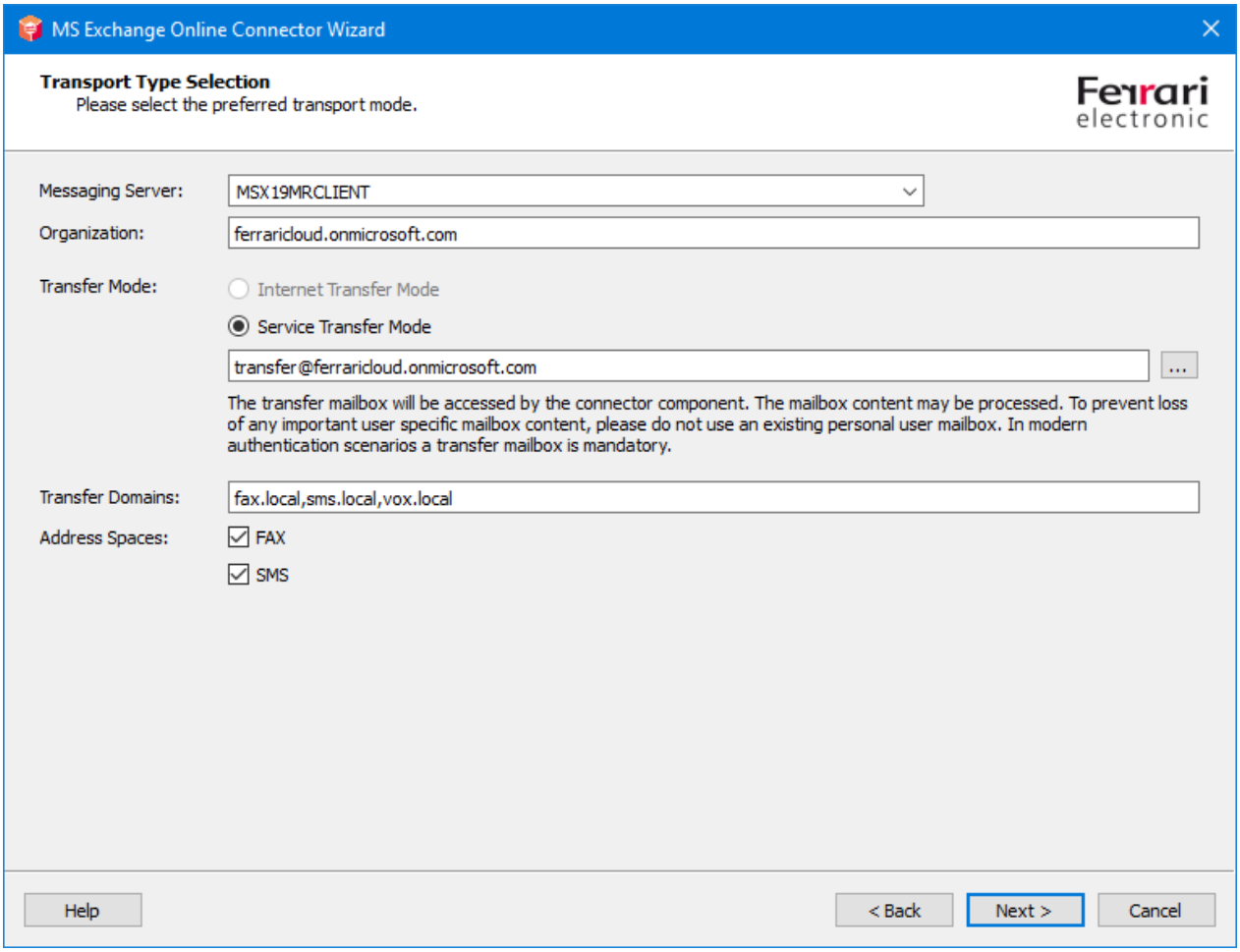


After successfully logging into the cloud, you get to the next wizard page. At this point, the transport is preconfigured. This step does not differ from the previous version.

Note!

- The successful and correct login to the cloud is shown with the correct display of the name of the organization.
- BCS connectors work in the cloud exclusively in service transfer mode, i.e. the outgoing messages are collected in a previously created mailbox. This transfer mailbox can also be a shared folder. The mailbox must first be created manually. **This mailbox cannot be the default recipient! A transfer mailbox must always be provided!**
- The transfer domains are created by default with the name of the organization. From experience, this should be changed to shorter domains. These domains do not need to have a DNS mail exchanger record, since the mails are intercepted by rule.
- The transfer domains should have a vox type to support read receipts for voice. (Turn off MWI lights when voicemails are read.)

When selecting the transfer mailbox, care must be taken to ensure that this is not an existing mailbox that a user is using. Incoming e-mails are processed, evaluated and moved. If an existing user mailbox is used, there could be a corresponding loss of data. The mailbox to be used is to be used exclusively for transfer purposes.



Messaging Server

The server on which the connector component is ultimately to be executed as an instance, can be selected in the Messaging Server input field. In the standard case, the field shows the OfficeMaster server. This field is purely informative.

Organization

In pure Microsoft 365 mode, this field only displays the read name of the organization of the current Microsoft 365 login. In this case, the field cannot be written on and is also only used for information.

Transfer mode

At this point the transfer mode can be selected. The mode is set to “Internet transmission mode” by default. It is generally recommended to change the mode to “Service Transfer Mode” for convenience.

Internet transmission mode

The Internet transmission mode is the classic form of transmission of outgoing documents to the OfficeMaster Server. The term “outgoing” specifies the direction from the mail client to the fax server. This is traditionally done over the Internet using the SMTP protocol. This form of transmission has some disadvantages and hurdles:

- In order to configure the OfficeMaster server for SMTP reception from the Internet, the server or SMTP reception must be accessible over the Internet. This is usually accomplished by front-end servers or by your own port forwarding scenarios. However, the OfficeMaster Server can now be reached from the Internet. The OfficeMaster Server has no SPAM or malware protection mechanisms. These would have to be additionally installed as third-party software if required.
- In order to correctly transport an e-mail with a domain specification, the selected domain (transport domain) must be linked to the IP address of the OfficeMaster. This means that the sending server (Microsoft 365) uses the domain to determine the address of the OfficeMaster computer. Such a configuration is made via a MX record, which is usually entered by an Internet provider in a global DNS server.

These configurations must always be made manually for the Internet transport of outgoing messages.

Service transfer mode

The service transfer mode uses a dedicated mailbox for outgoing message transport that is addressed by **msxbcsgate**. The contained e-mails, which are exclusively outgoing messages, are then processed and deleted. This method has advantages, but also disadvantages:

Advantages:

- FAX and SMS addresses can be used without restrictions. There is no obligation to use fax domains or SMS domains.
- Any values can be configured as transfer domains.
- Transfer SMTP domains do not have to be entered in global MX records.
- The OfficeMaster server does not have to be available as an SMTP server on the Internet. Administration as an SMTP server is not required.
- A transfer of outgoing messages via SMTP via the Internet is no longer necessary.

Cons:

- The transfer mailbox must have sufficient capacity to process any bulk mailings.
- The transfer mailbox must always be accessible from the OfficeMaster server.

- The transfer mailbox should be excluded from the password rotation.

The general recommendation is to use the service transfer mode, since this mode achieves greater flexibility in transporting the messages. FAX and SMS address spaces can be used without restrictions using this method.

Transfer Domains

Despite the possibility that the address spaces FAX and SMS are available in the service transfer mode, transfer domains should definitely be specified. Transfer domains are SMTP domain details that are used as fax or SMS sending domains. This domain information is also used for incoming messages. The sender can then send his outgoing documents to *fax number@domain*. By default, domains should be specified with the subdomain prefixes “fax” and “sms”.

- e.g. fax.exampledomain.de, sms.exampledomain.de

The domains can be separated with a comma or a semicolon.

> **Note!**
>
> In the service transfer mode, the information can be any domain information. With the Internet transfer mode, these domains must be known on the Internet via an MX record. This information is then no longer arbitrary.

Address spaces

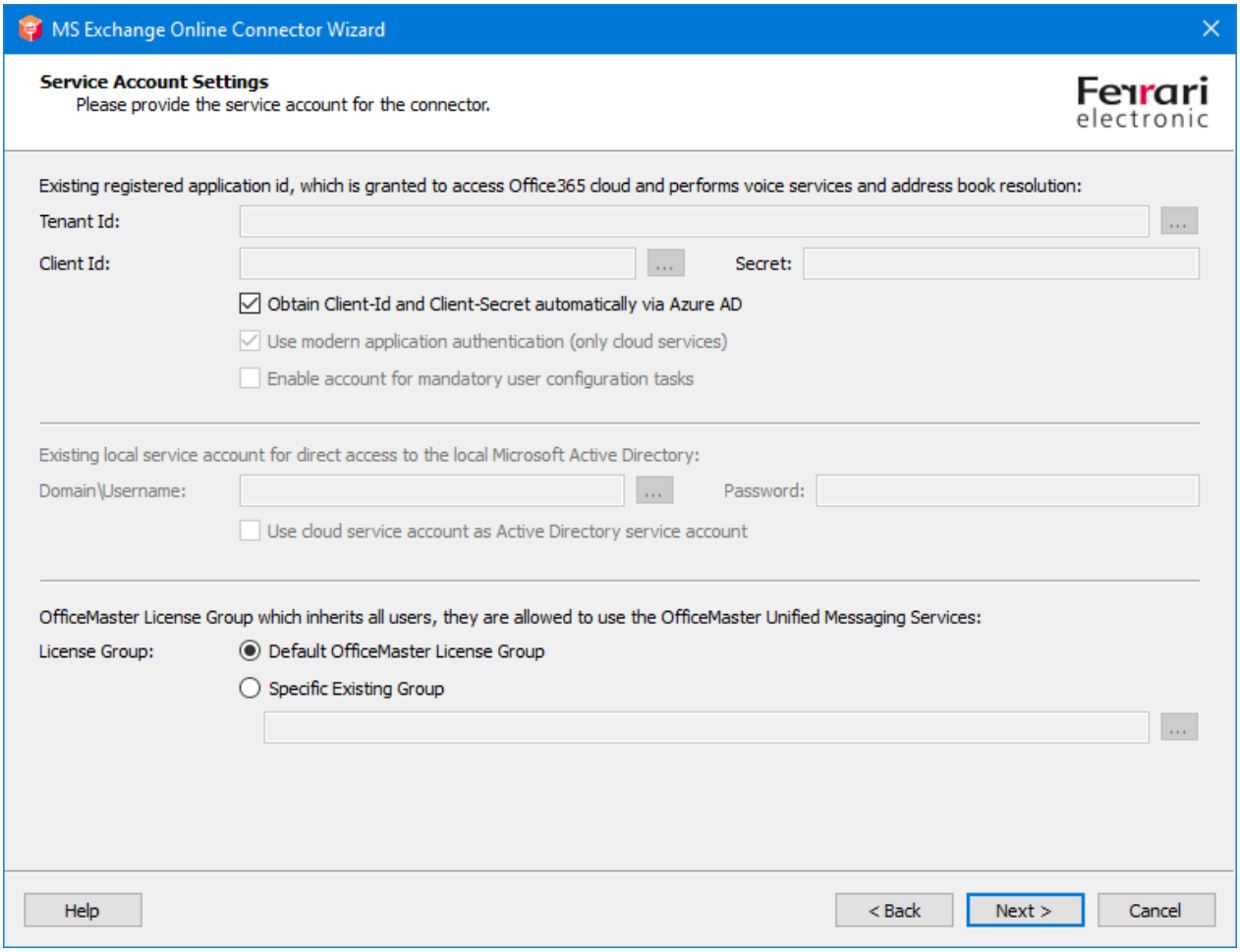
If the address spaces are activated, the traditional address spaces for FAX and SMS can be used in the same way as the local Exchange Connector installations.

In addition to transfer domain addresses, users can use addressing like follow:

- [FAX:fax number]
- [SMS:Smsnumber]

Likewise, when activating the FAX address space, the local Outlook fax contacts can be used without having to explicitly convert them to SMTP addresses.

> **Note!**
>
> Address spaces can only be activated in service transfer mode. In Internet transfer mode, addressing is mandatory via transfer domains.



The next step takes you to the account and security settings.

The installation is designed for “modern authentication” by default. This cannot be changed in the normal configuration.

The following steps are carried out internally for an application registration:

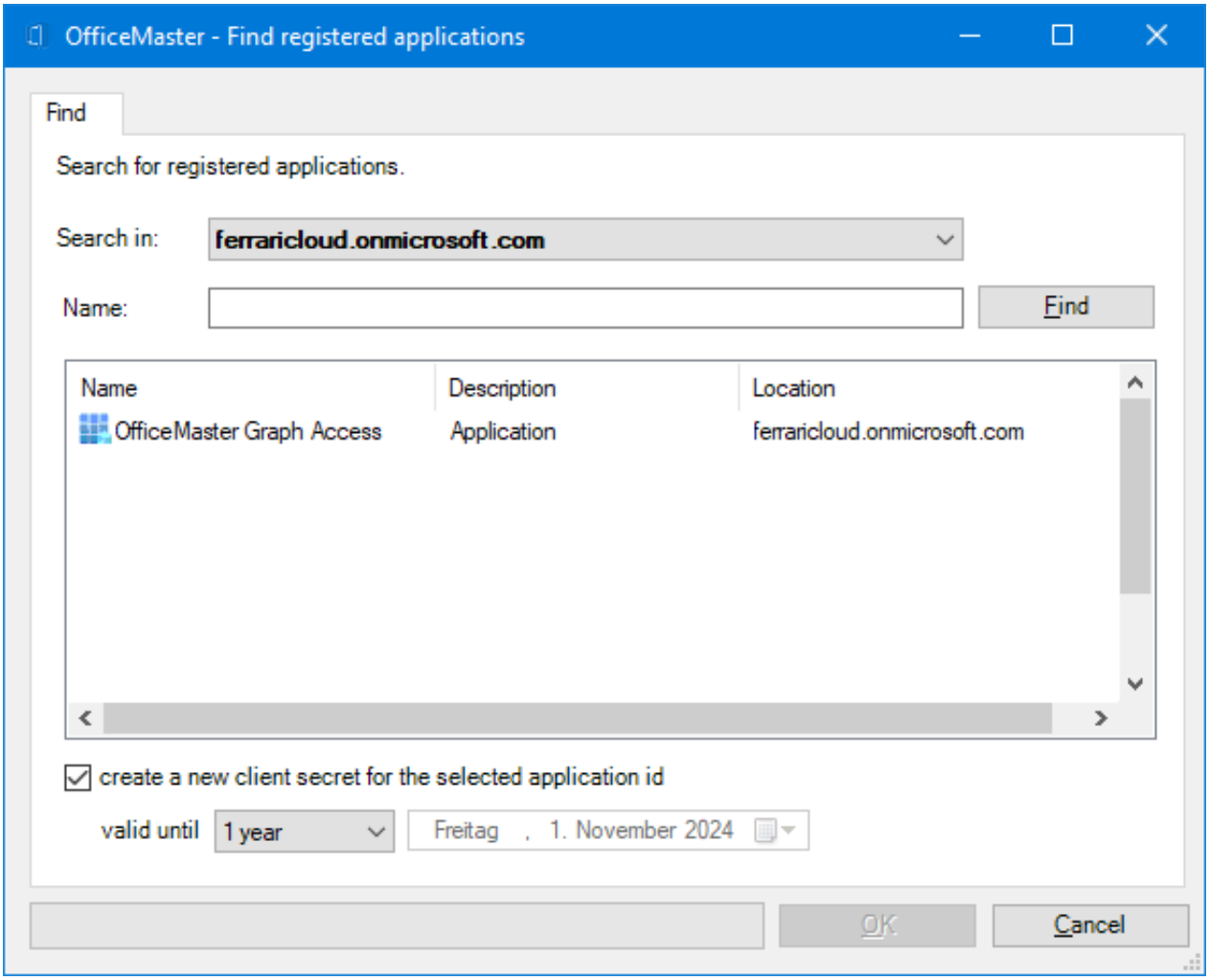
- The tenant ID (client ID) is determined.
- An application called “OfficeMaster Graph Access” is created in Azure AD.
- A client ID (application ID) and a client secret (secret) with a validity of 24 months are generated for the “OfficeMaster Graph Access” application.
- The following API permissions are granted for the “OfficeMaster Graph Access” application:
  - Microsoft Graph: Calendars.Read (as application permission)
    The permission is used for requests to users’ calendars. This is used for voice calendar queries to determine automatic free/busy statuses.
  - Microsoft Graph: GroupMember.Read.All (as application permission)
    The permission is used for requests to user groups. Distribution lists may have to be broken down for incoming fax or SMS messages. This authorization is also used for using the OfficeMaster license group.

- Microsoft Graph: Mail.ReadWrite (as application permission)
  This authorization is used for reading the e-mails in the user mailbox. At least this authorization is required for the transfer mailbox.
- Microsoft Graph: Mail.Send (as application permission)
  This authorization is set in order to be able to send e-mails via the users and the transfer mailbox. The connector uses this technology to carry out LPD mail dispatches and to be able to send e-mails from the transfer account to users.
- Microsoft Graph: People.Read.All (as application permission)
  This permission is used for requests to the cloud address lists.
- Microsoft Graph: User.Read (as delegated permission)
  This authorization is set automatically and has no meaning for the connector.
- Microsoft Graph: User.Read.All (as application permission)
  This permission is used for requests to the cloud address lists.
- Microsoft Graph: User.ReadWrite.All (as application permission)
  This authorization is required if individual user data is to be saved.

If the client ID and the client secret have been created manually beforehand, they can simply be entered. In this case, the option “Obtain program ID and secret automatically from Azure AD” must be deactivated. The values can then simply be specified.

If the tenant ID (client ID) is not known in such case, it can be determined automatically using the browser button.

The installation offers another option for preconfiguration. In some cases, the application has already been registered in Azure AD. In this case, perhaps no new application should be created. If so, a search window for applications can be called up via the browser button of the client id.

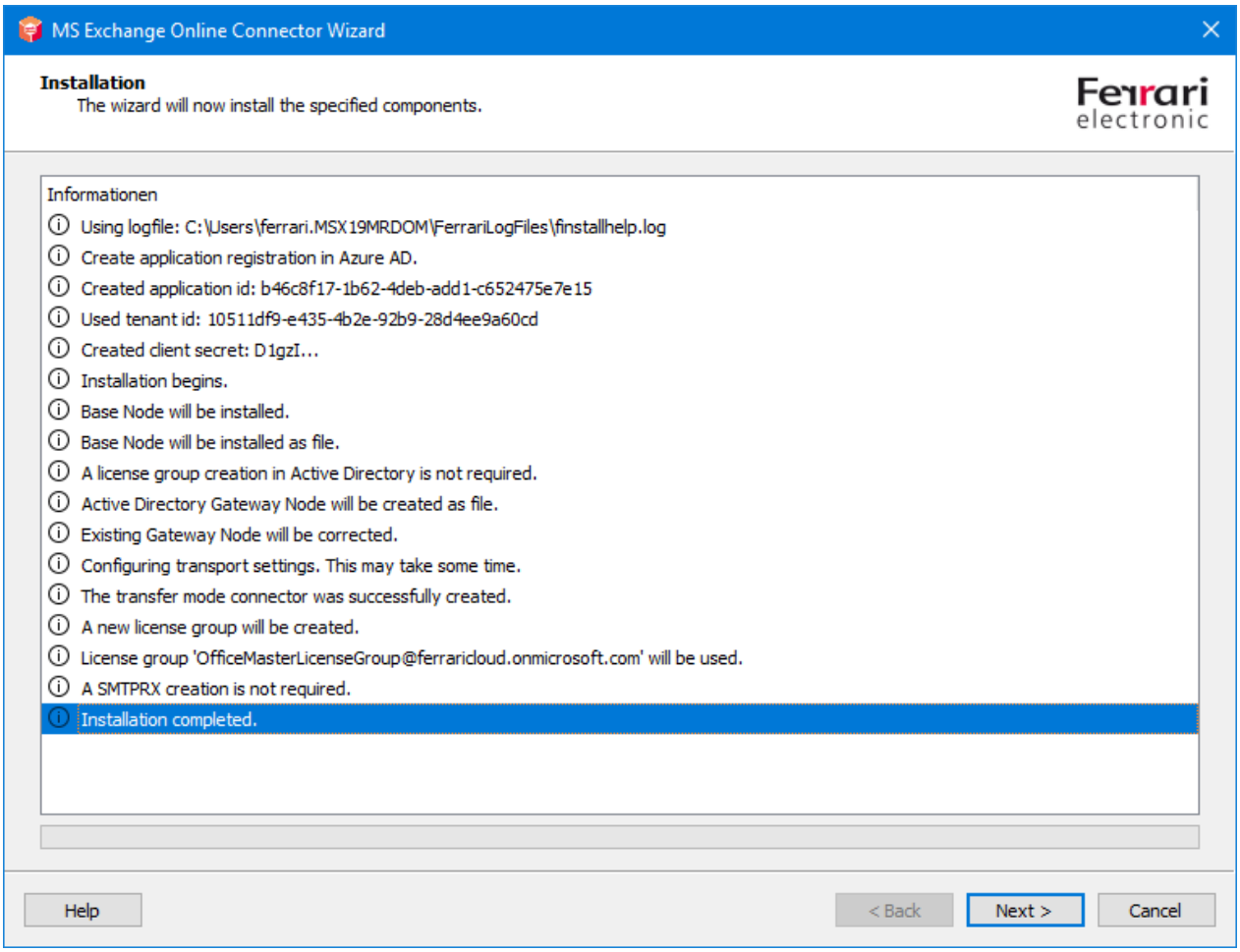


The special feature of a selected application is that no secret (client secret) can be read out. If this secret is not known, a new secret can be created during selection. Such secrets have a specific time limit. This can be set in the dialog.

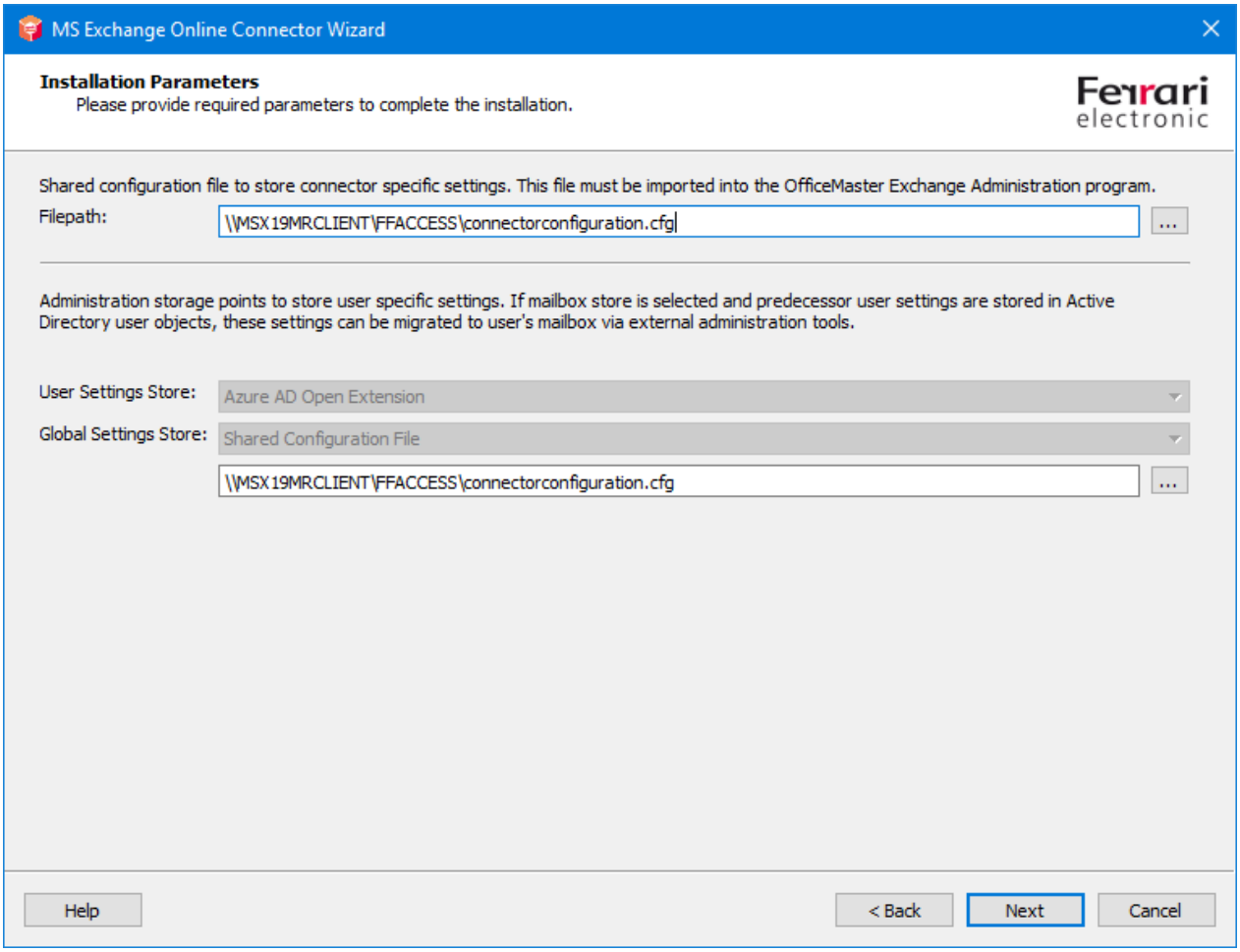
> Note!
>
> Apparently, a special service account is **not** necessary for access to Exchange Online with modern authentication with tenant ID, client ID and client secret. In this case, a transfer mailbox is still required for the outgoing messages. Whether this mailbox has multi-factor authentication protection is not important and is irrelevant for the connector.

Note!

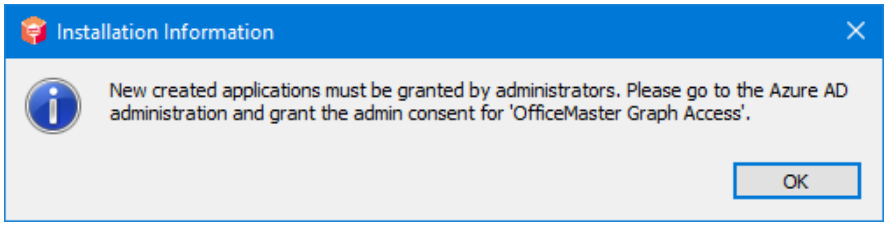
If the check box for using modern authentication is deactivated in the installation step for the account and security settings, the user name and password of a service account can be specified as in the previous version. **This is no longer generally recommended or supported.**



With the following installation steps, the connector can be installed as with the previous version.

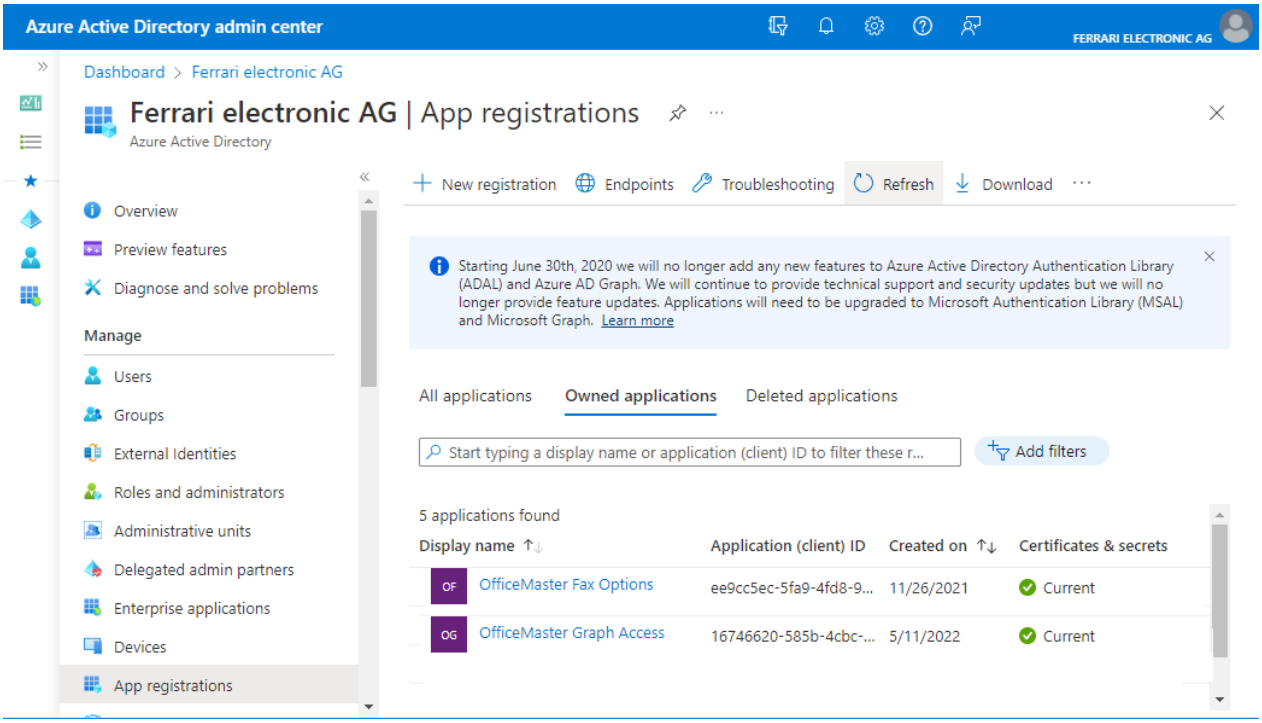


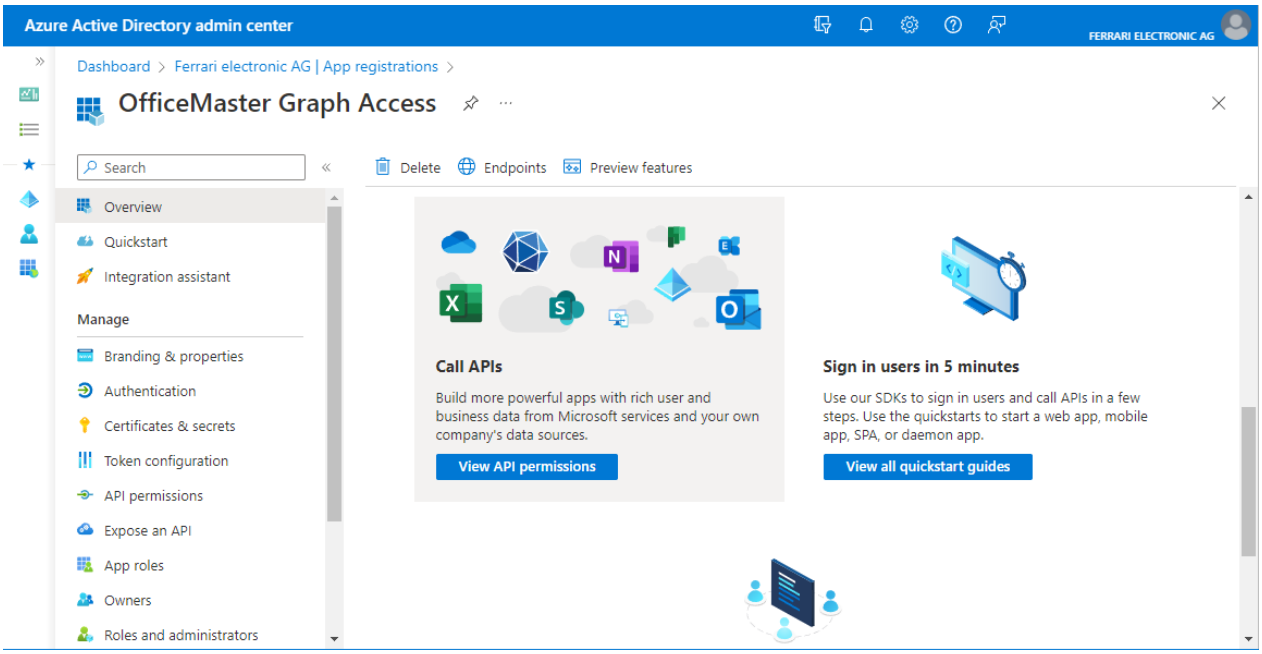
During the installation of the Azure AD application, a message appears:



This notice relates to API permissions. For security reasons, automatic confirmation of the release of API permissions was deliberately avoided. This must be done by an administrator in Azure AD after installation. If there are any concerns, the corresponding authorizations should be subsequently adapted to the (security) needs of the solution.

To do this, log on to the Azure AD of the Microsoft 365 tenant and navigate to the “OfficeMaster Graph Access” application:



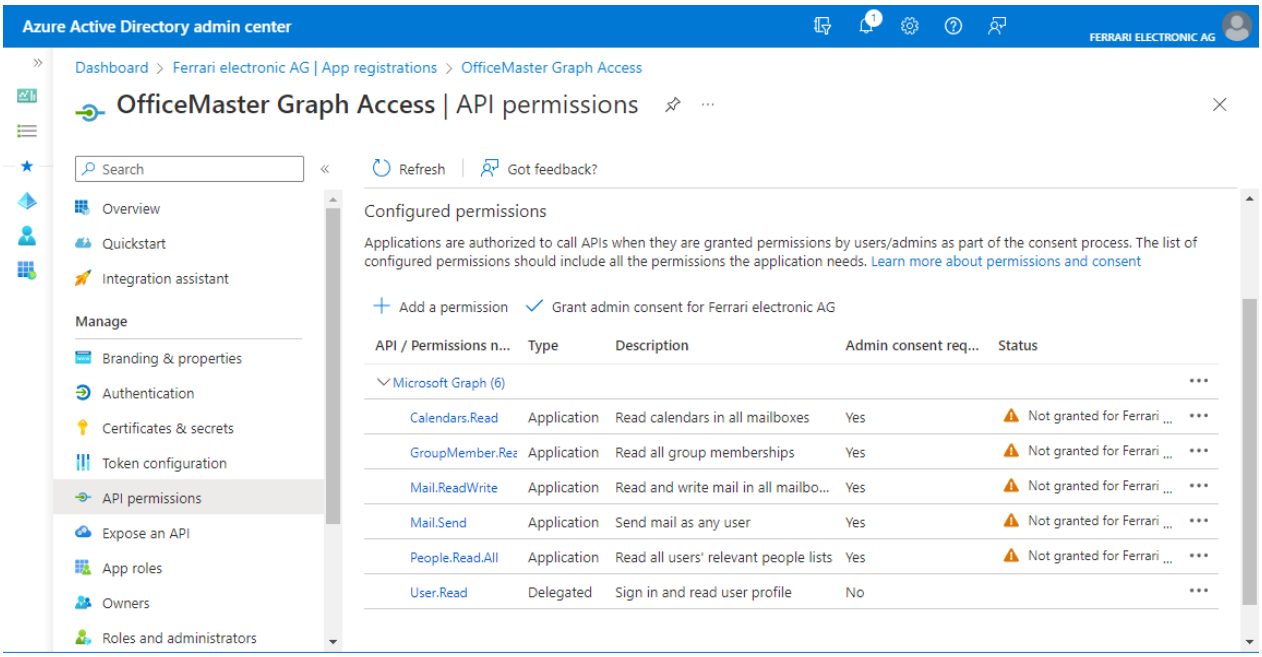


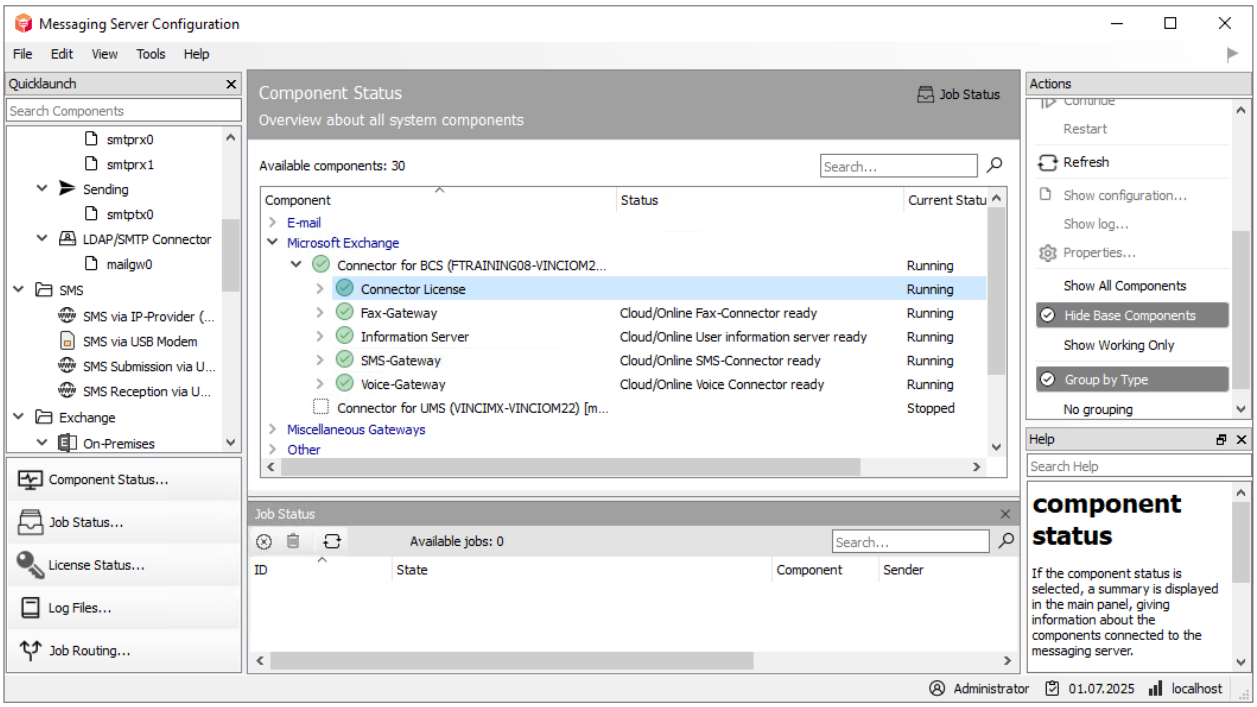
After selecting the application, the API permissions can be listed.

The API permissions must now be confirmed. This step only has to be carried out once for an application.

> **Note!**
>
> In this step, the authorizations can be redesigned according to customer requirements. Changing the permissions may have a negative impact on the productive operation of the connector.

After releasing the API permissions, the connector can be put into operation like the previous version.





After releasing the application permissions, the component can be started and should be ready to use.

7.3. Microsoft 365 Exchange Online with on-premises Active Directory (hybrid)

7.3.1. General

Another type of installation is the hybrid installation. A local Active Directory is used to store user information and determine SMTP addresses. The connector only requires an existing internet connection to access the Microsoft 365 server. A connection to the local Active Directory is also required.

The installation wizard carries out all important installation steps in the cloud automatically. Technically, however, it is also possible to carry out these individual steps using the administration console or PowerShell.

7.3.2. Installation requirements

Login to Microsoft 365 with an organization admin

An internet connection is required to install the connector. A Microsoft 365 sign-in is performed during the installation. This login refers to an administrative account that contains the necessary rights to create objects in the Microsoft 365 Exchange area (organization administrator).

> **Note!**
>
> The installation account is not a service account. This is primarily an administrative registration for the installation. This account must never be used as a service account.

Microsoft 365 service transfer account

The Microsoft 365 connector distinguishes between two transmission modes:

- Service transfer mode
- Internet transmission mode

With the service transfer mode, outgoing messages are not sent to the OfficeMaster Server via the Internet, but are redirected to an internal Microsoft 365 mailbox. This

saves time-consuming administration of the SMTP route to the OfficeMaster Server (MX record, provider, etc.)

The Internet transfer mode is the classic type of transfer of outgoing messages to the OfficeMaster Server via the Internet. A unique fax and SMS domain is selected (e.g. fax.domain.de, sms.domain.de), which is then linked to an Internet provider with an MX record that points to the **public Internet address of the OfficeMaster Servers** or an existing frontend server is configured.

In general, a transfer mailbox must always be created, which temporarily buffers the outgoing messages before the OfficeMaster Server picks them up. For this purpose, the size limit of this mailbox should be adjusted accordingly in order to be able to handle any bulk faxes.

Local Active Directory

The hybrid installation assumes that user-specific values can be stored in Microsoft Active Directory. The main purpose of this type of installation is to migrate a local Exchange installation to the Microsoft 365 cloud. The local Active Directory, which has the existing schema extension of the Exchange organization, remains in place. The required attribute fields (proxyAddresses, extensionAttribute15) are then available in the user objects.

If these attributes are not present because a new Active Directory was installed during the migration, or if these attributes were never present because this is a new installation, there are two ways to proceed.

1. **Extension of the schema to the Exchange attributes** In this case, such a schema extension can be made later. With a test version of any Exchange server downloaded from the Internet, the setup can be called with the following parameter:

   ```
   Setup/PrepareSchema
   ```

   Optional: In order to be able to create a global configuration node that is stored in Active Directory, the following command can create the Active Directory requirements:

   ```
   Setup/PrepareAD
   ```

   However, this is usually not necessary, since the global configuration node can be created using a configuration file. Such a schema extension should therefore be omitted.

2. **Installation as a pure Microsoft 365 connection**

   If a schema extension is not to take place, the installation variant of the pure Microsoft 365 connection can completely ignore the local Active Directory.

Local service account (access to local Active Directory)

The connector must have minimal access to the on-premises Active Directory to properly authenticate users. His read permissions in the organizational units of the domains should be correspondingly high.

There are several reasons for using a service account:

- Reading the configuration data of the connector stored in the Active Directory
- Reading global configuration values
- Resolve domain users and read user values
- Write customer specific values after configuration of voice parameters (own phone number, voice box pin, etc.)

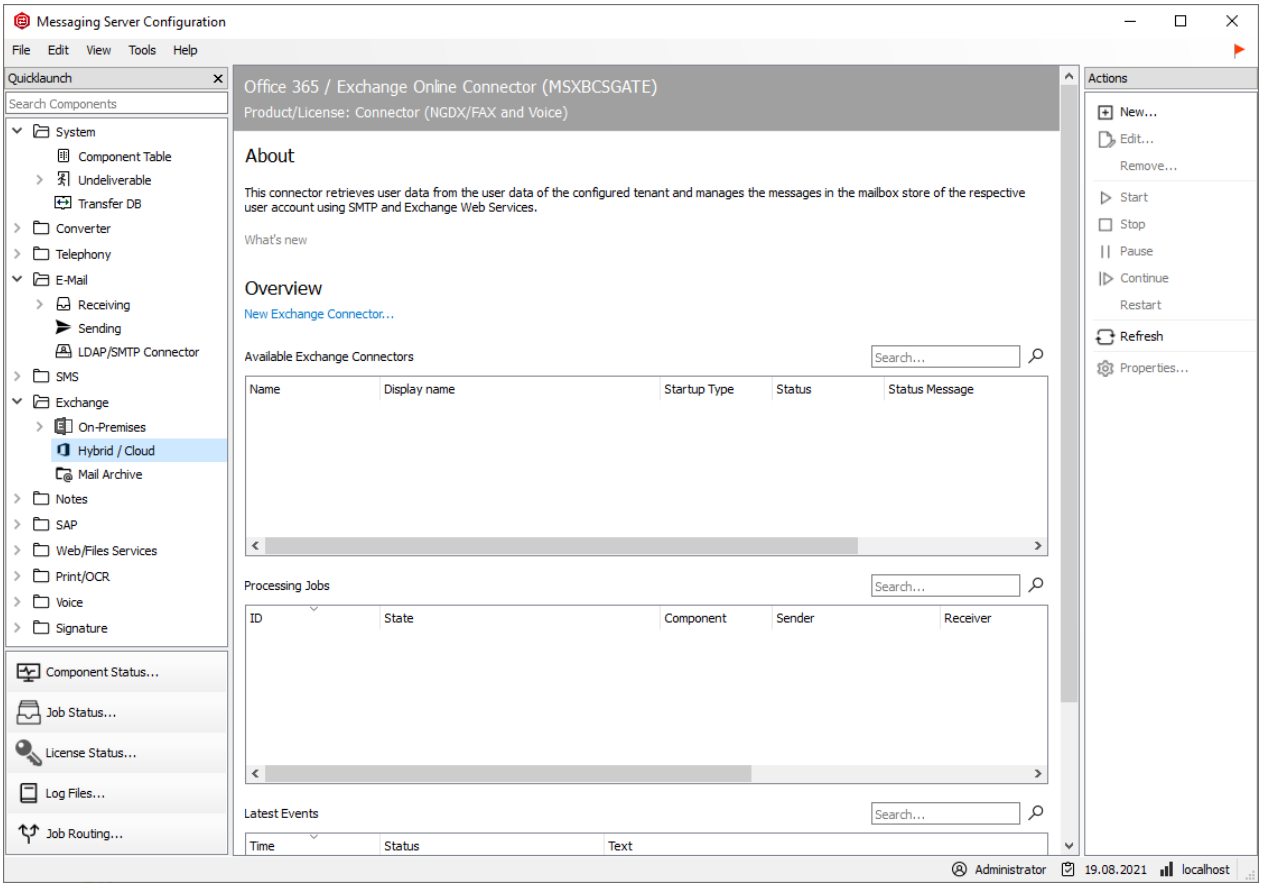
Such an account should have the following authorization structure:

- Member of the domain users group
- Local administrator of the installation computer
- Read access permissions on the path containing the configuration file
- (Installation option) Global data: Global Active Directory context
  In this case, the service account needs organizational permissions (Exchange-ViewOnly-Administrator). This setting is useful if connectors with this setting already exist.
- (installation option) Global data: Active Directory default context
  In this case, the account does not need any additional permissions.
- (Installation option) Global Data: Common Configuration File
  In this case, the account does not need any additional permissions.
- (Installation option) User data: Active Directory user object

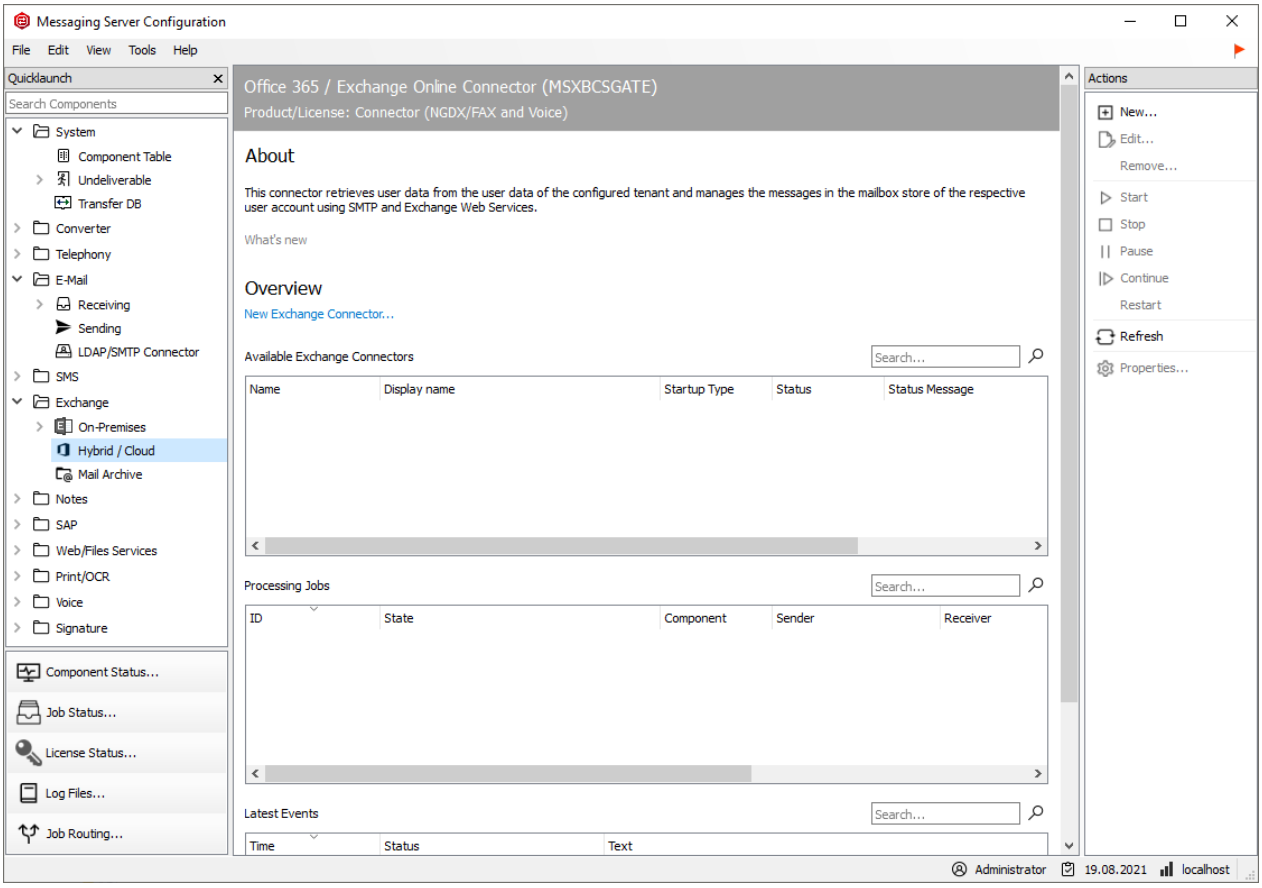
  If voice properties such as PIN or phone number values are also to be changed by users via remote inquiry or Outlook client with the connector, the account must have write permissions in the user objects of the connected domains. This is not necessary if the data is stored in the user mailbox.

7.3.3. Installation

The connector is installed in the properties of the component administration for the Exchange/ Online services.



An installation wizard will now appear. The components should only be created and deleted using this installation wizard.

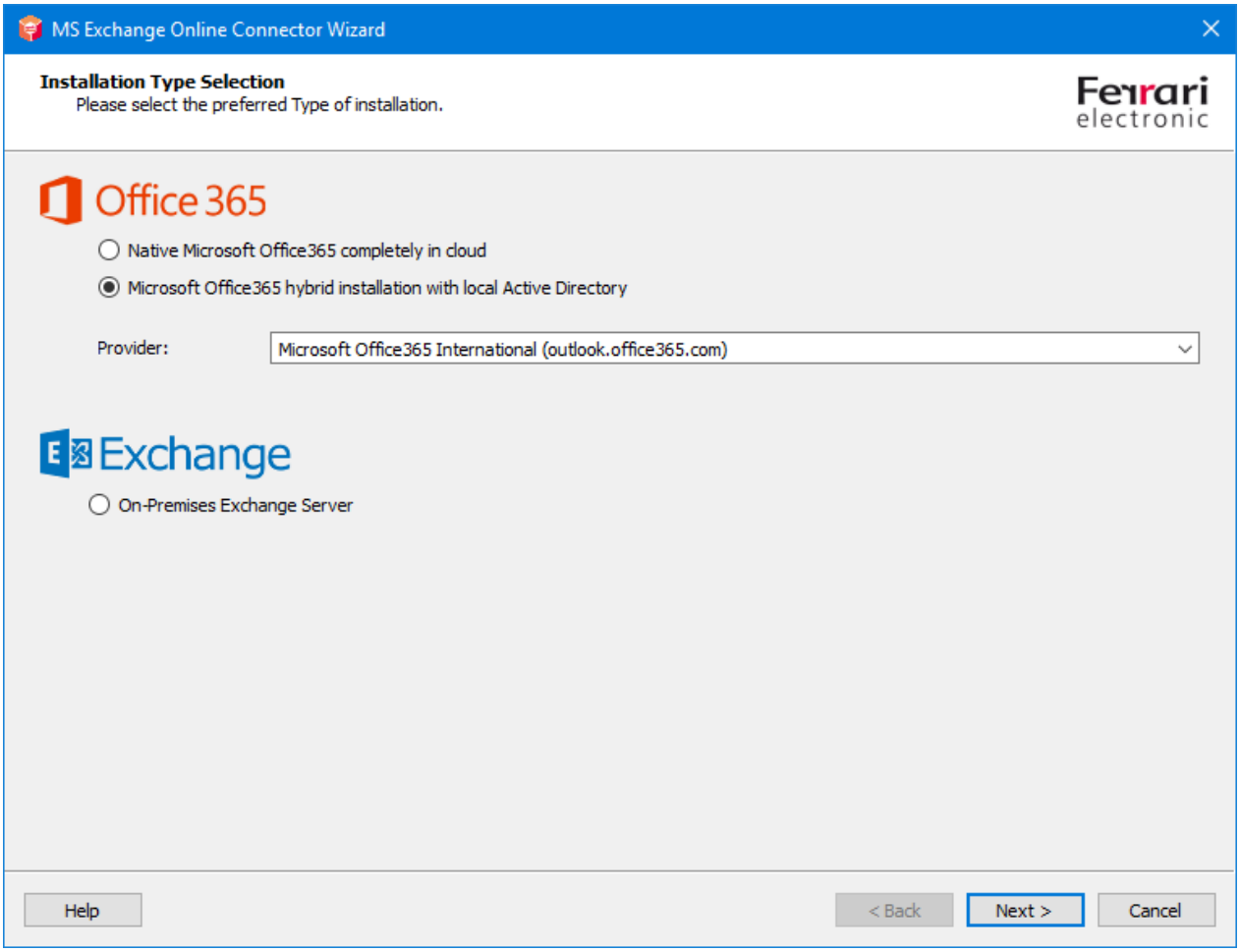


The welcome screen is followed by a dialog for selecting the type of installation. Three installation forms are available:

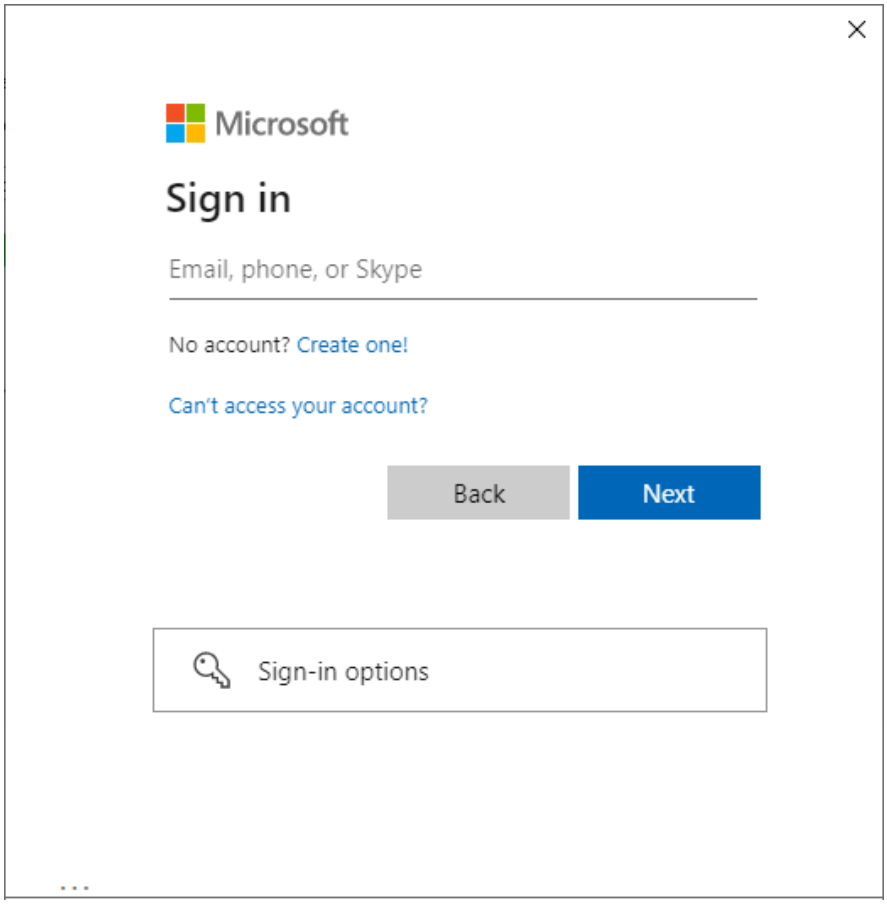
1. Microsoft 365 as a full cloud installation
2. Microsoft 365 hybrid installation with on-premises Active Directory
3. Local Exchange Server Installation (On-Premise)

For Microsoft 365 hybrid installations with an on-premises Active Directory, the second type of installation is used.

For the further creation of installation objects in Microsoft 365, a successful login to the Microsoft 365 organization is required.

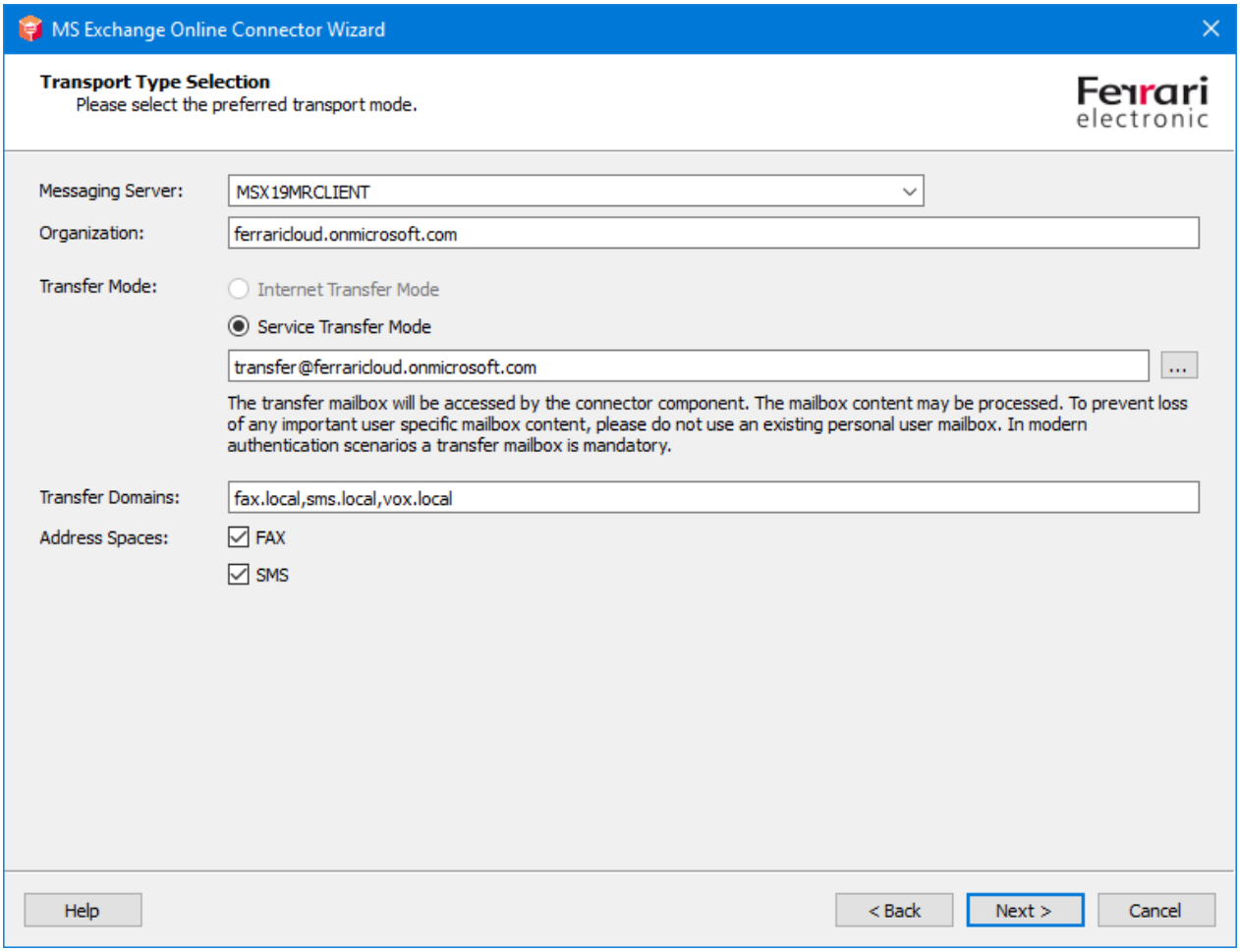


This should be done using an administrative account that has appropriate organizational permissions. The wizard will check the login and only release the next step if the login is successful.



At this point, logging in with multi-factor authentication is also supported.

In the next step, the transport type is selected. The transport type determines how outgoing documents are handled.



The decision is important with regard to whether the outgoing documents should be transferred via the Internet, or whether the documents should be collected in a collective mailbox and then picked up by **msxbcsgate**.

Messaging Server

The server on which the connector component is ultimately to be executed as an instance can be selected in the Messaging Server input field. The field has a purely informative character.

Organization

This field is the display of the parsed name of the organization of the current Microsoft 365 login. In this case, the field cannot be written on and is only used for information. If there is no registration, the name of an organization or a main suffix of a domain can be entered here. This information can serve as a template for the transfer domains.

Transfer mode

At this point the transfer mode can be selected. The mode is set to “Internet transmission mode” by default. It is generally recommended to change the mode to “Service Transfer Mode” for convenience.

Internet transmission mode**

The Internet transmission mode is the classic form of transmission of outgoing documents to the OfficeMaster Server. “Outgoing” here means the direction from the mail client to the fax server. This is traditionally done over the Internet using the SMTP protocol. This form of transmission has some disadvantages and hurdles:

- In order to configure the OfficeMaster server for SMTP reception from the Internet, the server or SMTP reception must be accessible over the Internet. This is usually accomplished by front-end servers or by your own port forwarding scenarios. However, the OfficeMaster Server can now be reached from the Internet. The OfficeMaster Server has no SPAM or malware protection mechanisms. These would have to be additionally installed as third-party software if required.
- In order to correctly transport an e-mail with a domain specification, the selected domain (transport domain) must be linked to the IP address of the OfficeMaster. i.e. based on the domain, the sending server (Microsoft 365) the address of the OfficeMaster computer. Such a configuration is made via an MX record, which is usually entered by an Internet provider in a global DNS server.

These configurations must always be made manually for the Internet transport of outgoing messages.

Service transfer mode

The service transfer mode uses a dedicated mailbox for outgoing message transport that is addressed by **msxbcsgate**. The contained e-mails, which are exclusively outgoing messages, are then processed and deleted. This method has advantages, but also disadvantages:

Advantages:

- FAX and SMS addresses can be used without restrictions. There is no obligation to use fax domains or SMS domains.
- Any values can be configured as transfer domains.
- Transfer SMTP domains do not have to be entered in global MX records.

- The OfficeMaster server does not have to be available as an SMTP server on the Internet. Administration as an SMTP server is not required.
- There is no transfer of outgoing messages via SMTP via the Internet.

Disadvantages:

- The transfer mailbox must have sufficient capacity to process any bulk mailings.
- The transfer mailbox must always be accessible from the OfficeMaster server.
- The transfer mailbox should be excluded from password rotation.

The general recommendation is to use the service transfer mode, since this mode achieves greater flexibility in transporting the messages. FAX and SMS address spaces can be used without restrictions using this method.

Transfer Domains

Despite the possibility that the address spaces FAX and SMS are available in the service transfer mode, transfer domains should definitely be specified. Transfer domains are SMTP domain details that are used as fax, SMS or voice sending domains. This domain information is also used for incoming messages. The sender can then send his outgoing documents to *fax number@domain*. By default, domains should be specified with the subdomain prefixes “fax” and “sms”. If MWI lamps are also to be switched off via read mail items, a “vox” domain should also be specified.

E.g. fax.exampledomain.de, sms.exampledomain.de, vox.exampledomain.de

The domains can be separated with a comma or a semicolon.

Note!

In the service transfer mode, the information can be any domain information.

With the Internet transfer mode, these domains must be known on the Internet via an MX record. This information is then no longer arbitrary.

Address spaces

By activating the address spaces, the traditional address spaces for FAX and SMS can be used in the same way as the local Exchange Connector installations.

In addition to transfer domain addresses, users can then use follow addressings:

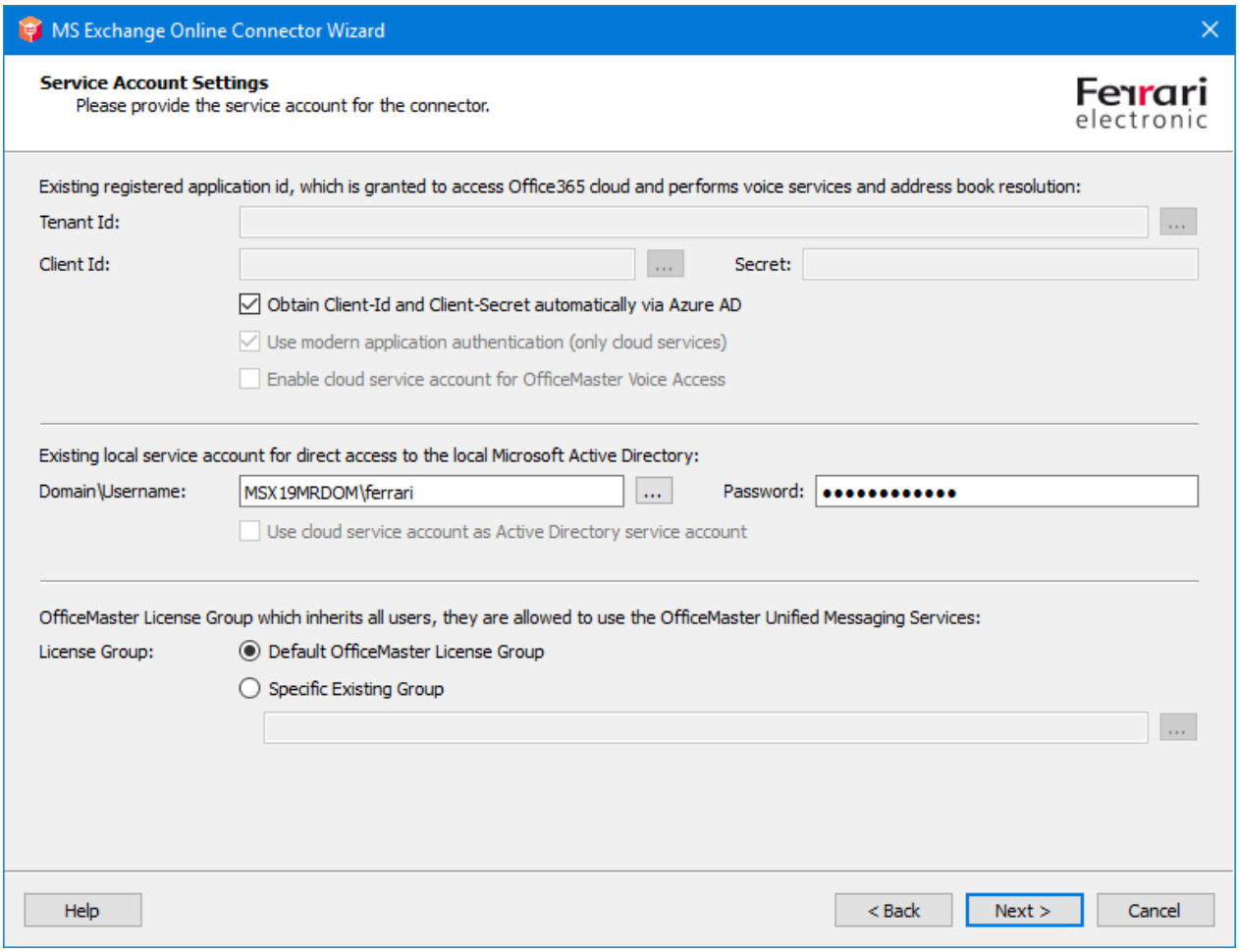
- [FAX:*fax number*]

- [SMS:*SMS number*]

Likewise, by activating the FAX address space, the local Outlook fax contacts can be used without having to explicitly convert them to SMTP addresses.

> **Note!**
>
> Address spaces can only be activated in service transfer mode. In the Internet transfer mode, addressing is mandatory via transfer domains.

In the following step, the service account for access to Microsoft 365 and the local domain is specified.



At this point the service account can be selected. The available account selection dialog shows all available mailboxes in the Microsoft 365 tenant that can be used as a service mailbox.

The service account of the current domain can also be specified here, which is used to access the local Active Directory.

The installation is designed for “modern authentication” by default. This cannot be changed in the normal configuration.

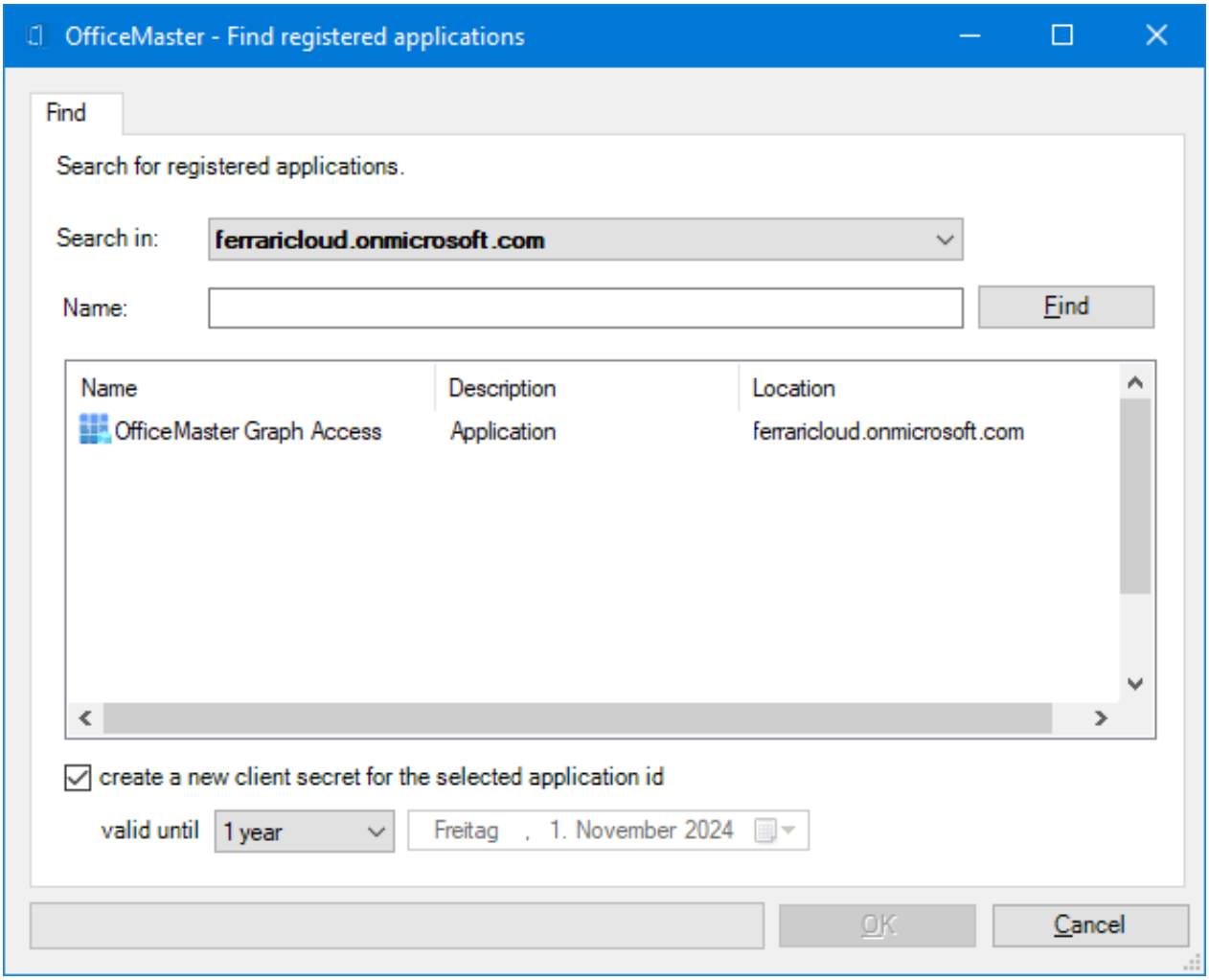
The following steps are carried out internally for an application registration:

- The tenant ID (client ID) is determined.
- An application called “OfficeMaster Graph Access” is created in Azure AD.
- A client ID (application ID) and a client secret (secret) with a validity of 24 months are generated for the “OfficeMaster Graph Access” application.
- The following API permissions are granted for the “OfficeMaster Graph Access” application:
    - Microsoft Graph: Calendars.Read (as application permission) The permission is used for requests to users’ calendars. This is used for voice calendar queries to determine automatic free/busy statuses.
    - Microsoft Graph: GroupMember.Read.All (as application permission)
      The permission is used for requests to user groups. For incoming fax or SMS messages, distribution lists may have to be resolved. This authorization is also used for using the OfficeMaster license group.
    - Microsoft Graph: Mail.ReadWrite (as application permission)
      This authorization is used for reading the e-mails in the user mailbox. At least this authorization is required for the transfer mailbox.
    - Microsoft Graph: Mail.Send (as application permission)
      This authorization is set in order to be able to send e-mails via the users and the transfer mailbox. The connector uses this technology to carry out LPD mail dispatches and to be able to send e-mails from the transfer account to users.
    - Microsoft Graph: People.Read.All (as application permission)
      This permission is used for requests to the cloud address lists.
    - Microsoft Graph: User.Read (as delegated permission)
      This authorization is set automatically and has no meaning for the connector.
    - Microsoft Graph: User.Read.All (as application permission)
      This permission is used for requests to the cloud address lists.
    - Microsoft Graph: User.ReadWrite.All (as application permission)
      This authorization is required if individual user data is to be saved.

If the client ID and the client secret have been created manually beforehand, they can simply be entered. In this case, the option “Obtain program ID and secret automatically from Azure AD” must be deactivated. The values can then simply be specified.

If the tenant ID (client ID) is not known in such a case, it can be determined automatically using the browser button.

The installation offers another option for preconfiguration. In some cases, the application has already been registered in Azure AD. In this case, perhaps no new application should be created. If so, a search window for applications can be called up via the browser button of the client id.



The special feature of a selected application is that no secret (client secret) can be read out. If this secret is not known, a new secret can be created during selection. Such secrets have a specific time limit. This can be set in the dialog.

Note!

Apparently, a special service account is **not** necessary for access to Exchange Online with modern authentication with tenant ID, client ID and client secret. In this case, a transfer mailbox is still required for the outgoing messages. Whether this mailbox has multi-factor authentication protection is not important and is irrelevant for the connector.

Note!

If the check box for using modern authentication is deactivated in the installation step for the account and security settings, the user name and password of a service account can be specified as in the previous version. **This is no longer generally recommended or supported.**

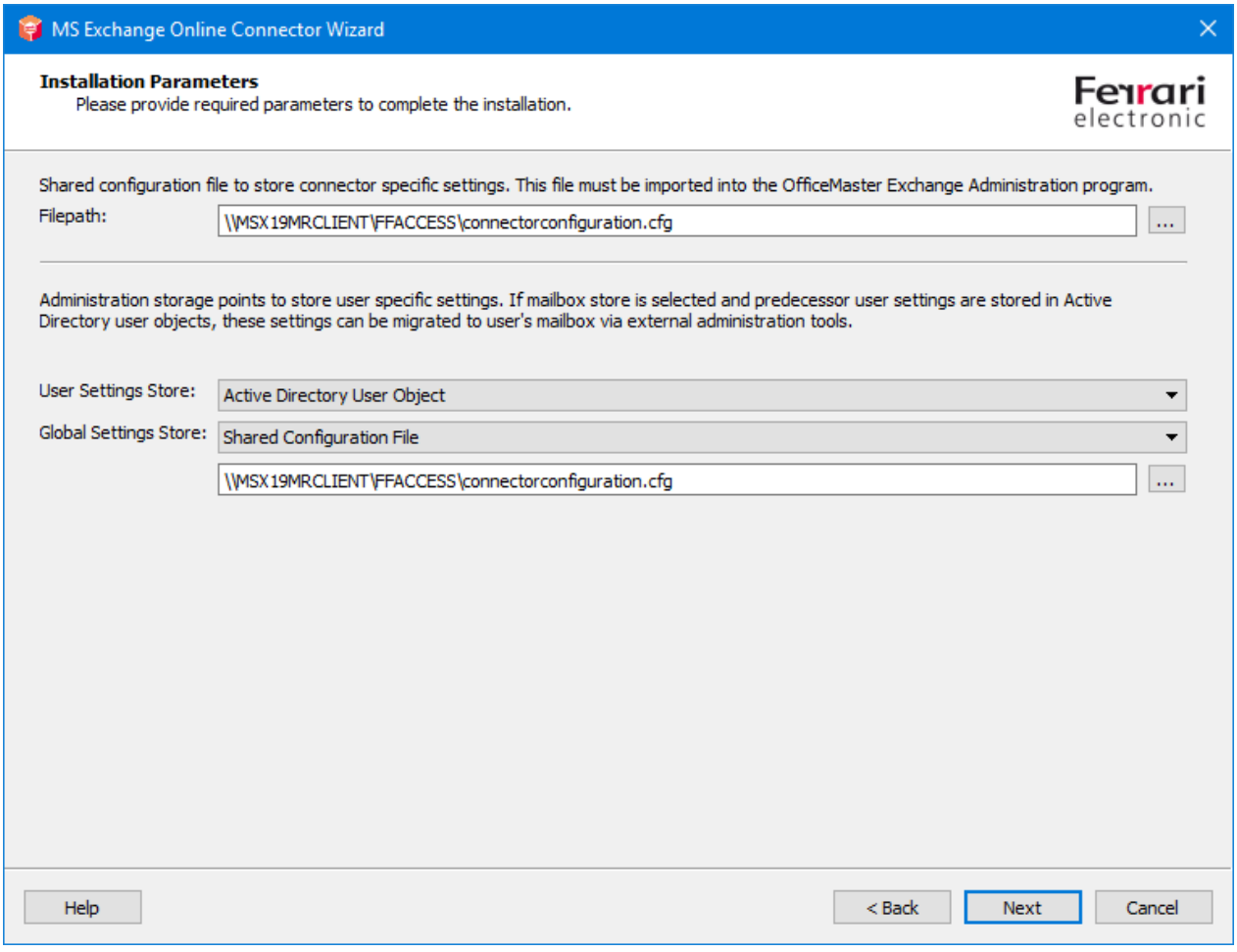
Local service account with access permissions to on-premises Active Directory

At this point, the service account should be selected to access the on-premises Active Directory. No Microsoft 365 mailbox can be specified here. The specification relates solely to local access to the current domain.

OfficeMaster license group

In the field of the license group, for the Small Business variants (e.g. OfficeMaster 250 for MS Exchange), the license group is specified in which the licensed users must be entered. By default, the license group is created automatically and is named “OfficeMaster License Group”. This entry point is not accessible for unlimited OfficeMaster versions. In the hybrid installation variant, this group is stored in the Active Directory.

In the next installation step, the local configuration points are specified in which the connector configuration is saved.



File path

The general configuration of the **msxbcsgate** component is traditionally administered via MMC configuration snap-ins. With this type of connector, the configuration data is always saved in a configuration file. The path of this file can be specified here. By default, a file that is in the OfficeMaster release *FFACCESS* is suggested here.

User data management

In the hybrid installation variant, there are two installation options available:

Active Directory user object

This is the recommended default if the current Active Directory can accommodate the user-specific values.

User mailbox

Alternatively, the user-specific values can also be saved in the user's mailbox. This is useful if the current Active Directory does not have an Exchange schema extension or if the local Active Directory is to be removed in the future.

> Note!
>
> If a previous version of the exchange gateways from Ferrari electronic AG was used and the user-specific values are already available in the Active Directory, they can continue to be used in a compatible manner. If the user management mode is then switched to *user mailbox*, these values must be migrated from the Active Directory to the Microsoft 365 mailboxes using special tools, otherwise the Active Directory will no longer be accessed.

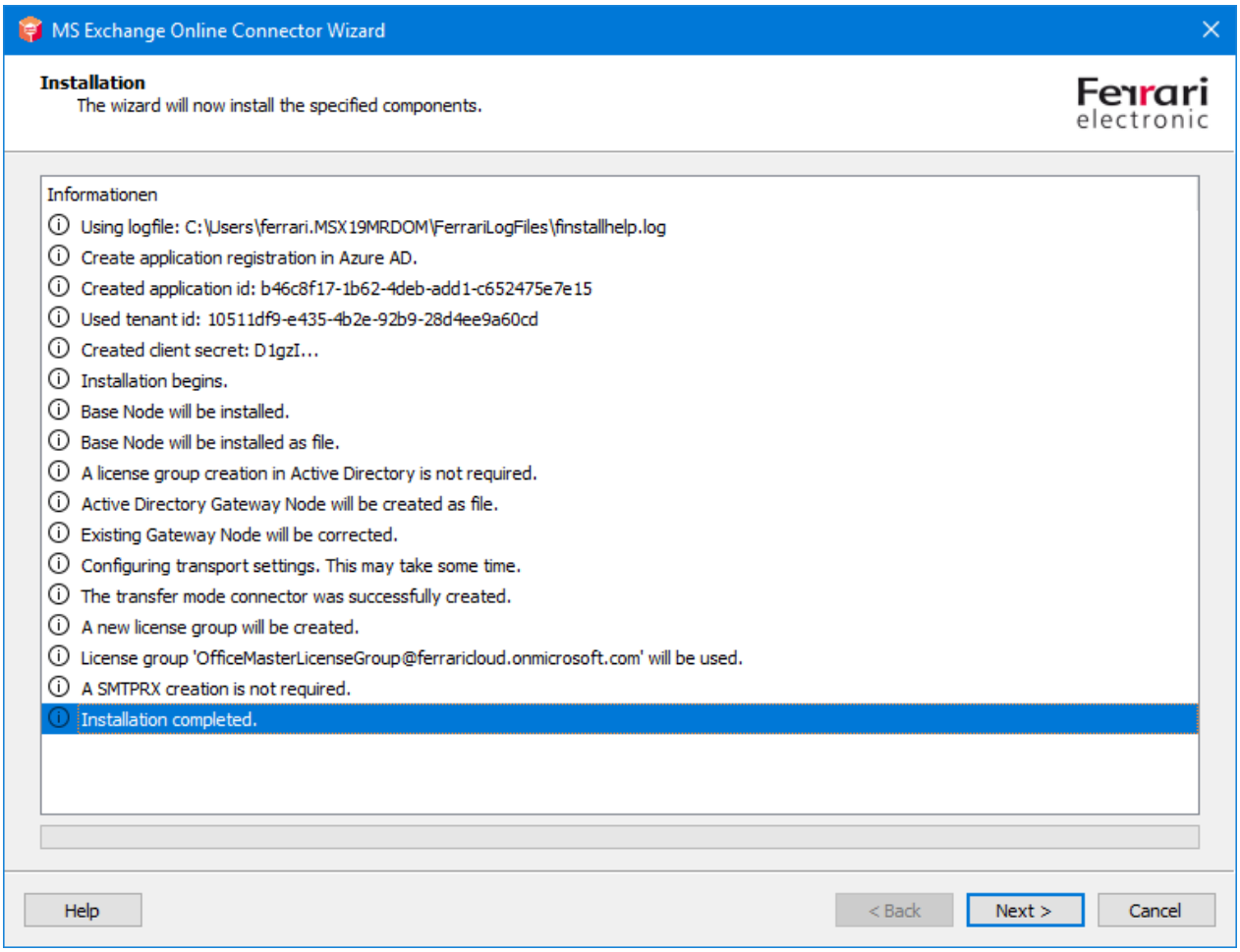
Global user data

Global user data is the template data that applies to all users for whom other values have not been explicitly specified (fax ID, header, cover sheet, etc.). In the pure Microsoft 365 installation variant, these global specifications can only be saved in a configuration file. At this point, it makes sense to use the same file that contains the connector configuration data. The default setting is that the values are written globally to the existing Active Directory. This default setting is only set for compatibility with the previous version. This makes sense if such a global configuration node has already been installed from the previous product.

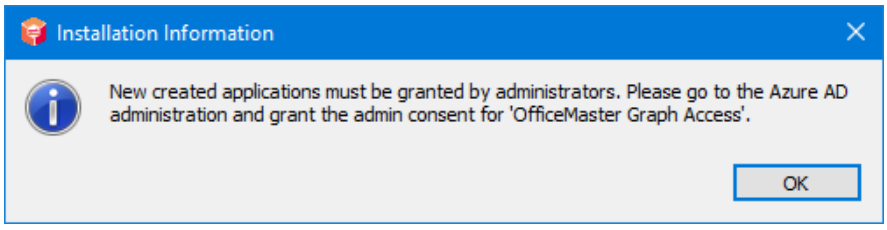
Note!

If there is no global configuration node yet, installation in a shared configuration file is recommended.

The necessary parameters for installing the connector are now known. The connector can now be created in the next installation steps.

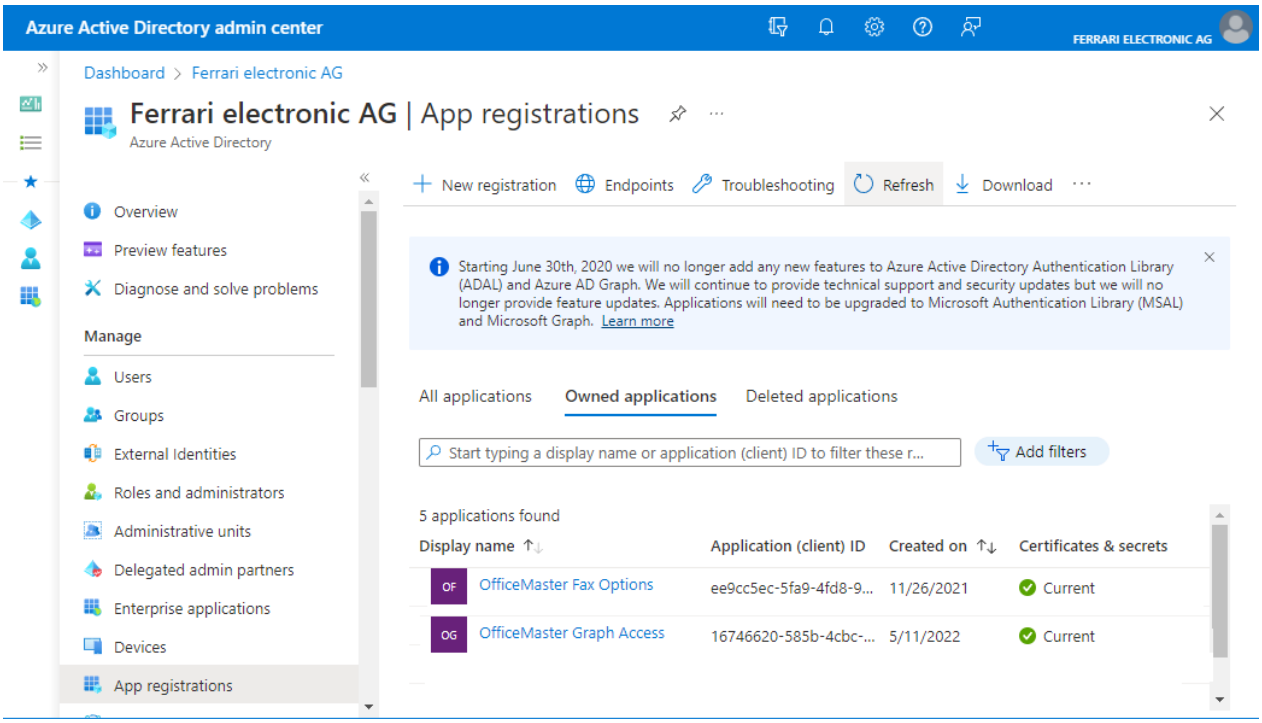


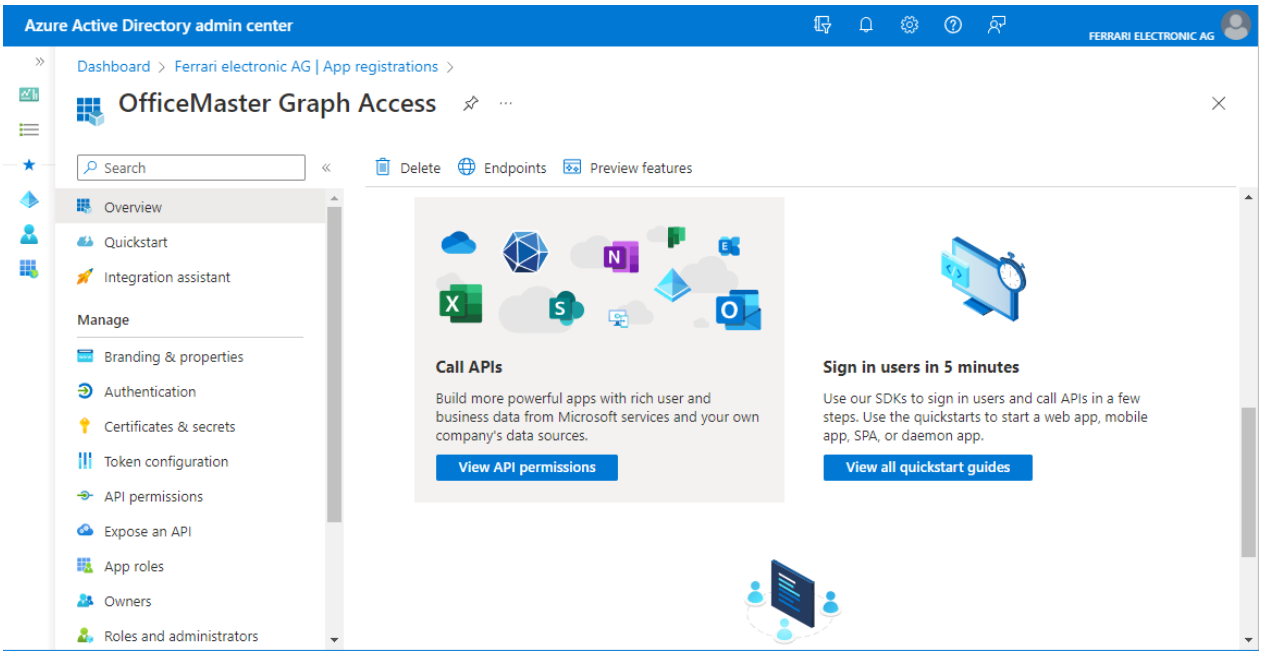
During the installation of the Azure AD application, a message appears:



This notice relates to API permissions. For security reasons, automatic confirmation of the release of API permissions was deliberately avoided. This must be done by an administrator in Azure AD after installation. If there are any concerns, the corresponding authorizations should be subsequently adapted to the (security) needs of the solution.

To do this, log on to the Azure AD of the Microsoft 365 tenant and navigate to the “OfficeMaster Graph Access” application:





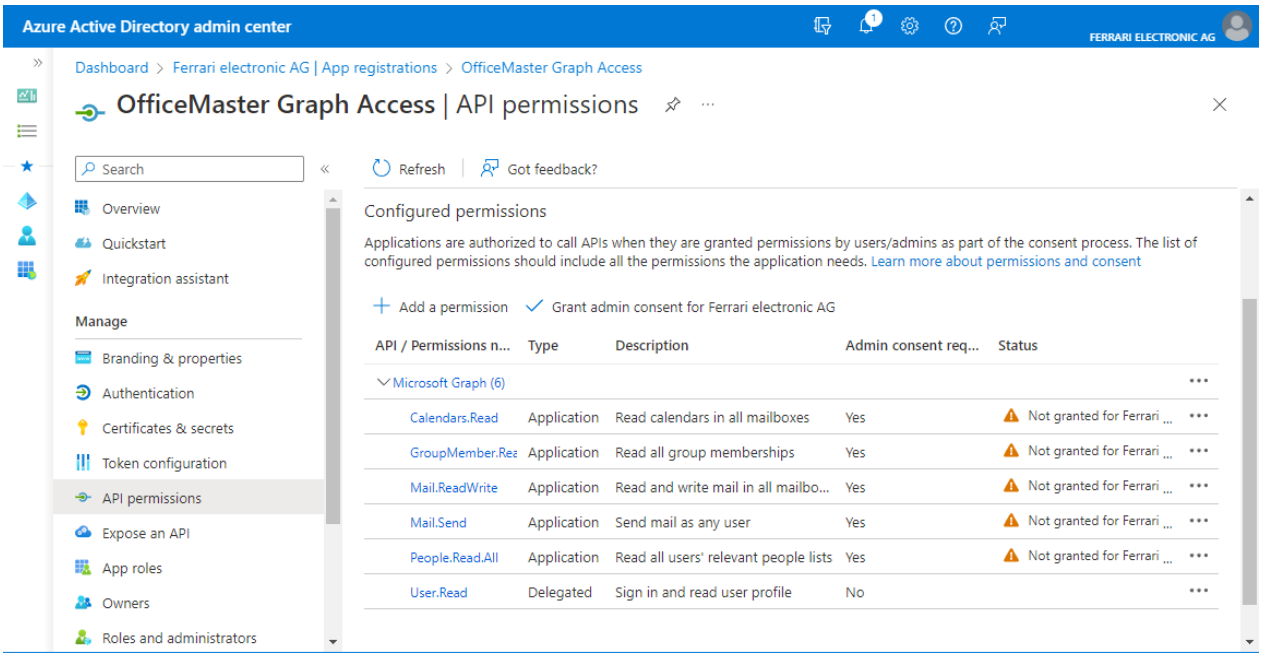
After selecting the application, the API permissions can be listed.

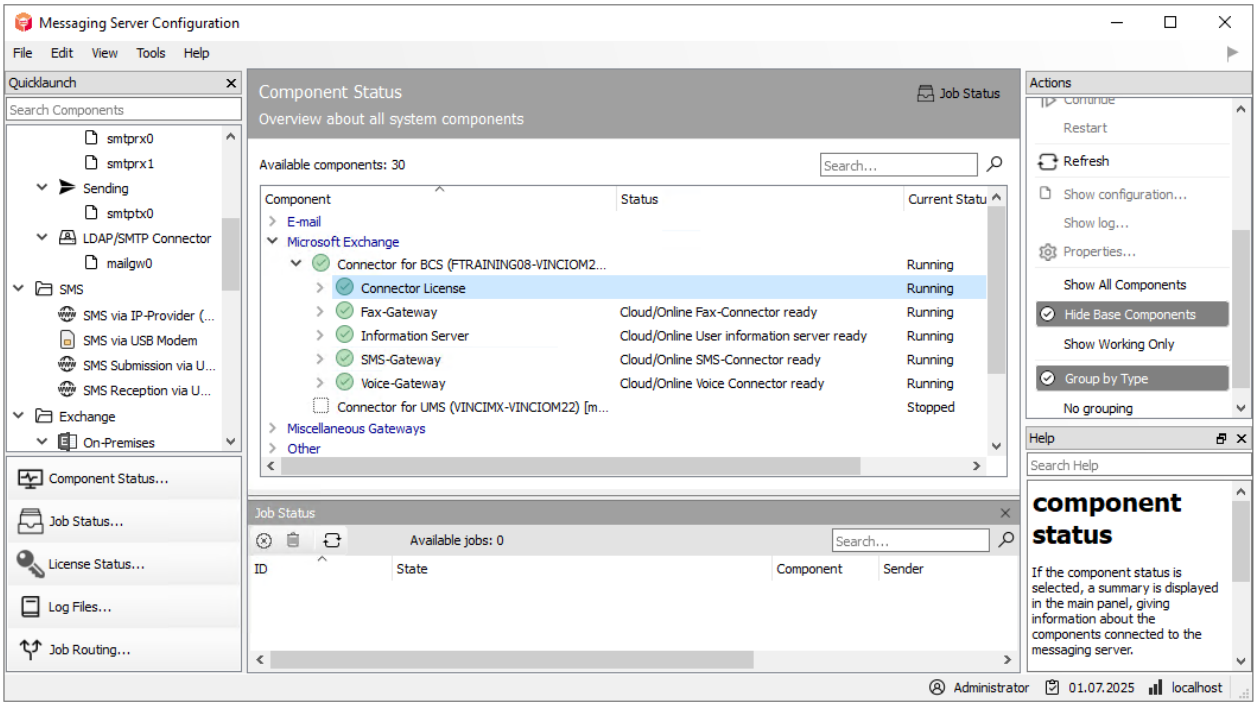
The API permissions must now be confirmed. This step only has to be carried out once for an application.

Note!

In this step, the authorizations can be redesigned according to customer requirements. Changing the permissions may have a negative impact on the productive operation of the connector.

After the API permissions have been released, the connector can be put into operation like the previous version.





After releasing the application permissions, the component can be started and should be ready to use.

7.4. Local Exchange Server installation

7.4.1. General

A special type of installation is the local Exchange Server installation (on-premise). This form is similar to installing the Exchange Gateway **msx2kgate**. A local Active Directory is used to store user information and determine SMTP addresses. The connector only requires a LAN connection to access the local Exchange server.

Local installation is usually supported by the default exchange gateway **msx2kgate**. However, when the previous product was installed, there were local environments in which the gateway **msxbcsgate** had to be used. The reasons for this were usually access problems via MAPI (Message Application Programmers Interface) and rights problems with Active Directory (configuration nodes could not be created due to missing authorizations). For compatibility with these installations, the installation variant of the local Exchange Server installations is also supported by **msxbcsgate**.

The installation wizard carries out all important installation steps automatically. After the installation, however, a manual adjustment to the Exchange Server is necessary. No objects are created automatically in the Exchange Server organization.

> **Attention!**
>
> The installation is based on bidirectional e-mail transmission. For this reason, the installation wizard installs its own SMTP server and opens port 25 by default. For this reason, such an installation should not take place on an Exchange server itself. An Exchange Server itself maintains a binding to the port **25**. The installation of an OfficeMaster server with a local installation variant of **msxbcsgate** should always take place on a dedicated server.
>
> If this is not possible, an alternative port must be configured for the **smtprx** component, to which the Exchange Server can then deliver the documents.

7.4.2. Installation requirements

Service account to access address books and the local Active Directory

A separate service account or mailbox is required to operate the connector. This service account should be created manually as a normal user mailbox beforehand. The mailbox is used to access the public address book of the Exchange Server and is stored in the connector.

Local service account (accessed from local Active Directory)

The connector must have minimal access to the on-premises Active Directory to properly authenticate users. His read permissions in the organizational units of the domains should be correspondingly high.

There are several reasons for using a service account:

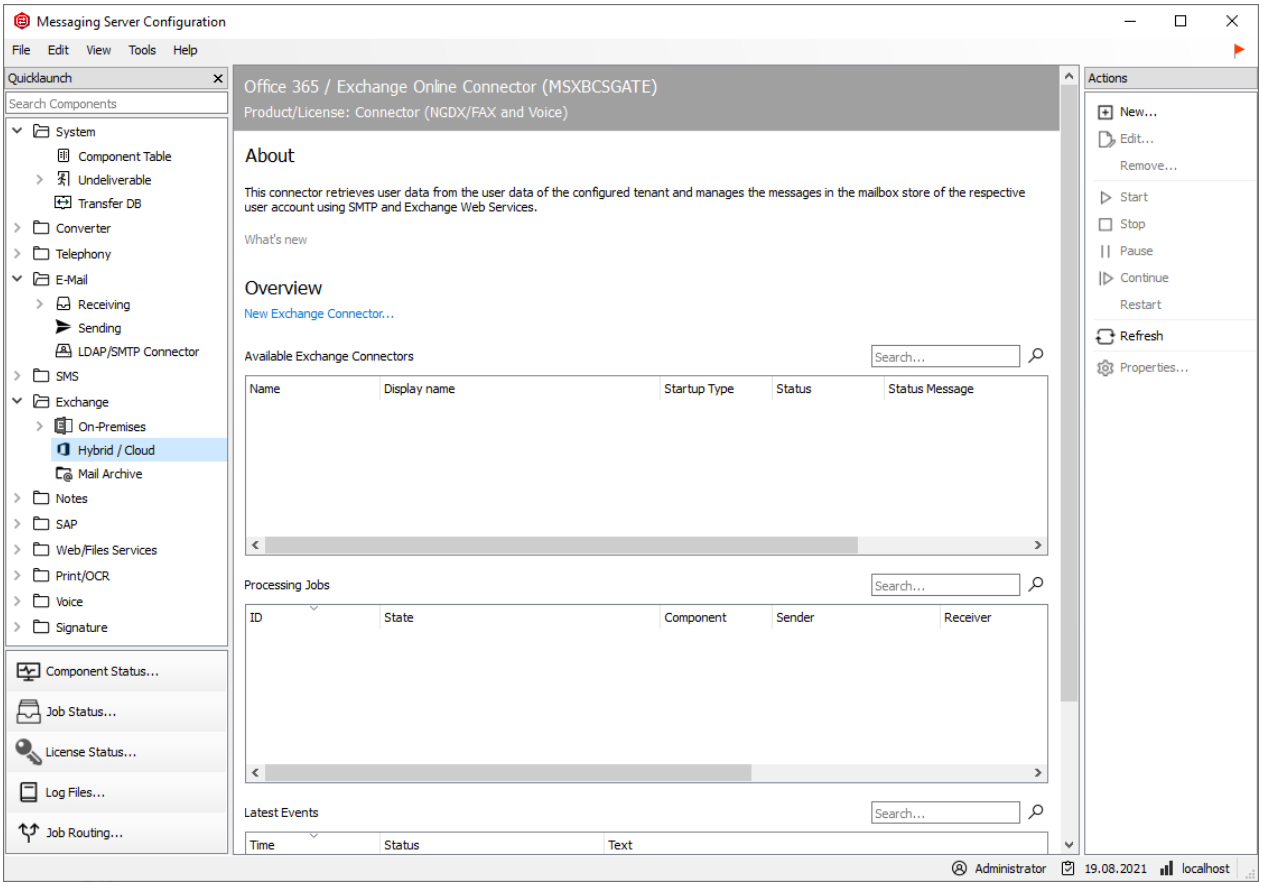
- Reading the configuration data of the connector stored in the Active Directory
- Reading global configuration values
- Resolve domain users and read user values
- Writing user-specific values after configuring voice parameters (own phone number, voice box pin, etc.)

Such an account should have the following authorization structure:

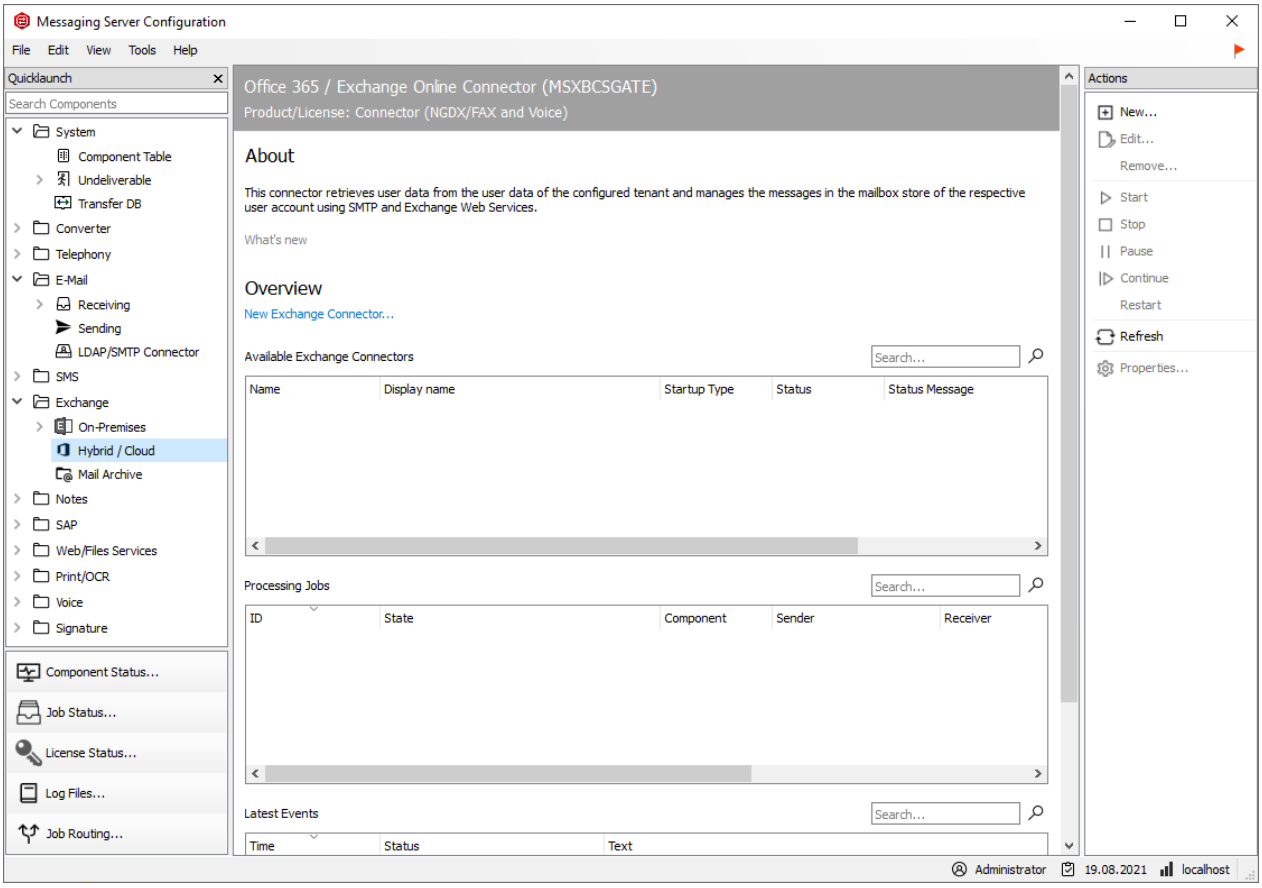
- Member of the domain users group
- Local administrator of the installation computer
- Read access permissions on the path containing the configuration file
- (Insinstallation option) Global data: Global Active Directory context
  In this case, the service account needs organization permissions (Exchange-Viewonly-Administrator). This setting is useful if connectors with this setting already exist. As of Exchange 2010, the organization can only have read permissions for Active Directory via membership of the *Exchange Public Folder Administration* group.
- (installation option) Global data: Active Directory default context
  In this case, the account does not need any additional permissions.
- (installation option) Global Data: Common Configuration File
  In this case, the account does not need any additional permissions.
- (installation option) user data: Active Directory user object
  If the connector should also be used to change voice properties such as PIN or phone number values by users via remote inquiry or Outlook client, the account must have write permissions in the user objects of the connected domains.

7.4.3. Installation

The connector is installed in the properties of the component administration for the Exchange/ Online services.



An installation wizard will now appear. The components should only be created and deleted using this installation wizard.

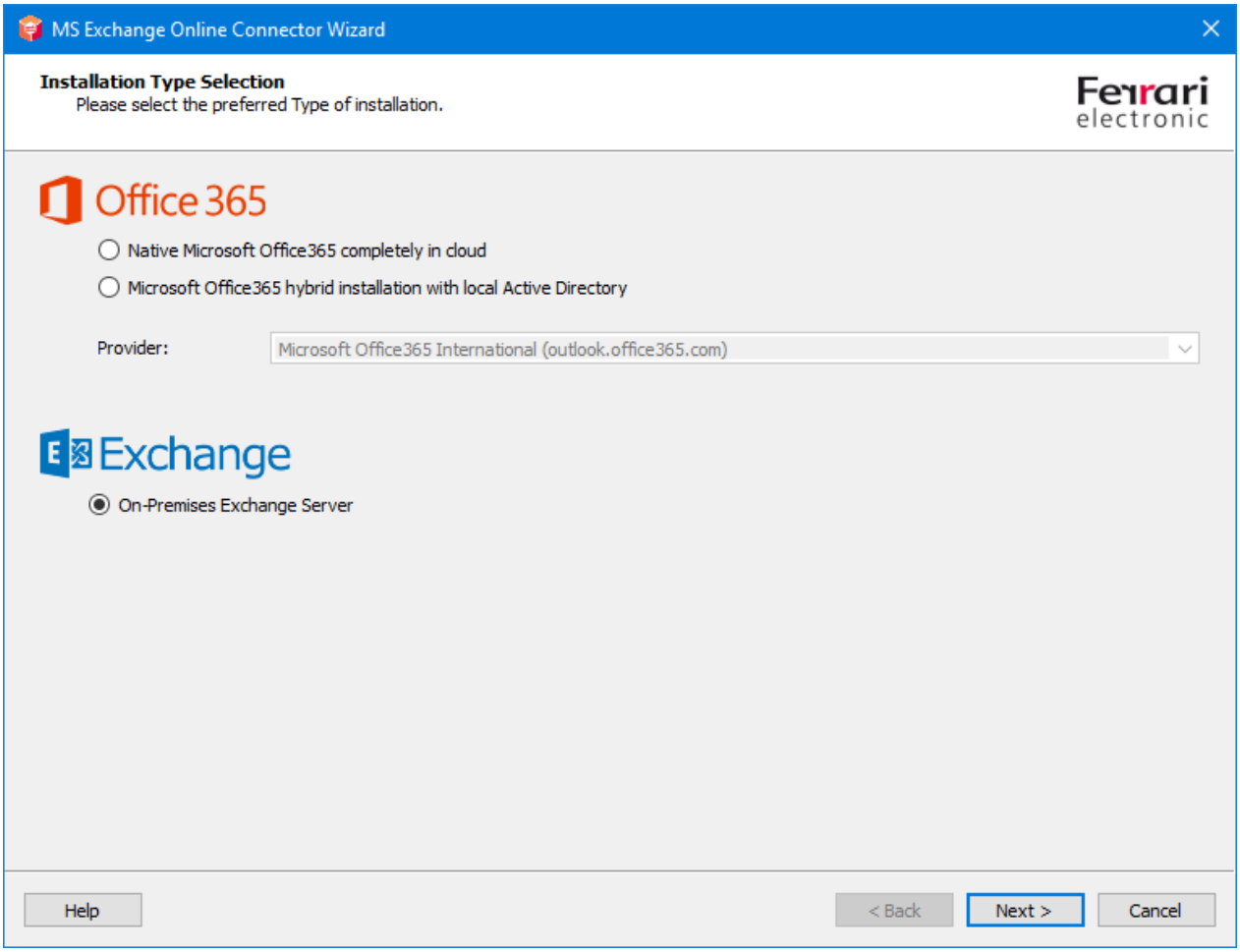


The welcome screen is followed by a dialog for selecting the type of installation.

Three installation forms are available:

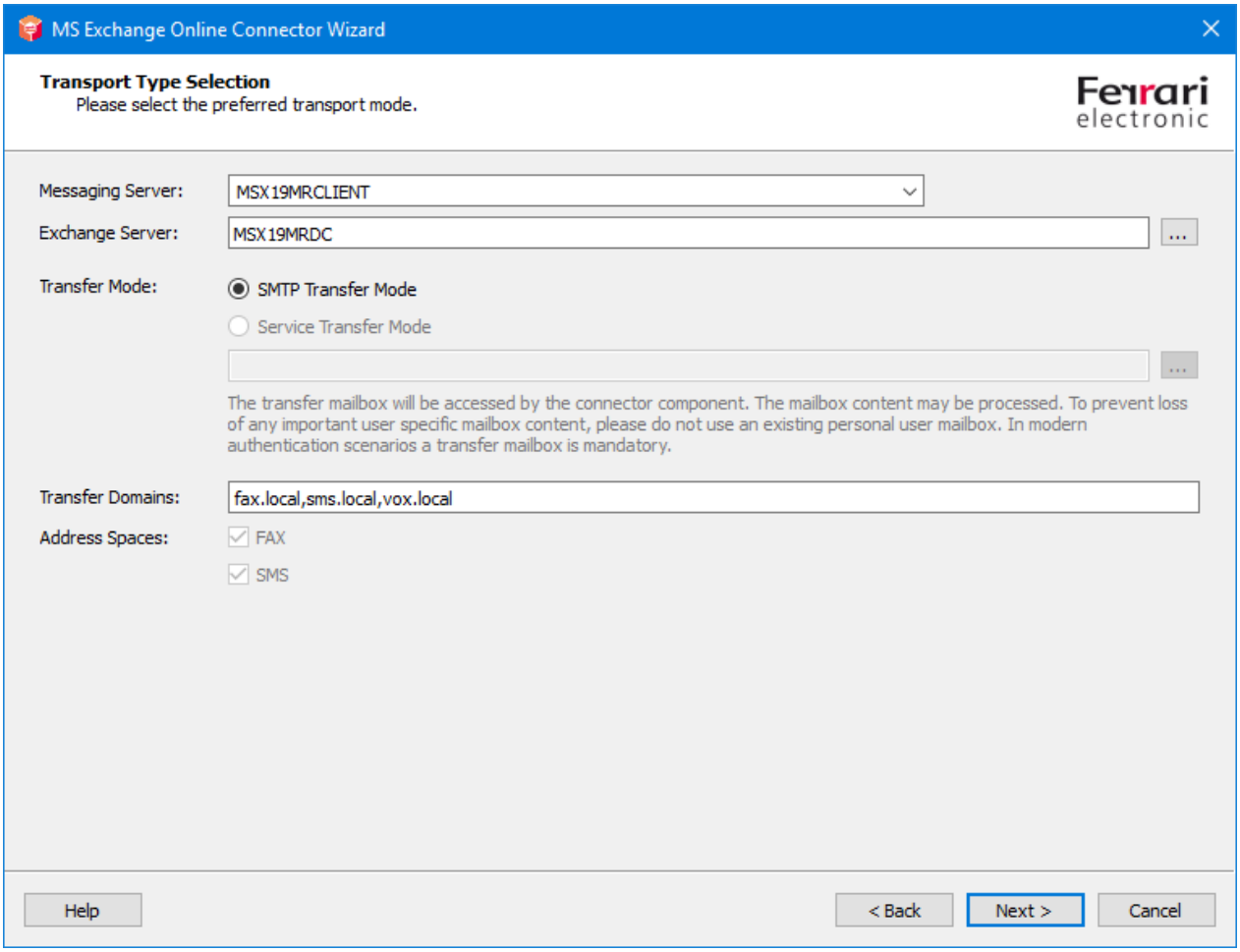
1. Exchange Online/Microsoft 365 as full cloud installation
2. Exchange Online/Microsoft 365 as a hybrid installation with on-premises Active Directory
3. Local Exchange Server Installation (On-Premise)

The third type of installation is used for local installations.



No explicit login to the Exchange Server is necessary.

In the next step, the transport type is selected. The transport type usually determines how outbound documents are handled.



In the local Exchange Server installation variant, no other transport variant is available than the SMTP transmission mode. No transport to an intermediate mailbox is required in the local network.

Messaging Server

In the Messaging Server input field, the server can be selected on which the Connector component will eventually run as an instance. The field shows in the main messaging server by default. It is also possible to specify here another messaging secondary server. If the list is not complete because the configuration program cannot fully access some of the slave servers, the desired name of the slave server can also be entered manually.

Exchange Server

For communication with an Exchange Server, this must be entered as the default communication partner. A fully qualified domain name (FQDN) or a NetBIOS name can be specified here. IP addresses should not be specified, as a display name is created from this specification.

Transfer mode

No further transfer mode can be selected at this point. The installation form only supports the SMTP transmission mode.

Transfer Domains

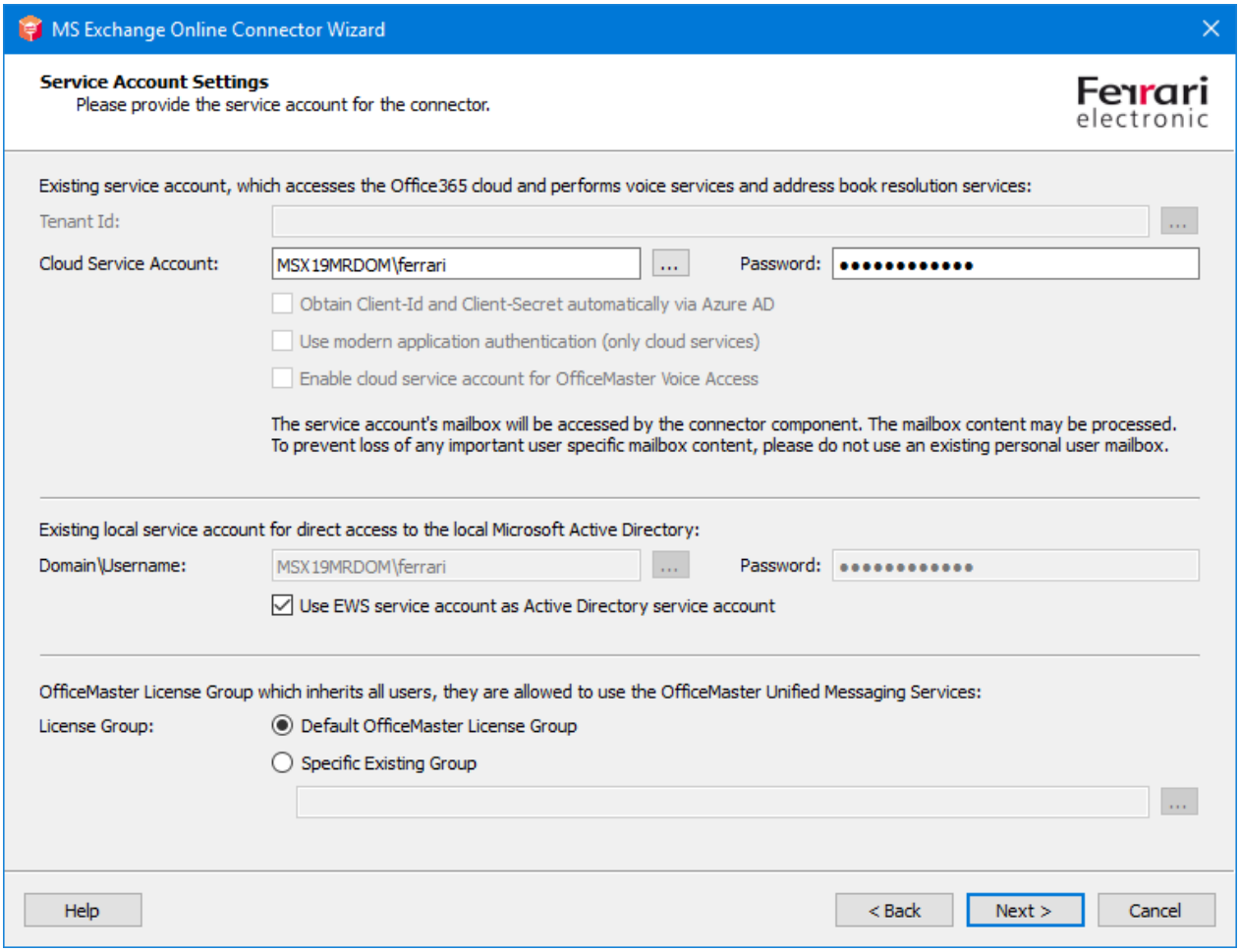
Despite the possibility that the address spaces FAX and SMS are available in the service transfer mode, transfer domains should definitely be specified. Transfer domains are SMTP domain details that are used as fax, SMS or voice sending domains. This domain information is also used for incoming messages. The sender can then send his outgoing documents to *fax number@domain*. By default, domains should be specified with the subdomain prefixes “fax” and “sms”. If MWI lamps are also to be switched off via read mail items, a “vox” domain should also be specified.

> E.g. fax.exampledomain.de, sms.exampledomain.de, vox.exampledomain.de
>
> **Note!**
>
> The domains are separated with a comma or a semicolon when they are specified. The transfer domains are given here purely for registration purposes. Whether the e-mails from the Exchange Server also reach the OfficeMaster Server with this domain specification depends on the manual administration of the Exchange Server.

Address spaces

Although the installation supports the use of address spaces, these are not stored here. Address spaces cannot be influenced during installation.

In the next step, the service account for access to the Exchange Server and the local domain is specified.



At this point the service account can be selected. Different service accounts can be specified for Exchange Server access (Exchange Web Services) and access to the local Active Directory. However, this is optional. It is recommended to use the same account for both accesses.

Authorize service account for voicemail services

This function is not available in this installation variant. The account for the OfficeMaster language services may have to be activated manually if language services are to be used.

To perform this step manually, this can also be done with the Exchange PowerShell:

```
New-ManagementRoleAssignment OfficeMasterVoiceAccess
-Role ApplicationImpersonation -User \<Service AccountEmailAddress\>
```

Local service account with access permissions to on-premises Active Directory

At this point, a separate account can be specified for access to the Active Directory.

Use EWS service account as Active Directory access account

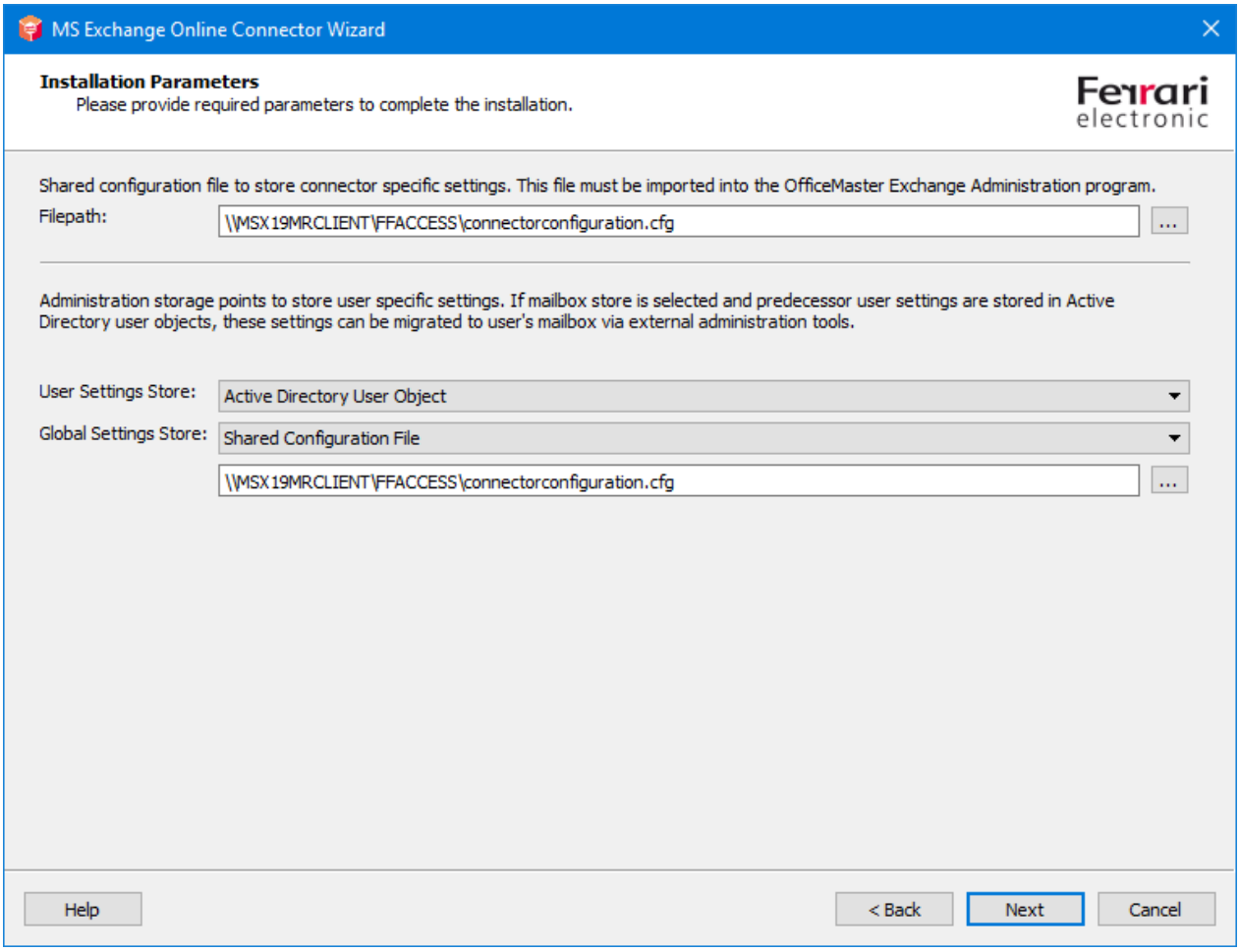
When activating this function, the values of the Exchange access account (EWS service account) are copied into the input fields for the Active Directory service account.

> Note!
>
> It is generally recommended to use the same service account for access to the Exchange Server (Exchange Web Services) and to the Active Directory.

OfficeMaster license group

In the field of the license group, for the Small Business variants (e.g. OfficeMaster 250 for MS Exchange), the license group is specified in which the licensed users must be entered. By default, the license group is created automatically and is named “OfficeMaster License Group”. This entry point is not accessible for unlimited OfficeMaster versions.

In the next installation step, the local configuration points are specified in which the connector configuration is saved.



File path

The general configuration of the **msxbcsgate** component is traditionally administered via MMC configuration snap-ins. With this type of connector, the configuration data is always saved in a configuration file. The path of this file can be specified here. By default, a file that is in the OfficeMaster release *FFACCESS* is suggested here.

User data management

In the local Exchange Server installation variant, there are two installation options available:

Active Directory user object

This is the recommended default.

User mailbox

Alternatively, the user-specific values can also be saved in the user mailbox. This does not make sense in the local installation variant.

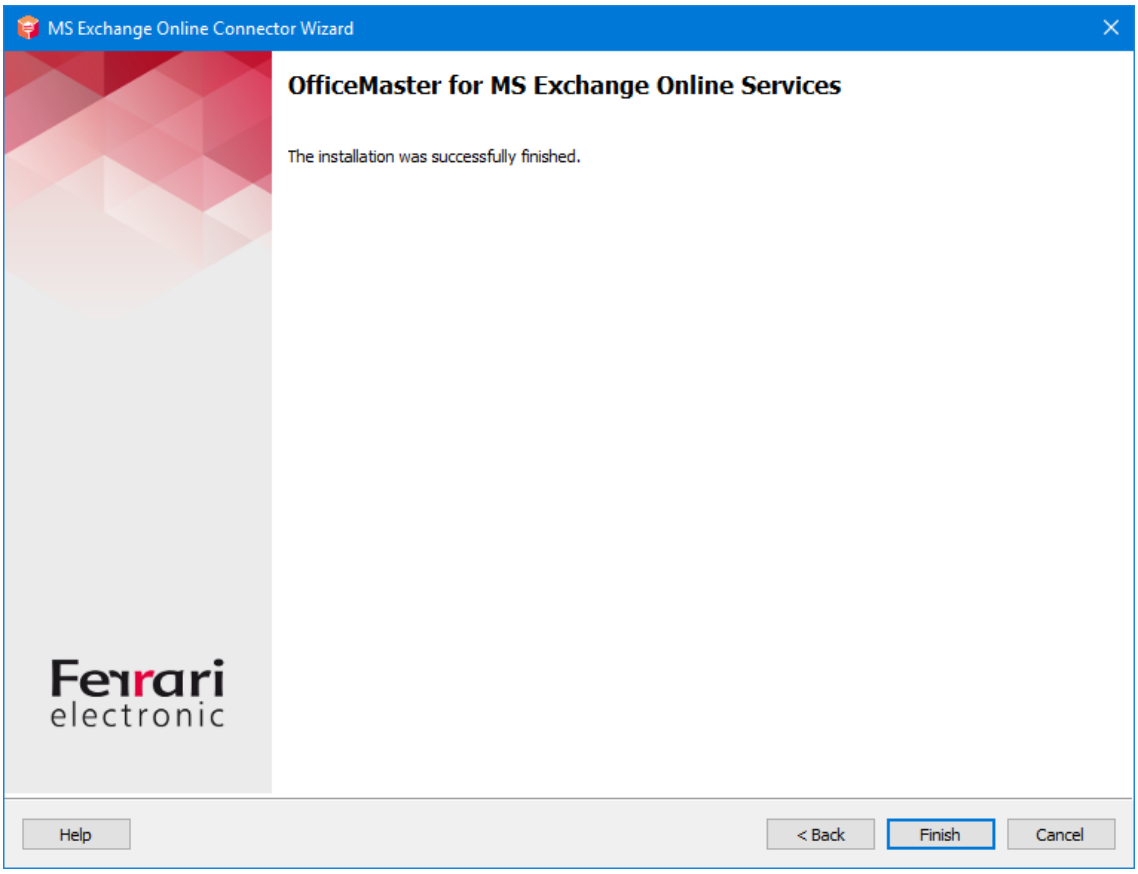
> Note!
>
> If a previous version of the exchange gateways from Ferrari electronic AG was used and the user-specific values are already available in the Active Directory, they can continue to be used in a compatible manner. If the user management mode is then switched to *user mailbox* (not recommended), these values must be migrated from the Active Directory to the Microsoft 365 mailboxes using special tools, otherwise the Active Directory will no longer be accessed.

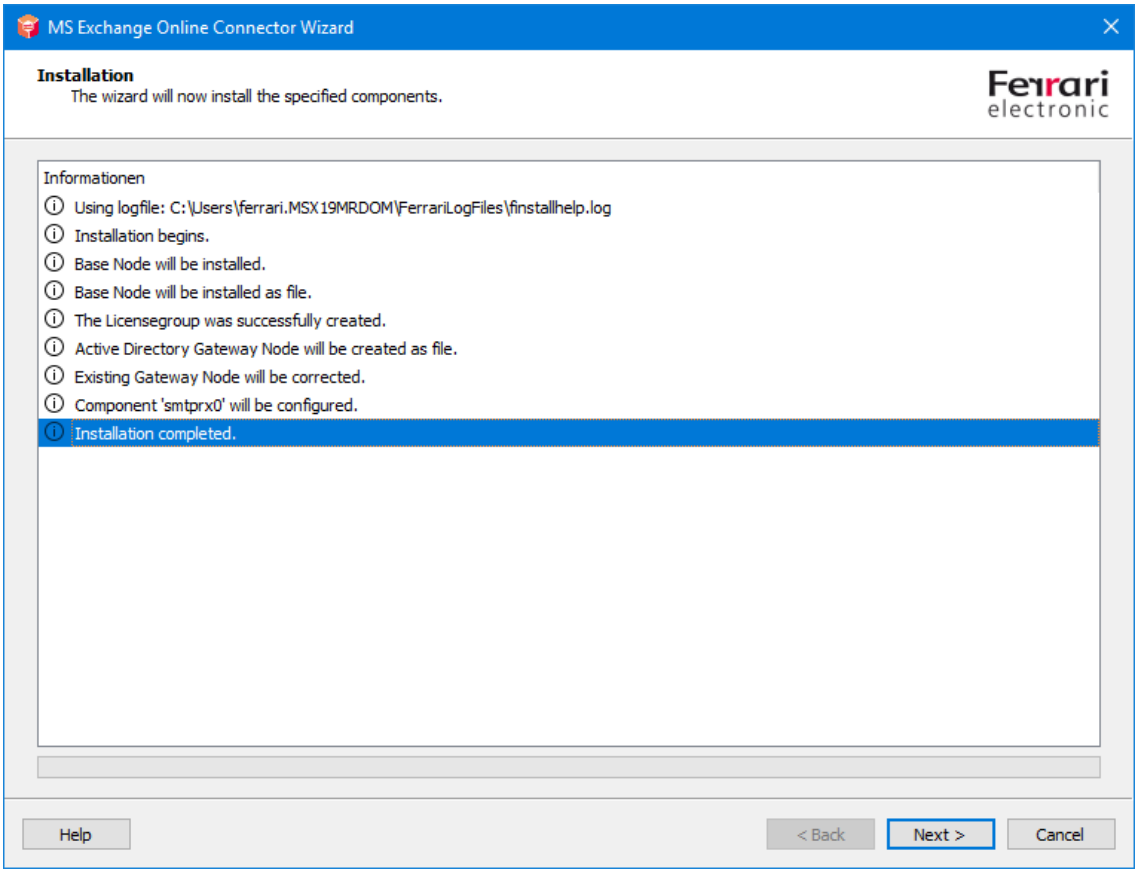
Global user data

Global user data is the template data that applies to all users for whom other values have not been explicitly specified (fax ID, header, cover sheet, etc.). These global specifications found in the Microsoft 365 only installation variant can only be saved in a configuration file. At this point, it makes sense to use the same file that contains the connector configuration data. The default setting is that the values are written globally to the existing Active Directory. This default setting is only set for compatibility with the previous version. This makes sense if such a global configuration node has already been installed from the previous product.

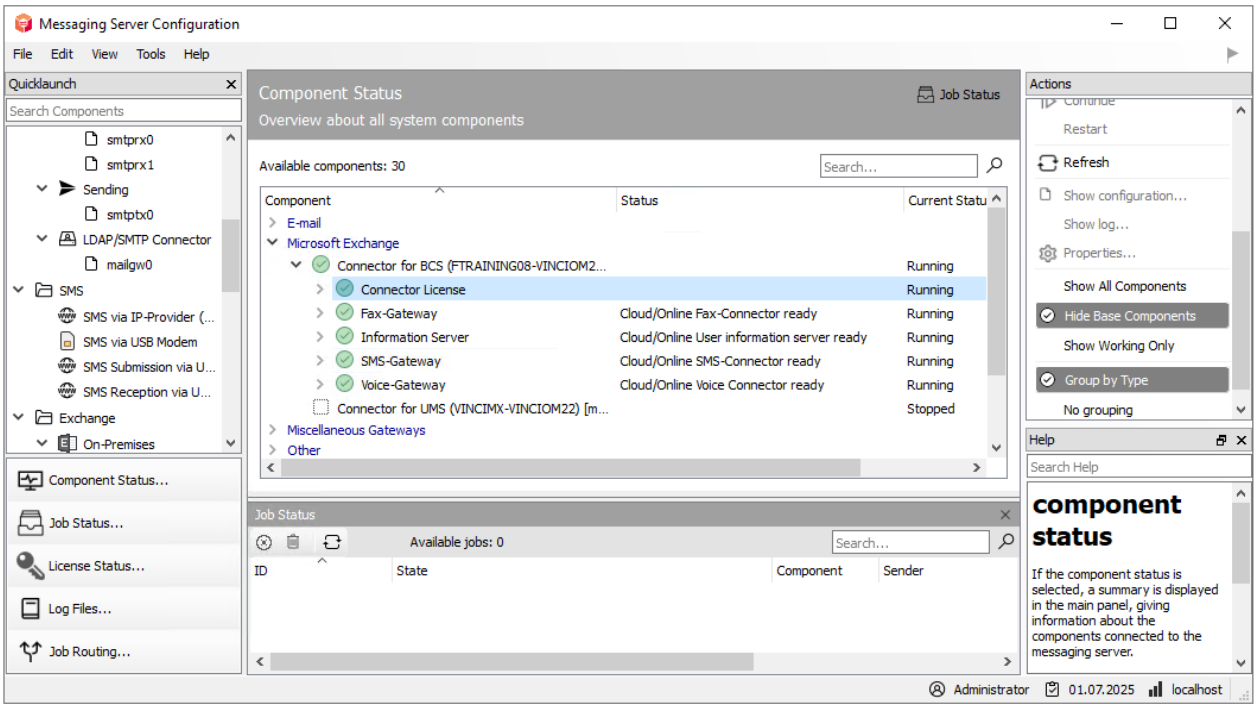
> Note!

If there is no global configuration node yet, installation in a shared configuration file is recommended.





The necessary parameters for installing the connector are now known. The connector can now be created in the next installation steps.



After installation, the component should start immediately and be ready for use.

7.4.4. Objects to be created manually in a local Exchange environment

If the connector is to be installed in a local Exchange Server environment, it must be ensured that outgoing emails are routed directly to the messaging server. This is usually regulated by a send connector or an SMTP connector. The following basic values can be configured:

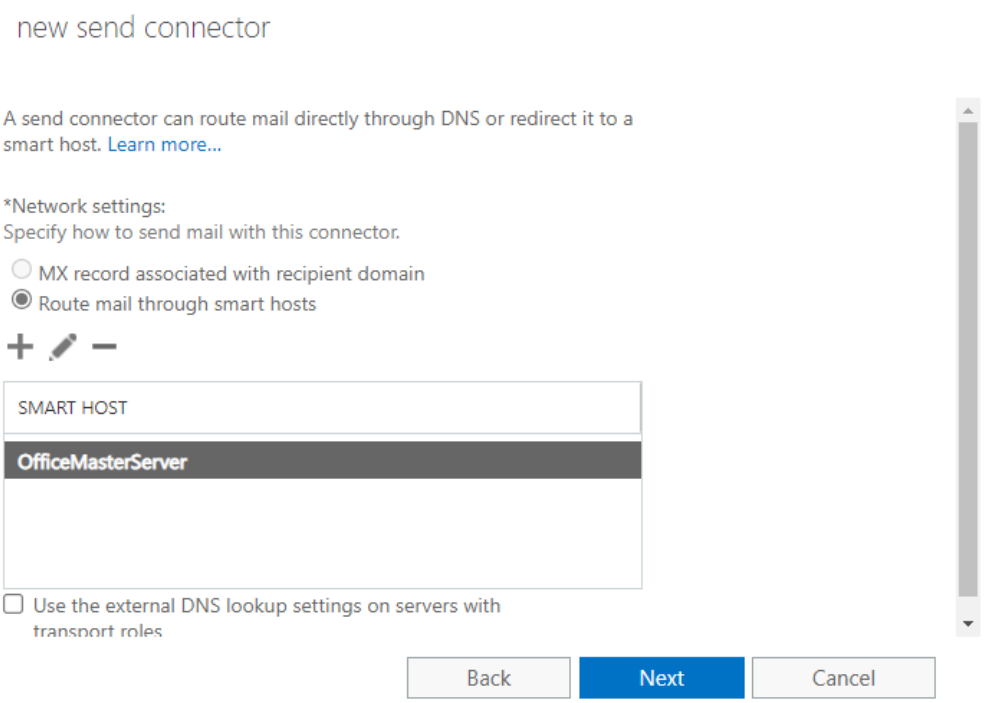
Object: SMTP send connector

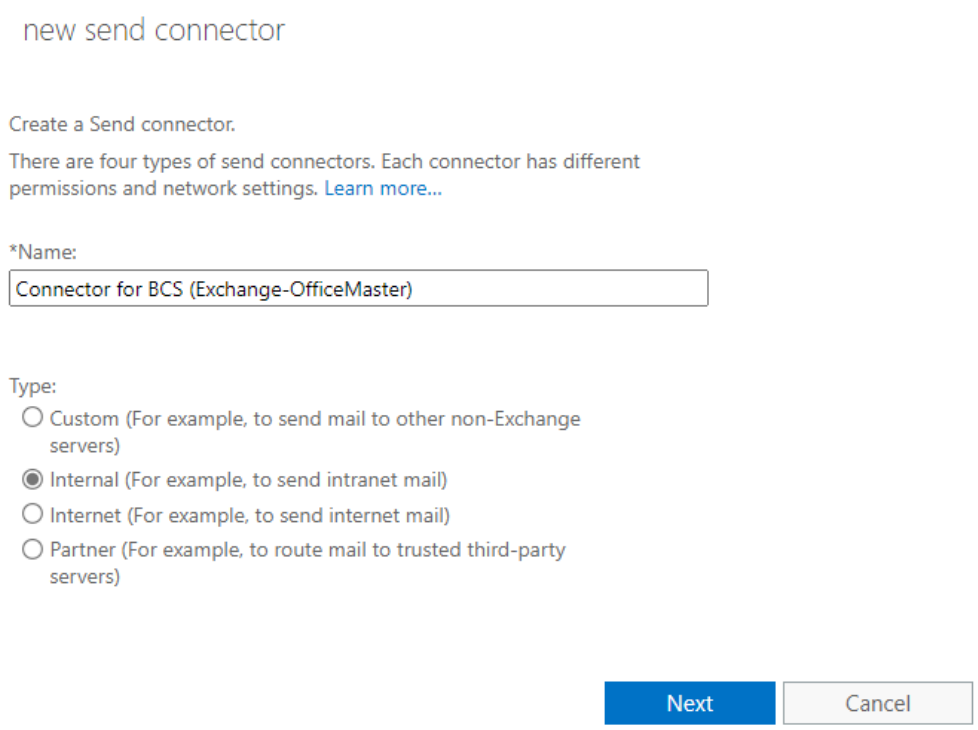
Type: SMTP Smarthostcommunication

Sending server: Exchange server to send from. (Source Server, Local Bridgehead)

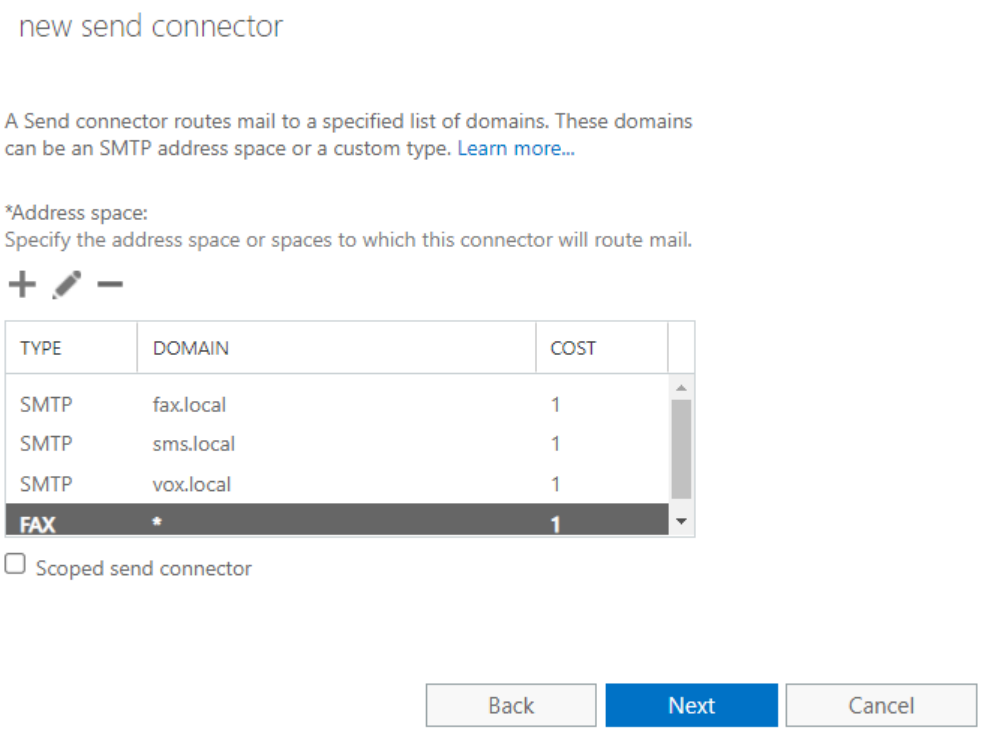
Smarthost: IP address, name or FQDN of the OfficeMaster server

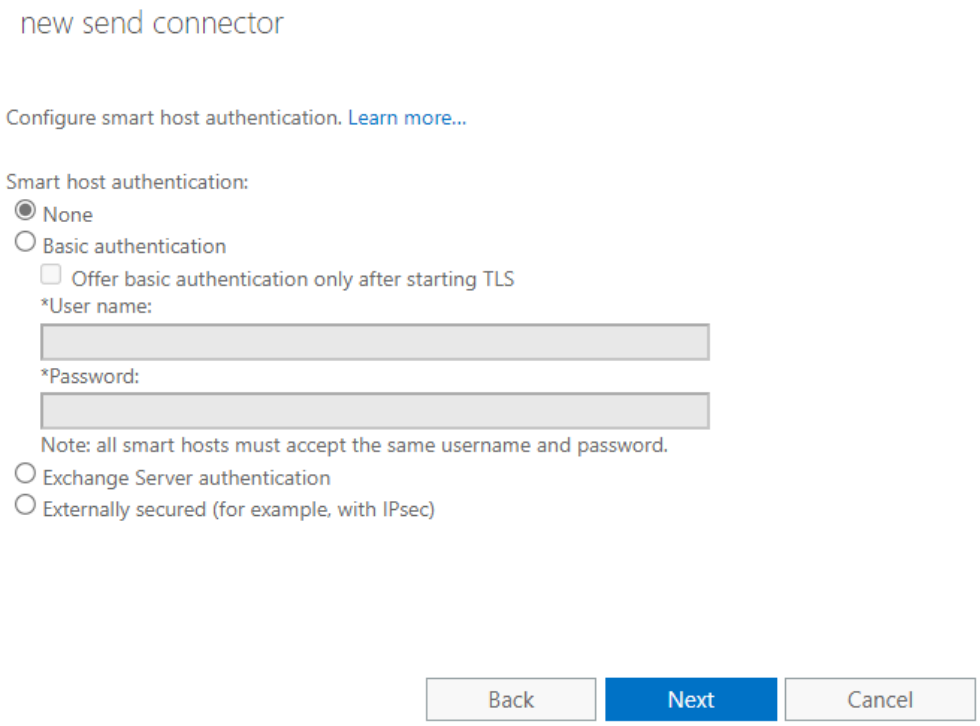
Such a send connector can then include the desired transfer domains in its address spaces. It is also possible to configure the FAX and SMS address space there. The creation of the send connector should be briefly addressed using an Exchange Server 2016 example.



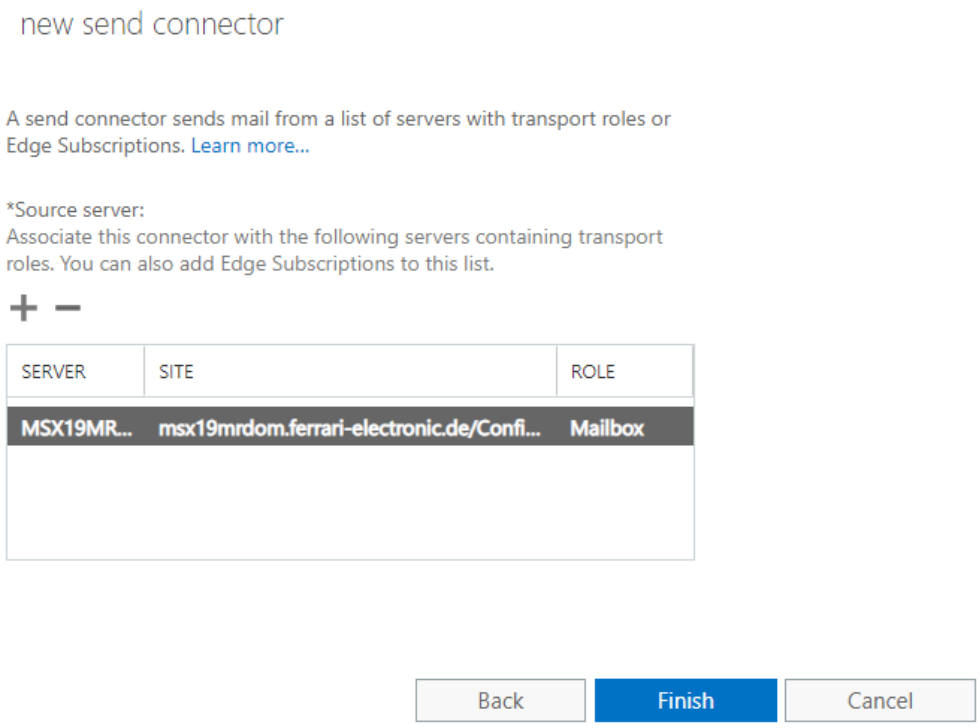


No authentication needs to be specified for communication with an OfficeMaster server. (The name OfficeMasterServer as smart host is only an example. The correct name or IP address of the server should be used!)





The last step is to add the source server. The Exchange Server can now send documents to the OfficeMaster.



Since the OfficeMaster also sends documents to the Exchange Server, a corresponding receive connector must be available. The **msxbcsgate** component does not use authentication by

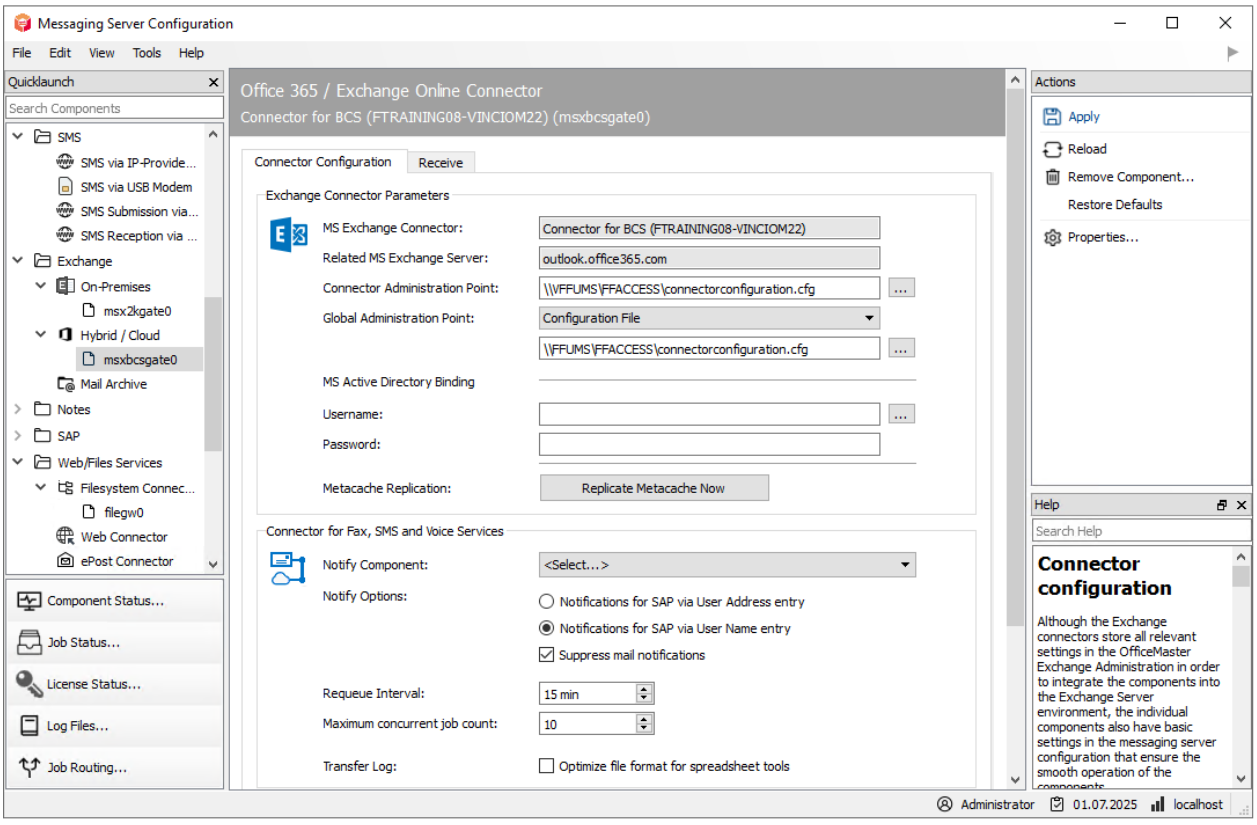
default, which is why either the standard SMTP receive connector should be activated for anonymous receipt, or a separate connector should be created.

7.5. Configuration

7.5.1. Messaging server configuration

Microsoft Active Directory is not required for the pure connection to a Microsoft 365 service. The connector only requires a working connection to Microsoft 365 via the Internet.

Although the connectors store all relevant settings in a configuration file in order to integrate the components into the Exchange Server environment, the individual components also have basic settings in the messaging server configuration that ensure smooth operation of the components.



The basic settings are on the Exchange connector parameters tab.

Exchange connector parameters

These settings are set by the installation wizard. They include the connector name, target server FQDN, configuration file path, and more.

Note!

Although the basic settings can be configured in expert mode, manual administration is not recommended. The basic parameters should only be set by the installer. Manual changes can severely disrupt the correct operation of the components.

MS Exchange Connector

The name of the connector component is displayed in this field. This field cannot be changed and is provided for information only.

MS Exchange Server

The field cannot be changed either and contains the selected server for information.

Connector administration point

The connector administration point is the configuration file in which the connector expects its actual configuration. This entry can be changed or restored accordingly. A change in this parameter is only available for restore purposes and should not be changed without the installation wizard.

Global administration point

The global administration point is the storage location for the global user preferences. One can only set the general access mode here.

- Microsoft Active Directory
  In this mode the connector looks for the global point in the configured Active Directory
- configuration file
  In this case, the connector uses the specified file to read out the global user values.

The entries can be changed or restored accordingly. A change in this parameter is only available for restore purposes and should not be changed without the installation wizard.

MS Active Directory connection

A user name and a password can be stored in the Active Directory connection fields, with which the connector accesses the configured Active Directory. With a pure Microsoft 365 connection, these entries are empty.

Metacache replication

There is a button in the configuration that can be used to trigger metacache replication outside of the set intervals. This option is only implemented for test purposes.

Status component

A status component is an additional component that is informed about the status of the sent fax document or the sent SMS. Here, for example, archive gateways can be specified.

Status options

The status options are used to optimize and customize the interaction with other components.

- Status messages for SAP based on the user address field
  If the **msxbcsgate** connector is used by an SAP gateway as a status component, there are various ways in which the SAP connector stores the sender in the order. The internal field **UserAddress** is used as a criterion for the sender.
- Status messages for SAP based on the user name
  The internal field **UserName** is used as a criterion for the sender.
- Suppress email status feedback
  If the **msxbcsgate** connector is operated with a **filegw** component (file interface) or a **lpd** component (printer component), the connector can print the document autonomously if an e-mail address is specified send via SMTP. This sending is carried out via the connected Exchange Server. With this transmission (exchange relay), the connector receives a report from the sending server as to whether the e-mail was accepted by the server. Since this report does not provide any real information as to whether the e-mail actually arrived at the recipient, but is only an indication that the e-mail was received by another part of a process chain, many users want to ignore this transmission report. This can be done by activating the function.

Requeue interval

If the msxbcsgate connector cannot deliver the messages to the target systems (maintenance intervals, converter problems, printing problems), the order will be delivered again. The time delay of this new delivery (requeue) can be specified here in minutes.

Simultaneous order processing

The connector is able to process several orders at the same time. The maximum number of simultaneous jobs to be processed can be specified here.

> Note!
>
> It should be mentioned that a number greater than 10 does not result in a greater increase in performance. The optimum number for current computers is 10. This is also the default. The value can be reduced to 1 to force sequential processing of the orders. This should only be done for testing purposes. It is recommended to enter a value between 5 and 10.

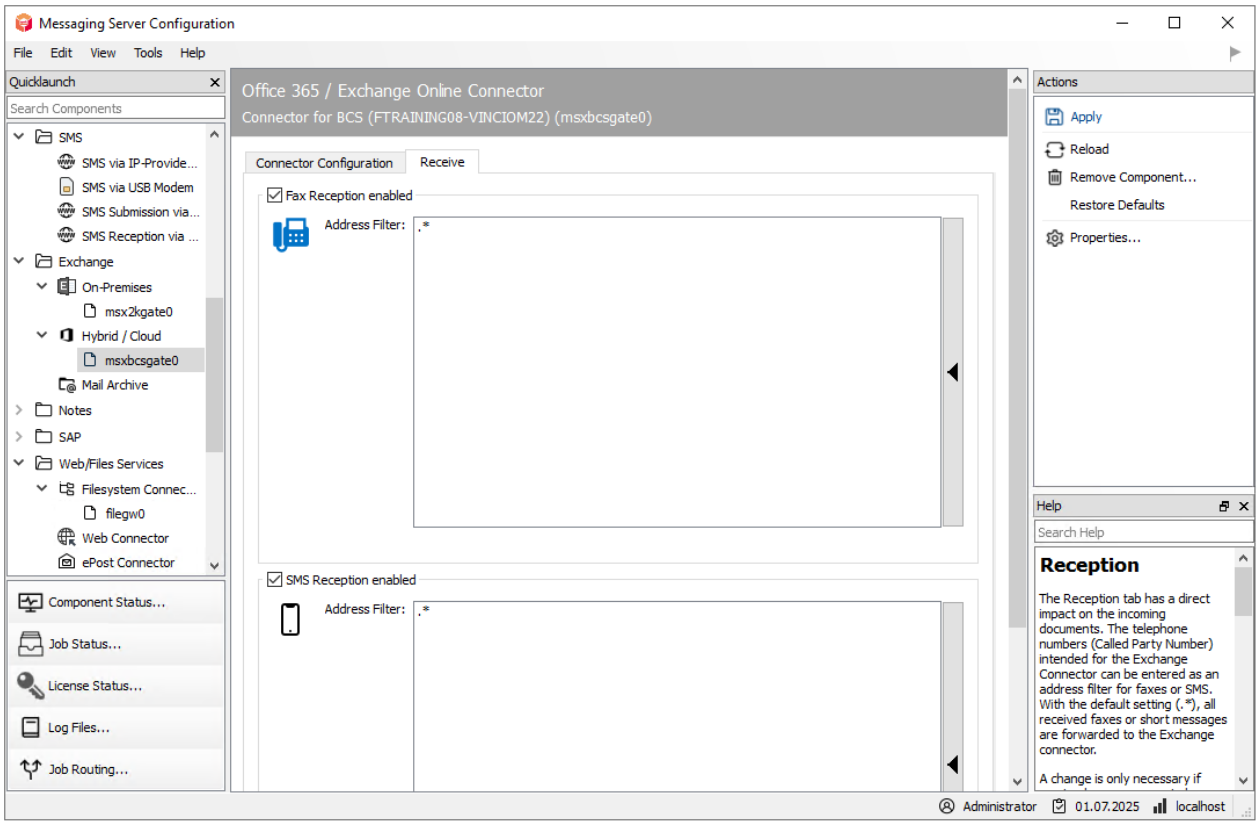
Transfer log file / Optimized for spreadsheet programs

The msxbcsgate component writes a file with the orders that have been processed for each day. Telephone numbers in E.164 format are also written to this file. It was often found that spreadsheet programs convert this notation (e.g. +49332845590) into a floating point representation (+49332845590 becomes 4.93E+10). Leading zeros are also mostly removed by the program. To mark these entries as text, the entry can be preceded by a single quote. Modern spreadsheet programs then interpret this data as unchangeable character strings and leave the display unchanged.

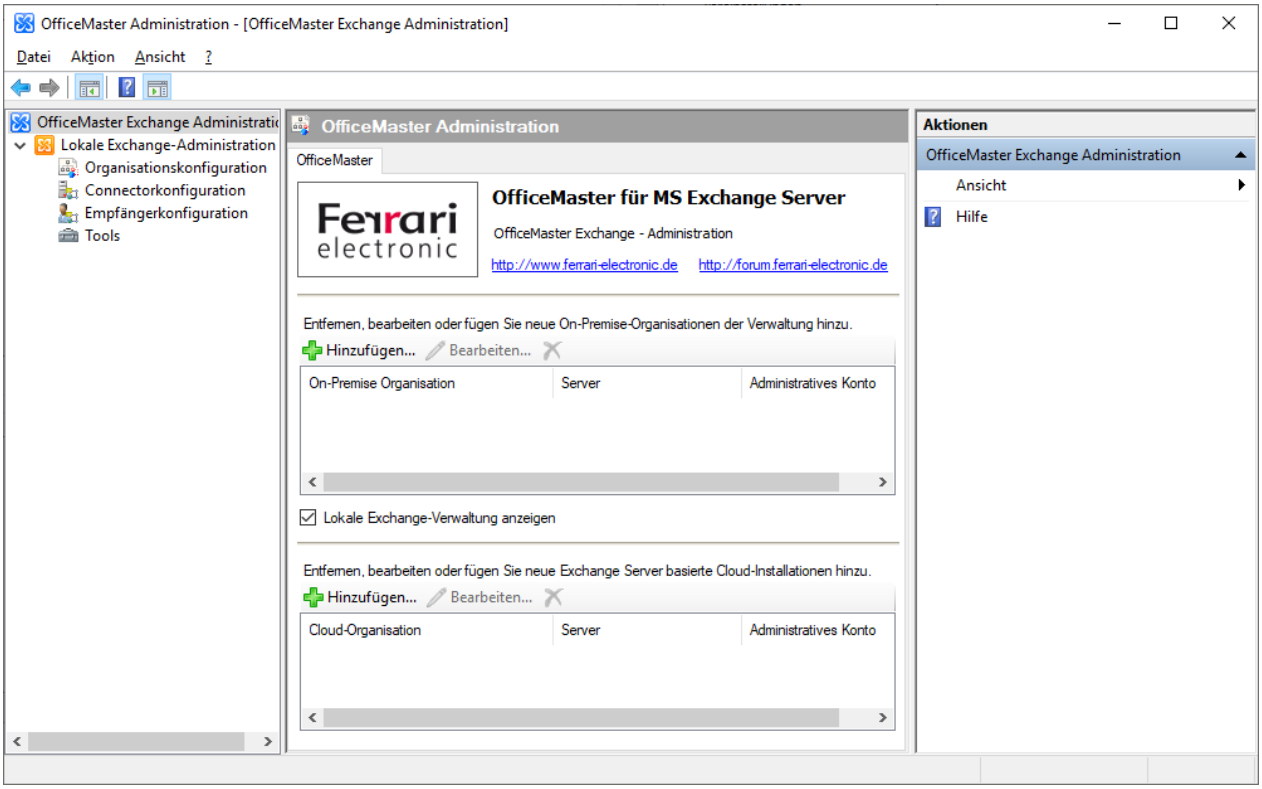
Reception tab

The “Receive” tab has a direct influence on the incoming documents. The phone numbers (Called Party Number) from the receiving processes intended for the Exchange Connector can be entered as an address filter for fax or SMS.

With the default setting (.*), all received faxes or short messages are forwarded to the Exchange connector. A change is only required if received messages are to be distributed to different gateways such as SAPCONN or FILEGW.



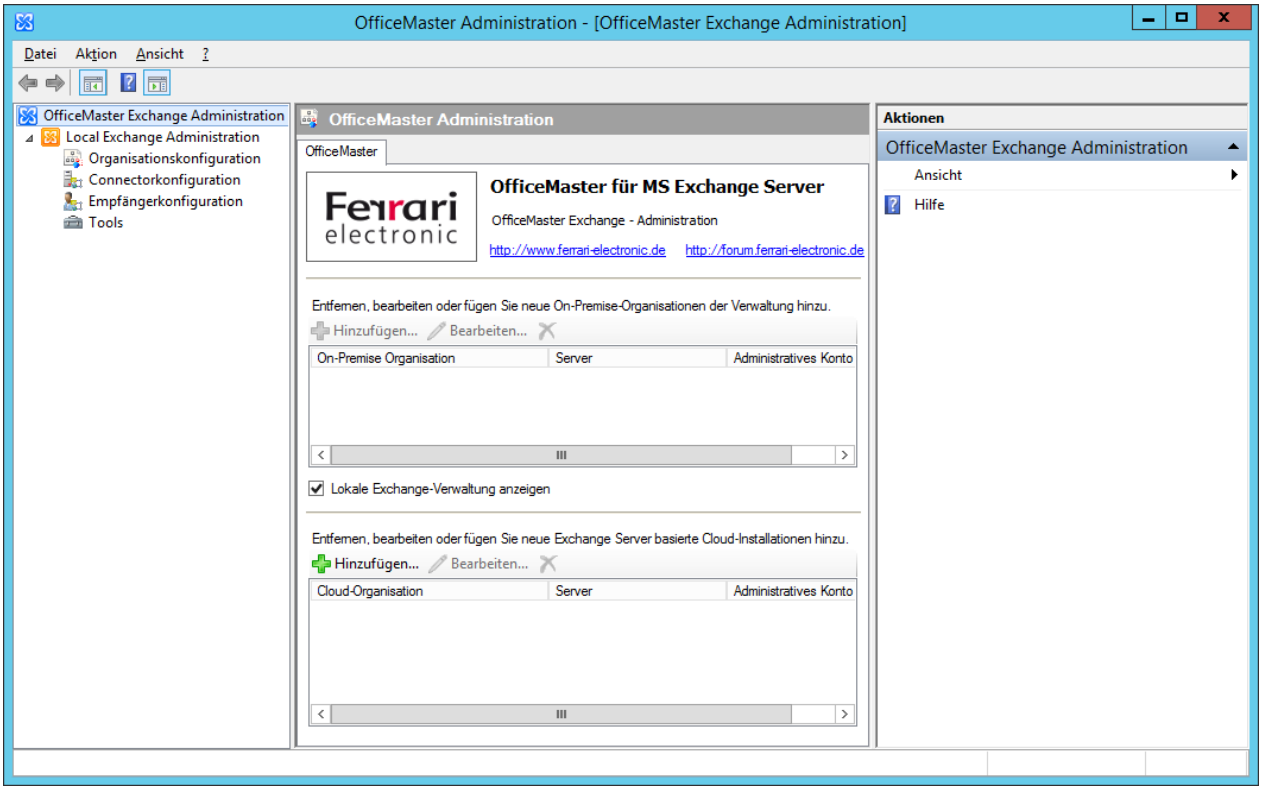
7.5.2. OfficeMaster Exchange administration



If during the installation of the OfficeMaster Suite the setup option **OfficeMaster for Exchange/ Exchange Online-Connector** was selected, the OfficeMaster Exchange management console is available on the system. At the time, this console extended the Exchange Server 2010 management console and can also represent its own management node. The structure of the current version has not changed compared to the OfficeMaster 7 predecessor. After starting the console from the available program icons, the following view appears:

Traditionally, OfficeMaster Exchange Connectors are configured via MMC SnapIns, which may also be integrated into existing Exchange Server administration tools or into Active Directory administrations.

With the OfficeMaster Exchange administration, individual user settings and connector settings can be conveniently configured.

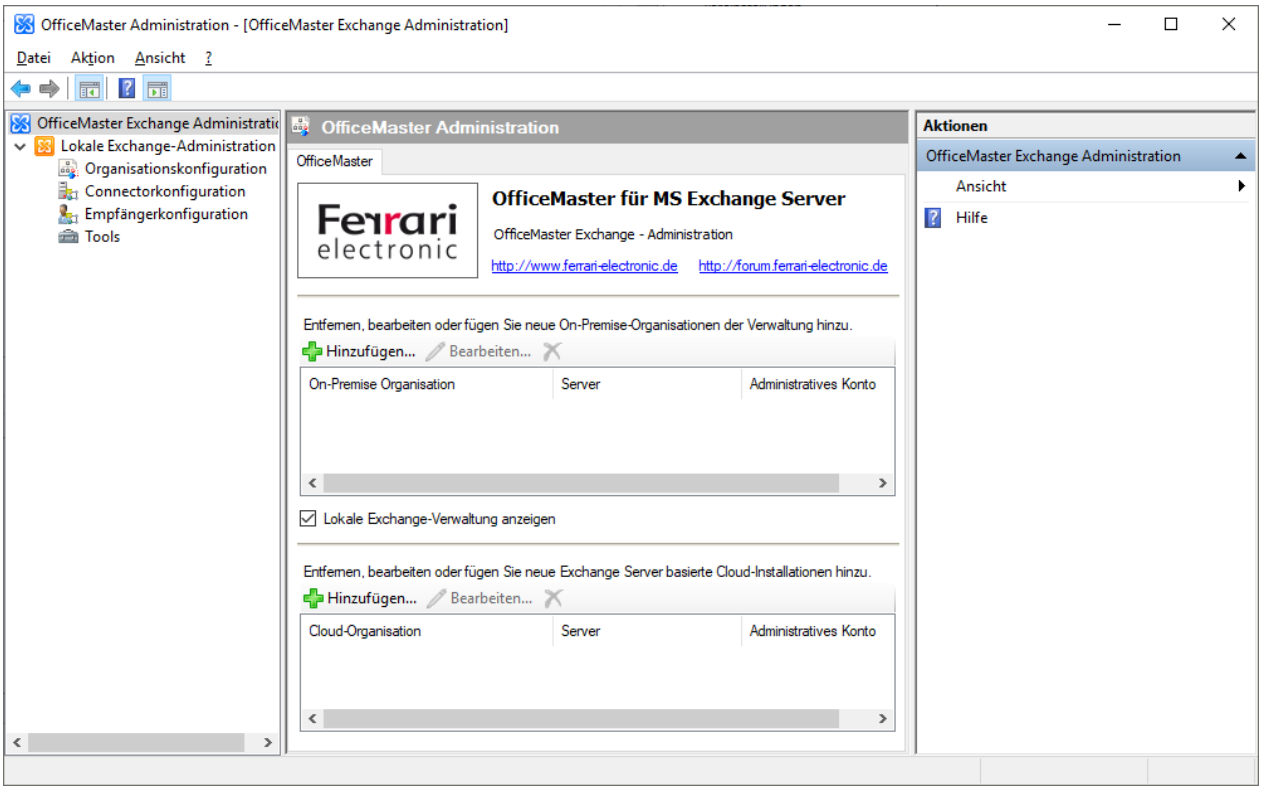


The areas of administration have the following meaning:

- OfficeMaster base configuration node
  The OfficeMaster base configuration node is the highest level of OfficeMaster Exchange administration. When you click on this node in the area window (left side, Scope Panel), the central administration dialog for adding the configurable clients appears in the result area (middle, Result Panel).
- Configuration of a local Exchange Server installation
  The local Exchange Server installation area is the local Exchange organization's traditional display of the current user logon to Windows. The display of the local administration can be switched off in the local client area.

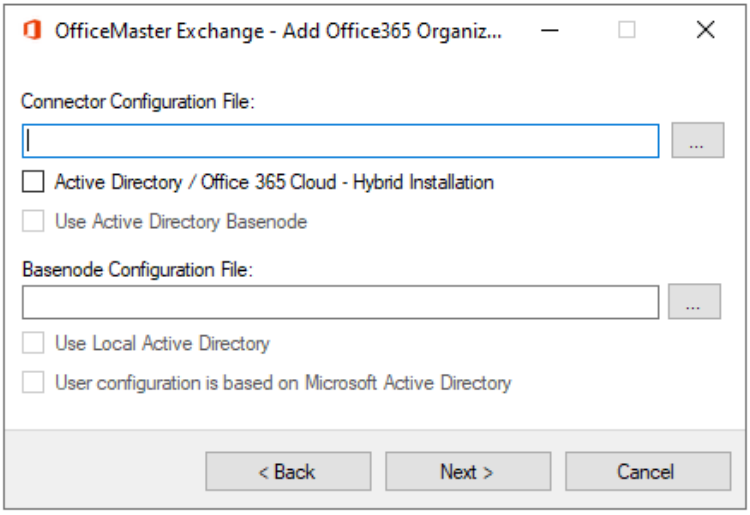
- Local client area
  On-premises Exchange organizations can be added using the local tenant area. The console will then connect to the added Active Directory.
- Cloud/Microsoft 365 Organization Panel
  Installed Cloud/Microsoft 365 organizations can be added in the Cloud/Microsoft 365 organization area. Added organizations are displayed in the area window (left side) as an additional main node, on a par with the local Exchange Server Administration.

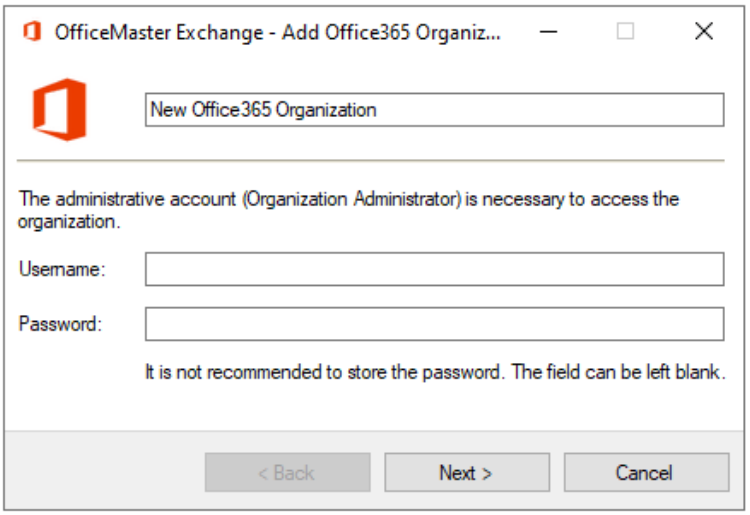
7.5.3. Configuration of a Microsoft 365 installation without on-premises Active Directory



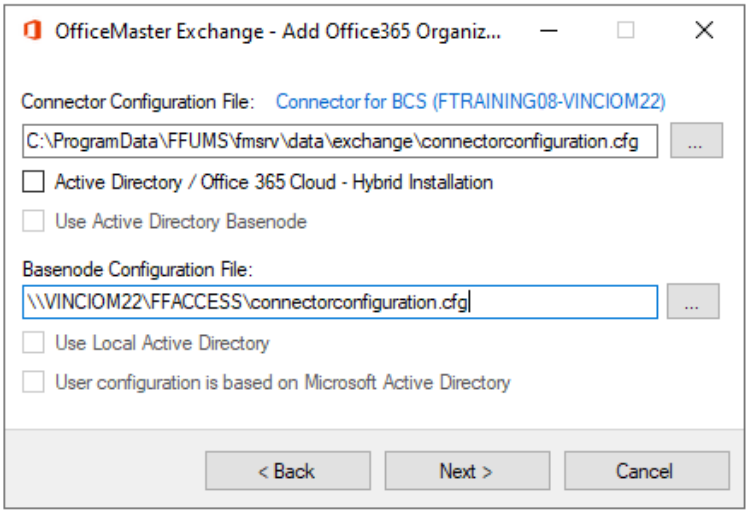
Since a pure Microsoft 365 installation does not have a local Active Directory, local administration should be switched off by ticking the local client area. The nodes are then removed from the range window. In order to then configure Microsoft 365 connectors, a new organization in the Cloud/Microsoft 365 organization area should be now added.

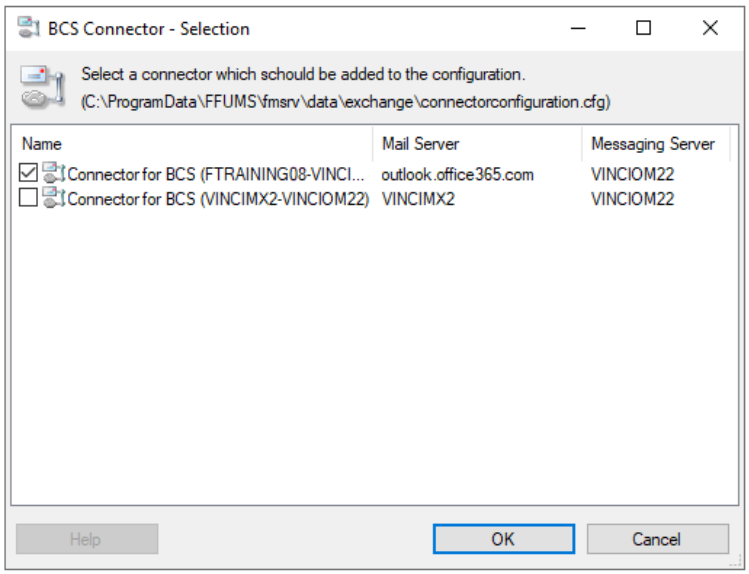
After clicking the “Add” button, a wizard opens with the parameters of the new organization. At this point, an adequate display name for the organization should be assigned. Likeweise, the default user name for access to Microsoft 365 is also stored here. The password can be specified here at this point, but would then be stored in a configuration table. This is a security concern, so it is not recommended. The password field can remain empty. Then follows the possibility to specify the connector configuration file.





After selecting the common connector configuration file that was specified during the connector installation, a window opens in which the responsible connector should be selected. Since the file can contain several connectors, the correct connector should be selected here.





After selecting the connector, the configuration dialog should fill in automatically. If necessary, the entered values and checked fields should be checked for correctness.

Connector configuration file

The configuration file is here specified, which was specified during the connector installation.

Active Directory / Microsoft 365 Cloud hybrid installation

If this option is enabled, the administration is prepared for access to an Active Directory. With a pure Microsoft 365 installation, this option is not active.

OfficeMaster base node is located in Active Directory

At this point it is specified where the global user data is located. When the feature is enabled, the data resides in an Active Directory node. If the option remains inactive, a configuration file that houses the global user data must be specified.

Base node configuration file

If it was specified during the connector installation that the global user data is in a configuration file, then this should be specified here. As a rule, this field will change itself automatically after selecting the connector configuration file.

Use local credentials for Active Directory access

As a rule, a server and an access account can be specified for access to an Active Directory. However, if this option is enabled, the optional user data are omitted. In this case, the Windows login account is used to access the Active Directory.

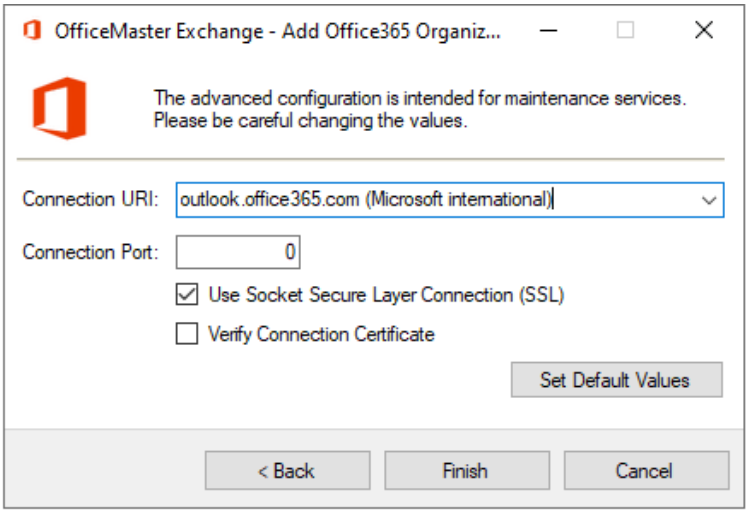
As a rule, this field will be filled in automatically after selecting the connector configuration file.

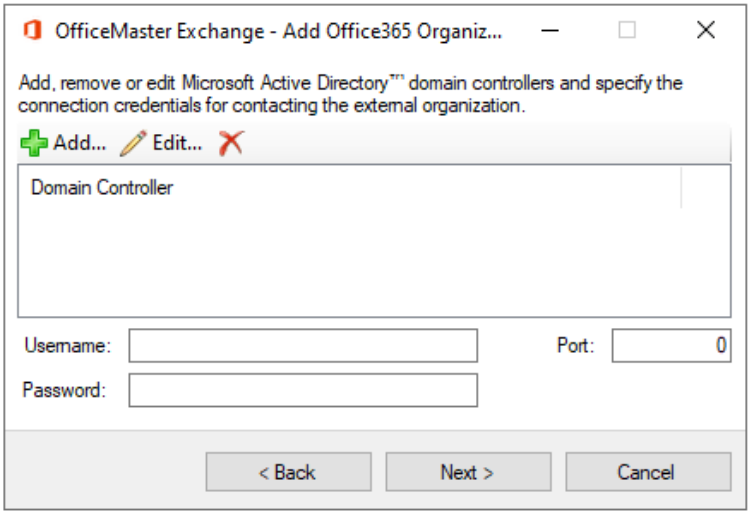
User configuration based on Active Directory entries

In order to be able to administer the OfficeMaster user properties correctly, the administration must know how the properties are saved. If the option is activated, the data is read and saved in the user object of the user to be administered in Active Directory. If the option remains inactive, the properties are read from the user mailbox and also saved in the user mailbox.

As a rule, this field will be filled in automatically after selecting the connector configuration file.

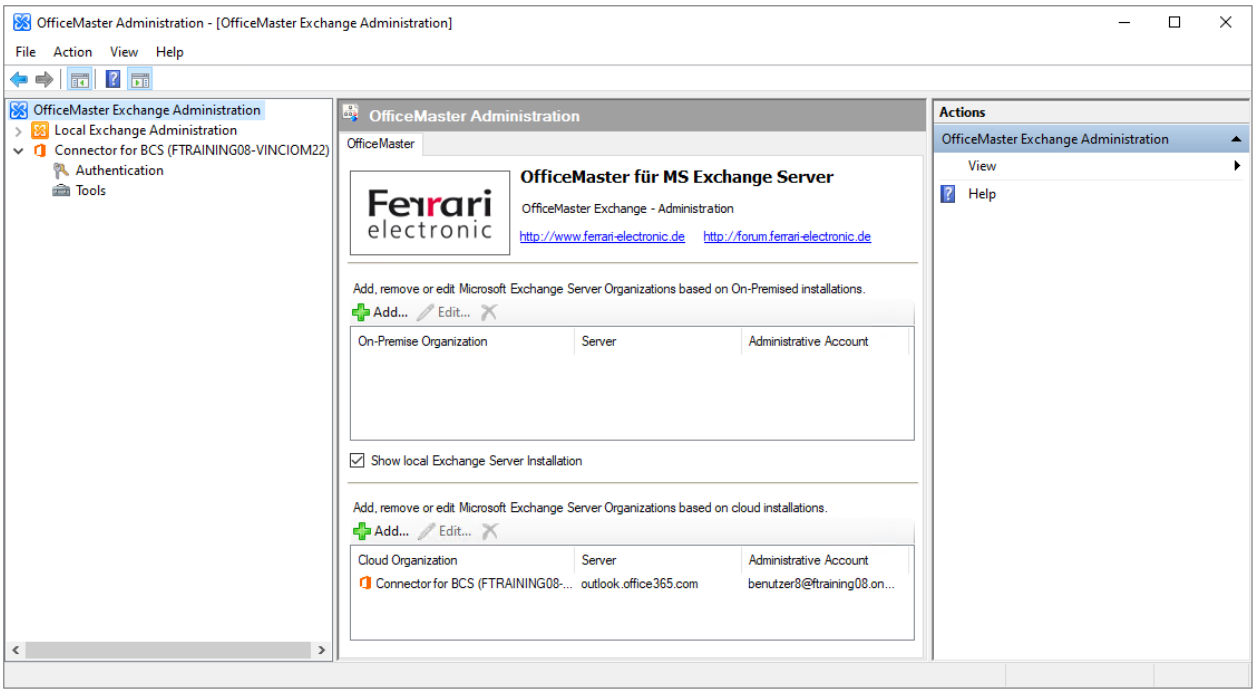
In the next step, login data for logging into an Active Directory can be specified. In a pure Microsoft 365 installation, these fields remain empty.



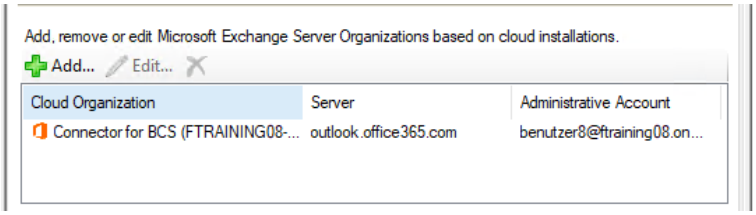


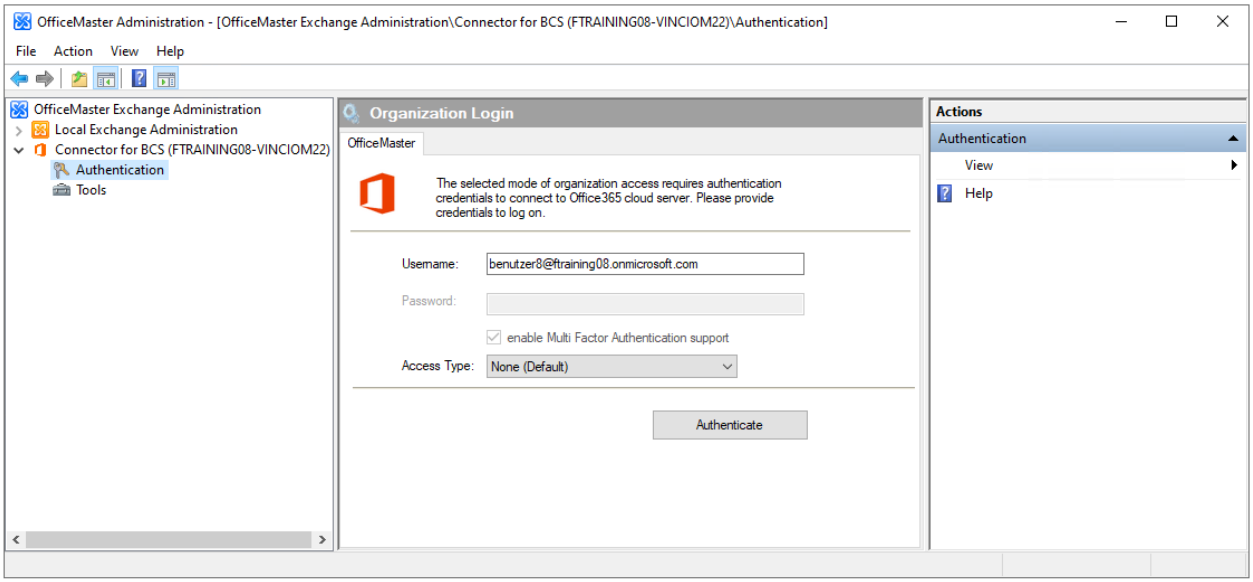
Extended parameters are requested in the last step of the assistant. These should not be changed. The parameters form the basis for the basic connection to Microsoft 365.

After completing the wizard for adding the organization, a new organization is added in the area window (left side). With a click on the node Registration, the corresponding authentication to Microsoft 365 can be carried out.



The added organization can be edited or removed in the Cloud/Microsoft 365 organization area.





Each organization added provides for an interactive registration.

Options

Since the login to Microsoft 365 is done in the background with a Powershell connection, it may be necessary to choose a local proxy configuration. These settings depend on the configuration of the computer environment, and questions about the need for the setting can usually be answered by the responsible administrator. The following selection can be made:

- No proxy configuration (default)
  In this case, no proxy configuration is accessed from a powershell session. This corresponds to the command “new-PsSessionOption -ProxyAccessType None”.

- IEConfig (Internet Explorer proxy configuration)
  The IEConfig setting reads the current user’s proxy configuration that the user made in the Internet Explorer settings. This corresponds to the command:

  ```
  new-PsSessionOption -ProxyAccessType IEConfig
  ```

- WinHttpConfig (WinHttp configuration via ProxyCfg tool)
  The WinHttpConfig setting uses the proxy configuration that the user created using Microsoft’s ProxyCfg.Exe tool. This corresponds to the command:

```
new-PsSessionOption -ProxyAccessType WinHttpConfig
```

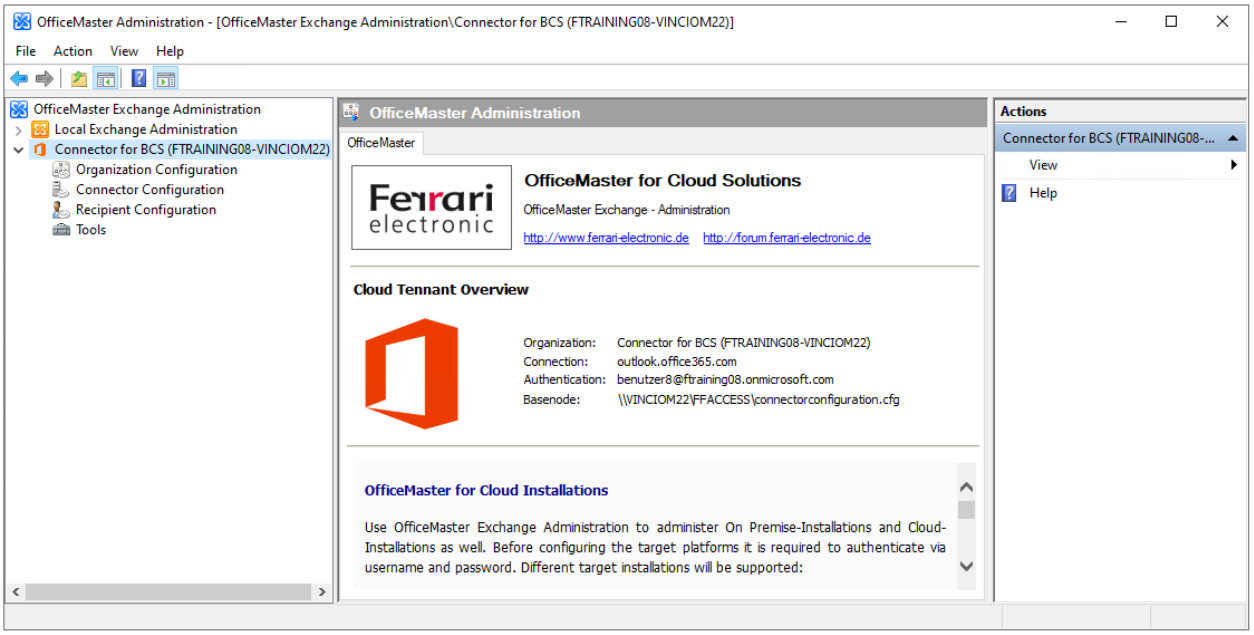
- Automatic proxy configuration
  The automatic determination tries to determine the proxy configuration automatically without further information. This does not always lead to success. This corresponds to the command:

```
new-PsSessionOption -ProxyAccessType AutoDetect
```

- No proxy server
  This option excludes the use of a proxy server and all resolutions are done locally. This corresponds to the command:

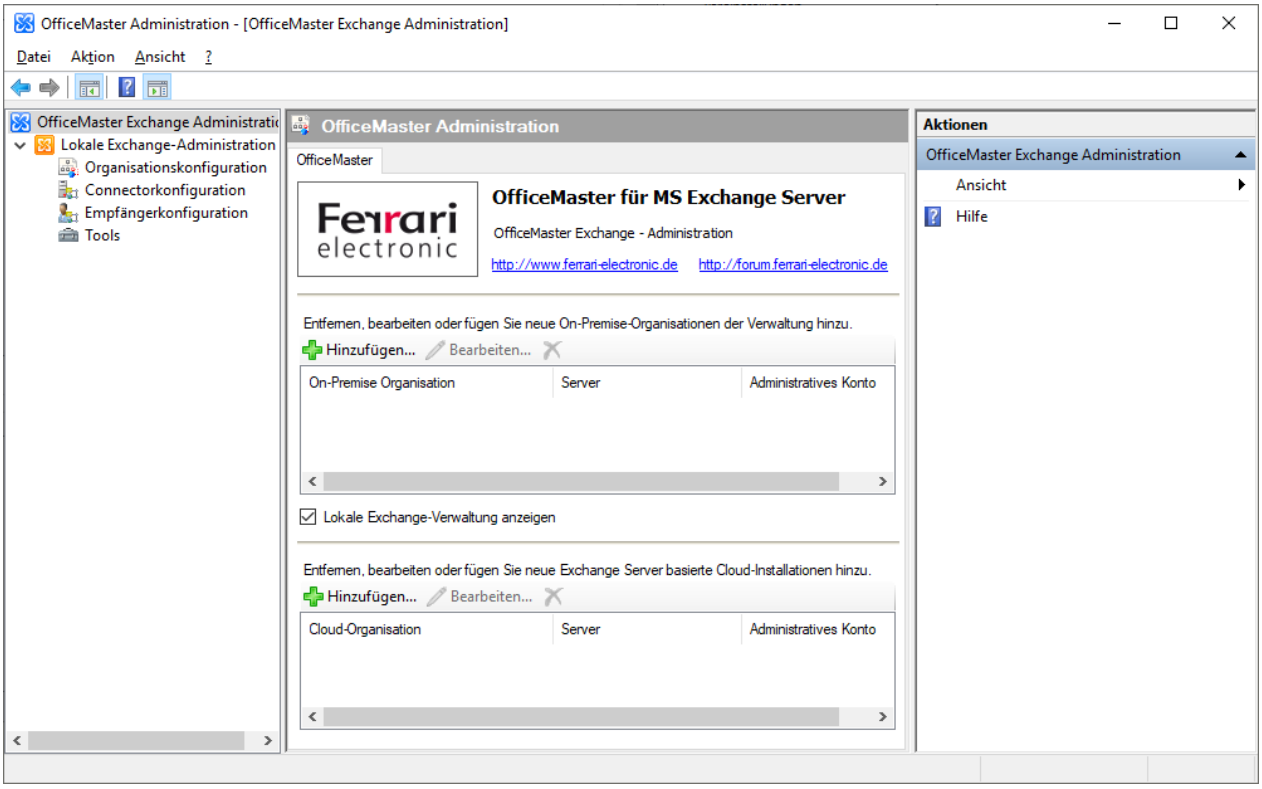
```
new-PsSessionOption -ProxyAccessType NoProxyServer
```

After a successful login, the area nodes for organization configuration, connector configuration and recipient configuration also become available for the cloud installations.



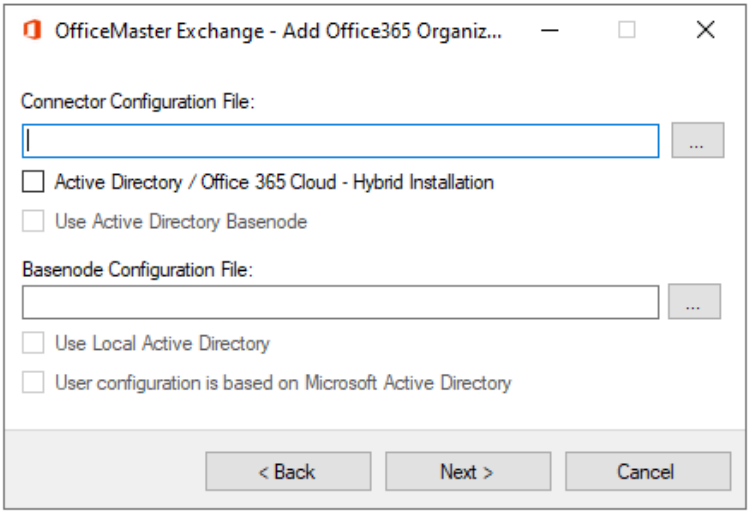
The configuration of the connector and the user can now be made. The added configuration is visible to all user logins on the local computer.

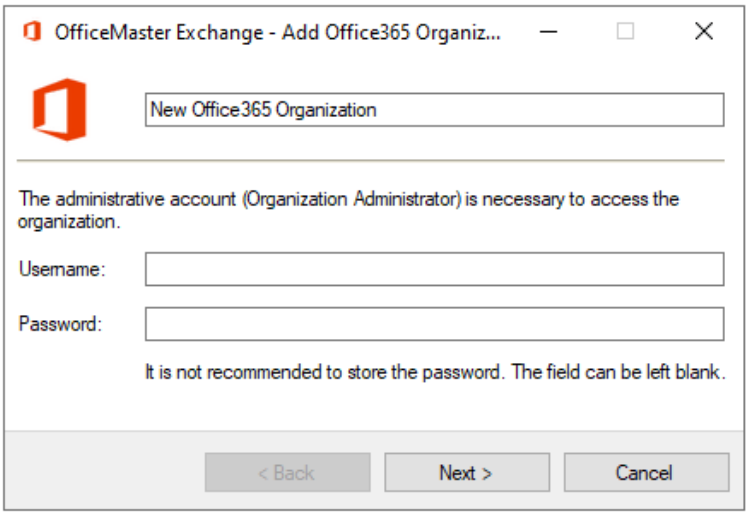
7.5.4. Configuration of a Microsoft 365 on-premises hybrid installation



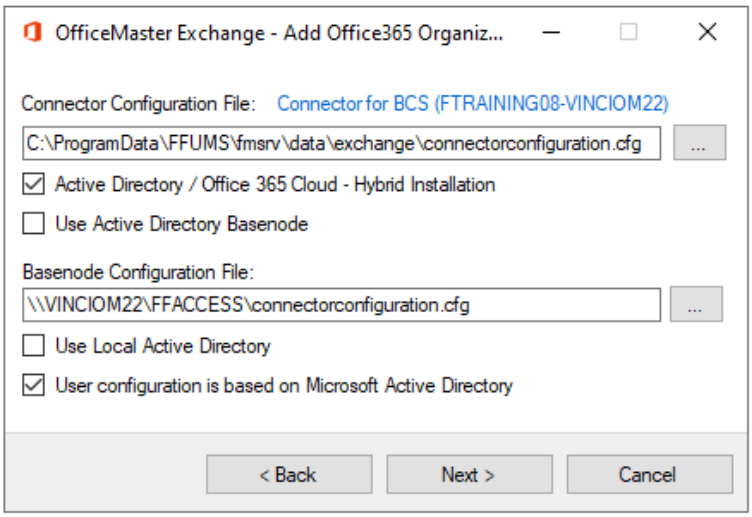
The Microsoft 365 on-premises hybrid installation uses an on-premises Active Directory, but a Microsoft 365 login may be required. This is decided based on the location of the custom properties. The local administration should therefore be switched off with a tick in the local client area. The nodes are then removed from the range window. To then make a configuration, you now add a new organization in the Cloud/Microsoft 365 organization area.

After clicking the “Add” button, a wizard opens with the parameters of the new organization. At this point, an adequate display name for the organization should be assigned. Likeweise, the default user name for access to Microsoft 365 is also stored here. The password can be specified here at this point, but would then be stored in a configuration table. This is a security concern, so it is not recommended. The password field can remain empty. Then follows the possibility to specify the connector configuration file.





After selecting the common connector configuration file that was specified during connector installation, a window opens in which the responsible connector should be selected. Since the file can contain several connectors, the correct connector should be selected here.



After selecting the connector, the configuration dialog should fill in automatically. If necessary, the entered values and checked fields should be checked for correctness.

Connector configuration file

The configuration file that was specified during the connector installation is specified here.

Active Directory / Microsoft 365 Cloud hybrid installation

If this option is enabled, the administration is prepared for access to an Active Directory. This is the default case in a hybrid installation.

OfficeMaster base node is located in Active Directory

At this point it is specified where the global user data is located. When the feature is enabled, the data resides in an Active Directory node. If the option remains inactive, a configuration file that houses the global user data must be specified.

Base node configuration file

If it was specified during the connector installation that the global user data is in a configuration file, then this should be specified here. As a rule, this field will be filled in automatically after selecting the connector configuration file.

Use local credentials for Active Directory access

As a rule, a server and an access account can be specified for access to an Active Directory. However, if this option is enabled, the optional user data are omitted. In this case, the Windows login account is used to access the Active Directory.

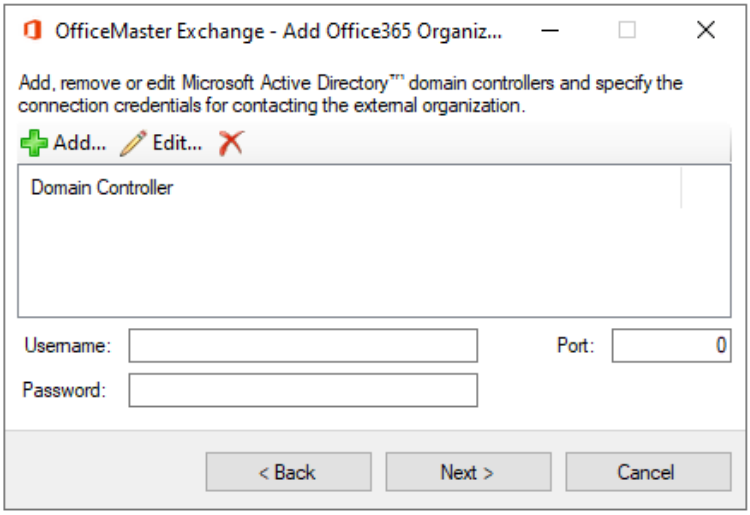
As a rule, this field will be filled in automatically after selecting the connector configuration file.

User configuration based on Active Directory entries

In order to be able to administer the OfficeMaster user properties correctly, the administration must know how the properties are saved. If the option is enabled, the data is read and stored in the user object of the user to be administered in the Active Directory. If the option remains

inactive, the properties are read from the user mailbox and also saved in the user mailbox. As a rule, this field will be filled in automatically after selecting the connector configuration file.

In the next step, login data for logging into an Active Directory can be specified.



List of domain controllers

A list of domain controllers (AD directory service providers) can be stored here for the connection to an Active Directory. Fully qualified domain names, NetBIOS names and also IP addresses can be specified. If this list is left empty, the ADSI (Active Directory Service Interface) tries to automatically determine the next domain controller of the current Windows logon.

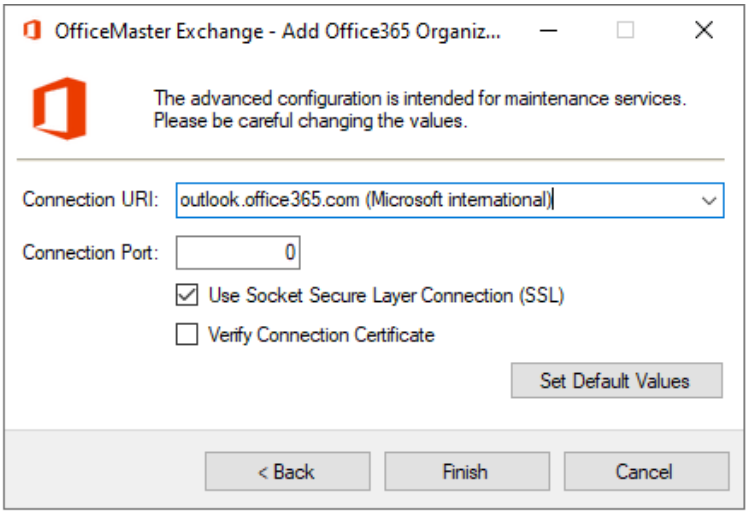
Username and Password

The credentials determine the account to log in with. The user name is specified in the notation DOMAIN\username.

Ports

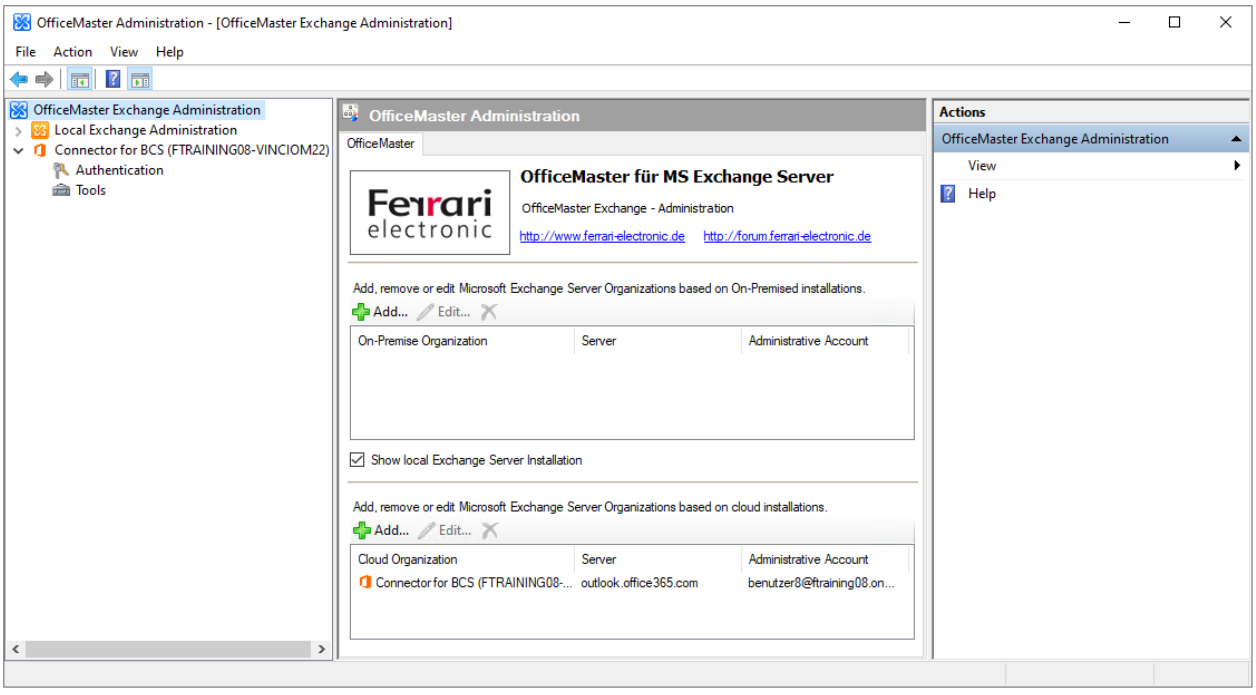
Communication with the Active Directory is usually via encrypted RPC (Remote Procedure Call) mechanisms. However, a dedicated communication port for LDAP (Lightweight Directory Access Protocol Port 389) can also be specified. However, pure communication via LDAP is slower than the standard connection. To use the default connection, the entry can be empty, or a zero can be specified.

Extended parameters are requested in the last step of the assistant.

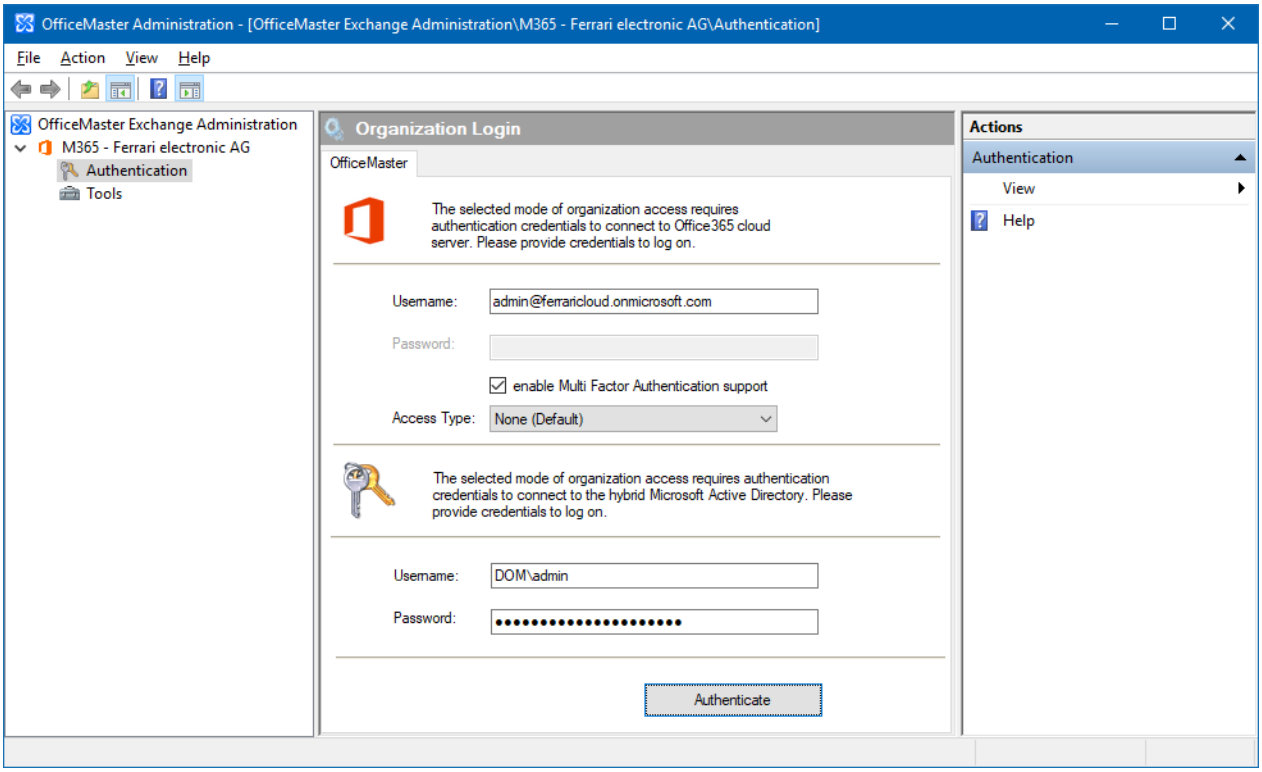


These should not be changed. The parameters form the basis for the basic connection to Microsoft 365.

After completing the wizard for adding the organization, a new organization is added in the area window (left side). With a click on the node Registration, the corresponding authentication to Microsoft 365 can be carried out.

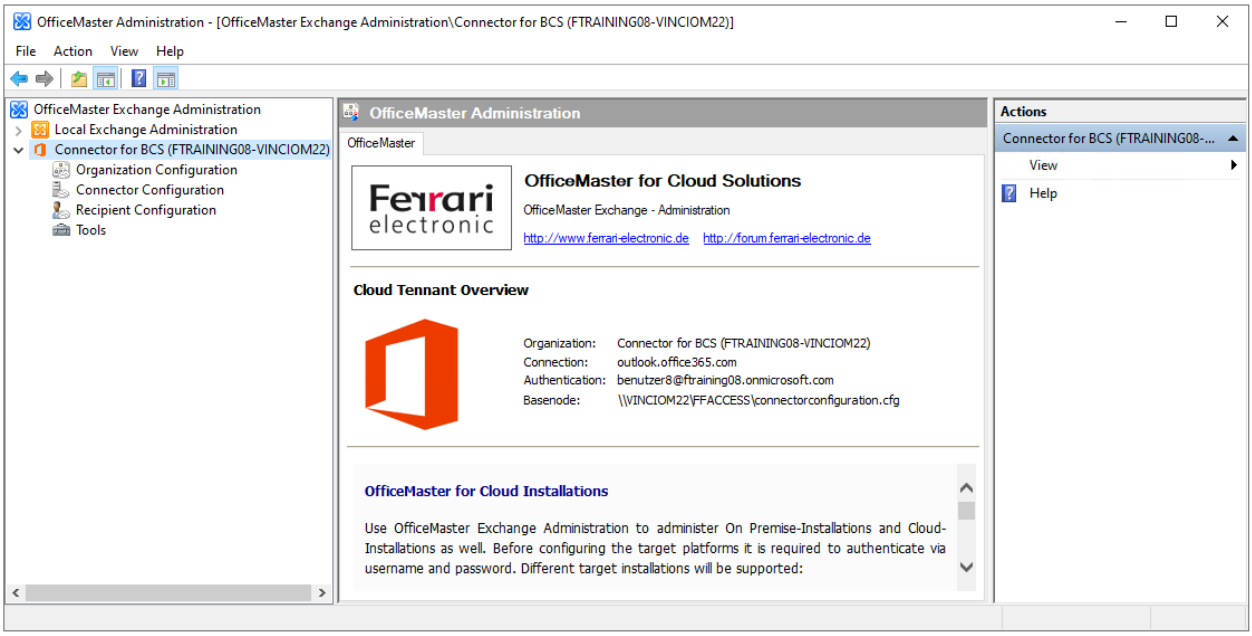


The added organization can be edited or removed in the Cloud/Microsoft 365 organization area.



Each organization added provides for an interactive registration.

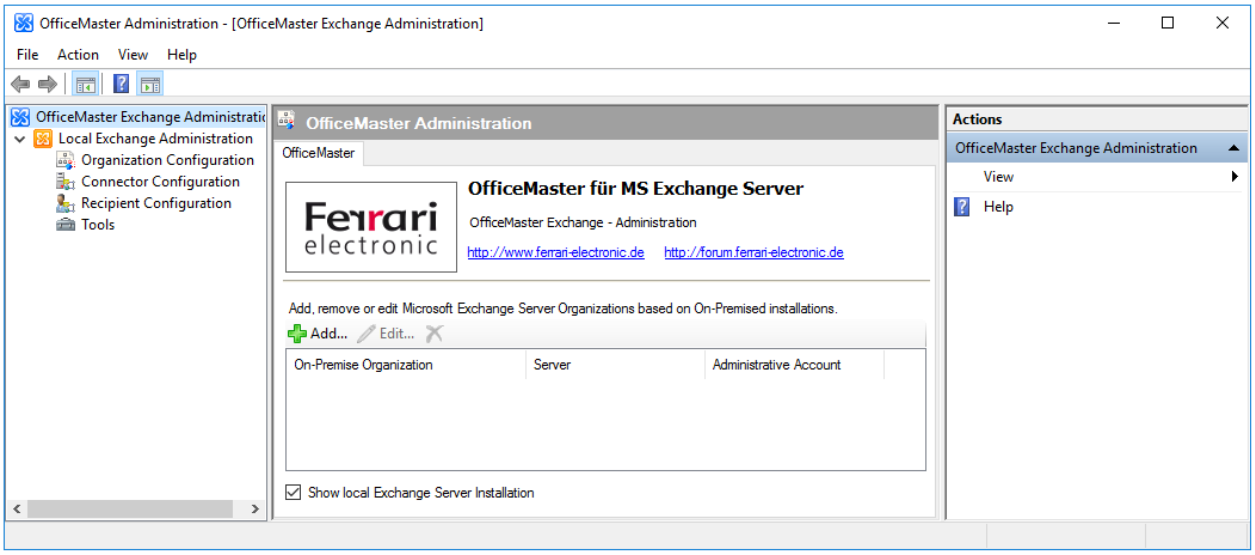
After a successful login, the area nodes for organization configuration, connector configuration and recipient configuration also become available for the cloud installations.



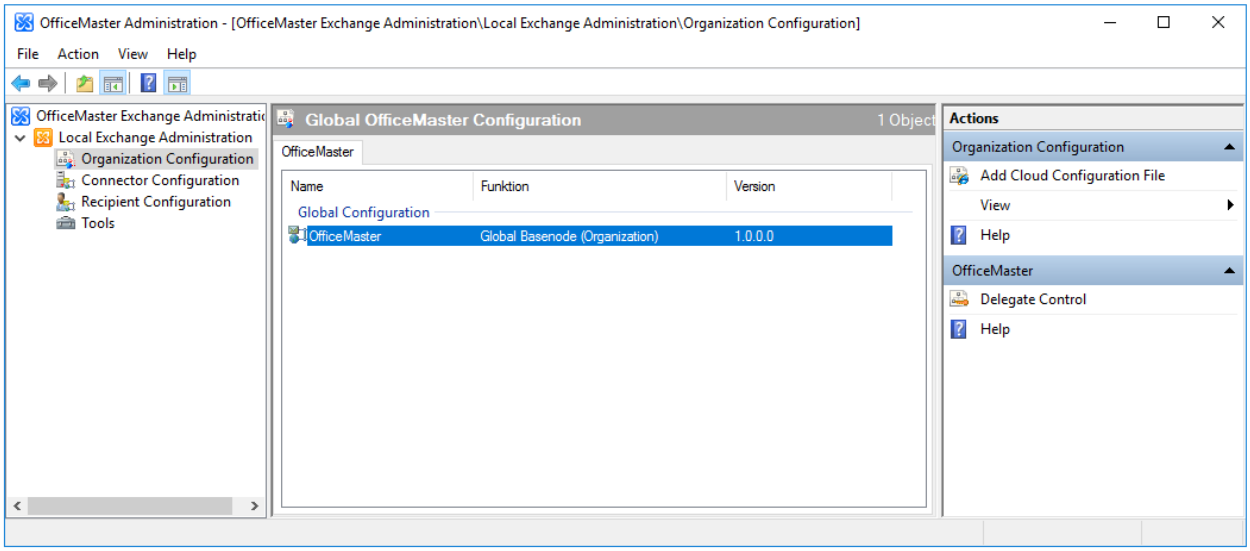
The configuration of the connector and the user can now be made. The added configuration is visible to all user logins on the local computer.

7.5.5. Configuration of a local Exchange Server installation

The support of a local Exchange Server installation with the **msxbcsgate** component represents a special case, since these functionalities are provided with the **msx2kgate** component. If such a constellation should nevertheless exist, this type of installation is configured with the local Exchange Administration. In this case, the Local Exchange Management should remain activated.

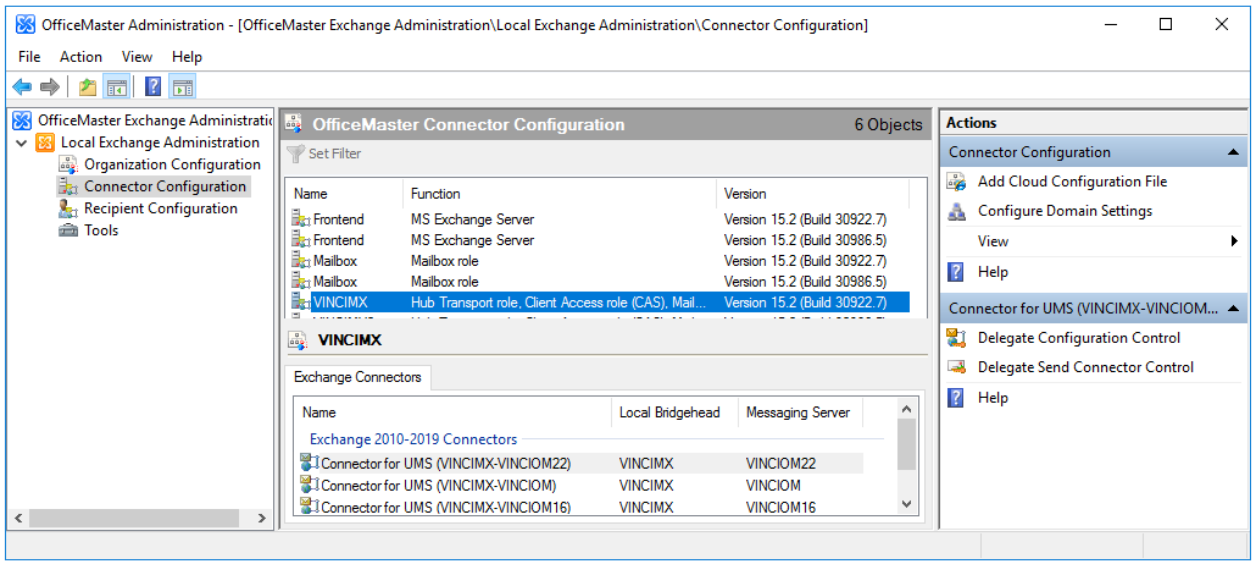


The further management procedure depends on the type of installation. When the connector was installed, it was determined at which point global user data is saved. If this data is stored in Active Directory, nothing needs to be added in the organization configuration. The base nodes in the local Active Directory are automatically displayed. However, if the data is in a configuration file, this must be added to the configuration.



Once added, the global user data can be configured.

In order to configure the properties of the connector (**msxbcsgate** component, “Connector for BCS”), the configuration file of the connector must be added to the connector configuration.



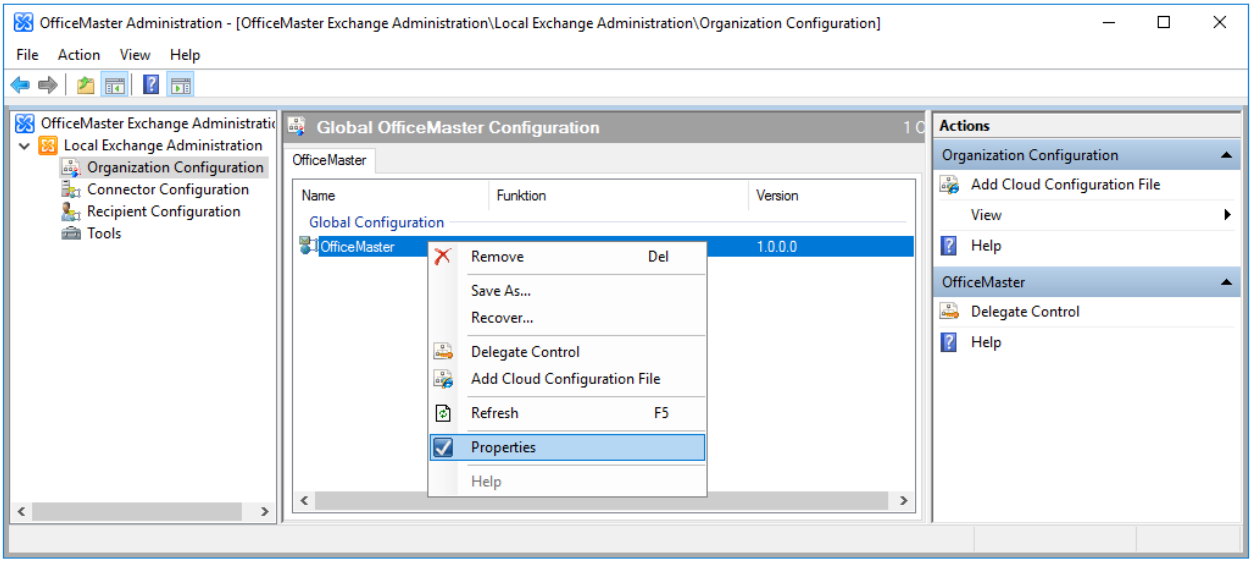
After adding the configuration, the connector appears in the list of Exchange connectors. The properties can now be configured.

Configuration files added in the local Exchange configuration are only visible to the logged in user.

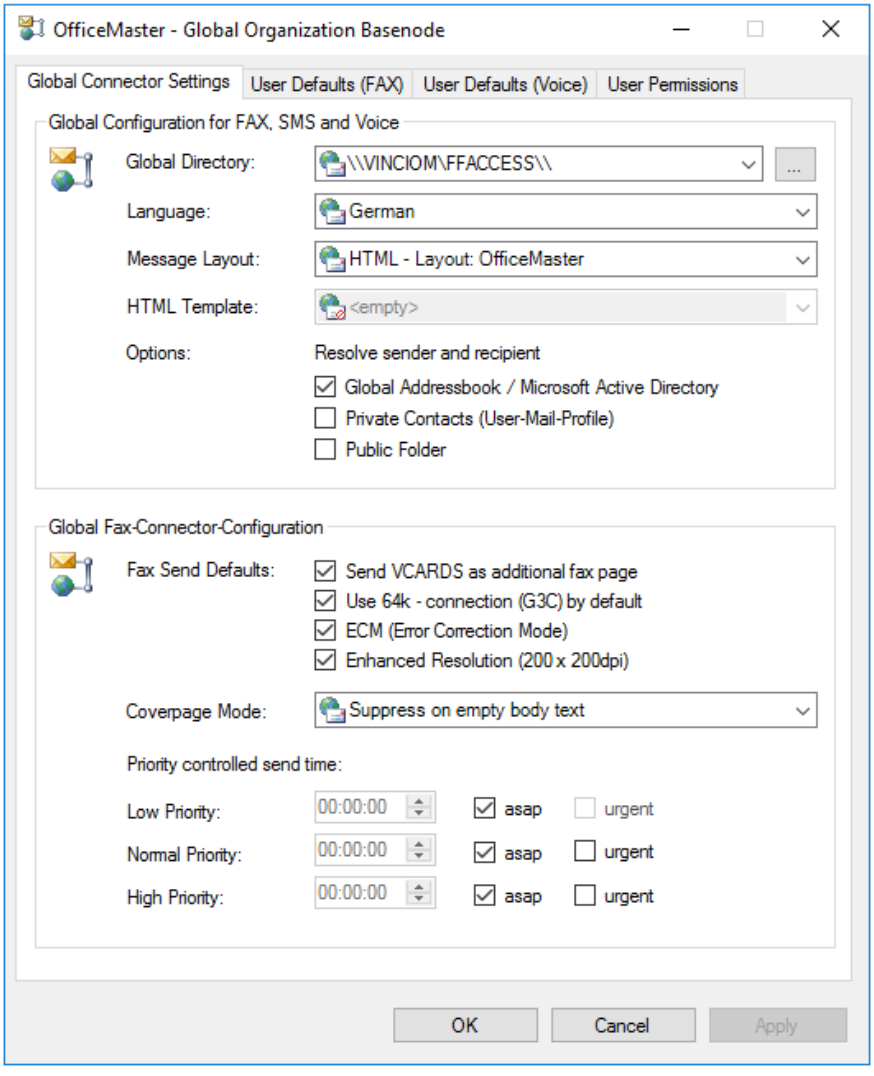
Nothing needs to be done in the user properties node. The user objects are displayed automatically and can be administered immediately.

7.5.6. Configuration of global user data

The global user data is administered in the organization configuration in the properties of the base node.



General settings



At this point, a global general setting can be made, to which all OfficeMaster Exchange connectors in the organization are based.

Global directory (for cover sheets etc.)

For storing cover sheets, signature files, stationery files and caller images, a global directory must be specified here as a UNC path that corresponds to the structure of the FFACCESS share. This means that at this point, the connectors expect subdirectories with the names COVER (cover sheets), LETTER (letterhead files), SIGN (signatures) and PICTURE (caller pictures). Administration of these directories only makes sense if there are several OfficeMaster connectors in an organization. During the installation, this directory may be changed. The administrator has the option of specifying a base directory in coordination with the operators of the other connectors. If the saved global settings in the local domain object option is selected during installation, each location will have its own global directory.

Language

Here you can set whether the notifications that the connectors send to the users should be generated in German, English, French or Spanish. This setting can be changed for each individual user in the receiver-specific settings.

Message format

The OfficeMaster connectors are able to generate the feedback as well as the incoming documents in various graphic adaptations. You can choose between the following internal options:

Text only

The documents are generated as an e-mail in text format. This setting offers the greatest compatibility with all user programs that can be connected to the Exchange Server.

HTML layout neutral, OfficeMaster and Outlook

The HTML layouts are graphical message formats. The message is generated as an HTML message and, in the case of fax documents, contains the first page of the attached documents as a preview.

Since replies contain the converted attachment files individually, the first page of each attachment object is displayed directly in the message. The format of the included preview graphic (PNG) is independent of the selected format of the actual attachment files. The three selectable internal layouts contain different colored designs. It is up to the administrator to select the layout. The OfficeMaster layout is set by default.

HTML template

In addition to the internally implemented HTML format templates, special external format templates can be loaded for further adjustments. These are generated in a special HTML/XML variation and can be stored in the global cover directory alongside the normal RTF cover sheets. These special template files (*.HTL) store complete language sets of HTML templates and can thus have a lasting effect on the appearance of the incoming documents and, if necessary, be adapted to the corporate design of your own company. The HTL editor program and documentation for the HTL script language can be found in the directory <SERVER>\FFACCESS\Redist\Tools.

Determine sender and recipient information

The connectors can resolve incoming and outgoing phone numbers into name information. You can specify here which databases should be searched by default.

Global Address Book / Microsoft Active Directory**

If this option is enabled, incoming phone numbers and outgoing cover sheet information are determined from Active Directory user data or Active Directory contact data. This option actually only ensures that internal phone numbers are resolved, since contact data is generally not stored in the Active Directory.

Private Contacts (User Email Profile)

“Private contacts” means contact information that is stored in the sender’s mail profile or, in the case of incoming documents, in the recipient. These are not private folder files (PST files) that have been included in the mail profile. Only the contact folders of the e-mail profile are meant here. It should be noted that this function can only be used successfully if the connector component’s service account has appropriate read rights to the corresponding user’s mailbox store.

Public Folders

The address book resolutions of the connectors generally relate to cover sheet fields and information of the senders of incoming and outgoing documents or messages. Since most information from such senders is not stored as Active Directory contacts, but is available as contact items in public folders, such an item can be used as a data source if this function is activated. The first contact element found applies. Duplicates are delimited by the display name. However, since no further information can be used to find the data, duplicates are not recognized as errors. The first entry found is used here.

> Note!
>
> The specified searches in private contacts and public folders refer to real-time searches with these settings. Such search processes can take considerable time. As an alternative, the metacache database is available to the connectors, which works independently of these settings.

Shipping specifications

Send business cards (VCARDS) as an additional fax page

In Microsoft® Outlook it can be set individually whether the Outlook electronic business card is also sent. This usual option for e-mails can also be used when sending faxes. When this option is activated, the business card is also converted into the fax as a separate page.

Require connection at 64 kbits/s by default

The OfficeMaster Card supports the fax protocol standard G3C, which allows transmission at 64 kbit/s on ISDN lines within the framework of fax group 3. In this case, when using the OfficeMaster Card, an attempt is first made to establish a 64 kbit connection to the remote station and to transmit the fax or file at this speed. If this is successful, significant time and cost savings become effective. If this attempt fails because the remote station does not have the corresponding function, a connection must be established again using the standard speeds. Additional time is required due to the double selection. If the option has been activated, the individual user has the option of deactivating it for his shipping order as part of the shipping options.

Use ECM (Error Correction Mode).

With this option it is determined that the transmission of a fax or a file should take place using the error correction option if the remote station supports this function. This allows error-free transmission of the data even with low quality phone lines. The erroneous data block is recognized and repeated. It is recommended enable the ECM function globally, as it can be switched off by the users for each job.

Use fine resolution (200 x 200 dpi).

If this option is deactivated, all faxes are transmitted with standard resolution (200 dpi horizontal, 100 dpi vertical). Compared to fine resolution (200x200 dpi), this saves considerable transmission time and costs. The individual user has the option of individually specifying the resolution for his shipping order within the scope of the shipping options.

Cover mode

By default, a cover sheet can be added to a message sent as a fax via Microsoft® Exchange. The cover sheet or the introductory text can be influenced with the selection field.

Never suppress cover sheet

This option ensures that a cover sheet (if set up) is always sent.

Suppress cover page if message is empty

If the actual message does not contain any text, but only a file attachment, the cover sheet can be suppressed with this option. If the Subject: field contains data, it will be ignored. Use should be made of this if the file attachment itself contains relevant information, e.g. a cover sheet created in a text program.

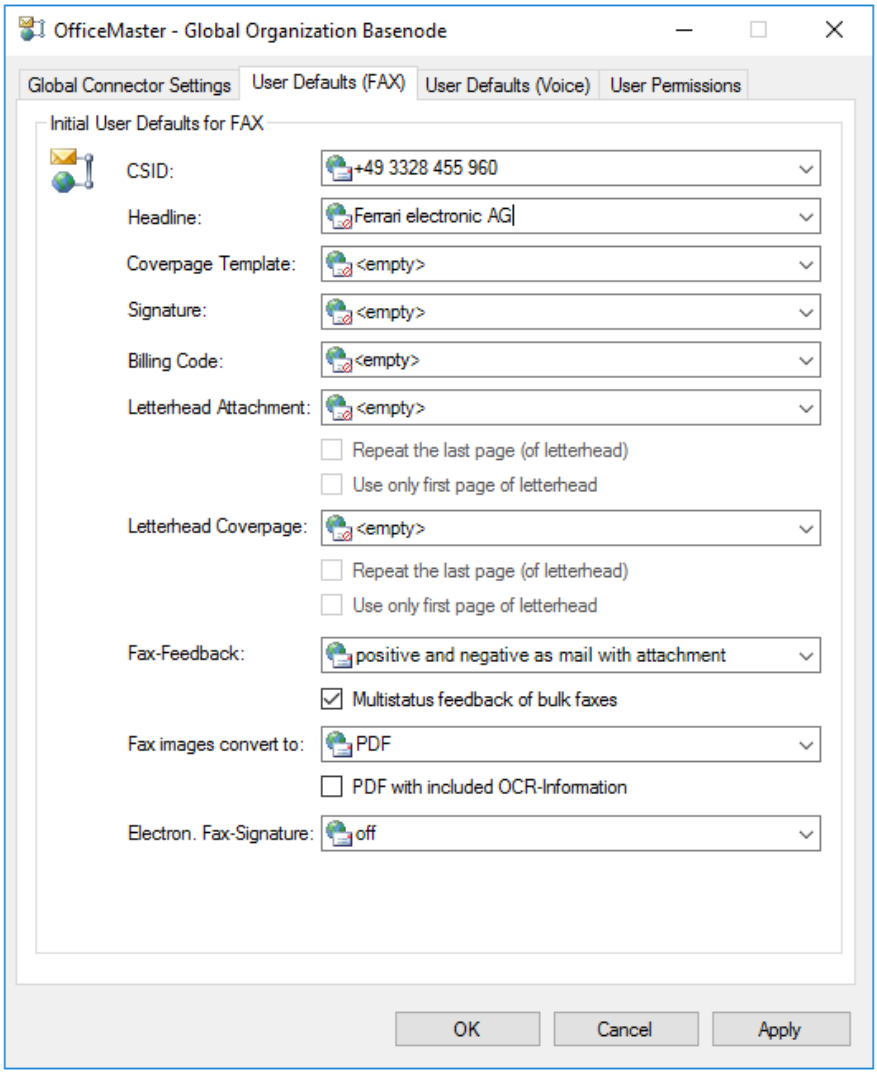
Suppress cover page if message and subject field are empty

This option suppresses a cover page only if both the message and the subject field are blank. It should therefore be used if a cover sheet is to be generated in any case if the subject field has been filled out, as this is typically also integrated into the cover sheet.

Time and Urgency Control (Send by Email Priority)

With these options, the sending times of fax and SMS documents can be set based on the e-mail priority. The “prioritized” option can be used to specify whether the documents in the sending messaging server are also treated with priority within the queues. The “prioritized” option should only be used with high e-mail priority, since it influences the classification of the documents in the server queue.

User preferences (Fax)



A user default can be created here as a global setting, which is automatically assigned to all users of the organization who are not individually administered. This tab corresponds to the user administration settings.

Identifier

The fax identifier that appears in the header of a sent fax can be set here globally for the users of the organization. According to the international standard, the information should be given in the form +country code area code (without the leading 0) phone number extension number.

```
Example: +49 3328 455 960
```

By specifying the identifier individually, the sender's fax number, including extension number, is transmitted correctly, so that corresponding reply faxes can be addressed directly to him. If the specification is omitted, the data that was specified when setting up the messaging server is used.

Header

In this line, a header text can be entered globally for the users of the organization. This can, for example, be the company name supplemented by the respective department name.

Cover sheet

A cover sheet can be activated at this point. This cover sheet is an RTF file whose name is entered in the associated field. Cover sheets are stored in the Cover subdirectory, which is automatically created during installation. The default setting for the cover page is inactive. If a cover sheet has been activated, this applies to all faxes that are sent via the connectors of this organization, unless the respective user has the right to switch off the centrally specified cover sheet or to replace it with their own.

> Note!
>
> If Microsoft® Word was used to create a cover sheet, it is strongly recommended to also use Microsoft® Word for the central conversion of the message. As it creates RTF files that are used by the internal RTF converter available in Microsoft® Exchange and are generally not correctly interpreted by Quick View Plus. This is especially true when using more complex formats such as tables and frames in Microsoft® Word.

Signature

The name of a signature file can be specified at this point. The default setting is inactive. The names of all signature files saved in the SIGN subdirectory are displayed. It is also possible to

enter another name. In this case, however, it must be ensured that a corresponding cover sheet file is saved in the SIGN subdirectory before the system is used.

Note!

It is the administrator's responsibility to correctly assign the signature file to the individual users. The signature file must be of type RTF so that it can be integrated into the Microsoft® Exchange message at the right place. It is created by scanning a signature, storing it in a graphic file, e.g. of the PCX type, and then importing this file into an RTF file as an object. The internal converter cannot convert objects into RTF files, so Microsoft® Word or alternatives must be set as converter in this case.

Cost centre

The specification of the cost center refers to an entry in the log file generated by the messaging server. The specification at this point only makes sense if users do not have any cost center information and the value should be set to the set value here. A cost center is an identifier with a maximum of 12 characters that uniquely identifies the user in the log file.

Stationery Attachment

The default setting for this field is standard, i.e. the stationery for attachments centrally set for the fax connector is used for the user. However, he can set a different stationery. The names of all letterhead files stored in the LETTER subdirectory are displayed in the combo box. A new name can be entered if it is ensured that a corresponding letterhead file is saved in the LETTER subdirectory before the system is put into operation. The use of the stationery file for multi-page documents is controlled by the checkboxes:

a) Repeat stationery (last page) b) only use the first page of the stationery

There are four possible combinations of options:

1. Both settings off (default setting)
   Each page of the letterhead is superimposed on the corresponding page of the cover sheet or message. If the cover sheet or message has more pages than the stationery, no deposit is made for the pages of the cover sheet or message for which there is no stationery.
2. Repeat stationery (last page)
   Each page of the letterhead is superimposed on the corresponding page of the cover sheet or message. If the cover sheet or message has more pages than the stationery, the last page of the stationery is deposited for the pages of the cover sheet or message for which there is no stationery.

3. Use only the first page of the stationery
   Only the first page of the stationery is used; it is stored on the first page of the cover sheet or message. Any subsequent pages of the stationery are not used. All subsequent pages of the cover sheet or message are not deposited.
4. Repeat stationery (last page), only use the first page of stationery
   Only the first page of the stationery is used. This page is deposited on all pages of the cover sheet or message.

Feedback

Each user who sends a fax can receive a corresponding response as a reaction to the fax being sent. This feedback can be configured differently according to the possibilities of the Exchange Server. The feedback provides information as to whether the dispatch could be completed successfully or not. If a non-delivery notification is requested, the sender receives a non-delivery notification (Non Delivery Report, NDR) in the event that the fax could not be sent successfully, which on the one hand describes the cause of the error and on the other hand allows the fax number to be changed and the process to be repeated.

Positive and negative as mail

Positive and negative feedback is sent to the sender's mailbox as an email without a converted fax.

Positive as mail, negative as NDR

The positive feedback is sent to the mailbox as an email, while the negative feedback is generated as a non-delivery message (NDR - Non Delivery Report). The non-delivery report has the advantage that you can easily resend the message with a special button.

Only in the negative case, as mail

The feedback will only be sent to the mailbox as an information e-mail if it is negative.

Only in the negative case, as NDR

A response in the form of an NDR is only generated in the event of transmission errors.

Positive and negative as mail with attachment

In the positive and negative feedback, the fax is included here as a converted attachment for viewing.

Positive as mail with attachment, negative as NDR

Positive replies are sent as an email with a converted fax, while negative replies are sent to the mailbox as an undeliverable message.

Only in the negative case, as mail with attachment (recommended)

Normally, after a fax has been sent, the fax connector sends a message to the user informing them whether the fax was sent successfully or not. In the case of serial faxes in particular, it does not make sense to also acknowledge all successful fax transmissions with a message. With the activation of this option, acknowledgment messages are only generated in the case of incorrect sending.

As an additional option, it can be specified that broadcast faxes (outgoing fax documents with the same content to several recipients) are only reported with one collective confirmation for all documents sent without errors and for all documents sent with errors instead of one confirmation for each outgoing fax. This option does not apply to form letters, which must be treated as individual orders. A summary of the feedback is not possible for serial letters.

File format

The standard format in which incoming fax documents are delivered as attachments is TIFF/G4. However, the formats displayed in the list can also be selected. Which format should be used for the attachments depends on which image program is to be used to display the faxes.

As an additional option, it can be specified here that an additional searchable document in PDF format is attached to the incoming document if the text recognition function is activated on the messaging server.

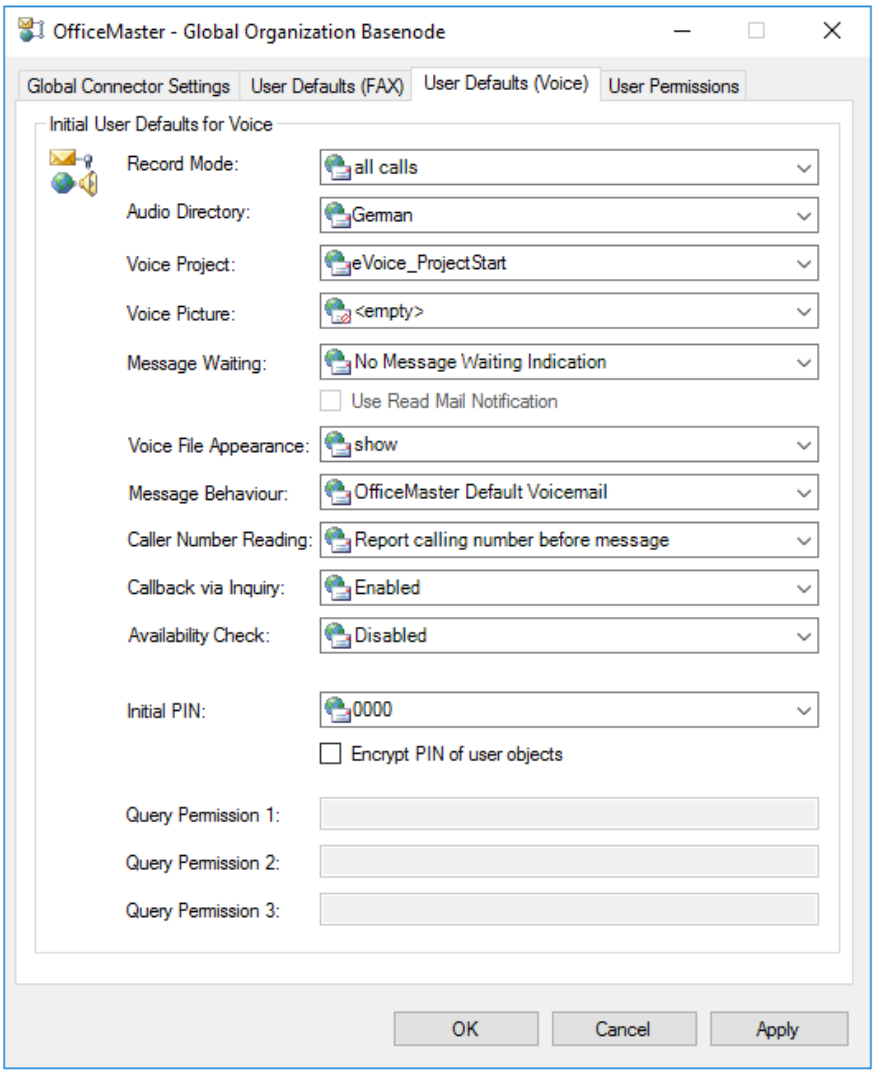
Electronic fax signature

At this point it can be specified whether outgoing fax documents should be provided with a qualified electronic signature. Setting this signature requires that the responsible OfficeMaster Exchange Connectors have configured a corresponding signature component. Since such

signatures are usually only used by individuals, they should not be activated at this point, but in the respective user settings.

User preferences (Voice)

A user specification can be created here as a global setting for the voice services, which is automatically assigned to all users of the organization who are not individually administered.



Recording

The recording mode distinguishes between the delivery of pure voice messages with a file attachment (“Voice Messages Only”) and the additional delivery of a notification of the mere call without a file attachment (“All Calls”), since the caller did not leave a message.

Language directory

The language directory designates the language tree of the messaging server. Every messaging server with an installed voice tree contains audio directories in which the voice-related announcements have been stored. At the time this document went to print, you could choose between “de” (German) and “en” (English).

Voice project

In this field the voice project of the voice server to be used is specified. The voice project determines the behavior of the voice server for incoming messages.

Caller picture

The caller picture shows a default picture if no picture was assigned to the user or the incoming caller could not be resolved. This image is a stored graphic file (PNG or JPG) that must be located in the global “PICTURE” directory. The graphic should not exceed 160 x 180 pixels (width x height).

Message waiting

The “message waiting” behavior determines the turning off of a message waiting lamp on the user’s phone. Switching on the lamp is largely determined by the messaging server configuration and the corresponding control of the message waiting function in the PBX. Shutdown supports three modes:

- Reset by general remote inquiry
- Reset by listening to at least one message
- Reset by listening to all messages

Show audio file

In the selection field you can specify whether the voice message file (WAV or MP3) is to be displayed or suppressed in the message. Suppressing it would have the effect that the file can no longer be played back over the PC speaker, but only over a remote query.

Initial PIN

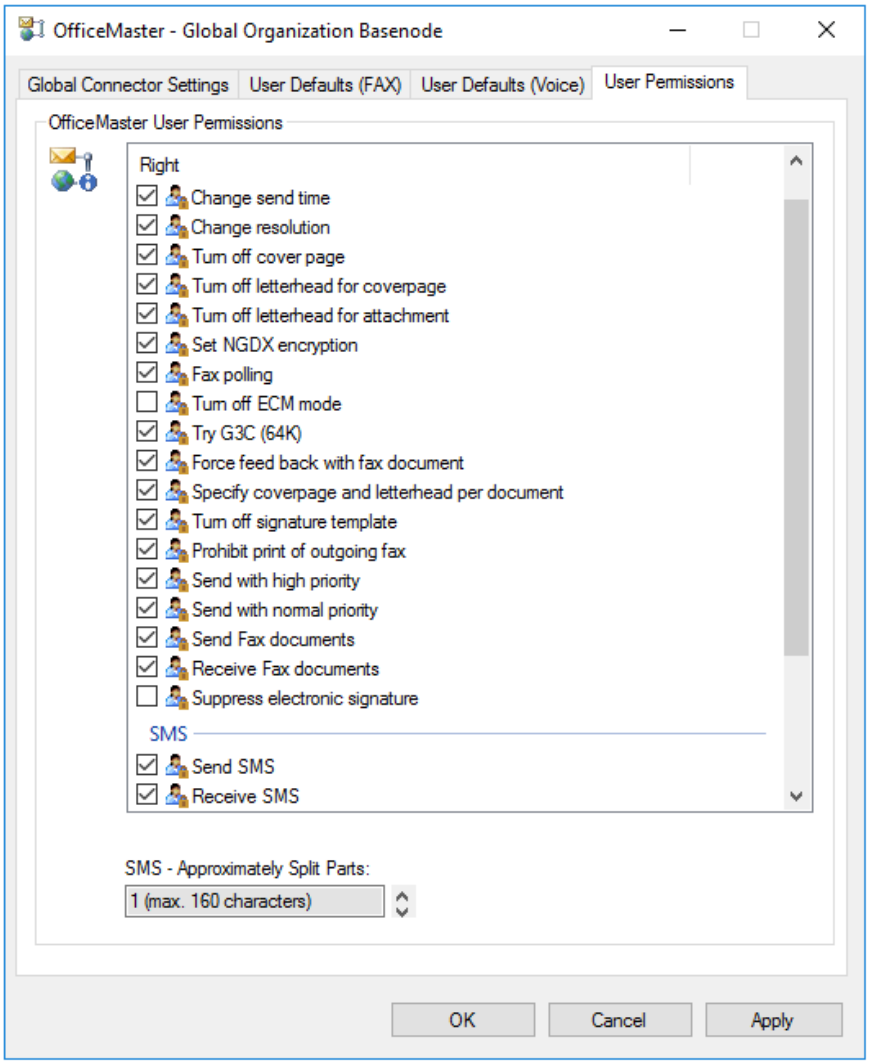
Each user who has not been administered directly uses this information from the initial PIN. When remotely querying a user's voice box, it makes sense to store a PIN. The initial PIN can be stored here in order to initially adapt the function sequence to the actual behavior. **If the voice server settings are also to affect the Exchange connectors, this entry must be administered here <empty>.**

Query permission 1-3

Telephone numbers can be specified here, which immediately put the called voice box into configuration mode when there are calls from these devices. The query permission is only implemented for the sake of completeness. This feature should only be used for selected phone numbers.

User Rights

The administrator can set a large number of authorizations for the individual users of the OfficeMaster Exchange connectors. All users are automatically assigned these displayed rights as a central default, as long as no other rights have been set individually for the user. The User Rights window contains all rights that can be assigned to a user by activating the corresponding check box. The individual rights have the following meaning:



Change transmission time

With this authorization, the user is able to specify the date and time for the sending time. If the option is activated, this information has priority over the priority selection high, medium or low. If only a time without a date is specified, it refers to today's date if the time has not already passed, otherwise to the following day.

Change resolution

With this permission, the user can choose between fine resolution and standard resolution when sending faxes. It's a good idea to let the administrator set the default resolution to keep transmission times and costs low. In special cases, the quality of the resolution can be set individually.

Turn off cover sheet

In the central administration, either a standard cover sheet for all users or a cover sheet for an individual user can be specified. With this option, the currently selected cover sheet can be suppressed by the user, e.g. if the document to be sent is created in a text program and already provided with its own cover sheet there. Cover sheets cause additional transmission times and costs.

Switch off stationery for the cover sheet

If the use of stationery for cover sheets has been set in the central administration, this option authorizes the user to suppress the deposit of stationery.

Turn off stationery for attachments

If the use of stationery for attachments has been set in the central administration, this option authorizes the user to suppress the deposit of stationery.

Set NGDX encryption

When sending a fax, this option enables the NGDX encryption parameters to be set via the Outlook send options.

Fax retrieval

This option gives the user the opportunity to use fax on-demand services like those offered by OfficeMaster. The fax number entered as the fax address is called and the fax protocol signals to the remote station that a fax document prepared for retrieval is to be transmitted. The user receives this document in the same way as a received fax.

Turn off ECM

This permission allows the user to suppress the recommended default transmission with error correction. The OfficeMaster hardware is one of the fax cards that support transmission in Error Correction Mode. It is strongly recommended to make use of this option. ECM is automatically suppressed when communicating with remote fax machines that do not have ECM. ECM ensures that faxes are transmitted error-free by repeating any transmission blocks that encounter errors. If the line quality is poor, this can lead to a slight increase in the transmission time. ECM

should only be suppressed if extremely long transmission times result from very poor transmission lines and if transmission errors can be tolerated.

Request feedback with fax document

When sending a fax, it can be set so that the user receives a response stating whether his fax could be sent without errors. With the above option, the user has the option of receiving the actual fax as an attachment in the form of a graphic file in addition to the status information. This option is always useful when the user has triggered several send requests and cannot assign the confirmations without further ado, but can only identify them using the original fax.

Specify cover sheet/letterhead per job

With this option, the administrator authorizes the user to use customized cover sheets and stationery graphics. By entering a name, he can select a cover sheet and/or stationery to be used for the fax to be sent. It is assumed that a corresponding cover sheet is stored in the installation share “<Messaging Server>\FFACCESS\Cover”.

Deselect signature

Via the central administration, it can be specified for a user that under his messages a signature (stored in a file in the installation share “<Messaging Server>\FFACCESS\Sign”) appears. This option authorizes the user to suppress the insertion of a default signature.

Prohibit printing of outgoing fax

The administrator can specify that all sent faxes are automatically printed out on a selectable printer. If the option is activated, the user can suppress the printout.

Send with high priority

The standard sending options include being able to set the priority for sending a message to high, medium and low levels. Since a fax with high priority is transmitted immediately after it has been ordered, considerable transmission costs can arise with longer faxes. It can therefore make sense to only allow users priority levels that are always cost-effective. This option allows the user to use the highest priority level.

Send with medium priority

Since the transmission of a medium-priority fax does not occur at the most cost-effective time, it may make sense to only allow users the low priority level, which is always cost-effective. This allows the user to use the medium priority level.

Send fax

This setting can be used to determine whether a Microsoft® Exchange user is allowed to send faxes.

Fax reception

Here the administrator can specify that a user may not receive any faxes directly. The faxes are forwarded to the mailbox of the default recipient, who can then decide whether to forward a fax that has arrived for the blocked user to this user.

Switch off electronic signature

The user has the option of switching off the electronic fax signature with a send option.

Sending SMS

With an installed SMS connector, the general SMS dispatch can be allowed with this option. Users who send an SMS without permission will receive an error message.

SMS reception

The SMS connector can also receive corresponding SMS messages. This reception can be switched off with this setting. The messages are forwarded to the mailbox of the default recipient, who can then decide whether to forward an SMS message that has arrived for the blocked user to them.

SMS sending of split SMS

If the SMS dispatch is generally allowed, SMS messages can also be sent with an excess length. Such messages are then divided into several messages with a maximum length of 160

characters and sent one after the other. Since this option can become correspondingly expensive, it is not activated by default.

Activate CTI

The CTI functionality is outdated and is no longer supported by OfficeMaster Server Version 5 or higher.

Voice administration

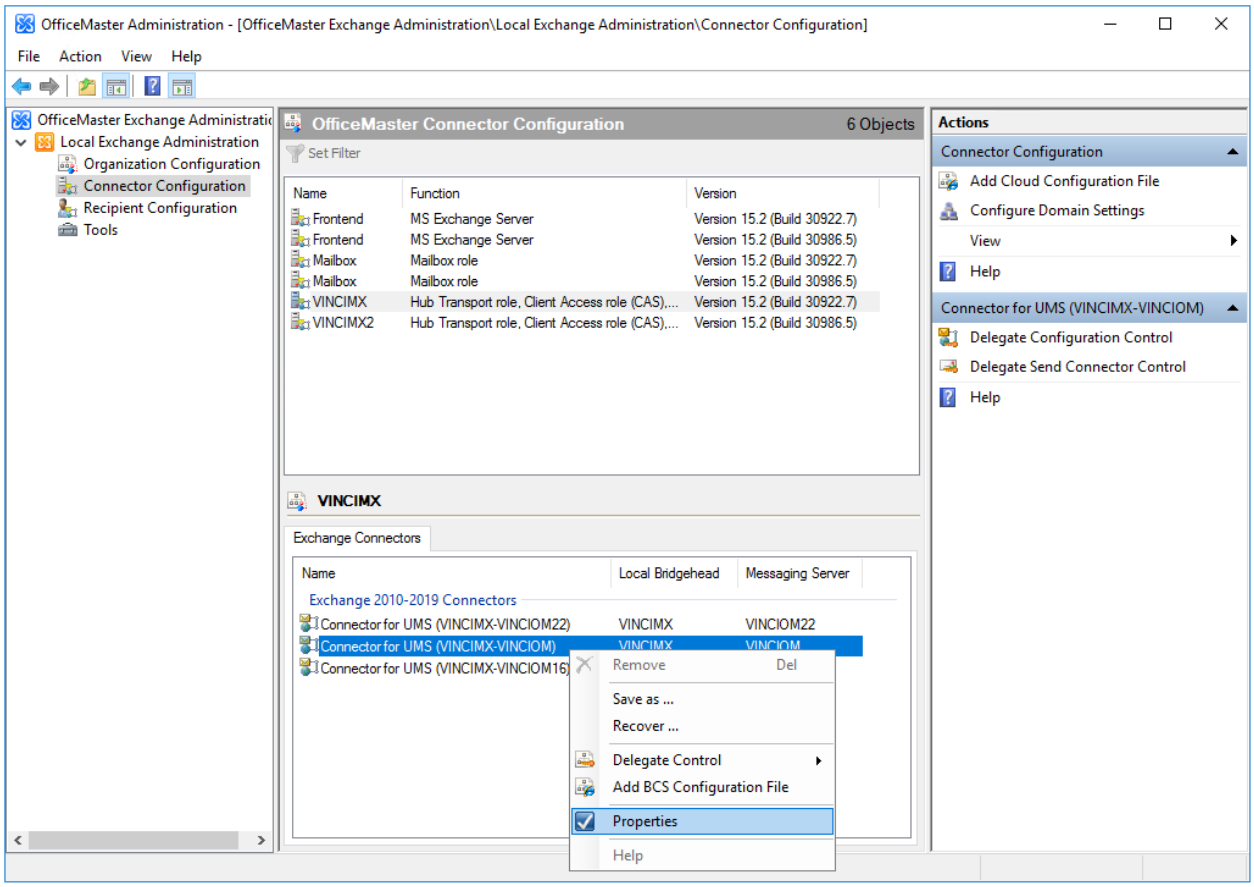
The CTI functionality also includes a call monitor, in which the telephone status of other participants can be displayed. The right to display can be configured here.

Maximum number of split SMS

The maximum number of SMS messages into which overly long SMS texts can be divided can be specified for sending SMS. If this maximum is reached, the message is truncated at this point. Overlong documents can be divided into a maximum of 99 SMS messages.

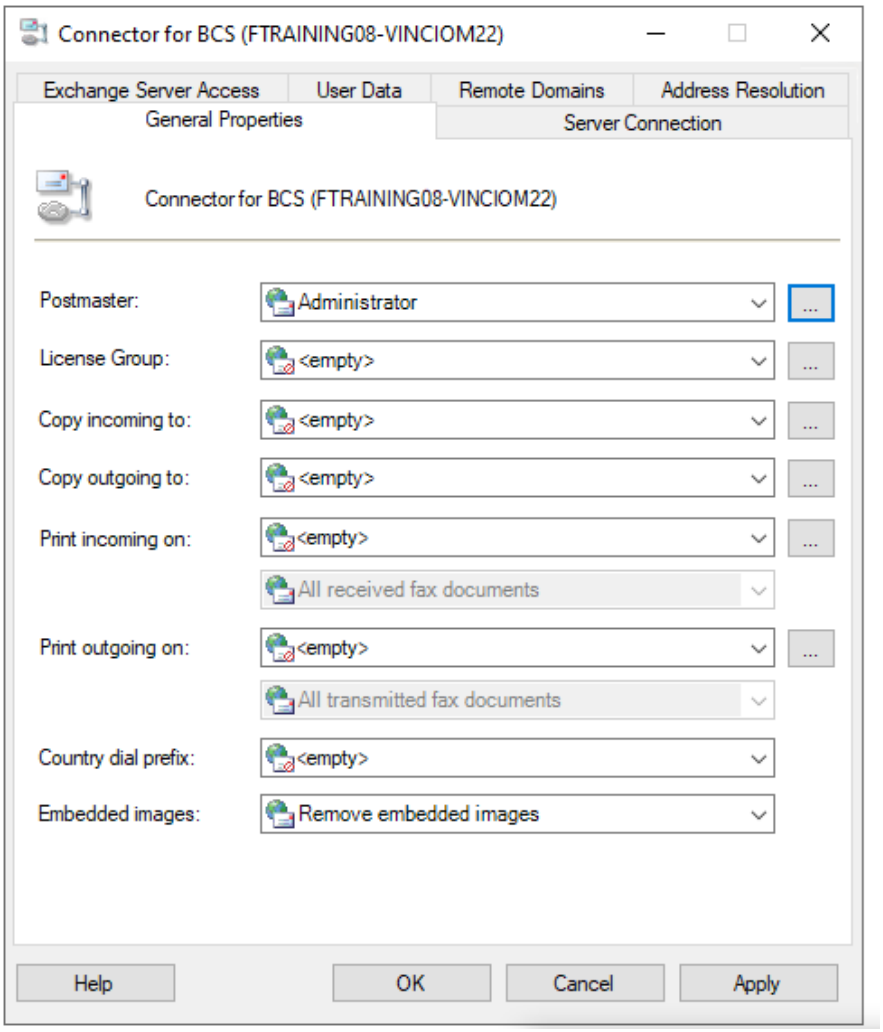
7.5.7. Connector configuration

The connector configuration is located in the Connector Configuration node. A list of servers that can be selected then appears. If a server has an installed associated connector, this is then displayed in the connector list.



General settings

Each connector needs its own specific settings. These are administered in the properties of the corresponding object.



Default recipient

A recipient or a public folder is specified under Default recipient, which will receive all documents (fax or SMS messages) that cannot be distributed automatically. The automatic distribution of faxes requires the use of ISDN hardware, with which it is possible to assign a unique fax extension number to each Exchange user. With an analog fax connection that does not support direct dialing, all faxes go to the default recipient. It is the task of the default recipient to forward the incoming faxes as a message to the correct recipients.

OfficeMaster server components (PRINTGW, FILEGW, etc.) can also act as default recipients. Distribution lists cannot be specified as default recipients.

Note!

In any case, it is necessary to enter a default recipient! If this entry is missing, it can happen that undeliverable documents cannot be sent to anyone by e-mail and may remain unnoticed in the OfficeMaster server's queue.

Input copy and output copy

With this, copies of all incoming and outgoing documents (fax) are filed in previously set up public folders or mailboxes. From these folders it is possible, for example, to archive the entire fax communication, search for specific processes or send copies again. The corresponding copy recipient is selected in the respective selection list. Public folders are in the Microsoft Exchange System Objects folder select list.

Printer input and printer output (UNC path only for fax documents)

A printer in the network can be selected in these fields on which all incoming faxes for the user are to be printed out. If the desired printer is not to be searched for, it can be entered manually in UNC notation (Universal Naming Convention). The default setting is inactive.

So that the connector can actually print out the incoming and outgoing faxes on the selected printer, the printer driver for the selected printer must be installed on the computer on which the connector component is running.

It is also possible to configure which documents are to be printed out for the printer. In this way, printing can be pre-filtered for incorrectly sent documents or successfully sent documents.

Note!

It should be noted that print gateways can be set up in the messaging server configuration, which also contain the mentioned function. The difference is that print gateways cannot be configured on a user-specific basis.

Note!

The MsxPrinterTest.exe tool can be used to test the print functionality. The tool is located on the OfficeMaster Server in the directory <SERVER>\FFACCESS\Redist\Tools.

Country code

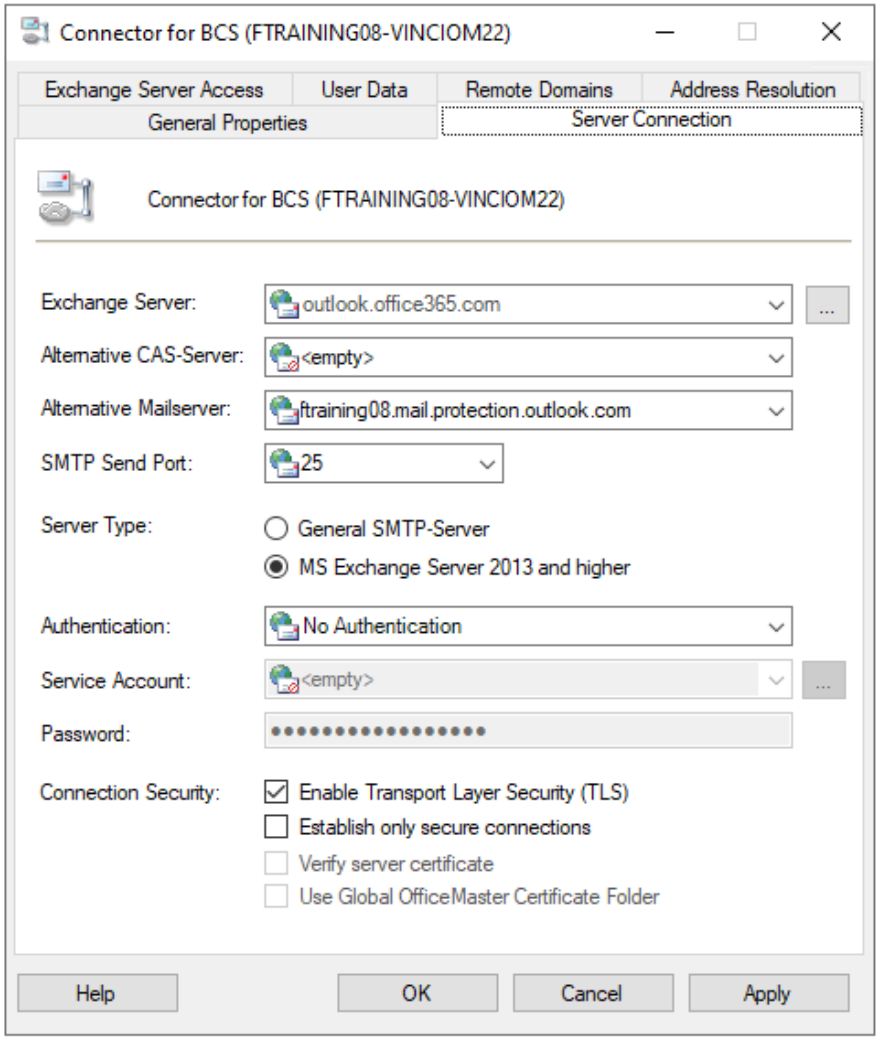
It is not possible to set up a correct call on most ISDN connections if the telephone number contains the international country code of your own country. To avoid this problem, you can enter the country code of your own country at this point. The Exchange connector will then convert this identifier to a zero. Since a central system can be set up with a messaging server in which the hardware is distributed across national borders, the connector could also be used for documents from foreign locations. In this case, the OfficeMaster server must be set in the ISDN settings for this correction. The entry for the country code must then be set to <blank>.

Embedded images

Image data contained in the email body is usually removed from the cover page. The Support embedded images function ensures that embedded images of the mail text are integrated into the cover sheet and are transmitted unchanged by fax. This means that signatures that have been supplemented with image data can be supported.

Server connection

This tab configures the SMTP client of the OfficeMaster Exchange Connector, i.e. the properties are set here for how the messaging server sends SMTP e-mails to the Exchange Server.



Exchange servers

The name of the Exchange Server that is entered here designates the Exchange Server to which the component is to send the mails. This field cannot be changed.

Alternative CAS server

In this field you can enter the address of an alternative server with which you want to communicate via EWS in local use. A CAS array, for example, can be specified here for on-premise installations.

Alternative mail server

The IP address of an alternative Exchange server to which the documents are sent can be entered in this field. Normally, all mails are sent to the entry in the Exchange Server field. This can be overwritten at this point.

SMTP send port

The SMTP port to which the component sends the mails to the Exchange Server entered above is specified here.

Receiving server type

The receiving server type regulates the creation of the e-mails, which can be different for different Exchange servers. By default, Exchange 2010 or higher should be selected here.

Authentication

The authentication determines the level of security of the mails from the messaging server to the exchange server. It cannot be arbitrarily administered manually here. A service account that is entered here must be specified at least once in the installation wizard during data verification, since a special adjustment is made. You can choose between two types here:

- None (Preferred)
  If this option is selected, no SMTP authentication is performed. This assumes that the Exchange Server allows anonymous access to the SMTP service. This is the default setting for connecting to Microsoft 365.
- NTLM
  This type of authentication (NTLM, WindowsNT Challenge/Response, WindowsNT Lan Manager Authentication, internal Windows authentication) uses a WindowsNT domain account to log on or to send SMTP e-mails. As there would be specific requirements for this account, it is not used in a Microsoft 365 installation.
- PLAIN
  This type of authentication (plain text password SMTP) uses a special login account for the related server. As there would be specific requirements for this account, it is not used in a Microsoft 365 installation.

Service Account, Password

The service account and password can be specified at this point. Changing the service account should not be done at this point. The installation wizard of the messaging server should always be used for such changes.

Connection security

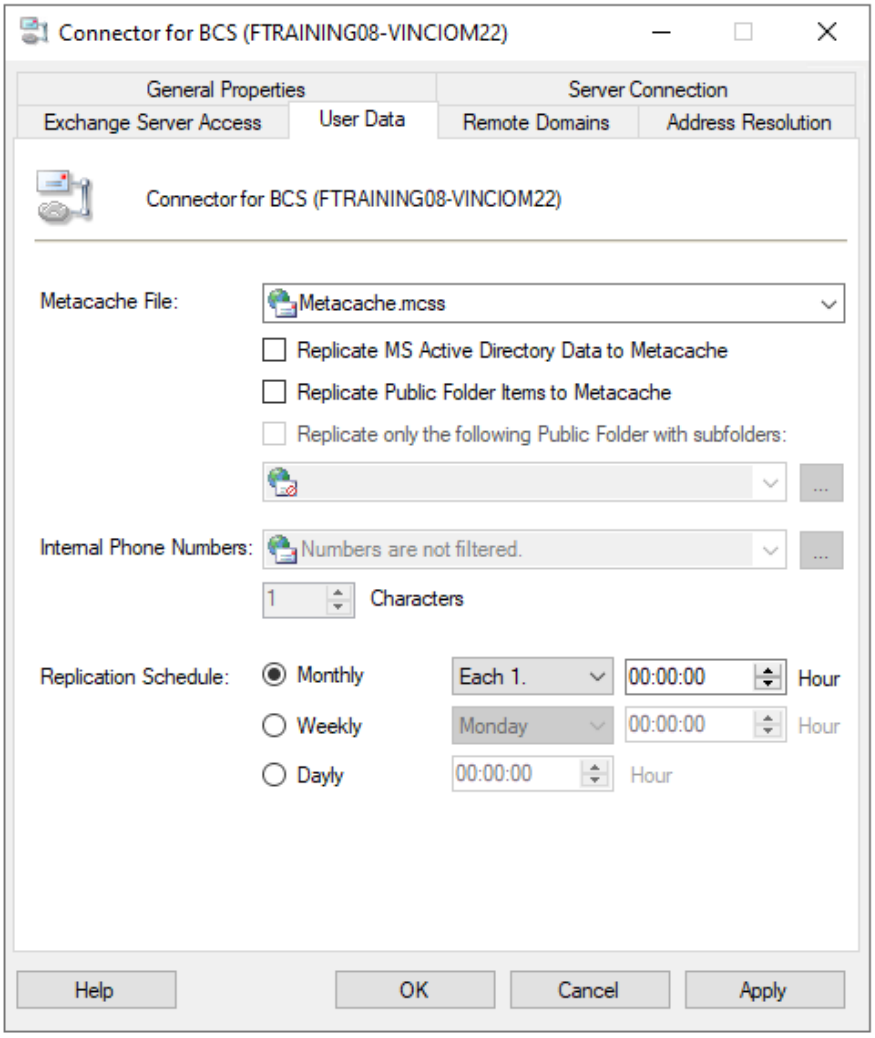
Connection security parameters determine how communication to the server is encrypted. While the option isn't enabled on Microsoft 365 installations, it can certainly be enabled for encrypted connections. This increases the corresponding security of the communication.

Different levels of security can be specified:

- Perform connection with TLS (Transport Layer Security)
  In this case, a general encryption via TLS is activated. The encryption levels are automatically negotiated between the systems and there is no authentication by certificate.
- Only allow secure connections
  If communication with remote stations that do not understand TLS is to be prevented, this can be activated with this option. If the option is activated, the connection is terminated immediately if the remote station requests TLS-free communication.
- Verify Server Certificate
  If verification of the server certificate is activated, the server's certificate can be checked against the local Windows certificate store. If the certificate options are not correct, the connection is terminated immediately.
- Use global OfficeMaster certificate directory
  Normally it is checked against the certificate chain of the Windows certificate store. If there are explicit certificates that are located in the global OfficeMaster certificate directory ("\\SERVER\FFACCESS\CERT"), then such certificates can also be checked exclusively. This can be activated with the option.

User data

User data tab can increase processing speed of incoming and outgoing documents for fax and SMS, as well as user resolution of voice calls.



Metacache file

The metacache database is a proprietary database that can be created at runtime of the connector component. Similar to a global catalogue, this database contains all relevant address data for the domain(s). By specifying a file with the extension ".mcss", the database is created based on the other settings in the course of the replication plan. The data, which can be accessed in the shortest possible time, is then used for user resolution when creating cover sheets and for obtaining information for incoming telephone calls. The database is optimized for speed and can be operated without any other installable database systems.

Replicate MS Active Directory to metacache

If this option is enabled, the Active Directory forest of the user data is copied to the database. This process can take some time.

Replicate public folders to metacache

In addition, this option can be used to copy public contact folders to the metacache. This process assumes the existence of public folders and may take some time.

Only use this public folder with subfolders

In order to optimize the access speed when accessing the public folder database, a public contact folder can be selected or specified here, which restricts the folder search.

Internal phone numbers

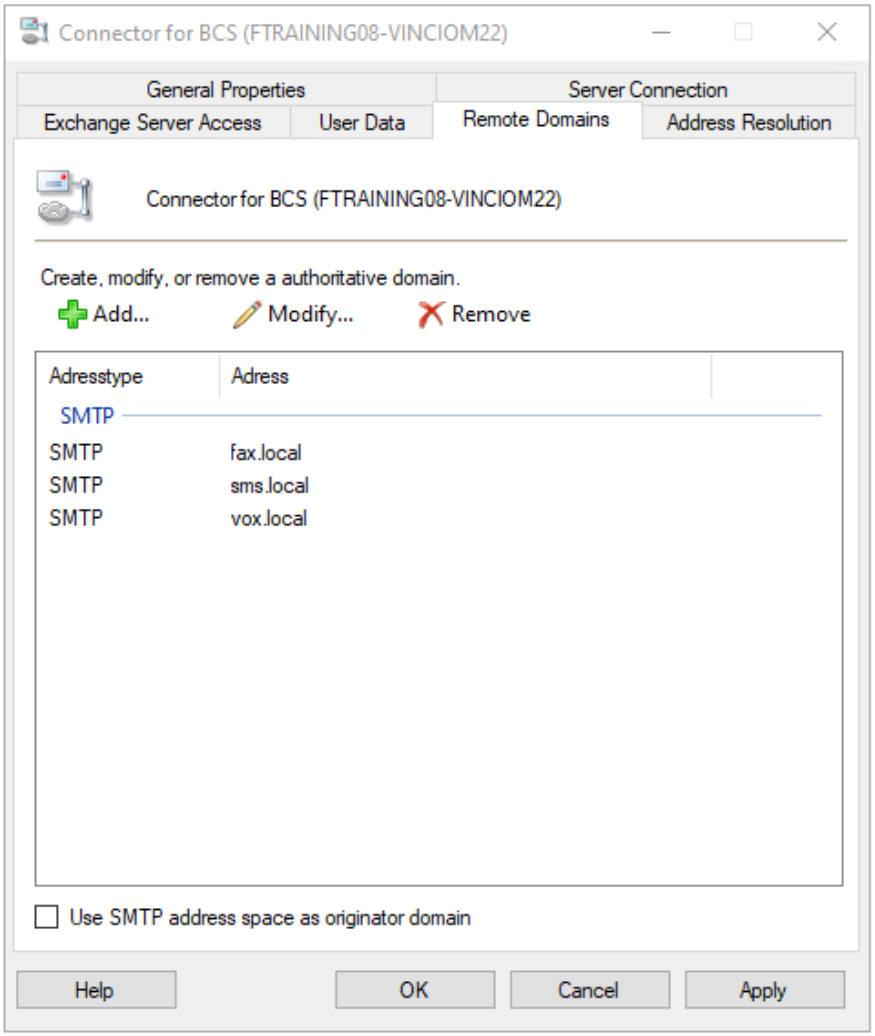
Since the metacache stores all phone number data, internal phone numbers that are not unique can result in duplicates. To prevent this, you can specify how the internal numbers are recognized based on their length and whether they should be assigned to individual domains.

Replication schedule

The replication schedule determines the time and interval of copying the data.

Receiving Domains

The address space specifies address ranges or types for which the connector provides its function on the output side.



The specification of these domains is not used for the automatic creation of objects in the target system, but for the registration of these domains in the OfficeMaster Server.

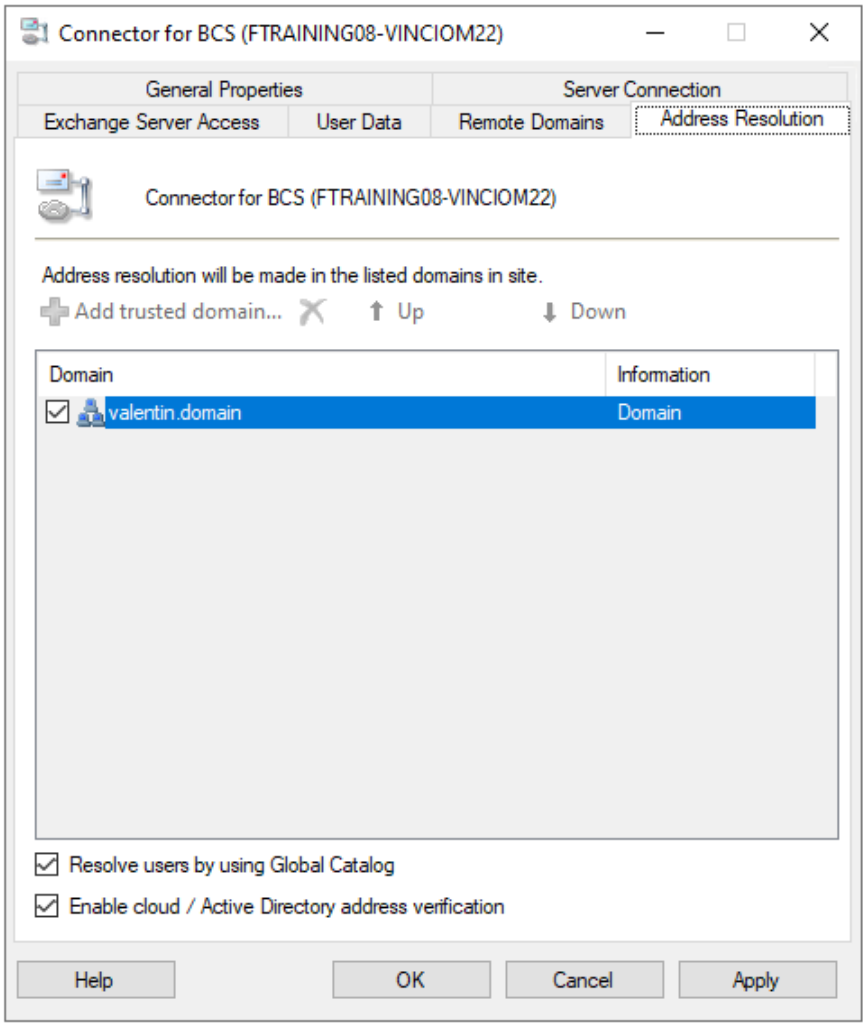
Link sender address of incoming messages to SMTP address space

Normally, the sender addresses of incoming messages are linked to the senders' phone numbers. Here it can happen that the outgoing SMTP mail server does not accept this format. Therefore it makes sense that the sender addresses are linked to the corresponding SMTP domains. When adding the addresses you can specify whether this address can be used for fax, SMS and/or voice.

Address resolution

The Address Resolution tab is used to optimize performance of the connector. When a document is sent/received, the corresponding sender/recipient is resolved in Active Directory to determine the user's information and send/receive rights. In a worldwide organization, all

domains of the Active Directory are searched by default. This can take some time. For this reason, a domain selection and domain sequence can be specified explicitly in this tab.



Add trust relationship

A trust relationship can be added as part of cross-domain networks. In this case, this domain is also contacted via the corresponding service account of the component.

Resolve users using the Global Catalog

This option can also be used to increase speed in networks with multiple domains. If possible, the global catalog will be consulted when the function is activated.

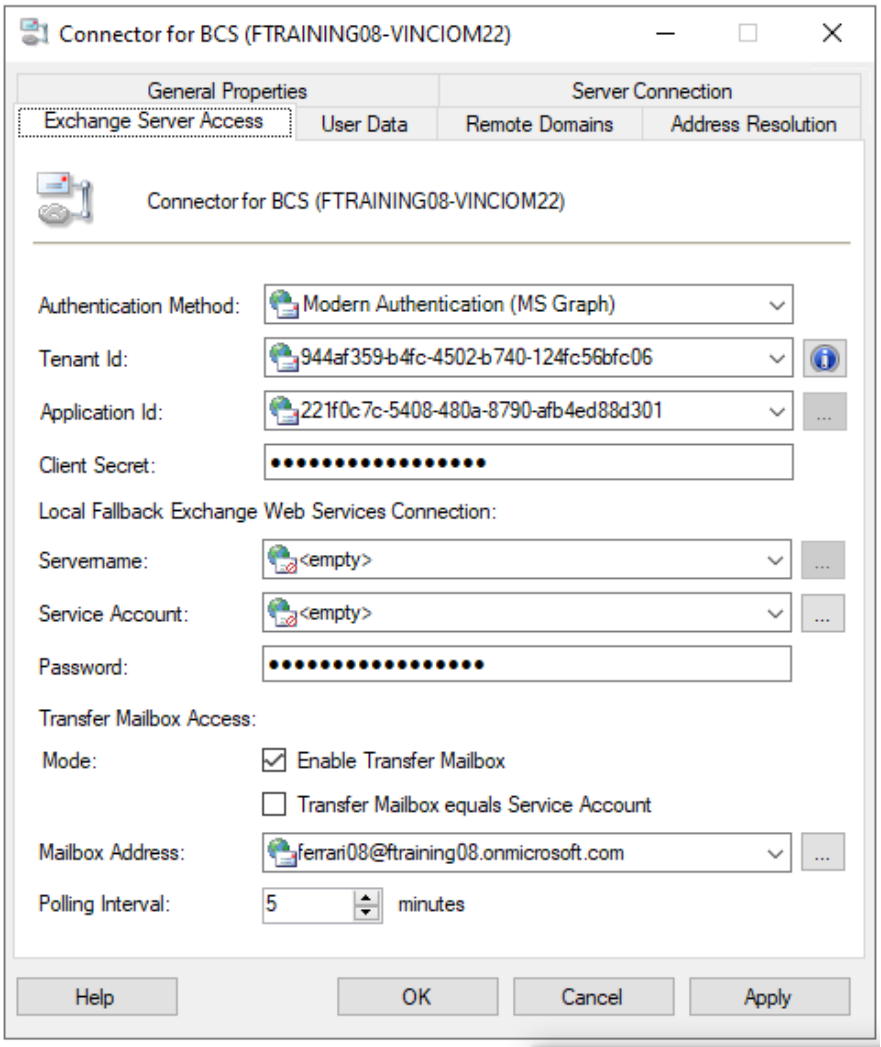
Enable Cloud/Active Directory address cross-checking

This option activates the check as to whether the determined sender address of the outgoing fax or SMS order also exists in the cloud. If this is not the case, the feedback would not be able to be sent. Therefore, this preliminary check can be activated here.

> Note!
>
> The administration of the user resolution only makes sense for hybrid installations or on-premise installations. With a pure Microsoft 365 installation, no domain query is required. In this case, the entries are irrelevant.

7.5.8. Exchange server access

The Exchange server access tab is used to set the access parameters for access to the mailboxes or address book of the controlled Exchange server (on-premises or Microsoft 365).



Authentication

At this point you can switch between “Modern Authentication (EWS)”, “Modern Authentication (MS Graph)” and “Basic Authentication”. Depending on the setting, the subsequent settings change from username to client ID and password to client secret. The tenant ID is only activated in the case of modern authentication.

Client ID

The Tenant ID is only relevant in the case of modern authentication. The info button can determine this ID automatically. A further registration may be necessary for this determination.

Program ID

In the case of modern authentication, a client ID (application ID or application ID) must be specified here. This can be selected with the browser button or must be determined manually beforehand so that it can then be entered directly.

ClientSecret

The client secret is a kind of password for the client id. If this is previously known, it can be stated here. If the client ID was determined using the search window, this search window cannot determine the client secret unless it is recreated accordingly. This can be specified in the application browser. Newly created secrets usually have a time limit.

On-premises Exchange Web Services connection

A local connection to an on-premises Exchange Server is advantageous when the organization is in a migration scenario. Mailbox messages to be queried remotely may then have to be queried on the local Exchange Server. If a special error is reported in the cloud that the requested mailbox does not exist, the BCS connector falls back to the local EWS connection specified here.

Server Name

The CAS server to be used, which is to act as the overflow target, is specified here.

Service Account

The service account is the account to use to access the mailboxes. This account must have appropriate impersonation permissions when using it to query content from other mailboxes.

Password

This represents the password of the service account,

Activate access to transfer mailbox

In order for a special transfer mailbox to be queried, it must be specified here that this function is activated.

Service account is equal to transfer mailbox

If the EWS access account is also the transfer mailbox, this can be specified here. The connector attempts to determine this connection automatically when it starts. However, this does not always lead to success. This option can therefore be specified here explicitly to switch off the internal check. Service accounts and transfer mailboxes have different handling of their mailbox contents. This feature is only useful in on-premises scenarios.

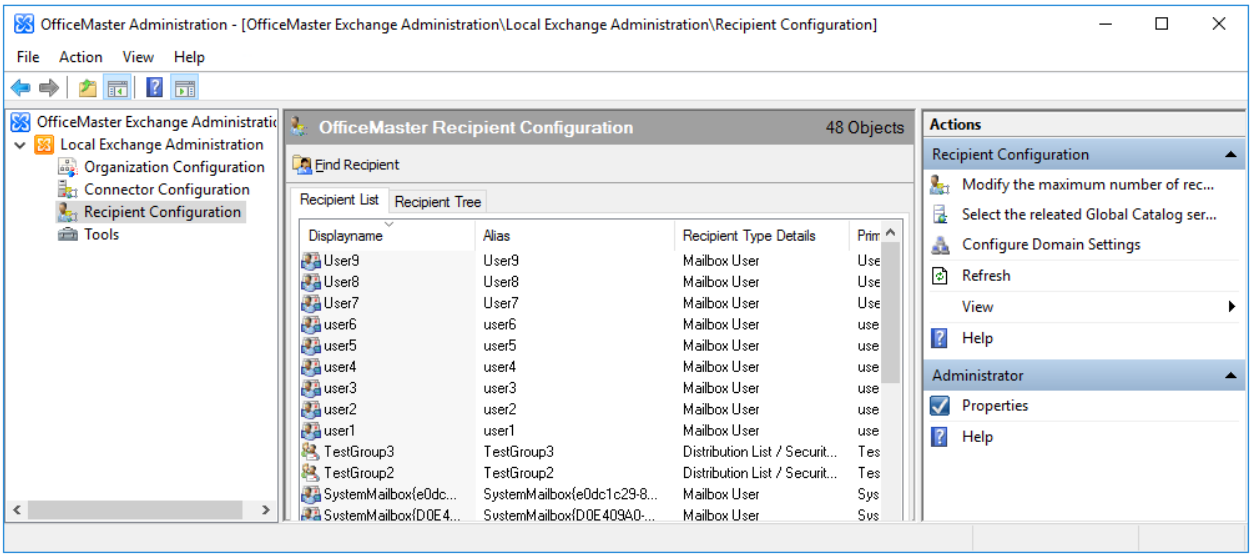
Mail box address

The e-mail address of the transfer account is entered in this field.

Access Interval

The value specified here determines the interval in minutes at which the connector collects the e-mails from the transfer account.

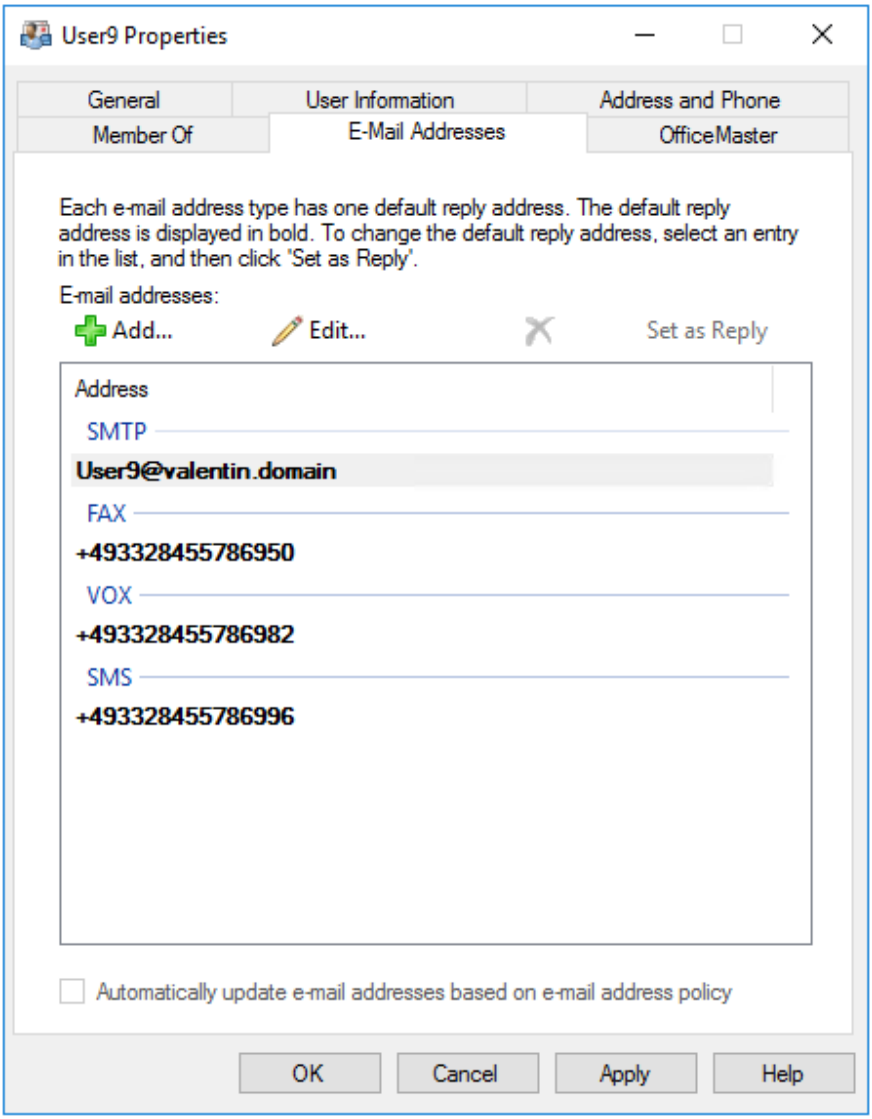
7.5.9. User configuration



A corresponding node is available in the OfficeMaster Exchange administration for professional user administration. In local Active Directory connections, a tree view corresponding to the Active Directory Users and Computers console is also available. This is not displayed in pure Microsoft 365 connections. A list of available users is displayed in the **Recipients** tab. In general, some properties (phone numbers, aliases, etc.) can be administered that correspond to normal user administration. However, the console is not primarily intended for this purpose.

Fax, SMS and VOX addresses

Just as in the normal web-based Exchange Server Administration (ECP – Exchange Control Panel), recipient addresses of various types can be administered in the OfficeMaster Exchange Administration.

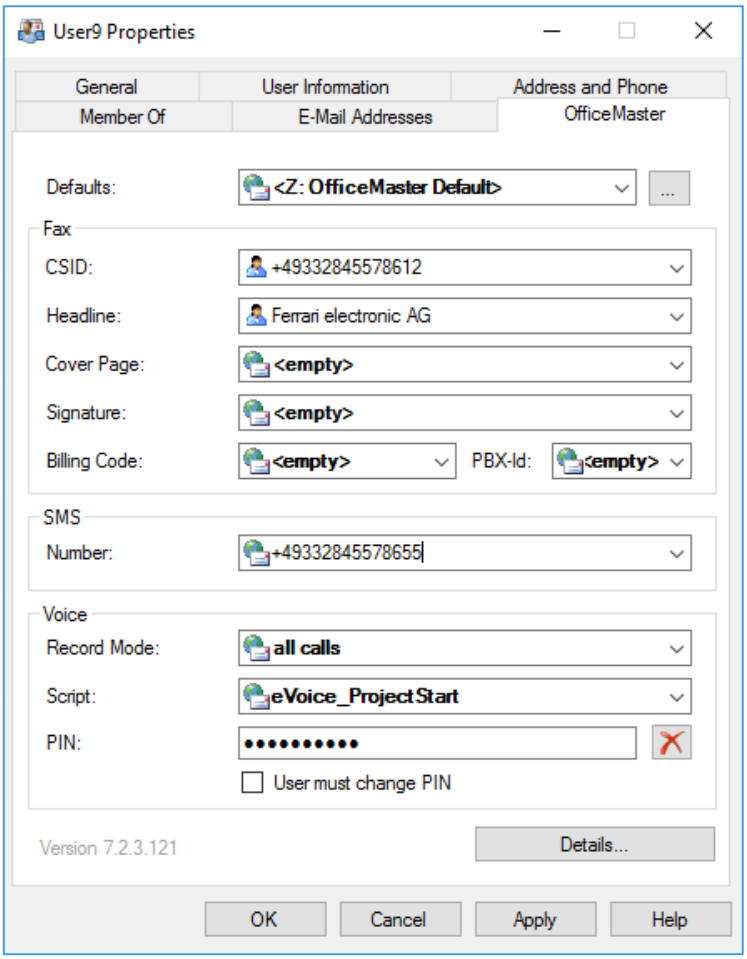


The user's fax extension number or SMS number is entered in the address field. These numbers should be unique.

> **Note!**
>
> It is not recommended to create FAX, VOX or SMS addresses via recipient policies! No meaningful addresses can be created via recipient guidelines for these purposes.

"OfficeMaster" tab

User-specific parameters are set via the **OfficeMaster** tab.



Specification

A user default profile can be selected here. If the user is not administered, the central user specifications are entered automatically after installation. If a user group is specified as a default that has not been administered, the central OfficeMaster settings automatically apply.

In the pure Microsoft 365 installation, user groups cannot be used as defaults because the data is stored directly in mailboxes. User groups do not have mailboxes, which is why they are not suitable as templates in this case.

Identifier

Here the user can set the fax identifier that appears in the header of a sent fax. According to the international standard, the specification should be in the form:
+country code area code (without the leading 0) phone number extension number.

```
Example: +49 3328 455 960
```

By specifying the identifier individually, the sender's fax number, including extension number, is transmitted correctly, so that corresponding reply faxes can be addressed directly to him. If the specification is omitted, the data that was specified when setting up the ISDN hardware is used. Setting an individual identifier for each user is particularly important in organizations where users send from different locations in order to send valid addresses for return faxes.

Header

In this line, an individual header text can be entered for each user (or user group). This can, for example, be the company name supplemented by the respective department name.

Cover sheet

The cover sheet designates the name of a user-specific cover sheet file. The default setting is inactive. The names of all cover sheet files that have been saved in the subdirectory COVER, which is automatically created on the computer on which the fax connector was installed, are displayed. It is also possible to enter another name. In this case, however, it must be ensured that a corresponding cover sheet file is saved in the COVER subdirectory before the system is used. The ending ".rtf" must also be specified.

Signature

The name of a signature file can be specified here. The default setting is inactive. The names of all signature files that are in the subdirectory SIGN will be shown. It is also possible to enter another name. In this case, however, it must be ensured that a corresponding cover sheet file is saved in the SIGN subdirectory before the system is used.

Cost centre

Any alphanumeric identifier of up to 12 characters can be entered as the cost center, which automatically appears in the log file of the messaging server for each send request sent by this user. In this way it is possible to clearly assign the order and the fees associated with this order to the user.

Telco ID

In some organizations, the costs for telecommunications are recorded centrally in the PBX. So that on connections that are used by several users, such. B. a fax line, the user causing the costs can be clearly identified, he must dial an additional code before dialing the actual

number, with which he identifies himself to the telecommunications system. This code is interpreted by the PBX, but of course it is not part of the phone number to be dialed by the PBX. If this option is used, the outside line access, i.e. the area code of a specific sequence of digits that causes the PBX to provide an outside line, cannot be carried out by messaging, otherwise the outside line access number would be placed in front of the TK-ID. The outside line access must then be integrated into the TK-ID.

SMS number

This entry specifies the main sender address and main recipient address for SMS messages. It is only relevant for SMS large account accesses. In all other cases, the user is assigned via the SMS address.

Recording

When selecting the messages to be recorded, a distinction can be made between:

All calls

If you dial all calls, the recipient also receives a message in the Exchange Client if nothing was said on the answering machine function. However, the recipient can understand that someone called and usually also who called.

Messages only

If you choose only messages, the recipient only receives a message in the Exchange Client if the caller left an explicit message on the answering machine function.

Voice Script

The voice script function involves the selection of the voice project in the voice server.

Voice PIN

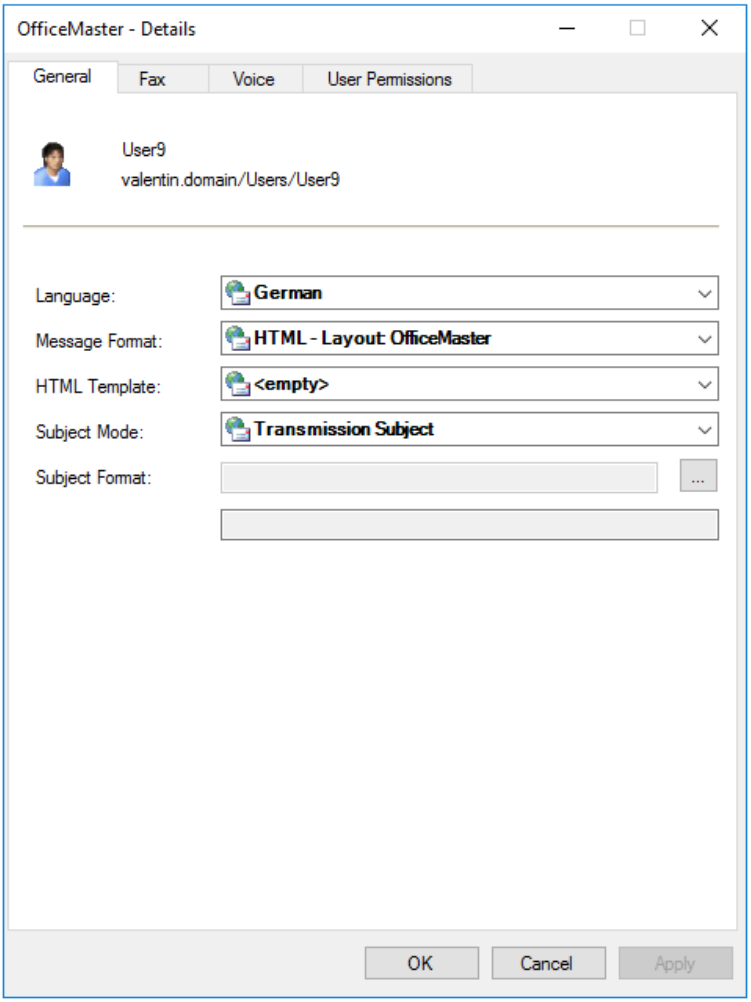
The PIN for the voice box can be entered here. This PIN is requested when switching to configuration mode. At this point, the PIN can also be deleted again. If the voice server has configured it in this way, the voice server can then automatically generate a PIN.

User must change PIN

This option is a non-persistent option. It tells the voice server to change the PIN over the phone. When this is done, the option is automatically reset. A prerequisite for the meaningful use of this function is the possibility that the service account of the connector can write to the local Active Directory.

Details

After clicking the Details button, a separate window appears with several tabs, which allow further administration of the user.



General

Language

The language (German, English, French or Spanish) in which the user would like to receive feedback can be selected here. The default setting is the central default, i.e. the language that was preset in the global connector settings is used.

Message format

In order to make the display of the documents more flexible for the user, the HTML layout can be specified for the user at this point.

The following options can be set:

- Only text
- Neutral
- Office Master
- Outlook

HTML template

In addition to the internally implemented HTML format templates, special external format templates can be loaded for further adjustments. These are generated in a special HTML/XML variation and can be stored in the global cover directory alongside the normal RTF cover sheets. These special template files (*.HTL) store complete language sets of HTML templates and can thus have a lasting effect on the appearance of the incoming documents and, if necessary, be adapted to the corporate design of your own company. The HTL editor program can be found in the <SERVER>\FFACCESS\Redist\Tools directory.

Subject line mode

The type of subject can be changed at this point in order to make the subject line of the reply to a fax document or a short message more flexible. Voicemails are unaffected by the Response Subject modes.

Three modes can be selected:

Transmission Status

This mode corresponds to the classic form of the response subject (e.g.: fax dispatch to <fax number> 1 page ok)

Original subject

The Original subject mode also places the subject line of the sent message in the reply. This is particularly advantageous if feedback from commercial applications is to be evaluated based on the subject. Such fax documents can be distinguished by the subject line, e.g. by an order number.

Custom

However, the subject line of the feedback can also be put together individually. The following placeholders are possible and are used according to the language setting:

%S Original subject line

%T Dispatch type (“Fax dispatch” or “SMS dispatch”)

%F to/from (depending on the type of dispatch and the language set)

%E Error status (“OK” or “Error”)

%P page number (e.g. “1 page”, “2 pages”, etc.)

%A Recipient (if resolvable in plain text, otherwise recipient number or fax ID)

%N Called telephone number transmitted via ISDN

%R Exchange recipient address (fax number)

%M short message (word “short message” in the set language)

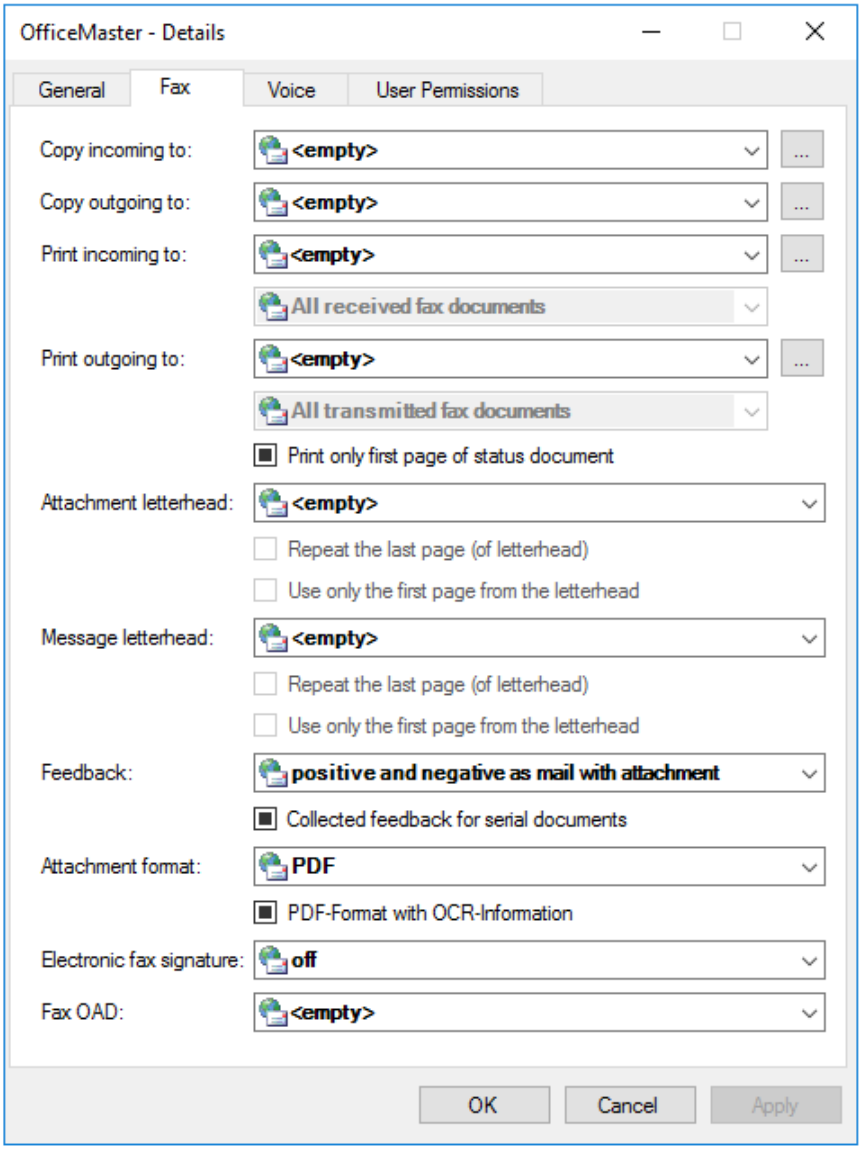
%% percent sign

e.g.: %S - %T %F %A %E

> If the subject text is “Offer No.0000145” and a fax is sent to the number “+49 3328 455 960”, the subject line of the response would be:
>
> “Offer No.0000145 – Fax to +49 3328 455 960 OK”

FAX tab

In the FAX tab, detailed settings can be made specifically for the fax service.



Incoming copy and outgoing copy

These settings are used to store copies of incoming and outgoing faxes in previously set up public folders or mailboxes. From these folders it is possible, for example, to archive the entire fax communication or to search for specific processes or to send copies again. The recipient of the copy, who has an email address of the FAX type, is selected in the respective field. In this selection, the public folders are located in the Microsoft® Exchange System Objects subfolder.

Printer input (UNC)

In this combo box, a printer can be selected in the network on which all incoming faxes for the user are to be printed out. If the desired printer is not displayed, it can be specified in UNC (Universal Naming Convention) notation. The default setting is inactive.

Printer output (UNC)

In this combo box, a printer can be selected in the network on which all sent faxes are to be printed out for the user. If the desired printer is not displayed, it can be specified in UNC (Universal Naming Convention) notation. The default setting is inactive. For the printer, you can also specify here which documents are to be printed out (all, successfully sent documents or incorrectly transmitted documents).

> Note!
>
> So that the Fax-Connector can actually print out the incoming and outgoing faxes on the selected printer, the printer driver for the selected printer must be installed on the computer on which the Fax-Connector is running.
>
> Note!
>
> It should be noted that print gateways can be set up in the messaging server configuration, which also contain the function mentioned, but such a configuration via print gateway is then not user-specific. The MsxPrinterTest.exe tool can be used to test the print functionality. The tool is located on the OfficeMaster Server in the directory <SERVER>\FFACCESS\Redist\Tools.

Stationery Attachment , Stationery Message

The default for this field is Standard; this means that the stationery centrally preset for the fax connector, which is assigned to attachments, is used for the user. However, a different stationery can be set. The names of all letterhead files stored in the LETTER subdirectory are displayed in the combo box. A new name can also be entered if it is ensured that a corresponding letterhead file is saved in the LETTER subdirectory before the system is started up.

The use of the stationery file for multi-page documents is controlled by the check boxes.

a) Repeat stationery (last page) b) only use the first page of the stationery

There are four possible combinations of options:

1. Both settings off (default setting)

Each page of the letterhead is superimposed on the corresponding page of the cover sheet or message. If the cover sheet or message has more pages than the stationery, no deposit is made for the pages of the cover sheet or message for which there is no stationery.

2. Repeat stationery (last page)

Each page of the stationery is assigned the appropriate corresponding page of the cover sheet or message. If the cover sheet or message has more pages than the stationery, the last page of the stationery is deposited for the pages of the cover sheet or message for which there is no stationery.

3. Use only the first page of the stationery

Only the first page of the stationery is used; it is stored on the first page of the cover sheet or message. Any subsequent pages of the stationery are not used. All subsequent pages of the cover sheet or message are not deposited.

4. Repeat stationery (last page), only use first page of stationery

Only the first page of the stationery is used. This page is deposited on all pages of the cover sheet or message.

Feedback

Here it can be set explicitly for the user how the feedback is sent to the mailbox. The following options can be selected:

- positive and negative as mail
- positive as mail, negative as NDR
- only in the negative case, as mail
- only in the negative case, as NDR
- positive and negative as mail with attachment
- positive as mail with attachment, negative as NDR
- only in the negative case, as an email with an attachment (recommended)

Collective feedback for broadcast faxes

Here you can specify whether the responses for broadcast faxes (fax documents with identical content and multiple recipients) should be sent together as a delivery report and non-delivery report. The settings in the Responses selection list apply to documents with only one recipient.

File Format

If the user wants a preferred file format for the fax delivery, this format can be specified in this field.

PDF format with OCR information

In addition to the file formats, it can be specified that if OCR text recognition software is installed, a PDF file containing searchable text will be generated.

File Format

The incoming faxes can be delivered in different formats. Only a TIFF format (usually TIFF/G3) or the PDF format makes sense here.

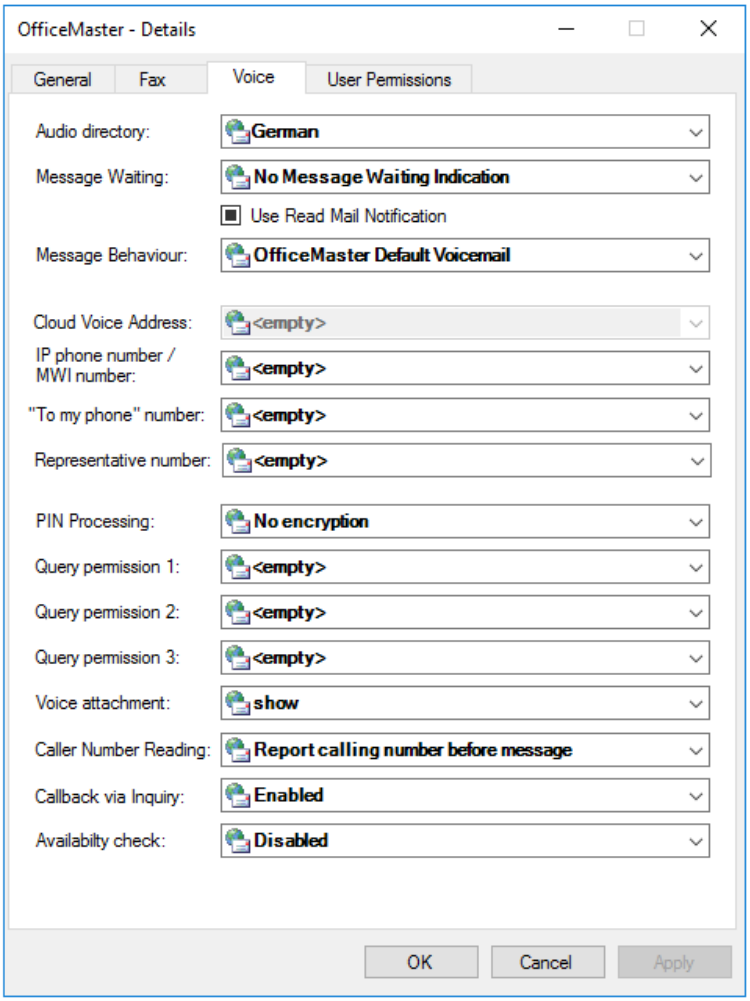
Electronic fax signature

At this point it is set whether the user provides his fax documents with an electronic signature. An activated signature can be deactivated via the OfficeMaster send options for Outlook (with the appropriate rights). It should be noted that the messaging server must support electronic fax signatures.

Fax sender number

The fax sender number is the telephone number that should signal to the receiving party who the sender is. Normally, the main sender address of the FAX type in the user's e-mail addresses is used here. In addition to this automated form, the sender number (OAD) can be specified explicitly at this point.

Voice tab



Detailed settings are made specifically for the features of the personalized answering machine on the Voice tab.

Language directory

In this field, a language tree can be selected that corresponds to a voice box language or a voice box voice. By default, the languages German (de) and English (en) are available.

Message Waiting

The “message waiting” behavior determines the turning off of a message waiting lamp on the user’s phone. Switching on the lamp is largely determined by the messaging server

configuration and the corresponding control of the message waiting function in the PBX. Shutdown supports three modes:

- Reset by general remote inquiry
- Reset by listening to at least one message
- Reset by listening to all messages

Cloud mailbox address

The cloud mailbox address is the phone number that is used to indicate to the receiving party who the sender is when transferring calls to external parties (or forwarding voice messages to a specific phone). Normally, the main sender address of the VOX type in the user's e-mail addresses is used here. In addition to this automated form, the sender number (OAD) can be specified explicitly at this point.

Own number

It cannot always be assumed that the number of the voice box corresponds to the telephone that is assigned to the voice box. In most cases, the telephone's direct telephone number differs from the voice box number. In order to also be able to switch off the MWI lamp correctly, the number of the telephone whose lamp is to be switched off when listening to the assigned voice box must be entered here. This entry therefore specifies the number of the workplace telephone.

"On my phone" - phone number

In the Outlook integration of the voice solution, messages can be forwarded to a telephone. In most cases this is the number of the desk phone. However, if the location of the workplace changes frequently, or the mail client is started from different computers, it is not absolutely necessary to have your own workplace telephone within easy reach. In these cases, another phone can be specified at this point.

Deputy phone number

At this point, the phone number of a deputy can be specified, which is made available to the voice server for further processes.

PIN processing

As a rule, the voice PIN is stored in compressed form in the Active Directory. To increase security, the PIN can be saved in encrypted form.

Query Permission 1...3

Telephone numbers can be specified here, which immediately put the called voice box into configuration mode when there are calls from these devices.

Voice file attachment

In the selection field you can specify whether the voice message file (WAV or MP3) is to be displayed or suppressed in the message. Suppressing it would have the effect that the file can no longer be played back over the PC speaker, but only over a remote query.

Read out caller phone number

It can be specified here that the caller's phone number is read out during remote inquiry. It can also be determined whether the reading takes place before or after listening to the individual message.

Remote Inquiry Callback

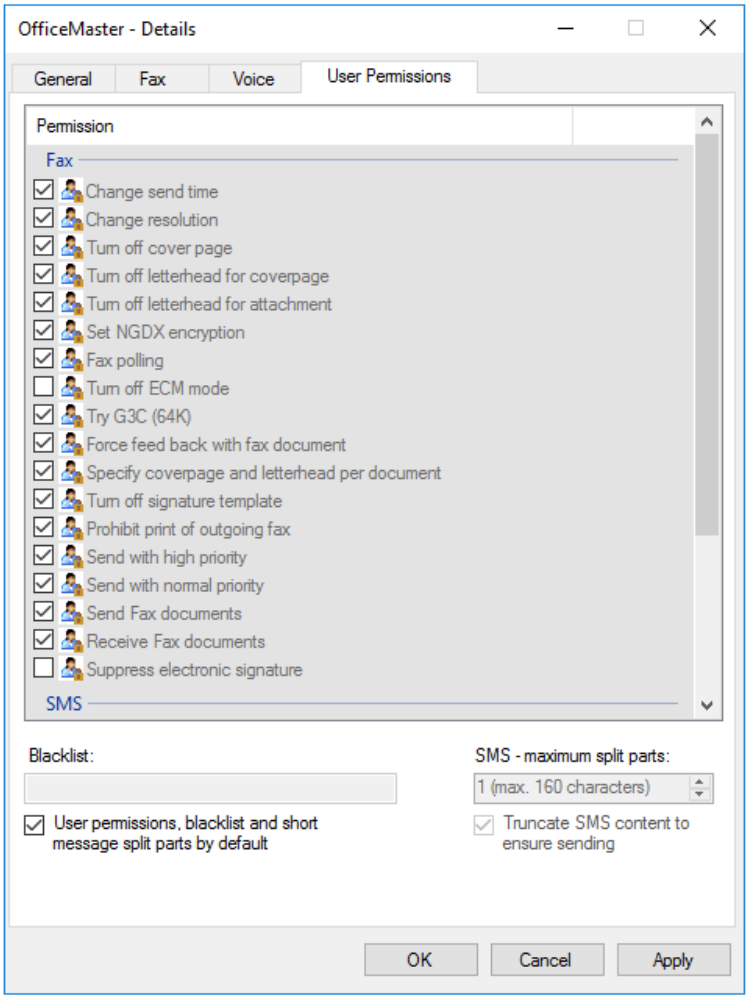
At this point it can be determined whether the option of calling back should be offered in the voice menu for remote inquiry.

Check availability

With this option, the connector checks the recipient's mailbox for calendar entries that mark the recipient as busy. In this case, the voice server can influence the mailbox recording process.

User Rights tab

The User Rights tab administrates the user-specific rights. The individual rights were explained in the *User rights* section.



Permissions and blacklist as specified

If this option is enabled, the user rights are set based on the rights specification. The configuration of the profile specified under Default then applies. If the option is activated, no entry can be made in the corresponding fields.

SMS split maximum

The maximum number of SMS messages into which overly long SMS texts can be split can be specified for the SMS split maximum. If this maximum is reached, the message is truncated at this point. Overlong documents can be divided into a maximum of 99 SMS messages.

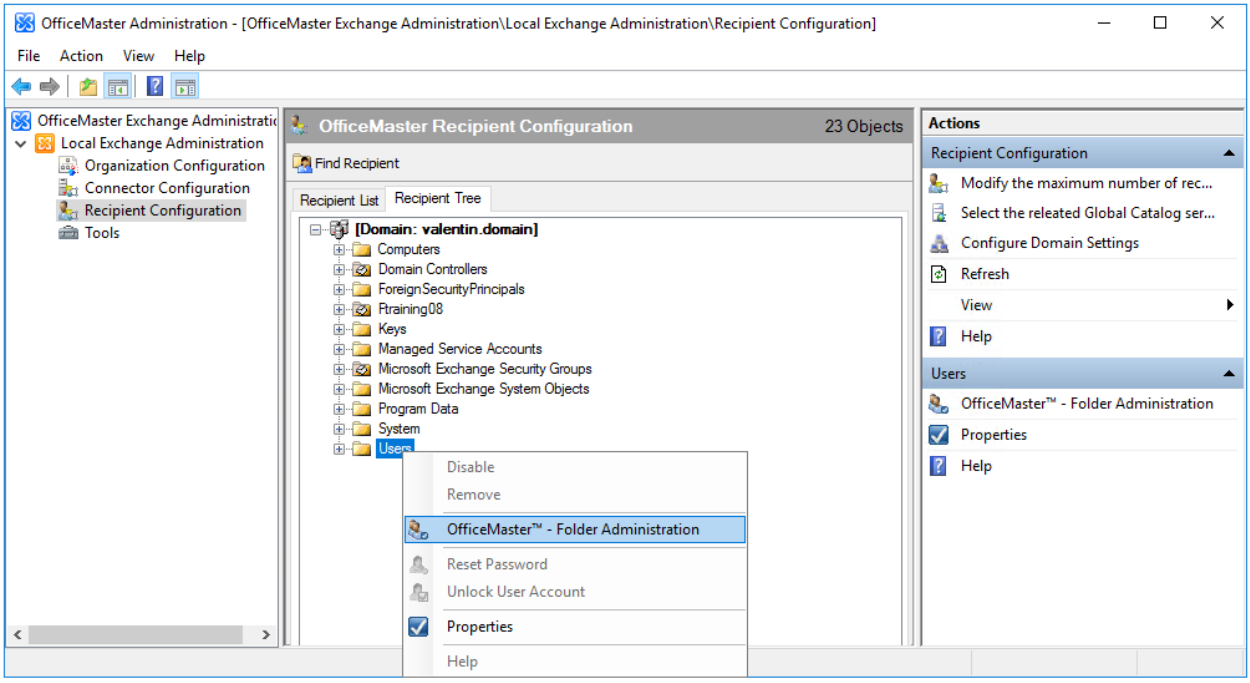
> Note!
>
> It should be noted that the connector only calculates using normal SMS sending methods. The connector has no information about the actual delivery method,

which can also affect the splitting of the SMS messages. Thus, a shortened text may still be too long to send.

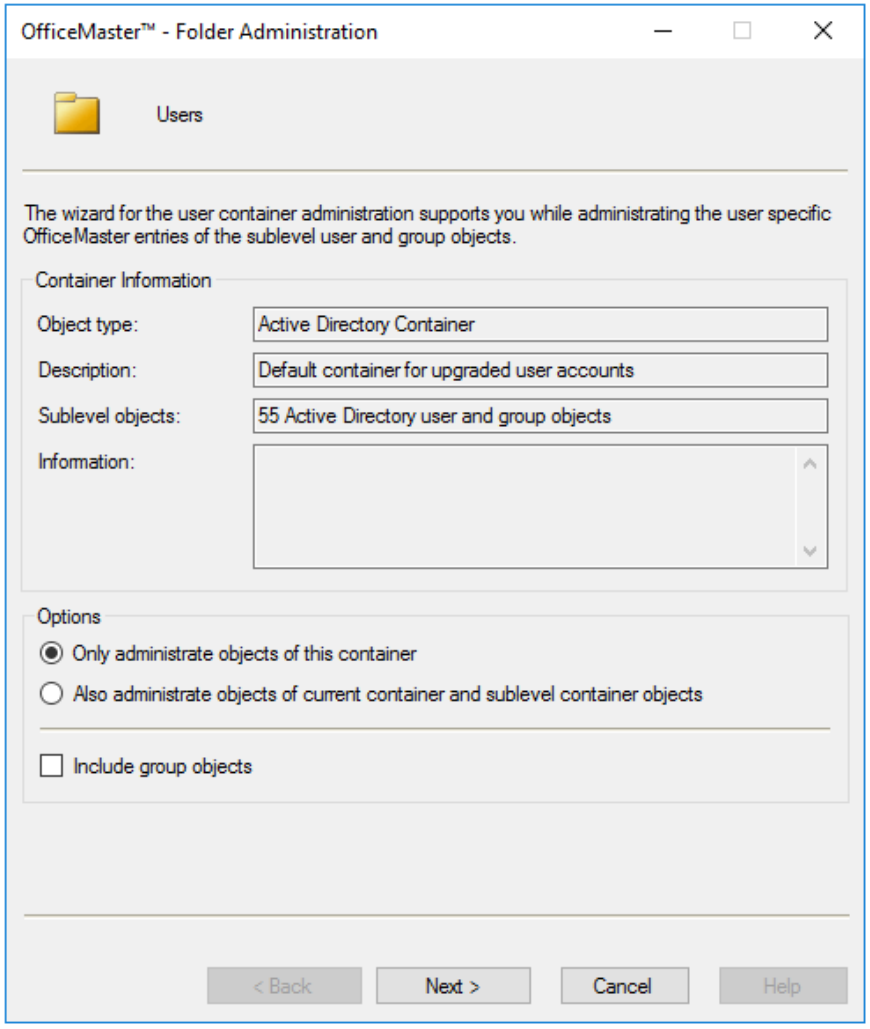
This function is only included in the connector for compatibility reasons and will be removed from the connector in the future. It is generally recommended not to use SMS truncation!

OfficeMaster group and folder assistant

In larger companies it can happen that individual user groups or recipients from certain locations cannot use the global settings of the connectors. The global settings for these users may not match the organization's policy.



The OfficeMaster Group and Folder Assistant can make these settings so that you can still change the user properties without having the administrator open and administer each object individually. Individual properties can be deliberately ignored during automatic administration in order to retain the original value.



To access the group and folder wizard, display the properties of the folder, organizational unit or group. The assistant can be selected in the receiver configuration in the receiver structure view. Folders and organizational units are also displayed in this view in order to access the groups and folder management wizard.

This object also has a special OfficeMaster tab. An administration assistant can then be started for containers and organizational units. For groups, this is a member administration.

Editing options

Only edit items in this folder

The option causes the wizard to only edit the users contained in the folder. If this folder has other folder objects that also contain user objects, these users will not be administered. This function is only available in the OfficeMaster folder management.

Objects in this folder and all contained subfolders

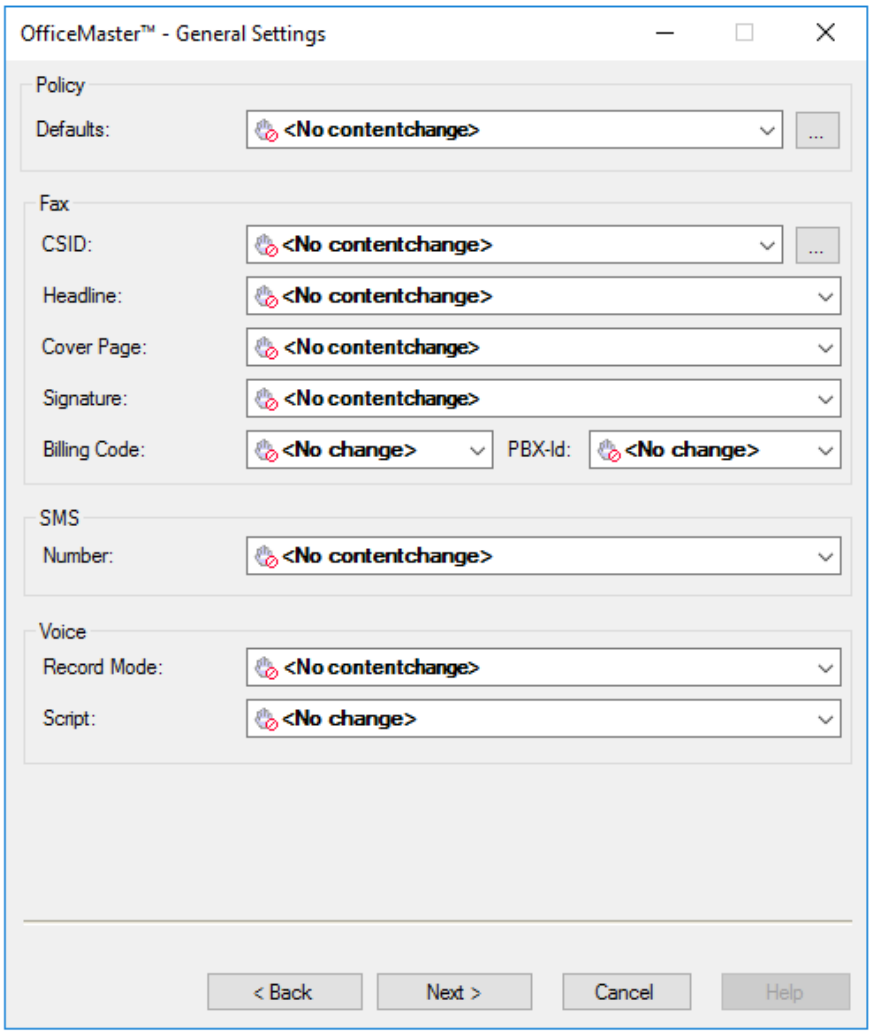
This option causes the wizard to also process users of the folder that are contained in subfolders. The function is only available in the OfficeMaster folder management.

Include group objects in processing

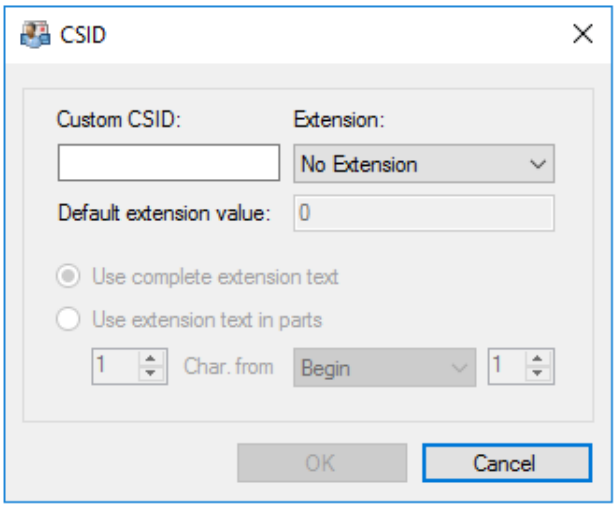
Enabling this option means that distribution lists and security groups also get the desired settings. It should be noted that such group objects do not represent senders for the OfficeMaster connectors but rather default properties.

General settings

The General settings wizard dialog reflects the main properties of the users' OfficeMaster tab. The individual properties are described in the section on the "OfficeMaster" tab.



As a special optimization of the fax ID setting, the value in this dialog can be expanded. In addition to the manually entered value, a value previously set by the user can also be added. With the help of the tool button [...] a useful help dialog opens.

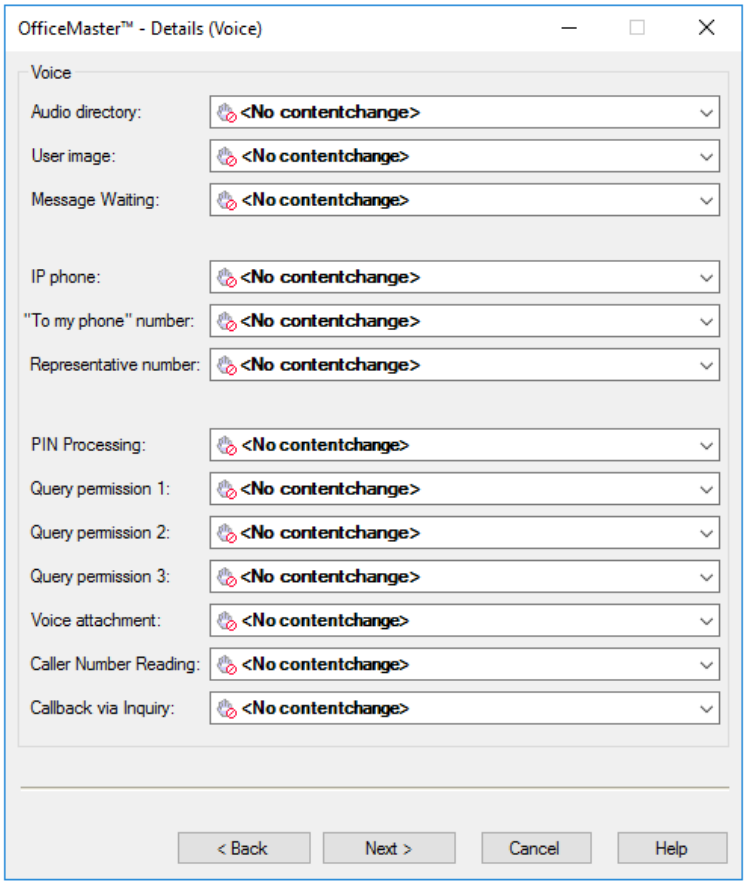


The fax identifier can be composed here using ready-made data. The following properties can be automatically added to the fax identifier:

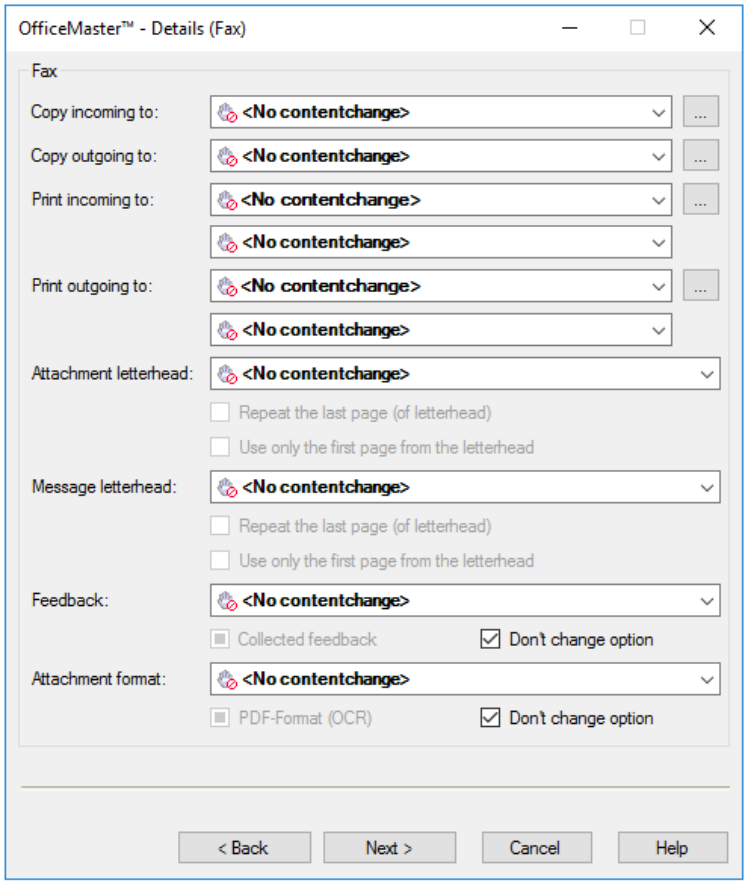
- Private number (First number from Active Directory - Telephone numbers field - Private)
- Radio call number (First number from Active Directory - Phone numbers field - Radio call)
- Mobile number (First number from Active Directory - Phone numbers field - Mobile)
- Fax number (First number from Active Directory - Telephone numbers field - Fax)
- IP telephone (first number from Active Directory - field phone numbers - IP telephone)
- FAX address (default reply address of type FAX if it is numeric)

Since the specified telephone numbers cannot always be used sensibly for the sender identification, adjustments can be made in relation to the digits of the telephone numbers in the point Apply additional text in extracts.

Details



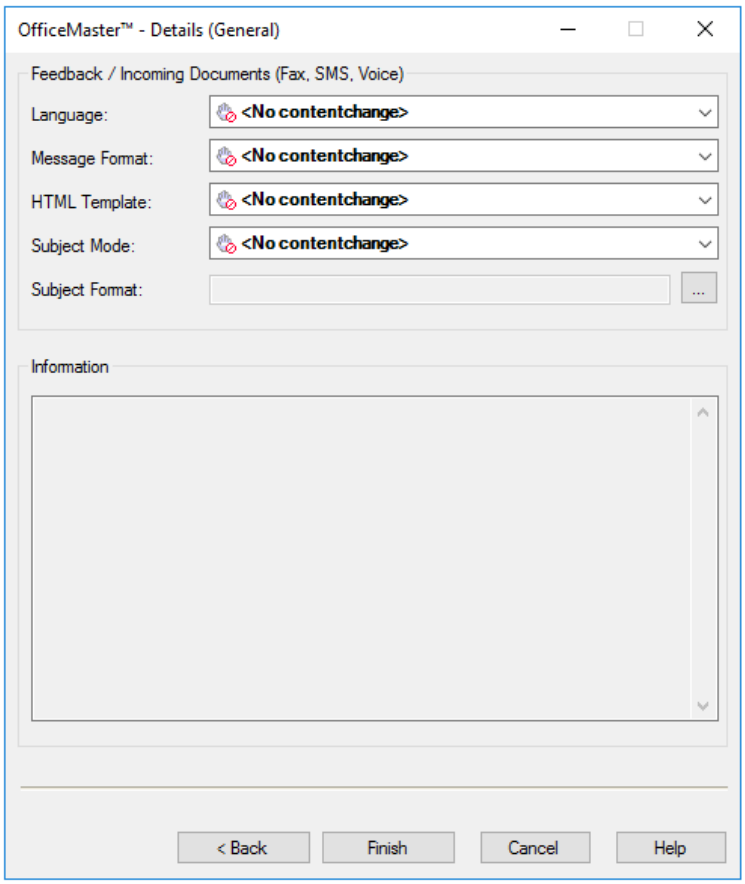
The Details (FAX) and Details (Voice) wizard pages represent the properties of the Details button of the users' OfficeMaster tab. The individual properties are described in the section on the "OfficeMaster" tab.



User Rights

The User Rights dialog reflects the properties of the **User Rights** button on the **OfficeMaster** user tab. The individual properties are described in the section on the “OfficeMaster” tab.

Details (General)



The general user properties (language, message format, ect.) can also be administered

The Finish button changes all administrable objects in the focus of the configuration to the extent that the values were specified.

> **Note!**
>
> At the time this document went to press, the folder wizard was not available for Microsoft 365-only installations.

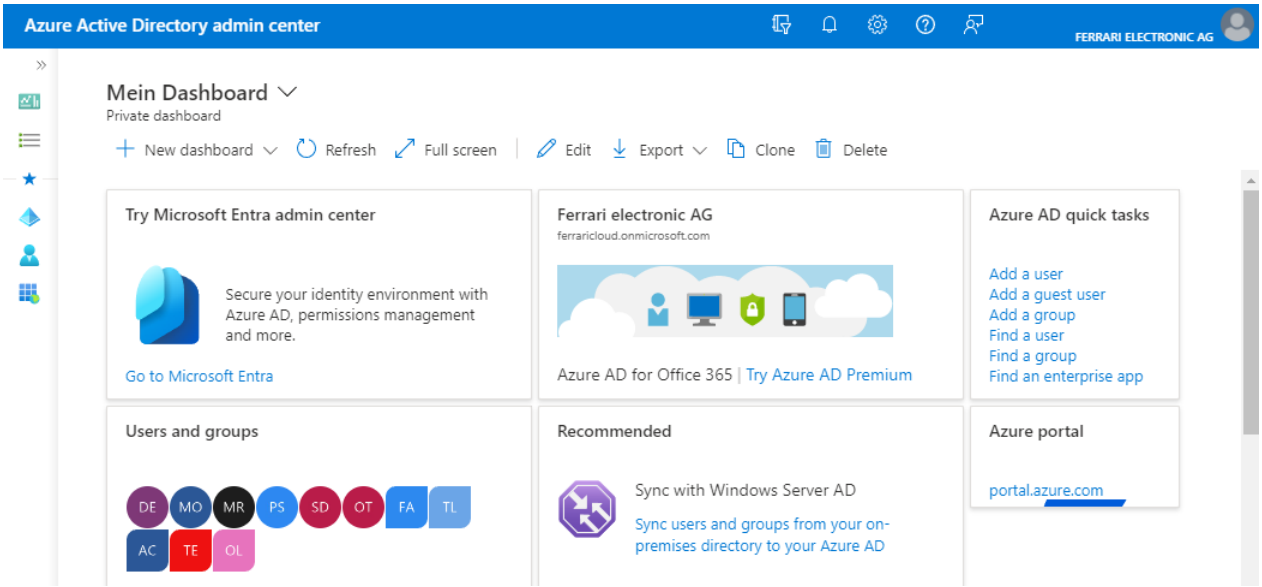
7.6. Technical notes on administration

7.6.1. Manual switch from OfficeMaster 7.1 to modern authentication or Microsoft Graph

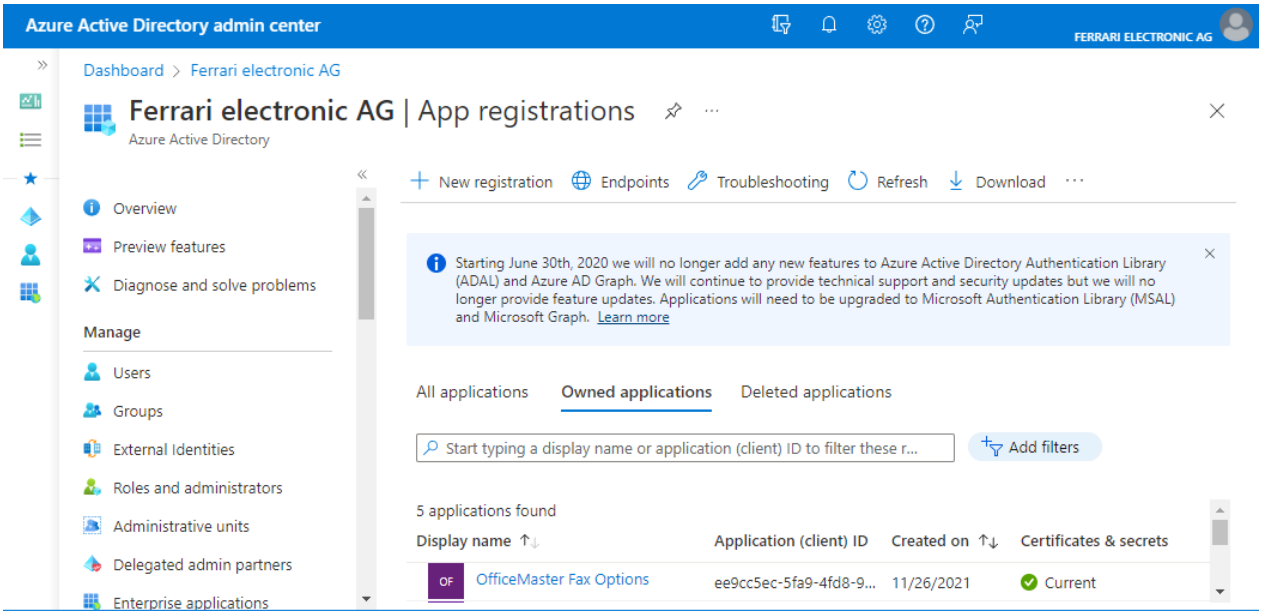
If an existing OfficeMaster Version 7.1 system is to be converted to the new OfficeMaster 8 interfaces, this can be done manually. The OfficeMaster application must be registered manually for this.

Manual registration of the cloud application

The first step is to log into the cloud and navigate to Azure AD.



To register the application, navigate to the registered applications (App registrations).



At this point, a new application can be registered to access the cloud.

The registry should contain the following values:

Application name: OfficeMaster Graph Access

You can enter any name here. The automatic installation wizard will use the name “OfficeMaster Graph Access”.

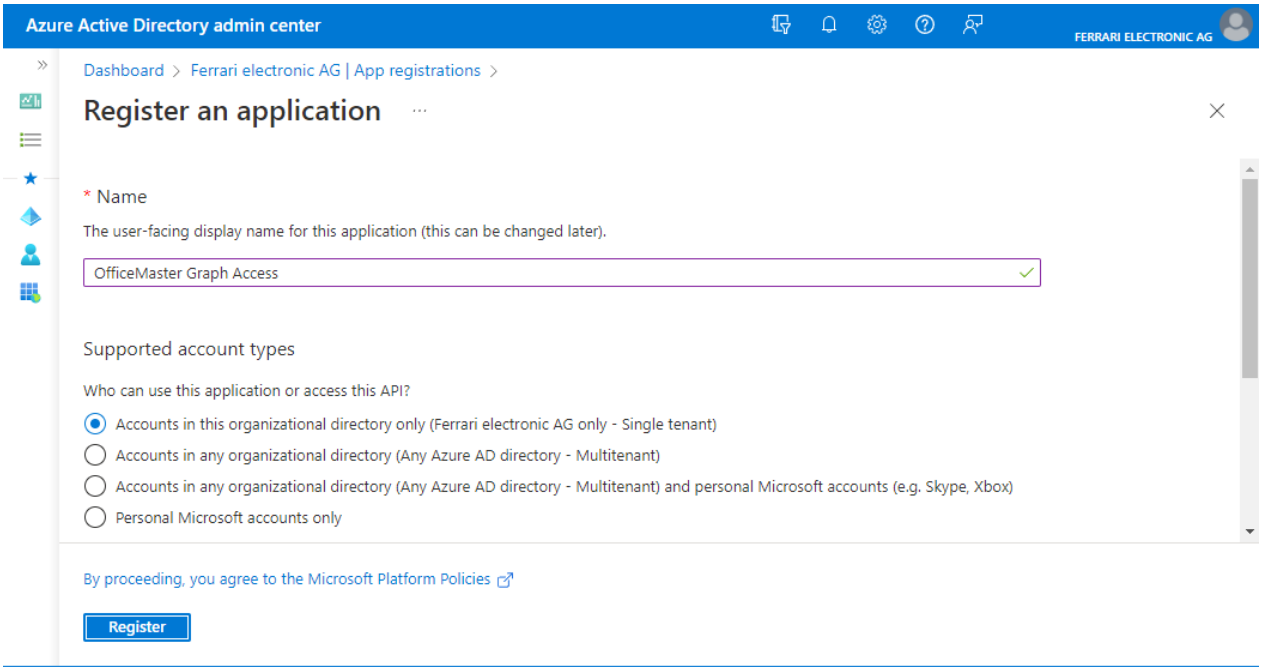
Supported Accounts: Accounts in this organization

You can also prepare the application for several clients here. The automatic installation wizard will restrict access to the registered organization (single tenant).

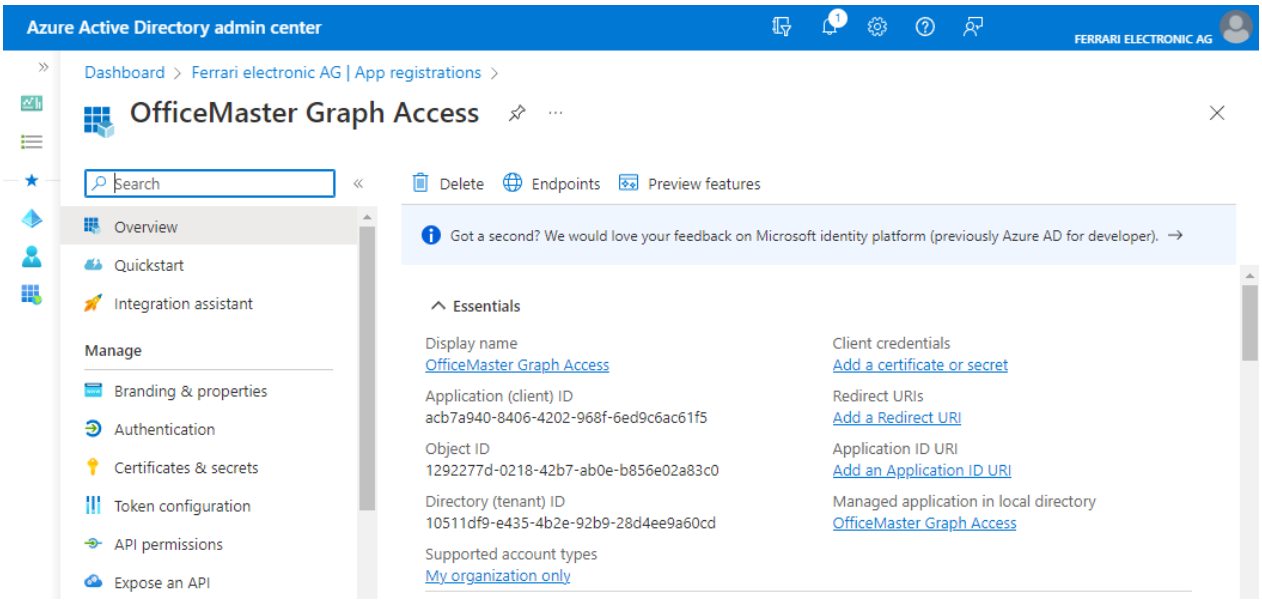
Redirect URI

```
Mobile and Desktop urn:ietf:wg:oauth:2,0:oob
```

Further information can be found at https://docs.microsoft.com/de-de/azure/active-directory/develop/scenario-desktop-app-registration.

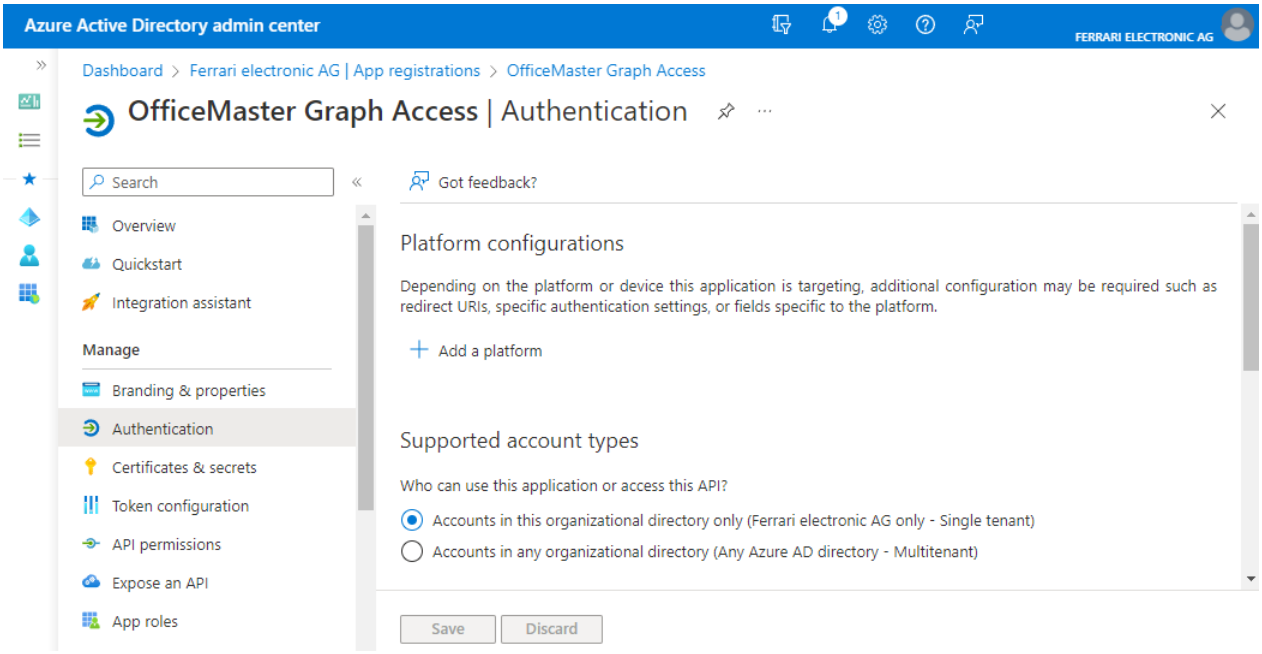


When the application is initially registered, this is a good time to note the Tenant ID and the Client Id.

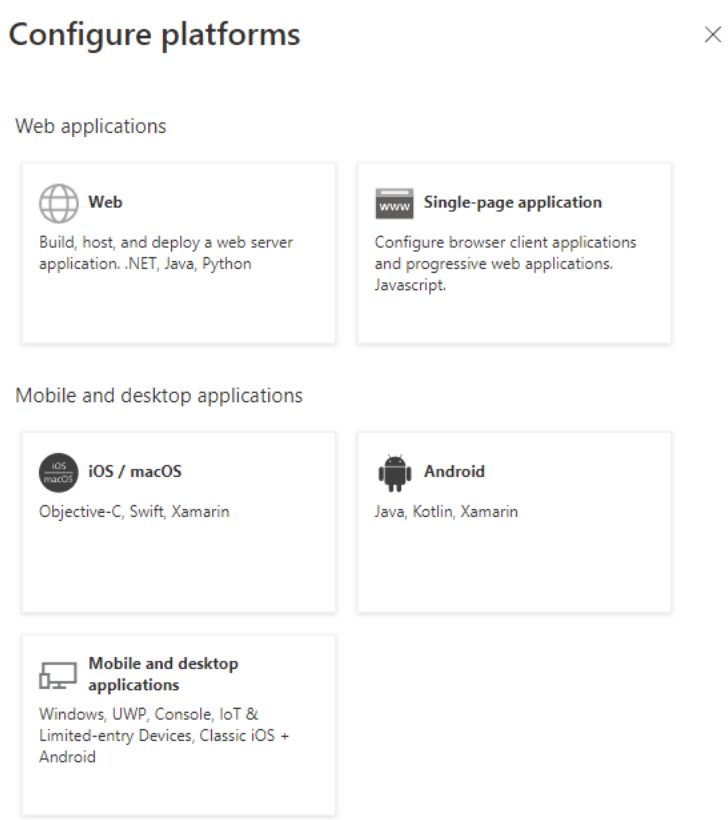


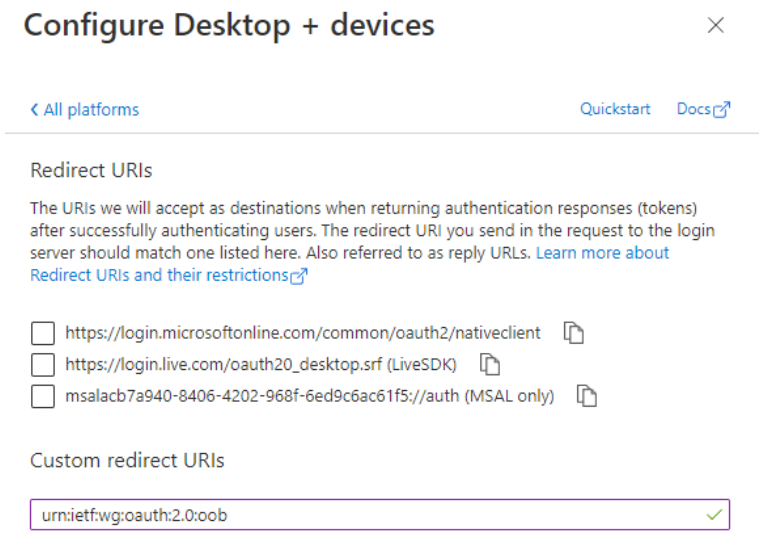
After the application has been created, the redirect URI should be entered next.

The Exchange connectors themselves do not have a web server that responds to redirects.



In the authentication field, add a platform entry of type “Desktop and devices”.

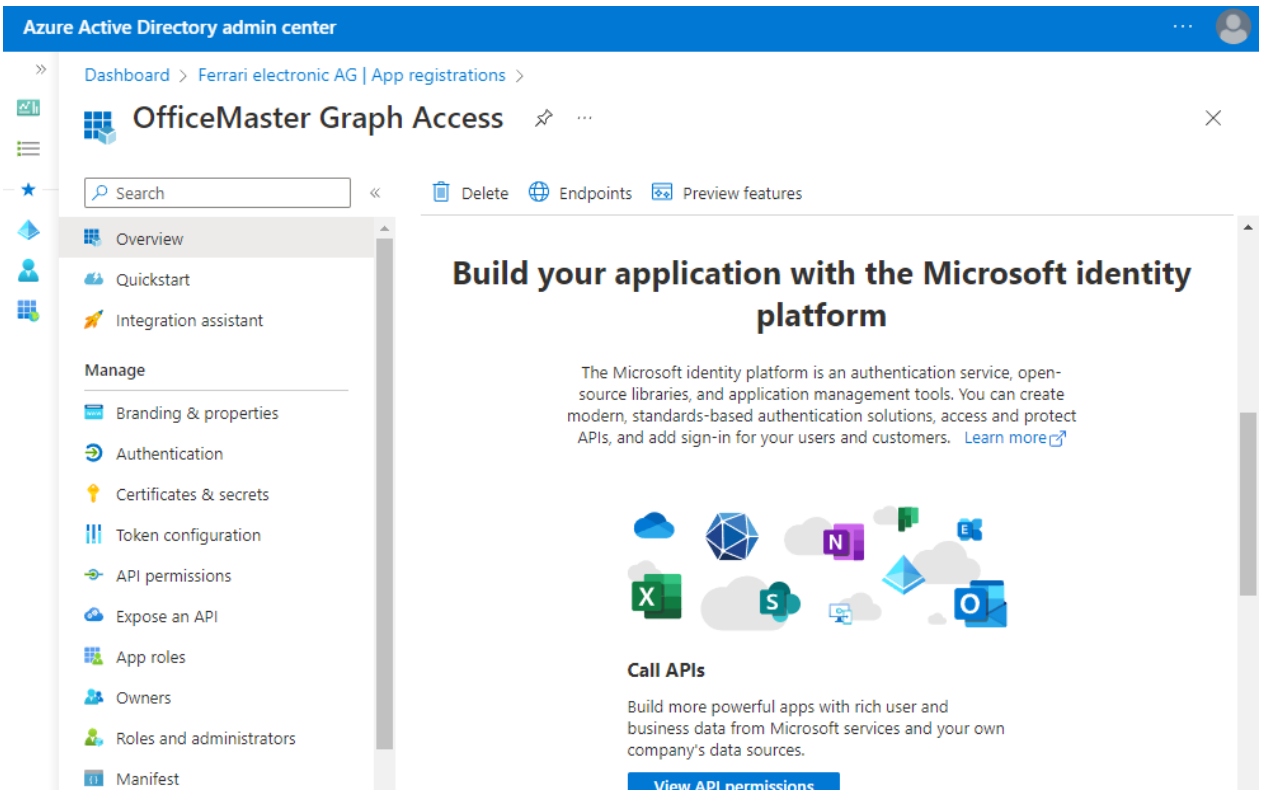




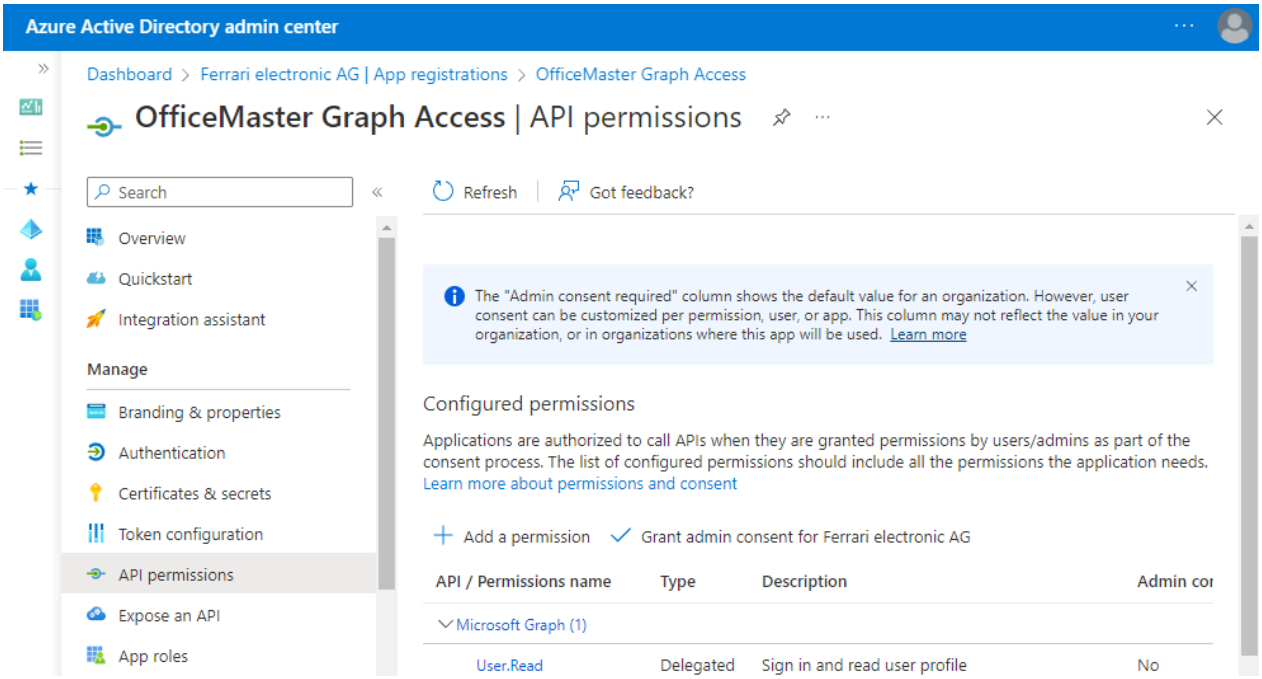
The value *urn:ietf:wg:oauth:2.0:oob* is then specified as the redirect URL.

Grant API permissions

Now the API permissions should be set. In the registered application, navigate to the API permissions.



You can see that an API permission has already been created automatically in the general creation. This is a basic permission. Further authorizations are required for further operation.



Existing Permissions:

- Microsoft Graph: User.Read (as delegated permission)
  This authorization is set automatically and has no meaning for the connector.

At least the following permissions should be granted for a hybrid connector (local AD + Microsoft 365 mailboxes):

- Microsoft Graph: GroupMember.Read.All (as application permission)
  The permission is used for requests to user groups. Distribution lists may have to be broken down for incoming fax or SMS messages. This authorization is also used for using the **OfficeMaster license group**.
- Microsoft Graph: Mail.ReadWrite (as application permission)
  This authorization is used for reading the e-mails in the user mailbox. At least this authorization is required for the transfer mailbox.
- Microsoft Graph: People.Read.All (as application permission)
  This permission is used for requests to the cloud address lists.
- Microsoft Graph: User.Read.All (as application permission)
  This permission is used for requests to the cloud address lists.
- Microsoft Graph: People.Read.All and User.Read.All (as application permission)
  These permissions are used for requests to the cloud address lists.

If the option is to be used of not sending e-mails to the cloud mailboxes via the Internet, it must also be possible for e-mails to be sent directly by any user.

- Microsoft Graph: Mail.Send (as application permission)
  This authorization is set in order to be able to send e-mails via the users and the transfer

mailbox. The connector uses this technology to carry out LPD mail dispatches and to be able to send e-mails from the transfer account to users. If this is not required, the authorization can be omitted.

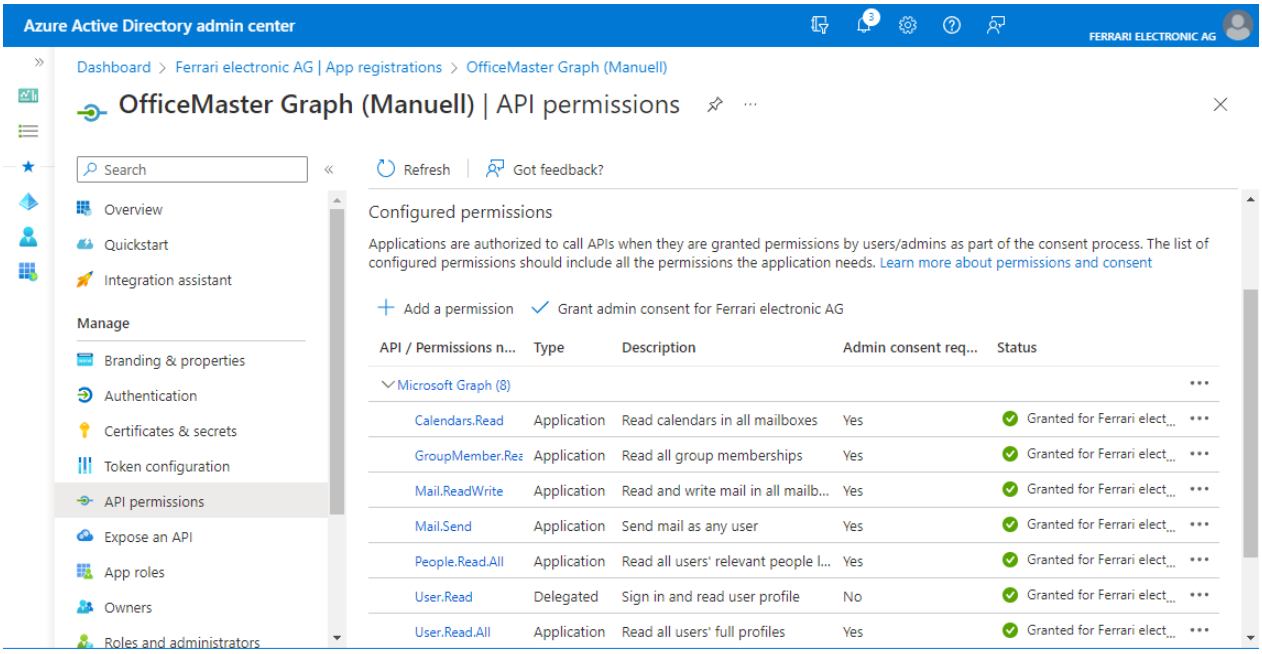
If, when recording a voice message, it should be checked whether the recipient has a corresponding appointment that lists him as “booked” in the calendar, the following authorization can be set:

- Microsoft Graph: Calendars.Read (as application permission)
  The permission is used for requests to users’ calendars. This is used for voice calendar queries to determine automatic free/busy statuses.

If user-defined values are to be saved in native environments, this can be done using an Azure AD OpenExtension. In this case, the following law must be set:

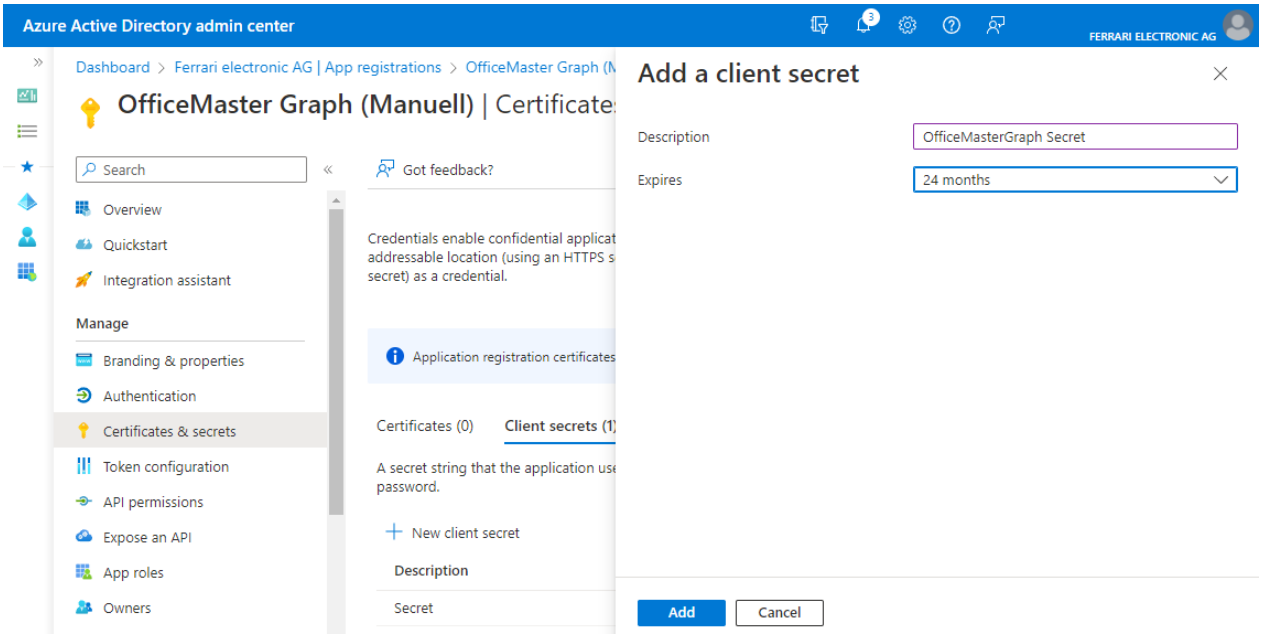
- Microsoft Graph: User.ReadWrite.All (as application permission)
  This authorization is required if individual user data is to be saved.

To add the permissions, check the corresponding points.



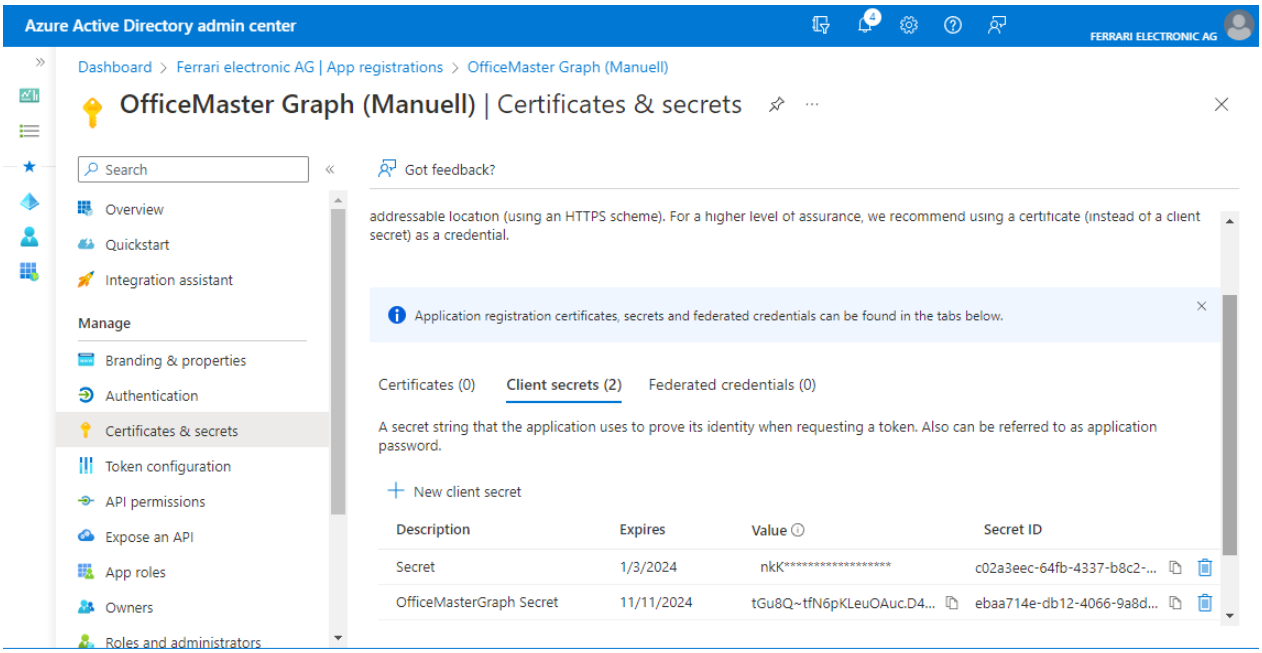
After the permissions have been added, they must be approved by an administrator (grant admin consent). After the API permissions have been released, they can be seen with a green tick.

Create or renew Application Secret (Client Secret).



A secret (client secret) is required for access with the client ID of the registered application. This must also be renewed after a specified period of time. To create this, navigate to the Certificates and secrets item in the registered application. You can then create a secret there.

The name of the secret only matters for administrative purposes. Since such names can be assigned more than once, this should be a meaningful name. The secrets usually have a validity period. The automatic installation wizard creates a secret with a validity of 2 years. This must be updated again after the validity has expired.



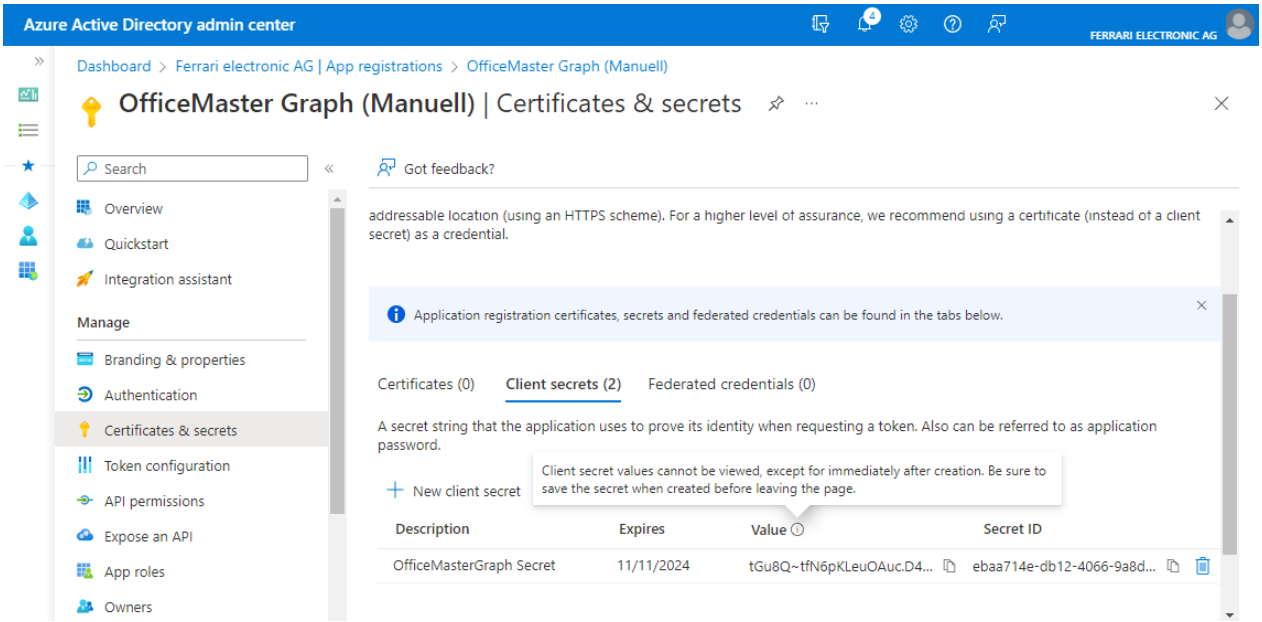
After the secret is created, it is only available for copying for this moment. This should definitely be noted. With the Tenant ID (client ID), the Client ID (application ID) and the Client Secret (secret), all the necessary values are then available to enter them.

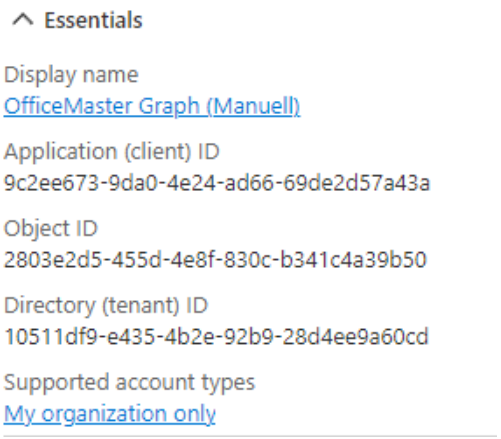
If the application has been created, the API permissions have been set and the client secret has been created, the application can be used by the connector. If the authorizations cannot be set in the form mentioned because this is not possible due to company specifications, the application should be limited using an **ApplicationAccessPolicy**. The procedure is described in the *Limit access to the created application* section.

If the application has to be created manually, it is generally recommended to do this using the Microsoft 365 or Azure AD graphical user interface.

Store registered application in Connector for BCS

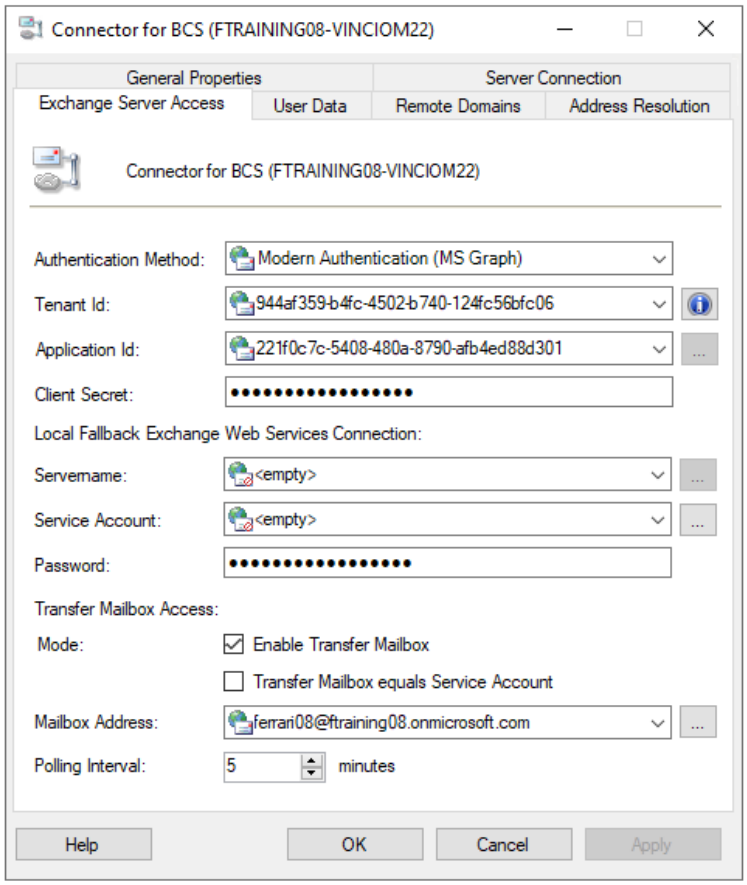
In order to store the registered application in the Connector for BCS, the parameters of the application must be stored in the properties of the Connector for BCS in the OfficeMaster Exchange administration.





The three important fields are noted: **Tenant ID**, **Application (Client) ID** and **Client Secret**.

The determined values are entered in the configuration of the connector in the OfficeMaster Exchange administration. The connector is then switched to “modern authentication”.



After the parameters have been entered, the connector component can be restarted. The component should now use the newly registered application.

7.6.2. Automated migration

A somewhat simpler transition is the automated transition. In this case, the connector is simply overinstalled with the installation wizard of the OfficeMaster Messaging Server configuration program. With this overinstallation, the transfer domains and the transfer mailbox must be specified again explicitly. If these entries are not available, we recommend registering the application manually as described in the section *Manual switch from OfficeMaster 7.1 to modern authentication or Microsoft Graph*.

7.6.3. Restrict access of created application

The registered application technology used here creates an application that covers the needs of the OfficeMaster connectors including remote voice access. For voice remote access, the application is granted the right to access other mailboxes within the organization.

In some organizations, this may not be wanted for legal reasons, and on the other hand, this is not necessary for a pure fax application in this form.

In order to limit access to the application, Microsoft offers an Exchange Online Powershell commandlet with which access can be granulated.

> **Note!**
>
> In order to ensure at least a smooth fax operation, at least unrestricted access to the transfer account must be allowed!

Powershell command:

```
New-ApplicationAccessPolicy -AppId \<applicationid\>
   -PolicyScopeGroupId \<group\>
   -AccessRight RestrictAccess
   -Description "Restriction to the members of the group"
```

<applicationid> Application ID (ClientId) of the OfficeMaster EWS application
<group> Group of members to be affected by this limit.

More information about this commandlet can be found on the Microsoft pages Scoping application permissions to specific Exchange Online mailboxes - Microsoft Graph | Microsoft Docs.

7.6.4. OfficeMaster 8 and the native Microsoft 365 operation

When switching from native operation (without local AD) to OfficeMaster 8, there are a few things to consider.

- The fax, SMS and voice addresses can no longer be used in the form of user-defined address types.
- The way custom values are saved has changed.

Note!

Due to the change in the interface to Microsoft Graph, the existing users may have to be modified in terms of their custom properties and in terms of their e-mail addresses.

Change of addresses

Assigning fax, SMS or voice addresses works when using local Active Directories by describing the proxy addresses. As a rule, user-defined address types (for One-Off Addressing) are used. Up until OfficeMaster 7, this was also permitted in native Microsoft 365 environments without local AD.

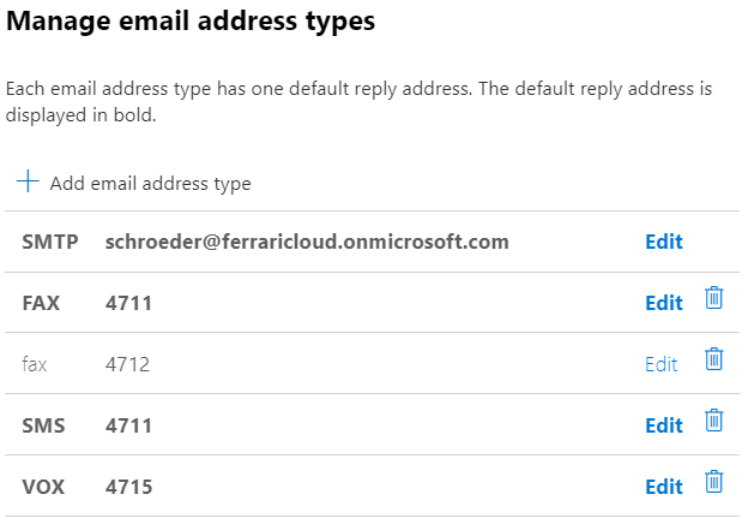
With the changeover to the Microsoft Graph interface, the address types in the e-mail addresses can no longer be used because Microsoft Graph suppresses the search for and publication of user-defined address types. By default, only SMTP address types are used.

To solve this problem, the email addresses of the users are changed:

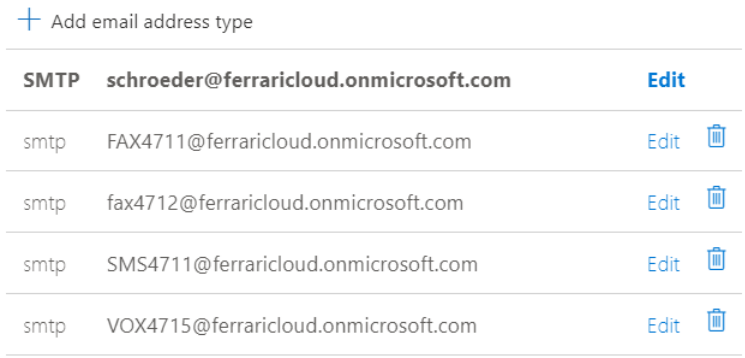
Conversion of OfficeMaster 6.x - 7.x Native Cloud Connector to OfficeMaster 8 Native Cloud Connector:

OMS6/7 address type	**address**	**OMS8 address type**	**address**
FAX	phone number	SMTP	FAX number
SMS	phone number	SMTP	SMS number
VOX	phone number	SMTP	VOX phone number

e.g.



to



If the planned conversion involves a higher number of users, Ferrari electronic AG can provide a corresponding script for the conversion. The **MakeAddressMigration.ps1** script can be used for this purpose. This script is located on an OfficeMaster server in the folder **\\<SERVER>\FFACCESS\redist** or **%PROGRAMDATA%\ffums\fmsrv\data\exchange\ redist**.

Change in user-specific data storage

OfficeMaster 6.x and OfficeMaster 7.x save the user-specific settings in the user's mailbox. This is done in a hidden mail object (Folder Associated Item). When OfficeMaster 8 was released, the Microsoft Graph interface was not yet able to read such settings. For this reason, the saving of the user-defined values had to be changed.

As of OfficeMaster 8, the user-specific settings are saved in an "open schema extension". This is a user data extension that can be created and deleted dynamically. This is not a schema extension as known from LDAP-based directory systems.

Note!

There is currently no automated way of transferring the user-specific data from OfficeMaster 6 and OfficeMaster 7 to the OfficeMaster 8 scheme.

If there is a need to do this for a large number of users so that this can no longer be managed using the standard configuration tools, then we ask you to contact the Ferrari electronic AG hotline () to get in touch.

7.7. Technical references and downloads

7.7.1. Technical references

More technical articles can be viewed at the following web address: http://ferrari-electronic.de

Ferrari electronic AG operates a partner forum. To register for the forum, please contact your responsible partner account manager. http://forum.officemaster.de

7.7.2. Additional articles from Microsoft

Registering applications in the cloud

https://docs.microsoft.com/de-de/azure/active-directory/develop/scenario-desktop-app-registration

Support for Basic Authentication

https://developer.microsoft.com/en-us/office/blogs/deferred-end-of-support-date-for-basic-authentication-in-exchange-online/

Turn off basic authentication in Exchange Online

https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/disable-basic-authentication-in-exchange-online

8. OfficeMaster Suite call routing

The OfficeMaster Suite can, through flexible routing of the calls, can be used very well in complex environments.

If you take into account some basic properties of the solution and have a template of when which call should be handled and how, nothing stands in the way of a successful setup.

8.1. The messaging server

The OfficeMaster Suite consists of the messaging server, which does not single program is, but made up of different components composed. It is between the basic components that the ensure the basic process and operation and the transmission and receiving components and the connectors are distinguished. All Components communicate directly with the controller (CTRL). This central unit is responsible for job handling.

A closer look at the connections in the messaging server is provided you in section *2.2. architecture of the OfficeMaster Suite*.

8.1.1. Registration on the controller

All components register on the controller in order to be there store the type of news you are interested in. Based on these registrations, the controller maintains a Routing table to route messages to the correct component forward.

The following properties are stored with the registration:

- Job type, like SMS, Fax, NGDX, Voice
- Message input format, such as PDF, RTF, DOCX
- Output message format, such as PDF, BFF
- Destination phone number, sender phone number, ...

Example 3.1.

Target:

A message received from the e-mail system with an attachment (Word file) Should be sent as a PDF via SIP.

sequence:

A SIP component is registered on the controller for everyone Destination numbers and the requirement that messages be both PDF can also be sent as a BFF. The controller is looking for a registered component that converts the received email to PDF and BFF can convert. Therefor can be found in the registrations, for example, a converter that Can perform HTML to PDF, DOCX to PDF, and PDF to BFF steps. Based on this, the controller calculates a routing in which the job Is routed first to the converter and then to the SIP component.

Unambiguous and ambiguous decisions

Basically, it is necessary to consider the nature and direction of each call. With incoming documents, fax messages or SMS messages, it is possible that more than one destination has been defined in the Messaging Server of the OfficeMaster Suite. This “duplication” occurs most commonly when using archive solutions. Incoming messages are usually transmitted to the recipient(s) and additionally placed in an archive.

With such solutions, it must be precisely defined when calls and the messages transmitted with them are to be accepted. If unknown destination numbers are to be blocked, it may be necessary to maintain these addresses in two places.

The situation is different when receiving voice messages or calls. Here the call acceptance decision and the associated behavior are based directly on the voice profile stored in the directory. The decision to use the connector must be unique.

In the case of outgoing messages, several sending components can register for the associated dispatch, but in the end only one call is established.

8.2. Incoming calls

This section is about calls from the telephone network to the messaging server. Here are the recognized faxes, documents, short messages or voice messages forwarded to the appropriate special connectors.

Entry components into the messaging server for incoming calls are accordingly SIP, OMCUMS and also SMPP (for SMS).

Call acceptance decision:

1. Header manipulation (SIP, SMPP only)
2. Number manipulation (SIP, SMPP)
3. Routing/service selection incoming (ISDN/SIP)
4. Number manipulation (ISDN/SIP)
5. Query on the controller blacklist/whitelist
6. Query on the connector as to whether a phone number is available
7. Handover to controller (all)

8.2.1. Manipulation of the SIP header (SIP, SMPP)

According to the SIP RFC, various places in the SIP header are possible, e.g. call forwarding information. It is also not always clear which job parameters from the OfficeMaster Suite are to be transferred to the SIP header and where should be transferred. One can make the appropriate assignments in the SIP header area. If you selected a profile that matches your connection when you created it, you will normally not have to adjust these settings, as this has already been done by the wizard.

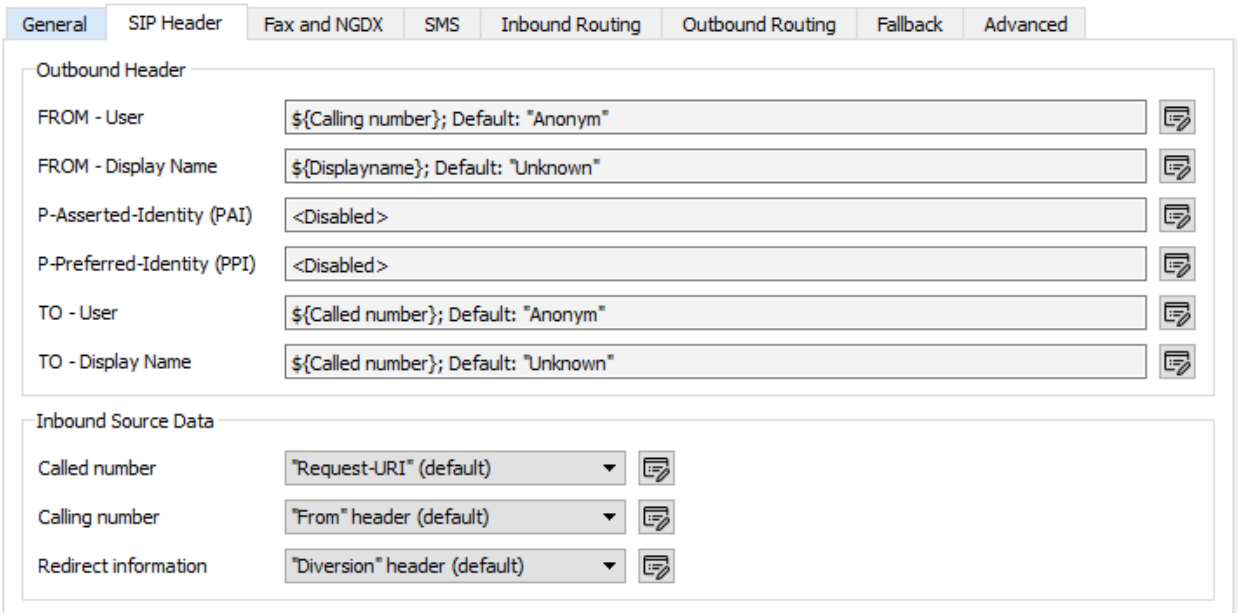


Figure 8.1: Advanced settings for the SIP header

Outgoing calls - SIP header

The processing of the SIP headers for outgoing calls also uses settings from this dialogue, but a description follows in a later section.

Incoming calls - source data

For incoming calls, the (NGDX/Fax/Voice/SMS) job in the OfficeMaster Suite evaluates the SIP header. It depends on the remote station in which fields the call information is to be transferred.

Here you enter the corresponding source data for the three values used by the OfficeMaster Suite *Called Party Number*, *Calling Party Number* and *Redirecting Number*.

If you were able to select a template for your IP trunk when you configured the SIP component, these settings are normally correct and do not need to be adjusted.

> **Note!**
> However, if an adjustment is necessary in your environment, you can open a dialog by clicking on the pencil icon to open a dialog for editing the assignment

Adjust SIP header dialog

For the assignment (also called mapping), you can specify various fixed values or also transport contents that are dependent on the respective job and thus flexible.

Depending on the selected entry under Type of value, the available options are as follows:

Type of value - Fixed value

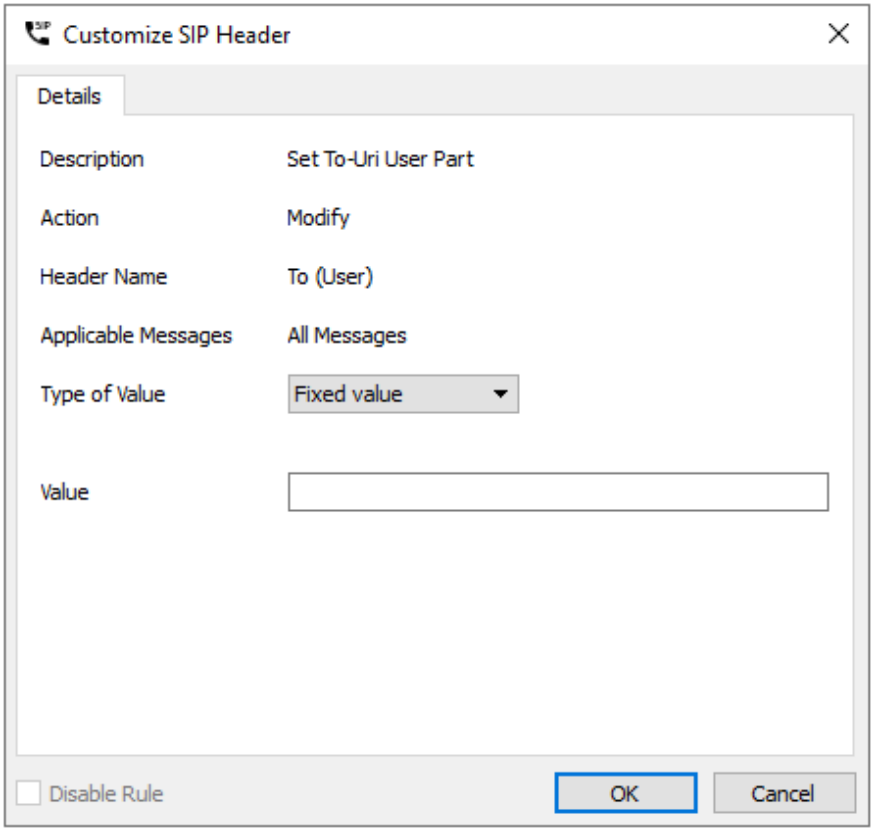


Figure 8.2: Write a fixed value in a header field

Attributes

Here you can enter a fixed value, for example a central sender phone number.

Type of Value - Attributes

Do you want an attribute from the job parameters of the OfficeMaster Suite or a fixed value from the general settings for this field, you can configure it here.

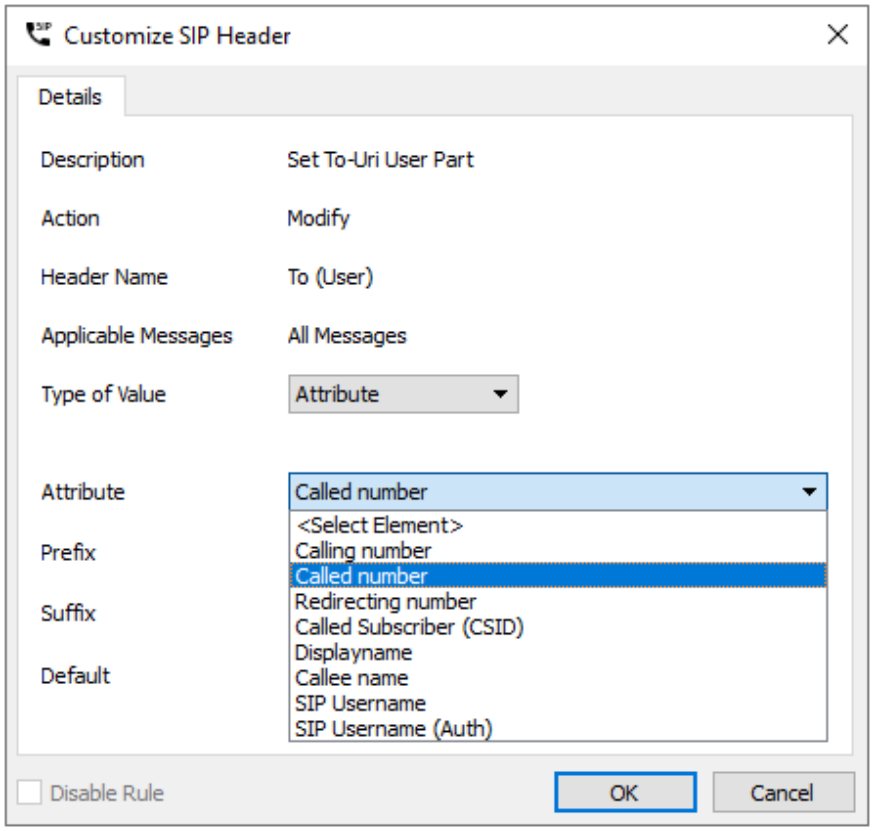


Figure 8.3: Type of value based on an attribute

Attributes

Here you select the attribute from which the value for the field in SIP header should be used. Available attributes are in the Image listed above.

Prefix, suffix

You can assign a fixed prefix or suffix to the attribute.

Default value

If it is not possible to read from the attribute because it is empty or not present in the job, you can specify a default value here.

> Note!
> If you want to configure a sender-based OAD, you can enter as the default value, for

example,the SIP user name and use as attribute the *Calling Party Number* as an attribute.

Type of value - Regular expression

Regex match

Here you can define a matching rule. The following rule e.g. matches all phone numbers with three digits after ...*455*

(\+493328455) (\. . .)

With the expressions in brackets you divide the phone number into two (at least in this example) applicable blocks.

Regex replace

Enter the target value here. By *\1*, *\2* and so on reference the saved blocks.

If we take the above example, you can replace *\191* with the Value *+49332845591* for all calls matched by the regex match rule reach.

Default value

+49332845590

If it is not possible to specify a value based on the source and the regular expression, the default value here will be used.

8.2.2. Number manipulation (SIP, SMPP)

Then the messaging server checks whether replacement rules have been configured (under Advanced > Replacement rules). These are then applied.

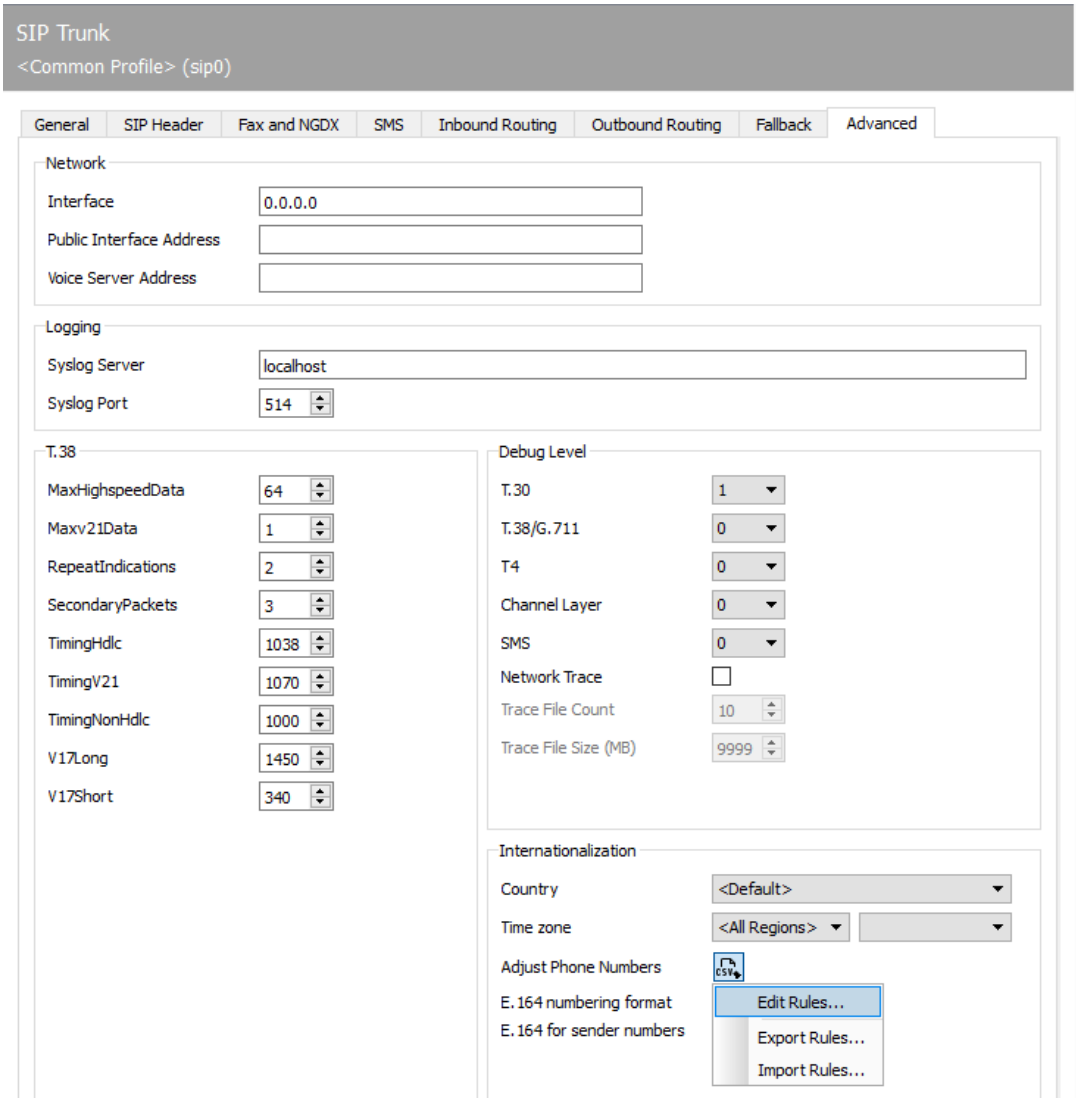


Figure 8.4: Extended settings with the possibility of phone number manipulation (SIP)

Replacement rules

Here you can store replacement rules. These rules exchange the characters of a phone number against other characters or delete them. This option is particularly useful in the following situations:

- To make calls to an internal number even when specifying the full number Internal phone number for example: 03328455 should not be changed.
- For a choice of provider for calls to certain countries.
- To avoid contingencies and gaps of the automatic correction.

Via the button selected in the figure above and with the Selecting *Edit Rules...* takes you get to the setup interface. From there, select *Add...* to create new rules.

The overview provides rules for incoming and outgoing messages separately. In the illustrated example, a simple correction is shown as an example.

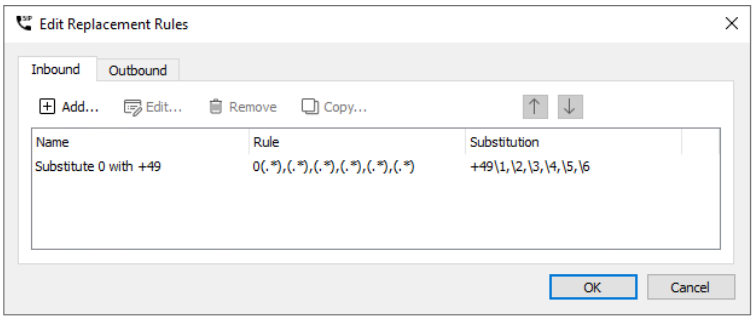


Figure 8.5: Overview of the created rules for manipulating phone numbers for incoming calls

Edit existing rules with “Edit...” or add new ones with “Add...”.

The top-down principle applies to created rules. Rules above are processed first. Regular expressions are used to check whether this rule can be applied to the current call. Only if all expressions on the left-hand side “match” for the call, the call numbers will be processed accordingly. After this step, the call numbers are processed according to the “After applying this rule”, either the next rule will be applied or the processing will be completed.

8.2.3. Routing incoming (ISDN/SIP)

Incoming calls are either blocked or sent as NGDX/fax, SMS or accepted as voice mail. In the *Routing incoming* tab you can decide on the basis of the transmitted phone numbers, how the OfficeMaster Suite should react to the corresponding call. For this the classic telephony features *To (Calling Party Number)*, *Diversion (Redirecting Number)* and *From (Called Party Number)* are available.

> **Note!**
> Which fields from the SIP headers are used to specify exactly these telephony characteristics differs depending on the provider and the type of SIP trunk. If you need to make changes to these assignments, proceed as described in the previous section.

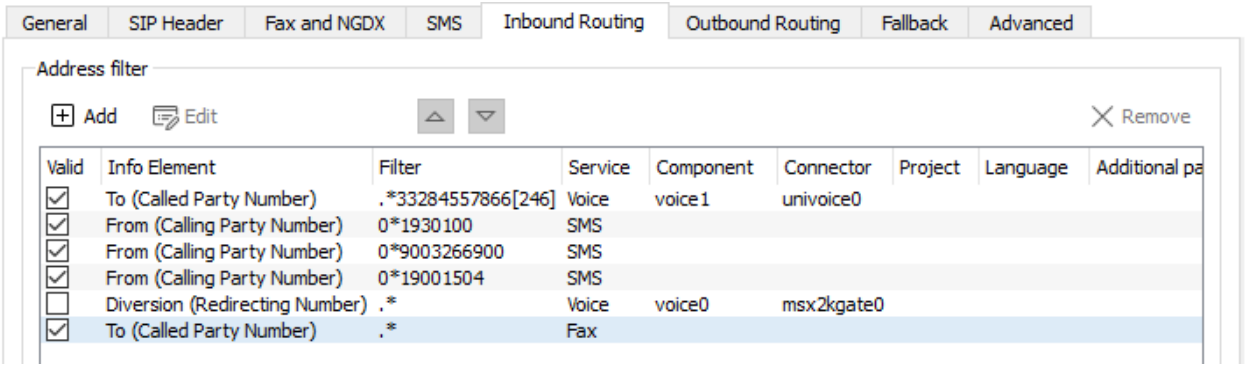


Figure 8.6: incoming service selection or routing

Address filter

The *address filter* is created with a standard assignment.

In order to reliably identify voicemails as such, the number of the redirecting extension (*Redirecting Number*) can be used. Once you get this rule activate, all diverted calls are processed as voicemails.

> **Note!**
> Every call that has not been identified as Voicemail will be received as a fax with this standard assignment.

> **Warning!**
> The OfficeMaster Suite requires an additional license for the simultaneous operation of fax and voicemail. Please note in the rules that the desired service (fax, voice) is also licensed. If routing is performed to a unlicensed service, the call will be rejected.

The assignment of numbers can vary per SIP component or per SIP remote station respectively. Accordingly, you can configure each component differently.

> **Note!**
> Right-click to open the context menu where you can set the factory settings for the service selection.

Add to

The service selection is based on a list of filters, which are successively applied to the information of the call. In the simplest case, a filter consists of the complete phone number.

However, the specification of the complete phone number as a filter is not mandatory, as the filter can also be specified using regular expressions.

The set filters are applied to the received phone numbers one after the other, starting with the first. Incoming calls are handled according to the first matching filter (First Match). With *Move up* and *Move down* the ranking of the filters can be adjusted.

Voicemail detection

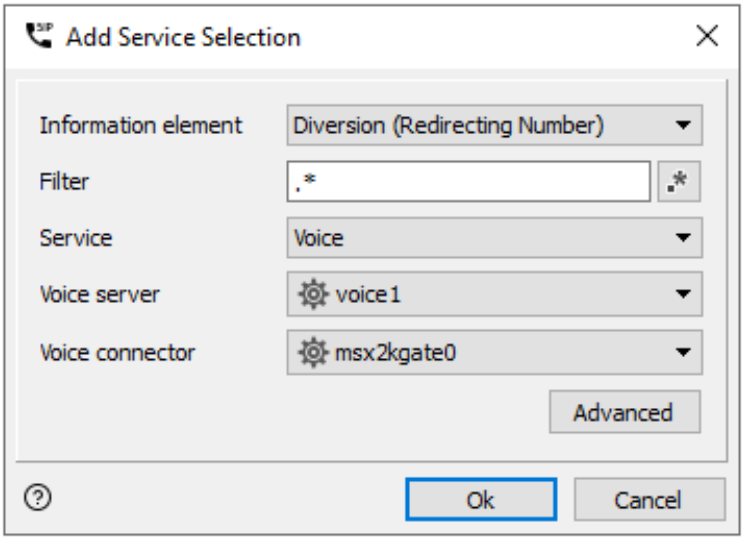


Figure 8.7: Configuration for incoming calls for the Voice service

Information element; filter; service; voice server; voice connector

To recognize voicemails, either the *Redirecting Number*, the *Calling Party Number* or the *Called Party Number* can be used. If the selected information element matches the configured filter, the filter is applied.

For example, if all calls with a three-digit *Redirecting Number* (=internal phone number of the redirecting extension) are accepted as Voicemail, three dots (...) can be used as a filter.

However, if the redirecting number is not available on a point-to-point connection, a separate number range must be provided for voice.

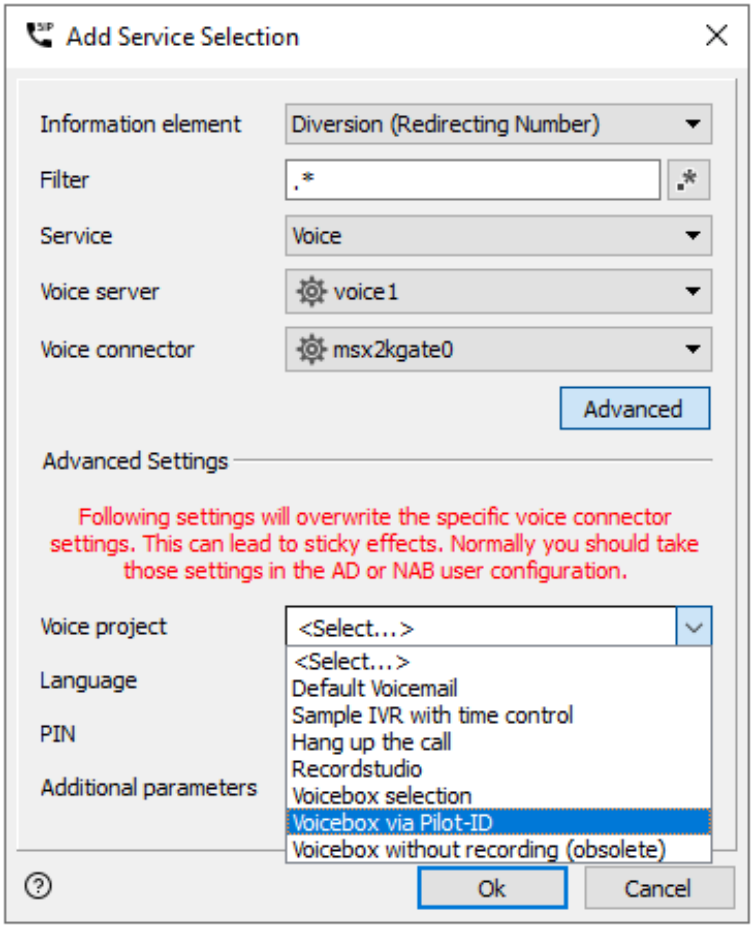


Figure 8.8: Project for "rotating" call forwarding information

So that the transmitted redirecting number can also be used as a destination (*Called Party Number*) , click here on Advanced and deposit the project "*Voicebox via Pilot-ID*". With the help of this Project, the phone numbers are adapted accordingly and then the voicemail project stored at the user is called.

Language, PIN, additional parameters

In special cases, it may make useful for you fill in use these fields. In standard, do not enter anything here.

Detect faxes

At the end of the address filter, i.e. if it is not voicemail, you should set up a filter for the Called Party Number, which ensures that all remaining calls are received as faxes.

> Note!
> When receiving from Messages (fax, NGDX) you do not need to do any further

settings. An incoming document can be fowarded to all connectors that register for the process. A common scenario is, for example, the parallel use of a file interface with the Exchange Connector. The same document is transmitted to both recipients.

8.2.4. Phone number manipulation (ISDN)

The options on the *Advanced settings* tab of the hardware controller allow one to configure the phone number correction to correct and redirect wrong recipient phone numbers.

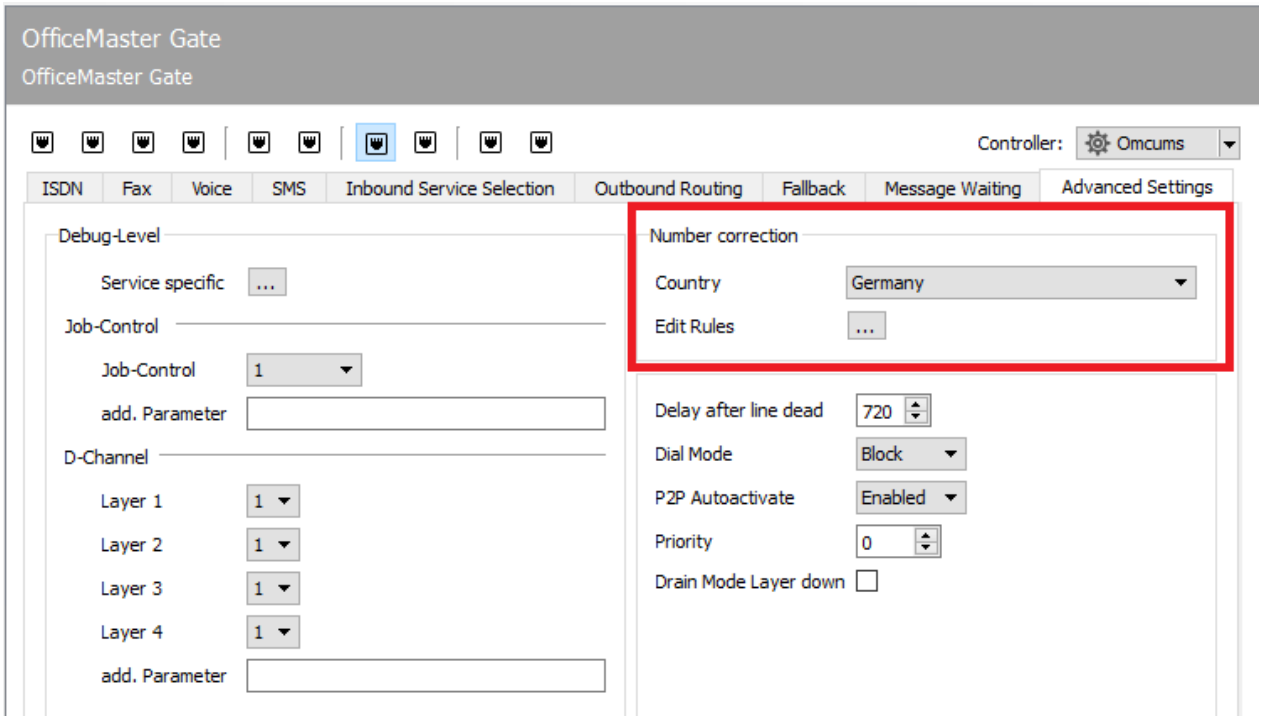


Figure 8.9: Advanced settings

Telephone number correction

OfficeMaster Messaging Server can analyze the call number syntax of send operations and correct the phone number if necessary. It is therefore not relevant for the inbound messages.

Edit rules

As an extension to the automatic correction, a substitution table can be maintained, which exchanges or deletes the characters of a phone number against other characters.

The corresponding configuration interface is reached via the Edit rules button. These settings are only valid for the selected ISDN channel. It is possible to edit rules for incoming and outgoing calls in various ways, adding or deleting them.

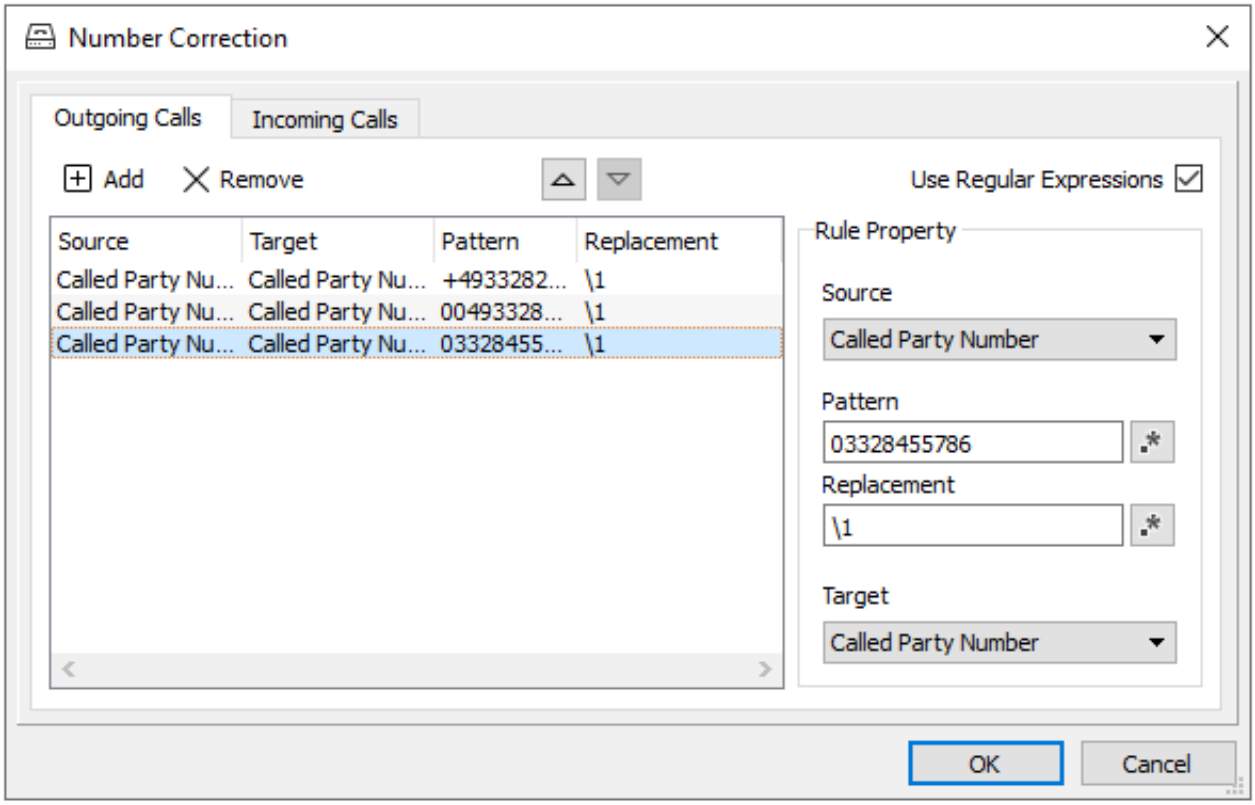


Figure 8.10: phone number correction; replacement table

Example 3.2.

The Ferrari electronic AG telephone system in *03328* Teltow has it Root number *455* and three-digit extensions. A fax/NGDX or Voice call to the number *03328-455-200* would work even with activated number correction. It will inevitably be handled through the office, though it is the internal subscriber *200*. With that OfficeMaster calls to this number can still be made internally in the replacement table stores with listed prefixes without replacement:

- *+493328455, 00493328455, 03328455, 455*

As a result, processes whose phone numbers start with the above/begins with the specified characters, removes the specified character strings and replaced with the values entered in *replacement*. Consequently the processes in this example are communicated internally.

Note!
The substitution table can only with activated phone number correction (*Use Regular Expressions*) be used.

Use of blacklist

Via the configuration interface (“Tools/Extras” > “Blacklist/Whitelist”) of the messaging server a global phone number list can be stored. The list can be used either as a blacklist or as a whitelist.

It is important to know that this list does not distinguish between individual components and only one phone number, that of the external subscriber, is taken into account.

The lists are TXT files. To create the tool “Directory Service” is suitable for the creation of the lists. LDAP-capable directories, such as Active Directory, can be read out according to certain criteria.

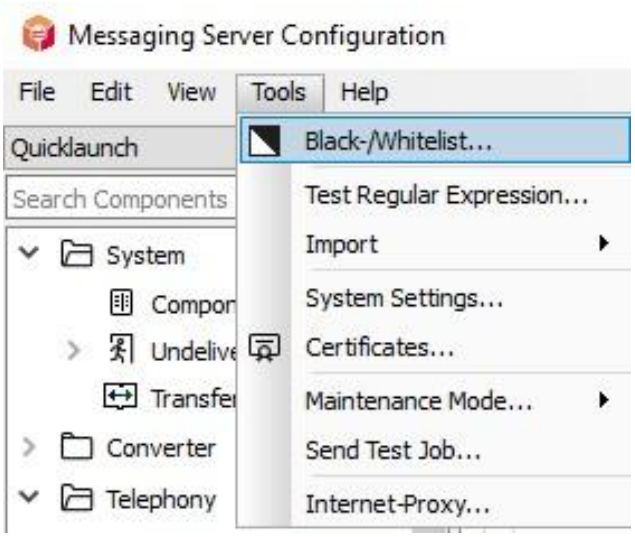


Figure 8.11: calling up the black/white list

Shortly before the call is put through, the call number runs through a *blacklist/whitelist* (can be stored under Tools > Blacklist/Whitelist...). This will now sort out the call number.

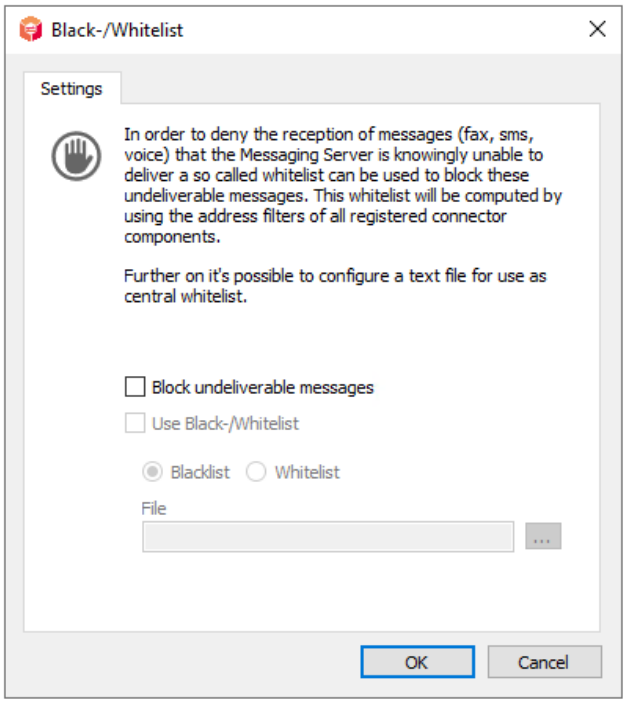


Figure 8.12: Inbound phone number manipulation

Number resolution using the example of the Exchange Connectors

The user resolution of the incoming information of the Exchange and the BCS Connector uses the following information for incoming fax documents to resolve the sender:

1. The CSID of the sender is entered
2. If the CSID is empty, the sender phone number is used
3. If the sender phone number is empty, “Fax-Connector” will be used

Insert: phone number normalization

A normalized search normalizes the source number and the Search number:

1. E.164 is converted to 0 prefix.
2. Leading zeros are removed.
3. Alphanumeric characters are removed.

Example 3.3.

Number Search Number Found

+493328455960 => +49 (03328) 455 -960

=>03328455960 => 0(03328)455-960

=>3328455960 => (3328)455-960

=>3328455960 => 3328455960

The following steps are processed to resolve the recipient

Is the metacache used?

If yes, the data is searched for. In the metacache will be all call digit normalized searched.

If nothing was found, the next step is to look in Active Directory.

The search in Active Directory

Domains are determined according to the domain list.

Global catalog is opened alternatively.

A subtree search is then performed either in the domain or in the GC, in which an object is searched, whose last digits matches with the end of the data content. From the search string the first three alphanumeric characters are removed.

Example:

CSID = +493328455960 => 3328455960 => results in the following search:

(|(proxyAddresses=FAX:*3328455960)(facsimileTelephoneNumber=*3328455960)
(telephoneNumber=*3328455960)(homePhone=*3328455960)(mobile=*3328455960))

Sender name resolution

Same as during the resolution of the recipient, initially the identification of the sender is attempted.

The extended name resolution of the sender is set with the option *by Exchange connector*. If this is the case, it follows these criteria:

Search in the public folders

The following procedure applies when searching in the public folders:

- Public Folder Root is opened via Exchange Web Services.

- Recursive search is performed over the accessible public folders.
- A normalized search is carried out in the phone number fields.

Search recipient user's private folder

The following procedure applies when searching in the Private Folder Store:

- Private Folder Root "Contacts" is opened via Exchange Web Services.
- A recursive search is performed via the subfolders.
- A normalized search is carried out in the phone number fields.

8.3. Outgoing calls

Outgoing calls, fax, voicemail are unique, one destination. If there are multiple registrations for one a job, the highest priority applies. In case of equal priorities:

- the first channel filled until it is full, then the next.
- There is a distribution based on the utilization across all available channels.

8.3.1. Order of processing

1. Registration on the controller (all)
2. Internationalization (all)
3. Number manipulation (SIP, SMPP)
4. Telephone number manipulation (ISDN)
5. SIP header manipulation (SIP, SMPP)
6. Fallback (all)

8.3.2. Define registration on the controller

All components of the OfficeMaster Suite register for specific tasks on the controller.

When installing with multiple telephony interfaces (different ISDN channels, multiple SIP trunks, ...), send jobs are distributed to the available interfaces depending on the workload.

In most installations with multiple interfaces, the routing of the calls should not be done randomly across the interfaces. With the help of regular expressions, you can create appropriate routing rules based on the destination and the sender.

If you create the SIP and OMCUMS type components and configure them without any outgoing routing or without any restrictions, outgoing calls will be randomly distributed over the available channels. Related to an installation with multiple SIP peers, e.g. in case of redundant PBXs or when using multiple SIP providers with equal rights, you can achieve load balancing and at the same time automatic selection of the currently available transmission path.

Routing distinguishes between the service types fax, voice, SMS and MWI. For all there is a distinction between recipient and sender. For each individual service it is possible to check whether the currently configured component is setting up external calls.

Useful regular expressions:

- -.* prevents the match of all phone numbers

- .* matches all phone numbers

Note!
With the settings under the *Fallback* tab you can use this SIP component for register the fallback behavior.

Here you can set outbound routing for NGDX and Fax, Voice, SMS and MWI usually as *Least Cost Routing* or as *Location Based Routing*.

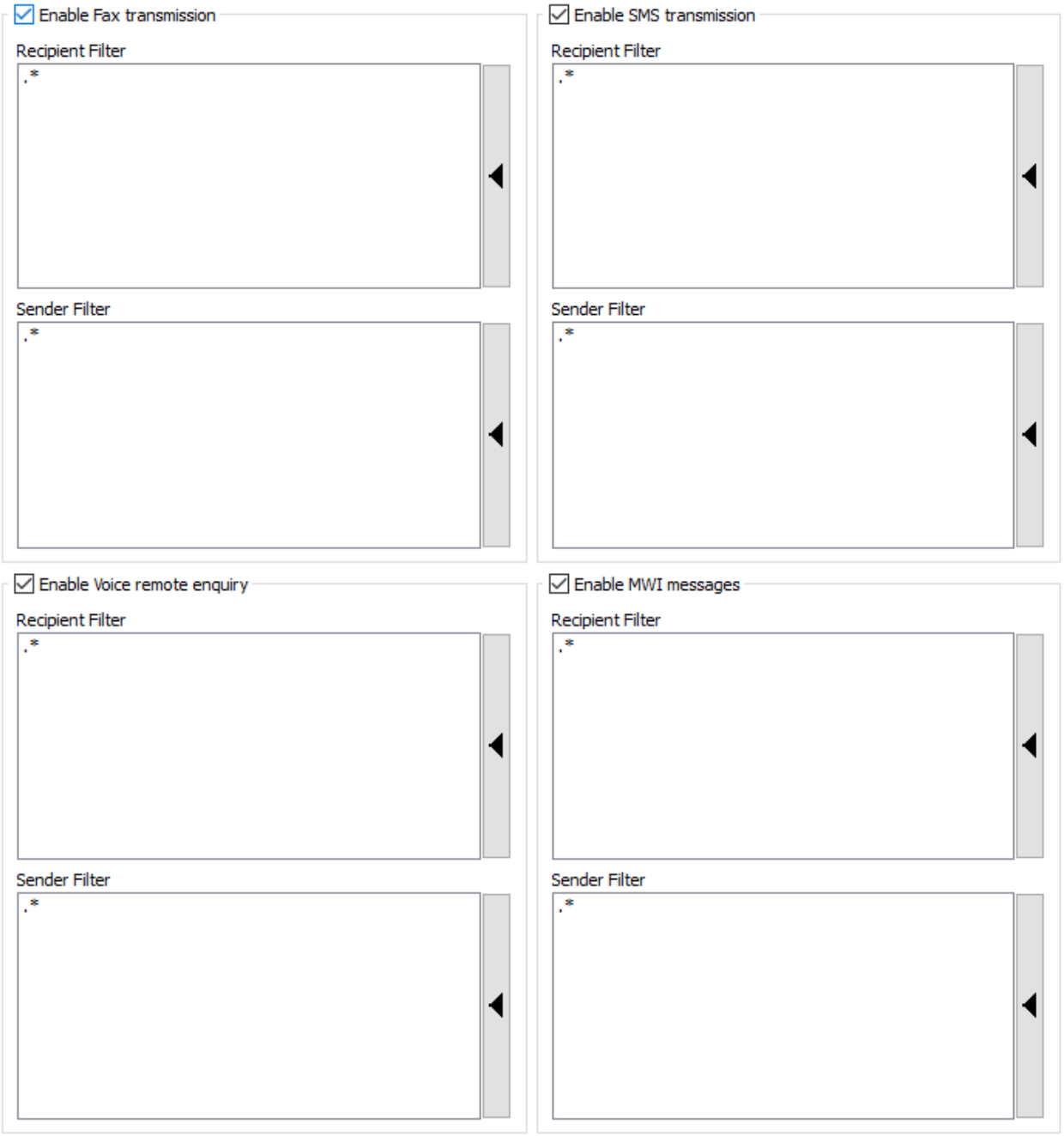


Figure 8.13: Default settings for outbound routing

Least Cost Routing

Send orders are sent via the SIP connection that causes the lowest transmission costs to the recipient.

Location Based Routing

Location Based Routing takes place using the sender information. In the simplest case, the sender information is the NGDX/fax or Sender's voice number.

Since the liberalization of the German telephone market, least cost routing has only been profitable on an international level. Different IP connections of an OfficeMaster Suite within a country are usually set to location-based routing, which means that the transmission costs are incurred. Location Based Routing is also increasingly used internationally.

8.3.3. Internationalization

With internationalization, the phone numbers are normalized to the format valid for the respective telephone channel (SIP trunk or ISDN connection). The country identifier can be configured per D-channel (ISDN) or SIP trunk.

With internationalization, parentheses, spaces, special characters and also the national country code (depending on the location) are removed.

For example, the "0049" or even the "+49" is always removed for calls via a German connection and only the normalized local number is used.

The internationalization is much easier to handle than the number manipulation described in the previous section, but not nearly as powerful.

Examples of phone number manipulation with the country setting DE/Germany (+49):

phone number before Internationalization	**after successful internationalization**
+49(3328) 455 960	03328455960
+49 3328 455 960	03328455960
+43(123) 456 789	0043123456789
03328455960	03328455960
0043123456789	0043123456789

If you do not set a country identifier, the call numbers must be entered in full on the OfficeMaster Gate or the SIP components (beforehand in the call number manipulation).

You can take a more detailed look at the effects of internationalization in the configuration under International (Tools > System settings). Here you will find the adjustments for different countries. If required, this can of course also be adjusted.

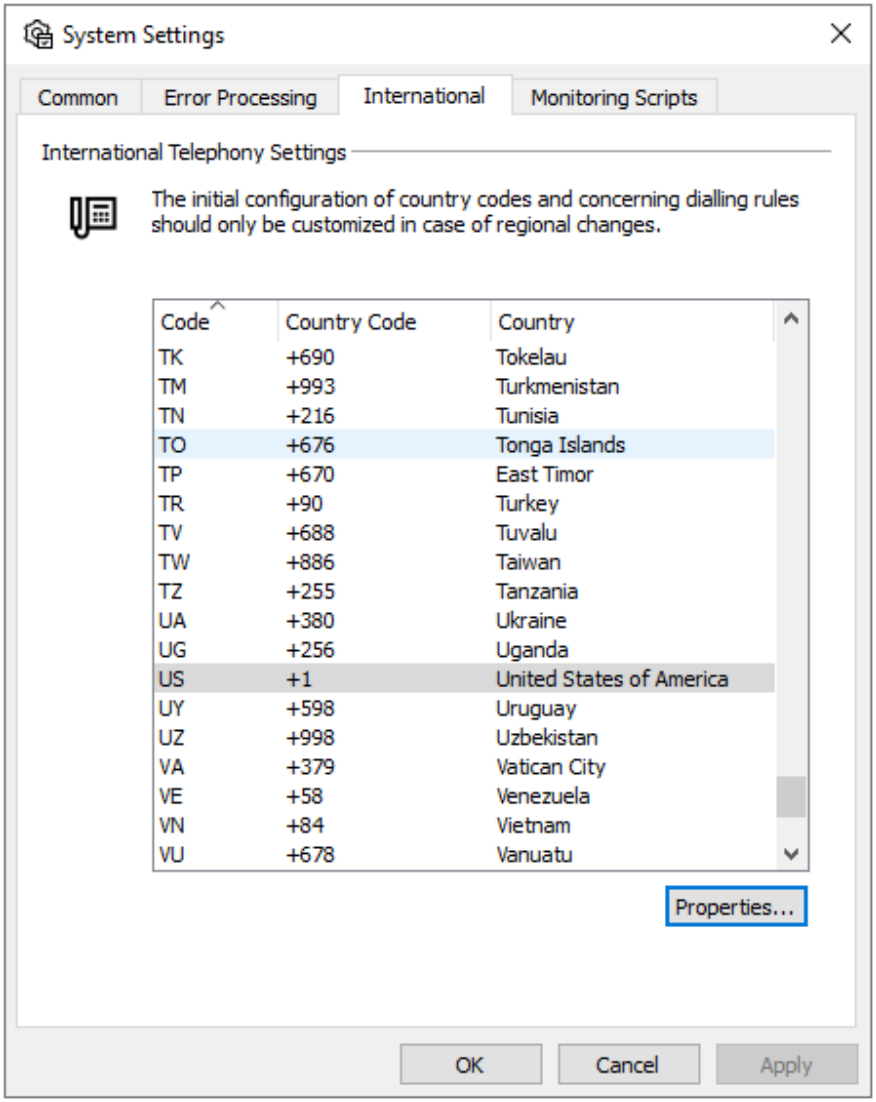


Figure 8.14: Internationalization with phone number manipulation

Select the desired country and click on *Properties* to see the specific settings and edit them if necessary. For example, in the United States, 011 it´s used nationally preselected. Should the OfficeMaster stand behind a TK and this already take over? Then one can adapt this accordingly so that the system processes the call correctly.

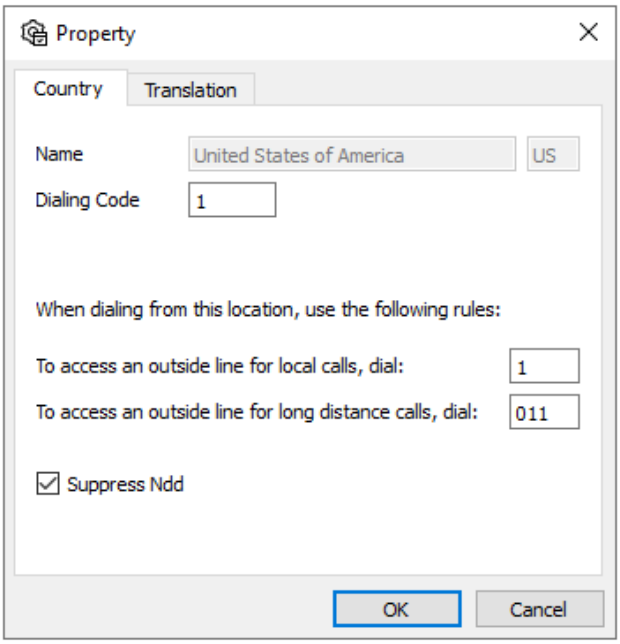


Figure 8.15: Telephone number correction for lines in the United States

Warning!

Another special feature is available for the Exchange Connectors, where an additional correction can be activated. If the country code is set to "+49", the additional "0" after the country code address books is removed.

Examples of phone number manipulation with the country setting DE/Germany (+49):

Phone number before correction	**After the correction**
+49(0) 3328 455 960	03328455960
+43(0)123456789	0043123456789
+39(0)123456789	0039123456789

The latter example shows the correction for a call to Italy. For Italy it is necessary that the "0" in front of the area code is always dialed. For this example this would mean that the following number would be required: "00390123456789". Therefore we do not recommend to enter the country code at the connector and to make sure that it is empty on the Exchange Connector!

If the phone numbers in the address books of the users are maintained in this non-standard format with the zero in parentheses, it is recommended to use the rules with number correction on the OfficeMaster Gate or the SIP component or, even better, to correct the database.

Time zone

The time zone to be set separately via continent and city has no influence on the handling of the phone numbers.

However, the time zone is decisive for the time stamp on the fax messages. If you have configured the operating system to a different time zone than the one that makes sense for the messages, you must make the appropriate setting here.

With a central solution for internationally (or across several Time zones) distributed users can the correct time zone can thus be selected on the basis of the SIP trunk.

8.3.4. Number manipulation (SIP, SMPP)

The messaging server then checks whether replacement rules (under Advanced > Replacement Rules) have been configured. These are then applied.

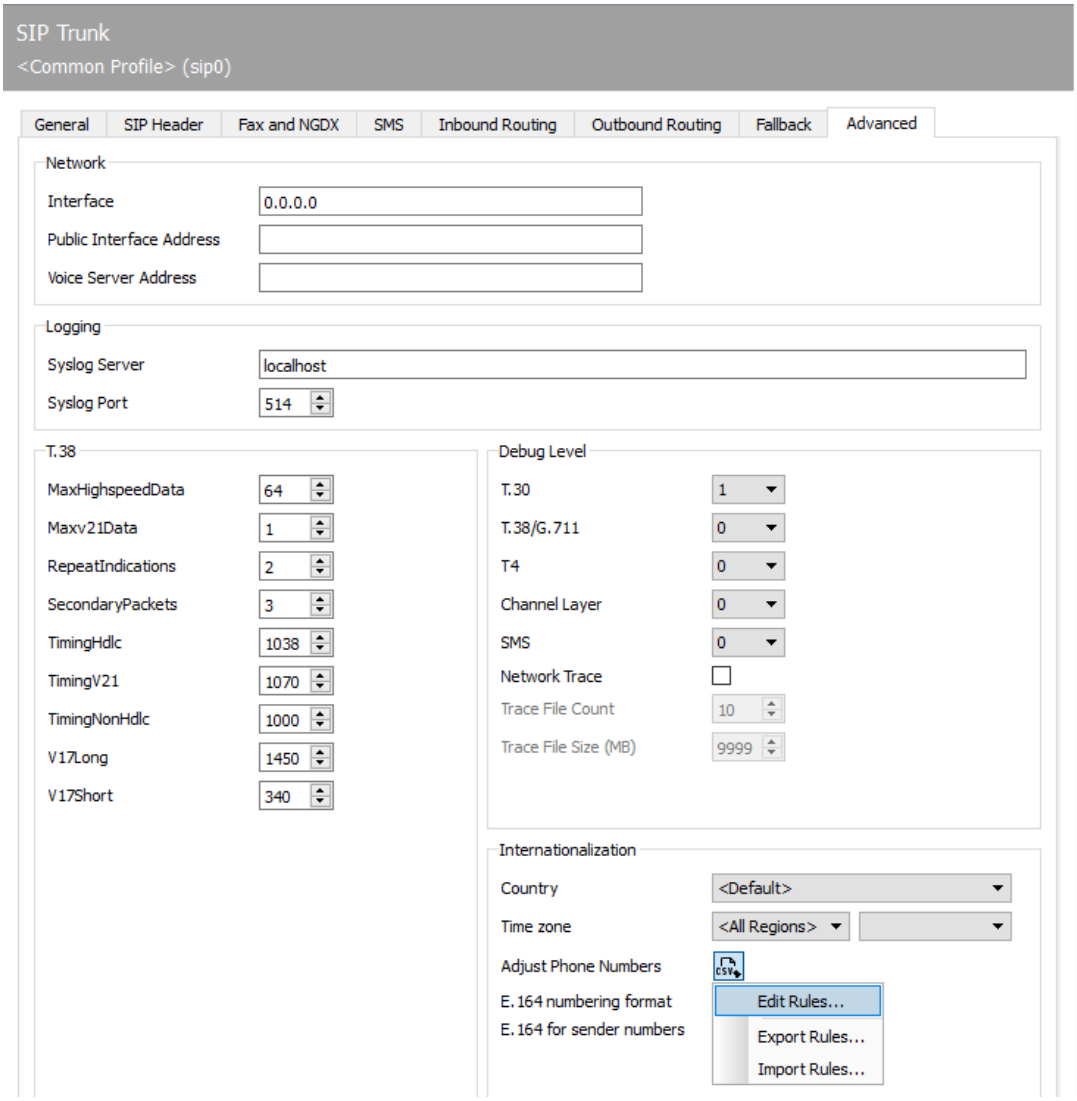


Figure 8.16: Extended settings with the possibility of phone number manipulation (SIP)

Replacement rules

Here you can enter replacement rules. These rules swap the Replaces or deletes characters in a phone number with other characters.

This option is particularly useful in the following situations:

- To make calls to an internal number even when specifying the full Internal phone number for example: 03328455 should not be changed.
- For a choice of provider for calls to certain countries.
- To avoid contingencies and gaps of the automatic correction.

Via the button selected in the figure above and with the Selecting *Edit Rules...* takes you to the setup interface. Select *Add...* to get an overview of the created rules.

The overview provides rules for incoming and outgoing messages separately. The example shown is a simple correction.

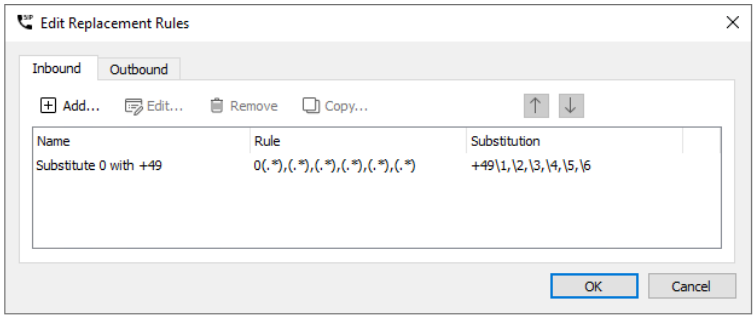


Figure 8.17: Overview of the created rules for manipulating phone numbers for incoming calls

Edit existing rules with “Edit...” or add new ones with “Add...”.

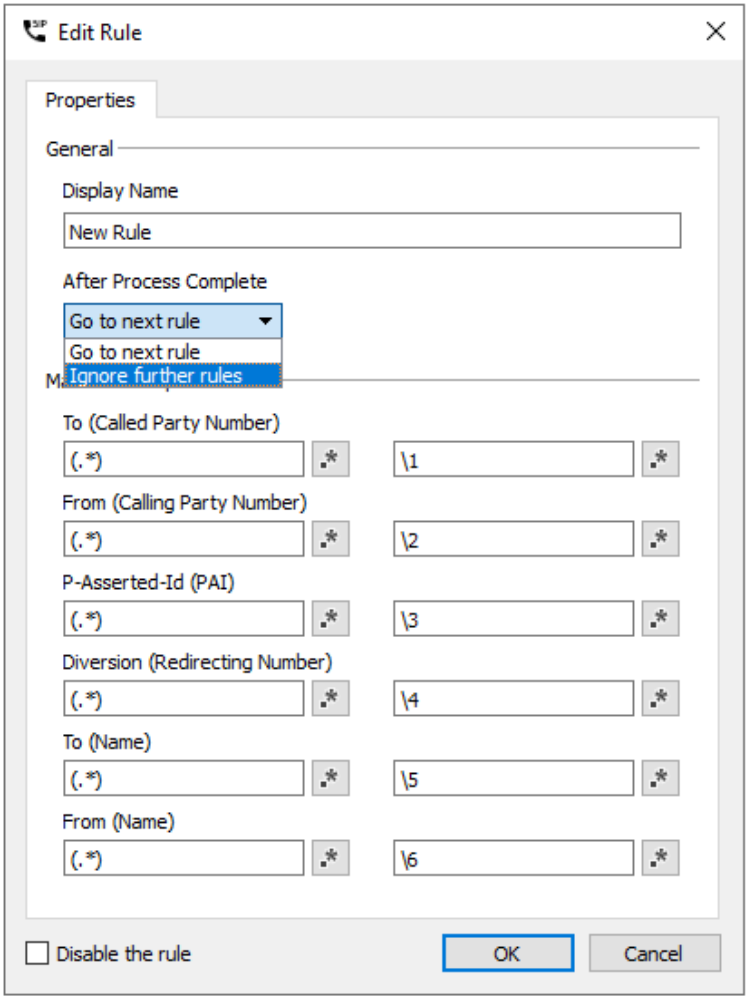


Figure 8.18: dialog for editing a rule

The top-down principle applies to created rules. Rules above are processed first. This is done using regular expressions to check whether this rule can be applied to the current call. Only if all left-hand expressions “match” for the call, the phone numbers are processed accordingly. After this step, either the next rule is applied or the processing is completed, depending on the processing.

8.3.5. Telephone number correction (ISDN)

OfficeMaster Messaging Server can analyze the call number syntax of send operations and correct the phone number if necessary.

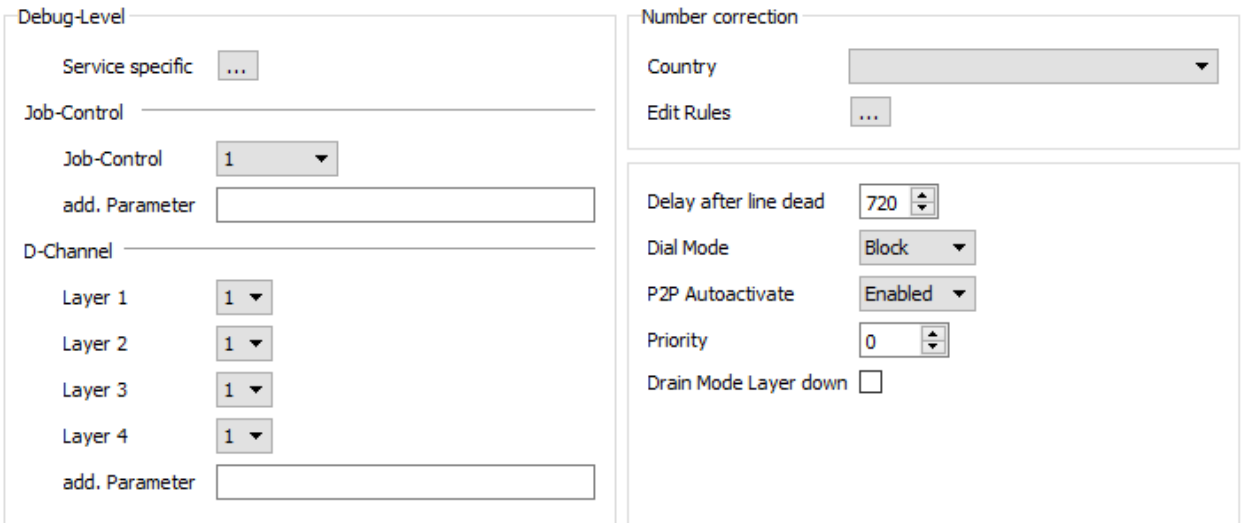


Figure 8.19: Advanced settings on the hardware controller

Edit rules

As an extension to the automatic correction, a substitution table can be maintained, which exchanges or deletes the characters of a phone number against other characters.

This may be necessary:

- To make calls to an internal number even when specifying the full internal phone number for example: 03328455 should not be changed.
- for provider selection for calls to certain countries.
- for call by call (*3U > 01078*; if supported by the gateway)
- to close eventualities and gaps in the automatic correction.

The corresponding configuration interface is reached via the Edit rules button. These settings apply only to the selected ISDN channel. Rules for incoming and outgoing calls can be edited, added and deleted in various ways

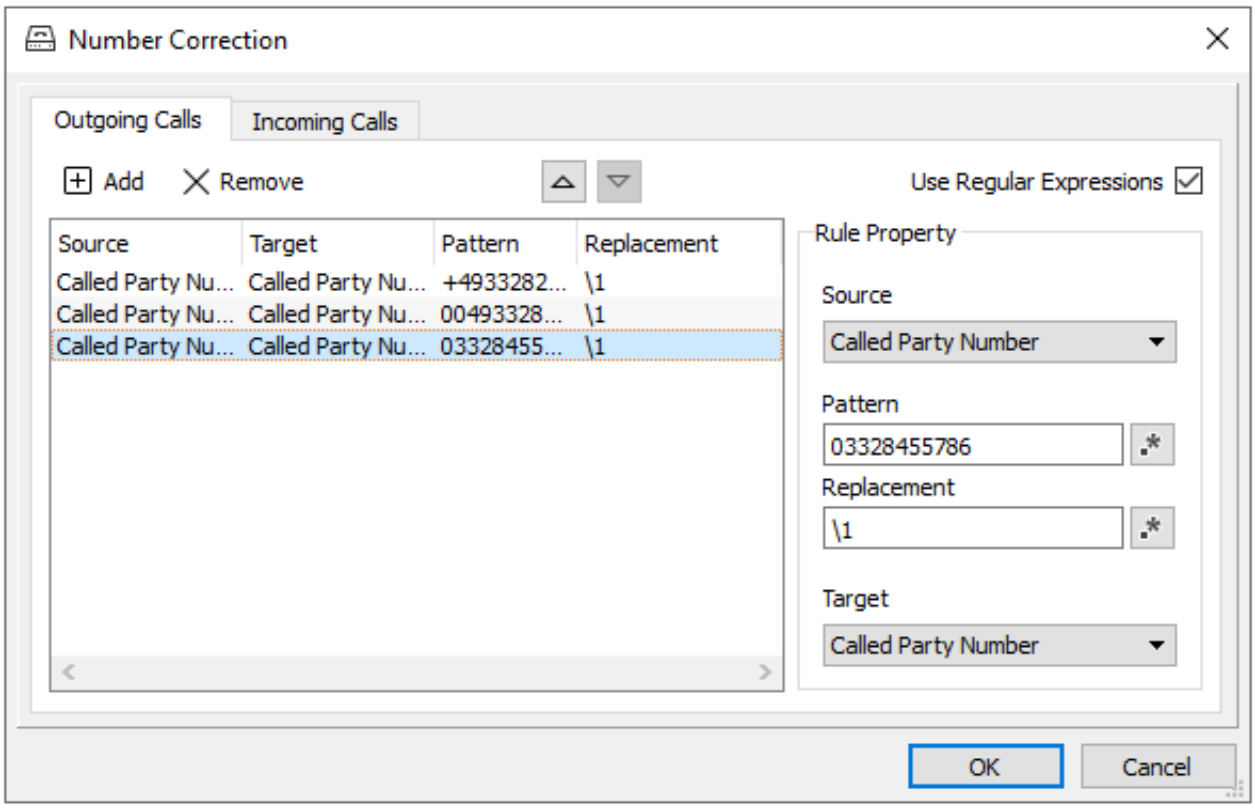


Figure 8.20: phone number correction; replacement table

Example 3.4

The telephone system of Ferrari electronic AG in 03328 Teltow has the root number 455 and three-digit extensions. A fax or voice call to the number 03328-455-200 would, even with activated number correction, inevitably be handled via the the exchange, even though it is the internal subscriber 200. So that OfficeMaster can nevertheless make calls to this number internally to this number, the listed prefixes are stored in the substitution table without substitution:

- *+493328455, 00493328455, 03328455, 455*

As a result, for operations whose phone numbers start with the above-mentioned characters, the specified strings are removed and replaced by the values entered in Substitution. Thus the operations in this example are switched internally.

Note!

The substitution table can only be used with activated phone number correction (*Use Regular Expressions*).

8.3.6. Manipulation of the SIP header (SIP, SMPP)

According to the SIP RFC, various places in the SIP header are possible, e.g. Call forwarding information. It is also not always clear which job parameters from the parameters from the OfficeMaster Suite are to be transferred to the SIP header and where should they be transferred. You can make the appropriate assignments in Advanced mode under SIP Header. If you have selected a profile that matches your connection when you created it, you will normally not have to adjust these settings, as this has been done by the wizard.

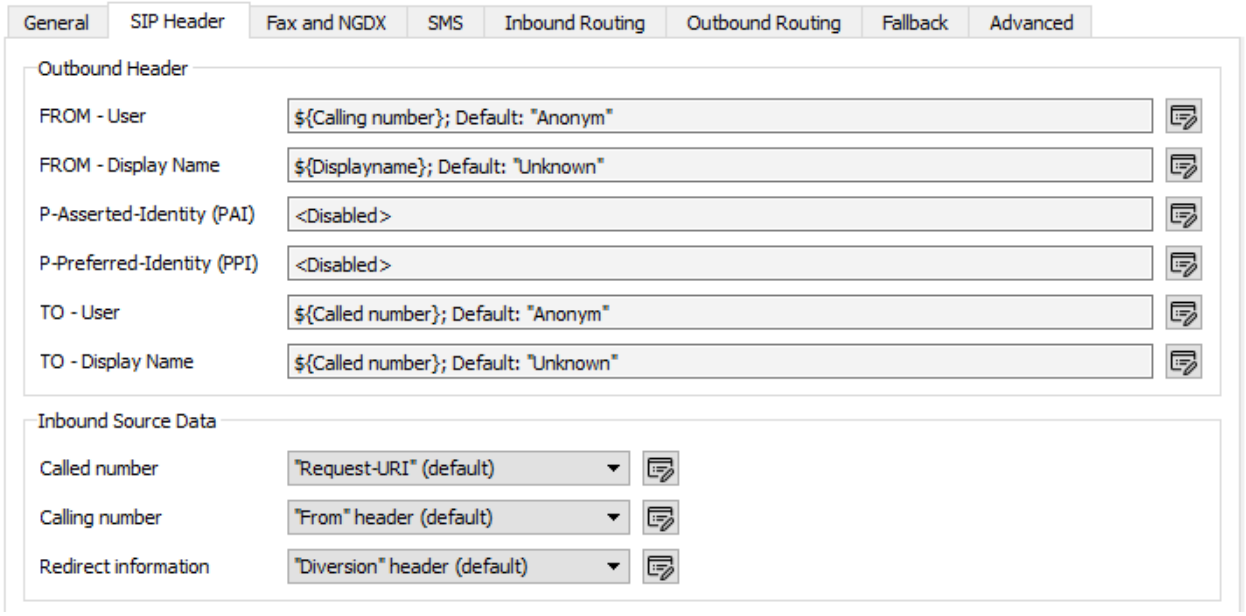


Figure 8.21: Advanced settings for the SIP header

Outgoing calls - SIP header

For outgoing calls, the (fax/voice) job in the OfficeMaster Suite uses the SIP header, depending on the Remote station, to fill in up to six fields. By clicking on the “Edit” button, you can edit the values in the dialog that opens to adjust.

This option affects the following SIP header attributes:

- FROM - users
- From - DisplayName
- P-Asserted Identity (PAI)
- P-Preferred Identity (PPI)
- TO - User
- TO - user name

Depending on the selected entry under *Type of value* follow options are available:

Type of value - Fixed value

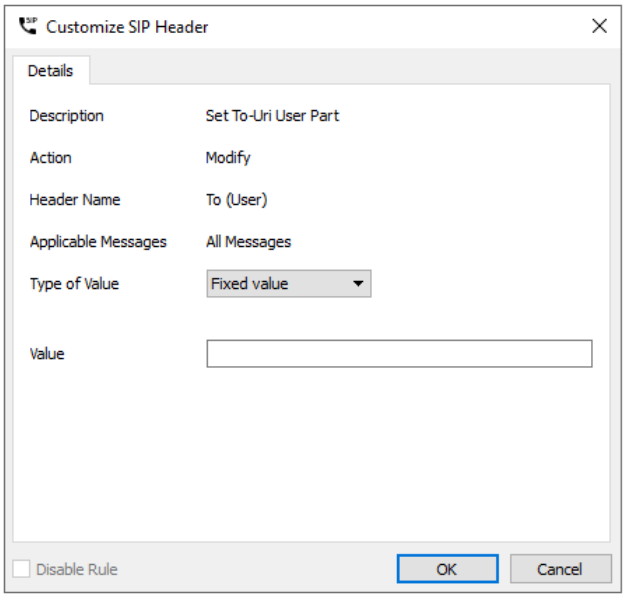


Figure 8.22: Write a fixed value in a header field

Attributes

Here you can enter a fixed value, for example a central Enter sender phone number.

Type of Value - Attributes

Do you want an attribute from the job parameters of the OfficeMaster Suite or a fixed value from the general settings for this field, you can configure it here.

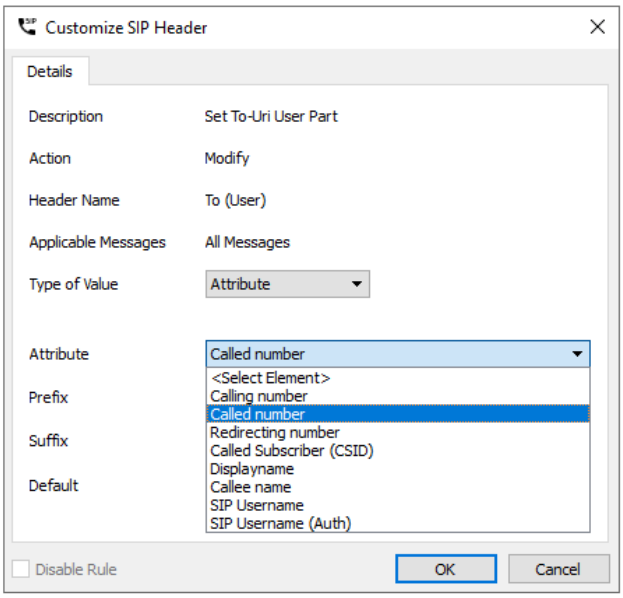


Figure 8.23: Type of value based on an attribute

Attributes

Here you select the attribute from which the value for the field in SIP header should be used. Available attributes are in the Image listed above.

prefix, suffix

You can assign a fixed prefix or suffix to the attribute.

Default value

If it is not possible to read from the attribute because it is empty or not present in the job, you can specify a default value here.

> Note!
> If you want to configure a sender-based OAD, you could use the SIP user name (default value) and use the *Calling Party Number* as an attribute.

Type of value - Regular expression

Regex match

Here you can define a matching rule. The following rule For example, matches all phone numbers with three digits after *...455*

(\+493328455)(\...)

With the expressions in brackets you divide the phone number into two (at least in this example) applicable blocks.

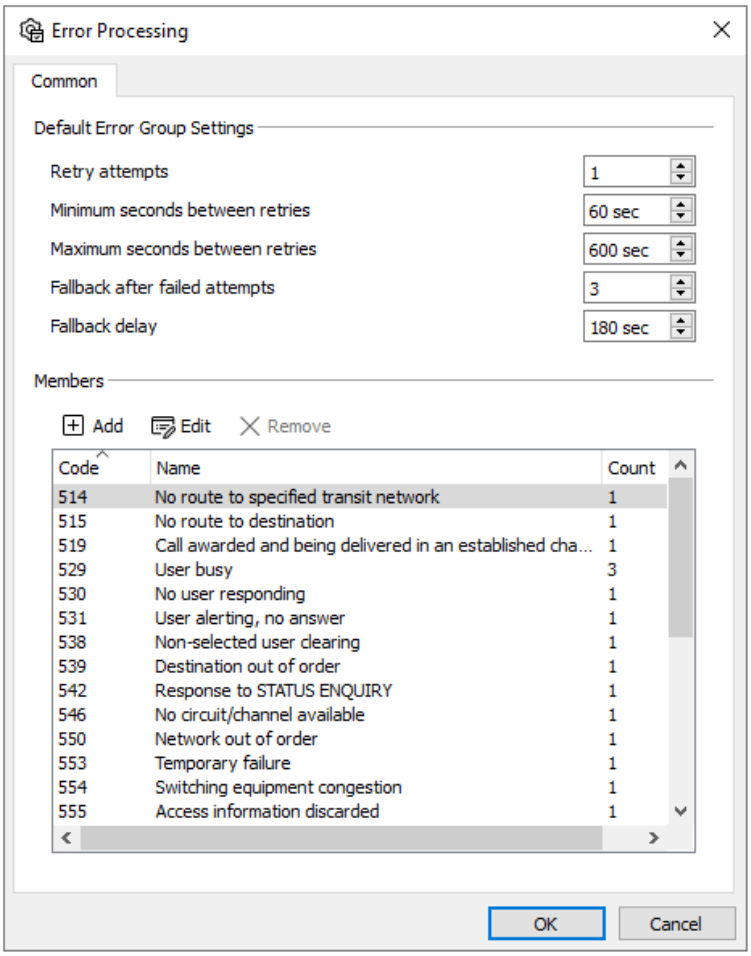


Figure 8.24: Properties of a rule

Regex Replace

If we take the above example, you can replace *\191* with the Value *+49332845591* for all calls matched by the regex match rule reach.

Default value

+49332845590

8.3.7. Fallback for outgoing calls

The fallback was implemented with OfficeMaster Suite 5 in order to provide a frequently frequently necessary addition to the outgoing routing. However, these settings only become relevant if more than one ISDN channel or SIP trunk is to be used.

The settings for the fallback behavior of the OfficeMaster Suite are made in two steps. The first step is the definition of when a fallback should occur. A fallback to another channel does not always make sense or is required differently depending on the customer scenario.

> **Note!**
> The fallback must be under Extras > System settings activated.

OfficeMaster Suite knows different error scenarios and for everyone of these cases the behavior can be defined. A default behavior is of course included with OfficeMaster Suite, but it can be adapted to you at any time.

Step 1: When do fallback settings take effect?

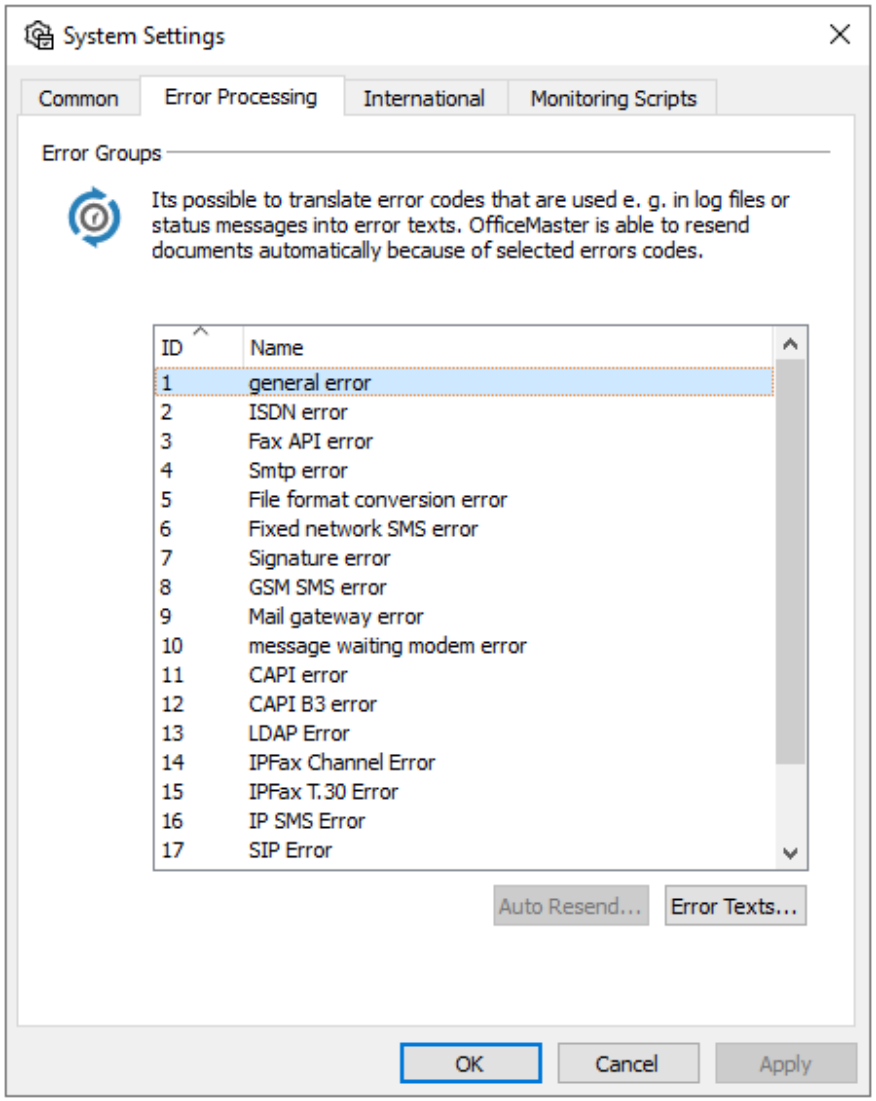


Figure 8.25: How can fallback be accessed?

Under the menu item Tools >System Settings on the tab *Error Processing* an error type selected and then with *Auto Resend* the next sub-dialog is called.

Error group default values

In this dialog for error processing, the same behavior can be defined for all errors of this type (e.g. ISDN error).

The settings can also be found in the errors and be adjusted accordingly.

Retries

Here it can be defined the number of retries attempted when an error occurs.

Minimum rest between two repetitions

How long should you wait at least between two attempts. In a busy remote station, a new dialing attempt is usually only possible after a certain period of time.

Maximum rest between two repetitions

When at the latest should the dispatching job be queued again (high priority).

Fallback after failed attempts

The number of attempts before the fallback mechanism intervenes is set here. If the number of attempts is smaller than the number of set send repetitions, no fallback will be executed for this error or group and the job is reset as faulty.

Dodge fallback after

The additional delay before the fallback mechanisms occur can be set here in seconds

> Note!
> Under the menu item Error texts, you can adjust the error messages globally. This may be useful, if you want to tell the users directly, what they should do in case of which errors.

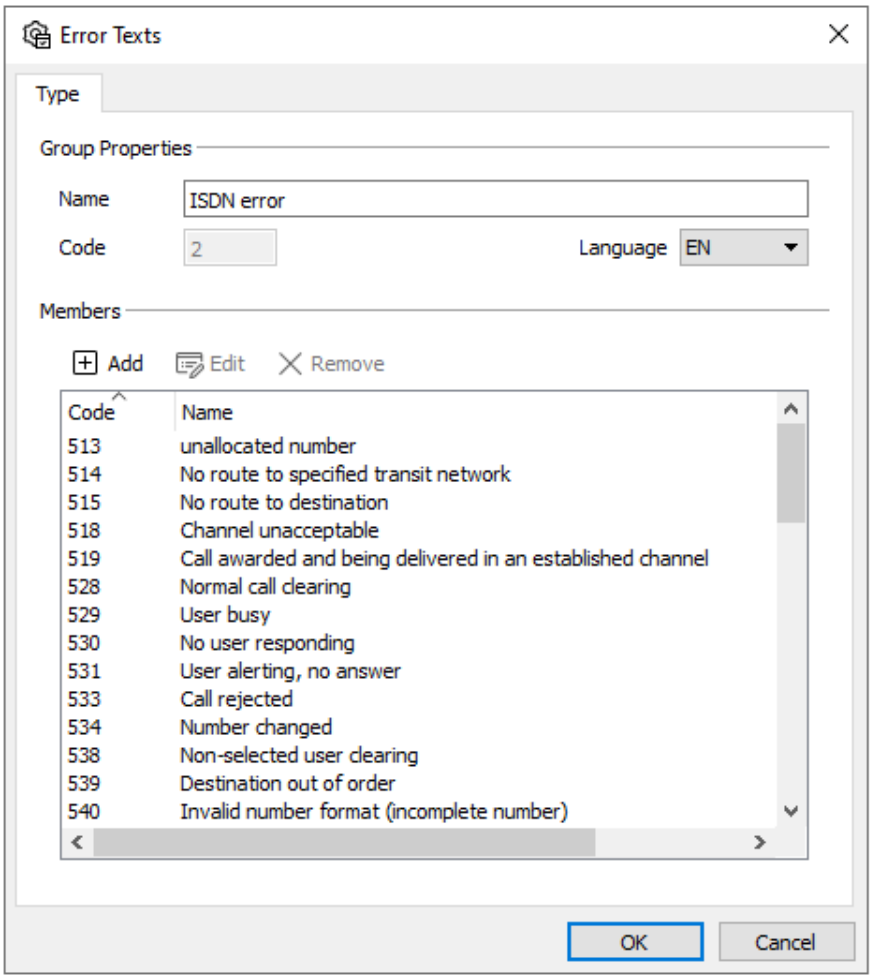


Figure 8.26: Adjust error texts individually

Step 2: Routing settings

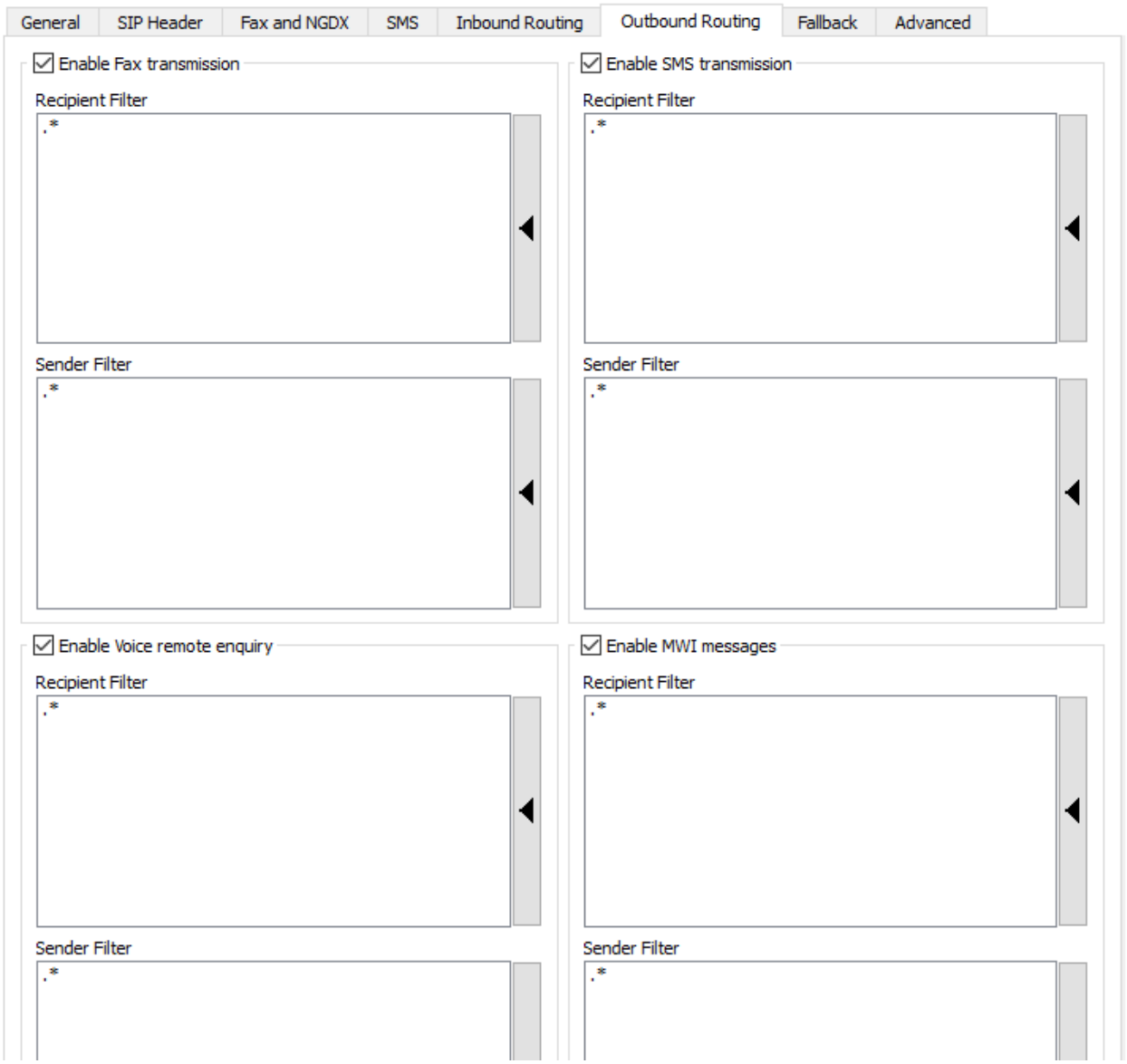


Figure 8.27: Fallback settings per D-channel

If all filters are set to **.***, this channel takes over, independent of the settings under Outbound Routing, this channel take over the sending of the documents in case of a fallback. A change at this point only makes sense if:

1. more than two D-channels are available or
2. a redial attempt is not desired for individual destination or originator numbers.

The Fallback settings configure the behavior of the D channel when an error occurs and whether this D channel for the suitable job and accepts it. This affects everyone D-channel errors (i.e. also over several Devices/OfficeMaster Gate).

Example 3.5:

Sending messages via the local OfficeMaster Gate with fallback to another location as shown in the table.

- In this case, the OfficeMaster Gate (OMG) in Berlin will take over the shipping for Vienna and Hamburg as soon as shipping is not possible there.
- OMG in Hamburg takes over for Berlin, if a fallback is needed there.
- OMG in Vienna does not take over any fallback tasks

Location	**Outbound Routing (Sender)**	**fallback (transmitter)**
Berlin	+4930.* ; -.*	.*
Hamburg	+4940.* ; -.*	+4930.*
Vienna	+43.* ; -.*	-.*

Table 8.1: fallback routing settings

9. Operation of the messaging server

9.1. Overview

In order to run the OfficeMaster Suite reliably in a production environment, a number of functions are included to support the administrator. These are presented in this chapter:

- Monitoring
- Drain Mode / Maintenance Mode
- Redundancy
- Administrator Alerts

9.2. Administrators

9.2.1. Adding Administrators

After installation, there is a user *Administrator* with the default password *OfficeMaster!*. This password should be changed first after installation.

Additional administrative users can then either be set up as local users by the administrator or potential new administrators can try to log in with their Active Directory login (user@ad-domain or user\ad-domain). The administrator can then unlock these users and the Active Directory password will be used in the future.

9.2.2. Roles

Administrative users can have different roles: - Administrator (full access) - Component manager (can start/stop components) - Job manager (can view and cancel jobs) - Support Assistant (can view logs and status)

9.2.3. Password policy

The required password complexity for local OfficeMaster administrators can be set in the *Settings* tab in the *Manage Administrative Users* dialog. There are three operating modes: - Disabled (no password complexity requirements), - Custom regular expression (see below), - Security policy complexity requirement (use of a Windows security policy, default setting)

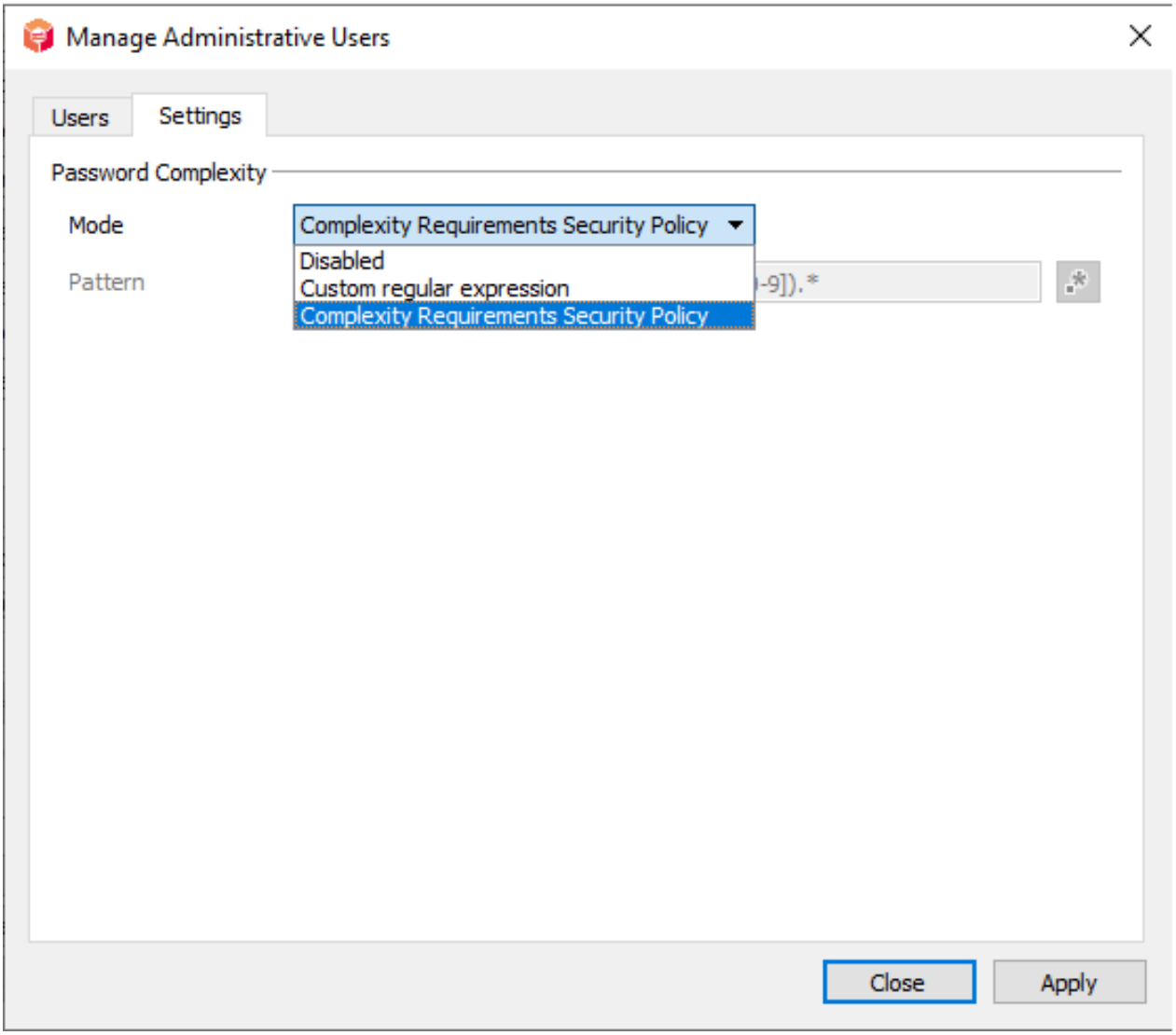


Abbildung 9.1: Dialog Passwort Policy

Custom regular expression

An example of a regular expression for password complexity is the following string:

```
^(?=.{8,32}$)(?=.*[A-Z])(?=.*[a-z])(?=.*[0-9]).*
```

A password with a length of 8-32 characters is defined here, which should contain upper and lower case letters as well as numbers.

Security policy / security policy

The security policy *Password Policy* of the Windows system is used by the OfficeMaster Suite. The Windows app secpol.msc can be opened and the corresponding settings can be made there. It is possible that this property is managed centrally.

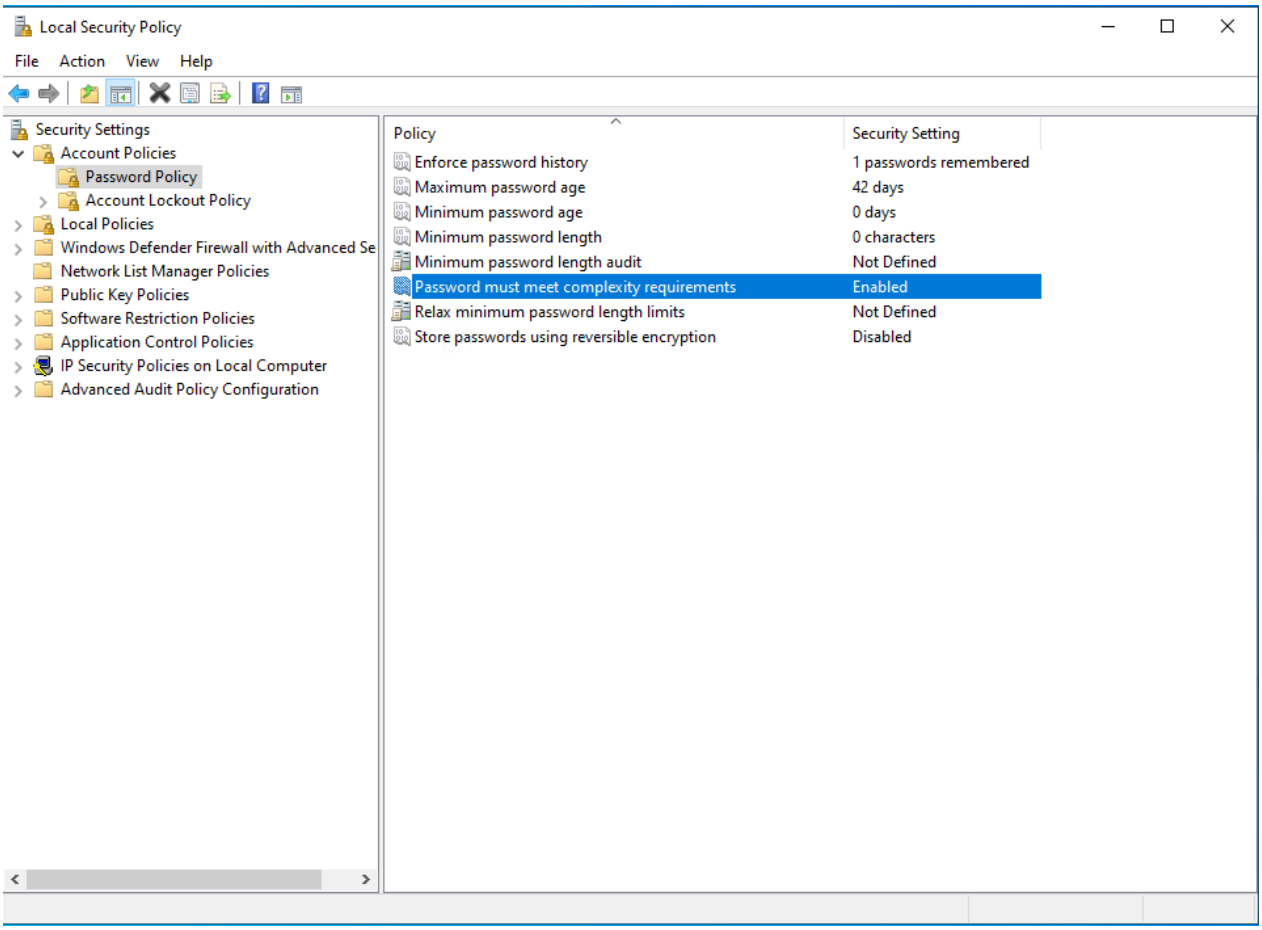


Abbildung 9.2: Dialog Security Policy

9.3. Monitoring

9.3.1. Overview

In order to maximize the availability of the service, it is helpful to be able to quickly identify and fix any failures. This is why monitoring systems are used. The OfficeMaster Suite has internal counters that record a series of events (e.g. number of pages sent). This allows an alarm to be triggered in the monitoring system based on thresholds.

A total of approx. 450 counters (only increasing) or measured values (display current value) are implemented. The values used for sending faxes are shown here as an example:

name	**meaning**	**MIB ID**
fmsrvSendRecFaxInActiveJobs	Number of currently incoming fax connections	.1.3.6.1.4.1.17524.1.1.1.2.2.15.2.1.20
fmsrvSendRecFaxInMinActiveJobs	Minimum value for this	.1.3.6.1.4.1.17524.1.1.1.2.2.15.2.1.21
fmsrvSendRecFaxInMaxActiveJobs	Maximum value for this	.1.3.6.1.4.1.17524.1.1.1.2.2.15.2.1.22
fmsrvSendRecFaxInCompletedJobsOk	Number of successful receive requests	.1.3.6.1.4.1.17524.1.1.1.2.2.15.2.1.23
fmsrvSendRecFaxInCompletedJobsError	Number of incorrect receive jobs	.1.3.6.1.4.1.17524.1.1.1.2.2.15.2.1.24
fmsrvSendRecFaxInChannelsSupported	Number of available receiving channels	.1.3.6.1.4.1.17524.1.1.1.2.2.15.2.1.25
fmsrvSendRecFaxInJobsTotalDuration	Duration of receipt of all receive jobs	.1.3.6.1.4.1.17524.1.1.1.2.2.15.2.1.26
fmsrvSendRecFaxInJobMaxDuration	Maximum duration of a receive request	.1.3.6.1.4.1.17524.1.1.1.2.2.15.2.1.27
fmsrvSendRecFaxInJobsTotalPages	Number of pages of all receive jobs	.1.3.6.1.4.1.17524.1.1.1.2.2.15.2.1.28
fmsrvSendRecFaxOutActiveJobs	Number of currently outgoing fax connections	.1.3.6.1.4.1.17524.1.1.1.2.2.15.2.1.40

name	meaning	MIB ID
fmsrvSendRecFaxOutMinActiveJobs	Minimum value for this	.1.3.6.1.4.1.17524.1.1.1.2.2.15.2.1.41
fmsrvSendRecFaxOutMaxActiveJobs	Maximum value for this	.1.3.6.1.4.1.17524.1.1.1.2.2.15.2.1.42
fmsrvSendRecFaxOutCompletedJobsOk	Number of successful send requests	.1.3.6.1.4.1.17524.1.1.1.2.2.15.2.1.43
fmsrvSendRecFaxOutCompletedJobsError	Number of failed send requests	.1.3.6.1.4.1.17524.1.1.1.2.2.15.2.1.44
fmsrvSendRecFaxOutChannelsSupported	Number of available transmission channels	.1.3.6.1.4.1.17524.1.1.1.2.2.15.2.1.45
fmsrvSendRecFaxOutJobsTotalDuration	Duration of receipt of all send jobs	.1.3.6.1.4.1.17524.1.1.1.2.2.15.2.1.46
fmsrvSendRecFaxOutJobMaxDuration	Maximum duration of a shipping order	.1.3.6.1.4.1.17524.1.1.1.2.2.15.2.1.47
fmsrvSendRecFaxOutJobsTotalPages	Number of pages of all send jobs	.1.3.6.1.4.1.17524.1.1.1.2.2.15.2.1.48

The complete set of counters or measured values is documented in the form of an Excel table (#4657). A MIB file is also available.

9.3.2. Integration of the OfficeMaster Suite into a monitoring system

OfficeMaster Suite offers three approaches for integration into a monitoring system.

Simple Network Management Protocol (SNMP)

SNMP is used to monitor network components and most monitoring systems offer the use of SNMP data sources. SNMP data sources can be network elements such as routers or switches, but also the *OfficeMaster Suite*. Further information on SNMP can be found at https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol.

The Windows SNMP service

The *OfficeMaster Suite* uses the Windows SNMP service. This supports the SNMP protocol in version SNMPV2c and thus the following RFCs:

- RFC 1901: Introduction to Community-based SNMPv2
- RFC 1905: Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2)
- RFC 1906: Transport Mappings for version 2 of the Simple Network Management Protocol (SNMPv2)

The Windows SNMP service uses plugin DLLs for expansion, which provide additional data sources for SNMP. These data sources are described by MIB (Management Information Base). Information on the functionality and structure of an MIB can be found at https://en.wikipedia.org/wiki/Management_Information_Base.

Integrating the *OfficeMaster Suite* into a monitoring system

The *OfficeMaster Suite* installs the Windows SNMP service as a feature and a plugin DLL which provides access to the counters and statistics of the messaging server. A MIB is also supplied. By default, this is located under C:\Program Files\FFUMS\snmp\MIB, but the path may differ if the installation location has changed.

Unfortunately, it is not possible to describe the setup of the monitoring system in this manual. Various systems are used by customers and reference is made to the documentation for these systems. Basically, the following steps are necessary:

- On the monitoring system:
  - A new system to be monitored must be added.
  - This system is monitored via SNMP.
  - The default SNMP port is 161/UDP, the IP address or resolvable name of the messaging server must be provided.
  - If a different SNMP community is used, the name of this (default value *public*).
  - The MIB must be imported, this describes the available/retrievable counters and values and provides an explanation.
- On the Windows Server (SNMP service settings):
  - Configure SNMP security. Here you can specify the communities and hosts from which this computer will accept SNMP requests. The address of the monitoring system should be specified and (if you want to deviate from the default value) the name of the SNMP community.

The new values should then appear in the monitoring system. Based on these values, other things can optionally be set, such as alerts when certain error thresholds are exceeded.

Note
The *OfficeMaster Suite* does not use SNMP traps on port 162/UDP

As an example for a configuration of a monitoring software, please refer to the check**mk** documentation: https://docs.checkmk.com/latest/en/snmp.html

Monitoring via plugin

A plugin can also be used instead of SNMP to monitor the messaging server. Such a plugin is typically provided by the provider of the monitoring solution.

The monitoring system calls this plugin periodically to query data from the system to be monitored. A local script can be configured as a data source. The controller can make the internal monitoring data available by query. A script can carry out this query and then make the data available to the monitoring system in JSON format.

Monitoring via web requests

There is a package for Checkmk (officemaster_suite_v2.mkp) to integrate the OfficeMaster Suite into Checkmk. This will be

mkp install officemaster_suite_v2.mkp

Installed. After that, the package needs to be configured. Under `Setup -> Hosts -> Hosts -> Add host` the host name of the messaging server can be specified under `Basic Settings` and its IP address under `Network Settings`. After saving this setting, further parameters can be specified under `Setup -> Agents -> Other integrations -> Other integrations -> Ferrari Electronic [...]`. The port of the AuthGateKeepers (3216) as well as the user and password of an administrator user for access to the messaging server are important here.

Parameters	**Default value**	**CLI Tag**
IP address	localhost	-url
Port	3216	-port
Username	admin	-u
Password	OfficeMaster!	-p

The newly created host can now be selected under `Setup -> Hosts -> Hosts`. After clicking on `Full service scan` components and their data should appear.

After setup

The parameters can then be assigned in the monitoring system and thresholds for warning messages can be defined. Many monitoring systems offer configurable administrator notifications when thresholds are exceeded. For the setup, please refer to the documentation of the monitoring system in use.

9.4. Drain Mode

9.4.1. Goals

The drain mode is characterized by the fact that the messaging server no longer accepts new orders from the network. The behavior is different for the individual components:

- A SIP component no longer accepts incoming faxes,
- an SMTP-RX component no longer accepts emails,
- an Exchange Connector no longer accepts orders from the transfer mailbox.

Apart from that, the messaging server still works. Faxes are sent or delivered to mailboxes. This should complete all orders that are currently being processed and then calm down.

This achieves several goals:

- in the event of an error, no orders are blocked in the messaging server (flow control),
- in active-active failover scenarios, the load is automatically distributed to the still functioning system,
- Before planned maintenance work, the messaging server can be taught so that all jobs are completed.

The drain mode (maintenance state) can be triggered by two things:

- The administrator requests the maintenance status (drain mode) in the messaging server configuration program.
- A component detects an error and generates an alarm and an alarm from this component has been configured as the reason for triggering the maintenance state (in the delivery state, component alarms do not lead to the maintenance state)

The behavior of the individual components of the messaging server in connection with the drain mode is shown below.

9.4.2. Monitor component

- triggers the notification chain
- generates a message that the CTRL distributes to other components

- constantly monitors the component status, the comptab and own cfg (maintenance on/off)
- reads relevant components from the comptab
- if a component with the property “DrainAlertEnabled” triggers an alarm, the CTRL is notified to put the system into drain mode and an email is sent to the configured address
- The actual state (state) depends on whether all relevant components in the system have actually reached the target state (mode).
- the target state (mode) is determined by an alarm (on/off) and the maintenance mode

9.4.3. Controllers

- distributes the notification
- remembers target state (mode) and actual state (state)
- this can be queried (DrainInfo) or via CfgProxy (SystemInfo(Ex))

9.4.4. Component (as passive receiver)

- Responds to the notification
- Mode parameter is the relevant value (target state)
- State parameter is for info purposes only
- In/Out and SendRec components no longer accept external orders
- All internal orders are processed normally
- enters the target state as soon as possible (component status message)

9.4.5. component (as active trigger)

- can initiate the entire notification chain by sending a component status message with an alarm
- must resolve the alert by sending a component status message with a normal status

9.4.6. Active alarm triggers

component	reason	recovery	test
ClientGw	Failed to connect to SQL Server	Connection successful	Change SQL ports
DsConv	Conversion Failed, Requeue Required, Requeue Alert Count Exceeded	Successful conversion	Remove smart card reader
gsmsms	SMS sending failed 5x in a row	Shipping ok	

component	reason	recovery	test
MailGw	Cannot connect to LDAP mode server	LDAP connection successful	Change LDAP port
Exchange	Graph / EWS connection faulty	Graph / EWS connection successful	turn off the network
MWI	MWI modem job failed 5x in a row	Shipping ok	
Notes	No free disk space, unable to read database, unable to initialize sending API	Database processing successful	turn off the network
Omcum's	"Drain Mode Layer down" activated and D-channel ISDN Layer2 Down	Layer2 Up	Pull the ISDN cable
PrintGw	Printing failed more than 2x (requeued)	Print Ok	bad printer path
SMTPTx	Mail delivery failed 5 times in a row	Shipping ok	wrong SMTP server
UcpTx	Failed to connect to UCP Provider	Connection successful	wrong UCP provider URL
SIP	Lost connection to SIP trunk (either TCP/TLS or UDP Options Ping)	SIP trunk reachable again	incorrect SIP trunk setting
Smpp	Disk full, provider error (keep-alive, login, disconnected, unreachable)		

9.4.7. Redundancy scenarios

In order to create redundancy and thus higher availability of the solution, two messaging servers can be operated in parallel. This approach is called active/active. Everything can be duplicated: Two SIP trunks and two VMs on different platforms. Many connectors are capable of supporting parallel operation. The M365 Graph Connector (Exchange Cloud Connector) is to be used here as an example.

If there is now an alarm that triggers drain mode on one of the two machines, it will no longer accept any orders. The SIP trunk will no longer accept incoming calls (however, outgoing calls will still be established if possible) and no orders will be accepted more taken over from the transfer mailbox.

If the second machine remains operational and is configured to use the same M365 account, it will then automatically take on the full load. When the problem on the failed machine has been resolved, it will then automatically process jobs again.

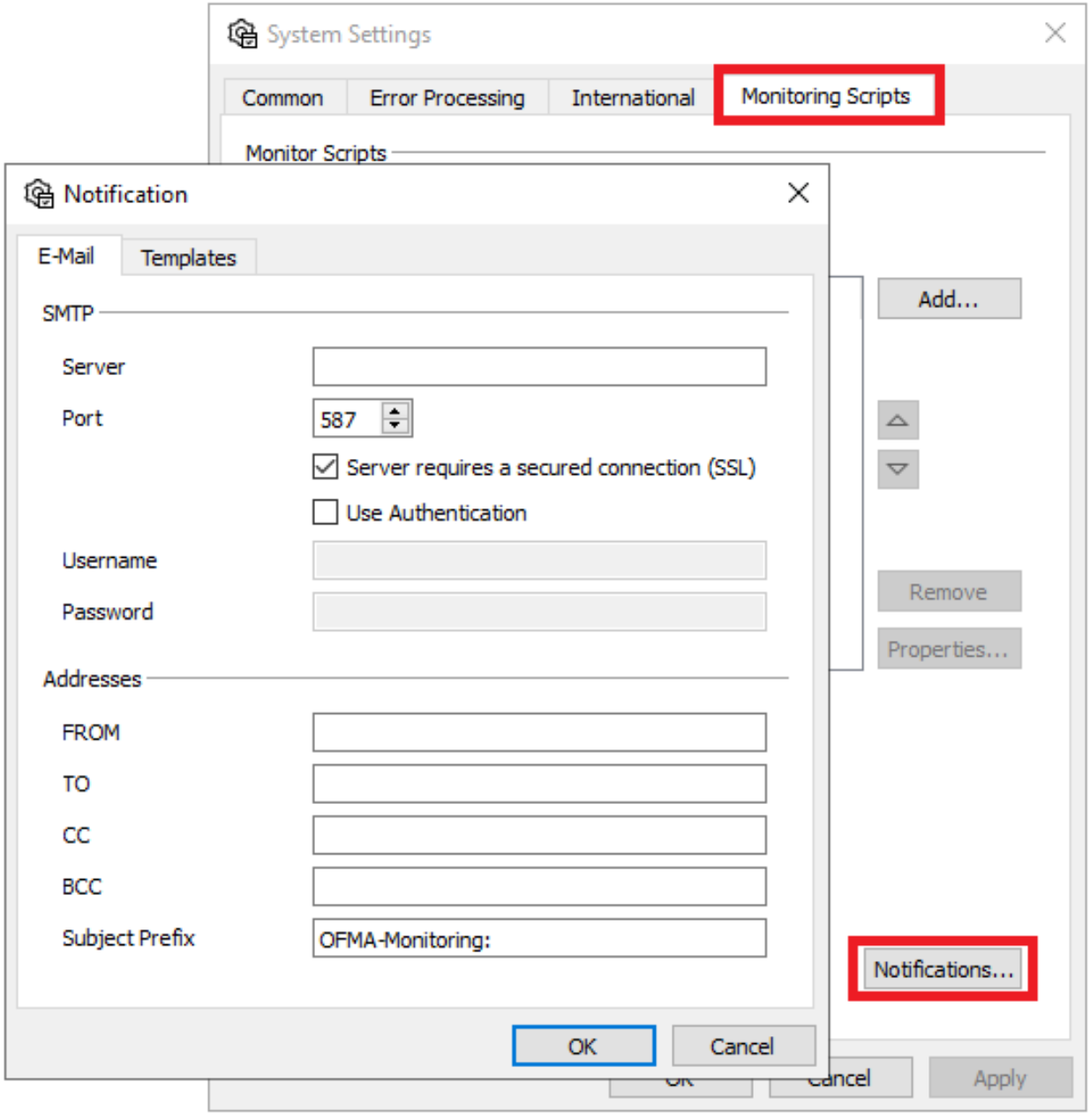
The redundant SIP trunks could be created in an SBC or a phone system with round robin/ overflow in the same phone number range.

> Note:
> The active/passive redundancy scenario (a messaging server in cold standby) does not increase availability, but can help to reduce any downtime by simply manually switching to the standby machine. After that, the error analysis can be carried out in peace.

9.5. Admin Alerts

In the event of alarms, the OfficeMaster Suite can send out admin alerts by email. This is configured in the Messaging Server Configuration in System Preferences. The alarm causes are the same as described above, which can also lead to entering maintenance mode (if so configured).

If SMS notifications are desired, it is recommended to use an external mail-to-SMS service. Although the OfficeMaster Suite provides this function, correct delivery in the error state cannot be guaranteed.



9.6. Firewall configuration

The OfficeMaster Suite uses external connections (e.g. to cloud services, SIP providers or mail servers) and also opens ports that should be accessible from outside. The following table lists the open server ports:

Port	service	Protocol	Function
25	SMTP	TCP, TLS	SMTP_RX Inbound Mail
80/443	HTTP/HTTPS	TCP/TLS	Access WEBVoice/WEBFax
161	SNMP	UDP	Monitoring, configurable
514	Syslog	UDP	Syslog data
515	LPR	TCP	LPD Print Services
3216	HTTPS	TLS	Gatekeeper: API, Config-WebUI, online help
5060-5068	SIP	TCP, TLS	When using directSIP
7060+	RTP, SRTP	UDP	When using an OfficeMaster Gate (depending on the remote station)
49152-50000	FOAM/JSON RPC	TCP (localhost)	dynamic Ports for Messaging Server Components
50000-50999	RTP, SRTP	UDP	DirectSIP (depending on the configuration setting)

The following table lists the typical client connections:

Destination port	service	Protocol	Function
3217+x	Job control	TCP	Connection to OfficeMasterGate one port per connection
3215	SNFS	UDP/TCP	Fax/Voice file access to OfficeMaster Gate, can be set there
123	NTP	UDP	Time server
25/10025	SMTP	TCP	Sending emails for MailGW or Exchange. Depending on the config also other ports
389/3268/636/3269	LDAP/ LDAPS	TCP/TLS	LDAP as a directory service

Destination port	service	Protocol	Function
1352	Notes	TCP	Connection to the Domino server when using Notes
80/443	HTTP	TCP	Access to EWS when using Exchange, Microsoft Graph with Exchange Online
33xx	SAP	TCP	Access to SAP, port dependent on SAP instance, e.g. sapgw00 = 3300
Nnnn	RTP/SRTP	UDP	When using directSIP, depending on the remote station
Nnnn	SIP/SIPS	UDP/TCP/TLS	When using directSIP, depending on the remote station

In current installations, DirectSIP (pure software solution) is usually used and OfficeMaster Gate is only relevant for legacy applications with ISDN.

10. Configuration of each Component

10.1. Basic converter

10.1.1. Above

The basic converter is created during the installation of the ***OfficeMaster Suite***. This is responsible for converting incoming messages.

10.1.2. Overview

Creation of the basic converter

The base converter exists by default, there is no need to create it (unless it was deleted).

In the Messaging Server Configuration quick launch bar, go to *"Converter > Base Converter"* and then add a new component of this type via *"New Base Converter Component..."*. The creation of this new component is supported by a wizard.

The subsequent naming dialogs correspond to the standard wizard and can be carried out accordingly. After the base converter has been successfully created, the general configuration of the component is available.

10.1.3. General

Display system job ID in status line

By enabling this option the system job ID is displayed in the status line of incoming documents (e.g. fax messages). This option is for better traceability in transfer logs.

By default it is disabled.

10.2. Web connector/client

With the web connector, OfficeMaster offers a basic connector for two use cases. 1. Web Client – OfficeMaster Workstation G5 enables users to conveniently communicate via fax and SMS without having to install it on the workstation computer. 2. Web Services - they allow third-party software to access the functionality of the messaging server.

A Microsoft SQL Server $^{2008}/_{2012}$ in the network is required to operate the OfficeMaster Web Client without the support of external groupware. The SQL Server takes over the user management and storage of the data.

> **Note!**
> You can find brief instructions for installing a Microsoft SQL Server Express under “Basic installation”.

10.2.1. Flow of communication

Web client, user view

For the use of the web-based user interface, techniques are used that enable the complete range of functions without the additional installation of plugins for the web browser. A corresponding URL (e.g. *http://UMServer/fax*) is called up for this purpose. Java scripts are used here, which, however, generate some computing load on the client system. This must be taken into account when using terminal servers.

Internet Information Service (IIS)

Scripts are stored on the IIS that call up stored procedures on the SQL server.

SQL

Two types of stored procedures are stored on the SQL server: one communicates with the IIS to process corresponding queries, the other communicates with the OfficeMaster Suite (OM Suite). If a new job is created by the web client in SQL (e.g. outgoing fax), a connection to the OM Suite is established with all the information for this job. In turn, the current status of the job in the OM Suite is transmitted to the SQL database via stored procedures. This status can then be queried accordingly.

Office Master Suite

In the OfficeMaster Suite, the CLIENTGW component handles communication with the SQL server. The jobs are queued from here in the rest of the messaging server for further processing.

10.2.2. Settings on the Clientgw component

If there is still no entry for the CLIENTGW, it is added as a component via the messaging server configuration. The details about adding individual components can be found in this document in *“Creating / deleting components”*.

Store service account

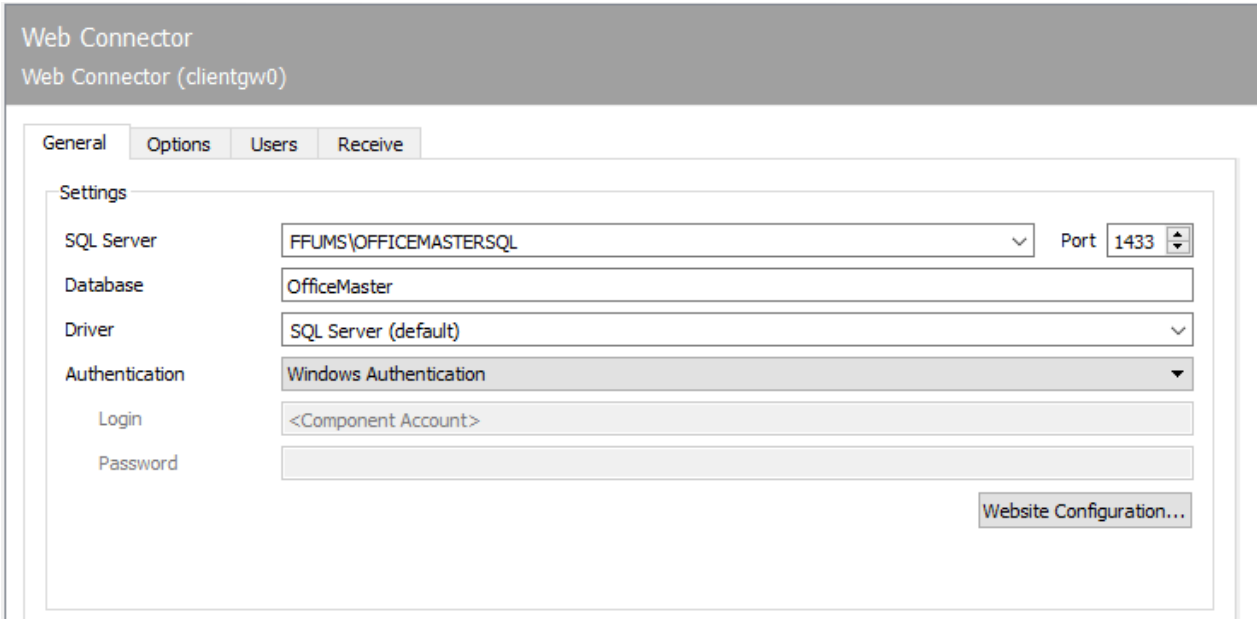
The first step after installing/creating the CLIENTGW leads to the properties of the component. These can be accessed either via the component table or via the component status view. Details on this can be found in *“Configuring components”*.

The component must not be started under the system account, otherwise the access authorizations on the SQL server cannot be transferred correctly. Accordingly, the field must be stored with a service account. The service account must be a member of the local administrators to have appropriate permissions on the system to create and delete job files. Furthermore, this user must be stored in the SQL database as an administrator.

> Note If an SQL server is set up especially for the OfficeMaster Suite, it is advisable to store this user when executing the SQL setup.

Configure access to the SQL Server

After opening the configuration menu for the CLIENTGW component, you get to the *General* tab, in which the SQL server to be used and the database are stored.



10.2.3. General

Settings

SQL Server

Select the SQL server in your network that is to be used for user maintenance and data storage.

Database

The database name specified here is used to create a new database on the SQL server or to use the existing database with this name. OfficeMaster is used as the database name by default. If you make a change at this point, the database must be changed accordingly in the section *"Settings for the website"*.

Driver

The ODBC driver to be used for database access is selected here.

Authentication

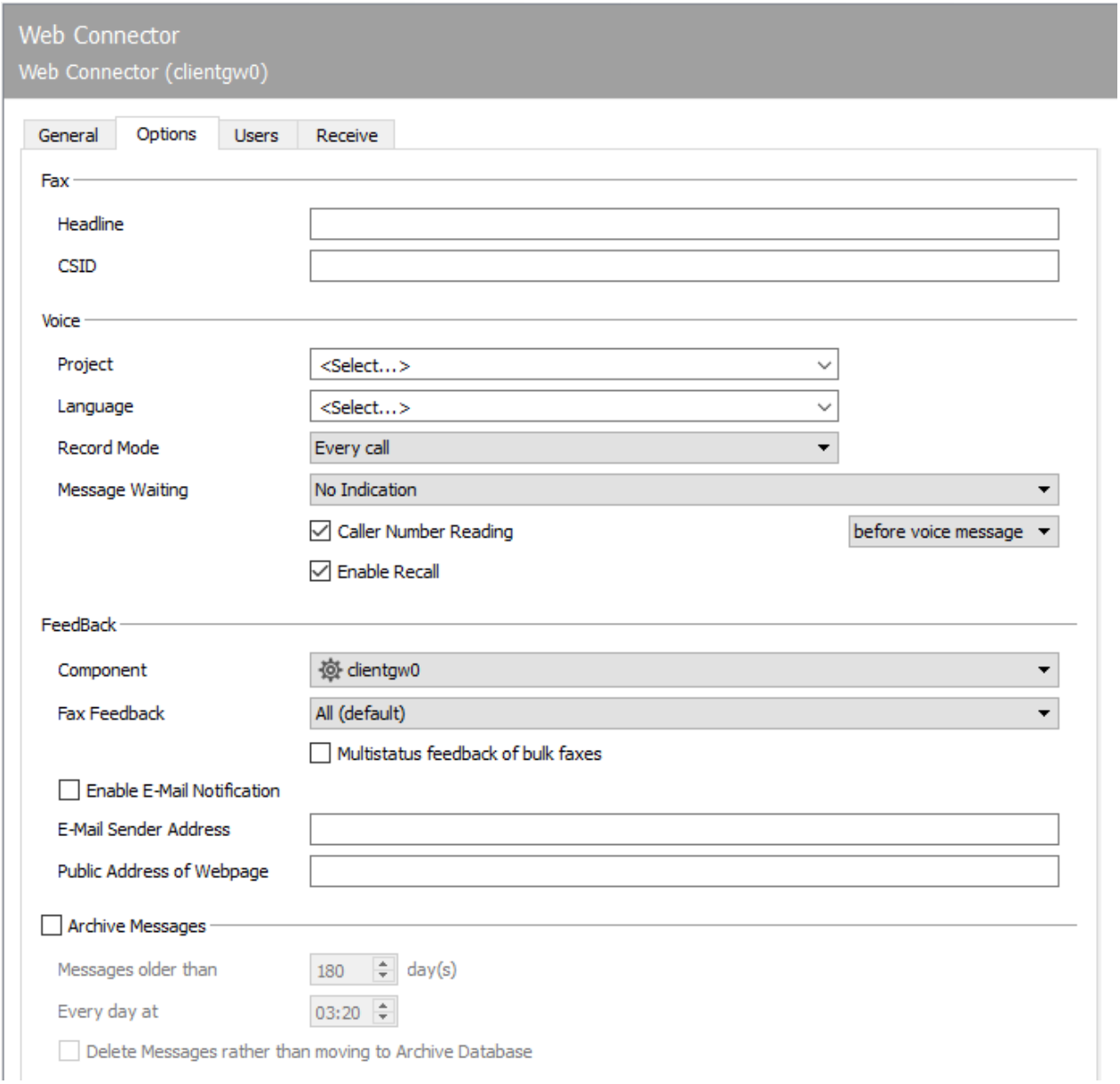
With the current release status, it is recommended to use Windows authentication. The service account stored for the component is taken over and used for authentication.

User name

Specification of a user name for authentication on the SQL database.

Password

Specification of the password for authentication on the SQL database.



10.2.4. Options

The global settings for all users and groups of the web connector are made in the Options tab. These settings apply if the user or group has the respective setting has not been made.

Fax

Header

Enter the fax header for all participants who are served via this connector. If the participant has their own header, that of the participant has the higher priority.

CSID

Store the general Called Subscriber Identification here for all subscribers for whom this is not maintained separately.

Voice

Project

The behavior of the voice box is defined with the project. *eVoice-ProjectStart* is recommended here for normal user behavior. Only then is the dynamic voice with the web configuration possible.

Language

Regardless of the project, OfficeMaster supports different languages with the same behavior. As of 2020, the languages *German*, *English*, *Spanish* and *Spanish Latin America* will be delivered and can be selected here. If another language with standard texts is desired, please get in touch with your contact person at Ferrari electronic AG.

Record

This is used to set whether missed calls should also be displayed in the web front end. With *All Calls* the user can also see the missed calls without leaving a message. With the option *Voice messages only*, only those calls are saved where a voice message was actually left.

Message Waiting

Set the behavior of the MWI here.

- No signalling
- Reset by general remote inquiry
- Reset by listening to at least one message
- Reset by listening to all messages

To do this, you must have activated MWI on the communication interface used (*OMCUMS* or *SIP*) and the telephone system.

Read the caller number on the phone

Decide whether the phone number should be read out when listening to the voice messages and, if so, whether this should be done before or after the message.

Callback active

If this option is enabled, the user can call the caller back directly from the remote inquiry menu of his voice box.

Status notification

Responses are an important but also simple topic when sending faxes. A feedback component is required for sent faxes and the definition of when feedback should take place.

component

Here the components available on the messaging server are selected to which any type of feedback is to be sent. The resolution of the corresponding addressee is taken over by the confirmation component. The currently configured CLIENTGW is stored as a component by default.

Fax status notification

Here you specify when a confirmation should be generated.

- For all sent messages
- For failed deliveries only
- Only for successfully delivered messages

Collective confirmation for broadcast faxes

If this selection box is activated, only one reply is created for broadcast faxes (instead of for each individual transmission).

E-Mail notification

If activated, an e-mail notification is sent to the user.

Email sender address

The e-mail address given here will be used as the sender address for e-mail notifications.

Public website address

Specification of a URL with which the web server can be accessed. When using firewalls or port forwarding, this address can differ from that of the machine on which OfficeMaster Suite is installed.

Archive messages

Automatic archiving on the SQL server can be activated. The messages that are older than the days to be set are moved to a separate table at a freely definable time. This simplifies the backup procedures on the SQL server if not all messages are to be archived and also enables a shorter processing time in the message store for large amounts of data.

Messages older than X days

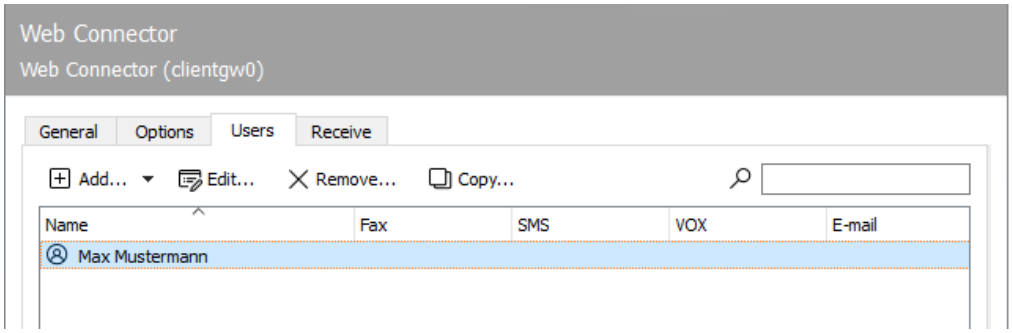
Specifies the number of days after which messages are to be archived.

Daily at

Time of the backup procedure run in the SQL server.

Permanently delete messages

Instead of archiving the messages, they should be deleted (a kind of quota mechanism for the database).



10.2.5. user

Add to

After selecting whether a user or a group should be created, the dialog for the user settings is called up.

To edit

If a user is marked in the overview and then edit is selected, the User Settings dialog opens for this user or this group.

Remove

The marked user or group will be permanently removed from the database.

Copy

As with Add, a dialog for creating a new group or user opens. All fields have the same assignment as the fields of the originally selected element. The data will only be saved after confirming this dialog window.

10.2.6. User Preferences

The settings described below apply to both groups and users.

10.2.7. General

Registration

Display name

The display name for users is displayed in the web interface, among other things, and should be legible accordingly.

User name

The user name can either be taken from the local Active Directory (AD) or created from scratch and only used with the OfficeMaster Web Services. When using the user data from the AD, the corresponding credentials (*username*, *password*) for domain users are used.

addresses

This is where the address under which the user can be reached and under which he sends messages is specified.

Account and Permissions

Account is disabled

If the account is set up but not to be used, then this box must be checked.

User management

If the user is allowed to make additional settings for other users, then this box must also be activated. An example of this is defining the projects for other users and creating announcements on the voice server.

Job Manager

If this option is enabled, an overview of all incoming and outgoing fax messages will be possible.

10.2.8. Fax

Transmission

Header

The header to be transferred is stored here.

CSID

The fax is acknowledged with the phone number specified here when it is sent.

10.2.9. Voice

voice box

A user's voice box can be reached at a specific number. This can be a normal voice mailbox with a recording function, a special *Interactive Voice Response System (IVR)* or any stored project.

voice box

The phone number of the voice box is stored here.

PIN

Use this field to store the associated PIN for remote querying of the voice box. The user can change this PIN at any time via the remote access menu or the website.

Project

The behavior of the voice box is defined with the project. Here, eVoice-ProjectStart is recommended for normal user behavior. Only then is the dynamic voice with the web configuration possible.

Language

Regardless of the project, OfficeMaster supports different languages with the same behavior. As of October 2017, the languages German, English and Spanish are supplied and can be selected here. If another language with standard texts is desired, please get in touch with your contact person at Ferrari electronic AG.

Record

This is used to set whether missed calls should also be displayed in the web front end. With *All Calls* the user can also see the missed calls without leaving a message. With the option *Voice messages only*, only those calls are saved where a voice message was actually left.

Read phone number (yes/no)

Decide whether the phone number should be read out when listening to the voice message and, if so, whether this should be done before or after the message.

Callback active

If this option is enabled, the user can call the caller back directly from the remote inquiry menu of his voice box.

Message Waiting

Set the behavior of the MWI here.

- No signalling
- Reset by general remote inquiry
- Reset by listening to at least one message
- Reset by listening to all messages

To do this, you must have activated MWI on the communication interface used (*omcums* or *sip*) and the telephone system.

MWI number

In this field, specify on which telephone or number *Message Waiting Indication* (MWI) is to be activated.

On my phone

phone

When using the web client, the user's own telephone is called to query left voice messages and also to record or listen to announcements. This can be stored here, or entered by the user himself from the web interface of the client.

Query authorized numbers

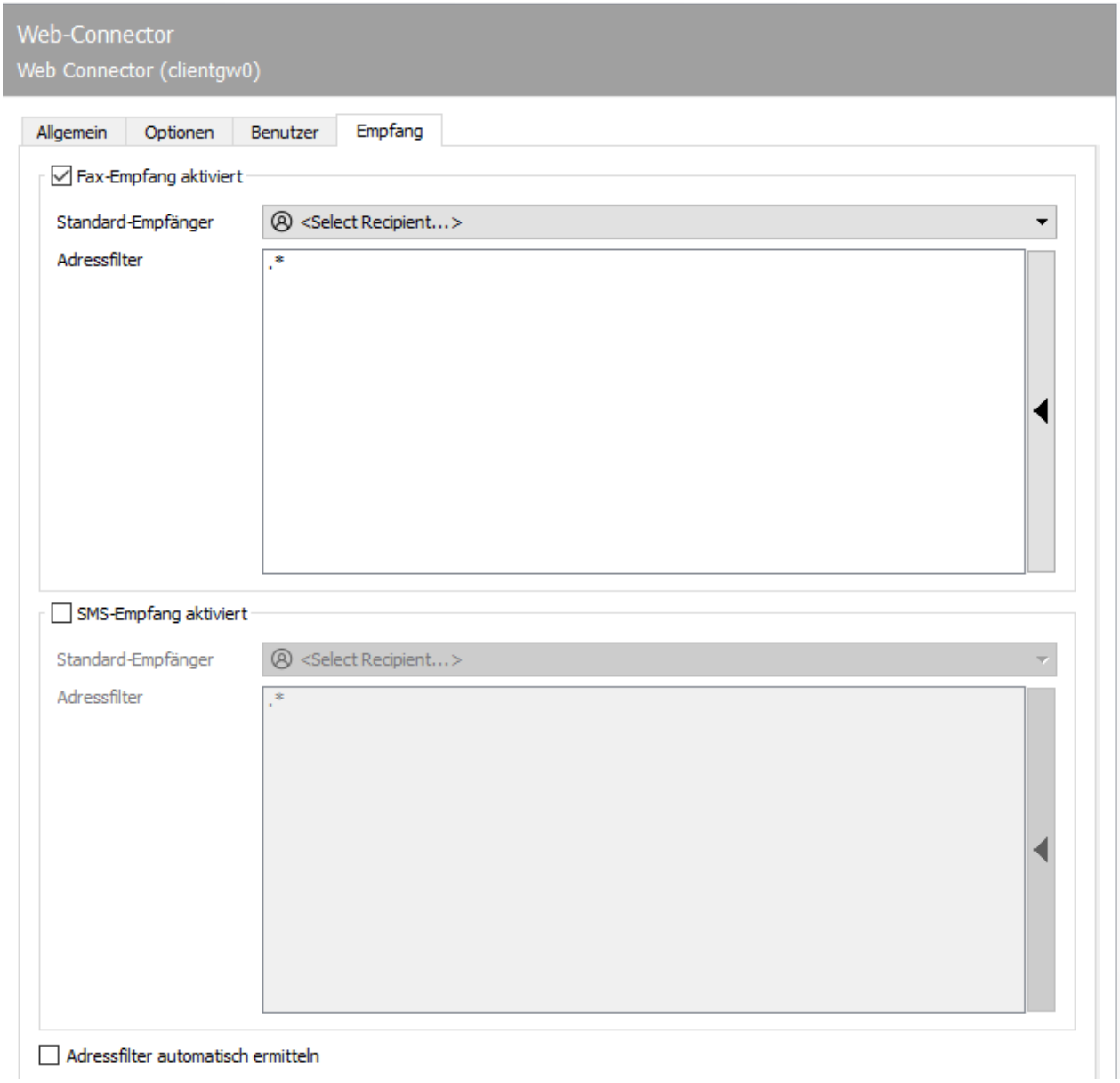
Up to three authorized phone numbers can be stored here, for which it is not necessary to enter the PIN in order to query the voicemails.

Members (only for groups)

Management of the members of this group.

Member of

Store the appropriate group memberships to get access to contact information and messages.



10.2.10. Reception

The Reception tab has a direct impact on the incoming documents. The telephone numbers (Called Party Number) for the reception processes intended for the Web Connector can be entered as address filters for faxes or SMS. With the default setting (.*), all received faxes or short messages are forwarded to the web connector.

A change is only required if received messages are to be distributed to different gateways, such as msx2kgate, sapconn, filegw, etc., or if messages from OfficeMaster are only to be received on certain phone numbers.

The latter, the so-called whitelist procedure, can be activated under Extras > Black & Whitelist > Reject undeliverable messages.

Note!
If the address filter is restricted to certain phone numbers without an activated whitelist procedure, the UNDELIVERABLE component of the messaging server should be configured so that received messages are not stored unnoticed on the server and “stay behind” despite the best address filter configuration.

In the simplest case, an address filter consists of a list of numbers that are assigned to the connector. For example, if all faxes to the numbers 150 to 154 are destined for the Exchange Connector, the address filter list contains the following entries: 150 151 152 153 154

The entries in this list can be combined with regular expressions into entry 15[0-4].

The default value (.*) for the address filter is also a regular expression. The dot (.) stands for any character. The asterisk gives the character in front of it the meaning as often as you like. At this point, only one address can be specified per line. It is not possible to combine several expressions in one line using OR (|) or AND (&).

Fax reception activated

Fax reception for the web connector can be activated here.

Default recipient

The default recipient is used for incoming faxes whose destination number cannot be assigned to a user. This user can be set here.

Address filter

Specification of regular expressions that are applied to the fax destination address in order to determine the routing destination for incoming faxes

SMS reception activated

SMS reception for the web connector can be activated here.

Default recipient

The default recipient is used for incoming SMS whose target number cannot be assigned to a user. This user can be set here.

Address filter

Specification of regular expressions that are applied to the fax destination address in order to determine the routing destination for incoming faxes

Determine address filter automatically

If active, the address filters are automatically generated from the phone numbers of the users in the database.

10.3. Command line converter

10.3.1. Description

The task of *CMDCONV* is to convert the documents supplied by the user into a format that the sending component (e.g. SIP) can process.

> **Note:**
> Starting with Release 7 of the ***OfficeMaster Suite***, the command line converter *CMDCONV* is increasingly replacing the function of the deprecated central converter component *CONV*.

The *CMDCONV* should keep the configuration effort for the administrator as low as possible and already support the most common formats by default. Installed programs are recognized after the startup of the cmdconv in their default system paths and are automatically used for the central conversion without interaction by the administrator. In addition to the conversion tools provided, these are currently:

- ***LibreOffice***
- ***Tesseract***
- ***PDFium*** (installed by default)
- ***Chromium*** (installed by default)
- in special cases also ***Ghostscript*** (only needed in correlation with Line Printer Daemon or SAP)

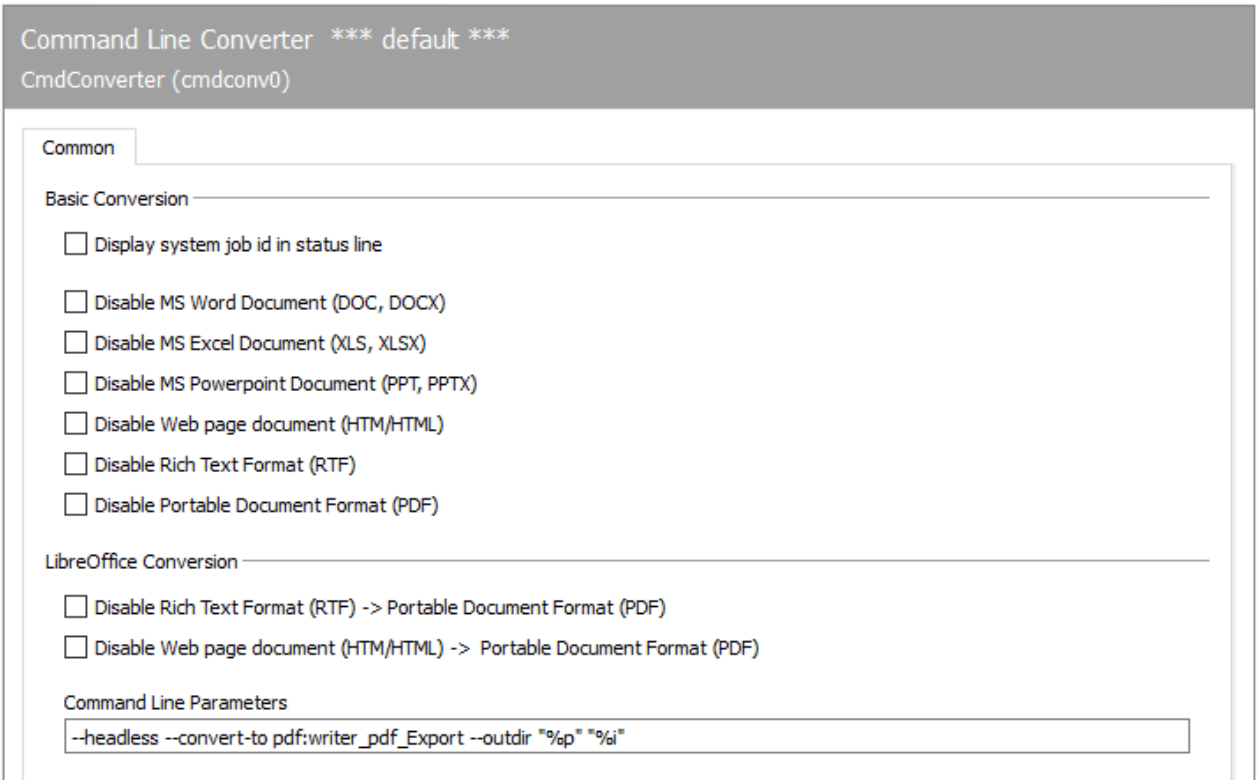
By default the *CMDCONV* can handle PDF, TIF, PNG, JPG, RTF and HTML files. If Office documents (Word, Excel and Powerpoint) should also be converted, ***LibreOffice*** can also be downloaded and installed. A final restart of *CMDCONV* activates the Office documents. The *CMDCONV* supports ***LibreOffice***, but not ***Microsoft Office*** versions. If ***Microsoft Office*** should be used for central conversion instead of ***LibreOffice***, this has to be implemented via the *OLECONV* component. To do this, the individual formats must be deactivated in *CMDCONV* and activated in *OLECONV* (DOC, XLS and PPT). Otherwise there will be overlaps and there is no guarantee that e.g. Word documents will be converted via the *OLECONV*.

10.3.2. Overview

Creation of the command line converter

In the quick launch bar of the Messaging Server configuration, call *"Converter > Cmd Converter"* and then add a new component of this type via *"New command line converter component..."*. The creation of this new component is accompanied by a wizard.

The upcoming dialogs correspond to the default wizard and can be carried out accordingly. After the converter has been successfully created, the general configuration of the component is available.



10.3.3. General

Basic conversion

Configure the converter for the use with ***Microsoft Office***.

Disable Microsoft Word documents (DOC, DOCX)

Disables the DOC & DOCX format for the *CMDCONV*. Should only be deactivated if another converter (e.g. *OLECONV*) adopts this function.

Disable Microsoft Excel documents (XLS, XLSX)

Disables XLS & XLSX format for *CMDCONV*. Should only be deactivated if another converter (e.g. *OLECONV*) adopts this function.

Disable Microsoft Powerpoint Documents (PPT, PPTX)

Disables the PPT & PPTX format for the *CMDCONV*. Should only be deactivated if another converter (e.g. *OLECONV*) adopts this function.

Disable website documents (HTM/HTML)

Disables the HTM/HTML format for the *CMDCONV*. This format is often used by ***Microsoft Outlook*** to send emails! Should only be deactivated if another converter (e.g. *OLECONV*) adopts this function.

Disable Rich Text Format (RTF)

Disables the RTF format for the *CMDCONV*. This format is often used by ***Microsoft Outlook*** to send emails! Should only be deactivated if another converter (e.g. *OLECONV*) adopts this function.

Disable Portable Document Format (PDF)

Disables the PDF format for the *CMDCONV*. Should only be deactivated if another converter (e.g. *OLECONV*) adopts this function.

LibreOffice conversion

Disable Rich Text Format (RTF)

At this point, the conversion of RTF and HTML documents using ***LibreOffice*** can be explicitly deactivated. This should only be deactivated if a ***LibreOffice*** is installed and there are display or layout problems with RTF files.

Disable website documents (HTM/HTML)

At this point, the conversion of HTML documents using ***LibreOffice*** can be explicitly deactivated. This should only be deactivated if a ***LibreOffice*** is installed and there are display or layout problems with HTML files.

Command line parameters

This parameter is used to manually control the internal PDF converter engine. This parameter should only be changed after consultation with or at the request of the hotline.

Show system job ID in status line

The job ID used to process a job is included in the status line of the received or sent job. This is used to track an order in the log files. This feature is turned off by default.

10.4. Signature converter

10.4.1. Description

This component is used to control the ***DigiSEAL*** server from Secrypt.

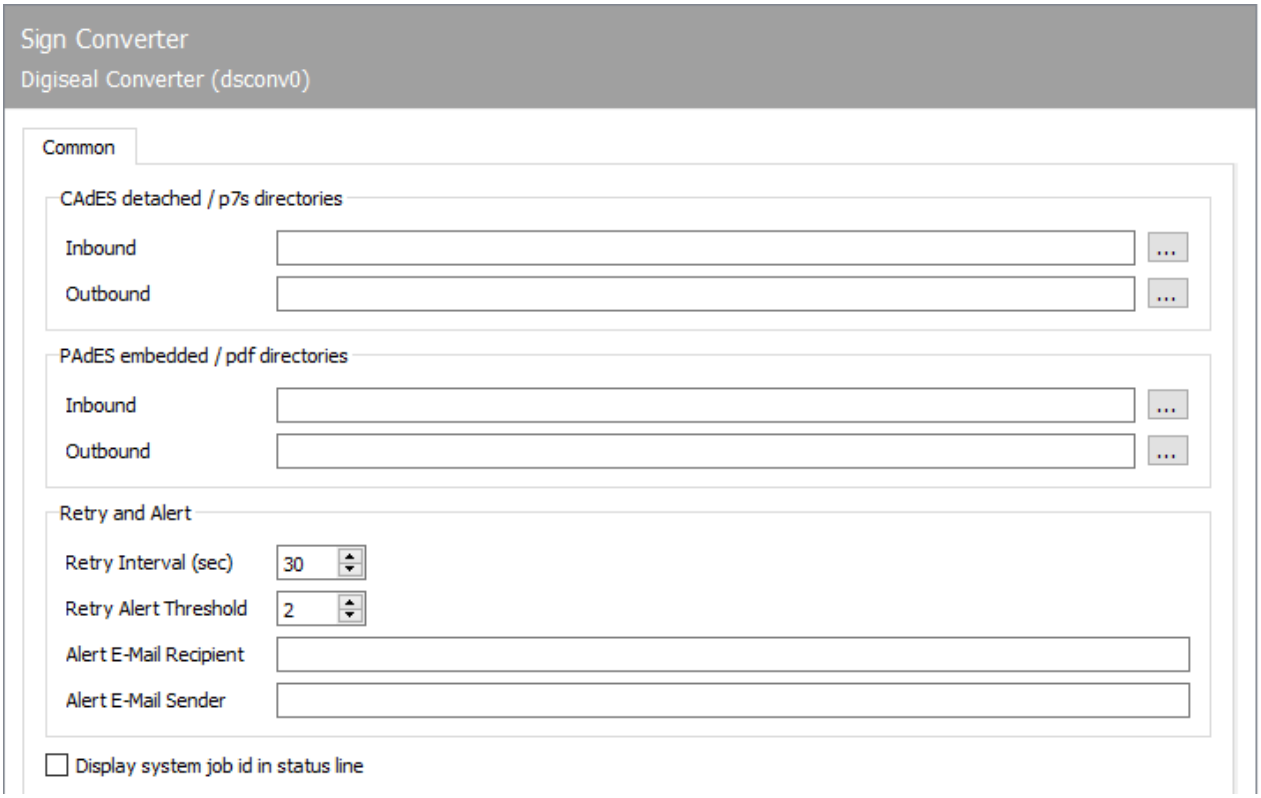
10.4.2. Overview

Creation of the signature converter

In the Messaging Server Configuration quick launch bar, go to *"Signature > Sign Converter"* and then add a new component of this type via *"New Signature Converter Component..."*. The creation of this new component is accompanied by a wizard that asks for a service account.

> **Attention!**
> This service account must be a local administrator!

The upcoming install dialogs correspond to the standard wizard and can be carried out accordingly. After successfully creating the signature converter, the general configuration of the component is available.



10.4.3. General

The DigiSEAL server is directory-based and distinguishes between two procedures for signature creation. On the one hand, documents can be signed using an additional signature file, on the other hand, an embedded signature is possible directly in the PDF document.

Signature file (CAdES)

The files to be signed are stored by *DSCONV* in the defined directory *Inbox*. There the files are signed using a signature file and moved to the initial directory. From there, signed files are received again by *DSCONV* and processed further.

> Note:
> The directories specified by the ***DigiSEAL*** server must be configured.

Embedded PDF (PAdES)

The files to be signed are stored by *DSCONV* in the defined directory *Inbox*. There the files are signed directly in the PDF document and moved to the output directory. From there, the signed PDF document is received again by *DSCONV* and processed further.

Note:
The directories specified by the *DigiSEAL* server must be configured.

Retry and Error

If the *DigiSEAL* server cannot be reached (e.g. because the license has expired), retry intervals can be configured in which the server is queried again.

Retry Interval (sec)

This value defines the repeat interval in seconds after which the *DigiSEAL* server is queried again.

Alarm threshold

The alarm threshold value specifies after how many errors an alarm should be sent via SMTP alarm. The system sends an email from the *alarm sender* to the *alarm receiver*.

Alarm transmitter

The e-mail address of the *alarm sender* can be entered here.

Alarm recipient

The e-mail address of the *alarm recipient* is defined here.

Display system job ID in status line

Activate this option if you want the system's job ID to be displayed in the status line. This is for better traceability.

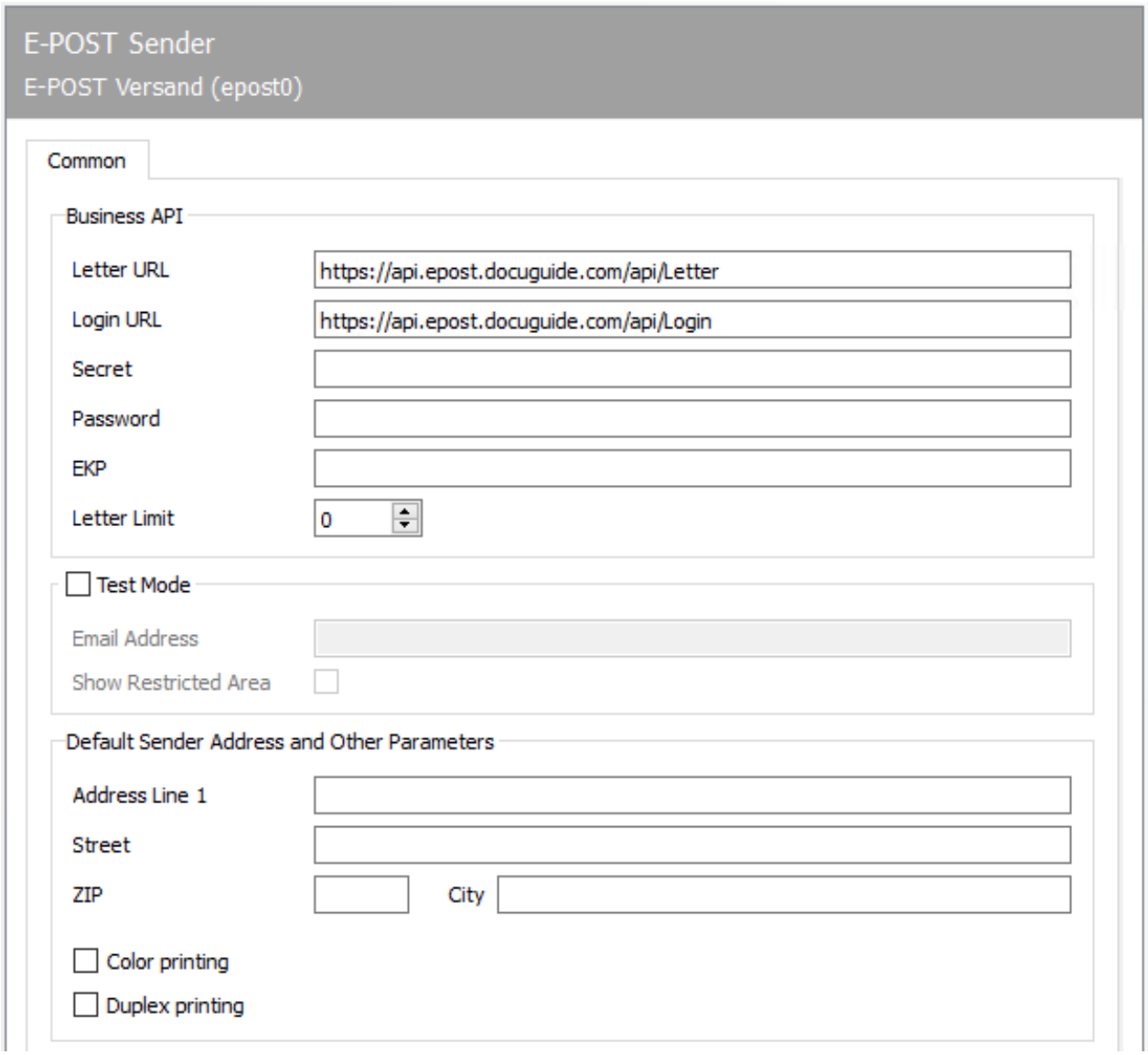
10.5. E-POST Connector

E-POST is a service provided by the Deutsche Post DHL Group, in which letters are transferred via a web interface, printed out close to the recipient's distribution center and delivered by regular mail. For the user in the company, this are the following advantages compared to classic letter mail: - Saving of inserting and franking machines, - Saving of pressure, holding stationery and envelopes, as well as - Lower postage compared to the classic letter.

The E-POST component makes it possible to send the new job type "Letter" via E-POST from the OfficeMaster Suite. This means that E-POST can be controlled directly from a CRM via the webapi interface, for example.

The E-POSTSCAN service, in which incoming mail is opened, scanned and delivered electronically, is currently not supported by the E-POST component.

Information on the registration process can be found here: https://api.epost.docuguide.com/faq



10.5.1. General

Mailing URL

The URL of the API for sending letters is specified here. As long as the post doesn't change the API, the default value can be left.

Login URL

The URL of the API for the login is specified here. As long as the post doesn't change the API, the default value can be left.

Secret

The API secret assigned by Deutsche Post is entered here.

Password

The password associated with the EKP is entered here.

EKP

The EKP is the customer number of Deutsche Post and is given in the registration letter. This value determines who ultimately pays for the stamps.

Letter limit

How many letters can be sent in one day? This serves to control costs, since letters to thousands of users can easily be ordered from a CRM system and the corresponding costs represent a risk.

Test mode

If the checkbox is active, the letters will not be sent as letters, but the orders will be sent as test e-mails to the client for checking.

E-mail address for testing

In test mode letters will not be printed for delivery, but sent as PDF attachments to the e-mail address entered here.

10.6. Filesystem Connector

The OfficeMaster Suite provides two fundamentally different APIs (Application Programming Interface).

- File interface
- Web Services

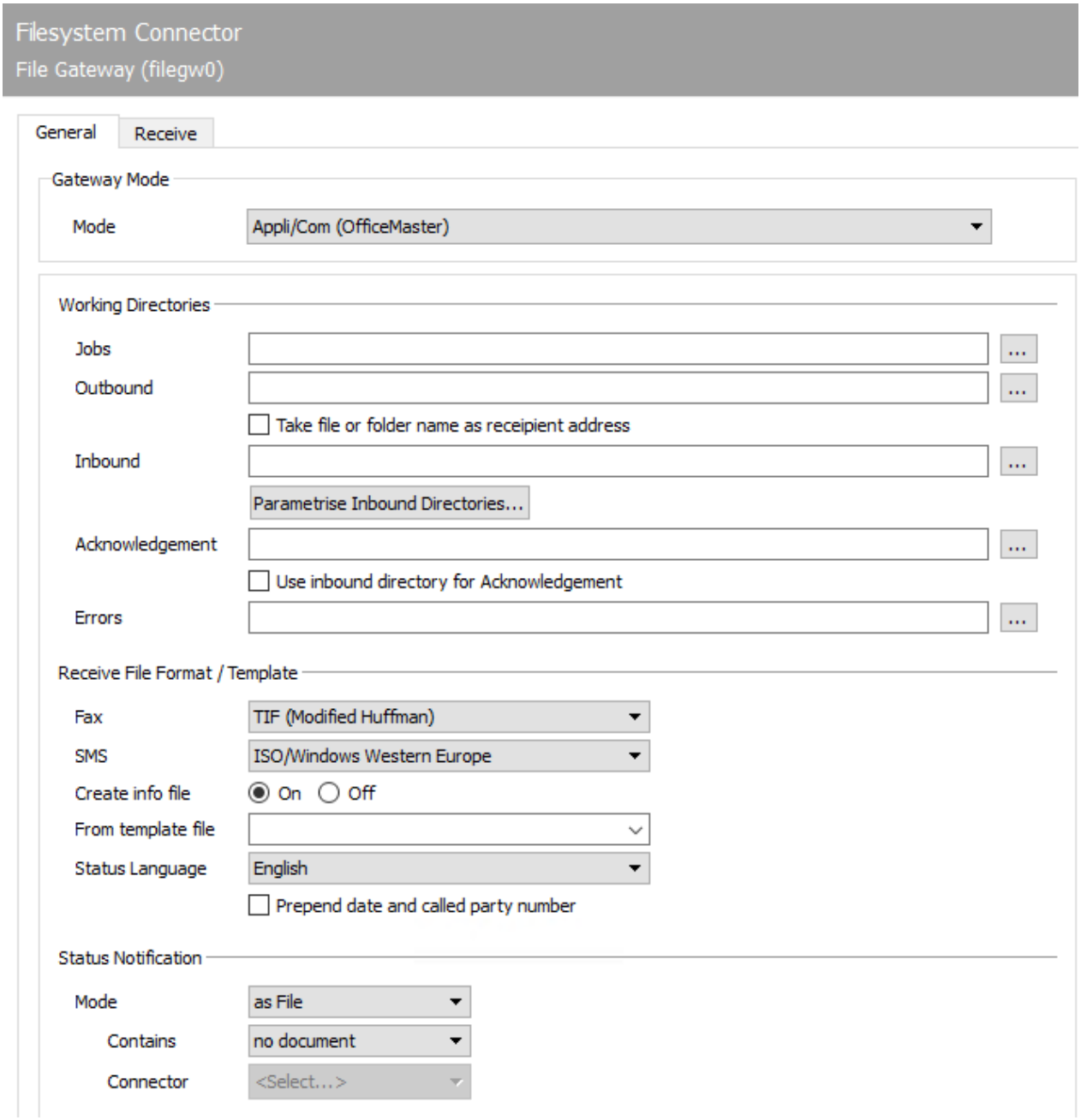
10.6.1. File interface modes

The file interface component (FILEGW) of the OfficeMaster Suite represents an interface to external systems that use files as a communication medium. In order to meet the requirements of different external systems, the file interface component can operate in different modes:

1. HP Digital Sender (MFP)
2. Xerox Work Center
3. Konica Minolta
4. Laser fax
5. Appli/Com (OfficeMaster)
6. Appli/Com (R/3)
7. Appli/Com (ValueSoft)

10.6.2. Creation of the FILEGW component

The file interface (filegw) can be created via the quick launch bar in the folder Web/File Services > Filesystem Connector > *New Filesystem Connector*.



Configuration of the file system connector (filegw)

The configuration of the file system connector (filegw) for the individual gateway modes is described below. The mode Appli/Com (OfficeMaster) is used most frequently.

General

- Gateway mode: Under ***Mode*** the connection to the individual system is specified, which should be used.

The following modes can be used:

1. HP Digital Sender (MFP)
2. Xerox Work Center
3. Konica Minolta
4. Laser fax
5. Appli/Com (OfficeMaster)
6. Appli/Com (R/3)
7. Appli/Com (ValueSoft)

10.6.3. General

Mode: HP Digital Sender (MFP)

The File System Connector in Digital Sender (MFP) mode processes documents generated by a Hewlett Packard scanner as fax messages. In this mode, text files with descriptions of the dispatch orders and the scanned documents are read from a configurable directory, transferred to the messaging server for dispatch and finally to a gateway component that enables the user to check the dispatch status. HP includes the HP Digital Sending Service with every HP digital sender and is optionally available for HP MFP products. The HP Digital Sending Service is installed on a server and transfers send jobs via a job directory to the file system connector (FILEGW) of the messaging server.

Working directories

Jobs

Both the scanned documents and the text files with the job descriptions are stored in a directory by the HP scanner. Here the file interface creates another directory with the name error. Job descriptions that could not be sent due to their incorrect content are stored there. Due to the nature of a scanner, there are no other directories for transmitting the shipping status or received documents.

Send Options

Resolution

The scanned documents can be transmitted with a vertical resolution of 200 dpi (fine) or 100 dpi (normal). The horizontal resolution is 200 dpi for each fax transmission. Although the fine

resolution ensures a higher image quality for fax transmission, the transmission times per fax page are somewhat longer.

Status Notification

Connector

The connector on the OfficeMaster Suite, via which the status message for the dispatch is to be sent, is selected as a component.

Installing the digital sending software

Installing and basic setup of the HP MFP Digital Sending Software (version 4.0) includes email setup and authentication. The fax function can be configured within the digital sending software on the *Fax* tab.

Fax method

To activate the fax function, select *LAN-Fax* as the fax method.

LAN Fax

- **Product designation:** The adaptation of the digital sending software to the capabilities of the filegw takes place via the product designation of LAN-Fax *General LanFax Product with Notification Support*. The transfer path to filegw should match that in the messaging server configuration.

For fine configuration, press Advanced. The file format for the transfer is set here, preferably MTIFF/G4 or PCL 5 (uncompressed).

Feedback in OfficeMaster format is generated via MFP user recognition. By default, the cn (common name) of the registered user is transferred to the fax as a recognition feature.

Queries from...

The login name (SAMAccountName) can serve as a substitute. This is set as a name with an attribute of...

After setting up the fax function in the *Digital Sending Software*, the fax functions are activated on the connected MFP devices. To do this, select the desired device on the *MFP configuration* tab and press *Configure the MFP device...*. In the window that appears you will find the index card *Send to Fax*. Here you tick *Enable Send to Fax*. After that, Send Faxes... is set to *via the Digital Sending Service*.

For a response to the user, the registration for fax is activated on the *Authentication* tab, otherwise the sender is unknown. These settings are sufficient for faxing and receiving feedback via the digital sending software.

10.6.4. General

Mode: Konica Minolta mode

The file interface in the *Konica Minolta* mode sends documents generated by a Konica scanner as faxes. All you have to do is specify the relevant working directories.

> **Note!**
> To send jobs from an MFP, settings are made using the Right Fax Setup Utility provided by *Konica Minolta*.

Working directories

The JOB directory is continuously monitored for new send jobs. Orders consist of the document to be sent as a TIF file and an job file that refers to the document file. The job file also contains the phone number of the recipient and the name of the sender.

Jobs

- **Status Notification:** The connector which receives the feedback message can be selected here as a component.

10.6.5. General

Mode: Laserfax

Similar to the LPD gateway, send jobs can be transferred to the OfficeMaster Suite as a file in PS or PCL format. For this purpose, the file system connector can operate in Laserfax mode.

Working directories

- **Jobs:** The filesystem Connector monitors this directory for new files with the extensions PCL, PDF, PS or TXT. It reads the embedded parameters for the outgoing job from the new file, such as the recipient's phone number or e-mail address. The file got the control commands embedded in it's document.
- **Acknowledgement & Inbound** The feedback message is stored in this directoryas a text file for each order. The associated transmission documents are saved in the Inbox directory.

Status Notification

- **Component:** Alternatively, the feedback message can be sent via a preconfigured component.

10.6.6. General

Gateway mode: Appli/Com (OfficeMaster)

The file system connector of the OfficeMaster Messaging Server in Appli/Com (OfficeMaster) mode is based on the APPLI/COM interface, which is described in the ITU standard T.611. There are separate target directories for message documents, meta information and feedback, which makes this mode of the file interface very flexible.

Working directories

- **Jobs:** Send jobs are transferred to the messaging server in the job directory. These requests consist of text files that only contain send attributes. For each job, a file with the filename extension .job is stored in the job directory. After the messaging server has read and evaluated this file, it removes it from the job directory.
- **Outbound:** Documents to be sent must be stored in the outbound directory before the associated job files are moved to the job directory.
- **Take file or folder name as recipient address:** By using the template (see section *Structure of file and folder names to interpret them as recipient addresses*) faxes can also be submitted via parameters in the file or folder names.
- **Inbound:** The messaging server stores received documents in the inbound directory before moving the associated job files to the Ack directory. These can be adjusted in more detail using the submenu **Parameterize Inbound Directories...** (A detailed description can be found in the *Parameterize Inbound Directories* section.

- **Acknowledgement:** The messaging server writes receive jobs and completed transmit jobs to the *Acknowledgement* directory. The job files stored in the *Acknowledgement* directory have the same .job file name extension as job files in the job directory. The document files associated with the send orders are deleted from the messaging server. Their names are removed from the order files before they are copied into the *Acknowledgement* directory. The document files belonging to a receive job are located in the inbound directory.
- **Use inbound directory for Acknowledgement**: If active, feedback will also be stored in the inbound directory.
- **Errors:** Job files that cannot be read due to syntactic errors are stored in the errors directory.

Receive File Format / Template

- **Fax**: File format for received fax documents
- **SMS**: File format for received short messages.
- **Create info file**: File with information about the receiving process is created.
- **From template file**: Template for an info file can be set.
- **Status Language**: Language for status messages.
- **Prepend date and called party number**: File name of the info file contains the date and phone number.

Status Notifications

- **Mode**: How should status messages be transmitted?
- **Contains**: What should status messages contain?
- **Connector**: Which component should status messages be delivered via?

Additional information

Structure of file and folder names to interpret them as receiving addresses

A template with the following structure is used: **serviceADDRESS-userinfo-usecsid-subject-oadext.ext**.

It should be noted that all fields except ADDRESS are optional and are not mandatory fields. If there is an @ in the ADDRESS field, the messaging server expects an SMTP address. If no service field (default) is specified, a standard FAX is assumed. If a field is to be left blank but a later one is to be set, the existing filling delimeter must of course still be present (e.g. ADDRESS–CSID.txt). This delimeter character is freely configurable and has the default value “-” (cfg:

OutDirSendDelimeter). If the syntax is used as the name of directories (below the set job directory), then the files stored therein will be sent according to the name of the directory. The name of the file is ignored. The individual fields have the following meaning:

field	**Meaning**
service	FAX/SMS/SMTP
ADDRESS	Destination where the document should be sent
user info	Sender and, if applicable, feedback recipient
usecsid	CSID to use for shipping
subject	Used in fax header or email subject
oadext	The sender's extension (is used if the sender's phone number is job-dependent. ext File extension/file type of the document may be used to give a converter a hint.

Dialog *Parameterize input directories*

Specific rules can be created to adapt the incoming folders. These are initially displayed without an entry. To do this, click on the *Parameterize input directory* button. *Add* opens a new dialog for creating a new customized rule.

Display name

The display name can be chosen arbitrarily, but should of course reflect the content of the respective "rule".

Base directory

A separate base directory can be selected for each input rule, on which the subdirectories described below are based.

Format

For messages that match this set of rules, the format set here is provided by the central converter.

List of job properties

####### Add

Clicking *Add* opens a dialog window. Individual rules are added to the set of rules here.

####### Rule

- **Filter:** This field is used to enter which messages are picked up by this rule. The limitation can be done using regular expressions. A list of possible commands can be found behind the button next to the input field.
- **Job Parameter:** This is where you enter which job parameter the filter should refer to. Normally it is the recipient address. The most frequently used properties can be accessed using the button behind the input field.

  Note!
  The parameter *DocumentIndex* is new here. This should be used if *PDF (status header/footer)* is set as the input format and the check mark *Use Last Extension as Filename* is also set.

- **Expand base directory by:** This specifies how the additional subdirectory created for this rule should be named. For example, with the dynamic entry **@@JobParamValue@@**, a subfolder with the extension is created for each destination number that applies to this rule. The corresponding jobs for this extension are stored there.

Preview

The description file is created based on the template set. This is the template a text file that must be located on every computer with the OfficeMaster Suite installation in the %ProgramData%\FFUMS\fmsrv\data\templates directory.

The description files created using this template have the same file extension and the same content structure. The content is defined in the template through the use of placeholders.

There is a placeholder in the template for each shipping information, such as

- @@Time@@ for the time of dispatch or receipt or
- @@Address@@ for the phone number

The template can be adapted to many formats (INI, XML, etc.), which means that the description files can take on almost any structure. By default, the description file archive.txt is installed, which contains a large selection of placeholders and can be copied and customized if necessary. The table _Parameters of a shipping order in Applicom (OfficeMaster) mode in the *further settings* section lists the placeholders.

Job formats

The send and receive jobs are text files in the ASCII character set. Each line consists of a parameter name, optional spaces, a colon, optional spaces, and the parameter value. Comments begin with a semicolon and can appear at the beginning of a line or after a parameter value.

> **Attention!**
> Umlauts (both in German and in other languages) are not part of the simple ASCII character set and should therefore be present neither in the order file nor in the file names of the documents ordered.

Transmit Jobs

Transmit jobs contain the parameters described in the table below. Any additional parameters can be added as long as this does not create a naming conflict with the parameters intended for completed transmit jobs. Fields that are not required are not written to the job file.

Table: Parameters of a transmit job in Applicom (OfficeMaster) mode

Parameter name	Description	Values
FUNCTION	Defines the type of job	SENDACK
REQID Unique identification of the order	any	
USER INFO	User name; is used for display in the messaging server	any
SERVICE	Communication service	FAX/SMS/SMTP
ADDRESS	Recipient's phone number	
FILELIST	Description of the document to be sent consisting of two parts separated by commas	
	Part 1: Format of the document file: see the following table	
	Part 2: Document file name without path	
	Can be repeated to describe jobs that contain multiple document files; missing if the POLLParameter has the value YES	
POLL	Indicates whether this is a polling order	YES, NO

Parameter name	Description	Values
USEBPS	Desired transmission speed	2400, 4800, 7200, 9600, 12000, 14400, MAX
DISABLEECM	Shutdown of ECM	YES, NO
USEDPI	Desired resolution	100, 200
USET4MODE	Desired resolution	MH, MR, MMR
HEADERS	Header	
USECSID	Sender CSID	
TRANSMITTER	From address for SMTP	
SUBJECT	Subject line for SMTP	
DSCOMPONENT	Name of a messaging server component for digital signature	e.g. E.g. signds0
SENDTIME	Specification of the start and end of the period during which the dispatch is to take place, format YYYY-MM-DD hh:mm:ss/YYYY-MMDD hh:mm:ss	2004-06-02 22:00:00/2004-07-02 06:00:00
PRIORITY	Priority, recommended values:	100...400
	100: Bulk Shipping	
	200: low priority	
	300: normal priority	
	400: high priority	
KEEPFILES	optional parameter in Applicom (OfficeMaster) mode: prevents the documents to be sent from being removed from the Out directory	YES, NO
OAD	Optional: complete sender OAD	
OADEXT	Optional: extension that is attached to a base OAD configured on the D channel	
MAXPARTS	Optional: specifies how many parts an SMS can be split into.	
NOTIFYADDRESS	Email address of a MAILGW user to be informed about the shipping status (only in Applicom (OfficeMaster) mode)	

Parameter name	Description	Values
NOTIFYNAME	Name of a MAILGW user who should be informed about the shipping status (only in Applicom (OfficeMaster) mode)	
COVER NAME	Name of a cover page file in the Messaging Server stationery directory (Applicom (OfficeMaster) mode only)	
COVERPAR	Placeholder definition for the cover page in the format =. The COVERPAR parameter can occur multiple times to define multiple placeholder values (in Applicom (OfficeMaster) mode only)	

Table: Supported file formats in Applicom (OfficeMaster) mode

Identifier	Descriptions	Fax	SMS	SMTP
TXTUTF8	Text encoded according to UTF8	x	x	x
TXTLATIN1	Text encoded according to ISO Latin 1 (Western Europe) or Windows Code Page 1252 (Western Europe)	x	x	x
TXTLATIN2	Text encoded according to ISO Latin 2 (Eastern Europe)	x	x	x
TXTWIN1250	Text encoded according to Windows Code Page 1250 (Central Europe)	x	x	x
BFF	B/W graphics for sending faxes	x		x
BMP	Microsoft Bitmap Format			x
DCX_ANY	DCX graphics file			x
DCX_FAX	DCX graphic file for sending faxes: b/w, 1728 pixels wide	x		x
DOC	Microsoft Word (required for conversion, only available on Windows)			
FFF	B/W graphics for sending faxes	x		x
GIF	Graphics format for the WWW			x
HTML	WWW			x
JPG	Compressed graphics			x
PCL	HP printer language (not included in all basic versions)	x		x

Identifier	Descriptions	Fax	SMS	SMTP
PCX	Single-page B&W graphics file	x		x
PDF	Adobe PDF (Acrobat Reader or Ghostscript required for conversion)	x		x
PNG	Graphics format for the WWW			x
PPT	Microsoft PowerPoint			x
PS	Postscript printer language (Ghostscript required for conversion)	x		x
RTF	Microsoft Rich Text (MS Word required for conversion)	x		x
SFF	B/W graphics for sending faxes	x		x
TIF_MH	B/W Tiff file with compression according to Modified Huffman	x		x
TIF_G3	B/W Tiff file with compression (Fax Group 3)	x		x
TIF_G4	B/W Tiff file with compression (Fax Group 4)	x		x
TIF_UNCMP	B/W Tiff file without compression			
XLS	Microsoft Excel (required for conversion)	x		x
ZIP				x

The next table shows an example of what the parameters of a shipping order can look like in the job file when using the Applicom (OfficeMaster) mode.

Table: Parameters in a job file in mode Applicom (OfficeMaster)

FUNCTION	SENDACK
REQID	123
USER INFO	Max Doe
SERVICE	FAX
ADDRESS	03328455960
FILELIST	BFF,000000001.bff
POLL	NO
USEBPS	MAX
DISABLEECM	NO
USEDPI	200

FUNCTION	SENDACK
USET4MODE	MMR
HEADERS	ferrariFAX
USECSID	+49 (3328) 455-960

Completed Transmit Jobs

In addition to the original parameters, completed transmit jobs contain additional entries, which are described in the table below. The FILELIST parameter present in the original send order except for fax polling is deleted from the messaging server, as are the files specified by this parameter.

For receive jobs, the FILELIST parameter is set by the messaging server. In this case, the file specified by this parameter must be deleted by OfficeMaster.

Table: Additional parameters of completed transmit jobs in Applicom (OfficeMaster) mode

Parameter name	Description	Values
BPSUSED	Transmission speed used	2400, 4800, 7200, 9600, 12000, 14400
ECUSED	Using ECM	YES, NO
DPIUSED	Resolution used	100, 200
T4MODEUSED	Encoding used	MH, MR, MMR
REMOTECSID	Recipient CSID	
FILELIST	Description of a document received during retrieval consisting of two parts separated by commas: Part 1: Format of the document file: BFF; in Applicom mode (OfficeMaster) also TIFF Part 2: Name of the document file without path information	
STATUS	Two numbers separated by a slash indicating a general status and a status-dependent error code	
STATTXT	An error text corresponding to the Status field	

10.6.7. General

Mode: R/3

In Appli/Com R/3 mode, Filegw can exchange orders with SAP R/3 systems. This operating mode is only available for existing customers. For new installations, the use of the SAP component is recommended.

The following directories must be configured for the exchange of orders: - **Jobs**: Directory in which order files are transferred - **Acknowledgement**: Directory in which feedback is given - **Errors**: Directory in which erroneous orders are stored. - **Inbound**: Directory for the document inbox. - **Outbound**: Directory for the document output.

Jobs

job properties

File Extension

The file extension for the job files is specified here, default value *job*.

10.6.8. General

Mode: Valuesoft

In Appli/Com Valuesoft mode, Filegw can exchange jobs with Valuesoft systems.

The following directories must be configured for the exchange of orders: - **Jobs**: Directory in which job files are transferred - **Acknowledgment**: Directory in which acknowledgments are sent - **Errors**: Directory in which erroneous orders are stored. - **Inbound**: Directory for incoming documents. - **Outbound**: Directory for document outbound.

Jobs

job properties

File Extension

The file extension for the job files is specified here, default value *job*.

Receive Formats

Desired reception formats for received documents can be selected in the list.

10.6.9. General

Mode: Xerox Scanners

Xerox Workcentre offers the possibility to fax scanned documents directly with OfficeMaster. To do this, Xerox Workcentre communicates with the OfficeMaster Suite's file system connector.

Working directories

- **Jobs:** The Jobs directory is continuously monitored for new send jobs from the Xerox Workcentre. Orders consist of the document to be sent as a TIF file and an order file that refers to the document file. The order file also contains the phone number of the recipient and the name of the sender.

Status Notification

- **Connector:** Here you can specify the gateway component, which should process the feedback message.
- **User:** The status message is sent to the user who has the login used at the Xerox Workcentre as the fax address in the address book.

The order format

A job directory is created for each job in the transfer directory. The name of teh directory ends with in .xsm. The job description file is located here. It's name ends with the extension .xst. It is a text file divided into several sections.

Each section begins with a line containing only the section name enclosed in square brackets.

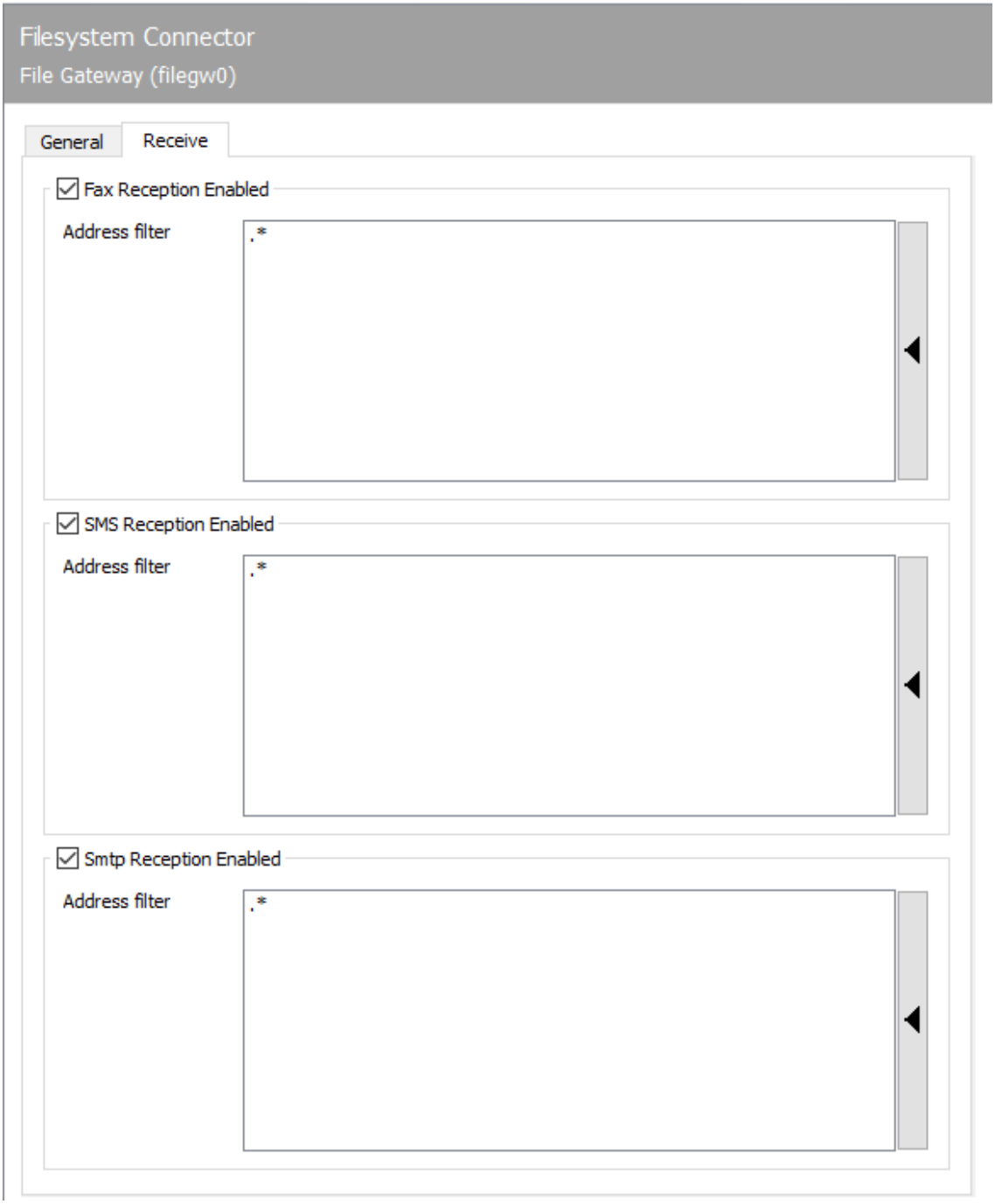
- This is followed by a line containing nothing but an opening curly bracket.

- The section ends with a line that contains a closing curly bracket.
- A status string enclosed in round brackets can follow.
- The last line of a section contains only the keyword *end*.

There can be any number of lines with parameters between the lines with the opening and closing brackets. Each line begins with a character string that defines the type of parameter. This is followed by the name of the parameter, an equal sign (=), the value of the parameter, and a semicolon(;). The value of the parameter can be enclosed in double quotes. Empty lines can appear anywhere in the job description file.

In the _doc_object xrx*document* section of the job description file is the value *DocumentObjectName*. Supplemented by the string .dat, this value specifies the name of the document list file. The document list file only contains lines with the names of the document files belonging to the job. These files must be of type TIF. The file names are specified without specifying the path.

Section	**name**	**meaning**
doc_object xrx_document	Resolution	Resolution: RES_FAX_FINE or RES_FAX_STANDARD
—-	DocumentObjectName	Name of the document list file without the path and without the filename extension .dat
service xrx_svc_general	NetworkUsername	Name of the user to whom the order is to be assigned
service xrx_svc_fax	PhoneNumber	Fax number to dial



10.6.10. Reception

The Reception tab has a direct impact on the incoming documents. The phone numbers (Called Party Number) for which the file system connector (filegw) should accept faxes or SMS messages are defined here. With the default setting (.*), all received faxes or short messages are processed.

In the event that SMTP messages are also sent via the OfficeMaster Suite, these would be processed by Filegw based on the standard setting **".*"**.

A change may be necessary if received messages are to be distributed to different gateways, such as msxbcsgate, sapconn, filegw, etc., or if OfficeMaster messages are only to be received on certain phone numbers. If this should take place, the so-called whitelist procedure, can be activated under Tools > Black & Whitelist > Reject undeliverable messages.

> **Note!**
> If the address filter is restricted to certain phone numbers without an activated whitelist procedure, the UNDELIVERABLE component of the messaging server should be configured in order to avoid the “silent” storage of received messages regardless the best address filter configuration.

In the simplest case, an address filter consists of a list of numbers that are assigned to the connector. For example, if all faxes of the numbers 150 to 154 should be routed to the Exchange Connector, the address filter list contains the following entries: 150 151 152 153 154

The entries in this list can be combined with regular expressions into one entry 15[0-4].

The default value (.*) for the address filter is also a regular expression. The dot (.) stands for any character. The asterisk gives the character in front of it the meaning as often as you like. At this point, only one address can be specified per line. It is not possible to combine several expressions in one line using OR (|) or AND (&).

10.7. SMS via USB modem

The sending/receiving component *GSMSMS* of the messaging server is responsible for sending and receiving short messages (SMS) with a GSM Modem. A GSMSMS component communicates with one or more GSM Modem(s) via the serial ports (*COM ports*) and USB ports (*USB Ports*). The modems are controlled by AT commands (Hayes). Traditionally, serial interfaces were used, which were later replaced by serial communication channels on USB. Modems are also available, which are controlled via TCP by the LAN-Interface. Special hardware (USB to LAN) adapters are needed for this. A messaging server system supports the operation of several GSM components.

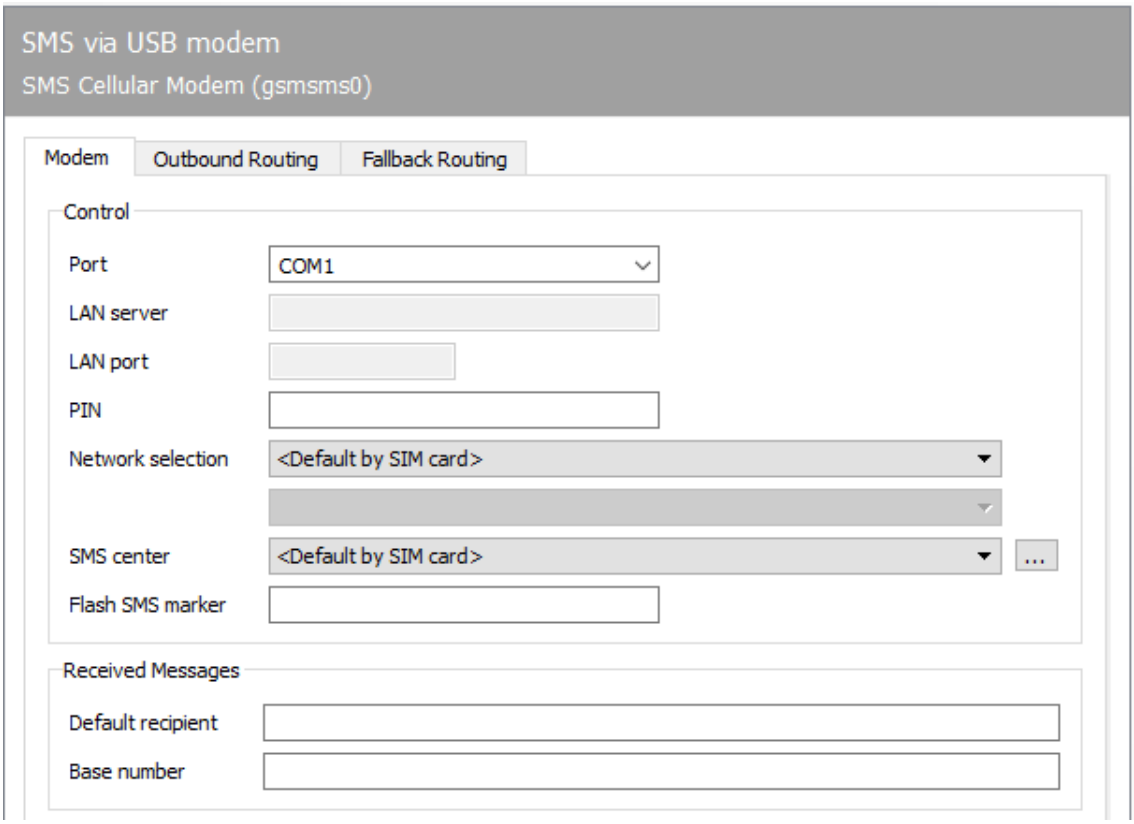
10.7.1. Create GSMSMS component

A GSMSMS component (usually *gsmsms0*) can be created in the default installation of the messaging server. If no GSMSMS component exists or another one has to be added, it can be added either via the component table or via the *SMS via GSM Modem* configuration dialog. A GSMSMS component can be created with *Create component*.

> **Note!**
> It is also possible to connect modems over the network via *COM/IP converter*.
> Please ask at support or in the Ferrari electronic AG forum for compatible solutions.

10.7.2. Configure GSMSMS component

The configuration can be achieved via the menu sequence Edit > Further Sender/Receivers > SMS via GSM Cellular Engine. A GSMSMS component can serve several modems, with each modem operating on its own serial/usb port on the server. The configuration takes place per connection or GSM Modem. The selection list at the bottom of the configuration determines which GSM modem is to be configured. The selection list only appears if more than one modem has been set for this GSMSMS component. To add or remove GSM Modems, the appropriate button next to the selection list is selected.



10.7.3. modems

The standard information and the connection information for the modem are entered on the *Modem* index card.

Steering

Connection

For each radio modem, GSMSMS must be informed of the serial port on which the GSM radio modem is located. On Windows, the serial ports are addressed by *COM1*, *COM2*, and so on.

LAN server

If LAN was selected for connection, the address of the GSM modem in the LAN can be entered here.

LAN port

If LAN was selected for connection, the TCP port of the GSM modem in the LAN can be specified here.

PIN

In addition to the connection, the PIN of the SIM card is required, which GSMSMS should use to communicate with the radio modem. If GSMSMS uses the wrong PIN several times for the authorization check, the SIM card will be blocked. In this case, the SIM card must be inserted into a conventional mobile phone and unlocked by entering the PUK code or Super PIN.

Select network

The mobile network is dictated by the SIM card used. In regions close to the border, however, the radio modem can automatically switch to a foreign provider if the home network is (temporarily) unavailable. Since roaming charges may apply to third-party networks, the mobile network can be specified with *Choose network*. If the specified home network is not available, the send orders are reported to the sender as incorrect.

SMS center

The phone number of the SMS center is usually included on the SIM card when it is delivered. If another SMS center is to be used for sending SMS, its number must be entered. This makes sense for mobile phone providers who offer several SMS centers with different transmission fees (e.g. one SMS center for private customers and one for business customers).

Flash SMS marker

Based on the flash SMS tag, GSMSMS recognizes which short message should be sent as a flash SMS. A flash SMS is immediately signaled to the recipient on the mobile phone display. If the beginning of the short message to be sent matches the flash SMS marking stored here, the message is sent as a flash SMS.

Received messages

Received short messages are read out of the radio modem by GSMSMS and further processed in the messaging server. The decisive criterion for the further processing of received messages in

the messaging server is the number to which the message was sent. In the case of short messages received via landline SMS, this number is specified in the ISDN. However, short messages received via GSMSMS do not have any phone numbers that can be evaluated.

Default recipient

In order to distribute messages received via GSM in the messaging server, a phone number can be configured as the default recipient, which is assigned to all received messages that do not contain any recipient information.

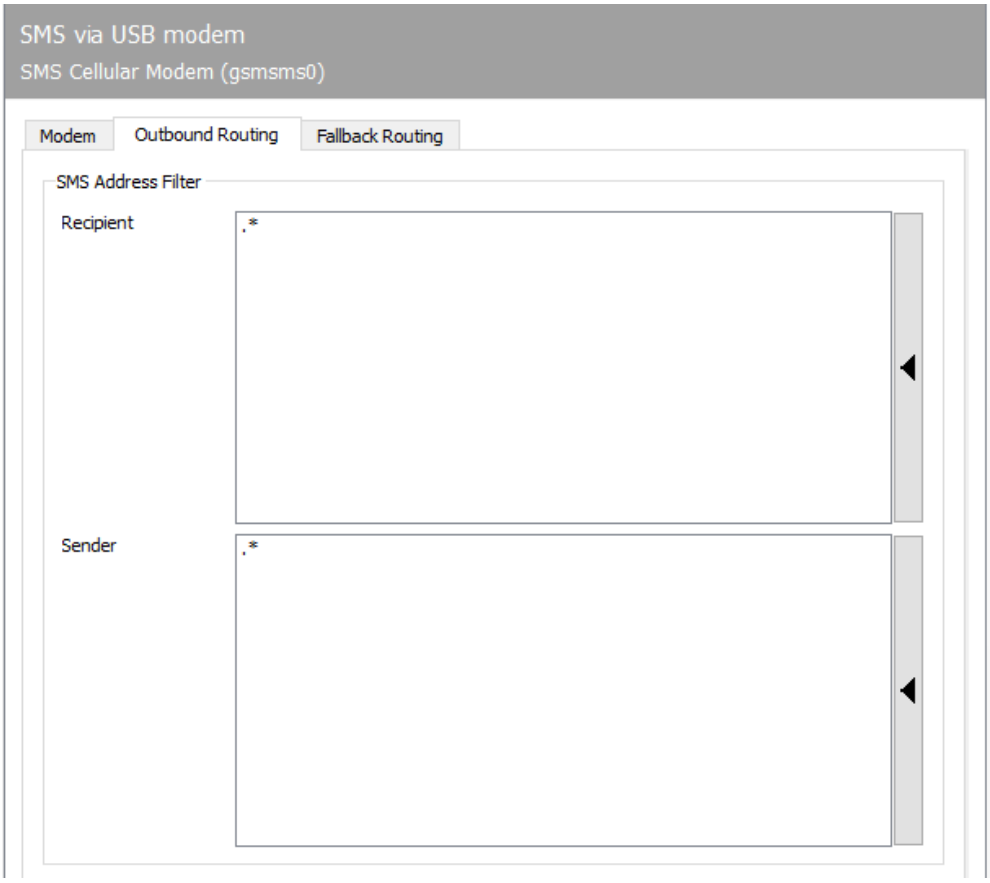
Base number

The sender can specify the recipient in the text of the SMS. It must appear at the beginning of the SMS, begin with a period and end with a period.

> Example:
> Does the short message have the content *.960. This is an SMS*, the *960* is removed from the SMS text and interpreted as the recipient information.

The configured base number is used as a prefix for the recipient information, so that the base number and recipient information result in the phone number for further processing of the message.

> Note!
> The recipient information does not have to be written as a number in the SMS. For convenience, the letters associated with the number are also used as Recipient information interpreted. For example, behind the recipient *FERRARI* the phone number *3377274*.



10.7.4. Routing (outgoing)

Address filter for SMS

If short messages are to be sent by the messaging server in several ways, e.g. via a GSM radio modem, via ISDN (as landline SMS) and via provider SMS, it makes sense to set up routing for SMS send jobs. There is also an *address filter for SMS* on the *Routing (outgoing)* tab.

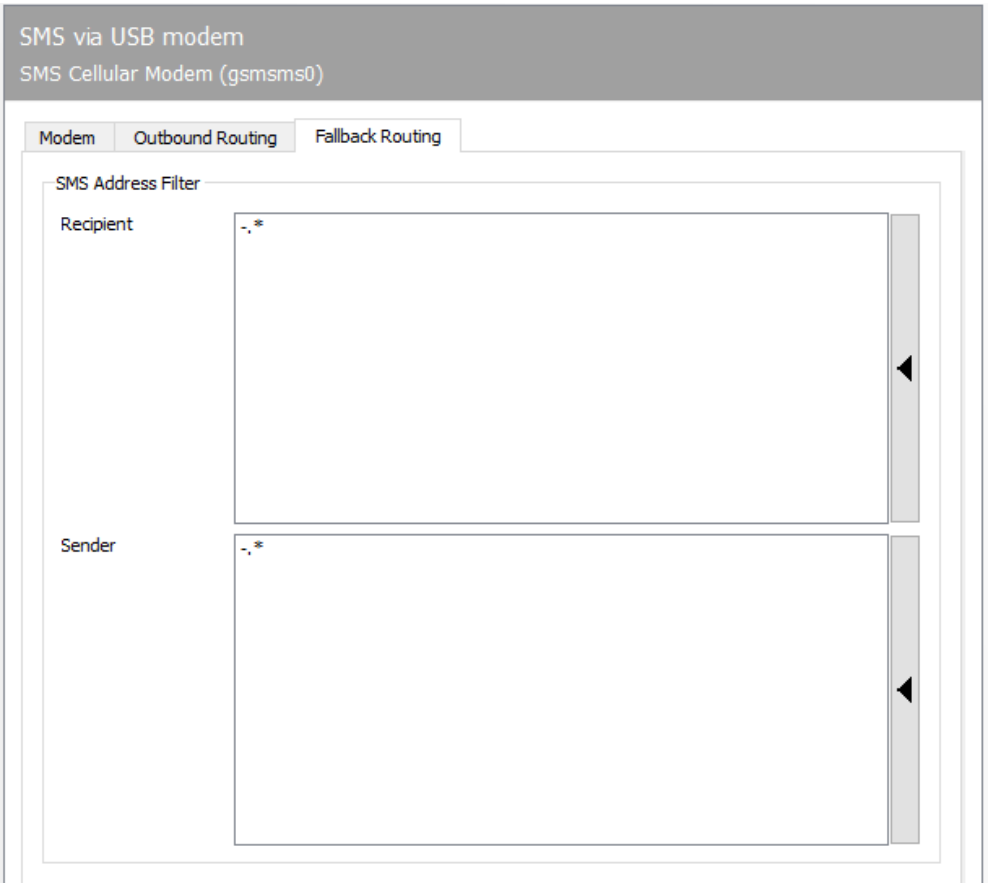
In the simplest case, the complete telephone numbers of *sender* and *recipient* can be entered as an address filter. To make things easier, you can also configure the address filter using regular expressions.

Basic configuration

When selecting the SMS service to be used, the first-match principle applies: the first GSM radio modem, the first ISDN connection or the provider SMS provider whose SMS address filter matches the sender and recipient phone number of the send order, is used for shipping.

> **Note!**
> If short messages are only to be sent via GSMSMS and not via ISDN (*OMCUMS*), it is

in most cases easier to switch SMS dispatch to to deactivate the relevant ISDN connections.



10.7.5. Fallback routing

Fallback routing is applied if it is activated under Extras > System settings and the corresponding number of redials has been reached.

Address filter for SMS

If short messages are to be sent by the messaging server in several ways, e.g. via a GSM radio modem, via ISDN (as landline SMS) and via provider SMS, it makes sense to set up routing for SMS send jobs. There is also an *address filter for SMS* on the *Routing (outgoing)* tab.

Recipient sender

In the simplest case, the complete telephone numbers of *sender* and *recipient* can be entered as an address filter. To make things easier, you can also configure the address filter using regular expressions.

Basic configuration

When selecting the SMS service to be used, the first-match principle applies: the first GSM radio modem, the first ISDN connection or the provider SMS provider whose SMS address filter matches the sender and recipient phone number of the send order, is used for shipping.

> **Note!**
> If short messages are only to be sent via GSMSMS and not via ISDN (*OMCUMS*), it is in most cases easier to switch “SMS dispatch to” to deactivate the relevant ISDN connections.

10.8. Transfer protocol

10.8.1. Preparation

Create a service account and add it to the local administrators group on the fax server's operating system. The service account must later be made the database administrator. If you have already created components such as *msx2kgate or oleconv*, you can also use the service account that is already used here.

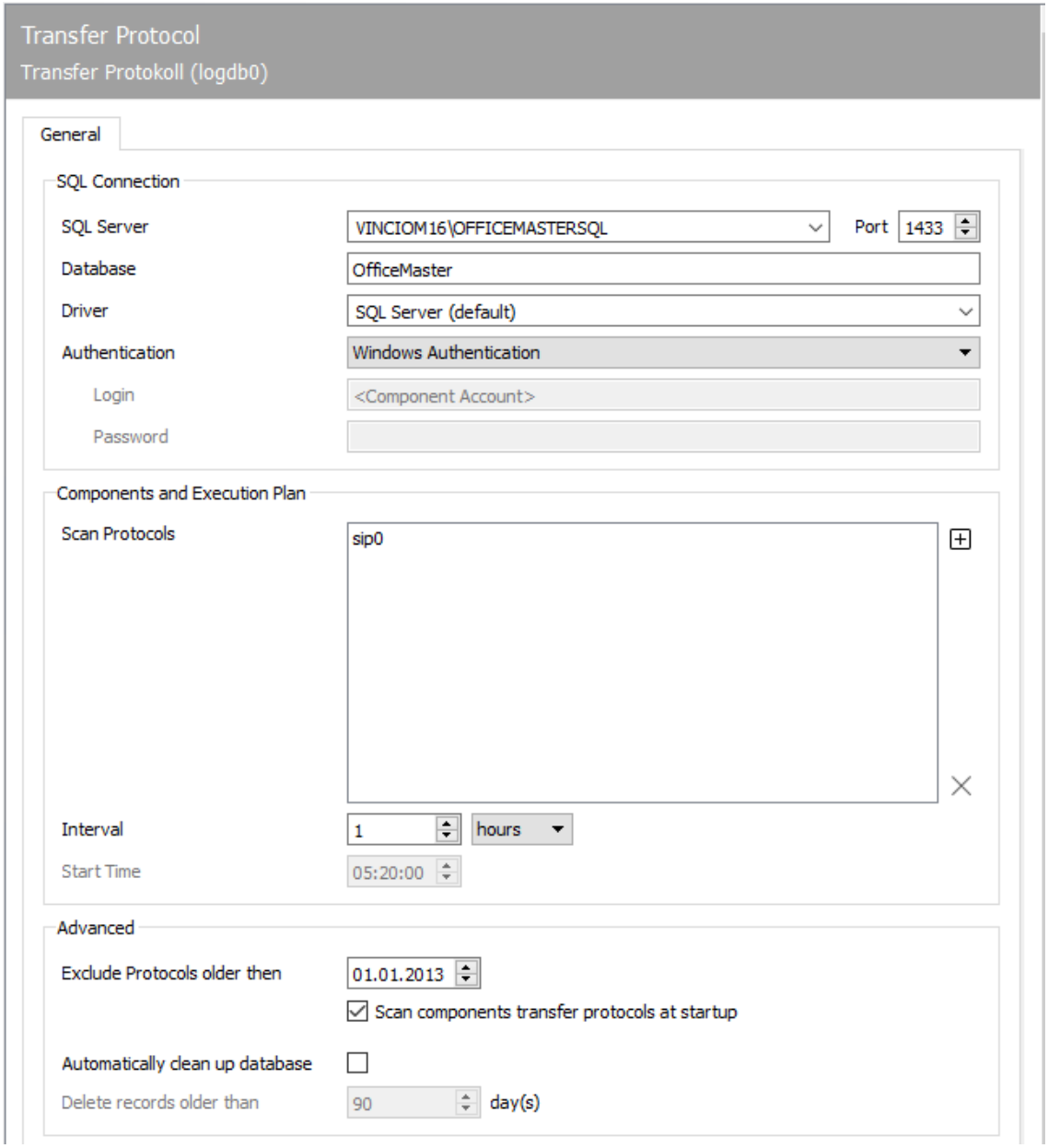
10.8.2. Installation

It is advisable to create the Logdb component via the quick launch bar > Transfer DB > New transfer log component.

During the installation wizard, select the desired data storage:

- **New SQL Server Instance:**
  an automatic installation process of a SQL-Server 2014 Express follows (mouse click on the blue link).
- **Choose an existing SQL server in your environment:**
  Please specify the SQL server to be used and the database to be used. It should be noted here that the *Service Account* has write access to the database.

When asked about *Service account*, enter the service account that has already been created.



10.8.3. General

SQL connection

SQL Server

Enter SQL server and instance

Database

Store the database to be used

driver

Drivers for the SQL connection can be selected here

Authentication

If you do not want to access Windows authentication here, you can also switch to internal SQL Server access and enter a user accordingly.

Components and execution plan

Scan logs

The *+ - character* can be used to select the transfer log files to be scanned. It is advisable here to select all files from the components that have been configured in the OfficeMaster Suite.

Interval

Configure scan interval. If *Days* is selected, the start time on the day can also be configured.

Extended

Logs not older than

Scan logs that are not older than the set date. If the *Scan transfer logs after start-up* box is ticked, the transfer logs will be scanned each time the component is started, regardless of the set scan interval.

Clean database automatically

Here you can set the age at which data records should be removed from the database.

10.9. Line printer daemon

Print integration in third-party software

10.9.1. Send documents as a fax or email attachment

The advantages of OfficeMaster are evident when sending business documents such as offers, orders, reminders, etc. The easiest way to integrate into the existing commercial ERP software (e.g. Axapta, cd2000, Infor, Navision, proALPHA, sage KHK, SAP Business One, Varial) is to use the print function.

The business documents are output on OfficeMaster, possibly provided with an electronic signature and sent as a fax or as a PDF attachment to an e-mail. After sending, the ERP user receives the sending status via e-mail in his mailbox (Microsoft Outlook, Notes).

For the print order, OfficeMaster Messaging Server offers an LPD gateway that accepts print data, creates the necessary send order and thus determines the further processing of the print by the system. The print data includes the document to be sent and information such as the name of the printed file and the network name of the user who is printing, which can be used to assign the process to a user and to provide the transmission status.

OfficeMaster takes the information required for sending, such as the fax number, e-mail address of the recipient, time of sending, etc., directly from the document. To do this, this information must be specified in several commands embedded in the document of the ERP system. These commands are referred to below as control commands.

The table below shows the individual processing steps that a document goes through when it is sent with OfficeMaster.

OfficeMaster Messaging Server	**Description**	**processing step**
	ERP client at user workstation or ERP server	Outputs the document with embedded control commands to the printer set up for OfficeMaster.
	Printer with printer spooler and IP address & printer queue configured for OfficeMaster	Converts the printed document to a print format (PCL, PDF, PS or Text) and sends it via LPR to the IP address of OfficeMaster
LPD	Line Printer Daemon	

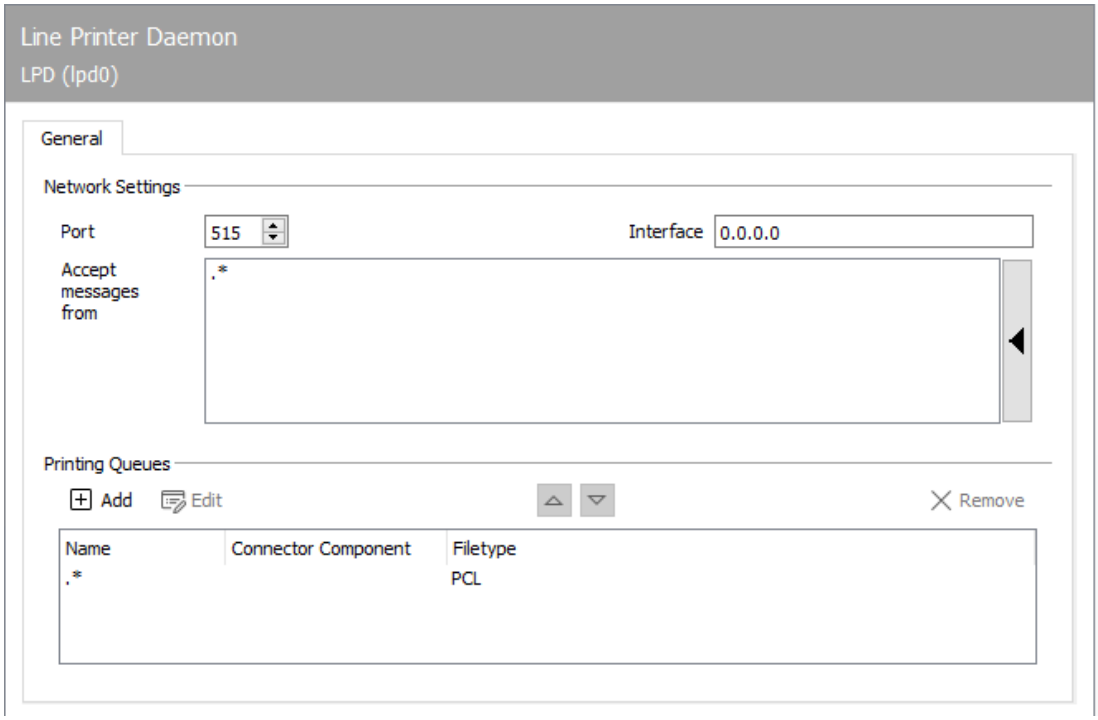
OfficeMaster Messaging Server	Description	processing step
		Receives the document and other print data (sender and file name) and determines the further processing steps based on the printer queue used by the printer
CMDCONV / CONV / OLECONV	Converter with internal PCL converter and/or AFPL Ghostscript	Converts the document from the print format to graphics (for fax) or to PDF (for e-mail) and extracts the contained control commands
NOTESCONN, MAILGW, FILEGW, MSX2KGATE, CLIENTGW, ...	Connector for Notes, mail gateway, file interface	Assigns the document to a connector user based on the LPD sender and creates the send job with user-specific parameters (such as your own fax ID)
OMCUMS / SIP (for fax)	ISDN hardware control or SIP	Sends the document as a fax via the configured ISDN hardware or SIP interface
SMTPTX (for email)	Mail sender	Sends the document as a PDF/email attachment via SMTP
NOTESCONN, MAILGW, FILEGW, or CLIENTGW	Gateway for Notes, mail gateway, file interface or web client	Provides the gateway user with the send status (NOTESCONN by Notes mail, MAILGW by email, FILEGW by file)

The connection of an ERP system using LPD is therefore quite complex and requires one-off settings in the ERP system used, in the mail system and on some components in the OfficeMaster Messaging Server. The following table provides an overview of the necessary and optional configuration steps.

Add and configure LPD gateway

To configure the LPD gateway, select Edit > Other Connectors > Line Printer Daemon in the Messaging Server Configuration. All LPD gateways that are available in the messaging server system are displayed in the quick launch bar. By default, this is the gateway lpd0.

> **Attention!**
> A prerequisite for the proper operation of the LPD is that no print server is installed on the system!



10.9.2. General

For example, the LPD gateway should be called lpd0. The host should be the IP address or resolved name of the server on which the LPD gateway is to run (usually the main server). The new settings are then applied and the display is updated.

The default settings of the LPD gateway are suitable for the majority of installations and only need to be changed in the following cases (sorted by frequency):

1. OfficeMaster Suite (10) and OfficeMaster Suite (25) do not have a PCL converter (parameter to be adjusted: file format).
2. The LPD send requests are to be processed by a gateway such as the fax connector for Exchange (MSX2KGATE), the fax gateway for Notes (NOTESCONN), the mail gateway (MAILGW) or the file interface (FILEGW). This is necessary, for example, if OfficeMaster is also to send the business documents as an e-mail.
3. The LPD gateway should either accept orders on a different port, only on certain IP addresses (parameters to be adjusted: port, interface, process messages from). In the latter case, the parameters must be changed in the Network frame. For 1 to 3, the rule entered in the printer queue frame must be adjusted or new rules must be added.

Network settings

The network settings can also be made on the same tab.

Ports

By default, the LPD gateway receives the data streams on the designated port 515 (so-called well-known port). In this case, the applications printing via LPD/LPR must also send their data streams to the new port. However, when setting up a printer driver, this port cannot be adjusted on the Windows side.

Interfaces

Similar to the port setting, the IP address can be specified as the interface on which the LPD gateway should wait for incoming data streams. This is particularly useful on servers with multiple network cards and router functions, where the LPD gateway should only accept data streams from one network segment. With the default setting 0.0.0.0, the LPD gateway binds itself to every interface or to all IP addresses and accepts send requests from all network segments.

Process message from

Under *message process from* can be used to specify a list of IP addresses that are allowed to send data to the LPD gateway using regular expressions. With the default setting (.*), the LPD gateway accepts data streams from any IP address.

Printer queues

How the received data streams are further processed in the messaging server is controlled via the printer queue on which the sender prints the send jobs. In the factory setting, send jobs are processed identically, regardless of which printer queue they were printed to.

> Note!
> The printer queue is determined by the printing sender. The name ".*" entered in the standard only has to be changed if send jobs are to be processed further by different messaging server connectors, e.g. Faxes through *MSX2KGATE* and e-mails through *FILEGW*. The LPD gateway must differentiate between the printer queues by creating a rule for each printer queue to be differentiated.

Name

The name of the printer queue can be stored in plain text and as a regular expression. By default, send requests to all printer queues (.*) are processed in the same way. The name only

has to be configured if several rules have been created in order to implement different processing paths based on the queue used.

Gateway component

After the LPD gateway has received a send job, it is forwarded to the gateway component configured for the print queue. The gateway component checks the order (“May the sender send documents?”), sets user-specific sending parameters (“Should the order be signed?”) and ensures that the sender receives a status message once the order has been sent. Depending on the existing OfficeMaster license, the following gateway components can or should be used:

Table: Gateway components depending on the environment

Messaging Server Component	Shipping methods supported with LPD	SMTP	Notes	Exchange	clientgw
Connector for Exchange (MSX2KGATE)	Fax	-	-	X	-
Gateway for Notes (NOTESCONN)	Fax and Email	-	X	-	-
Mail Gateway (MAILGW)	Fax and Email	X	-	-	-
File interface (FILEGW)	Fax and Email	optionally	optionally	optional	optional
CLIENTGW	Fax	-	-	-	X

file format

Because the file format that needs to be received by the LPD gateway and converted by the messaging server cannot be determined automatically, it needs to be configured for each individual print queue rule. File formats that can be converted by OfficeMaster Messaging Server are PCL (Printer Common Language), PDF (Portable Document Format), PS (Postscript) and TXT (ASCII text). OfficeMaster Messaging Server has its own converter in Windows environments for converting TXT and PCL to graphics (for fax) or PDF (for e-mail).

> Note!
> The PCL converter is only included in the user-free OfficeMaster, so customers with OfficeMaster 10 or OfficeMaster 25 must use the PS conversion. To do this, AFPL Ghostscript must be downloaded, installed and set up on the server.

> Note!
> At first glance, the use of AFPL Ghostscript appears to be disadvantageous due to

the additional installation effort, but searchable PDF documents (for e-mail!) can be created through PS conversion. When using the PCL converter, the printed document is integrated into the PDF file as a bitmap.

Connector for Microsoft Exchange (MSX2KGATE)

The LPD send order is assigned to the Fax Connector for Exchange (MSX2KGATE). MSX2KGATE recognizes the process as an LPD send request and checks the user-specific parameters in the Active Directory. MSX2KGATE then initiates the sending of the document. In order to identify the Active Directory user, either the login name of the LPD user received from the LPD gateway or the fax address contained in the control command of the document (U parameter) is used. This is compared with the users' FAX addresses stored in the Active Directory. For this purpose, each Active Directory user can be provided with several FAX addresses, e.g. with a FAX address for fax receipt or identification and a FAX address for the assignment of LPD send jobs.

Example:
Is the control command contained in the document
@@+FAX:<fax number>@@
the document is assigned to the Active Directory user whose FAX address in Exchange matches the login name (LPD user) received when printing. If the login name of the LPD user cannot be used for user assignment because the print process is always triggered by an automatic server task under the same login name, for example, the responsible Active Directory user can be transferred in the control command using the U parameter:
@@+FAX:<fax number>;U<AD user fax address>@@.

Connector for Notes

Print or send jobs forwarded to NOTESCONN by the LPD gateway are assigned to a Notes user in the name and address book. NOTESCONN uses either the LPD name that was transmitted as the sender when printing, or the name that was contained in the embedded control command as a U parameter. As soon as the name is available as a U parameter, it is searched for.

Example without U parameters:
The user is logged into the network with the user account MUSTERMANN and prints an offer from the ERP system that contains the following control command:
@@+FAX:0123/456789@@
The LPD gateway receives the offer with the user information MUSTERMANN and sends it to NOTESCONN as a send request. NOTESCONN is now looking for a personal document for MUSTERMANN in the name and address book and checks

user-specific data, whether MUSTERMANN is allowed to send, which fax ID should be communicated to the recipient, etc. NOTESCONN then transfers the document to the messaging server as a send order to 0123/456789 and later provides sends the receipt to the Notes user.

If there is a U parameter:

Example with U parameters:
The user is logged into the computer network with the SAMPLE user account and prints an offer from the ERP system that contains the following control command:
@@+FAX:0123/456789;U SALES@@
The LPD gateway receives the offer together with the user information MUSTERMANN and forwards it as a send order to NOTESCONN, which is looking for a personal document for SALES to find the user-specific data etc. in it and the messaging server with the fax dispatch to 0123/ 456789 to commission. Irrespective of whether the LPD user name is determined from its network login name or from the U parameter of the control command, this name must be found in the name and address book configured for NOTESCONN. The user name is searched for in the alias field here, provided no other settings have been made in the NOTESCONN configuration.

SMTP connector/mail gateway

The mail gateway (MAILGW) processes LPD send requests in a similar way to the gateway for Notes (NOTESCONN). First, the corresponding MAILGW user is searched for using the LPD sender. Either the sender name that was communicated to the LPD gateway upon receipt of the print job or the sender name that was specified in the embedded control command of the printed document as a Uparameter is used as the sender. Here, too, the sender name given as a U parameter is treated preferentially.

Example without U parameters:
The user is logged into the computer network with the SAMPLE user account and prints an offer from the ERP system that contains the following control command:
@@+FAX:0123/456789@@
The LPD gateway receives the offer together with the user information MUSTERMANN and sends it to MAILGW as a send order. MAILGW searches for a user named SAMPLE and checks user-specific data, e.g. whether SAMPLE is allowed to send or whether SAMPLE is authorized for the signature server specified in the control command. MAILGW then transfers the document to the messaging server as a send request to 0123/456789 and later sends the receipt to the user by email.

Example with U parameters:
The user is logged into the computer network with the SAMPLE user account and

prints an offer from the ERP system that contains the following control command:
@@+FAX:0123/456789;U SALES@@
The LPD gateway receives the offer together with the user information MUSTERMANN and sends it to MAILGW as a send order. MAILGW is looking for a user with the name SALES to find the user-specific data and instruct the messaging server to send the fax to 0123/456789. To assign the process to a user, the mail gateway compares the determined name either with the user name stored in the mail gateway (with user administration on MAILGW) or with the user name stored in the directory service (with user administration via LDAP).

Send data via LPR command

After installing and configuring the LPD gateway, the function should first be tested without the interaction of third-party software (such as Winword). Since this can only be done with files (PCL, PS or TXT) that can be converted by the messaging server, create a text file with some example sentences and insert a simple control command:

Example:
@@+FAX:03328/455-960;EFerrari electronic AG@@
This is my first fax using LPD and OfficeMaster Messaging Server.
To send this file to the LPD gateway manually, use the *lpr* command under Windows. In order to transfer the created text document to the LPD gateway as an e-mail send order, the fax number is converted into an e-mail address.
@@+FAX:info@ferrari-electronic.de;EFerrari electronic AG@@
@@+PAR:from=sender@ferrari-electronic.de@@
This is my first email via LPD and OfficeMaster Messaging Server.

Please note

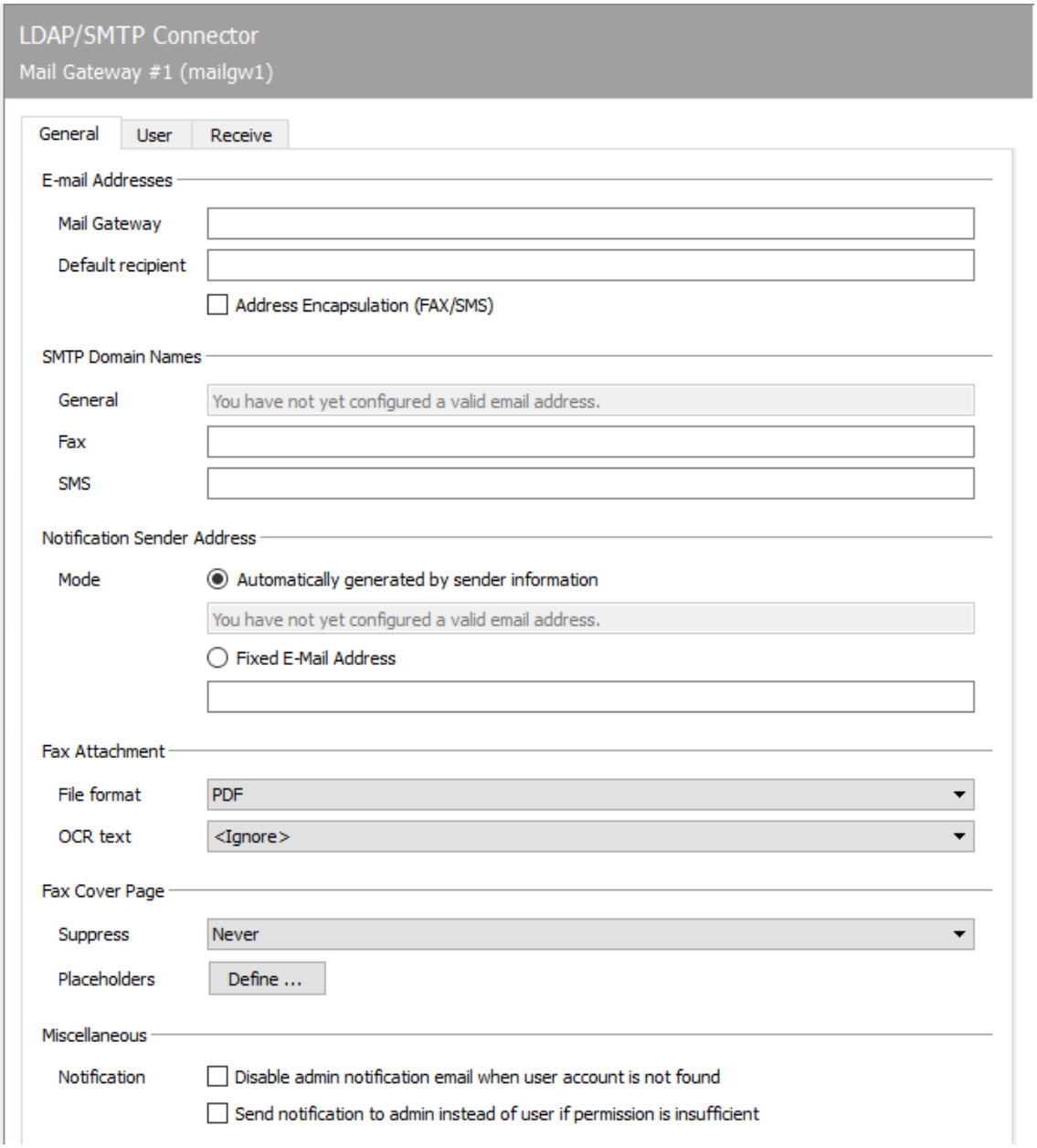
Note:
The messaging server component SMTPTX must be set up and started for sending e-mails. In addition, the FILEGW or the MAILGW must be selected as a gateway component on the LPD gateway.

10.10. LDAP/SMTP connector

10.10.1. Description

The mailgw component is used to connect the OfficeMaster suite to generic e-mail systems (not Microsoft Exchange or Exchange Online). The messages to the users/mailboxes are sent to the mail server via SMTP. Orders to be sent are received by the mail system via SMTP.

The user information (mapping fax number to e-mail address) is either read from an LDAP server or kept as a local database.



10.10.2. General

Email address

Mail gateway

The mail connector sends status reports to the users as e-mails. With these SMTP mails, the value configured for mail gateway is used as the sender address.

> Note!
> In addition, the domain specified after the @ sign under Mail gateway is used (in the example “fax.company.net”) to assign e-mails received from the SMTPRX component of the messaging server to the mail gateway. The domain specification must therefore be configured in the same way as the fax domain used.

Default recipient

All processes that were created by unauthorized users or that cannot be assigned to a user are forwarded to the e-mail address specified as administrator.

Address Encapsulation (FAX/SMS)

This function ensures that the syntax [Fax:0123456789] can also be used when sending from the e-mail client.

SMTP domains

General

Display of the default SMTP domain configured under Email Addresses Mail Gateway.

Fax

Messages to the OfficeMaster Suite with this target domain are interpreted as fax messages.

SMS

Messages to the OfficeMaster Suite with this target domain are interpreted as SMS messages.

Sender address of status messages

Mode

Generate automatically from sender information (with a corresponding example based on the configured data)

in this setting, an incoming fax is represented in the user mailbox as 0123456789@fax.company.

Static email address

You can store a fixed value here so that incoming fax messages always come from the same sender and are therefore easier for the user to identify.

Fax attachment

File format

Faxes that have been received or sent are delivered to the user as a file attachment to an e-mail. The fax file can be delivered in the following file formats:

- TIF (G4 or MH)
- PDF (not searchable)
- PDF-OCR if the messaging server has a licensed OfficeMaster OCR installation

OCR text

If OfficeMaster OCR is available, the OCR text recognized on the fax can also be specified in the e-mail message. The text is written into the mail either visibly or invisibly. Invisible text can be found and interpreted by the mail program in an automatic search. If the text is visible in the email, it can also be copied and processed by the user.

Fax cover sheet

In the case of faxes to be sent, the text of the e-mail message is inserted into a cover sheet template and used as the fax cover sheet for this transmission process, provided the mail sender has been assigned a cover sheet template on the messaging server. The cover sheet templates are saved as RTF files on the messaging server in the %ProgramFiles% \FFUMS\FMSRV\data\stationery\ directory and can be used e.g. can be adapted to the corporate design with Winword.

Suppress

The mail gateway can suppress the use of the mail text as a fax cover sheet on a case-by-case basis, e.g. the fully formatted mail attachment is to be sent as a fax. The decisive criterion is the text content of the subject line and the e-mail. If either one is blank, no cover sheet is used depending on the configuration. Various information from the sending process can be used in a fax cover sheet, such as the e-mail text, the subject line and other information related to the e-mail (sender, recipient). This information is taken from the send order or the user administration by the mail gateway and can be referenced by placeholders in the cover sheet template.

|Parameters |Description |Origin | |————————————-|————————————— ————————|———| | @@SENDERNAME@@ |Sender’s name (display name from CFG/LDAP)|User management| | @@FAXORIGINATOR@@ |Sender’s fax number |User Management| | @@SMTPORIGINATOR@@|Sender’s email address |User Management| |@@RECEIVER@@ | Recipient address (fax number) |Send order (e-mail or LPD)| |@@RECEIVERNAME@@ | Recipient name from SMTP-To-Header-Field for mail order send order (e-mail) |send order (e-mail) | |@@SUBJECT@@ |Subject line for mail order |Send order (e-mail or LPD via +PAR) | | @@BODY@@ |Body text for mail order |Send order (for e-mail) | |@@DATE@@ |Date on conversion |System time | |@@TIME@@ |Time of conversion |System time |

Placeholder

In addition, other user-specific information can be referenced as placeholders in the cover sheet template. The Define button opens a list in which the additional parameters are defined.

By default, the list already contains the placeholder DisplayName and additional parameters can be added. The content for the parameters is defined on the User tab.

Miscellaneous

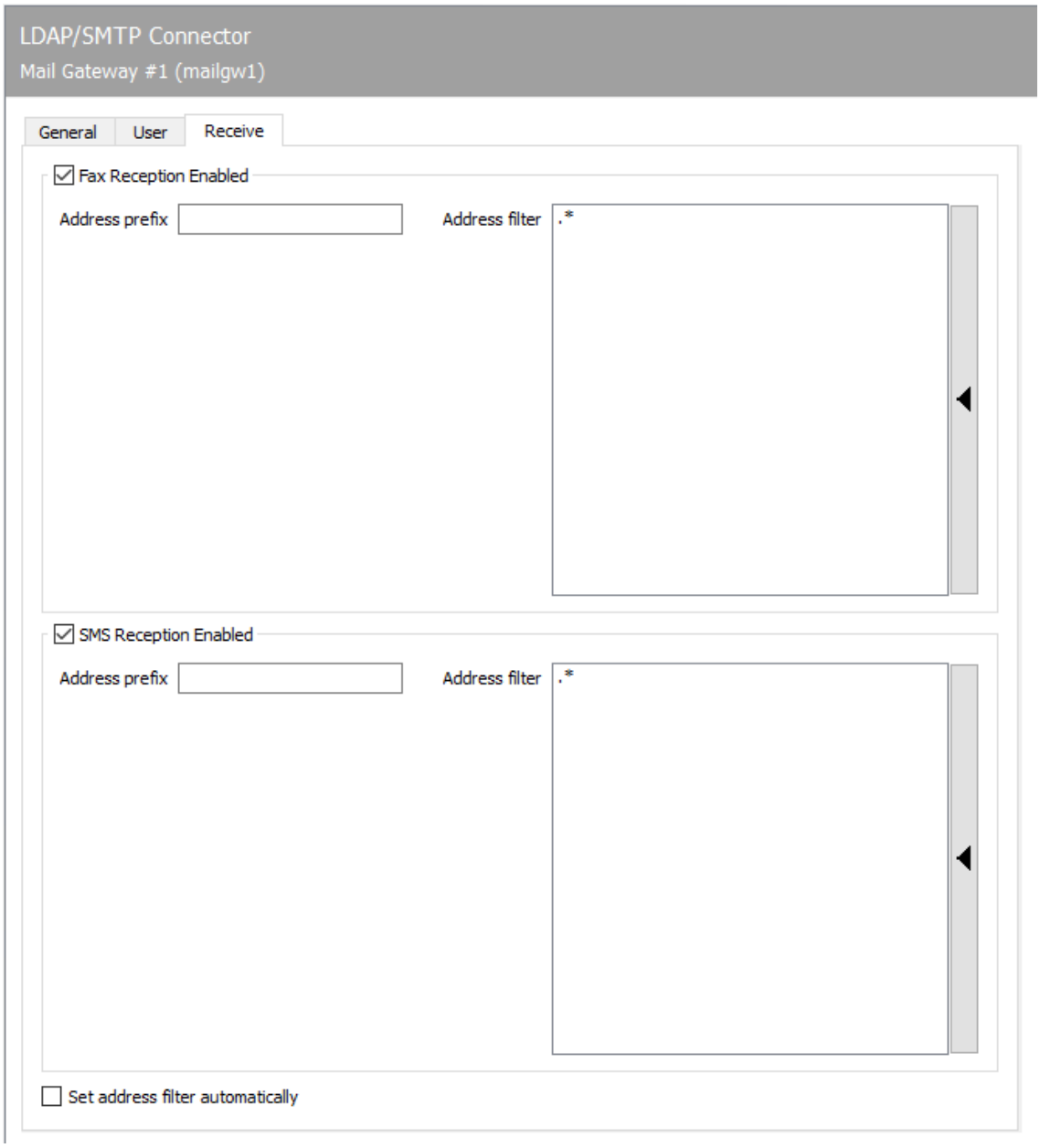
Notification

Disable email to admin if user account not found

All transactions that cannot be sent to users because the fax address could not be found are forwarded to the e-mail address specified as administrator. This function can be deactivated here.

Email admin instead of user if permissions are insufficient

All processes created by unauthorized users are forwarded to the e-mail address specified as the administrator.



10.10.3. Reception

The relevant parameters are configured on the Reception tab.

Enable fax reception, enable SMS reception

In general, fax and SMS reception can be activated/deactivated independently of one another. All phone numbers that are relevant for the mail gateway must be specified for message receipt. They can either be specified as an address filter or be determined by the mail gateway from the configured user data.

Address prefix

Irrespective of whether the phone numbers are determined using an address filter or from the user data, it is essential to configure the address prefix. If complete phone numbers such as e.g. +49 (3328) 455 960 are stored, the mail gateway cannot find the users in the LDAP, since only the extension 960 is transmitted to OfficeMaster. To avoid this, the recipient prefix +49 (3328) 455 is entered for both fax and SMS. When entering the prefix in the ISDN connection, it is not necessary to make an entry here, since this applies to all gateways in the messaging server.

Address filter

In the simplest case, an address filter consists of a list of all numbers intended for the mail gateway.

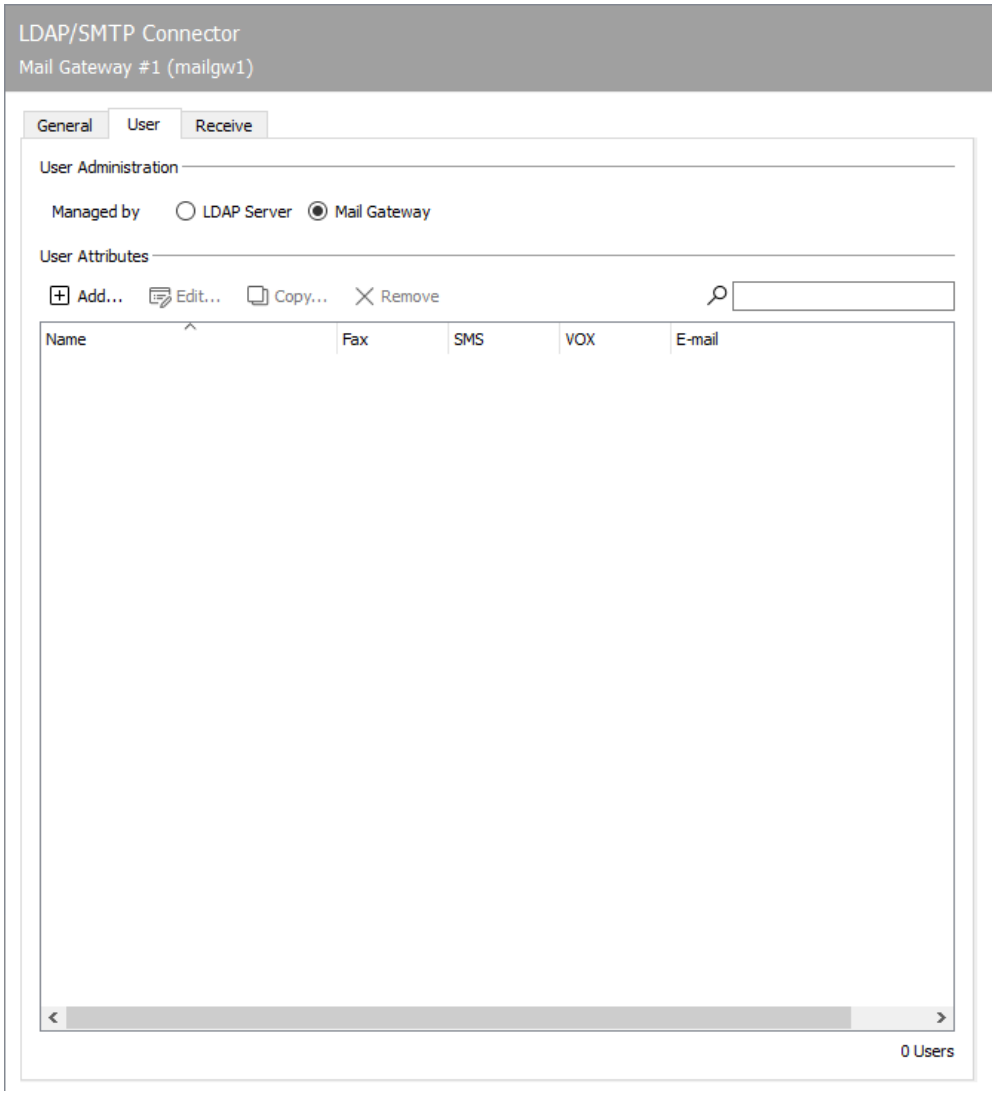
> Example:
> If fax messages to the numbers 305, 306, 307 and 308 are to be processed by the mail gateway, they must be entered one below the other as address filters. Since the mail gateway may have a large number of phone numbers, entering phone numbers can be summarized and simplified using regular expressions. The four numbers can be reduced to the entry 30[5-8].

In the default configuration, the address filter consists of a period followed by an asterisk (.*). The period is a regular expression and stands for any character. The asterisk gives the previous character the meaning any number of times. In this way, the receipt processes of all phone numbers are forwarded to the mail gateway by default.

Determine address filter automatically

As an alternative to the address filter, the mail gateway can also determine the relevant phone numbers from the user master, regardless of whether the users are maintained directly on the mail gateway or in the directory service. Reception processes to the phone numbers found are delivered to the mail gateway in the OfficeMaster Messaging Server. To do this, the Automatically determine address filter check box at the bottom edge of the tab must be activated. The stored address filters become invalid and are grayed out by the messaging server configuration.

> Note!
> If the address filter is restricted, receipt processes that were received on phone numbers that are not maintained are no longer sent to the mail gateway and its administrator, but are stored by the Undeliverable (UNDLVRBL) component of the messaging server. It is important to configure this component so that no received messages are lost unnoticed.



10.10.4. user

Mode: LDAP

Alternatively, the user administration can be maintained in an LDAP-enabled directory service or in the user administration directly on the mail gateway.

10.10.5. Configure LDAP access

Working in a directory service simplifies user maintenance because all user settings can be made centrally in the directory. Since, depending on the existing directory service, commissioning is associated with additional effort, the advantage of uniform user administration only pays off if the number of users is correspondingly high.

In general, most directories contain a lot of custom fields that are useful for fax communication. e.g. *facsimileTelephoneNumber* as a field for the user's fax number.

There are also user-specific parameters for which a standard directory does not offer any initial fields (e.g. when using *OfficeMaster Sign*, where each user also has to store the messaging server components that can provide their send jobs with an electronic signature).

User-specific fax/SMS parameters for which there are no explicit fields in the directory can be saved either in newly created fields or in fields that have not been used for their intended purpose and have not been used up to now. Since new fields often mean an irreversible schema extension of the directory, the misappropriation of previously unused fields is usually to be preferred. Many parameters can also be derived from the user's group membership. Specifically, the specific parameters listed in the table must be saved for each user in the directory service.

Custom parameters	**Required for...**	**Recommended field in Active Directory (without Exchange Server)**	**Radio button in Active Directory (with Exchange Server)**
Name	LPD user to mail gateway user mapping	sAMAccountName	proxyAddresses
email address	Delivery of received messages and assignment of mail orders	mail	mail
Fax address	Fax Reception	facsimileTelephoneNumber	proxyAddresses
SMS address	SMS reception	facsimileTelephoneNumber	proxyAddresses
Fax allowed	Authorization check shipping	memberOf	memberOf
SMS allowed	Authorization check shipping	memberOf	memberOf
Fax identifier	ID for sending faxes	facsimileTelephoneNumber	facsimileTelephoneNumber
Header Text	Fax dispatch header	department	department
Fax cover sheet		memberOf	memberOf

Custom parameters	Required for...	Recommended field in Active Directory (without Exchange Server)	Radio button in Active Directory (with Exchange Server)
	Determination of the fax cover sheet		
Fax Signature	Electronic signature of transmissions	memberOf	memberOf
Max Priority	Processing Priority	memberOf	memberOf
TK Prefix	Prefix for recipient phone number when sending faxes and SMS	pagers	pagers
OAD	Sender phone number for sending faxes and SMS	facsimileTelephoneNumber	facsimileTelephoneNumber

Note!
Regardless of the OfficeMaster Messaging Server, a third-party LDAP browser should be used on the server in order to look up individual fields and to be able to search for examples of the parameters to be configured. LDAP browsers are available as freeware on the Internet, e.g. the Softerra LDAP Browser (www.ldapbrowser.com).

The mail gateway accesses the *searching* and *reading* fields. Searching access takes place on the fields (LPD) *name*, *e-mail address*, *fax address* and *SMS address* in order to find the right user for the send and receive processes to be processed.

Example: Searching access to the directory service

Table: Application examples for search fields

field	use case
email address	If a send request is received by e-mail, the e-mail gateway uses the sender's e-mail address to search for the associated user in the directory service and then determines the user-specific parameters such as cover sheet, fax ID, etc.

field	use case
Fax address	The phone number at which a fax was received is looked up in the directory service's configured Fax Address field to determine the e-mail address to which the fax should be mailed.
name	A send job received via LPD/network printing is assigned to the user in the directory service based on the LPD name in order to determine his e-mail address or to check sending permission.

Almost all fields are also used for reading. If the user for the e-mail address of a send job was found, the mail gateway reads the associated cover sheet and the fax ID to be used for this user from the directory. Access to the fields in the directory service always follows the pattern:

Seek

In the directory service, the relevant entry or user is identified using the LPD user name (for LPD send requests), the e-mail address (for send requests received by e-mail) or based on the fax or SMS address (for receive processes). identified.

Find

The LDAP parameters required for further processing are taken from the entry or user found. These are mostly the e-mail address (for received messages), the list of signature components (for LPD send jobs) and the cover sheet (for e-mail send jobs).

Replace (optional)

If the parameters found in the directory service cannot be used for the mail gateway in the syntax stored there, it is possible to derive the relevant job parameters from the field content (LDAP parameters) in the directory. So e.g. only part of the identified field content is interpreted by the mail gateway. If the fax numbers are stored in the directory service in the form 03328 455 960, receipts cannot be delivered because usually only the extension (in this case 960) is signaled as the recipient (called party number) in the ISDN. The mail gateway can only compare the last three digits of the fax numbers stored in the directory service. Instead of only interpreting part of the field content, parameters can be derived from the field content in a completely abstract manner.

Example: If the memberOf field in the directory service contains the content accounting, the mail gateway can be configured in such a way that the signature component signds0 is inferred from it. Such a replacement is not included in the delivery status, as it relates to a specific

installation and only needs to be configured when required. If the user data is to be taken from a directory service, the Management in LDAP server option is selected on the Mail gateway on the Users tab (Figure 9.6). Before the individual fields can be set, the access data for the directory service must be configured. With the help of a third-party LDAP browser installed on this server, the access data should be checked for correctness. »» End of example

10.10.6. LDAP access

Servers; port; protocol version

The IP address or the resolved name of the directory server must be configured as the LDAP server. The default port is the well-known port 389, on which LDAP directory access is expected by default. If the configured directory server expects LDAP queries on a different port, this must be set here. Most LDAP servers support the default protocol version 2.

User; password

Furthermore, an administrative user is required, which has read access to the directory service via LDAP. This user (e.g.: *CN=administrator,CN=users,DC=company* or *administrator@domain*) is specified under *User* and *Password*.

10.10.7. LDAP queries

Base DN

Base DN specifies the container from which the mail gateway should look for user data in the directory service. In the case of larger directories in particular, a container should be specified for performance reasons that contains all users or is located directly above all containers with users. In the Active Directory, this is the container CN=users. If all company-internal users are in their own container, this can be addressed directly.

Example:

At Ferrari electronic AG, the following basic DN would result: *OU=Ferrari electronic AG user,DC=Teltow*.

User Filter

The user filter is applied to the entries or users of the base DN. This filter is *(objectclass=*)* by default and is used for license monitoring. If the number of entries or users contained in the configured *Base-DN* is less than the purchased OfficeMaster user license, the filter can be retained. If the filter results in more *Active Users* than there are user licenses, this is signaled by the mail gateway in the component status of the messaging server configuration with the text *license error, required X, allowed Y* (X, Y = variable user numbers). In this case either user extensions have to be licensed or the user filter has to be reduced. The table below shows some example configurations for reducing the size of the filter.

Table: Configuration for reducing the user filter

Authorized Users	**Base DN**	**User Filter**
All of a container	OU=Ferrari electronic AG user,DC=Teltow	(objectClass=*)
All in the group OfficeMaster Users	DC=Teltow	(memberOf=CN=OfficeMaster Users,OU=Special Mailboxes, DC=Teltow)
All with fax number	OU=Ferrari electronic AG user,DC=Teltow	(facsimileTelephoneNumber=.+) or (proxyAddresses=FAX:.+)
All with @ferrari-electronic.de as the email address	DC=Teltow	(mail=*@ferrari-electronic.de)

Note!
The asterisk (*) can be used as a wildcard for most fields. An exception, however, is the memberOf field, where the entire content or the fully qualified name must be specified. Here in particular it is advisable to try out the filter with an LDAP browser and without interacting with the messaging server.

10.10.8. User Attributes

The same user-specific parameters are available for user data maintenance in the directory service as for user data maintenance at the mail gateway. To configure the required user attributes, select the *Define* button. The available settings are described below.

10.10.9. General tab - General user attributes

UID & Name

The *Name* or the *UID* is used for the user assignment of send jobs that were transferred to OfficeMaster. For example, if an LPD user *Administrator* prints a send request to OfficeMaster, the process is assigned to the user in the directory service whose name in the field configured here is also Administrator. By default, the name is stored in the *sAMAccountName* field.

If the LPD user name and the user in the directory are not identical, this are the following options for user assignment: - The correct name of the user in the directory service is specified as the LPD user in the embedded control command (U parameter) of the print job. - The LPD user names are maintained in the directory service. Another field in the directory can also be used for this, but this must be taken into account in the configuration of the mail gateway.

The username is derived from values stored in the directory service.

> Note!
> Deriving parameters from values stored in the directory service is relatively complex, but increases the flexibility of the mail gateway. Therefore it can be used in almost any prevailing directory structure.

Email; Fax; SMS; voice (addresses)

The fields for e-mail, fax, SMS and voice are specified under Addresses. Based on the addresses entered here, the corresponding users are selected from the directory service.

If OfficeMaster is instructed to send faxes or short messages via SMTP mail to *FAX=call number@server*, the user is identified using the sender address stored in the *E-Mail* field.

For example, if a mail is received from *user@company.net*, it will be assigned to the user in the directory service whose stored e-mail address has this value.

If the senders use different e-mail addresses than those stored in the directory, the same methods are available as for determining the login name.

In order to be able to deliver received faxes to a user by e-mail, the user data is determined using the telephone number under which the fax was received. The field in which the phone numbers are assigned to the users in the directory service must be specified as a fax address. In most directory services, the *facsimileTelephoneNumber* field is intended for maintaining a user's fax number. Since *facsimileTelephoneNumber* is usually the complete telephone number, e.g. in the canonical number format like *+49 (3328) 455 960*, and when receiving from ISDN only the extension *960* is communicated to OfficeMaster, a simple assignment between phone

number and LDAP user is usually not possible. In this case, there are several ways to solve the problem:

The number in *facsimileTelephoneNumber* is reduced to the number known by OfficeMaster.

- In the messaging server, *+49 (3328) 455* is configured as the receive prefix for the affected ISDN connections.
- The receive prefix *+49 (3328) 455* is only configured for the mail gateway, since the previously mentioned fix affects all gateways present in the messaging server.
- The search expression for the fax number is modified to *facsimileTelephone-Number=+49 (3328) 455 @@value@@*.

If the directory service is *Active Directory Service* with a corresponding schema extension by an Exchange server, the *proxyAddresses* field can alternatively be used for the fax number. It should be noted here that this field usually has the content ***FAX:@@value@@***, which must then be taken into account in the search expression to be used.

Received short messages are assigned to the LDAP user via the field specified under *SMS address*. Short messages are usually received as landline SMS via the existing ISDN hardware, using the same phone number as for fax reception. Therefore, the phone number for SMS reception is also assumed to be in the *facsimileTelephoneNumber* field in the standard. However, if the SMS is received by the OfficeMaster GSM radio modem or via an Internet Service Provider, the phone numbers for fax and SMS reception are different. In that case, another field, e.g. *mobile*, can be used to store SMS phone numbers. Irrespective of the field in which the telephone number for SMS reception is maintained, it must always be ensured that often only the extension number is communicated as the recipient number. Since the phone number is usually given in full in the directory service, the same general conditions apply as for the fax address (see above). In most cases it is sufficient to correctly configure the address prefix on the *Receive* tab.

Fax; SMS (permission)

In the *Authorization* section, the LDAP conditions can be specified that must be met in order to activate or block an LDAP user for the corresponding communication type. Group membership (*memberOf*) is best suited for authorization checking. LDAP groups can be specified using the button behind the text field. Advanced settings can be made for each attribute.

10.10.10. Index card Fax/SMS (Fax)

User-specific parameters for send jobs are configured on the *Fax/SMS* tab. There are parameters specifically for fax and for fax and SMS.

Fax

identifier; header

In many cases it is desirable for each user to use their own identifier and header for faxes to be sent. These values are taken from the directory service.

The entry *facsimileTelephoneNumber* is suitable for the identification, which is also used in the standard to determine the fax address. If the fax number is saved in the format *+49 (3328) 455 960*, it can be used in its entirety as an identifier. If the field is also used for the fax address, *+49 (3328) 455* must be entered as the *receipt prefix* on the *receive* tab. If the text of the *header* is to be designed individually for each user, a separate field such as *department* is recommended for storing the values.

If no fields are referenced for *Identification* and/or *Header*, outgoing faxes carry the standard values configured on the ISDN or SIP connection as header text.

Cover sheet

The LDAP field specified under Cover sheet is used to specify the cover sheet in which the e-mail text, subject and other information of the send job are fitted and converted into graphics. Here again the group membership of the sender (*memberOf*) is suitable for determining the cover sheet. Clicking on the button behind the text field opens the dialog where the groups with fully qualified names (*CN=Sales,CN=users,DC=Company*) can be assigned to a specific cover sheet template. The cover sheet must be saved in Rich Text Format (RTF) on the computer running the messaging server converter in the directory _%ProgramFiles% \FFUMS\FMSRV\data\stationery_ (on Windows).

If business documents, such as invoices and credit notes, are automatically transferred to the mail gateway by network printing (LPD) from commercial third-party software, the printed documents can be provided with an electronic signature during further processing. The embedded *+PAR command* of the print job refers to the signature component to be used.

In order to prevent the (accidental) misuse of signature components, the mail gateway checks for each user which signature components are permissible for them. This is also done using groups to which the possible signature components are assigned.

Signature

The field in the directory service that is decisive for the group membership (default: ***memberOf***) is specified under *Signature*. Groups are assigned to signature components using the button next to the text field.

Fax and SMS

For *Fax* and *SMS*, the *maximum priority*, the *TK prefix* and the sender number (*OAD*) can also be configured. The OfficeMaster Messaging Server can process send jobs with different priorities. Orders with a higher priority (such as orders) are given preferential treatment at crucial points (e.g. during conversion and when sending with *OMCUMS* or *SIP*). They thus overtake send jobs with a lower priority (such as bulk faxes). The sender can specify different priorities when placing the order.

Priority when ordering by email	**Priority when ordering via network printing/LPD**
The priority is determined based on the importance of the mail (in Outlook: “arrow down” = low, exclamation mark” = high).	In the embedded +command, the priority can be specified using the P parameter (@@+FAX:123;PHigh@@)

Max Priority

In order to prevent (accidental) misuse of the priority, a *maximum priority* can be specified for each user. The four priorities *very low*, *low*, *normal* and *high* are available for this. Send requests with a higher priority are processed with the *maximum priority* allowed for the user. Priority control should also be based on group membership. Priorities are assigned to groups using the button to the right of the text field.

TK prefix

The TC prefix is required if the telephone system is to assign the transmissions to individual users for the purpose of evaluating charges using an area code. This area code (*TK-Prefix*) is maintained for each user in the directory service. The field *pager* is recommended for this, which is unused in most directories. Alternatively, another free field in the directory service can be referenced.

OAD

However, telephone systems usually carry out the charge evaluation using the sender information *Originator Address Digit (OAD)*. This OAD is communicated to the telephone system as a *Calling Party Number* when the call is set up, provided the messaging server is configured for the use of order-dependent OADs.

The OAD can normally be determined based on the *facsimileTelephoneNumber* field based on the *facsimileTelephoneNumber* field. However, since the OAD usually only consists of the extension of the *fax address*, the content of *facsimileTelephoneNumber* for the mail gateway must be adjusted using the button at the end of the text field.

Cost Center

The specification of the cost center refers to an entry in the log file generated by the messaging server. The specification at this point only makes sense if users do not have any cost center information and the value should be set to the set value here. A cost center is an identifier with a maximum of 12 characters that uniquely identifies the user in the log file.

10.10.11. Voice tab

access

PIN

The PIN protects the voice box against unauthorized access via voice remote inquiry. The PIN is a combination of numbers that can be one to ten characters long. Four to six-digit PIN codes have proven their worth.

Project

A special voice project can be set for the user under *Project*, which best suits his or her habits in the menu navigation. If the entry is empty, the voice server uses _evoice*projectstart* as the voice project by default.

Language

The language can be set per user. OfficeMaster is delivered with German (*DE*) and English (*EN*) announcements. The language configuration made here affects the menu navigation for querying and configuring the voice box and the standard greeting if the user has not stored a personal greeting.

On my phone

phone

This phone number is used to play voice messages on this phone.

Query authorized numbers

In addition, up to three authorized numbers can be stored per user. These phone numbers are compared with the *Calling Party Number* of the caller (also with the possibly prefixed zero). If the phone number is the same, the PIN query is dispensed with and the caller goes directly to the query mode.

10.10.12. Cover sheet placeholder tab

Additional fields in the directory service can be defined as placeholders on the *Cover sheet placeholder* tab, which can be referenced in the cover sheet template. For example, the department name (*department*) or the description (*description*) can be used as a placeholder in the cover sheet.

Adjust user attributes (LDAP)

The necessary settings to derive user-specific parameters from the values stored in the directory service are made on the two tabs *Search* and *Properties* (accessible via the button behind the relevant text field).

10.10.13. Handling of job parameters

Search tab

The *Search* tab describes how to deal with the parameters that were communicated to the mail gateway by the order, such as the LPD user name or the sender's e-mail address (*Job-Parameter*). The *Search* tab specifies the field in which the mail gateway should search for the fax number in order to identify the user. To do this, search expressions are used that consist of two parts: the actual LDAP query and the job parameters it contains, which are known to the mail gateway. In this case the job parameter is the fax number.

Custom search expression

A customized search expression (*LDAP-Query*) can be defined as part of the LDAP search. By default, the affected field is compared to the job parameter (***facsimile-TelephoneNumber=@@value@@***). The job parameter is represented by the placeholder ***@@value@@***. If the search expression is modified, the wildcard must be used. In the Format parameters for search frame, the value can be modified in three ways:

Format parameters for search

Take over completely

The entire value of *facsimileTelephoneNumber* is interpreted as a fax address, which means that the value stored in the directory service would be *+49 3328 455 960* in its entirety.

Accept part

Only part of the value is used for the search. If only the three characters at the end are to be interpreted, the fax number *+49 (3328) 455 960* stored in the directory service would assume the value *960*.

Apply regular expressions

With *Use regular expressions* the value determined by LDAP can be formatted with the help of regular expressions.

Properties tab

The handling of the parameters stored in the directory service (LDAP parameters) is configured on the *Properties* tab. After the correct user has been found in the directory service, the LDAP parameters must be taken from the directory.

Format attribute

Take over completely

The value found is completely used by the mail gateway as a parameter, e.g. B implemented for the fax identifier. For *facsimileTelephoneNumber* this means that the entire stored value is used as is.

Accept part

Only part of the field content is converted as a parameter.

Apply regular expressions

With Apply regular expressions, the LDAP parameter can be reshaped in almost any way. Groups can be specified with a fully qualified name and then provided with the desired authorization (*Yes* or *No*):

> Example:
> *CN=Administrators,CN=Builtin,DC=Teltow* or
> *CN=PMC,OU=Ferrari electronic AG user,DC=Teltow*

Many directory services do not allow the use of wildcards in the *memberOf* field. With *Edit* or *Add* a dialog for the replacement for inputs captured by regular expressions is reached.

10.10.14. user

Mode: Mail Gateway

For a limited number of users (1 to 20), it is advisable to carry out user maintenance directly on the mail gateway. This saves the increased effort associated with integration into an existing directory service, such as Active Directory or Novell Directory.

To do this, the intended users are entered in the mail gateway using the *Add* button. The user data can be changed at any time with the *Edit* button.

User Attributes

user list

10.10.15. *User Properties*

10.10.16. General

Registration

Surname

The name to be entered here is used to assign network print/LPD jobs to mail gateway users. The login name of the LPD user must match the name of the mail gateway user configured here.

Addresses

Email; Fax; SMS

The mail gateway uses the e-mail address to identify the sender of fax or SMS transmission requests in order to insert user-specific parameters (cover sheet, header, etc.). The phone numbers of received faxes and short messages are compared with the stored fax or SMS address. If there is a match, the receipt process is assigned to the user and sent by e-mail to the stored e-mail address.

For comparison, the phone number is provided with the address prefix configured on the *Reception* tab.

Example:

If the messages were received under the number 960 and the address prefix is *+49 3328 455*, the user must be assigned the fax address *+49 3328 455 960*.

Authorization

Fax; SMS; Voice

The services can be allowed individually for each user. To do this, the corresponding checkboxes at the foot of the index card are activated/deactivated. Sends from users without authorization will be answered with an error mail.

10.10.17. Fax/SMS

The identifier to be used, the header, a cover sheet and the permitted signature components can be optionally configured for fax and SMS transmission jobs.

Fax

Identifier; Header; Cover sheet

The values stored for *Identification* and *Header* appear in the header of the sent fax message every time this user sends a message. If the parameters have not been maintained, the default values set in OMCUMS or SIP are used for this. The *cover sheet* is saved as a cover sheet template in the directory %Program-Files%\FFUMS\FMSRV\data\stationery. Parameters with placeholders (e.g. **@@RECEIVERNAME@@**) that are known from the send request can be used in the template.

Signature

The components activated for *Signature* are used for the authorization check for send jobs sent via network printing (LPD). For example, if the component *signds0* with the embedded command **@@+PAR:sign=signds0@@** was specified in an LPD send request, this component must be activated for the user at the mail gateway. If the user was not authorized for this signature component, the document is sent unsigned. The signature components specified at the mail gateway are therefore used for the authorization check for send jobs that were transferred to OfficeMaster Messaging Server via LPD/network printing.

Auto Print

If incoming messages are to be printed out in parallel on a printer, the appropriately defined print gateway can be specified here.

Archive

If an archiving component is defined (e.g. file gateway in archive mode), this can be stored here.

Fax and SMS

Max Priority

With the *maximum priority* an upper limit can be defined with which the user's send requests are processed. If a user transmits his job with a higher priority (adjustable in Outlook via *arrow down* or *exclamation mark* or with LPD network printing via P parameter in the +FAX command), the job is processed further with the priority configured here.

TK prefix

Some telephone systems require an individual, multi-digit sequence of numbers from each user in order to be able to allocate the costs incurred by the call to the user. In order to use this cost allocation for faxes and SMS as well, the sequence of digits can be configured as a *TK prefix*. The *TK-Prefix* is preselected by the ISDN card for each transmission and is used as a prefix for the recipient number (*Called Party Number*).

OAD

Telephone systems mostly use the sender address *Originator Address Digit* (OAD) to evaluate charges. The OAD stored here is communicated to the telephone system as the sender number (*Calling Party Number*) when the call is set up, provided the ISDN card has been configured to use order-dependent OADs.

10.10.18. Voice

The *Voice* tab is only relevant for operating the mail gateway as OfficeMaster's *Userinfo server*.

10.10.19. Cover page placeholder

If activated, each sending process is provided with the cover sheet specified on the *Sending Options* tab. If user-specific parameters that go beyond the standard scope are to appear in the cover sheet, these must be incorporated into the cover sheet template with appropriate

placeholders and then defined for the mail gateway on the General tab. The values of the placeholders are set for each user on the *Cover sheet placeholder* tab.

10.11. Exchange 2013-2019 On-Premise Connector

OfficeMaster integrates into Microsoft® Exchange Server 2013, 2016 and 2019. A connector is available for all communication services (fax, SMS, voicemail). The connector can be operated on any member server in the Exchange organization, as long as they have the Exchange system administration tools. OfficeMaster can also be installed directly on an Exchange server (but not recommended for maintenance reasons).

The Exchange connector accesses the user data stored in the Active Directory via the Active Directory Service Interface (ADSI). All parameters relevant to the user, such as fax identification, SMS direct dialing and voice PIN, are maintained in the OfficeMaster Exchange administration. Existing fields are used for this so that the Active Directory schema for using OfficeMaster does not have to be extended.

To communicate with the Exchange server, the connector uses Simple Mail Transfer Protocol (SMTP) and Exchange Web Services (EWS).

Communication Protocol	**Email**	**Voice**
SMTP	deliver and send	deliver
EWS	encode and decode	Remote inquiry (access to the corresponding user mailbox)

Note!
As both the Active Directory and the Exchange server allow access via LDAP or EWS only if certain authorizations are available, special care must be taken when commissioning OfficeMaster with the service account to be used by the connector.

Connectors for Microsoft Exchange 2013-2019

Note!
The following section deals with the technical connection to Microsoft Exchange 2007-2016 and the integration into Active Directory. The content is intended for advanced users who want to know more about the internal workings of OfficeMaster connectors. Therefore, details about the basic connector technology

are included, which are not essential for the commissioning and operation of the solution.

Although the OfficeMaster Exchange Connector is a messaging server component, it is deeply integrated into the structure of the Exchange server and Microsoft Active Directory. A technique is used that does not require any extension of the Active Directory schema.

Mail flow based on an Exchange Server 2016 with installed Hub Server, Mailbox Store and Client Access role

1. Sending the message from Outlook

After the message has been sent, it is sent from the Exchange server to the messaging server via SMTP.

2. Receiving message from Microsoft Exchange server

The message is ready for processing in the messaging server. There it is passed to the connector component.

3. Processing the message files

Data provided by the Exchange Server is processed by the responsible connector component.

This processing includes:

- Resolving the sender through ADSI queries in Microsoft Active Directory
- Editing the data based on the user's rights specifications or global specifications
- Generation of a fax send order and transfer to the messaging server

4. Fax the document

The messaging server receives the send order from the connector component and sends the message as a fax.

5. Response to the success of the sent fax document

The messaging server informs the connector about the status of the document dispatch.

6. Generate feedback

A shipping status is reported to the connector component. This is configured in the user-specific form.

7. Delivering Feedback to User

The response is sent to the Exchange Server via SMTP. The connector processes messages both with the Microsoft Active Directory and directly with the global address book of the Exchange server. Accordingly, the service account must also be provided with a rights structure.

Flexible installation

Due to the further development of the connection and the SMTP technology, it is possible to install the complete connector system, including the Exchange Connector, on an external computer that is connected to the Exchange server via the network. Since no physical installation is required on the Exchange server, the installation is much more flexible (the OfficeMaster Exchange connector does not work on the basis of transport agents or foreign connectors). The technology used enables it to be used on a cluster system.

Configuration without schema extension

The configuration settings of the connectors are stored in the Microsoft Active Directory. No schema extension is necessary for these settings. Existing attributes are used. The configuration attributes of the connectors are saved in a compressed format. In order to design the configuration across domains, the global settings are installed in a central access point. This results in complete independence from domains.

> Note!
> Access to this area of the Active Directory requires reading rights from the Exchange organization.

The following Exchange servers in the network are supported:

- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019

Administration components

If the recipient update service for fax and SMS addresses is to be used in the Exchange organization (not recommended!), then the shared directory with the name *Address* of all Exchange servers in the organization must be accessible via the network during installation.

> Note!
> If this is not the case or if it is not possible for legal reasons, a proxy extension

installation should be carried out on the Exchange servers that cannot be reached, but this is not recommended.

The administration of the connectors takes place in the OfficeMaster Exchange administration. These components are installed on the connector server by default. The components must also be installed on every other computer that is to be used for administration. The OfficeMaster Exchange Administration can be installed later via the setup of the OfficeMaster Suite (custom installation). To support the organization-wide recipient updates (formerly RUS), OfficeMaster supplies corresponding proxy description objects for each address type during the installation of the connectors, which must be present on every Exchange Server of the organization, but this is not recommended.

Creating the service account

The OfficeMaster connector service account is the logon account of the msx2kgate component. This component must be started with a special service account.

The Exchange connectors must be installed using an account with the following rights:

- Domain administrator or authenticated user with corresponding domain rights
- Exchange organization administrator (complete)

Note!
The service account can also be created with this installation account. Since the service account should have limited permissions, **the installation account and the service account are two different user accounts (!)**

Attention!
The connector component accesses the service account mailbox and/or the transfer mailbox. This leads to processing of e-mails. To avoid losing important personal mailbox content, an existing personal user account should never be used as a service account.

Creation of the service account for operating the Exchange connector

- A user account is created via the user management or the Exchange 2013/2016/2019 system management console, which is a member of the domain user. This account needs its own mailbox.
- The mailbox must not be suppressed in the global address list.
- The account needs full read permissions of the Exchange organization (membership of the group PublicFolder Management)
- The account is added to the local administrators group of the installation computer.

Note!
When using Voicemail, the service account for the Exchange Connector must have write access to the user object so that the PIN can be changed remotely, for example.

Note!
A domain controller has no local administrators. If an OfficeMaster Exchange connector is to be installed on a domain controller, the service account must be included in the administrators group.

Note!
If the service account has the user authorization for changing user-specific values (write authorization of the corresponding Active Directory attributes), no domain administrators can still change voicemails via remote inquiry. This behavior is normal and is due to the service account being an authenticated user that does not have the right to change administrator attributes as these are protected via the AdminSDHolder services.

Allow the service account to access the users' mailbox store:

- No further authorizations are required for the use of fax and SMS.
- Access to the corresponding mailboxes is required for remote querying of the voice mailboxes via the Exchange Connector.

Set access permissions to mailboxes:

Using the Exchange Management Shell command New ManagementRoleAssignment "OfficeMasterVoiceAccess"-user "Domain\Account" -Role ApplicationImpersonation

Installation of the OfficeMaster Exchange connector

The OfficeMaster Connector for Microsoft Exchange Server is part of the complete installation of the OfficeMaster Suite. After OfficeMaster has been installed, the connector is ready for installation.

Note!
The connector requires the previously described service account, which should therefore already have been created.

After the complete installation of OfficeMaster, a folder called Exchange is available in the quick launch bar of the configuration program. After clicking on On-Premises (local) under the

Exchange folder, the display of the previously installed connectors appears in the main configuration window.

A connector instance for all communication services can be added by selecting New Exchange Connector. A separate installation wizard will appear. The components should only be created and deleted using this installation wizard. After the welcome dialog, the installation requires the specification of an Exchange server. The Exchange Server (local bridgehead) to be specified here is used for bidirectional communication with the Exchange connector. This server sends e-mails to the Exchange connector and all incoming documents and feedback are sent to this server. If this server is going to be an Exchange 2013/2016/2019 server, make sure it is an Exchange hub server. If the Exchange Server confirms, the installation wizard calls up the installation parameters. Only a few parameters can be specified here:

- **Messaging Servers:**

This field only serves to provide information on which messaging server the connector is installed on.

- **Exchange Servers:**

The Exchange Server displayed is the server that was previously selected. This field cannot be changed and is for information only.

- **Create receive connector:**

With a selected Exchange 2013-2019 hub server, it is possible to create a special receive connector that gets a different port than the default receive connector of the hub server, since the data of the receive connectors should not overlap on an Exchange server. The suggested port can be changed individually.

Receive connector (Exchange 2007-2016 hub servers) By default, Exchange 2013/2016/2019 hub servers already have the appropriate connectors. However, these are only intended for client and intersite transport purposes. Such a receive connector does not accept anonymous authentication. If the service account for the connector is to be enabled for connector communication, either the security settings of the standard connector would have to be changed (this happens automatically if you deselect the *Create receive connector* item) or the connector would have to be enabled for anonymous authentication. Both are safety-related interventions that need to be discussed. An alternative is therefore to create a receive connector that is only used for communication with the messaging server. The installation wizard automatically configures this **receive connector** as follows:

- Name: Connector for UMS (ExchangeServer-MessagingServer)
- Configuration of reception only via the specified port
- No anonymous authentication
- NTLM authentication is enabled
- Service account is activated specifically for this connector

- Communication to this connector is only allowed from the IP address of the messaging server

Send connector:

In addition to the alternative of setting up a receive connector, an SMTP send connector is automatically created with the following configuration: - Name: Connector for UMS (Exchange Server - Messaging Server) - SMTP port 25 - No outgoing authentication enabled - The sending server (local bridgehead) is the selected Exchange server - Receiving server (smart host) is the specified messaging server that hosts the component of the connector

The created connectors should be operational immediately after installation. Of course, every administrator is free to adapt these connectors individually to the organization.

> **Note!**
> The connectors should not be renamed because the installation wizard uses the name of the connector as a criterion for installation and uninstallation.

- **Global Directory:**

The global directory refers to a shared directory of the Messaging Server installation. Every messaging server from version 3.0 that has selected an OfficeMaster for Microsoft Exchange Server option as an installation variant has an FFACCESS directory release. This directory share contains the following content:

Directory	**content**
Cover	Cover sheets in rich text format (RTF) and HTL template files can be stored by the administrator or users
signs	Signature files in rich text format (RTF), can be deposited by the administrator or by users
letters	DCX image documents (multi-page PCX), which are merged into the outgoing fax documents, can be deposited by the administrator or by users
Pictures	Image files in Portable Network Graphics (PNG) format. The images can be assigned to different users and appear in the voice messages. The images should not exceed a size of approx. 160 pixels (width) x 180 pixels (height). Can be deposited by the administrator or by users

The global directory is the basis for all administration snap-ins and all connectors. Alternatively, a directory share can be specified on a file server, under which the same content tree as in the table above should be located. The global directory entry may be modified by another installation. This fact is pointed out.

- **License group:**

In the *License group* field, the license group is specified in the user-limited versions (OfficeMaster Suite for 10, 25 or 250 users), in which the licensed users must be entered. By default, the license group is automatically created in the *Users* container and is named *OfficeMaster Licensegroup*. Alternative groups can also be specified here. In the Messaging Server configuration, the license group is not disposable.

> **Note!**
> The license group should not be moved after installation! Only the corresponding reference is saved. This is not automatically corrected when shifted manually. When moving the license group, the connector must be "overinstalled" or alternatively the entry for the license group in the OfficeMaster Exchange administration in the connector settings must be adjusted.

- **Service Account:**

The previously prepared account of the *msx2kgate* component is entered in the input field for the service account. The account is specifically authorized to access the connector.

> **Note!**
> A change or subsequent specification of the account can only be made completely by reinstalling (over-installing) the connector.

- **Global setting:**

Install base configuration object globally (recommended)

The global user settings are used as a template for all users who are not administered directly. These settings are stored in an object that is replicated centrally and made available across the organization. This setting is the default for organizations with a single administrative group or only one routing group.

Install base configuration object domain-wide

In larger organizations, the corresponding service account or the site's maximum installation account may not have the right to save the global settings organization-wide. In this case, the settings can be written to the current domain object. All other locations should also perform the form of installation in this way. Different global settings then apply in each location (or each domain).

> **Note!**
> The way in which the global settings are saved should only be selected once and should always be retained accordingly for future installations. Changes to installations that followed each other in quick succession would result in a duplicate object installation. This problem can only be remedied by uninstalling. If a storage object has been installed organization-wide and in the local domain, the settings of the local domain object apply.

After confirming the installation parameters, the connector is installed and initialized. In this step, all configured options are created. The connectors are mainly created in the Active Directory. If the current login account does not have sufficient rights, corresponding problems will be displayed in the installation status window or in the finstallhelp.log.

> **Note!**
> A “finstallhelp.log” file is always created for support purposes. This log file is continuously written during each installation and deinstallation process and can be helpful for the Ferrari electronic hotline. The storage location is displayed as the first entry in the information window.

The installation creates an SMTP receiving component (smtprx) in addition to the component for the Exchange Connector. It makes sense for a messaging server to have only one SMTP receiving component and then to distribute the documents further, since other messaging server components (mailgw, sapcon) can be set up on this interface and operated in parallel. Shouldn’t have an SMTP receiving component exist that uses the current messaging server as the basis for receiving, such a component is created.

> **Note!**
> In the event that the installation takes place directly on an Exchange server (not recommended), port 25 cannot be selected as the send port, since the send connector would then supply its own receive connector. In order not to have to reconfigure IP addresses, the send connector is configured to a different port (10026) and the *smtprx* component is automatically prepared for this port. Such installations are carried out fully automatically by the installation wizard, but can be reconfigured with the administration snap-ins if required.

- **Distribution of proxy address generators (not recommended!):**

Later in the installation, a dialog box appears for distributing the proxy address generators to support the organization-wide Recipient Update Service. This service requires a specific generator component on each Exchange Server. This component should be installed manually on servers that do not have installation rights. If this point has already been carried out during an installation, this can be switched off with the button *Delete selection*. With *Next* you get to the next installation step. Otherwise the distribution is initiated with the *Installation* button. The server list provides information about the success of the distribution.

Here you can create fax and SMS addresses with which outgoing orders can be processed, since the connectors can use these addresses as sender authentication.

> **Note!**
> Recipient guidelines are not created. Recipient policies cannot be used to create meaningful fax, SMS, or voice addresses. Using Recipient Update Services to create fax, SMS, and voice addresses is not recommended. Fax, SMS and voice addresses should always be created manually or using a script.

In the following dialog, the installation assistant is closed with *Finish*. The component has now been created in the messaging server and then started.

> Note!
> In addition to the connector component *msx2kgate*, it should be checked whether the corresponding SMTP receiving component *smtprx* has been started. If this is not the case, the component must be restarted manually. If the *smtprx* component cannot be started, this is usually due to the running Windows service Simple Mail Transfer Protocol. This service would have to be deactivated or set to a different port or IP.

Multiple connectors within an organization

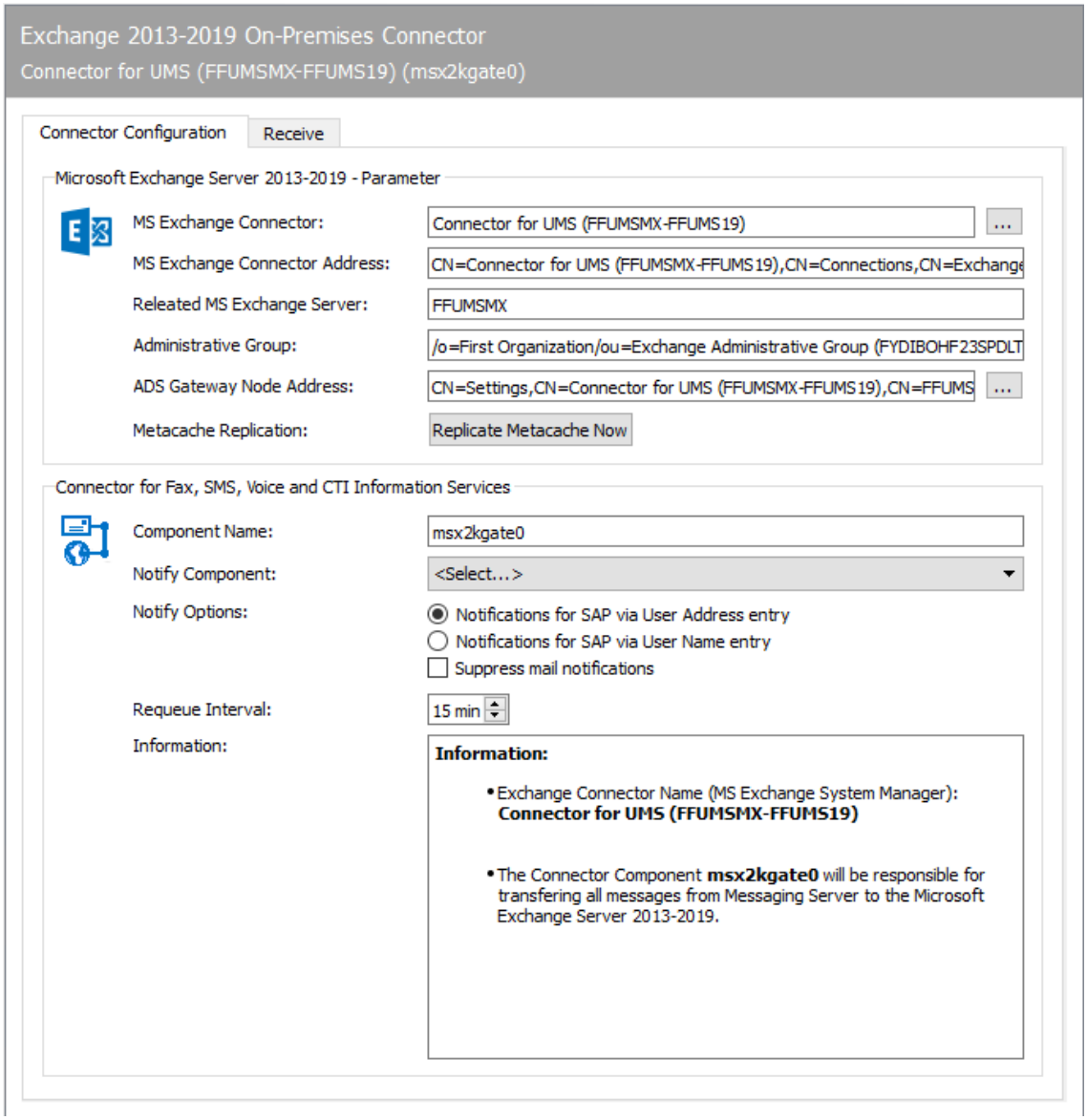
If several connectors are installed in an organization with several Microsoft Exchange Servers, the installation process described above must be repeated in each case.

Only one connector to the same Exchange Server can be installed on a component server. However, several connectors to different Exchange servers can be installed on a component server.

Update the connectors (overinstallation)

If an OfficeMaster Exchange Connector has already been installed and another installation is carried out that refers to the same Exchange Server, the old installation will be updated to the latest version and repaired if necessary. Settings that have already been made will not be overwritten. The installation updates any parameters that may be missing. In the course of such a repair installation, the OfficeMaster license group or the service account can be changed.

With existing connectors, the previous configuration settings are largely retained. Only server-specific data is corrected. One setting that may change is the global directory. If this directory is to be changed, the installation wizard will ask. If the *global directory* is not to be changed, the selection must be acknowledged with *No*.



10.11.1. Connector configuration

Although the Exchange connectors store all relevant settings in the OfficeMaster Exchange Administration in order to integrate the components into the Exchange Server environment, the individual components also have basic settings in the messaging server configuration that ensure the smooth operation of the components.

The basic settings are on the Connector Configuration tab.

Microsoft Exchange Server 2010-2019 parameters

These settings are set by the installation wizard. They include the name of the Exchange connector, the name of the Exchange server for logging on to Exchange onPremise, the path in Active Directory to configure the connector or the base node.

MS Exchange Connector

The field contains the name of the Exchange Connector that was installed via Active Directory. If necessary, this entry can be adjusted.

MS Exchange Connector address

This field contains the X.500 address of the Exchange Connector.

MS Exchange Server

Name of the Exchange Server on which the Send and Receive connector is installed.

Admin group

The entry contains the X.400 address of the administrative group.

ADS gateway node address

The address entered here indicates the X.500 path of the configuration object. The path can be adjusted if necessary.

Metacache replication

There is a button in the configuration that can be used to trigger metacache replication outside of the set intervals. This option is only implemented for test purposes.

> **Note!** While basic settings can be configured, manual administration is not recommended. The basic parameters should only be set by the installer. Manual changes can severely disrupt the correct operation of the components.

Connector for fax, SMS, voice and information services

The settings in this area determine the interaction of the Exchange Connector components with other messaging server components.

Component name

The name of the connector component is displayed in this field. This field cannot be changed.

Status component

A status component is an additional component that provides information about the status of the sent fax document or the sent SMS. Here, for example, archive gateways can be specified.

Status options

The *msx2kgate* component can also act as a state component for other gateways. Here you set additional options:

1. Status messages for SAP based on the user address field

In cooperation with a SAP connector sapconn, it can be set that the sender determination is based on the order field of the user address. This field is then used by the connector to resolve the address in Active Directory.

1. Status messages for SAP based on the user name

In cooperation with a SAP connector sapconn, it can be set that the sender determination in this case is based on the order field of the user name. This field is then used by the connector to resolve the address in Active Directory.

Suppress email status feedback

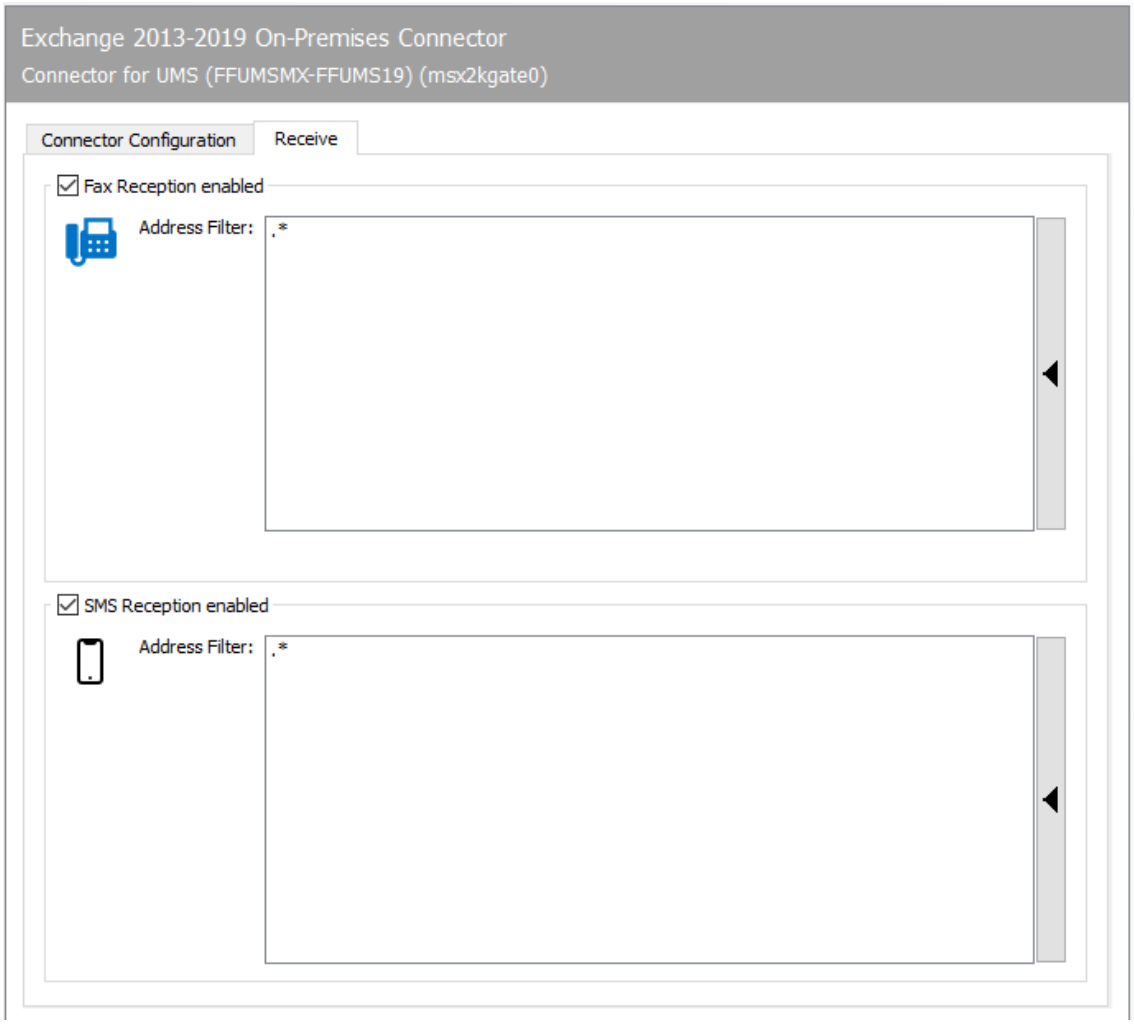
If the connector is connected to an LPD, it can also process e-mail addresses in addition to fax numbers. The feedback as to whether the LPD has processed the e-mails correctly via the Exchange Server via relay forwarding can be suppressed here.

Requeue Interval

If messages cannot be delivered to the mail server due to faulty connections, they are queued again. The waiting time until the new order can be set here. The default setting is 15 minutes.

Info

Here is general information about the created object. The text cannot be changed afterwards.



10.11.2. Reception

The Reception tab has a direct impact on the incoming documents. The telephone numbers (Called Party Number) intended for the Exchange Connector can be entered as an address filter for faxes or SMS. With the default setting (.*), all received faxes or short messages are forwarded to the Exchange connector.

A change is only required if received messages are to be distributed to different gateways, such as msx2kgate, sapconn, filegw, etc., or if messages from OfficeMaster are only to be received on certain phone numbers.

The latter, the so-called whitelist procedure, can be activated under Extras > Black & Whitelist > Reject undeliverable messages.

> **Note!**
> If the address filter is restricted to certain phone numbers without an activated whitelist procedure, the UNDELIVERABLE component of the messaging server should be configured so that received messages are not stored unnoticed on the server and “stay behind” despite the best address filter configuration.

In the simplest case, an address filter consists of a list of numbers that are assigned to the connector. For example, if all faxes to the numbers 150 to 154 are destined for the Exchange Connector, the address filter list contains the following entries: 150 151 152 153 154

The entries in this list can be combined with regular expressions into entry 15[0-4].

The default value (.*) for the address filter is also a regular expression. The dot (.) stands for any character. The asterisk gives the character in front of it the meaning as often as you like. At this point, only one address can be specified per line. It is not possible to combine several expressions in one line using OR (|) or AND (&).

10.12. Exchange 2017-2019 email archiving

The MSXARCHIVE component is presented here as an alternative to the normal FileGW of the messaging server, which can be operated in archive mode. This component is a pure SMTP processing unit. E-mails received via the SMTPRX component can be archived in the TIF and PDF formats using the MSXARCHIVE component.

10.12.1. Similarities to FILEGW (archive mode)

- Archiving of e-mails as TIFF format with description file

10.12.2. Differences to FILEGW (archive mode)

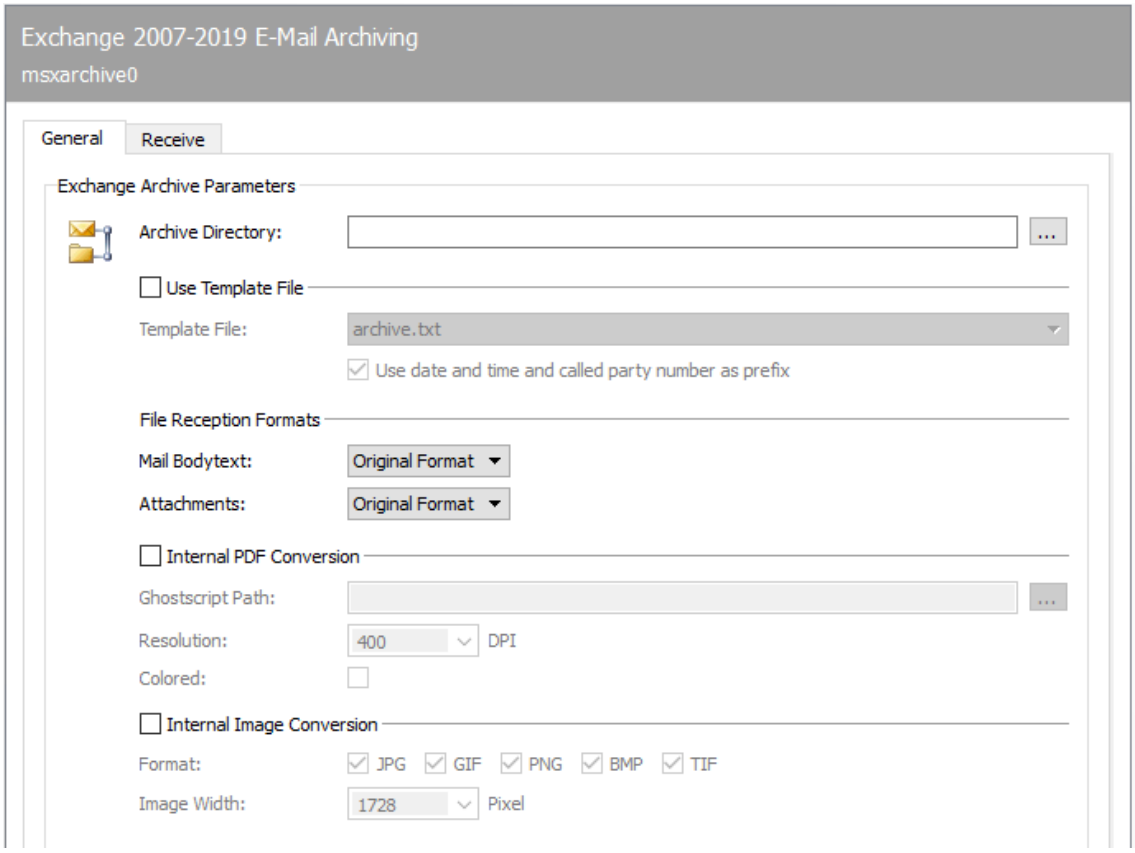
- Process optimization for Exchange Server mails
- Support of standard emails (MIME)
- Support for extended Exchange emails (TNEF)
- Mail body text is converted to TIFF graphics in MS Outlook theme with embedded graphics
- Original e-mails are provided as an Outlook data file (*.msg).
- Support for emails with mail-in-mail attachments up to second level
- Support for PDF conversions with colored content and configurable resolutions
- Support for colored image content and configurable resolutions
- Support of XML description files (also UTF-8)
- XML-optimized document description data is supported as a tree structure
- Archive component cannot be used by other components as a feedback component

10.12.3. System requirements

- Installed messaging server
- Specially created service account with MAPI access to Exchange Server
- Installed smtprx component for receiving SMTP messages

10.12.4. Creation of the component msxarchive

The msxarchive component can be added via the quick launch bar > Exchange > Mail archive via the *New Exchange archive component* button.



10.12.5. General

Some information must be provided for the correct operation of the components. Although the design of the MSXARCHIVE component is based on the Exchange Connectors, no properties are stored in the MS Active Directory.

The basic parameters are set via the General tab. These parameters should be fully administered correctly to allow the component to work correctly.

Archive directory

The archive directory is the directory into which the files are ultimately written. This can be selected via the browser button. The directory must already exist. It is not created by the component.

Use template file

It can be specified whether a template should be used for the description file. If this point is not activated, no description file will be created.

Placeholder

The placeholders in the table are currently supported.

Placeholder	meaning
@@DATE_TIME@@	Timestamp of processing in the format yyyy-mm-dd hh:mm
@@Time@@	Timestamp of processing in the format yyyy-mm-dd hh:mm
@@SUBJECT@@	Email subject line
@@Subject@@	Email subject line
@@PRIORITY@@	Email priority (low, normal or high)
@@Priority@@	Email priority (low, normal or high)
@@MESSAGECLASS@@	Email message class
@@MessageClass@@	Email message class
@@ORIGINATOR@@	Sender email address (SMTP)
@@Originator@@	Sender email address (SMTP)
@@RECEIVER@@	List of recipients (comma separated)
@@Receiver@@	List of recipients (comma separated)
@@JOBID@@	Internal job number of the messaging server job
@@Jobid@@	Internal job number of the messaging server job
@@MESSAGE_ID@@	SMTP Mail ID
@@MessageId@@	SMTP Mail ID

List placeholder

The placeholder @@PAGESFORMATBEGIN ... PAGESFORMATEND@@ is supported for file attachments. Within these placeholders, the format text contained is repeated for each file attachment. The format text contained can also contain placeholders for each file attachment:

Placeholder	meaning
@@CONVERTEDFILENAME@@	Filename of the converted image file of the corresponding attachment
@@FILENAME@@	Unique file name of the attachment file

Placeholder	meaning
@@ORIGINALFILENAME@@	Original attachment file as used in the original email
@@CONVERTED_FILESIZE@@	Size of the converted file in bytes
@@FILESIZE@@	Size of the original file in bytes
@@CONVERTER_STATUS@@	“OK” if the file was successfully converted

Template

If a template file is used, it can be selected here. This template must be located in the central template directory of the messaging server. This is usually located under the following path: %PROGRAMDATA%\FFUMS\fmsrv\data\templates

Use date, time and called party number as prefix

Similar to FILEGW (Applicom OfficeMaster), it can be specified that the time stamp is placed in front of the files in order to be able to distinguish and organize them better. There is no called party number for incoming mails. For this reason, only the time stamp of the processing is put in front.

File receiving formats

Email body text

The format TIFF G3 or PDF can be selected for the e-mail body text. The gateway makes the original mail available as an Outlook data file (*.msg). The converted image of this mail was modeled on the printout of Microsoft Outlook on a printer.

> Note!
> The converted image supports logos and embedded graphics only if MS Winword is used as the central converter on the system.

> Note!
> In the case of e-mails generated via Outlook Webaccess or pure SMTP clients, the Outlook data file must be created from scratch. The gateway then tries to convert the fonts as best as possible. This conversion may differ slightly from the original when displayed.

Attachments

TIFF G3 or PDF can also be specified for the file attachments. The gateway transfers the original files to the messaging server for conversion to TIFF or PDF. This conversion does not always have to be successful. There are formats that cannot be converted by the messaging server. In this case only the original file is archived and the placeholder for the converted file remains empty. In order to archive the mails, the gateway must register with the messaging server. The settings for this are made in the Reception tab.

Internal PDF conversion

Ghostscript path

The component internally uses the third-party program “Ghostscript” for the PDF conversion. This would have to be installed on the system. It is recommended to install a current component. Whether it is a 64-bit or 32-bit variant is irrelevant for the component. When specifying the file, the command file gswin32c.exe or gswin64c.exe must be specified.

Resolution

The target resolution of the PDF documents to be converted can be selected at this point.

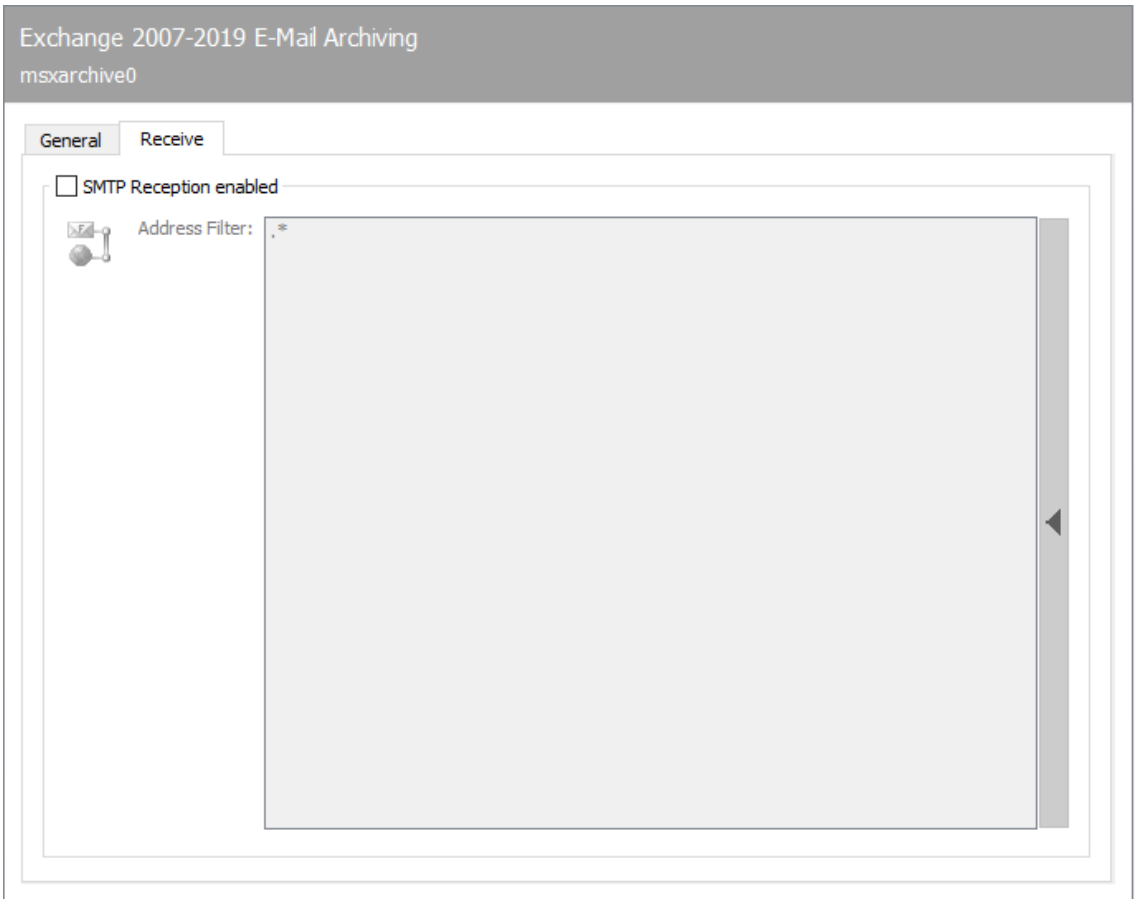
Coloured

A colored TIFF conversion is also supported. This can be turned on at this point.

Internal picture format conversion

Format

Target width



10.12.6. Reception

The *Receive* tab controls the supply of e-mails to the component. E-mails that fit into the scheme of the entered address filter are assigned according to the component. This does not happen exclusively. If other components (exchange connectors, SMTP gateways) have also registered for the address spaces, these components will also receive the messages.

SMTP reception enabled

This option can be used to disable SMTP reception of the component. If reception is activated, the specified address filter applies.

Address filter

The address filter determines the addresses for which the gateway makes itself available. This entry is made with a regular expression. It should be mentioned here that no regular expressions are linked via a concatenation operator in the input field, but are processed individually in the list. Contrary to the normal dialects of regular expressions, the expressions can be negated with a preceding minus sign.

10.13. Office 365® / Exchange Online Connector

This section describes the installation and configuration of the Connector for Microsoft Office 365® of the OfficeMaster® server.

10.13.1. General

What is the OfficeMaster Connector for Microsoft Office 365?

Since OfficeMaster 4.0, an additional connector for online services has been offered with the Exchange connectors. This connector is a further development of the proven Exchange connector *msx2kgate*.

msxbcsgate (Microsoft Exchange Business Communication Services Gateway)

The development of the new connector pursued the following goals:

- Compatibility with previous versions
- Possibility to use an existing Active Directory
- Can also be used in on-premise and hybrid scenarios
- No storage of connector configurations in Active Directory
- Use of the well-known and proven administration tools

Bidirectional support of the Exchange Server transmission format (TNEF)

Advantages:

- Easy installation
- No lower permissions required in the Exchange organization
- Can be used for Office 365 (Full Featured)
- No use of a MAPI for mailbox access
- Use of existing user configuration in Active Directory for on-premise and hybrid installations

Disadvantages:

- SMTP transfer connectors must be created manually for on-premise installations

Areas of application

The product is an Exchange Connector for fax, SMS and voice mail services. It can connect all installation forms of Exchange Server-based messaging environments.

- Connection to Microsoft Office 365
- Connection to Microsoft Office 365 Hybrid (local Active Directory)
- Connection to Microsoft Exchange Server 2013 On-Premise
- Connection to Microsoft Exchange Server 2016 On-Premise
- Connection to Microsoft Exchange Server 2019 On-Premise

Differences to the pure Exchange Connector

The Online Connector *msxbcsgate* differs from the Exchange Connector *msx2kgate* in the following ways:

- The *msx2kgate* traditionally requires a Microsoft Active Directory with an intact Exchange Server organization.
- In a *native installation*, the online connector *msxbcsgate* always stores its configuration data in a data file. If the hybrid installation (local Active Directory available) is selected, then the decision can be made as to where the configuration data for the base node should be stored.
- The Online Connector *msxbcsgate* can support the individual user configuration by saving the values in the Active Directory in a way that is compatible with *msx2kgate*. However, this is only a compatibility for migration environments. The *msxbcsgate* supports storing the individual data directly in the user's mailbox. Therefore, the connector does not necessarily require an Active Directory here either.
- The online connector msxbcsgate supports mail transfer via a transfer mailbox (service transfer mode). This avoids outbound SMTP transfer over the Internet.
- The Online Connector is optimized to communicate directly with Microsoft's Mailprotection endpoint.
- The msxbcsgate installation wizard supports direct communication with Microsoft Office 365.

Modern authentication and communication with Exchange Online/ Azure AD

The secure authentication forms the basis for the installation and administration of the components in Microsoft Office365. In this case, the concept of "modern authentication" refers to manual login via the web, usually with OAuth 2.0 mechanisms, possibly with multi-factor authentication, to ensure secure interactive login.

Applications/programs that access the interfaces of the Microsoft Graph Interface (AzureAD, etc.) via the Internet must also support this “modern authentication”. Older programs that were designed for on-premises exchange servers can be used to communicate with the interfaces that use basic authentication. However, since this is correspondingly less secure, support for this authentication in the cloud is switched off.

The configuration of modern authentication was available for the first time in July 2020 in the AzureAD portal under “Modern authentication”.

Up to version 7, the OfficeMaster BCS connector only communicated with the Office365 Exchange Online via the Exchange Web Services. This was changed from version 8.0, since Microsoft will no longer support the creation of applications for the Exchange Web Services in the future.

As of version 8.0, OfficeMaster will no longer create any applications based on Exchange Web Services (EWS). As an alternative, an application based on the Microsoft Graph interface is then created. This way is the official interface supported by Microsoft for mail-based applications.

General installation requirements

An OfficeMaster installation is required to use the Connector for Office 365. Ideally, ISDN hardware or VoIP access points should be correctly installed. I.e. ideally a DirectSip or hardware connection should be correctly available.

Different service accounts are required to use the different work modes. These are described separately in the various sections on the installations.

Existing installations

With a pure update to OfficeMaster Version 8, the form of communication between the connectors does not change. The pure update only updates the program components. The cloud installation remains as it was before the installation.

Hybrid Installations

- As long as communication based on Exchange Web Services is technically possible in the cloud, a connector with Exchange Online communicate.
- If EWS communication is no longer possible, the connector should be overinstalled and the communication (as described in the section “Migrating from an existing OfficeMaster 7.1/7.2 to modern authentication or Microsoft Graph”) changed.

Native installations without local AD

- As long as communication based on Exchange Web Services is technically possible in the cloud, a connector can communicate with Exchange Online. Then nothing changes.

- If EWS communication is no longer possible, the connector should be overinstalled and the communication changed. However, the addressing of the fax addresses will then change.

  Notice about native installations!
  When changing the communication to the Microsoft Graph interface, the addresses must be changed. Pure FAX, SMS or VOX address types are then no longer recognized or supported!

New installations

In the course of future-proof communication to the services of the cloud, access to Exchange Online should take place with the Microsoft Graph interface. A downgrade to the EWS interface is not possible. The installation is largely automated. The degree of manual intervention can be chosen to be minimal during installation.

10.13.2. Installation of the Connector for BCS

The Connector for BCS installation wizard supports two types of cloud installation:

- Cloud-only - In this case, there is no local Active Directory.
- Hybrid - This installation requires a local Active Directory to be used as the user address book.

The installation should take place here using the example of a cloud-only installation:

The installation can be done via the quick start bar in the Exchange folder under the entry Hybrid/Cloud and *New Exchange Connector* or via the component table.

If you want to add a new connector or change the current connector, the installation wizard for BCS connectors opens. If the Office365 installations are selected, a login to the Office365 cloud is then carried out. Cloud login supports multi-factor authentication.

Note!
This registration is carried out internally via a remote powershell. Certain requirements must be met for this:

- Presence of Microsoft Powershell at least version 5.0
- Internet Explorer Enhanced Security Mode **must** be turned off. The Powershell modules work with an internal browser module for the login dialogs, which cannot work correctly without JavaScript execution and access to the cloud login endpoints.

Note!
If this login to the cloud is done for the first time by the installing account,

modules may have to be installed later. This can take a moment. A dialog indicates the post-installation. After closing this dialog, the display of the login window can also be delayed by around 30 seconds.

After successfully logging into the cloud, you get to the next wizard page. At this point, the transport is preconfigured. This step does not differ from the previous version.

Note!
- The successful and correct login to the cloud is shown with the correct display of the name of the organization.
- BCS connectors work in the cloud exclusively in service transfer mode, i.e. the outgoing messages are collected in a previously created mailbox. This transfer mailbox can also be a shared folder. The mailbox must first be created manually. This mailbox must not be the default recipient! A transfer mailbox must always be provided!
- The transfer domains are created by default with the name of the organization. This should be changed to shorter domains from experience. These domains do not need to have a DNS mail exchanger record. since the mails are intercepted by rule.
- The transfer domains should have a vox type to support read receipts for voice. (Turn off MWI lights when voicemails are read.)

When selecting the transfer mailbox, care must be taken to ensure that this is not an existing mailbox that a user is using. Incoming e-mails are processed, evaluated and moved. If an existing user mailbox is used, there could be a corresponding loss of data. The mailbox to be used is to be used exclusively for transfer purposes.

The next step takes you to the account and security settings.

The installation is designed for “modern authentication” by default. This cannot be changed in the normal configuration.

The following steps are carried out internally for an application registration:

- The tenant Id (client Id) is determined.
- An application called “OfficeMaster Graph Access” is created in AzureAD.
- A client Id (application Id) and a client secret (secret) with a validity of 24 months are generated for the “OfficeMaster Graph Access” application.
- API permissions are granted for the “Office Master Graph Access” application:

1. **Microsoft Graph: Calendars.Read (as an application permission):** The permission is used for queries to the users’ calendars. This is used for voice calendar queries to determine automatic free/busy statuses.
2. **Microsoft Graph: GroupMember.Read.All (as application permission):** The permission is used for requests to user groups. Distribution lists may have to be resolved for incoming fax or SMS messages. This permission is also used to use the Office Master license group.

3. **Microsoft Graph: Mail.ReadWrite (as application permission):** This permission is used for reading the e-mails in the user mailbox. At least this authorization is required for the transfer mailbox.
4. **Microsoft Graph: Mail.Send (as application permission):** This permission is set to be able to send emails via the users and the transfer mailbox. The connector uses this technology to carry out LPD mail dispatches and to be able to send e-mails from the transfer account to users.
5. **Microsoft Graph: People.Read.AII (as application permission):** This permission is used for requests to the cloud address lists.
6. **Microsoft Graph: User.Read (as delegated permission):** This permission is set automatically and has no meaning for the connector.
7. **Microsoft Graph: User.Read.AII (as application permission):** This permission is used for requests to the address lists of the cloud.
8. **Microsoft Graph: User.ReadWrite.AII (as application authorization):** This authorization is required if individual user data is to be saved.

If the client ld and the client secret have previously been created manually, they can simply be entered will. In this case, the option “Obtain Client ld and Client Secret automatically via AzureAD” must be deactivated. The values can then simply be specified.

If in such a case the tenant ld (client ld) should not be known, this can be done via the browser button be determined automatically.

The installation offers another option for preconfiguration. In some cases, the application has already been registered in AzureAD. In this case, perhaps no new application should be created. If so, an application browser can be called up via the browser button on the client ld.

The special feature of a selected application is. that no secret (client secret) can be read out. If this secret is not known, a new secret can be created during selection. Such secrets have a specific time limit. This can be set in the dialog.

> **Note!**
> Apparently, a special service account is not required for access to Exchange Online with modern authentication with tenant ld, client ld and client secret. In this case, a transfer mailbox is still required for the outgoing messages. Whether this mailbox has multi-factor authentication protection is irrelevant and plays no role for the connector. In the case of modern authentication, the transfer mailbox is used as an access point for address book resolutions and is therefore a prerequisite for smooth operation.

> **Note!**
> If the checkmark for using modern authentication is deactivated in the installation step for the account and security settings, the user name and password of a service account can be specified as in the previous version. **This is no longer generally recommended.**

When installing the Azure AD application, a note appears during the installation that refers to an additional configuration in Azure AD.

This notice relates to API permissions. For security reasons, automatic confirmation of the release of API permissions was deliberately avoided. This must be done by an administrator in AzureAD after installation. If there are any concerns, the corresponding authorizations should be subsequently adapted to the (security) needs of the solution.

To do this, log on to the AzureAD of the Office365 client and navigate to the “OfficeMaster Graph Access” application. After selecting the application, the API permissions are listed. The API permissions must now be confirmed. This step is only required for one application be made once.

> **Note!**
> In this step, the authorizations can be redesigned according to customer requirements. Changing the permissions may have a negative impact on the productive operation of the connector.

After the API permissions have been released, the connector can be put into operation like the previous version.

Conversion of an existing OfficeMaster 7.1/7.2 to modern authentication or Microsoft Graph

Automated migration

A somewhat simpler transition is the automated transition. In this case, the connector is simply overinstalled with the installation wizard of the OfficeMaster Messaging Server configuration program. With this overinstallation, the transfer domains and the transfer mailbox must be specified again explicitly.

10.13.3. OfficeMaster 8 and the native Office365 operation

When switching from native operation (without local AD) to OfficeMaster 8, there are a few things to consider.

- The fax, SMS and voice addresses can no longer be used in the form of user-defined address types.
- The way custom values are saved has changed.

> **Note!**
> Due to the change in the interface to Microsoft Graph, the existing users may have

to be modified in terms of their custom properties and in terms of their e-mail addresses.

Change of addresses

Assigning fax, SMS or voice addresses works when using local Active Directories by describing the proxy addresses. As a rule, user-defined address types (for one-off addressing) are used. Up to OfficeMaster 7, this was also permitted in native Office365 environments without local AD.

With the changeover to the Microsoft Graph interface, the address types in the e-mail addresses can no longer be used because Microsoft Graph suppresses the search for and publication of user-defined address types. By default, only SMTP address types are used.

To solve this problem, users' email addresses need to be changed:

OfficeMaster 6.x - 7.x Native Cloud Connector:

address type	**address**
FAX	phone number
SMS	phone number
VOX	phone number

OfficeMaster 8 Native Cloud Connector:

address type	**address**
SMTP	FAX number
SMTP	SMS number
SMTP	VOX phone number

If the planned migration involves a higher number of users. Ferrari electronic AG can provide a corresponding script for the conversion. The script ***MakeAddressMigration.ps1*** can be used for this purpose. This script is located on an OfficeMaster server in the \\FFACCESS\redist or %PROGRAMDATA%\ffums\fmsrv\data\exchange\redist folder.

Change in user-specific data storage

OfficeMaster 6.x and OfficeMaster 7.x save the user-specific settings in the user's mailbox. This is done in a hidden mail item (Folder Associated item). When OfficeMaster 8 was released, the

Microsoft Graph interface was not yet able to read such settings. For this reason, the saving of the user-defined values had to be changed.

As of OfficeMaster 8, the user-specific settings are stored in the “open schema extension”. This is a user data extension that can be created dynamically and also deleted again. It is not a schema extension as used by LDAP-based directory systems is known.

There is currently no automated way of transferring the user-specific data from OfficeMaster 6 and OfficeMaster 7 to the OfficeMaster 8 scheme.

If there is a need to do this for a large number of users so that this can no longer be managed using the standard configuration tools, then please contact the Ferrari electronic AG hotline (hotline@ferrari-electronic.de) To get in touch.

10.13.4. Local Exchange Server installation

A special type of installation is the local Exchange Server installation (on-premise). This form is similar to installing the Exchange Gateway *msx2kgate*. A local Active Directory is used to store user information and determine SMTP addresses. The connector only requires a LAN connection to access the local Exchange server.

Local installation is usually supported by the default exchange gateway msx2kgate. However, when the previous product was installed, there were local environments in which the *msxbcsgate* gateway had to be used. The reasons for this were usually access problems via *Message Application Programmers Interface (MAPI)* and rights problems with Active Directory (configuration nodes could not be created due to missing authorizations). For compatibility with these installations, the installation variant of the local Exchange Server installations is also supported by msxbcsgate.

The installation wizard carries out all important installation steps automatically. After the installation, however, a manual adjustment to the Exchange Server is necessary. No objects are created automatically in the Exchange Server organization.

> **Attention!**
> The installation is based on bidirectional e-mail transmission. For this reason, the installation wizard installs its own SMTP server and opens port 25 by default. For this reason, such an installation should not take place on an Exchange server itself. An Exchange Server itself maintains a connection to port 25. The installation of an OfficeMaster server with a local installation variant of msxbcsgate should always take place on a dedicated server. If this is not possible, an alternative port must be used for the *smtprx* component be configured to which the Exchange Server can then deliver the documents.

Installation requirements

Service account to access address books and local Active Directory

A separate service account or mailbox is required to operate the connector. This service account should be created manually as a normal user mailbox beforehand. The mailbox is used to access the public address book of the Exchange Server and is stored in the connector.

Local Service Account (access to local Active Directory)

The connector must have minimal access to the on-premises Active Directory to properly authenticate users. His read permissions in the organizational units of the domains should be correspondingly high.

There are several reasons for using a service account:

- Reading the configuration data of the connector stored in the Active Directory
- Reading global configuration values
- Resolve domain users and read user values
- Writing user-specific values after configuring voice parameters (own phone number, voice box pin, etc.)

Such an account should have the following authorization structure:

- Member of the domain users group
- Local administrator of the installation computer
- Read access permissions on the path containing the configuration file
- (Install option) Global data: Global Active Directory context: In this case, the service account needs organizational permissions. As of Exchange 2010, the organization's Active Directory read permission can be granted via membership of the Exchange Public Folder Administration group.
- (Installation option) Global data: Active Directory default context: In this case, the account does not need any additional permissions.
- (Installation option) Global data: Common configuration file: In this case, the account does not need any additional permissions.
- (Installation option) User data: Active Directory - User object: If voice properties such as PIN or phone number values are to be changed by users via remote inquiry or Outlook client with the connector, the account must have write permissions in the user objects of the connected domains.

Installation

The connector can be installed via the Exchange quick launch bar in the Hybrid/Cloud submenu.

An installation wizard will now appear. The components should only be created and deleted using this installation wizard.

The welcome screen is followed by a dialog for selecting the type of installation. Three installation forms are available:

1. Microsoft Office 365 as full cloud installation
2. Microsoft Office 365 hybrid installation with on-premises Active Directory
3. Local Exchange Server Installation (On-Premise)

The third type of installation is used for local installations.

In the next step, the transport type is selected. The transport type usually determines how outbound documents are handled. In the local Exchange Server installation variant, no other transport variant is available than the SMTP transmission mode. No transport to an intermediate mailbox is required in the local network.

Messaging Server: The server on which the connector component is ultimately to be executed as an instance can be selected in the Messaging Server input field.

Exchange Server: For communication with an Exchange Server, this must be entered as the default communication partner. A fully qualified domain name (FQDN) or a NetBIOS name can be specified here. IP addresses should not be specified, as a display name is created from this specification.

Transfer mode: No other transfer mode can be selected at this point. The installation form only supports the SMTP transmission mode.

Transfer Domains: The transfer domains are a guide to installation for messaging. The connector will register with the OfficeMaster Server for this domain information. The sender can then send his outgoing documents to fax number@domain. By default, domains should be specified with the subdomain prefixes “fax” and “sms”.

E.g. fax.exampledomain.de, sms.exampledomain.de

> **Note!**
> The domains are separated with a comma or a semicolon when they are specified. The transfer domains are given here purely for registration purposes. Whether the e-mails from the Exchange Server also reach the OfficeMaster Server with this domain specification depends on the manual administration of the Exchange Server.

Address spaces: The installation supports the use of address spaces, but these are not stored here. Address spaces cannot be influenced during installation.

In the next step, the service account for access to the Exchange Server and the local domain is specified.

At this point the service account can be selected. Different service accounts can be specified for Exchange Server access (Exchange Web Services) and access to the local Active Directory. However, this is optional. It is recommended to use the same account for both accesses.

Entitle service account for voicemail services: This function is not available in this installation variant. The account for the OfficeMaster language services may have to be activated manually if language services are to be used.

> **Note!**
> In order to carry out this step manually, this can also be carried out with the Exchange PowerShell: New-ManagementRoleAssignement OfficeMasterVoiceAccess –Role ApplicationImpersonation –User

Local service account with access rights to local Active Directory: A separate account for access to Active Directory can be specified here.

Use EWS service account as Active Directory access account: When activating this function, the values of the Exchange access account (EWS service account) are copied into the input fields for the Active Directory service account.

> **Note!**
> It is generally recommended to use the same service account for access to the Exchange Server (Exchange Web Services) and to the Active Directory.

OfficeMaster standard license group: A license group with the name *OfficeMaster Licensegroup* is created in the Active Directory below *Users*

Individually existing license group: A license group already used for the OfficeMaster Suite and created in a previous installation can be selected here.

> **Note!**
> The license group is only used with a user-limited license (10, 25 or 250 users).

In the next installation step, the local configuration points are specified in which the connector configuration is saved.

File path: The general configuration of the msxbcsgate component is traditionally administered via MMC configuration snap-ins. With this type of connector, the configuration data is always saved in a configuration file. The path of this file can be specified here. By default, a file that is in the OfficeMaster release *FFACCESS* is suggested here.

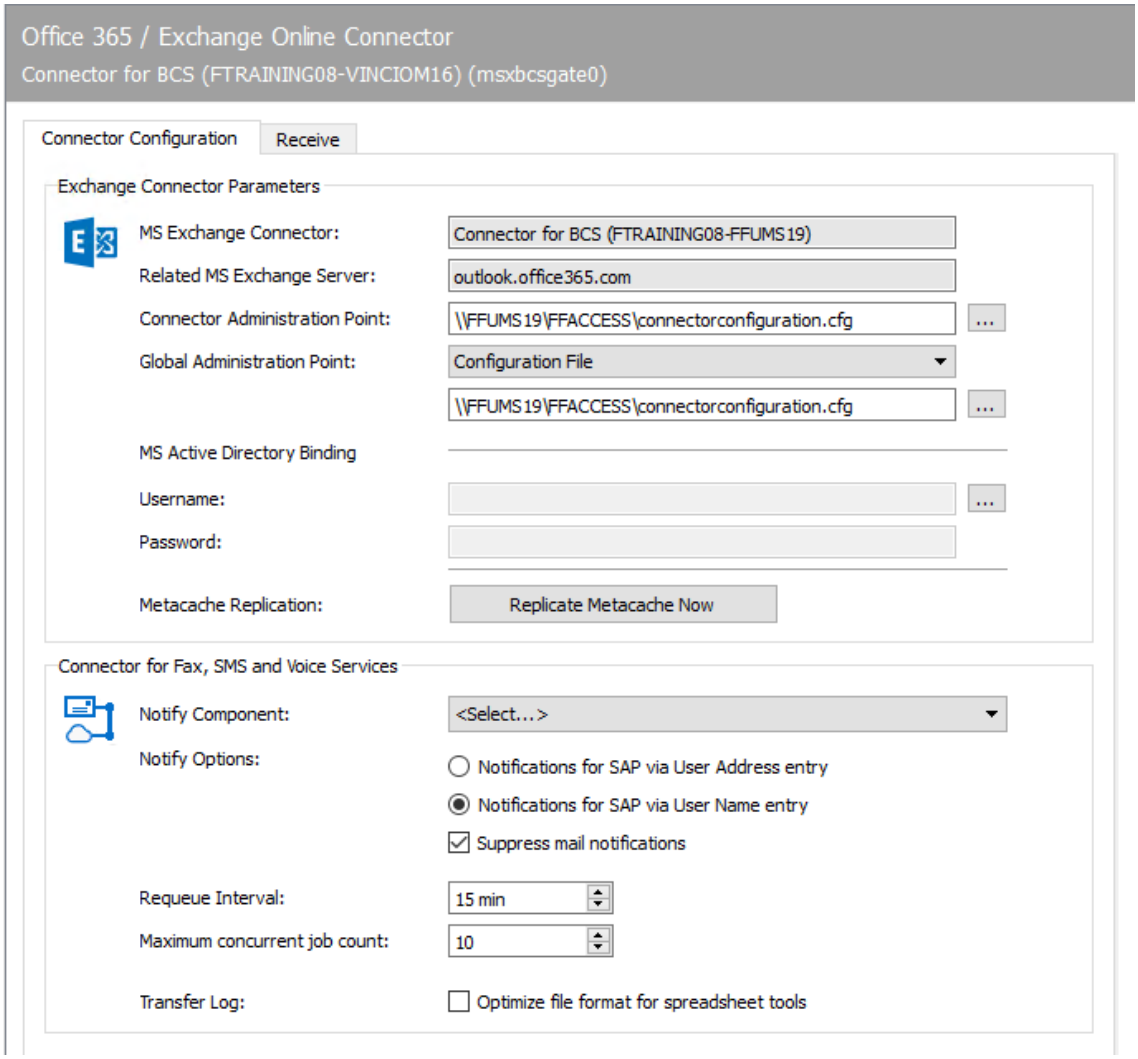
User data management: In the local Exchange Server installation variant, there are two installation options available: - Active Directory – User Object: This is the recommended default. - User mailbox: Alternatively, the user-specific values can also be saved in the user mailbox. This does not make sense in the local installation variant.

Note!
If a previous version of the exchange connectors from Ferrari electronic AG was used and the user-specific values are already available in the Active Directory, they can continue to be used in a compatible manner. If the user management mode is then switched to user mailboxes (not recommended), these values must be migrated from the Active Directory to the Office 365 mailboxes using special utilities, otherwise the Active Directory will no longer be accessed.

Global user data: Global user data is the template data that applies to all users for whom other values have not been explicitly specified (fax ID, header, cover sheet, etc.). In the pure Office 365 installation variant, these global specifications can only be saved in a configuration file. At this point, it makes sense to use the same file that contains the connector configuration data. The default setting is that the values are written globally to the existing Active Directory. This default setting is only set for compatibility with the previous version. This makes sense if such a global configuration node has already been installed from the previous product.

Note!
If there is no global configuration node yet, installation in a common configuration file is recommended.

The necessary parameters for installing the connector are now known. The connector will now be created in the OfficeMaster Suite by the wizard. After installation, the component should start immediately and be ready for use. The next step is to create the required send and receive connector manually in Exchange on premises.



10.13.5. Connector configuration

Although the Exchange connectors store all relevant settings in the OfficeMaster Exchange Administration in order to integrate the components into the Exchange Server environment, the individual components also have basic settings in the messaging server configuration that ensure the smooth operation of the components.

The basic settings are on the Connector Configuration tab.

Exchange connector parameters

These settings are set by the installation wizard. They include the name of the Exchange connector (rule in Exchange Online), the name of the Exchange server for login (Outlook.office365.com), the path to the configuration file (connectorconfiguration.cfg) to configure the connector or base node . If the base node is stored in the local Active Directory in

a hybrid installation, the corresponding path is also automatically stored here, as well as the account used to read out the Active Directory.

MS Exchange Connector

This field contains the name of the Exchange Connector (OfficeMaster Suite) / Exchange Rule (Exchange Online)

MS Exchange Server

When connecting to an Exchange Online, the address *outlook.office365.com* is always included.

Connector admin point

The connector administration point is the configuration file in which the connector expects its actual configuration. This entry can be changed or restored accordingly. A change in this parameter is only available for restore purposes and should not be changed without the installation wizard.

Global administration point

Microsoft Active Directory: In this mode, the connector searches for the global point in the configured Active Directory

Configuration file: In this case, the connector uses the specified file to read out the global user values.

The entries can be changed or restored accordingly. A change in this parameter is only available for restore purposes and should not be changed without the installation wizard.

MS Active Directory connection

A user name and password can be stored in the Active Directory connection fields, with which the connector accesses the configured Active Directory. With a pure Office 365 connection, these entries are empty.

Metacache replication

There is a button in the configuration that can be used to trigger metacache replication outside of the set intervals. This option is only implemented for test purposes.

> Note!
> While basic settings can be configured, manual administration is not recommended. The basic parameters should only be set by the installer. Manual changes can severely disrupt the correct operation of the components.

Connector for fax, SMS and voicemail services

The settings in this area determine the interaction of the Exchange Connector components with other messaging server components.

Status component

A status component is an additional component that provides information about the status of the sent fax document or the sent SMS. Here, for example, archive gateways can be specified.

Status options

The *msxbcsgate* component can also act as a state component for other gateways. Here you set additional options:

1. Status messages for SAP based on the user address field

In cooperation with a SAP connector sapconn, it can be set that the sender determination is based on the order field of the user address. This field is then used by the connector to resolve the address in Active Directory.

1. Status messages for SAP based on the user name

In cooperation with a SAP connector sapconn, it can be set that the sender determination in this case is based on the order field of the user name. This field is then used by the connector to resolve the address in Active Directory.

Suppress email status feedback

If the connector is connected to an LPD, it can also process e-mail addresses in addition to fax numbers. The feedback as to whether the LPD has processed the e-mails correctly via the Exchange Server via relay forwarding can be suppressed here.

Requeue Interval

If messages cannot be delivered to the mail server due to faulty connections, they are queued again. The waiting time until the new order can be set here. The default setting is 15 minutes.

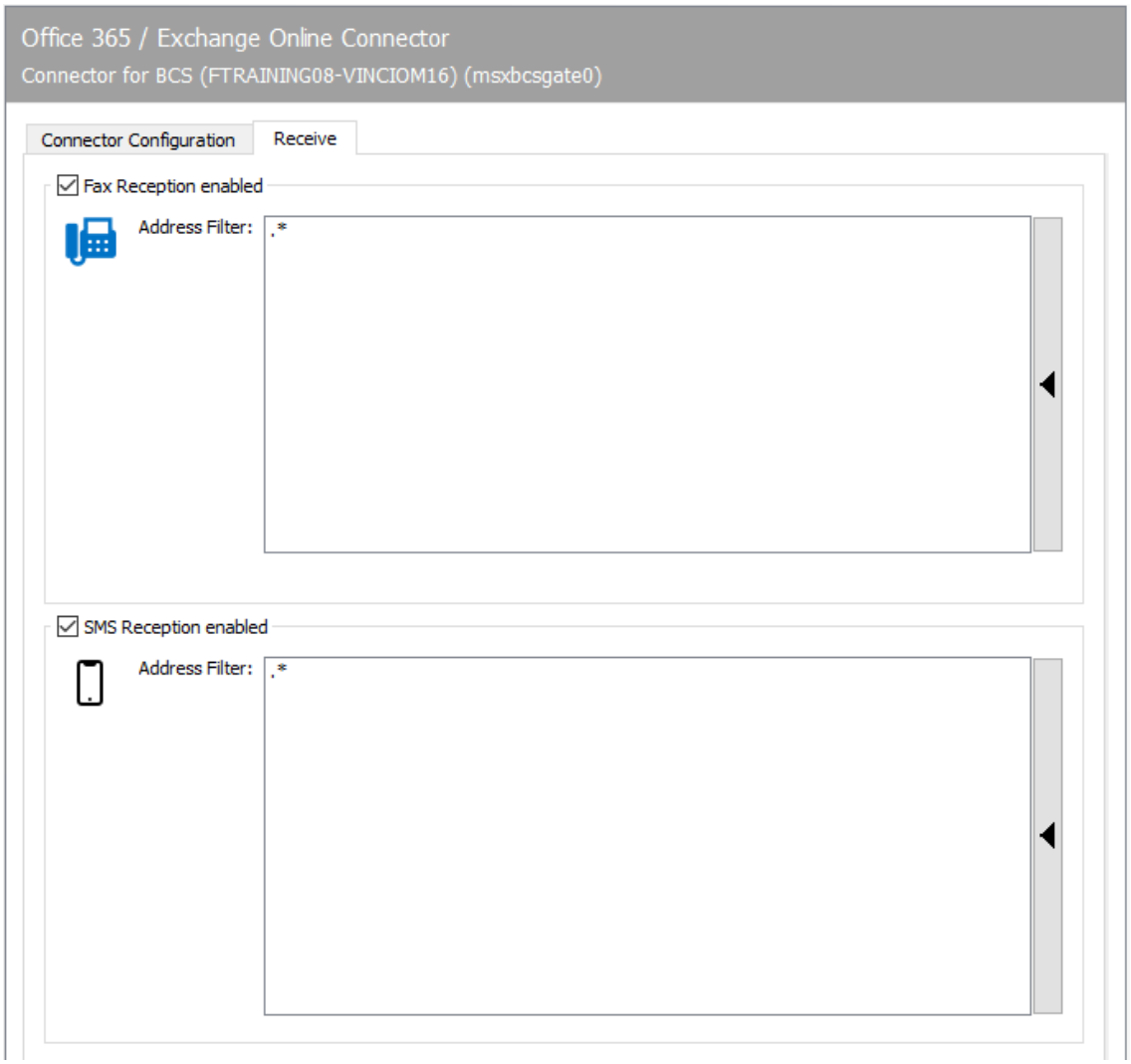
Simultaneous order processing

The connector is able to process several orders at the same time. The maximum number of simultaneous jobs to be processed can be specified here.

> Note!
> The optimum number for current computers is 10. This is also the default setting. The value can be reduced to 1 to force sequential processing of the orders. This should only be done for testing purposes. It is recommended to enter a value between 8 and 10.

Transfer log file / Optimized for spreadsheet programs

The msxbcsgate component writes a file with the orders that have been processed for each day. Telephone numbers in E.164 format are also written to this file. It was often found that spreadsheet programs convert this notation (e.g. +49332845590) into a floating point representation. (+49332845590 becomes 4.93E+10) Leading zeros are also mostly removed by the program. To mark these entries as text, the entry can be preceded by a single quote. Modern spreadsheet programs then interpret this data as unchangeable character strings and leave the display unchanged.



10.13.6. Reception

The Reception tab has a direct impact on the incoming documents. The telephone numbers (Called Party Number) intended for the Exchange Connector can be entered as an address filter for faxes or SMS. With the default setting (.*), all received faxes or short messages are forwarded to the Exchange connector.

A change is only necessary if received messages are to be distributed to different gateways, such as msxbcsgate, sapconn, filegw etc., or if messages from OfficeMaster are only to be received on certain phone numbers.

The latter, the so-called whitelist procedure, can be activated under Extras > Black & Whitelist > Reject undeliverable messages.

> **Note!**
> If the address filter is restricted to certain phone numbers without an activated whitelist procedure, the UNDELIVERABLE component of the messaging server

should be configured so that received messages are not stored unnoticed on the server and “stay behind” despite the best address filter configuration.

In the simplest case, an address filter consists of a list of numbers that are assigned to the connector. For example, if all faxes to the numbers 150 to 154 are destined for the Exchange Connector, the address filter list contains the following entries: 150 151 152 153 154

The entries in this list can be combined with regular expressions into entry 15[0-4].

The default value (.*) for the address filter is also a regular expression. The dot (.) stands for any character. The asterisk gives the character in front of it the meaning as often as you like. At this point, only one address can be specified per line. It is not possible to combine several expressions in one line using OR (|) or AND (&).

10.14. Notes connector

OfficeMaster has a fax/SMS/ and a voice gateway (*NOTESCONN*) for the connection to IBM Notes/Domino Server. To communicate with the Domino server, the gateways use a Notes Basic Client, which must be installed on the OfficeMaster server and set up with a *Notes User ID* and mailbox provided for OfficeMaster. While the fax and SMS users can be maintained in the existing *name and address book* (short: NAB), OfficeMaster includes a database template for managing the voice users. User groups in the *name and address book* are to be created or existing ones used for sending permissions, standard recipients and user maintenance.

10.14.1. Initial configuration steps

Notes Basic Client with Notes user ID

- Necessary steps:
- Create Notes user ID
- Install Notes Basic Client

The relevant information for the connection to the Domino server is set up on the server computer for the fax/SMS/voice gateway (*NOTESCONN*) by the Notes client. In addition, the messaging server uses the Notes client for each outgoing fax in order to convert Notes mails into fax cover sheets.

It is necessary to run the Notes client on the OfficeMaster server under a *Notes User ID* without a password. The *Notes-User-ID* can be identical to the *Notes-Server-ID* if the Domino server is running on the same computer, otherwise a separate *Notes-User-ID* is assigned.

To start up OfficeMaster, some settings must be made on the *Domino* server and the OfficeMaster Messaging Server.

> **Attention!**
> A Notes user ID without a password cannot be saved in the name and address book. When registering the Notes user ID, storage in the name and address book must be deactivated.

Furthermore, the *Notes-User-ID* requires unrestricted access to the Notes mailboxes of the users who want to query voicemails remotely. Voicemails can also be received without this full access.

10.14.2. Outbound routing and mailbox (administrative client)

Documents to be sent are sent by the users as a Notes mail to *fax number@fax domain* or *telephone number@SMS domain*, e.g. *03328-455-960@fax* or *01520158924@sms*. The domain information is a foreign domain. Messages are stored by the Notes mail router in a mailbox on the Domino server, where they are found and processed by the messaging server's *NOTESCONN* gateway.

For commissioning, an external domain must now be set up for fax and SMS, which save the send jobs in the *NOTESCONN* transfer database. By default, the names *fax* and *sms* are used for the domains. If different names, e.g. *berlin-fax* or *fax01* are used, these must be taken into account in the *NOTESCONN* configuration.

A mailbox is required for the domains, which is monitored by *NOTESCONN* for new send jobs. The user mailbox can be used as a transfer database either with the created *Notes-User-ID* or with a new mailbox to be created (previously *ffax.box*). Both steps are described below.

User mailbox of the Notes user ID as transfer database

By default, *NOTESCONN* uses the user mailbox of the *Notes-User-ID* as the transfer database. This means that no special access authorizations need to be configured. However, test faxes and SMS must always be sent from a workstation computer with its own user ID.

Separate mailbox as transfer database

As an alternative to the user mailbox of the *Notes User ID*, a separate mailbox can be created as a transfer database. This must be done manually on the Domino server responsible for *NOTESCONN*. The default name of the separate mailbox is *ffax.box*.

> **Note!**
> In order to avoid authorization conflicts, it is advisable to create the mailbox with the Notes Client from the OfficeMaster Messaging Server. To do this, select the menu sequence File > Database > New in Notes

Since the messaging server may need to use the masks used in the documents to create the cover sheet, the standard mail template (*Mailxx.ntf*) should be used when creating the *ffax.box*. The standard mail mask is contained in the *ffax.box*.

After the mailbox has been created, it must be taken into account in the access control list (*ACL*) that the Notes user ID with which the *NOTESCONN* gateway is operated can open, print and delete documents. If the *NOTESCONN* gateway runs under the server ID, the server must also be declared as a person in order to receive the necessary authorizations.

Foreign domains for Fax/SMS (Foreign Domains)

The external domains for fax and SMS are configured in the company-wide name and address book (*names.nsf*) under Configuration > Messaging > Domains (Configuration > Messaging > Domains.

One domain for fax and one domain for SMS is required. These domains are of the type *Foreign Domain* or *Foreign Domain*. The name of the domain can be chosen freely. Experience has shown that the names *fax* and *sms* have proven useful, since they achieve a high level of acceptance of the solution by Notes users.

In larger installations, with several fax gateways, the domain names must of course be different, such as *fax-berlin* and *sms-vertrieb*.

The name of the Domino server on which the transfer database (*officema.nsf or ffax.box*) is stored is entered under *Gateway server name*. The gateway mail filename consists of the path and filename of the handoff database on the gateway server. If the mailbox of the gateway's Notes user ID is used as the transfer database, *mail\officema.nsf* must be configured accordingly as the mail file name.

If it is a separate mailbox, enter its name (like *ffax.box*).

> **Note!**
> After setting up a new domain, the router task of the Domino server may have to be restarted.

10.14.3. Journal database (ffaxlog.nsf)

Access with administrator rights

The fax and SMS gateway can also deliver each send and receive process to a *journal recipient*. Every Notes user, every Notes user group and every mail-in database can serve as a *journal recipient*. If a special mail-in database is to be used, OfficeMaster offers a Notes template that visually enhances the journal entries in the journal database. The journal database has the default name *ffaxlog.nsf*.

The installation program makes the template _ffaxlog*om4.ntf* available on the OfficeMaster server computer for designing the journal database. This template contains the mask *FFAX*. By default, the individual fax processes are displayed with this. It contains the most important information about the process.

> **Note!**
> If OfficeMaster is installed before the Notes Basic Client is available on the

computer, the OfficeMaster templates are stored in the directory C:\Program Files (x86)\Lotus Notes\Data. These must be moved to the correct Notes data directory so that access from the Notes client is possible.

10.14.4. Editing of the templates with the Notes Designer

You can use the Properties > Document.. function, which can be activated by right-clicking on the selected journal entry, to obtain detailed information about all the process parameters.

Authorized users can see the incoming and outgoing journals for all fax transactions. The *OfficeMaster Journal* template offers the following views:

One of the following two access rights to the database must be granted:

- Reading rights: only your own messages can be read
- Special rights: the access rights can be freely distributed to the database

In addition, rights to the corresponding document are required:

- readable by recipient/sender
- all *LocalDomainAdmins* (default group in *Dominodircetory*) with it backup/fallback of OfficeMaster
- Owner of the *Operator* role

10.14.5. Default recipient in NAB (FFAXcentral)

Received faxes and short messages that cannot be delivered to the correct recipient due to an extension number are first sent to one or more standard recipients who are specially provided for this purpose and who can carry out manual distribution. They are defined in a special group.

The default suggested name is *FFAXcentral*.

Since the group of standard recipients is addressed on the fax and SMS gateway using the group name, the group does not need to have a fax extension number; the name is case-sensitive.

10.14.6. Permission Management

In the OfficeMaster standard configuration, every Notes user who is listed in the *Names and Address Book* (*names.nsf*) for the connectors is authorized to send and receive faxes and short messages (assuming a sufficient number of OfficeMaster user licenses).

If faxes and short messages are only to be sent and received by selected Notes users, these Notes users can be combined in a group. This is usually necessary when the number of users in the *name and address book* exceeds the number of users licensed for OfficeMaster. This group must first be set up. The suggested name for the group in the NOTESCONN configuration is *FFAXUser* – case sensitive. In the group, each fax-authorized person must be entered individually. Entering groups is not permitted. To start the connector it is required that at least one user is a member of this group. When a Notes user sends/receives faxes and short messages, it is checked whether he is a member of the *FFAXUser* group.

As an alternative to a group, fax and SMS authorizations for Notes users can also be checked using fields in the person document. There are three additional variants available for this purpose:

- By condition: All persons who have a field with a certain value in the person document (e.g. the company entry Ferrari electronic AG / Teltow) are authorized to fax.
- Field with any value: All people who have any entry in a specific field, e.g. a registered fax number, are fax authorized.
- According to the formula: All persons who are in a view (view) are authorized to send faxes. You don't have to specify the name of the view, but the corresponding formula.

If an unauthorized user sends a fax or an SMS to OfficeMaster, this message is sent back to the sender with an error message.

10.14.7. Voice User Address Book (fvoice.nsf)

In order to ensure the necessary authorizations, the address book should be created from the OfficeMaster Server. To do this, open the Notes client and select the menu sequence File > Database > New.

The name of the address book can be freely selected. In the further course, the name *fvoice.nsf* is assumed. The address book must be created on the Domino server, since other Notes clients can also access the address book for user maintenance within the scope of their authorizations. *OfficeMaster Voice* must be used as *Template*. This template is installed with OfficeMaster and is available locally on the OfficeMaster server.

After the address book has been created, OfficeMaster's *Notes-User-ID* must be assigned all roles in the access control (ACL) so that the implemented scripts for creating users can be started. Of course, these roles must also be assigned to the Notes users who are to maintain voice users.

> **Note!**
> So that the Notes user ID can now add users, the address book may have to be closed and opened again via File > Database > Open.

In the address book, Notes users can be added via the toolbar and then administered.

10.14.8. Access to user mailbox

Received voicemails are only saved in the user mailbox of the corresponding Notes user. If a voicemail is to be played back on the telephone as part of remote inquiry, the voice connector must transfer the voicemail from the user mailbox to the voice server. To do this, OfficeMaster's *Notes-User-ID* must be granted access to the user mailbox. Since voicemails can not only be picked up but also deleted as part of remote inquiry, it makes sense to allow the *Notes-User-ID* full access to the user mailboxes of all Notes users who want to listen to voicemails with the telephone.

Since this is particularly problematic in larger companies, it can sometimes be dispensed with. Received voice messages are then not listened to on the telephone, but are only played back on the PC speakers at the workplace. This does not affect the receipt of voicemails.

10.14.9. User maintenance

Fax and SMS users

The fax and SMS users are maintained in the *names and addresses book* (*names.nsf*) specified in the *NOTESCONN* configuration. By default, the extension number under which a Notes user can be reached via fax is entered in the *Fax (office) (OfficeFaxPhoneNumber)* field. If a different field is to be used for organizational reasons, this can be specified by making appropriate entries in the *NOTESCONN* configuration.

> **Note!**
> When writing the extension numbers, it should be noted that the extension digits must be right-justified without special characters.

Any characters are allowed to the left of these digits. It makes sense to enter the entire fax number including the area code and possibly also the country code, since this field e.g. can also be transferred to documents.

> **Example:**
> The following values are all equivalent
> - (49) (0) 3328 455 349
> - Mustermann fax no.: 03328 455 349
> - 349
> - (03328) 455 349
> - 03328455349

The fax extension can also be appended to the company's base number as a sender identifier. *NOTESCONN* uses the digits to the right of the last separator as the fax identifier.

Groups and mail-in database

If a direct dialing number is to be assigned to a group or a mail-in database (only the group is described below), this is done by default in the *Description* field (*Description*).

Description

The same syntactical rules apply in the *Description* field as for individual persons. A separator must be placed in front of the fax number. Another field can be specified in the NOTESCONN configuration as part of the administration. This ensures that all members of the group receive an incoming fax automatically.

Voice user

The voice users are administered in the address book *fvoice.nsf*, which is to be maintained separately. Here you can add new users in the toolbar.

Provided the appropriate authorizations are available, users who have already been set up can be edited.

Notes user

For configuration, the *Notes user* is selected from the *Name and address book* and displayed.

Display name

The display name is used for the visualization of the address resolution of calls.

Login name

When logging in via the web UI, their login name is checked against this field.

Login Password

With free login to the web client, the password is searched for in this field.

Voicemail number

The *Voicebox number* depends on whether a separate extension number range is available for the voice users (*Called Party Number*) or whether the relevant voicebox is to be addressed using the redirection information (*Redirecting Number*). The latter assumes that the ISDN connection signals this diversion information to the voice server.

On my phone number

OfficeMaster Flex uses this phone number to play voice messages on this phone.

PIN for remote access

The *PIN* protects the Voicebox against unauthorized access via voice remote inquiry. The PIN is a combination of numbers that can be one to any number of characters long. In practice, four to six-digit PIN codes have prevailed.

Message waiting phone

The message lamp (*Message Waiting Indicator - MWI*) is activated on the telephone with this call number when there are new voice messages.

Query permission

In addition, up to three authorized numbers can be stored per user. These phone numbers are compared with the calling party number of the caller (also with the possibly prefixed zero). If the phone number is the same, the PIN query is dispensed with and the caller goes directly to the query mode.

Voice project

One of the voice trees can be set here for the user. B. differ in the menu navigation. If the entry is empty, the voice server uses the standard *Voiceprojekt* as the voice tree.

Language

The *Language* can be set per user. OfficeMaster is delivered with German (*DE*) and English (*EN*) announcements. The language configuration affects the menu navigation for querying and configuring the voice box and the standard greeting if the user has not stored a personal greeting.

10.14.10. Connectors for Notes

The *NOTESCONN* component can be created via the quick launch bar > Notes > Fax/SMS Voice > *New Notes Connector*.

> **Note!**
> If the connectors have not yet been set up as components of the OfficeMaster Suite, they can also be added manually in the component table.

Create connectors in component table

The component table can be accessed via the *Create components* option in the *NOTESCONN* configuration.

10.14.11. Conversion and cover pages

Since when faxing, in contrast to sending an e-mail, graphic information is not sent to the recipient but graphic information, the message to be sent must first be converted into fax format. Depending on the type or structure of the document, different procedures are used:

- Centrally through the OfficeMaster Messaging Server, which controls its own Notes client.
- Embedded documents are converted together with the Notes documents.
- Attached documents are always converted centrally by the messaging server after the associated Notes document has been converted.
- As an alternative to the Notes mask, RTF documents can be stored on the messaging server and used as a cover sheet.

Conversion with the Notes client

The documents are converted directly in the mailbox of the fax gateway by opening the incoming fax like an e-mail and converting it using the *ferrariFAX32/64 Windows printer*. Since

the fax is opened there according to Notes mechanisms with the mask stored in the *Form* field, any Notes document can be faxed if the corresponding mask is available in the mailbox.

For this conversion, the fax gateway uses the Notes client on the server (also referred to below as the conversion client). Using the Notes client for the central conversion has the following advantages for the user:

- All of your own Notes documents can be faxed without having to make any adjustments to the fax solution.
- If the current version of the Notes client is installed on the server for the central conversion, all RTF elements can be converted, even if you switch to a newer version of Notes.
- By using the latest client, OfficeMaster is always able to convert the latest Notes RTF elements.
- A very simple central administration and creation of fax forms can take place on this client.

If a Notes document is sent, the following options are conceivable with regard to the mask and the conversion:

1. The mask used does not exist on the conversion client. The document is opened and converted with the standard mask defined there, whereby the fields of the document that are present in the standard mask are displayed.

2. The mask used is available on the conversion client under the same name as the original mask. The document is opened and converted with the original mask.

3. The mask used is not available on the conversion client, but is saved in the document. The document is opened and converted with the original mask.

4. The mask used does not exist on the conversion client, but another mask with the same name is stored in the conversion client. This opens and converts the document.

With the second and third variants, the fax looks like a printout of the original document. In the fourth variant, fax cover sheets can be designed centrally without having to make any modifications to the user's mail templates. In this way, a user can write a fax in his standard memo mask, which later receives the company's standard fax design when it is sent.

10.14.12. RTF cover sheets (recommended)

As an alternative to Notes templates, *rich text documents* can be stored on the messaging server and used as a cover sheet. The cover sheets are stored on the messaging server in the %ProgramData\FFUMS\FMSRV\data\stationery\ directory. Placeholders can be embedded in the RTF document, which contain additional information about the specific transmission

process. This information is sent by *NOTESCONN* when the send request is created and replaced by the messaging server (_CMDCONV) in the RTF cover sheet before conversion.

> **Note!**
> In order to use the RTF cover sheet design, corresponding cover sheets must be stored on the OfficeMaster server and addressed in the messaging server configuration for *NOTESCONN*.

10.14.13. Notes cover sheets/templates (alternative to RTF cover sheets)

A fax form can be created based on the memo mask and corresponding sub-masks. The actual Notes mask serves as a form. An attached document is in a field specially set up for this purpose with the property *Do not print*, so the icon is not converted. Each appendix always starts on a new page. A cover page with page breaks can also be created, with the actual text starting on the next page.

These are custom Notes forms that exist on the user client and have their own *Form* name. In the case of central conversion, these must be available to the conversion client by being saved either in the document or in the mailbox of the fax gateway.

Central conversion of the memo mask

If Notes users want to send messages to both e-mail and fax recipients, a specially adapted mask for the e-mail recipient is not necessary and often not desired. By using the central conversion client, there is a very simple solution for designing the cover sheet: The Notes client opens the fax with the mask whose name was given to it. If this mask is designed differently than the original mask, the Notes client will use it during the conversion.

> **Example:**
> The usual letterhead is removed from the *Memo* mask on the conversion client and replaced with the company address and logo.
>
> The user now sends a message from the Notes client from his mail mask to mail and fax recipients.
>
> Mail recipients usually open the received mail with the same standardized mask. The conversion client opens the mail it has received with the customized mask and converts it.
>
> Fax recipients receive the message on a fax form with company address and logo.

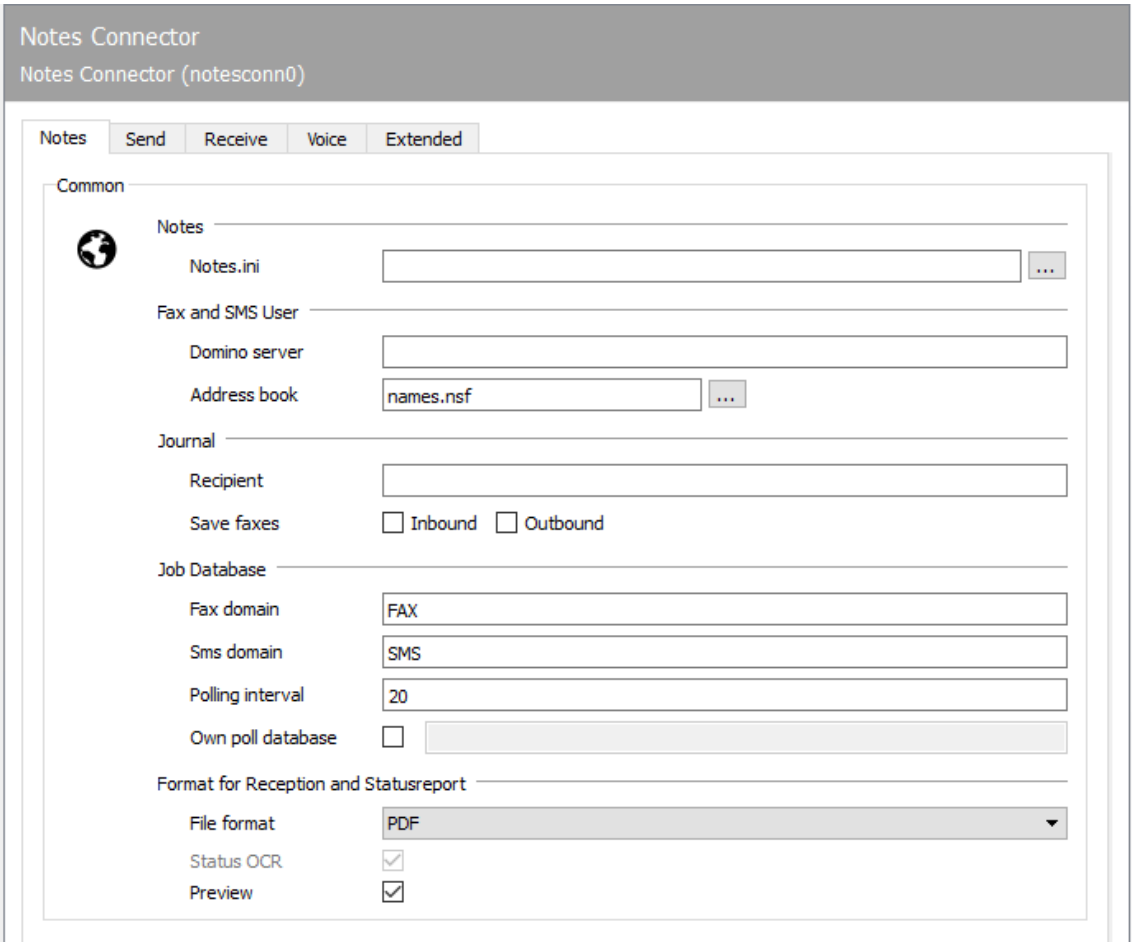
In order to transfer recipient names and numbers to cover sheets, the fax gateway saves the individual parts of the e-mail address in the defined fields _FFAX*ReceiverName*, _FFAX*ReceiverNumber* and _FFAX*ReceiverDomain*. These can be integrated into the mask on the conversion client. In this case, the individual recipient's name is also on the cover sheet of documents that are sent by the sender to several addressees.

All Notes design options can be used in the Notes masks on the conversion client, e.g. Database queries and user-dependent sub-masks. A cover sheet can also be selected by passing a specific parameter or a script that passes the name of the selected form. There are almost no limits to the possibilities for designing the cover sheet.

10.14.14. Embedded documents

Another document, e.g. a Microsoft Word file can be inserted. This file then becomes part of the message. Like the message, it is converted to fax format via the printer driver, retaining all RTF attributes, and appears in the document at the point where it was inserted.

If the same file is defined as an attachment using the Notes function *Attach*, it is converted centrally by the fax gateway into fax format. The format definitions within the document are retained if it is ensured that all typefaces (fonts) that were used when the document was created are also available during central conversion. In contrast to the inserted document, each attached document starts on a new page.



10.14.15. Notes

If the gateways are available in the messaging server, the fax/SMS and voice gateway (*NOTESCONN*) can be configured in the quick launch bar > Notes > FAX/SMS/Voice. All parameters required for commissioning can be set here.

General

Notes.ini

In order for the fax and SMS gateway to be able to use the Notes client, the name and path to *Notes.ini* are required. If the messaging server configuration is executed on the *NOTESCONN* server, the *Notes.ini* can be selected using the [...] button behind it. The *Notes.ini* is usually located in the Lotus Notes directory under ...\Programs\Lotus\Notes.

Fax and SMS users

Domino server, address book

In addition to the *Notes.ini*, the *Domino Server* and the *Address Book* are required, in which the fax and SMS users are maintained in Notes. This is usually the company-wide *names and addresses book* (*names.nsf*) and its Domino server.

In global companies with several international locations, the company-wide name and address book can contain several thousand entries. In such environments, it makes sense to maintain the Notes users intended for OfficeMaster in a separate address book. This reduces the connector's access times to the user-specific parameters required for each send process and thus increases message throughput.

This separate address book can be stored on any Domino server on the network as a partial replica of the company-wide name and address book. If the database is to be saved on the OfficeMaster Server, the Domino server to be configured is left empty. If the fields for reading out the configured values in the address book have to be adjusted, this is done using the *button* [**...**], whereupon the *Notes Fields* window opens. If the user-specific parameters are to be taken from fields other than those provided in the name and address book, or if a completely different database template than the typical Notes address book is used for the *NOTESCONN* address book, the fields can be configured using the button of the same name (see the *Section Notes Fields*)

Journal recipient

Recipient, save faxes (receipt, send)

All sending and receiving processes processed by *NOTESCONN* can be sent to a *journal recipient* via Notes mail for the purpose of logging. Behind the *journal recipient* is either a Notes user, a Notes person group or a mail-in database.

With the OfficeMaster installation, the database template *ffaxjournal.ntf* is installed, which contains customized views (views) with which the received Notes mails can be divided into send and receive processes.

Whether the sent or received faxes should be included as a mail attachment in the Notes mails to the *Journal recipient* can be set using the two check boxes *Receive* and *Send*.

Order database

Fax domain, SMS domain

In order for NOTESCONN to be able to distinguish fax send jobs from SMS send jobs, the names for the *fax domain* and the *sms domain* must be configured.

Polling interval

The *polling interval* indicates the number of seconds at which the gateway should search the transfer database for new transmission jobs. The default value (*20 seconds*) is sufficient for productive operation and should only be changed for test purposes.

Own order database

By default, *NOTESCONN* uses the gateway user's mailbox as the job database. Alternatively, a separate order database can be monitored for new transmissions. This database must be created again and assigned to the foreign domain in the name and address book.

Reception and feedback format

PDF, *PDF OCR*, *TIF-G4* and *DCX* (multi-page PCX) are available as file formats for received faxes and status reports. In order to make orientation easier for the Notes user, status messages and received faxes can already be delivered open in the Notes mail. This default can be changed using the ***Fax Preview*** check box.

10.14.16. Notes Fields dialog

People/Contacts

Recipient number, SMS number, fax ID

The receipt number, email address and header (for send requests) of a Notes user are taken from the *OfficeFaxPhoneNumber* field by default. Only the field content from the last space to the end of the field is interpreted. Contains *OfficeFaxPhoneNumber* e.g. the value *03328 455 960*, the *960* is used as the receipt number and SMS number. If the field also contains letters, such

as *Fax-DW 960*, the *960* is also used as the value to be processed. The complete field content is written into the fax identifier for send jobs.

Email address

A person's mail address is required by *NOTESCONN* for receiving processes. First, the Notes users are selected from the configured address book whose receive number (*OfficeFaxPhoneNumber*) matches the phone number (*Called Party Number*) under which the fax or SMS was received. The document is then sent to the determined email address.

Header

The header of a fax is generated from the *CompanyName* field of the sender's person document. For a fixed header, leave the field empty and make an entry in the ISDN configuration.

Groups

Receipt number

In order to be able to deliver receipts to special Notes user groups, receipt numbers must be assigned to them. By default, the *ListDescription* field is used, which must contain the phone number with the same syntax as in *OfficeFaxPhoneNumber*. The text, starting with the last space, is used as the value for the receipt number.

Surname

Receives to Notes user groups are delivered via *Name*. By default, ***ListName*** is used.

Mail-In Databases

Receipt number

In order to be able to send receipts to a special Notes mail-in database, receipt numbers must be assigned to them. By default, the *Description* field is used, which must contain the phone number with the same syntax as in *OfficeFaxPhoneNumber*. The text, starting with the last space, is used as the value for the receipt number.

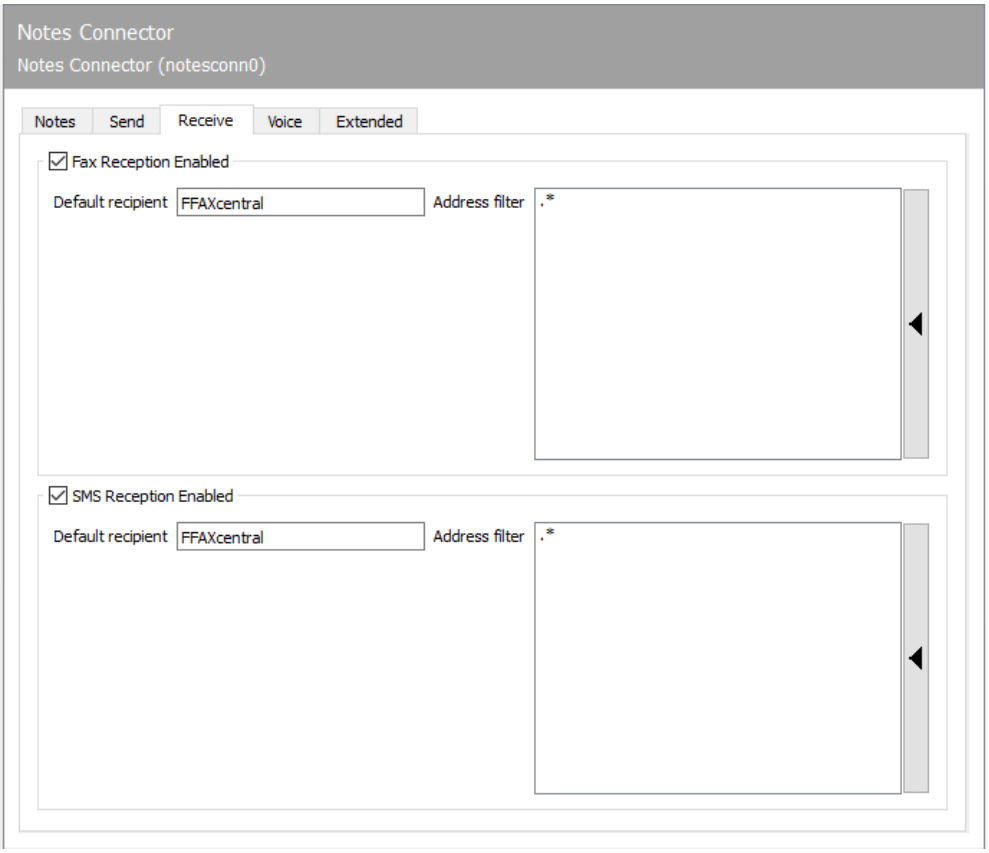
Surname

Receives to Notes user groups are delivered via *Name*. The default *Name* field is ***FullName***.

Status of other gateways

By default, the sender information from LPD and SAPCONN is searched for in the *FullName* field.

> **Note!**
> If status messages from other gateways are also to be sent to the sender via *NOTESCONN*, the sender information of the third-party user or gateway (LPD, SAPCONN) must be stored in the address book of the desired Notes user.



10.14.17. Reception

Activate Fax/SMS reception.

Default recipient

The phone number of received faxes and short messages is compared with the phone number assigned to the users of the address book. In the scope of delivery, the phone number is searched for in the OfficeFaxPhoneNumber field. This setting can be changed if the phone number is stored in a different field in the address book. If there is no entry in the address book under the phone number, the process is forwarded to the default recipient. As a standard recipient e.g. a Notes user, a Notes user group or a mail-in database. The default value FFAXcentral for the default recipient must be created depending on the installation.

Address filter

In addition to the standard recipient, the phone numbers (Called Party Number) from the reception processes intended for NOTESCONN can be entered as address filters for faxes and SMS. With the default setting (.*), all received faxes and short messages are forwarded to the NOTESCONN gateway. A change is only required if received messages are to be distributed to different gateways such as NOTESCONN, SAPCONN and FILEGW, or if messages from OfficeMaster are only to be received on certain telephone numbers. The latter, the so-called white list procedure, can be activated under Extras > System settings via the Reject undeliverable messages option.

> **Note!** If the address filter is restricted to certain phone numbers without an activated whitelist procedure, the undeliverable component of the messaging server should be configured so that received messages are not stored unnoticed on the server and “stay behind” despite the best address filter configuration.

Example:

If all faxes to the numbers 150 to 154 are intended for NOTESCONN, the address filter list contains the following entries: 150, 151, 152, 153, 154. The entries in this list can be combined with regular expressions to the entry 15[0-4]. The default value (*.) for the address filter is also a regular expression. The dot (.) stands for any character. The asterisk (*) gives the preceding character the meaning any number of times.

Connections when receiving messages

Resolution of phone numbers

By default, *NOTESCONN* looks for the extension number in the *FAX-Office* (OfficeFaxPhoneNumber) field in the public address book's Person documents, and also reads it out of the full fax number.

If there is no receiving hardware with extension capability or if an extension number is dialed that has not been assigned to a Notes user, the received faxes are delivered to the members of a standard recipient group (*FFAXcentral*) as a Notes mail, who can then forward these faxes manually to the Notes users . If an extension has accidentally been assigned twice, the fax will also be forwarded to the members of the standard group.

An extension number can also be assigned to a group; the faxes are delivered to all members of this group as Notes mail.

A member of a group can also be a mail-in database. Authorized users can access the faxes collected in it. If a fax has arrived for a Lotus Notes user, he receives the usual notification for newly arrived messages in the status line of his window. The fax is in his inbox and can be treated like any other mail.

FFAX in the *Who* column indicates that it is a fax. The *Subject* field shows the sender ID of the received fax if the sender has set a valid fax ID on his device. Double-clicking opens the Notes mail and shows the actual fax as a file attachment in the body field.

SMS reception with only one phone number

OfficeMaster offers the possibility of receiving short messages and forwarding them to recipients' own mailboxes.

It may be that only one phone number is available for sending/receiving. If there are no extensions, the messages are forwarded in the following way:

- Automatic distribution

In order to forward incoming short messages automatically, a *direct dialing number* must be passed in the text of the message. This is done at the beginning of the message in the syntax .extension.text or +extension+text

Example

.349.Please call me at the office.

+66+New price list in the download area

End of example

In order to simplify the input, it is possible to enter the corresponding letters on the keyboard instead of the numbers. This input method only applies to conventional cell phones with a number pad.

Example

Instead of .349. > .DGW. enter

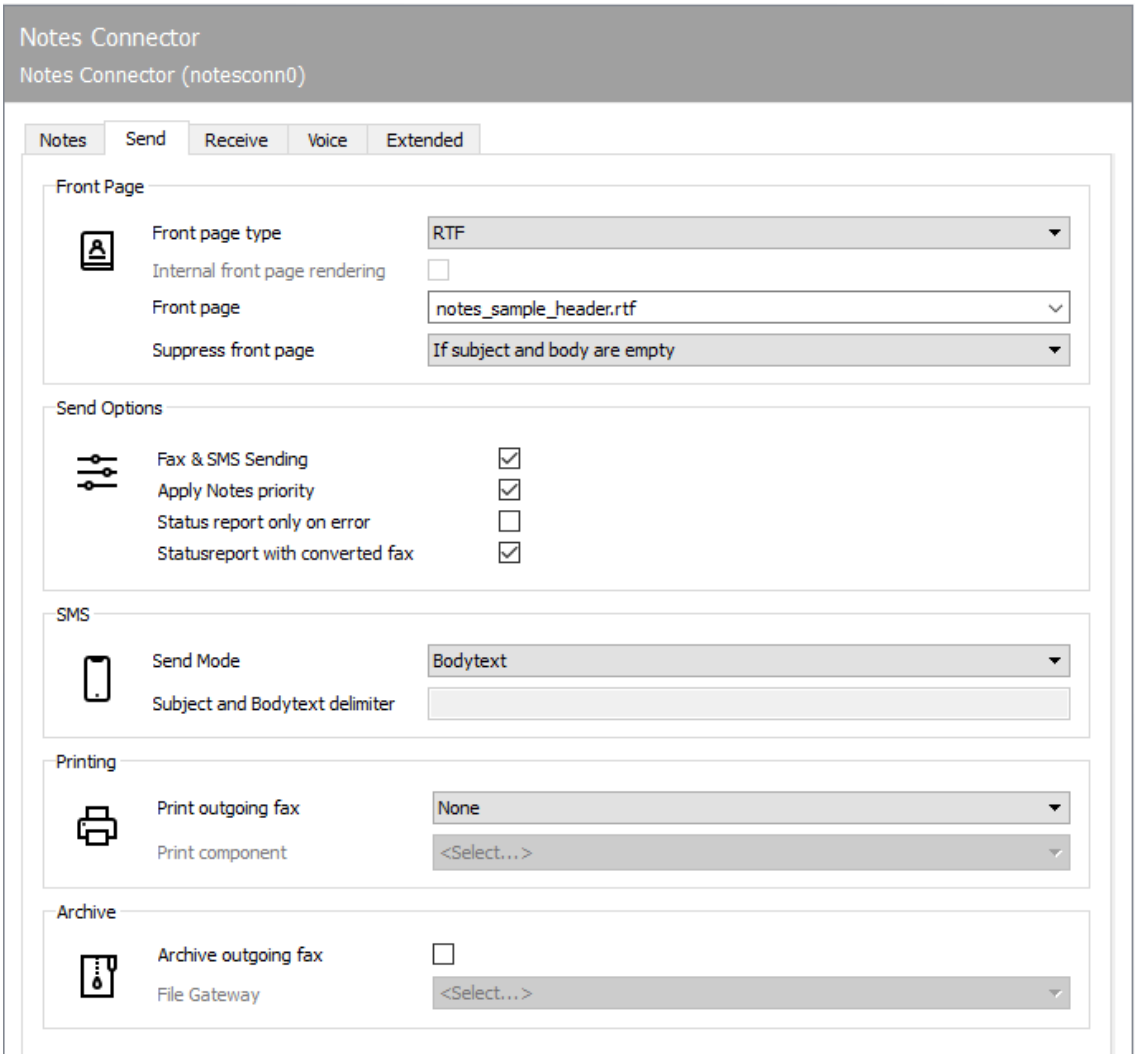
Enter > +MM+ instead of +66+

End of example

Since these numbers are arbitrary and purely imaginary numbers, they can be used i.e, the fax or telephone extension numbers can be dialed for this purpose. *NOTESCONN* reads the telephone number from the person document as an extension number (field *OfficePhoneNumber*). Any other field from the personal document, such as the fax number (*OfficeFaxPhoneNumber*) or the mobile phone number (CellPhone), can also be used. The selection must be set in the NOTESCONN configuration.

- Manual distribution

All unidentifiable short messages are delivered to the default recipient for manual forwarding. Standard recipients are all members of a specially set up group in the address book.



10.14.18. Shipment

The standard values for cover sheet, sending options and printing are configured on the *Shipping* tab. These settings only apply if the send request (in the Notes e-mail or in the address book) does not contain any deviating parameters.

Cover sheet

Cover sheet type

Fax transmission jobs can be provided with a cover sheet by OfficeMaster before they are sent. The cover sheet is created from a cover sheet template into which the values associated with the send order (sender, recipient, subject, message text, etc.) are inserted. Either the Notes form of the send order (usually the memo form) or a rich text document stored on the OfficeMaster

server serves as a cover sheet template. This means that either Notes Format (NTF) or Rich Text Format (RTF) can be selected as the cover sheet type.

- Internal cover sheet provision:

RTF cover sheet

The Notes mask of the send order is used for the Notes cover sheet. This Notes mask can be adapted in the gateway's transfer database (mailbox) with the Notes Designer and designed as a fax cover sheet. As a result, all databases accessible to the Notes client and all techniques that can be implemented with Notes script are used for designing the cover sheet.

The use of the RTF cover sheet offers the advantage that the cover sheet design e.g. with Microsoft Word, can be created without further knowledge of Notes. In addition, the converter component cmdconv of the messaging server achieves a higher throughput than with Notes-NTF conversion. A lot of the information from Notes belonging to the send order can be used in the RTF cover sheet, but there are more design options with NTF cover sheets.

Is the RTF cover sheet template to be used on the server on which the converter cmdconv of the OfficeMaster Messaging Server is operated in the directory %Programdata%\FFUMS\FMSRV data\stationery\, it can be selected as an RTF cover sheet.

OfficeMaster uses third-party software for the central conversion of the cover sheet. Notes cover pages are converted with Notes and RTF cover pages with Microsoft Word or LibreOffice. The third-party programs must be installed on the server where the CMDCONV or OLECONV converters are running and can then be configured for use by OfficeMaster.

Suppress cover page

The subject line (subject) and the message text (mail body) can be used to control the use of the set cover sheet. If NOTESCONN should suppress the cover sheet, this options are available:

- Never
- If subject is empty
- If message is empty
- If subject and message are empty
- Always

to disposal. In practice, the setting if subject and message are empty has proven to be effective. This way Notes mails containing only ready formatted documents can be sent without a cover page.

Options

Fax and SMS sending options

Interpret Notes priorities

In order to influence the order in which send requests are processed, OfficeMaster can interpret the Notes priorities assigned to the Notes mails by the sender. Send jobs with a high priority overtake those with a lower priority on almost every messaging server component. The prioritization particularly affects the components NOTESCONN (to generate the send job in the OfficeMaster Messaging Server), CMDCONV (for the conversion) and OMCUMS or DirectSip (for the dispatch), which are mainly responsible for the processing time of the fax volume. The following table contains examples of which priorities can be selected for which user groups or transmission documents:

Notes Priority	Document type	User Group
High	Urgent documents, such as orders, recalls, etc.	Management, disposition at “Just-In-Time”
Normal	Normal fax dispatch	Standard User
Low	serial fax, group fax	Marketing

Sending status only in the event of an error

If this option is set, status feedback will only be given if there is an error.

Send status with fax document

If activated, the confirmation is sent with the sent fax or with the sent short message.

SMS

SMS communication

Sending the messages

When sending a short message from any Notes database, the message is in the *Body* field - ie in the text entry field of a new mail. Only the content of this field is sent as a short message. If the SMS dispatch is to be limited, this can be done via the *Send mode*.

Shipping mode

- Message text
- Subject text
- Message text and subject text

In order to send a message as a short message, the recipient's mobile number must be specified in the form of an email address and sent to the foreign domain created during the installation of the SMS gateway.

In order to send an SMS, the address in the form *mobile number@SMS domain* must be entered in the field *AN* (SendTo), e.g. *015201589249@sms*

Print

If OfficeMaster is to print sent faxes, these are forwarded to a previously configured print component (PRINTGW). In order to print received faxes automatically, the telephone numbers (Called Party Number) on which the faxes to be printed were received must be stored in the corresponding print component (PRINTGW) using regular expressions. If faxes need to be printed or not, it can be set under the parameter ***Print sent faxes***. The following options are available here:

- None
- Sent successfully
- Incorrectly sent
- Everyone

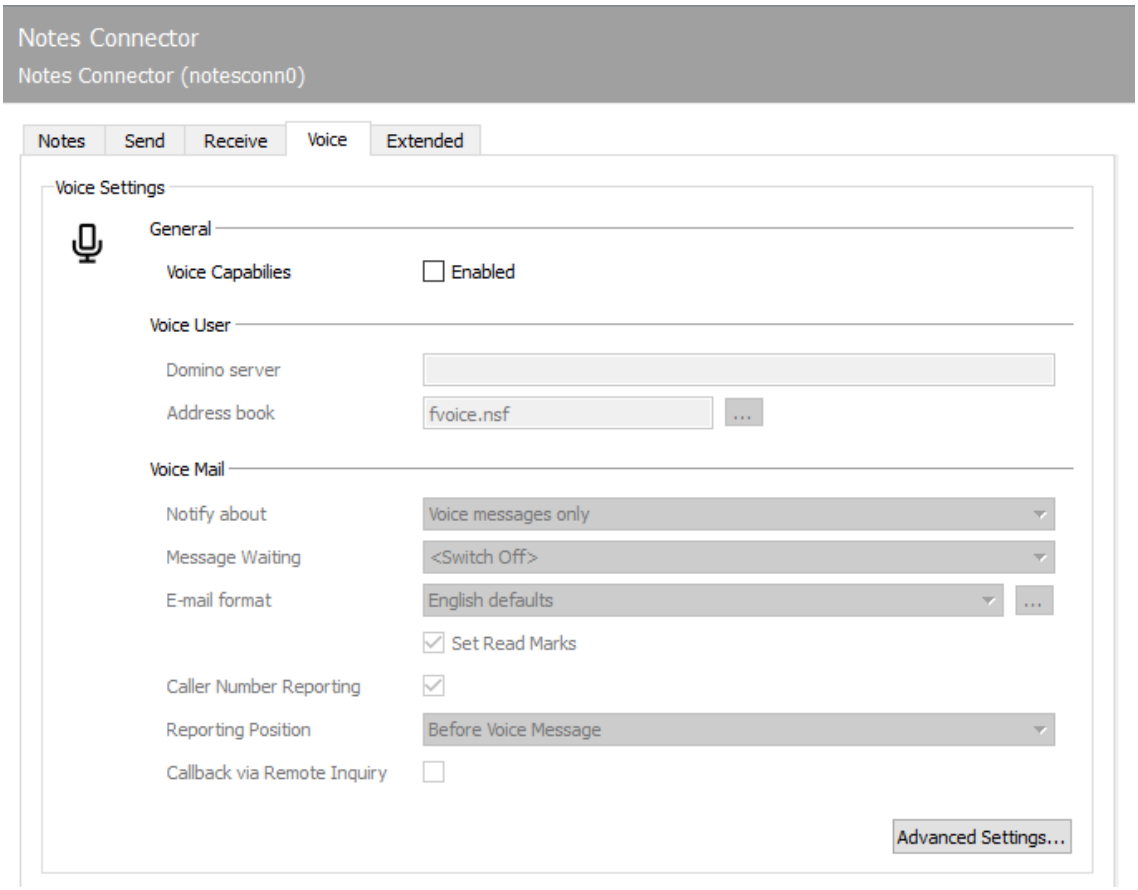
Print component

Select the print component where the printer to be used has been configured.

Archive

File interface

OfficeMaster can archive all outgoing faxes via an existing file interface/file system connector (FILEGW) that is selected here.



10.14.19. Voice

The voicemail for Notes is configured via the *Voice* tab.

The first start-up requires information on the voice server that is responsible for this voice gateway and information on the address book in which the Notes user parameters relevant to voice are maintained. This address book may have to be created as a separate address book (*fvoice.nsf*) for voice before the *NOTESCONN* configuration, since the standard address books (*names.nsf*) in Notes do not have any fields in which voice-specific parameters such as PIN and Language can be saved

General

Voice Mail Boxes

If this function is to be used, it must be activated

Voice user

Domino server, address book, fields: You also enter the *Domino server* and the *address book* in which the voice users are maintained. In an existing address book (e.g. *names.nsf*), the fields required for voice may have to be provided by a schema extension. The field identifiers are then assigned to the voice parameters on the Notes gateway. The assignment is possible via the *Fields* button. All other parameters represent options that optimally implement the Notes gateway in the customer's individual environment.

Voice message

Notification of

If the caller was connected to the voice box but did not leave a message or voice mail, the voice gateway can report this to the Notes user as a call without voice mail. This behavior is activated or deactivated centrally for all Notes users here.

Message Waiting

With telephone systems you can switch on *Message Waiting* for the telephones belonging to the voice box. The selection box can be used to decide when message waiting should be switched off again.

Email format

Voicemails that are delivered to the Notes user by the voice gateway consist of a subject line, the body of the message with additional information, and the audio file in which the message is saved. Two *e-mail formats* can be selected for this on the voice gateway: *German Standard* and *English Standard*. Alternatively, the voicemails can be created by the voice gateway in a different language, with different identifiers or with a completely different layout. The configuration required for this is carried out using the [...] button.

Set ‘read’ flags

The Voice-Gateway can *mark the messages heard over the phone as read* (subject to appropriate authorizations in the user mailbox). Since Notes only reconciles these markers after replicating again, the marker change may only be visible in the user mailbox after a longer period of time. If the query is made from the workplace telephone, the message may be deleted by the Notes user with the Notes client in the meantime, which may irritate the user concerned. This behavior can therefore be activated or deactivated centrally here.

Read out the phone number

Yes/No.

Call number - position

Select whether the caller’s phone number should be played before or after the message to be played.

Callback via remote inquiry

Is callback allowed when querying the message by telephone: Yes/No.

> Note!
> If this function is permitted, additional telephone costs may arise.

Advanced Settings...

The *Advanced Settings* button can be used to provide additional, non-standard information about the databases and fields used by the voice gateway.

- Address books

In addition to the information that is available to OfficeMaster about the call, the voice gateway can transport further information about the caller from any Notes address book to the Notes user with the voice mail.

The caller is identified using the *Calling Party Number* (call number signaled in ISDN), which is already displayed in the voicemails as the *From number*. This phone number must be assigned as an additional entry in the *Username* (*Full Name*) field of the caller’s person document stored in the Notes address book.

Use special database for caller information

By default, all address books accessible to the voice gateway are used, i.e. the local address book and the company-wide *name and address book* (*names.nsf*). Alternatively, the name and path of the caller database can be specified.

If a person document is found that contains the caller's _Called Party Number as an entry in *Full Name*, selected information from this person document is included in the voicemail as message text and as field content. Which information this is, with which prefix it is implemented in the message text and in which field of the voicemail it is written, is saved on the OfficeMaster Messaging Server in a text file in the voice tree. This text file is called *notesfields.txt* and is located in the directory %ProgramData\FFUMS\FMSRV\Data\voice\projectRecord\fvoice.

Each line to be added to the voicemail is maintained in the text file *notesfields.txt*. It consists of three string variables. Each string is delimited by quotation marks and separated from the following string with a comma. The last string of a record is delimited with a semicolon (;). Basically, a line has the structure: *"Text to be displayed","Field in person document","Field in voicemail"*.

Example:

If the caller's fax number stored in the person document is to be used in the voicemail, a line with the following content must be added to the *notesfields.txt* file:

_"Fax:","OfficeFAXPhoneNumber","FVOICE*OfficeFAXPhoneNumber";*

The content of *OfficeFAXPhoneNumber* along with the prefix *Fax:* is included in the message body and in the _FVOICE*OfficeFAXPhoneNumber* field of the voicemail.

If the message text of the Voicemail should contain a blank line for the sake of clarity, only one point is used as *Text to be displayed*. The other two string values remain empty in this case: *".","","";*

End of example

DID Field, PIN Field, Default PIN

As an alternative to the created user database, the PIN codes of the Notes users can be saved in a separate Notes database (*PIN DB*). The storage location and the name of the PIN database are required for this. In order for the voice connector to receive the correct PIN information, the PIN codes (*PIN field*) must be maintained in this database with reference to the corresponding voice box number (*DID field*). In addition, a *Standard PIN* can be stored, which is used if the Notes user has not yet been assigned a PIN. In order to prevent the set PIN codes from being read or even changed by unauthorized persons, only the Notes user ID of the voice connector

and that of the Notes user for access to the corresponding personal document or PIN document must be authorized. Of course, this also applies to the user database *fvoice.nsf*.

- Memo flags

Assuming the necessary authorizations, the voice server can play the messages from the selected user mailbox on the telephone together with the voice gateway. To distinguish whether the message has already been listened to or not, the *read* flag is used.

Mail; Fax; Voice; SMS

However, since this may not be a 100% satisfactory solution for Notes (see *Marking messages as read* above), the voice gateway can distinguish between messages that have already been heard and new messages in a separate field within the voicemail. This is marked in the *Read* field by *FREAD*.

In addition, the voice gateway must be able to differentiate between the message types during remote inquiry in order to e.g. to be able to listen to voicemails or e-mails via text-to-speech. This distinction is also made using flags, the existence of which allows the different message types to be clearly distinguished. The table below shows the flags used by default to identify the voice gateway.

Flags	**message type**
CopyTo	Received emails
FFAX	Faxes received with OfficeMaster
FSMS	Short messages (SMS) received with OfficeMaster
FVOICE	Voicemails received with OfficeMaster

Various

On the *Miscellaneous* tab, the voice connector can be configured for use with Domino servers running in the cluster and for use with encrypted user mailboxes.

- Decrypt for the following email addresses

If the user mailboxes of the Notes users are encrypted, access to the voicemails for the voice gateway is not possible. In order to still be able to listen to messages with the telephone, a key can be stored for the voice gateway with which it can decrypt the user mailboxes.

- Add one or more Domino server clusters

If several Domino servers are used together as a cluster, the voice gateway can be configured to a series of Domino servers with which it tries to connect in sequence if the current Domino

server fails. The user database *fvoice.nsf* must be found in the same directory structure on these Domino servers so that OfficeMaster can continue to operate smoothly.

Voicemail functionality test

First, the configuration must be adjusted for the *DirectSip* or *Omcums* connection on the *Routing (incoming)* tab. As a test, a rule can be set here that treats all calls as voice mail.

Table: Voicemail Test Rule

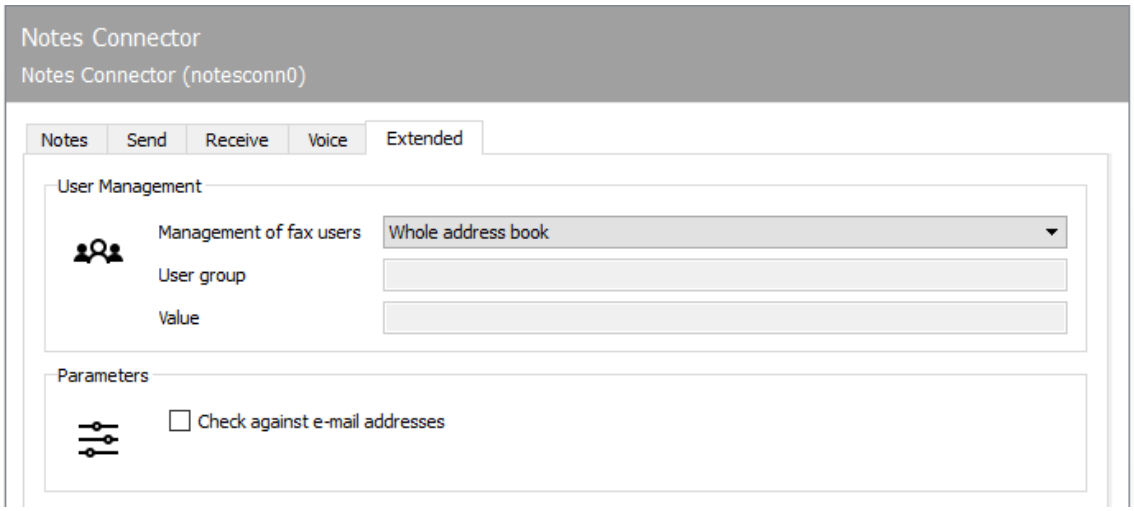
info item	Filters	service	voice server	Voice Connector
Called Party Number	.*	Voice	voice0	notesvoice0

This rule must be moved to the top of the list using the *Up* button.

> Note!
> The rule configuration described here causes all calls to be treated as voice mail as a test, which means that fax reception is not possible. Therefore *Routing (incoming)* has to be reconfigured for productive use.

A voice box must then be created. One of the phone numbers (*Called Party Number*) of the SIP or ISDN connection can be used as the voicebox number for the test. Now you call the voice box directly and leave a message of at least five seconds in length.

The recorded voice message is delivered to the user as a Notes mail in his Notes inbox, it can be opened here and if wanted, listened to over the loudspeaker. If a PIN is configured for the Notes user in the voice user database and OfficeMaster's *Notes-User-ID* has the appropriate authorizations, the message can also be queried remotely by telephone.



10.14.20. Extended

User management

Authorized Users

The Notes users who are allowed to work with OfficeMaster must be specified for the authorization check and license control. *Authorized users* includes every user of the specified *address book*. This setting only needs to be changed if:

- Only selected Notes users should send and receive faxes and short messages with OfficeMaster, or
- The number of users contained in the configured *address book* exceeds the number of licensed OfficeMaster users.

Group of people

As an alternative to the entire *address book*, the *authorized users* can also be combined in a Notes user group. In this case, the name of the user group must be specified.

Contents

As a further possibility of determining the authorized users, fields can be specified which must have either an arbitrary value or a defined value in the Notes user's person document, so that this can be recognized as authorized and used for license determination.

Parameters

Verification against email address

Checking the box will perform verification against the email address.

10.15. OLE converter

10.15.1. Above

If you would like to use ***Microsoft Office*** for the conversion instead of the standard conversion with ***LibreOffice***, we recommend using the specially designed converter, the OLE converter (*OLECONV*).

The OLE converter described below uses ***Microsoft Office*** for conversion. It can be used when *UAC (User Access Control)* is on.

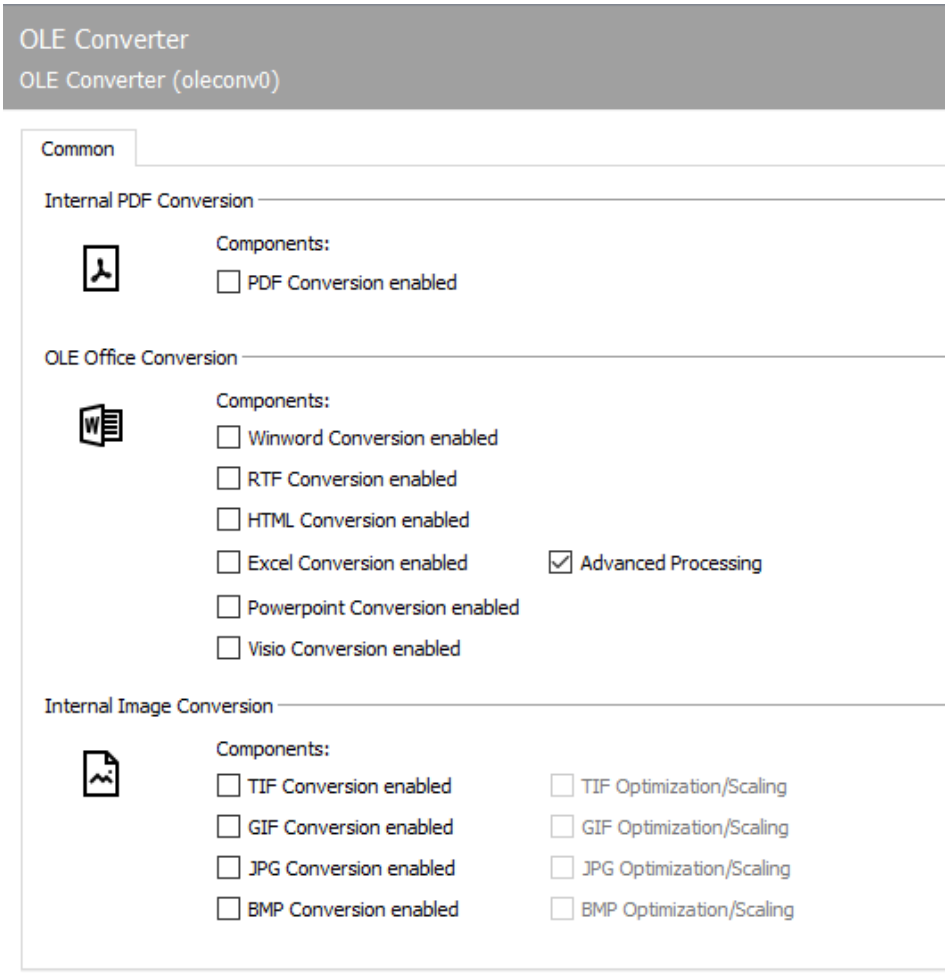
10.15.2. Overview

Creation of the OLE converter

In the quick launch bar of the Messaging Server Configuration call *"Converter > OLE Converter"* and then add a new component of this type via *"New OLE Converter Component..."*. The creation of this new component is accompanied by a wizard that asks for a service account.

> **Attention!**
> This service account must be a local administrator!

The subsequent naming dialogs correspond to the standard wizard and can be carried out accordingly. After successfully creating the OLE converter, the general configuration of the component is available.



10.15.3. General

Internal PDF conversion

Enable PDF conversion

If the OLE converter is to register itself for the conversion of the PDF document type, the corresponding check mark must be set here.

OLE Office conversion

The document types for which the converter should register are selected here. The document can only be converted into a graphic by the OLE converter if the registration is carried out for a document type.

Microsoft Word conversion

Activates the *OLE-CONV* for the conversion of the document type ***Microsoft Word***. After activation, please check whether another converter (e.g. *CMDCONV*) has taken over this function and deactivate it if necessary.

HTML conversion (web page format)

Activates the registration for the document type of the HTM/HTML format for the *OLE-CONV*. This format is often used by ***Microsoft Outlook*** to send emails! After activation, please check whether another converter (e.g. *CMDCONV*) has taken over this function and deactivate it if necessary.

RTF (Rich Text Format) Conversion

Activates the registration for the document type of the RTF format for the *OLE-CONV*. This format is often used by ***Microsoft Outlook*** to send emails! After activation, please check whether another converter (e.g. *CMDCONV*) has taken over this function and deactivate it if necessary.

Microsoft Excel conversion

Activates the *OLE-CONV* for the conversion of the document type ***Microsoft Excel***. After activation, please check whether another converter (e.g. *CMDCONV*) has taken over this function and deactivate it if necessary.

Advanced Excel controls

This feature enables advanced Excel control in case the ***Microsoft Excel*** conversion does not produce the desired result.

Microsoft Powerpoint conversion

Activates the *OLE-CONV* for the conversion of the document type ***Microsoft Powerpoint***. After activation, please check whether another converter (e.g. *CMDCONV*) has taken over this function and deactivate it if necessary.

Microsoft Visio conversion

Activates the *OLE-CONV* for the conversion of the document type ***Microsoft Visio***.

Internal image converter

If the OLE converter is also to be used for graphic formats, the corresponding format must be activated here.

TIF conversion

Enables registration for the TIF image type for conversion.

TIF fax optimization/scaling

This feature enables an optimized TIF control in case the TIF conversion does not produce the desired result.

GIF conversion

Enables registration for GIF image type for conversion.

GIF fax optimization/scaling

This feature enables an optimized GIF control in case the GIF conversion does not produce the desired result.

JPG conversion

Enables registration for image type JPG for conversion.

JPG fax optimization/scaling

This feature enables an optimized JPG control in case the JPG conversion does not produce the desired result.

BMP conversion

Enables registration for BMP image type for conversion.

BMP fax optimization/scaling

This feature enables optimized BMP control in case the BMP conversion does not produce the desired result.

Unregister the default converter for the desired formats

Call up the configuration of the command line converter to deactivate the (un)desired formats accordingly. Then restart both converters in order to obtain a correct job processing.

10.16. OfficeMaster Gate

The ISDN interface is controlled by the component *OMCUMS* (OfficeMaster Card Unified Messaging Service). For configuration, the *OfficeMaster Suite Configuration* is opened and then the menu sequence Edit > OfficeMaster Gate... is selected. In the dialog that appears, all ISDN cards, virtual cards and already added OfficeMaster Gate that were found by OMCUMS when starting are displayed on the left side under *Name*.

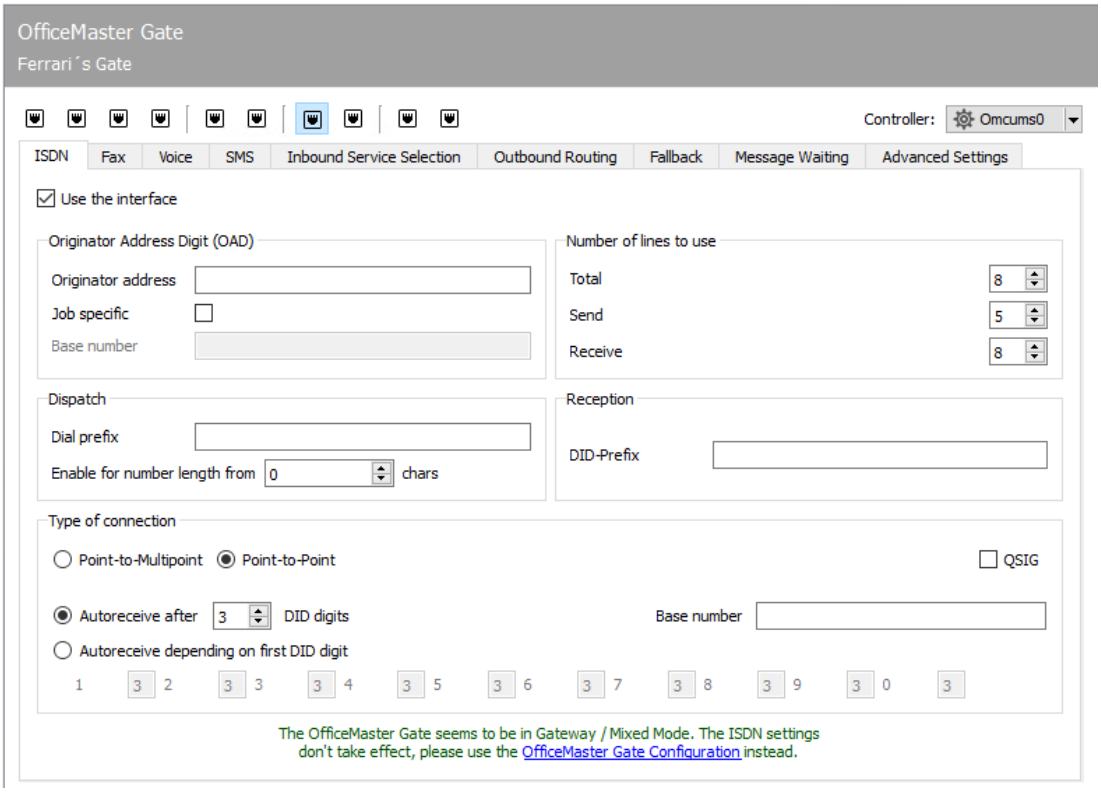
The respective controller to which the listed gates and cards are assigned is selected at the top right. In the case of *CAPI* cards or *XCAPI*, the *JCISDN* component is also required.

If OfficeMaster Gate is connected to the network, it can be added to the OfficeMaster Suite. The available ISDN hardware is displayed in the left dialog box. OfficeMaster Gate has the prefix *omg* followed by the serial number. CAPI cards found are marked with the prefix *capi*. If necessary, the hardware used can also be given a suitable name later. This is particularly useful for distributed installations. To do this, select the hardware and press *F2*. The configuration visible in the right dialog box always refers to the hardware selected on the left.

If the check box *Use ISDN interface* is activated, the tabs for the configuration are accessible. After completing the configuration, press *OK* to save the settings and apply them to the ongoing operation of OMCUMS.

Before starting the initial configuration, the OMCUMS component should be stopped and only started after the settings have been accepted.

> **Note!**
> The ISDN controller is still included in the OfficeMaster Suite 8 in order to simplify updates of existing installations. However, due to the ISDN switch-off, it is no longer possible to set up the ISDN controller again recommended. The DirectSIP component takes over the tasks of the ISDN controller.



10.16.1. ISDN

The information on the ISDN connection that applies to fax, landline SMS and voice is made on the *ISDN* index card.

Sender phone number (OAD)

Some telephone systems require an *Originator Address Digit* (*OAD*) from ISDN terminals for identification on the ISDN connection. This OAD is used by the telephone system when setting up a call for the authorization check and, if the telephone system is available, also for evaluating charges. If the telephone system does not require an OAD, no settings are required here.

Default number

Normally, the OAD corresponds to the telephone number of the ISDN connection. A *standard number* can be configured for all orders on the messaging server.

Depending on the order and base number

Optionally, the OAD can be determined depending on the order. To do this, e.g. the configured extension of the *Exchange*, *Notes* or *SAP* user can be included as an OAD in the send order. It is reported to the telephone system together with the configured base number when the call is set up. This means that every transmission process in the telephone system, regardless of whether it is a fax or SMS, can be assigned to an OAD or an Exchange, Notes or SAP user. If the send order does not contain an order-dependent OAD, the *standard number* is used as the OAD.

Number of channels to use

> Note!
> If the OfficeMaster Gate used is in “mixed” mode, it is important that the setting entered here for > the outgoing channels is not larger than those available on the OfficeMaster Gate!

In total

The *total* parameter is used to specify how many channels of the ISDN connection are to be used by the messaging server. Normally, all available channels, i.e. two per ISDN basic rate connection (*S0*) and 30 per ISDN primary rate connection (*S2M*), are used by the messaging server, provided the appropriate line licenses are available. Different information is required if the ISDN connection is also to be used permanently by other ISDN hardware that is not available to the system. Deviating information on license distribution may also make sense if e.g. only one channel is to be used on different ISDN connections.

Dispatch or receipt

For the best possible channel utilization, the number of channels for *send* and *receive* per ISDN connection can be configured. While transmissions wait for a free channel to become available, a few channels should be reserved for receptions.

> Example A:
> 2 lines licensed (through the base license). 1 ISDN basic connection with 2 channels in total, 1 channel for sending, 2 channels for receiving

2 channel licenses are required for the selected hardware. It may only be sent via one channel, but received via both. During the setting, a channel is blocked for reception, even with various outgoing messages.

Example B:
2 lines licensed (through the base license). 2 ISDN basic connections. BRI 1: 1 channel total, 1 channel transmission, 0 channels reception. BRI 2: 1 channel total, 0 channels transmission, 1 channel reception.

Receiving and sending should be done via different ISDN basic connections, the usage is so low that a total of 2 channels are sufficient for fax communication.

Shipment

Public line access

The number or the character with which an exchange line is fetched at this connection (usually *0*) is configured as the outside line access. In addition, the dial-in number of a telephone service provider can be set here, via which faxes and short messages are to be sent.

For phone numbers longer than

For automatic detection of internal fax extensions on the telephone system, configure the parameter “Phone numbers longer than” to the length of the longest internal telephone extension. As a result, fax transmissions to internal extensions are not sent via the central office. Regardless of the settings for outside line access, the implemented telephone number correction can be used to influence the telephone numbers for outgoing calls.

This is required, for example, for international installations with several locations, where the ISDN connections of a messaging server system are distributed across different countries.

Another application is the internal processing of mailings, although the entire phone number (including the area code) was specified as the recipient. The phone number correction is activated and configured on the *Advanced Settings* tab by selecting the country.

Reception

Extension prefix

The extension prefix is placed in front of the received phone number of every received fax, every received SMS and every incoming voice message. This makes it part of the received phone number for further processing. If you configure e.g. *0123* as *extension prefix*, the received phone number *456* is supplemented with it and the Exchange, Notes or SAP user must have the fax address *0123456*.

Connection type

Setting the type and parameters of the ISDN connection.

> Note!
> If the user interface indicates that OfficeMaster Gate is in “mixed” mode, the settings for the connection type no effect. These configurations must then be carried out on the OfficeMaster Gate via the OfficeMaster Gate Configuration program to be carried out.

Point-to-Multipoint; point to point

A distinction is made between point-to-multipoint and point-to-point as connection types. While several ISDN devices (telephone 1, telephone 2, fax) can be connected with point-to-multipoint, *point-to-point* only supports the connection of one ISDN device, which is normally a subordinate telephone system.

In addition, a point-to-multipoint connection only has a limited number of recipient telephone numbers (usually 3 to 10), so-called *Multiple Subscriber Numbers* (*MSN*), while a point-to-point connection has a complete range of numbers assigned. If more than 10 users are to be provided with a direct extension, the point-to-point connection is to be preferred. OfficeMaster Gate can be operated on both connection types.

QSIG

In addition to Euro-ISDN or *DSS1*, OfficeMaster Gate also supports *QSIG* as an ISDN protocol, which is used by some telephone systems for point-to-point connections. Which connection types are supported by third-party ISDN hardware can be found in the third-party hardware documentation. There you will also find information on further settings and the commissioning of this hardware.

Depending on the existing connection type, the receipt of faxes and short messages can now be configured.

MSN independent; MSN dependent

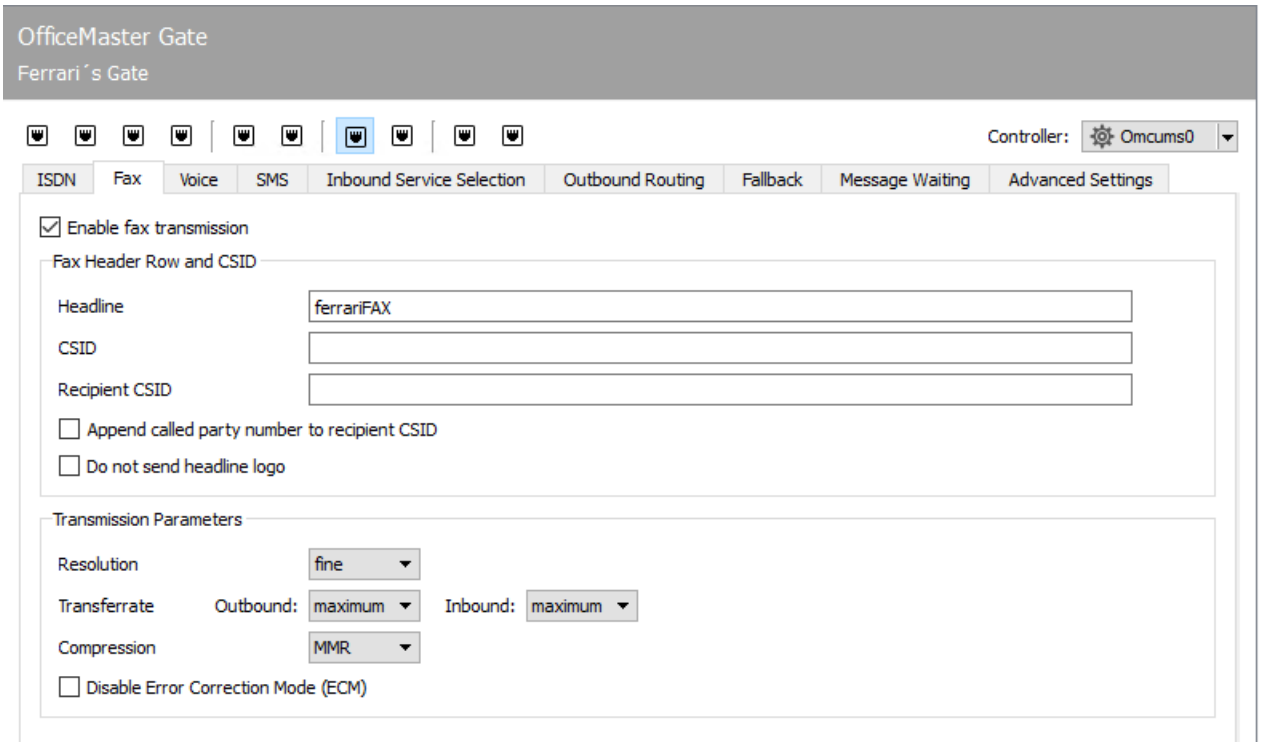
With a point-to-multipoint connection, reception can take place on all recipient phone numbers (*MSN independent*) available on the connection or only on selected recipient phone numbers (*MSN dependent*). The latter makes sense if additional end devices use this ISDN connection in addition to the ISDN hardware. In this case, the desired MSN is entered separated by a comma, semicolon or space.

Base number

With a point-to-point connection, the *base number*, which is reported by the telephone system before the extension, is configured (usually empty, except for the main connection). After receiving this base number, the reception of the direct dialing begins. The length of the extension to be expected is required for this before fax reception is started.

Receive after X extension digits; Reception depends on the first extension number

The length of the sequence of extension numbers can either be fixed with reception after X extension numbers for all extension numbers or dynamically set with reception dependent on the first extension number for individual extension number ranges.



10.16.2. Fax

The parameters for fax communication are specified on the *Fax* tab. Fax transmission can be activated/deactivated centrally for the ISDN connection here. Fax reception is deactivated on the *Service selection (incoming).* tab.

Fax Header and CSID (Fax Identifier)

Header / Fax ID

Header configures the default header text (e.g. company name) for outgoing faxes. This header text also contains the *fax identifier*. The *fax identifier* to be used is derived from the international number of the telephone connection, i.e. from the country code, area code and telephone number, in accordance with the ITU standard T.30. Only digits, plus signs and spaces may be used in the fax identifier. The area codes are to be entered without a leading zero.

> Example:
> The central fax address *03328/455-960* for Ferrari electronic AG in Germany is the fax code *+49 3328 455 960*.

In addition to the header text, the fax identifier is communicated with every fax transaction (incoming and outgoing) in the fax log and also appears on the display and in the transmission report of the remote station.

The standard parameters configured for the header and fax ID are only used for sending if no order-specific settings, e.g. the Exchange, Notes or SAP user.

Recipient CSID

Here you can specify the CSID shown during the transmission process on the remote fax device.

Append called party number to recipient CSID

If a different fax ID is to be communicated for the reception of the sending party, a special receiving ID can be configured. Optionally, the function “Append called party number to recipient CSID” can be activated. This has the effect that, i.e. when sending a fax to the number 348, the reception ID +49 3328 455 will be appended to it, the fax ID +49 3328 455 348 will be indicated in the sending confirmation for the sending party. If one or more number correction rules are configured, the correction of the incoming number will take place before the addition.

Do not send header logo

With *Do not send header logo*, the Ferrari electronic logo, which otherwise appears in the header of outgoing faxes, is suppressed.

Transmission parameters

Resolution

Choice between standard (100dpi) and fine (200dpi) resolution. A low resolution saves some transmission time at the expense of document quality.

Transmission rate Outgoing and incoming

The transmission speed for sending faxes can be limited for *Outgoing* and for receiving faxes for *Incoming*. In the event of transmission problems, e.g. due to poor telephone lines or remote stations, it can make sense to reduce the speed globally. In addition, the transmission speed can be specified in each order.

Compression

Image compression for fax transmission is either MH (Modified Huffman), MR (Modified Read/G3 Fax) or MMR (Modified Modified Read/G4 Fax). The latter is only available in connection with the ECM error correction mode. In the case of compatibility problems with remote stations which, for example, only implement MMR incorrectly, it can make sense to limit the image compression to even older methods.

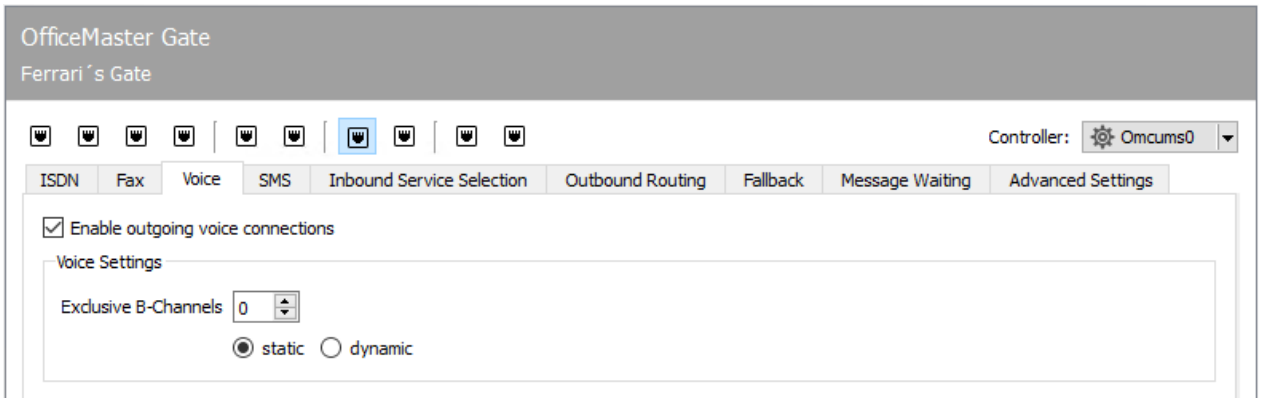
OMCUMS does not support NGDX and therefore no PDF transfer.

Enable Error Correction Mode (ECM).

The fax protocol has a transmission method in which modem transmission errors can be corrected. It always makes sense to enable this, with one exception: There are incompletely implemented T.38 fax gateways that do not support HDLC for the faster modem standards. If you use a telephone system with such limited T.38 functionality, you should switch off ECM.

Activate T.38 fax transmission

If the OfficeMaster Gate is connected via SIP trunk, it may (depending on the SIP trunk provider) also support T.38. This cannot be used on classic ISDN interfaces.



10.16.3. Voice

All hardware-related settings for Voicemail are configured on the *Voice* tab.

Allow outgoing voice connections

With *Allow outgoing voice connections* it is activated/deactivated whether the ISDN connection is allowed to set up telephone connections, e.g. is needed to play back a previously received voicemail on an internal or external telephone.

Exclusive B channels

In addition, *Exclusive B channels* can be used to specify the number of B channels or lines that are reserved for incoming and outgoing voice connections.

Although it is also possible to reserve voice connections for ISDN basic accesses with a maximum of two lines, this should not be done here because the aim is to separate fax and voice by using different ISDN basic accesses on this scale.

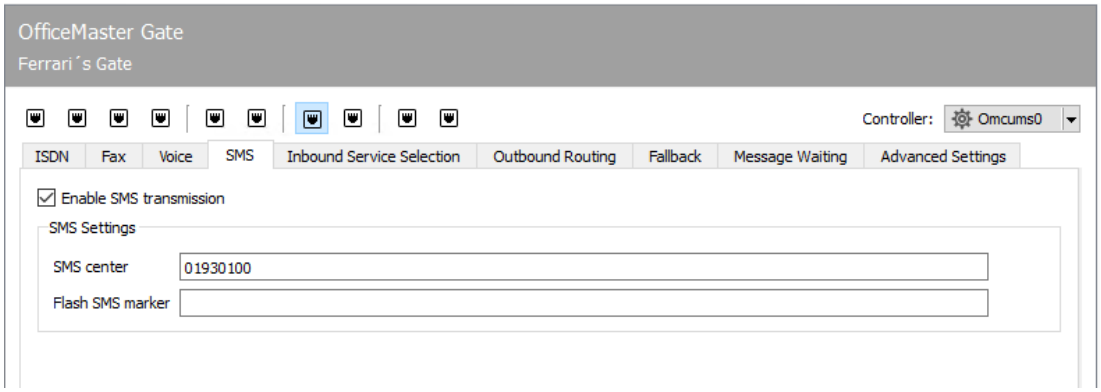
The reservation was implemented for the use of ISDN primary rate connections with 30 lines, on which faxes and voicemails are sent and received. Here it can happen that e.g. if there is a high volume of faxes, no more voicemails can be accepted or no telephone calls can be made via ISDN. As a result, the caller (in the case of voicemail) would feel the consequences of insufficient channel capacity directly, e.g. a busy signal is signaled.

Static; dynamic

Since voice connections have to be given priority, a certain number of the (30) licensed lines can be reserved for voicemail inbound. The reservation can be made *static* and *dynamic*. Static means that the configured number of channels is kept free for voice.

Example:
If, for example, *20* of *30* possible channels are *statically* reserved for voice, a maximum of a maximum of *10* channels are used for fax and fixed network SMS, although only *12* of the of the *20* voice connections are occupied. If *20* voice connections already exist no new voice connections are accepted (voicemail inbound) and the caller is signaled with a busy tone. In addition, no more voice connections are established although maybe *6* of *10* possible Fax/SMS Fax/SMS connections are free.

Example:
If, for example, *4* of *30* possible channels are *dynamically* reserved for voice, a maximum of *26* channels are used for fax and fixed network SMS if no channels are currently occupied with voice connections. If there are voice connections, however *4* additional lines are always reserved for possible future voice connections. If there are now 20 voice connections, only *6* lines are available for fax and fixed network SMS. If a maximum of *30* lines are available for voice connections no further calls (neither fax, SMS nor voice) can be accepted.



10.16.4. SMS

If the current telephone service provider offers the *Fixed-line SMS* service, OfficeMaster can also be used to send/receive short messages (SMS) over the fixed line. The settings for sending SMS via landline SMS are made on the *SMS* tab.

Note!
If an alternative SMS is to be sent via an Internet Service Provider, the corresponding settings must be made.

SMS center

In contrast to faxes, with landline SMS, communication does not take place directly between the sender and recipient, but via an SMS center operated by the network provider. Short messages are handed over to the SMS center for delivery or received by it. The ISDN hardware therefore does not communicate with the intended recipient of the SMS, but with the SMS center whose number is configured on the *SMS* index card. Short messages can be received in the fixed network in two different ways:

Call from the SMS center and receive the short message

Lure call from the SMS center (calling and hanging up), followed by the OfficeMaster Gate calling back and receiving the short message

Note!
Settings on the *Service selection (incoming)* index card are required for the first reception variant.

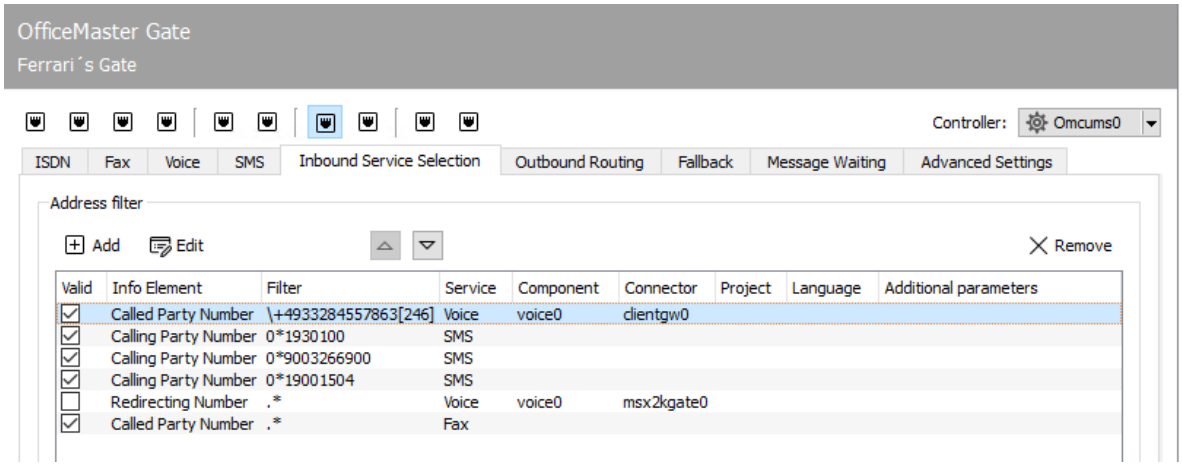
In Germany u. a. *T-Com* (*Deutsche Telekom AG*) the first variant. In order to be able to receive short messages in the fixed network, the phone number that is to receive messages from the SMS center must register once as a fixed network SMS-enabled subscriber. Otherwise, short messages to this phone number will not be sent by the SMS center as landline SMS, but read out via text-to-speech on the phone.

With *T-Com* this registration takes place via SMS to the number *8888*. If the SMS contains the text *ANMELD*, the sending phone number is activated to receive landline SMS.

This results in requirements for the ISDN configuration. If each user is to receive short messages, their SMS extension *depending on the order* must be sent to the telephone system as an OAD. The entire phone number must then be registered for landline SMS at the SMS center.

In Austria, *Telekom Austria* offers the variant of landline SMS as *HomeSMS*. HomeSMS is not supported on every ISDN connection. HomeSMS does not work with:

- ISDN basic connection with non-clip capable NT a/b
- ISDN multi-connector
- Serial connection, connection with direct dialing
- Apron facility
- Charge block
- Connections with phone number suppression set up (e.g. secret number)



10.16.5. Service selection (incoming)

Address filter

By creating rules in an address filter list, you can specify which service and thus which component is selected for specific phone numbers or phone number blocks. A filter expression is applied to a selectable ISDN information element and, if this is fulfilled, routed to the corresponding component.

Add to

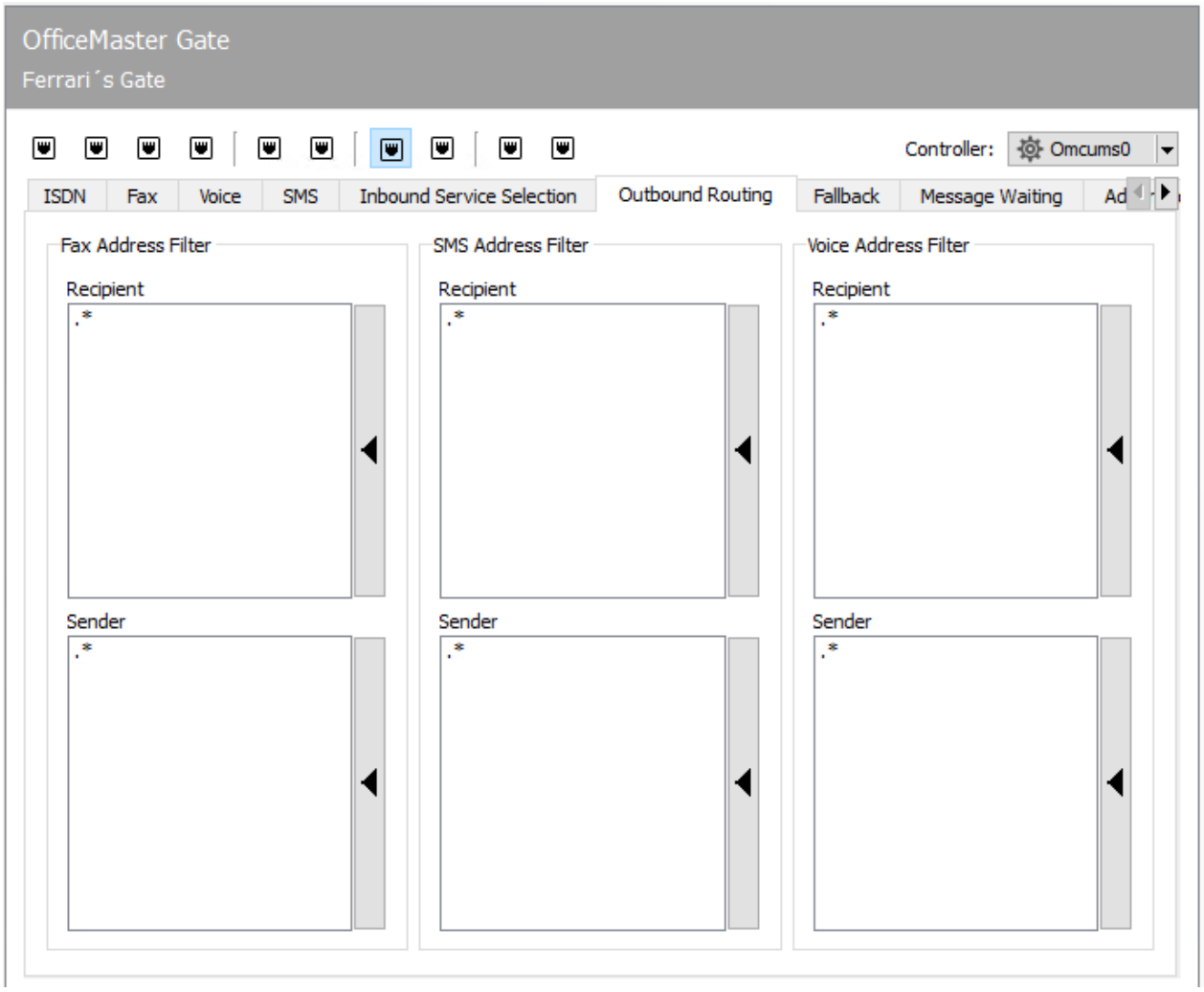
With *Add* a new rule can be created and added to the list.

To edit

An already existing rule can be edited with *Edit*.

Up or Down

This allows you to move the selected rule and thus change the order of the rules. This is relevant because the routing decision is made with the first applicable rule.



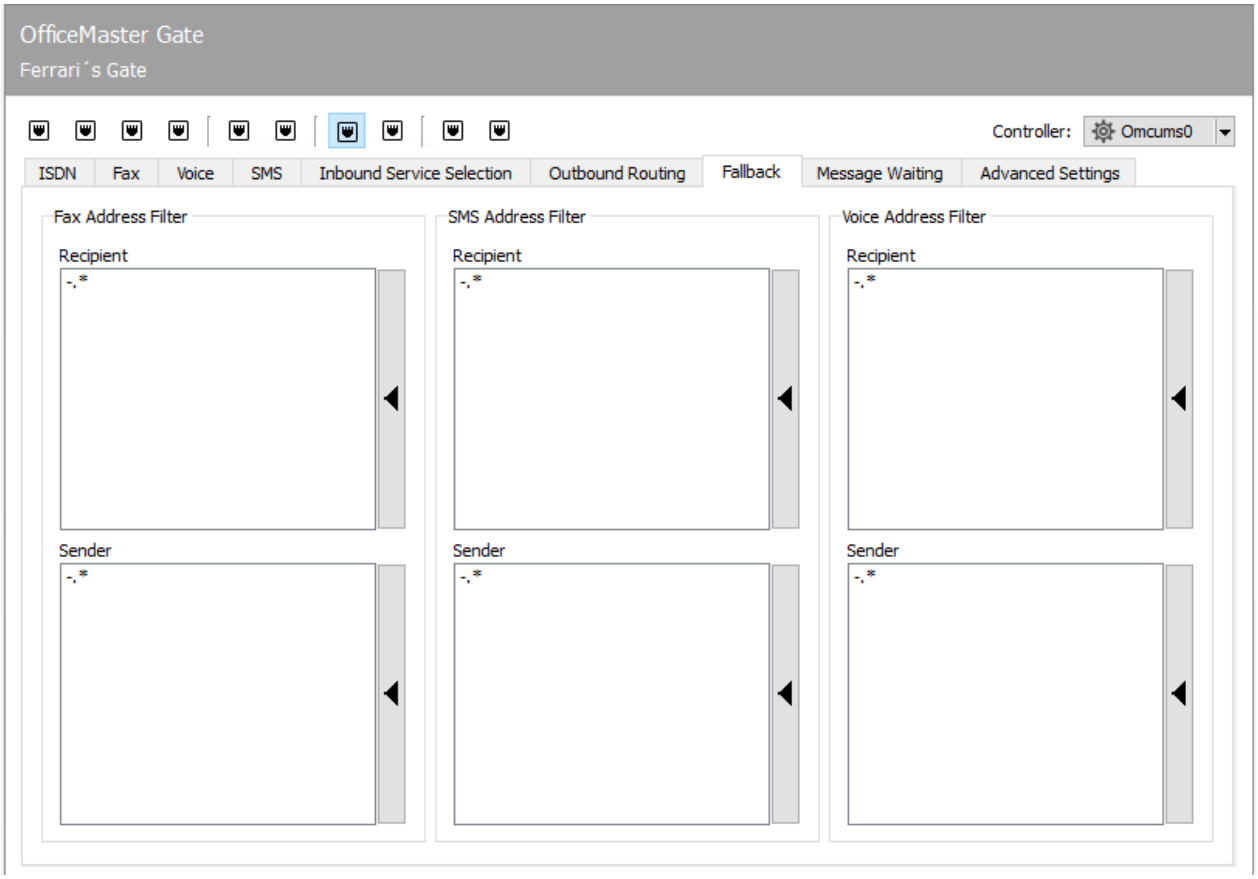
10.16.6. Routing (outgoing)

It can be specified for the four different service types (fax, SMS, voice mail and MWI/message waiting indication) whether the currently configured SIP component should be responsible to process the corresponding outgoing job. Regular expressions are specified for the destination phone number and sender number. In a match, the ISND\ port is the outbound routing target.

> **Note!**
> The setting for the outgoing routing for MWI is on the *Message Waiting* tab.

The expressions of all set up send components are used for the routing decision of a send job. This makes it possible, for example, to send specific orders to specific destination numbers on the appropriate ISDN connection.

Clicking on the right sidebar of a list allows entering a regular expression. Syntax examples are also given. The regular expression syntax is based on the PCRE2.



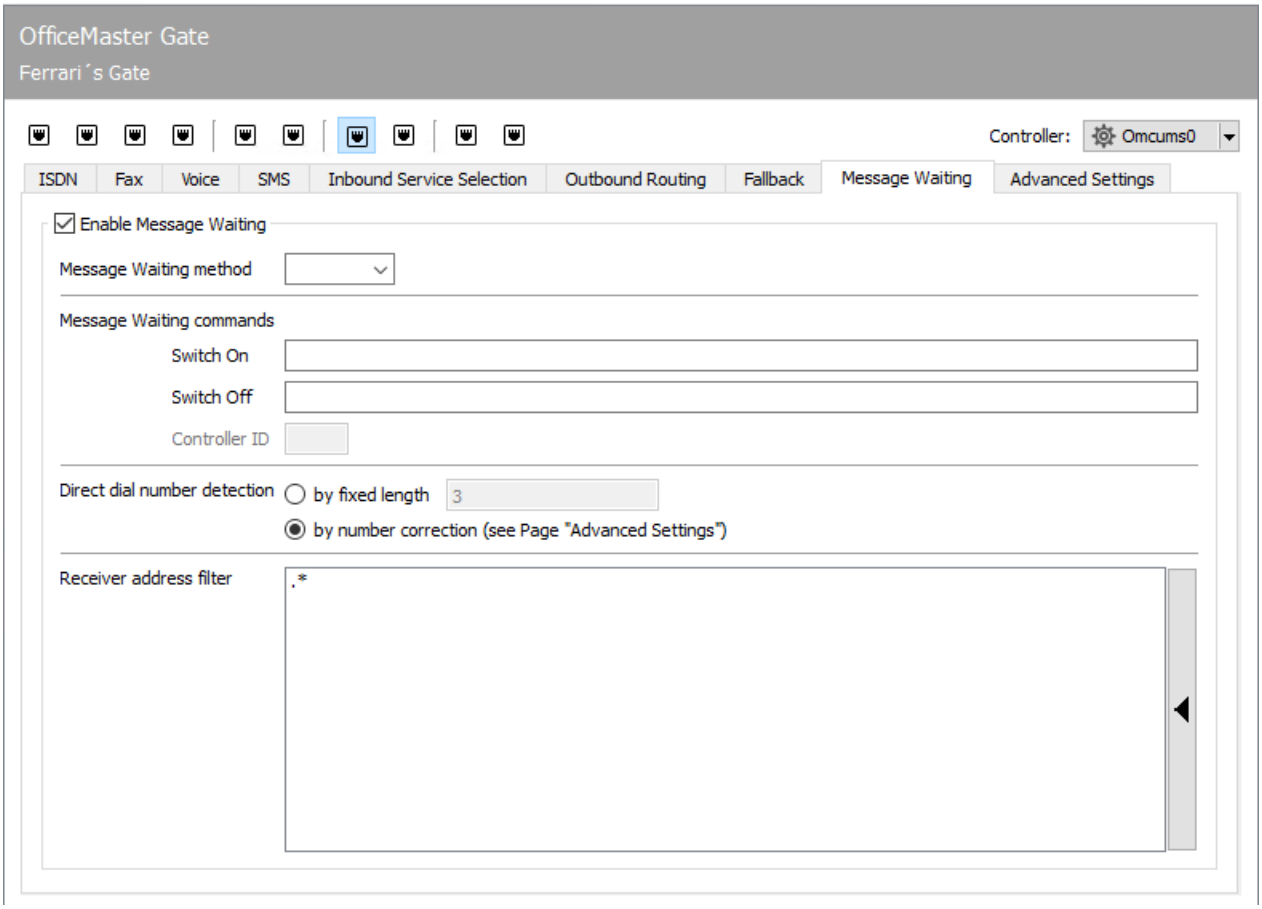
10.16.7. Fallback Routing

Fallback routing is used if a certain number of redial attempts did not lead to a successful transmission. To do this, fallback routing must be activated under Extras menu > System settings > General by ticking *Activate fallback mechanism*. Then, on the *Error processing* tab, you can set the number of redials for each error type (e.g. ISDN error > Send redial) that are carried out before the messaging server switches to fallback routing and thus possibly selects a different send component for the job. The actual set of rules is similar to routing (outgoing).

For the four different service types (fax, SMS, voice mail and MWI/message waiting indication) it can be specified whether the currently configured ISDN should be responsible to process the corresponding outgoing job. Regular expressions are specified for the destination phone number and sender number. In the case of a match, the ISDN controller is the outgoing routing target.

The expressions of all set up send components are used for the routing decision of a send job. This makes it possible, for example, to send specific orders to specific destination numbers on the appropriate ISDN connection.

Clicking on the right sidebar of a list allows entering a regular expression. Syntax examples are also given. The regular expression syntax is based on the PCRE2.



10.16.8. MessageWaiting

The Message Waiting Indication (MWI) feature allows an indicator to be activated on a telephone to notify the user that a voice message is available and can be retrieved.

Message waiting active

The check box for activating the message waiting function must be selected if the function is to be used.

Message waiting procedure

The method for signaling a message waiting for retrieval can be selected in the selection box. This depends on the respective telephone system.

- Message waiting control commands

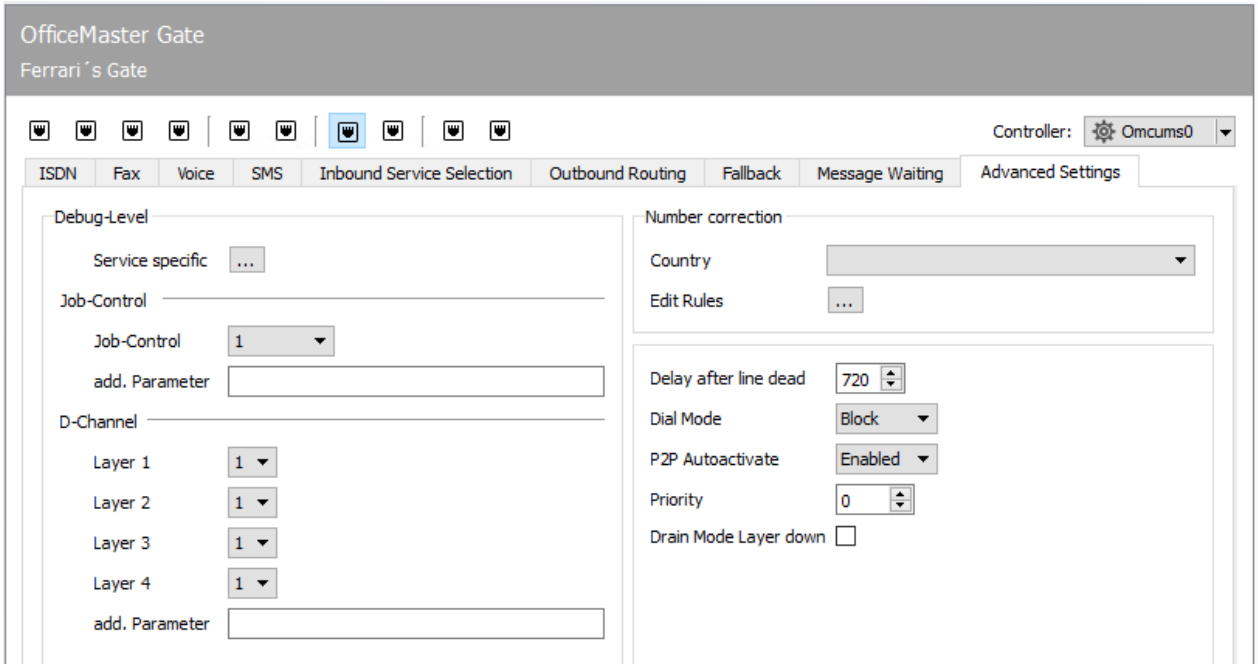
The control command for *switching on* or *switching off* the message waiting display can be entered in the text fields.

Determination of extension

In order for the telephone system to be able to influence the message waiting display on the correct telephone, the direct dialing of this extension is important. Either a fixed length (e.g. last 3 digits) is selected or a number manipulation is carried out to extract the extension from the phone number.

Recipient address filter

Regular expressions can be entered here, which are used to determine which message waiting jobs are to be sent on the currently configured ISDN connection. The same principles are applied here as for *Routing (outgoing)*.



10.16.9. Advanced settings

The options on the *Advanced Settings* tab are essentially intended for two use cases:

- for phone number correction, to correct and redirect wrong recipient phone numbers, as well as

- to set log levels that are requested by the hotline in the event of support cases.

Debug level

The log sensitivity can be set to different levels. Changes to the settings are only recommended after consultation with Ferrari electronic AG Support.

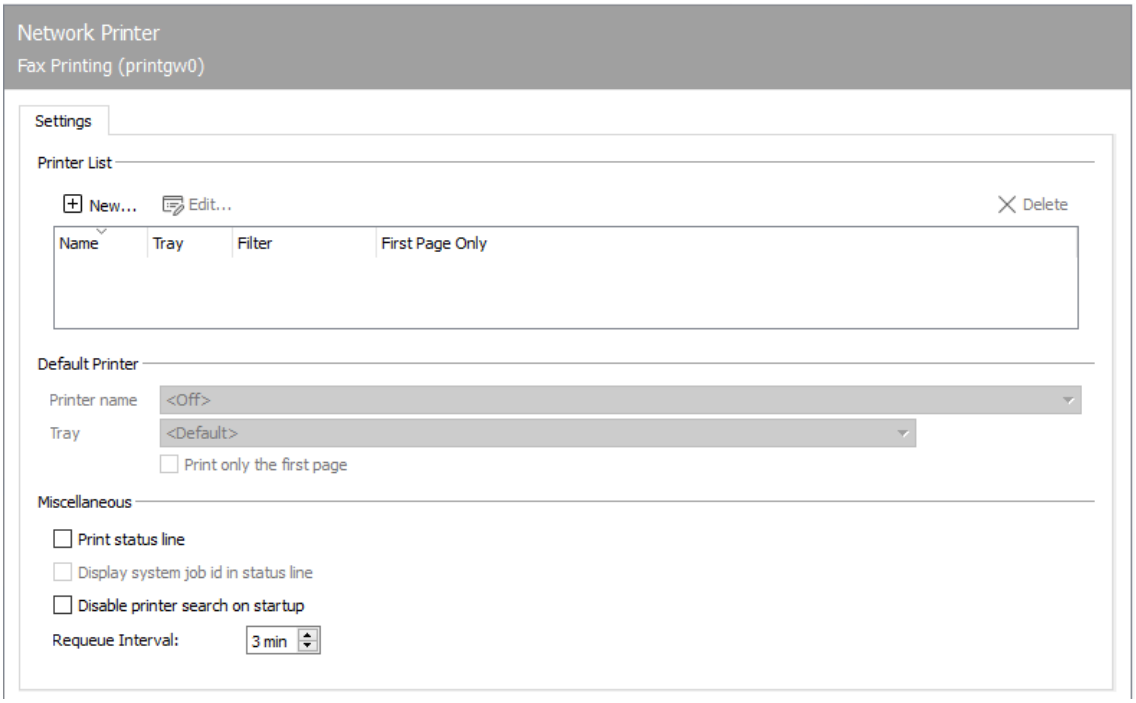
10.17. Network printer

In order to print received faxes automatically on network printers, the messaging server uses the PRINTGW component. The phone numbers will be assigned to the corresponding printer. Additionally the PRINTGW can be requested to print documents by other messaging server components such as MSX2KGATE, SAPCONN and Undeliverable (UNDLVRBL). The configuration is done via the quick launch bar under Print/OCR > Network printer First you have to create a new component and then you can configure it.

If received fax messages will be printed on multiple printers located in the company, descriptive names such as *printgwVertrieb* or *printgwFinance* can also be used if each PRINTGW is assigned to one printer.

New... > Edit > Remove

You can add a new printer, edit an existing one or delete it.



10.17.1. Settings

Printer list

Printer

If the PRINTGW is started in the component status of the OfficeMaster Suite configuration, it first searches for all printers available in the network (e.g. all in the Windows domain). One of these printers can then be assigned in the desired PRINTGW component. Alternatively, the printer name or IP-Adress can also be entered manually in the form *\SERVERNAME\PRINTERNAME*.

Paper tray

If the printer was found using the PRINTGW's printer search, the possible paper trays are also offered for selection.

Print only the first page

If desired, only the first page can be printed. This is usually sufficient for a status report.

Fax address filter

The fax address filter refers to the fax number (*Calling Party Number*) of the incoming faxes. The filter is stored as a list consisting of regular expressions. In the simplest case, a regular expression consists of the complete number.

Example

If faxes to the numbers *349*, *342* and *348* are to be printed automatically, enter these numbers in the list one after the other: *349 342 348* With the regular expression *34[928]* these three numbers can be configured in one line.

End of example

10.17.2. Default printer

Printer name

If the PRINTGW prints out sent faxes and the address filters do not allow assignment to one of the configured printers, this printer is selected for printing out the feedback messages.

Paper tray

The paper tray of the selected default printer is selected here.

Print only the first page

If desired, only the first page can be printed. This is usually sufficient for a status report.

10.17.3. Various

Print status line

The PRINTGW can print the most important information summarized in one line on each document.

Embed order ID in status line

When the printout of the status line is activated, the PRINTGW can add the job ID.

Prevent printer search on startup

In order to shorten the startup time and to minimalize the network traffic of the PRINTGW, the search for the printers can be deactivated with this option. In practice it is recommended to disable this option.

Interval for repetitions

The interval can be set here in order to reprint jobs in the event of unsuccessful printing.

10.18. Connector for SAP

The connection to SAP takes place via the SAPconnect interface.

- SAPconnect has been delivered in R/3 Basis since R/3 version 3.1G and is based on *Remote Function Calls (RFC)*.
- Since R/3 version 4.7 with *Web Application Server (WAS)* version 6.10, SAPconnect can alternatively be operated on the basis of *Simple Mail Transfer Protocol (SMTP)*.

The concept behind SAPconnect is independent of RFC and SMTP. The individual SAP applications (MM, SD, FI, CO) create send requests that are transferred from SAPconnect to OfficeMaster via RFC or SMTP. After OfficeMaster has processed the send request, the final send status is also reported back to R/3 via RFC or SMTP. In order to be able to operate the two SAPconnect technologies, OfficeMaster includes the RFC connector SAPCONN, SAPCONNU, SAPCONNW and the SMTP gateway SAPSMTP.

SAPconnect can be connected in two ways:

- With RFC
- Via SMTP

Both RFC and SMTP support the sending of documents by fax, SMS and e-mail, but the RFC variant offers a larger range of functions and better integration than the SMTP variant.

The status and trace function of the RFC variant allows the system status of the messaging server and detailed log files to be viewed in the SAPconnect administration, which is not possible with SMTP due to the concept.

Various settings are required for commissioning, both in the R/3 system and in the messaging server. The required settings and the recommended sequence can be found in the table below.

Configuration step	**RFC connector(SAPCONN)**	**RFC connector(SAPCONNU)**	**RFC connector(SAPCONNW)**	**SMTP Connector(SAPSMTP**
Set up CPIC users	X	X	X	-
Setting up SAPconnect via RFC	X	X	X	-
Creating and configuring	X	X	X	-

Configuration step	RFC connector(SAPCONN)	RFC connector(SAPCONNU)	RFC connector(SAPCONNW)	SMTP Connector(SAPSMTP
RFC connectors				
Setting up SAPconnect via SMTP	-	-	-	X
Creating and configuring SAPSMTP gateways	-	-	-	X
Set up mail receiving and sending	optional (only for email)	optional (only for email)	optional (only for email)	X
User Management	X	X	X	X
Schedule messaging	X	X	X	X
Test message with SAP Business Workplace	X	X	X	X

10.18.1. Set up SAPconnect via RFC

Depending on the SAPconnect connection via RFC or SMTP, SAP must be configured to use a SAPconnect node for fax, SMS and e-mail. This is used to reach either OfficeMaster's RFC connector (SAPCONN, SAPCONNU, SAPCONNW) or OfficeMaster's SMTP gateway (SAPSMTP).

> **Note!**
> Further information on the SAPconnect configuration can be found in SAP Note 17194 Telefax in various SAP releases.

OfficeMaster's SAPCONN connector must be set up in each client of an SAP system. In R/3, it represents a SAPconnect node to which the document to be sent with the associated recipient list is transferred via RFC. For the sake of clarity, the necessary "customizing" for SAP ECC 6 is described in this chapter.

A **CPIC** user is required to operate the RFC connector, the configuration of which is described in the following section.

Create CPIC / system user

Transaction: SU01

The RFC-SAPCONN connector requires a CPIC user account under which it can log on to R/3 and transmit status messages and received documents. This user account is created in the R/3 user administration SU01 as follows:

The user account, such as B. _FERRARI*CPIC*, is specified and confirmed with *Anlegen* in the toolbar. The _last*name* of the user can be chosen arbitrarily, e.g. **OfficeMaster**.

Logon data tab

Password: A password for the user is assigned here. The assigned password will later be assigned to the SAPCONNConnector.

User type: The *User type* is changed to **System** or **CPIC**.

Authorization profile S_A.SCON: With _authorization profile S*A.SCON* the required rights are given to the user account on the index card *Profile*.

Now the user account is secured. If there is already a user account with the above settings, it can be shared. Several connectors of a client can also share a CPIC user account.

RFC communication

The SAPconnect interface between R/3 and communication systems uses RFC connections for data exchange. Remote Function Call (*RFC*) is the SAP implementation of the Remote Procedure Call (*RPC*) concept. This concept describes the execution of subprograms on remote computers including the transfer of parameters and return values.

An RFC connection always has two sides. On the one hand, the RFC server offers the execution of functions for other processes. On the other hand, the RFC client calls these functions. Since an RFC connection consists of a server and a client, function calls can only be made in one direction. Therefore, two RFC connections are required for communication between R/3 and communication systems.

- The first RFC connection transfers the data to be sent from R/3 to the communication system. Here the R/3 system is the RFC client and calls functions of the communication system, which the RFC server represents.
- The second RFC connection returns feedback about the success of the communication. It transports received messages from the communication system to the R/3 System. As an RFC client, the communication system calls functions in the R/3 system, which is the RFC server here.

These two directions of communication are considered separately below.

From R/3 to the communication system

A communication system is represented in the R/3 database by a SAPconnect node. A so-called RFC destination is assigned to this node. The attributes of this RFC destination are the information that R/3 needs to set up an RFC connection to a communication system. RFC destinations can be viewed and edited using transaction *SM59*.

If you start transaction *SM59*, you will find a large number of RFC destinations of different types. If an RFC destination is to be used for the SAPconnect interface, it must be of the *TCP/IP* type. This type is available in variants

- *Start*: When executing an RFC, R/3 starts an external program and waits for it to end.
- *Registration*: must be selected for SAPconnect. An external program registers with R/3 and waits for remote function calls.

Such RFC destinations have three attributes:

- Gateway host
- Gateway service
- Program ID

Example:
Gateway here is an R/3 process that handles communication with an external component. Gateway host is the network name or TCP/IP address of the R/3 application server through which communication is to run. Gateway service is the TCP/IP port to be used for this communication. Here you can either enter the port number directly (***3300-3399***) or the name defined by SAP (***sapgw00-sapgw99***). Usually the last two digits of the gateway service correspond to the system number of the R/3 system. Finally, the program ID is a unique name that is used to distinguish between different RFC partners that register on the same application server at the same port.

These three parameters are also sufficient for the other side of the RFC connection (*SAPCONN*-Connector from OfficeMaster) to register with the SAP gateway. It must be ensured that the network and port names are also known on the computer on which the *SAPCONN* connector is running. If you have configured the same gateway host, gateway service and program ID on the R/3 and *SAPCONN* side and started the *SAPCONN* connector, it is already possible to transfer fax jobs from the R/3 system to *SAPCONN*.

In transaction **SM59** you can check the existence of this RFC connection with the function *test connection*. Alternatively, each registered system can be displayed via the menu sequence Go to > Registered Systems in the Gateway Monitor (transaction **SMGW**).

From the communication system to the R/3

In the opposite direction of communication, OfficeMaster transfers information to the R/3 system. The network name of the application server and the system or instance number of the system for which the message is intended are required to establish the connection. Normally, the application server here is the same computer that was specified as the gateway host for the RFC connection from the R/3 system to the communication system. Since exceptions are possible, both computer names can be configured separately in the configuration of the *SAPCONN* connector.

If status messages for fax jobs or received faxes are to be transferred to the R/3 System, data in the R/3 System must be changed. This requires rights that can only be assigned to users. The communication system must identify itself as an R/3 user. To do this, a so-called CPIC or RFC user is created in R/3 with the rights required by the communication system. The communication system must transfer the logon data of this user to the R/3 system with every communication. The login data includes the name and password of the CPIC user and the name of the client for which the CPIC user was created.

Configuration Files

It may happen that the TCP/IP configuration of the computer on which the *SAPCONN* connector is running needs to be adjusted. This is done by editing the hosts file and the services file.

The hosts file contains a mapping of names to TCP/IP addresses. On Windows, it is located in the %systemroot% \system32\drivers\etc directory and is named *hosts*. So if the name of the R/3 server cannot be resolved on the machine running the *SAPCONN* connector, a line with the name and IP address of the R/3 server is added to the hosts file.

The Services file contains a mapping of names to TCP/IP ports. It is located in the %systemroot%\system32\drivers\etc directory (on Windows) and is named *services*. If you use names of the form *sapgwXX* instead of port numbers *33XX* in the _SAPCONN_Connector configuration, add a line with the name and port number to the services file for each name used. These settings are made automatically by installing a SAPgui.

Create RFC destination

Transaction: SCOT or SM59

The *SAPCONN* connector of the messaging server is represented in R/3 as a SAPconnect node. An RFC destination is assigned to this node, to which the requests are sent after conversion. The RFC destination can also be created during the installation of the node.

You can maintain the RFC destination with transaction *SM59* or with the node assistant of the SAPconnect administration. An RFC destination is created with *Create* in the toolbar.

RFC destination: Maintaining the RFC destinations involves system-wide settings. Since the RFC destination will later be linked to client-related settings of the SAPconnect node, a name with client number (e.g. _fercon*100* for SAPCONN connector for *client 100*) should be selected.

Connection type: The connection is made via TCP/IP, select **T** for this.

Activation type: The activation type must be set to “Registered server program”. Depending on the selection, the associated program ID can then be entered. To ensure clarity, the name of the destination (in the example: _fercon*100*) can be used (capital - & note lower case!).

Gateway options: The host name of the R/3 server is entered under Gateway host. The gateway service is the TCP port that SAPconnect uses to set up the RFC call to the SAPCONN connector. Enter **sapgwXX** here, where **XX** stands for the two-digit system or instance number of the R/3 system (e.g. *sapgw00*). Finally, the RFC destination is saved.

Create SAPconnect node

Transaction: SCOT, Menu: View > Node

Each SAPconnect node in SAP is created with the help of an R/3 wizard. In the *SCOT* transaction under the menu item View > Node, select the *Create Node* button from the toolbar.

First you will be prompted to enter the node name (e.g. *FERCON*) with description and the node type.

In order for the RFC node to transfer send requests to the SAPCONN connector via RFC, it needs an RFC destination. This can be entered in the subsequent dialog. It is created with the *RFC Destination* button. Then select the RFC destination and click *Next*.

Fax with SAPconnect via RFC

The creation of a node of the address type *Fax* is described below. The descriptions for *Internet-Mail* and *SMS* follow afterwards.

Address range:

In the next dialog, a fax address range for this node is specified so that outgoing fax messages are routed to it. This routing can be set using the recipient fax number. To set up only one SAPconnect node or SAPCONN connector, “*” is entered in the address area.

If there are several SAPCONN connectors (and thus several nodes), the address ranges for the individual nodes are divided (e.g. **CH*** for the node _FAX*Z* or **DE 030*** for the node _FAX*B*).

Document formats: In the next step, the document formats that can be processed by the messaging server are specified. The following document formats are possible for fax communication with SAP: *PCL* or *PS* (mutually exclusive), PDF, RAW and TIF (for forwarded faxes).

> **Note!**
> The converter component of the messaging server must be configured accordingly. If *PS* is used as the file format, *Ghostscript* must be installed as the conversion software.

The *PCL* and *TIF* formats are preferred, since the internal PCL converter can be used for them.

Documents in the R/3 internal document format (such as *ALI*, *SCR*) are converted to PCL or PS format in the R/3 spool. Depending on the previously configured document format, the printer driver *HPLJ5* (for PCL) or *POST2* (for PS) is specified as the device type. Optionally, the transmission times for the three different priority levels can be specified in the following dialog.

Configuration of the location: This is followed by the configuration of the location. The country code (e.g. *DE*) indicates the location of the OfficeMaster Messaging Server. This input is required for controlling the country code of the fax numbers (like *+49*).

After clicking on *Next* you can either add further address types (Internet mail and SMS) to the node or exit the configuration wizard.

If no further address types are to be added, settings for all address areas of the node can be made by selecting *No* in the following dialog.

Maximum waiting time for resend attempts: The interval for resend attempts (see Figure 10.10) is entered as the first setting for the entire node if an RFC error occurs during the transfer from R/3 to SAPCONN.

Node can resolve path references / node should be monitored by the alert monitor: The checkboxes *Node can resolve path references* and *Node should be monitored by the alert monitor* should not be checked.

Node is operational: Finally, the *Node is operational* check box is checked.

Result:

The SAPconnect node *FERCON* was set up for the *SAPCONN* connector. The node can be reconfigured if necessary.

Internet mail with SAPconnect via RFC

Equivalent to fax, a (further) address range is created for the node for sending Internet e-mails. The dialogs are adjusted accordingly. If only this SAPconnect node with Internet mail functionality is to be specified in the R/3 client, the entry * (asterisk) in the address area is sufficient.

The transmission of e-mails is usually not limited to any specific document format. Therefore, all document formats are generally supported.

If orders and lists in the *OTF*, *SCR*, *ALI* and *INT* formats are to be converted into externally understandable formats beforehand using SAPconnect, these formats should be excluded. To do this, select the option *All formats except the following* and add the above formats to the list by clicking the *SAP internal formats* button. In addition, the formats PCL and PS should be excluded from mailing.

The previous step presumably converts all internal SAP formats to PDF or HTM, depending on the conversion rules set. Thus, no device type is required.

All the settings required for e-mail have now been made. If desired, paging / SMS can be configured. Otherwise *No* is selected.

Paging/SMS with SAPconnect via RFC

Since R/3 Version 4.5, SAPconnect has supported the sending and receiving of short messages/ SMS. A prerequisite is a configured SMS communication interface on the OfficeMaster Messaging Server. Under these conditions, *Pager* (=SMS) is selected as the address type.

When configuring the address range for this node, the short messages are routed to the node. If only this SAPconnect node is to be addressed with SMS functionality, * is entered in the address area. Pager subtypes such as *E+.** or *02:017** can be specified for a more precise specification.

RAW data (ASCII) are supported for the transmission of short messages. In order to convert the R/3 internal data (e.g. SCR) into RAW, ASCIIPRT is required as the device type.

Configure SAPconnect node (optional)

Since SAP 4.7, external formats must be set for the four internal SAP formats, depending on the service. There is no need to configure conversion rules, output devices or supported document formats. The following table provides an overview of the recommended target formats.

SAP internal formats	**Fax**	**SMS/Pager**	**Internet Mail**
SAPscript / Smart Forms	PCL or PS	TXT	PDF
ABAP list	PCL or PS	TXT	HTM
Business Object / Reference	TXT	TXT	HTM
RAW Text	TXT	TXT	TXT

10.18.2. RFC connector (SAPCONN)

The connection of an R/3 system to the messaging server takes place via the gateway component SAPCONN with a non-Unicode connection. At least one gateway component must be

created, configured and operated as a connector for each SAP client. To do this, select in the quick launch bar > SAP > RFC in the messaging server configuration.

All created connectors are displayed on the left side. The selected SAPCONN connector can be configured on the right side. If no connector is displayed, the corresponding SAPCONN connectors must be created using the *Add* button.

Create RFC connector

A new component of type SAPCONN is created for the messaging server. A SAPCONN connector is set up for each SAP client or for each SAPconnect node.

Since the connectors are numbered consecutively by name, it is advisable to use descriptive display names in order to simplify administration later. For example, the SAP system abbreviation and the SAP client number can be used in the display name, resulting in names like *SAP DEV 100*. Once the component has been created, it can be configured.

Test sending faxes via SAP GUI

R/3 user administration

Transaction: SU01 or SU51

R/3 users should be assigned fax numbers, radio numbers and e-mail addresses in the R/3 user master for the following reasons:

- Only users with a sender address in the desired communication type are allowed to send messages in this way, i.e. only users with a fax number are allowed to fax.
- The maintained sender number or e-mail address is also communicated to the recipient as the sender address.
- Received faxes, short messages and e-mails are assigned via the phone numbers or e-mail addresses maintained in the R/3 user master.
- In the log files of the SAPCONN connector, the operations of a specific R/3 user are identified by their sender address in the R/3 user master.

Of course, the fax number can also be maintained in transaction SU51 (System > User settings > User address).

Messaging

Transaction: SCOT, in the menu sequence View > Jobs

The R/3 internal program *RSCONN01* is responsible for transferring the messages from R/3 to OfficeMaster via RFC. In order for this to happen, a job is scheduled that starts the program every 10-15 minutes. Depending on how sensitively communication is handled in a company, the interval for program execution should be selected. It should not be less than 5 minutes.

The process is activated with *Schedule sending process* in the toolbar of the SAPconnect administration and the input of a name for the job is expected.

Then the variant *FAX* is selected with the cursor and confirmed with *Schedule*.

The time interval for the program starts of *RSCONN01* can be entered via *Schedule periodically*. The first start date is generally one hour in the future. After saving these settings, the job is scheduled.

The procedure is analogous with Internet mail and pagers / SMS.

To test the configuration, the transmission of faxes, short messages and e-mails can also be started manually and not job-controlled. This is also possible in the SAPconnect administration. The *Start send process* button is available for this. *FAX*, *Pager*, *INT* or "*" is selected as the address type. Alternatively, the transfer program (*RSCONN01*) can be started in transaction *SE38*.

> **Note!**
> Another very useful R/3 program is *RSCONN05*. It allows faxes with errors to be resent without having to recreate the documents using the R/3 applications (such as MM, SD, etc.). This program can be accessed via transaction *SOST* or the menu sequence Utilities > Overview of send requests. More information is available in SAP note number *92287*.

Test message with SAP Business Workplace

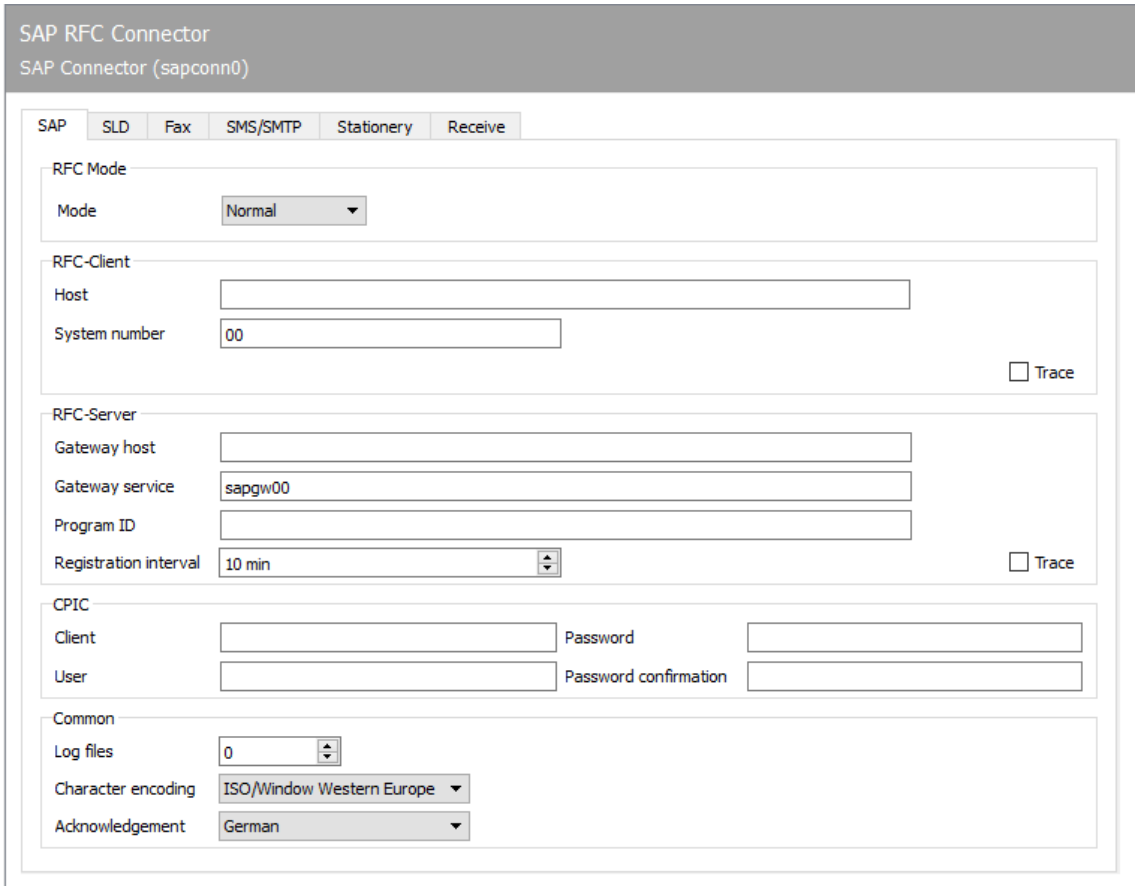
In order to send a test message from SAP, both the messaging server and the connectors must be started. You log on to R/3 with the *SAPgui*. A new message is now created in the Business Workplace (transaction *SBWP*). The recipient number must be entered in the syntax *<country code> number* (e.g. ***DE 0123456***, ***US 555-$^{456}/_{89}$***), which is automatically generated by the R/3 recognized as a fax number.

With the _Send_button from the toolbar, the document is saved as a send order in the office outbox. Here it waits for the ABAP program *RSCONN01* to transmit it to the connector. The current transmission status of the document can be read at any time on the *Recipient list* tab in the office exit. This tab is associated with the message.

The status of other SAP documents, such as B. Orders. The SAP applications use the Business Workplace as a transport medium and therefore store the fax jobs in the office outbox. A document has the following status messages in the course of sending:

R/3 release	Version 6.x
Before RSCONN01	Waiting
After RSCONN01 and before completion of sending by the fax server	Message passed from node ... to communication system
After successful completion of sending by the fax server	Delivery to ...
After the fax server failed to complete the transmission	No extradition

If the document cannot be sent, the R/3 sender also receives an express document, which draws his attention to this fact.



10.18.3. SAP

The first configuration steps for the *SAPCONN* component relate to the direct connection to the SAP system and are carried out on the *SAP* tab.

RFC mode

The type of RFC connection is determined in the *RFC mode* area. The choice made here changes the input options of the tab:

Mode

*normal
In RFC mode *Normal*, both the RFC server and the RFC client connection take place without load balancing. This is the standard case, i. H. this setting applies to most of the installation.

- Load balancing
  In *RFC mode load balancing*, the RFC client connection is subject to load balancing. Since this setting only affects incoming messages and status messages, this option only makes sense for a very small number of installations.

*RFC-INI
The *RFC mode RFC INI* is only intended for experts who want to manually describe the RFC connection in the configuration file *saprfc.ini*.

> Note!
> For most installations, *Normal* is sufficient as the RFC mode.

RFC client

In this area, information about the RFC inbound connection from *SAPCONN* to the R/3 system is made (depending on the *RFC mode*).

Host, system number *(normal in RFC mode)*

With RFC mode *Normal*, the TCP/IP address or the resolved name of the R/3 application server must be entered as *Host*. The two-digit system or instance number of the R/3 system is required as the *system number*. This number can e.g. read in the SAPlogon program.

Host, name, group (in RFC mode *load balancing*)

In the RFC mode *Load Balancing* the TCP/IP address or the resolved name of the R/3 application server that provides the load balancing must be entered as *Host*.

name is the name of the R/3 system and *group* is the name of the group of R/3 application servers with load balancing. If such systems are available, you can also find this information in the SAPlogon program of the SAPgui.

RFC section (in RFC mode *RFC INI*)

The section in *saprfc.ini* that describes the RFC connection to the R/3 System is specified (note the use of upper and lower case!).

Trace (all modes)

Regardless of the RFC mode, the RFC trace can be activated/deactivated with *Client-Trace*. The trace files are stored in the work directory of the SAPCONN connector. The work directory is in %ProgramFiles%\FFUMS\FMSRV\work\SAPCONN.

RFC server

Here the RFC outbound connection from the R/3 system to *SAPCONN* is configured. This information must be the same as the information in R/3, and must therefore be configured later in R/3 for the RFC destination (SM59).

Gateway host, gateway service (in RFC mode *normal* and *load balancing*)

The TCP/IP address or the resolved name of the R/3 application server (normal RFC mode) or the computer on which the SAP gateway is running (load balancing) must be specified as *Gateway host*. The resolved TCP/IP port over which the RFC connection is to run is specified under *Gateway service*. The gateway service name (e.g. *sapgw00*, *sapgw01*) may need to be resolved on the server in the *services* file.

Program ID (in RFC mode *normal* and load balancing)

A unique name is configured as the *program ID* under which SAPCONN registers in R/3. R/3 uses this program ID to find the *SAPCONN* connector. For this purpose, the same program ID is stored in R/3 in the RFC destination assigned to the SAPconnect node (Note: upper and lower case letters!).

RFC section (in RFC mode *RFC-INI*)

In RFC mode *RFC INI*, the section in *saprfc.ini* that describes the connection from the R/3 system to SAPCONN must be specified as *RFC-Dest.* (note the use of upper and lower case!).

Registration interval (all modes)

After the connector is started, *SAPCONN* registers itself with the configured *program ID* on R/3. This registration allows transmission jobs to be transferred to the connector via the RFC server connection (SM59) configured in R/3. Since the R/3 system in some environments e.g. *SAPCONN* repeats the registration in the *registration interval* set here. If the new registration were not carried out, the R/3 could not have a registered connector after the restart, which would lead to an RFC error for all send requests.

Trace (all modes)

Regardless of the RFC mode, the *Server Trace* can be activated/deactivated. The trace files are then in the work directory of *SAPCONN* (as above).

CPIC

A *CPIC* or RFC user account, which must be created as a service account for *SAPCONN* in R/3, is specified here.

Tenant, User, Password, Confirm Password:

To do this, enter the three-digit number of the R/3 client in *Mandant* in which the CPIC user account is created. The R/3 user name of the CPIC user account is specified as *user*. Finally, the password of the CPIC user account is stored in the fields *Password* and *Confirm password*.

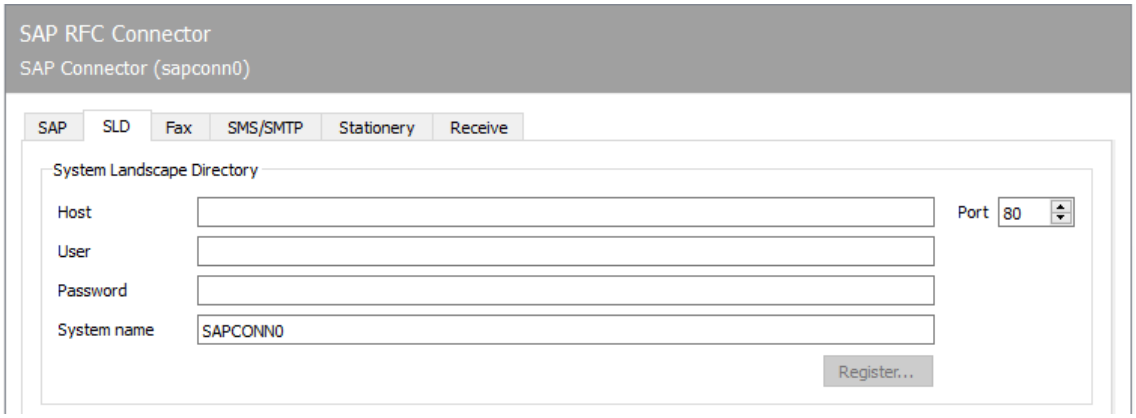
General

Log files

In addition, *SAPCONN* can log the connection to R/3 daily in a so-called communication log. To do this, enter the number of days under *Log files* for how long a communication log should be kept. If all log files are to be saved, configure the value **0*.

Character encoding

If R/3 sends unformatted files as text (TXT or RAW), the *character encoding* cannot be taken from them. Since faxes are mostly sent as formatted files in PCL, PS or PDF, this mainly applies to short messages (SMS) and e-mails. If the character encoding of the file does not match the *SAPCONN* setting, individual characters in the file may be converted incorrectly.



10.18.4. SLD

System Landscape Directory

All information about an IT system landscape in the SAP environment is stored in the System Landscape Directory (SLD). This information is used both to inform the employees responsible in SAP customer support and to provide the customer's employees with an overview of the installed system landscape and the communication channels.

Host

Name of the server that provides the System Landscape Directory in this environment.

User

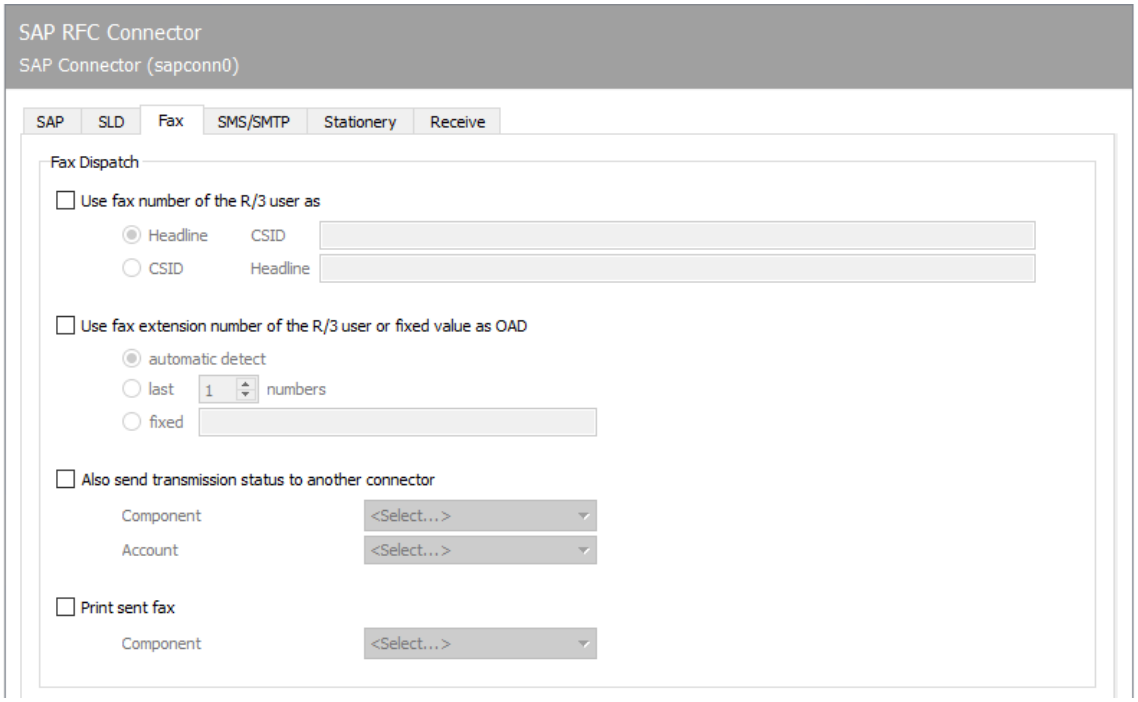
Name of a user who is authorized to make entries in the System Landscape Directory.

Password

User password for authentication in the System Landscape Directory.

System name

SLD name of the OfficeMaster Suite system under which the SLD entry is made.



10.18.5. Fax

Fax dispatch

Use fax number of R/3 user as ...

A separate fax identifier can be determined for each transmission process, which is communicated in the fax log and entered in the header. If no values are maintained for *Fax-ID* and *Header* for *SAPCONN*, the default values configured in OMCUMS or in DirectSip are used.

Selection	ID	Header
(disabled)	as stored for OMCUMS/SIP	as stored for OMCUMS/SIP
Header	as stored for SAPCONN	Fax number of the R/3 sender
identifier	Fax number of the R/3 sender	as stored for SAPCONN

Use fax extension of R/3 user or fixed value for OAD

The connector supports two modes for determining the sender number or the *Originator Address Digit (OAD)*, which is communicated to the telephone system for send requests from *SAPCONN* by *OMCUMS* or *SIP*:

- A fixed OAD is always transmitted (regardless of whether OMCUMS or SIP is used). Selection: ***fixed***

or

- The OAD is determined for each transmission depending on the fax number stored in R/3 for the sender.

In the latter case, the OAD can be *determined* ***automatically*** from the fax sender number or the ***last x digits*** of the fax sender number are used for this. The number that was stored in R/3 as the fax extension for the user is used for automatic determination.

Also transmit the transmission status to another gateway

In addition to the status message in R/3, the messaging server can send the final send status to the user via other components configured in the messaging server.

The user information that is forwarded to the selected connector consists of the fax number as assigned to the sender in the R/3 user master, including the country code - but in the normalized state.

The normalized fax number must be assigned to the user or object (database, distribution list, group) in Active Directory (for Exchange) or in the name and address book (for Notes) to which the send status is to be sent.

In the Active Directory, the assignment is made using an additional FAX address that is distributed to the user.

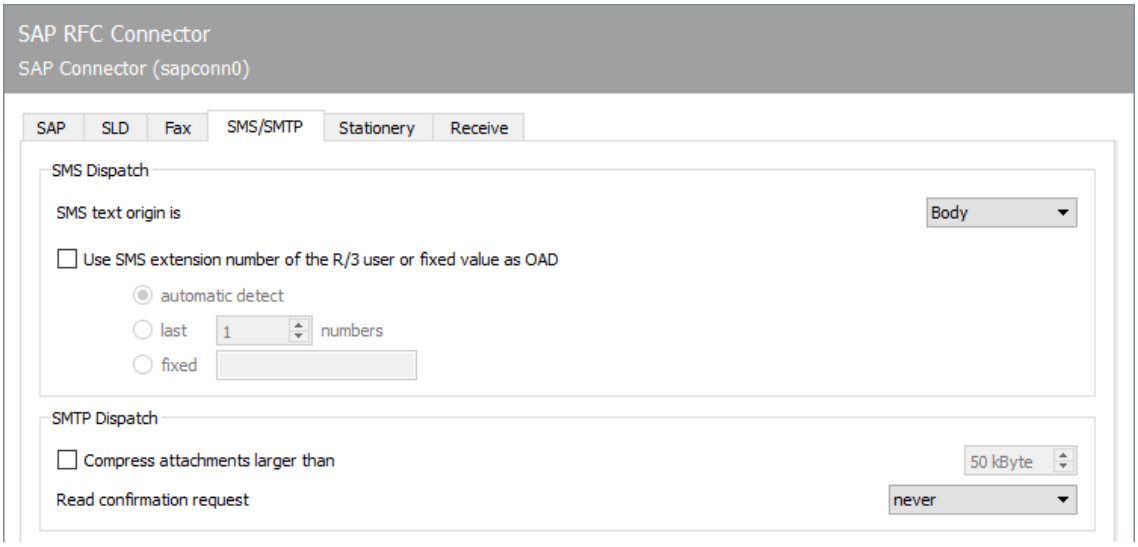
In the name and address book, the normalized number is usually entered as an additional alias for the user.

Normalization of phone numbers:

Country	Original value	Normalized value
Germany	03328-455-960	493328455960
Austria	01-23456-77	4312345677

Print sent faxes

OfficeMaster Messaging Server can optionally output the faxes sent by *SAPCONN* to a network printer after sending. To do this, a print component *PRINTGW* must first be set up in the messaging server. The corresponding *PRINTGW* is then selected as a *component* on the connector.



10.18.6. SMS/SMTP

Sending SMS

SMS text origin

While fax messages and e-mails consist of several pages or files, a short message/SMS is limited to text. In SAP documents, the subject line and/or the message text come into consideration for this text. Accordingly, either the text from the subject line, from the message text or from the subject line and message text can be used as the origin of the SMS text.

If the resulting SMS text exceeds the maximum number of 160 characters permitted for a short message/SMS, the message can be split into several short messages. The maximum number of short messages to which a message should be distributed can be specified under Extras > System settings.

Use the R/3 user's SMS extension or a fixed value for OAD

In the latter case, by ticking this checkbox, a number that differs from the ISDN or SIP configuration can be specified as the SMS sender number or OAD, which is communicated to the telephone system when the call is set up. The mobile phone number assigned to the SAP user in the R/3 user master is used as the SMS sender address. In general, two modes are possible:

- A fixed OAD is always transmitted (regardless of whether OMCUMS or SIP is used). Selection: ***fixed***

or

- The OAD is determined for each transmission depending on the mobile phone number stored in R/3 for the sender.

In the latter case, the OAD can be *determined* ***automatically*** from the fax sender number or the ***last x digits*** of the cell phone sender number are used for this. The number that was stored in R/3 as the mobile phone number for the user is used for automatic determination.

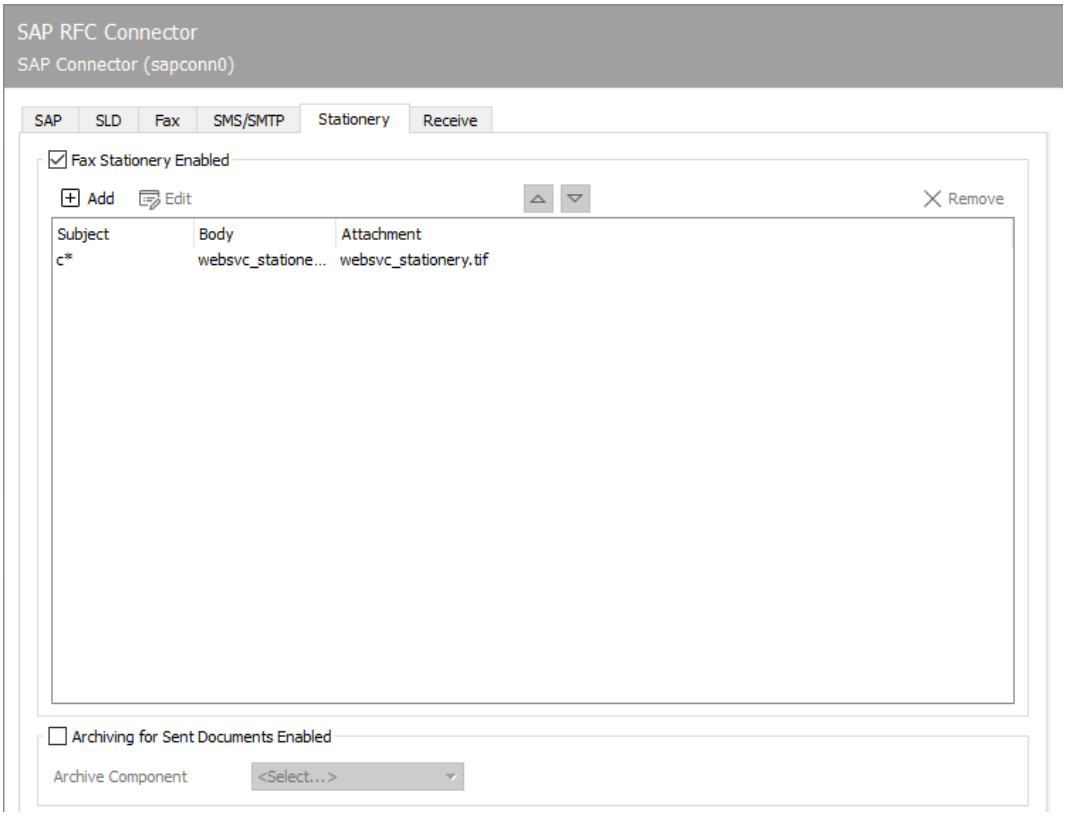
SMTP dispatch

Compress attachments larger than

For sending e-mail attachments, the size of file attachments in kByte can be specified with *Compress attachments larger than*, from which the OfficeMaster Messaging Server should automatically pack the file attachments in ZIP archives.

Request read receipt

- Never
- According to SAP order
- Always



10.18.7. Stationery, archiving

Enable fax stationery

Not all messages from R/3 are permanently provided with stationery or an electronic signature. These two functions can be activated via the *Stationery/Signature* tab, depending on the subject line contained in each transmission.

Archiving of sent documents enabled

An archiving interface can be selected for all documents sent via the RFC connector.

10.18.8. Stationery

If *fax stationery is activated*, different stationery can be stored. Clicking on *Add* opens a dialog in which the necessary settings can be made. A graphic file can be specified here, which is stored as stationery for outgoing messages and their file attachments. The stationery is stored on the messaging server in the %Programdata%\FFUMS\data\stationery\ subdirectory. The

graphic must be saved as a TIF or as a DCX (multi-page PCX) in black and white with a width of 1728 pixels and a height of 2200 pixels (recommendation).

Filters

Regarding

Which stationery to use is decided based on the content of the subject line, which is applied in the form of regular expressions. The regular expression **.*** (dot + asterisk) stands for a subject line with any content.

Body/Attachments

Stationery

If documents with the subject line ***Offer 123xyz*** are to be assigned a special stationery, this stationery can be added to the list using a rule with the regular expression **Offer.***. For multi-page stationery, a mode should be specified for how the stationery is to be used by the messaging server. The following modes are available:

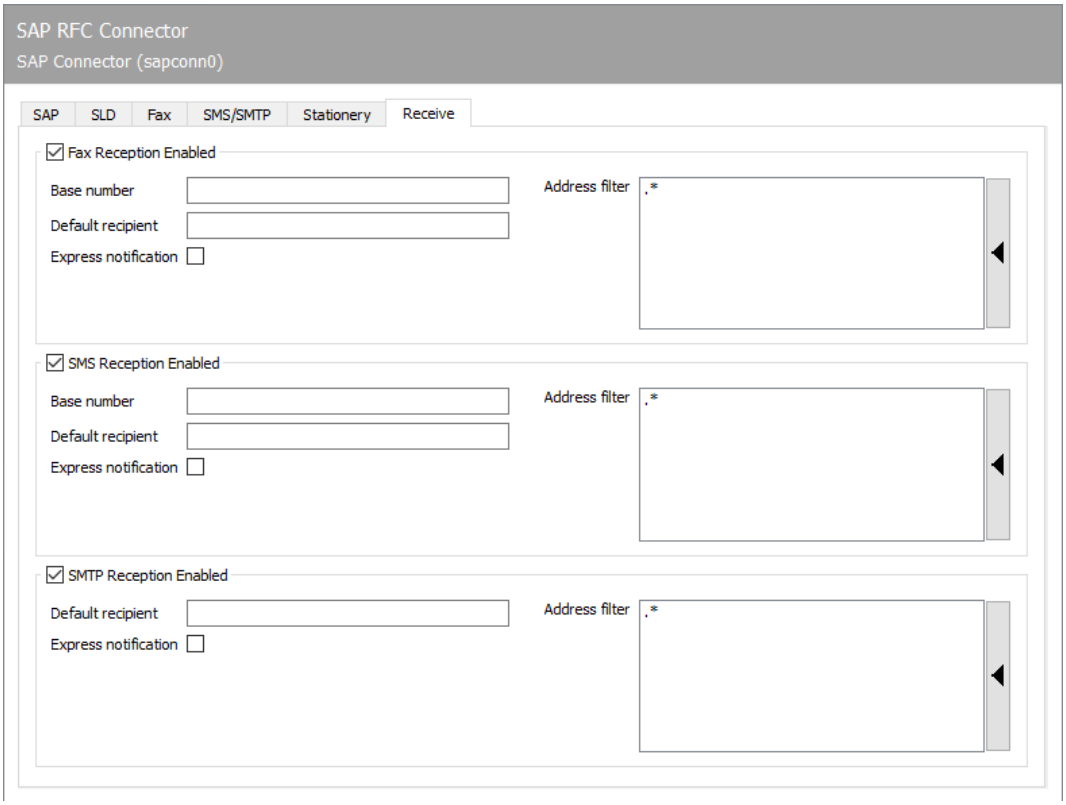
- No stationery
- Use first page only
- Use all pages
- Repeat first page,
- Repeat last page

The stationery configuration can be made differently for the first document and for subsequent documents.

Pixel Options

In addition, you can specify the *pixel operation* to be performed when using the stationery.

- With the pixel operation *or* (or; real stationery), a pixel is black as soon as the pixels that belong together in the send document or in the stationery are black (otherwise white).
- With the pixel operation *xor* (exclusive or fake stationery), a pixel is black in the result as soon as the pixels in the sending document or stationery are black. If both pixels are black, the result is that the pixel is white.



10.18.9. Reception

Fax reception activated

Base Number

If fax reception is activated, faxes are delivered to the corresponding R/3 user in the SAP Business Workplace (transaction *SBWP*). For fax reception, the trunk fax number with country code of the country specified for the users in R/3 must be configured as *Base Number* (e.g. $+^{493328}/_{455}$ - if the user in R/3 country information Germany and the fax number *03328 /455 960* was assigned to the user master). The country code must be specified with a *plus sign* (**+** , no double zero).

Default recipient

In addition to the base number, the full phone number of the R/3 user (master fax number plus extension or called party number) is required as the standard recipient, to whom all received faxes that cannot be assigned to an R/3 user are delivered. The input notation corresponds to the base number (see above).

Address filter

In addition, an address filter must be stored that specifies which faxes are to be reported from *SAPCONN* to R/3. The address filter is maintained in the form of regular expressions. If fax reception is desired in R/3, the connector receives all faxes received from the messaging server with the entry **.*** (dot + asterisk). If the address filters of several connectors overlap, each applicable connector gets the incoming faxes.

SMS reception activated

Base number, default recipient

Similar to fax reception, SMS reception can be activated so that short messages received from the messaging server are also transferred to R/3. As with fax reception, you need the *base number* and a *standard recipient*. Both specifications are configured with the same notation as for fax (see previous section). However, the cell phone number stored for the user in the R/3 user master record is used for comparison when receiving SMS messages. Furthermore, an address filter in the form of regular expressions must be specified, which is applied to the addresses of the short messages (SMS) received.

SMTP reception enabled

Default recipient, address filter

E-mails received by the messaging server are delivered to the recipient in the *SAP Business Workplace*. For receipt, a user's e-mail address must be stored as the *standard recipient*, to which all messages are delivered whose recipient addresses are not maintained in R/3. In addition, *SAPCONN* requires an address filter in the form of regular expressions, which is also applied here to the e-mail address of received messages.

10.19. Connector for SAP

The connection to SAP takes place via the SAPconnect interface.

- SAPconnect has been delivered in R/3 Basis since R/3 version 3.1G and is based on *Remote Function Calls (RFC)*.
- Since R/3 version 4.7 with *Web Application Server (WAS)* version 6.10, SAPconnect can alternatively be operated on the basis of *Simple Mail Transfer Protocol (SMTP)*.

The concept behind SAPconnect is independent of RFC and SMTP. The individual SAP applications (MM, SD, FI, CO) create send requests that are transferred from SAPconnect to OfficeMaster via RFC or SMTP. After OfficeMaster has processed the send request, the final send status is also reported back to R/3 via RFC or SMTP. In order to be able to operate the two SAPconnect technologies, OfficeMaster includes the RFC connector SAPCONN, SAPCONNU, SAPCONNW and the SMTP gateway SAPSMTP.

SAPconnect can be connected in two ways:

- With RFC
- Via SMTP

Both RFC and SMTP support the sending of documents by fax, SMS and e-mail, but the RFC variant offers a larger range of functions and better integration than the SMTP variant.

The status and trace function of the RFC variant allows the system status of the messaging server and detailed log files to be viewed in the SAPconnect administration, which is not possible with SMTP due to the concept.

Various settings are required for commissioning, both in the R/3 system and in the messaging server. The required settings and the recommended sequence can be found in the table below.

Configuration step	**RFC connector(SAPCONN)**	**RFC connector(SAPCONNU)**	**RFC connector(SAPCONNW)**	**SMTP Connector(SAPSMTP**
Set up CPIC users	X	X	X	-
Setting up SAPconnect via RFC	X	X	X	-
Creating and configuring	X	X	X	-

Configuration step	RFC connector(SAPCONN)	RFC connector(SAPCONNU)	RFC connector(SAPCONNW)	SMTP Connector(SAPSMTP
RFC connectors				
Setting up SAPconnect via SMTP	-	-	-	X
Creating and configuring SAPSMTP gateways	-	-	-	X
Set up mail receiving and sending	optional (only for email)	optional (only for email)	optional (only for email)	X
User Management	X	X	X	X
Schedule messaging	X	X	X	X
Test message with SAP Business Workplace	X	X	X	X

10.19.1. Set up SAPconnect via RFC

Depending on the SAPconnect connection via RFC or SMTP, SAP must be configured to use a SAPconnect node for fax, SMS and e-mail. This is used to reach either OfficeMaster's RFC connector (SAPCONN, SAPCONNU, SAPCONNW) or OfficeMaster's SMTP gateway (SAPSMTP).

> **Note!**
> Further information on the SAPconnect configuration can be found in SAP Note 17194 Telefax in various SAP releases.

OfficeMaster's SAPCONNU connector must be set up in each client of an SAP system. In R/3, it represents a SAPconnect node to which the document to be sent with the associated recipient list is transferred via RFC. For the sake of clarity, the necessary "customizing" for SAP ECC 6 is described in this chapter.

A **CPIC** user is required to operate the RFC connector, the configuration of which is described in the following section.

Create CPIC/system user

Transaction: SU01

The RFC-SAPCONN connector requires a CPIC user account under which it can log on to R/3 and transmit status messages and received documents. This user account is created in the R/3 user administration SU01 as follows:

The user account, such as B. _FERRARI*CPIC*, is specified and confirmed with *Create* in the toolbar. The _last*name* of the user can be chosen arbitrarily, e.g. **OfficeMaster**.

Logon data tab

Password: A password for the user is assigned here. The assigned password will later be assigned to the SAPCONNConnector.

User type: The *User type* is changed to **System** or **CPIC**.

Authorization profile S_A.SCON: With _authorization profile S*A.SCON* the required rights are given to the user account on the index card *Profile*.

Now the user account is secured. If there is already a user account with the above settings, it can be shared. Several connectors of a client can also share a CPIC user account.

RFC communication

The SAPconnect interface between R/3 and communication systems uses RFC connections for data exchange. Remote Function Call (*RFC*) is the SAP implementation of the Remote Procedure Call (*RPC*) concept. This concept describes the execution of subprograms on remote computers including the transfer of parameters and return values.

An RFC connection always has two sides. On the one hand, the RFC server offers the execution of functions for other processes. On the other hand, the RFC client calls these functions. Since an RFC connection consists of a server and a client, function calls can only be made in one direction. Therefore, two RFC connections are required for communication between R/3 and communication systems.

- The first RFC connection transfers the data to be sent from R/3 to the communication system. Here the R/3 system is the RFC client and calls functions of the communication system, which the RFC server represents.
- The second RFC connection returns feedback about the success of the communication. It transports received messages from the communication system to the R/3 System. As an RFC client, the communication system calls functions in the R/3 system, which is the RFC server here.

These two directions of communication are considered separately below.

From R/3 to the communication system

A communication system is represented in the R/3 database by a SAPconnect node. A so-called RFC destination is assigned to this node. The attributes of this RFC destination are the information that R/3 needs to set up an RFC connection to a communication system. RFC destinations can be viewed and edited using transaction *SM59*.

If you start transaction *SM59*, you will find a large number of RFC destinations of different types. If an RFC destination is to be used for the SAPconnect interface, it must be of the *TCP/IP* type. This type is available in variants

- *Start*: When executing an RFC, R/3 starts an external program and waits for it to end.
- *Registration*: must be selected for SAPconnect. An external program registers with R/3 and waits for remote function calls.

Such RFC destinations have three attributes:

- Gateway host
- Gateway service
- Program ID

Example:
Gateway here is an R/3 process that handles communication with an external component. Gateway host is the network name or TCP/IP address of the R/3 application server through which communication is to run. Gateway service is the TCP/IP port to be used for this communication. Here you can either enter the port number directly (***3300-3399***) or the name defined by SAP (***sapgw00-sapgw99***). Usually the last two digits of the gateway service correspond to the system number of the R/3 system. Finally, the program ID is a unique name that is used to distinguish between different RFC partners that register on the same application server at the same port.

These three parameters are also sufficient for the other side of the RFC connection (*SAPCONNU*-Connector from OfficeMaster) to register with the SAP gateway. It must be ensured that the network and port names are also known on the computer on which the *SAPCONNU* connector is running. If you have configured the same gateway host, gateway service and program ID on the R/3 and *SAPCONNU* side and started the *SAPCONNU* connector, it is already possible to transfer fax jobs from the R/3 system to *SAPCONNU*.

In transaction **SM59** you can check the existence of this RFC connection with the function *test connection*. Alternatively, each registered system can be displayed via the menu sequence Go to > Registered Systems in the Gateway Monitor (transaction **SMGW**).

From the communication system to the R/3

In the opposite direction of communication, OfficeMaster transfers information to the R/3 system. The network name of the application server and the system or instance number of the system for which the message is intended are required to establish the connection. Normally, the application server here is the same computer that was specified as the gateway host for the RFC connection from the R/3 system to the communication system. Since exceptions are possible, both computer names can be configured separately in the configuration of the *SAPCONNU* connector.

If status messages for fax jobs or received faxes are to be transferred to the R/3 System, data in the R/3 System must be changed. This requires rights that can only be assigned to users. The communication system must identify itself as an R/3 user. To do this, a so-called CPIC or RFC user is created in R/3 with the rights required by the communication system. The communication system must transfer the logon data of this user to the R/3 system with every communication. The login data includes the name and password of the CPIC user and the name of the client for which the CPIC user was created.

Configuration Files

It may happen that the TCP/IP configuration of the computer on which the *SAPCONNU* connector is running needs to be adjusted. This is done by editing the hosts file and the services file.

The hosts file contains a mapping of names to TCP/IP addresses. On Windows, it is located in the %systemroot% \system32\drivers\etc directory and is named *hosts*. So if the name of the R/3 server cannot be resolved on the machine running the *SAPCONNU* connector, a line containing the name and IP address of the R/3 server is added to the hosts file.

The Services file contains a mapping of names to TCP/IP ports. It is located in the %systemroot%\system32\drivers\etc directory (on Windows) and is named *services*. If you use names of the form *sapgwXX* instead of port numbers *33XX* in the _SAPCONNU_Connector configuration, add a line with the name and port number to the services file for each name used. These settings are made automatically by installing a SAPgui.

Create RFC destination

Transaction: SCOT or SM59

The *SAPCONNU* connector of the messaging server is represented in R/3 as a SAPconnect node. An RFC destination is assigned to this node, to which the requests are sent after conversion. The RFC destination can also be created during the installation of the node.

You can maintain the RFC destination with transaction *SM59* or with the node assistant of the SAPconnect administration. An RFC destination is created with *Create* in the toolbar.

RFC destination: Maintaining the RFC destinations involves system-wide settings. Since the RFC destination will later be linked to client-related settings of the SAPconnect node, a name with client number (e.g. _fercon*100* for SAPCONNU connector for *client 100*) should be selected.

Connection type: The connection is made via TCP/IP, select **T** for this.

Activation type: The activation type must be set to “Registered server program”. Depending on the selection, the associated program ID can then be entered. To ensure clarity, the name of the destination (in the example: _fercon*100*) can be used (capital - & note lower case!).

Gateway options: The host name of the R/3 server is entered under Gateway host. The gateway service is the TCP port that SAPconnect uses to set up the RFC call to the SAPCONNU connector. Enter **sapgwXX** here, where **XX** stands for the two-digit system or instance number of the R/3 system (e.g. *sapgw00*). Finally, the RFC destination is saved.

Create SAPconnect node

Transaction: SCOT, Menu: View > Node

Each SAPconnect node in SAP is created with the help of an R/3 wizard. In the *SCOT* transaction under the menu item View > Node, select the *Create Node* button from the toolbar.

First you will be prompted to enter the node name (e.g. *FERCON*) with description and the node type.

In order for the RFC node to transfer send requests to the SAPCONNU connector via RFC, it needs an RFC destination. This can be entered in the subsequent dialog. It is created with the *RFC Destination* button. Then select the RFC destination and click *Next*.

Fax with SAPconnect via RFC

The creation of a node of the address type *Fax* is described below. The descriptions for *Internet-Mail* and *SMS* follow afterwards.

Address range:

In the next dialog, a fax address range for this node is specified so that outgoing fax messages are routed to it. This routing can be set using the recipient fax number. To set up only one SAPconnect node or SAPCONNU connector, “*” is entered in the address area.

If there are several SAPCONNU connectors (and thus several nodes), the address ranges for the individual nodes are divided up (e.g. **CH*** for the node _FAX*Z* or **DE 030*** for the node _FAX*B*).

Document formats: In the next step, the document formats that can be processed by the messaging server are specified. The following document formats are possible for fax communication with SAP: *PCL* or *PS* (mutually exclusive), PDF, RAW and TIF (for forwarded faxes).

> **Note!**
> The converter component of the messaging server must be configured accordingly. If *PS* is used as the file format, *Ghostscript* must be installed as the conversion software.

The *PCL* and *TIF* formats are preferred, since the internal PCL converter can be used for them.

Documents in the R/3 internal document format (such as *ALI*, *SCR*) are converted to PCL or PS format in the R/3 spool. Depending on the previously configured document format, the printer driver *HPLJ5* (for PCL) or *POST2* (for PS) is specified as the device type. Optionally, the transmission times for the three different priority levels can be specified in the following dialog.

Configuration of the location: This is followed by the configuration of the location. The country code (e.g. *DE*) indicates the location of the OfficeMaster Messaging Server. This input is required for controlling the country code of the fax numbers (like *+49*).

After clicking on *Next* you can either add further address types (Internet mail and SMS) to the node or exit the configuration wizard.

If no further address types are to be added, settings for all address areas of the node can be made by selecting *No* in the following dialog.

Maximum waiting time for resend attempts: The interval for resend attempts (see Figure 10.10) is entered as the first setting for the entire node if an RFC error occurs during the transfer from R/3 to SAPCONN.

Node can resolve path references/node should be monitored by the alert monitor: The checkboxes *Node can resolve path references* and *Node should be monitored by the alert monitor* should not be checked.

Node is operational: Finally, the *Node is operational* check box is checked.

Result:

The SAPconnect node *FERCON* was set up for the *SAPCONNU* connector. The node can be reconfigured if necessary.

Internet mail with SAPconnect via RFC

Equivalent to fax, a (further) address range is created for the node for sending Internet e-mails. The dialogs are adjusted accordingly. If only this SAPconnect node with Internet mail functionality is to be specified in the R/3 client, the entry * (asterisk) in the address area is sufficient.

The transmission of e-mails is usually not limited to any specific document format. Therefore, all document formats are generally supported.

If orders and lists in the *OTF*, *SCR*, *ALI* and *INT* formats are to be converted into externally understandable formats beforehand using SAPconnect, these formats should be excluded. To do this, select the option *All formats except the following* and add the above formats to the list by clicking the *SAP internal formats* button. In addition, the formats PCL and PS should be excluded from mailing.

The previous step presumably converts all internal SAP formats to PDF or HTM, depending on the conversion rules set. Thus, no device type is required.

All the settings required for e-mail have now been made. If desired, paging/SMS can be configured. Otherwise *No* is selected.

Paging/SMS with SAPconnect via RFC

Since R/3 Version 4.5, SAPconnect has supported the sending and receiving of short messages/SMS. A prerequisite is a configured SMS communication interface on the OfficeMaster Messaging Server. Under these conditions, *Pager* (=SMS) is selected as the address type.

When configuring the address range for this node, the short messages are routed to the node. If only this SAPconnect node is to be addressed with SMS functionality, * is entered in the address area. Pager subtypes such as *E+.** or *02:017** can be specified for a more precise specification.

RAW data (ASCII) are supported for the transmission of short messages. In order to convert the R/3 internal data (e.g. SCR) into RAW, ASCIIPRT is required as the device type.

Configure SAPconnect node (optional)

Since SAP 4.7, external formats must be set for the four internal SAP formats, depending on the service. There is no need to configure conversion rules, output devices or supported document formats. The following table provides an overview of the recommended target formats.

SAP internal formats	**Fax**	**SMS/Pager**	**Internet Mail**
SAPscript / Smart Forms	PCL or PS	TXT	PDF
ABAP list	PCL or PS	TXT	HTM
Business Object/Reference	TXT	TXT	HTM
RAW Text	TXT	TXT	TXT

10.19.2. RFC connector (SAPCONNU)

The connection of an R/3 system to the messaging server takes place via the gateway component SAPCONNU with a non-Unicode connection. At least one gateway component must be created, configured and operated as a connector for each SAP client. To do this, select in the quick launch bar > SAP > RFC in the messaging server configuration.

All created connectors are displayed on the left side. The selected SAPCONNU connector can be configured on the right side. If no connector is displayed, the corresponding SAPCONNU connectors must be created using the *Add* button.

Create RFC connector

A new component of type SAPCONNU is created for the messaging server. A SAPCONNU connector is set up for each SAP client or for each SAPconnect node.

Since the connectors are numbered consecutively by name, it is advisable to use descriptive display names in order to simplify administration later. For example, the SAP system abbreviation and the SAP client number can be used in the display name, resulting in names like *SAP DEV 100*. Once the component has been created, it can be configured.

Test sending faxes via SAP GUI

R/3 user administration

Transaction: SU01 or SU51

R/3 users should be assigned fax numbers, radio numbers and e-mail addresses in the R/3 user master for the following reasons:

- Only users with a sender address in the desired communication type are allowed to send messages in this way, i.e. only users with a fax number are allowed to fax.
- The maintained sender number or e-mail address is also communicated to the recipient as the sender address.
- Received faxes, short messages and e-mails are assigned via the phone numbers or e-mail addresses maintained in the R/3 user master.
- In the log files of the SAPCONN connector, the operations of a specific R/3 user are identified by their sender address in the R/3 user master.

Of course, the fax number can also be maintained in transaction SU51 (System > User settings > User address).

Messaging

Transaction: SCOT, in the menu sequence View > Jobs

The R/3 internal program *RSCONN01* is responsible for transferring the messages from R/3 to OfficeMaster via RFC. In order for this to happen, a job is scheduled that starts the program every 10-15 minutes. Depending on how sensitively communication is handled in a company, the interval for program execution should be selected. It should not be less than 5 minutes.

The process is activated with *Schedule sending process* in the toolbar of the SAPconnect administration and the input of a name for the job is expected.

Then the variant *FAX* is selected with the cursor and confirmed with *Schedule*.

The time interval for the program starts of *RSCONN01* can be entered via *Schedule periodically*. The first start date is generally one hour in the future. After saving these settings, the job is scheduled.

The procedure is analogous with Internet mail and pagers/SMS.

To test the configuration, the transmission of faxes, short messages and e-mails can also be started manually and not job-controlled. This is also possible in the SAPconnect administration. The *Start send process* button is available for this. *FAX*, *Pager*, *INT* or "*" is selected as the address type. Alternatively, the transfer program (*RSCONN01*) can be started in transaction *SE38*.

> Note!
> Another very useful R/3 program is *RSCONN05*. It allows faxes with errors to be resent without having to recreate the documents using the R/3 applications (such as MM, SD, etc.). This program can be accessed via transaction *SOST* or the menu sequence Utilities > Overview of send requests. More information is available in SAP note number *92287*.

Test message with SAP Business Workplace

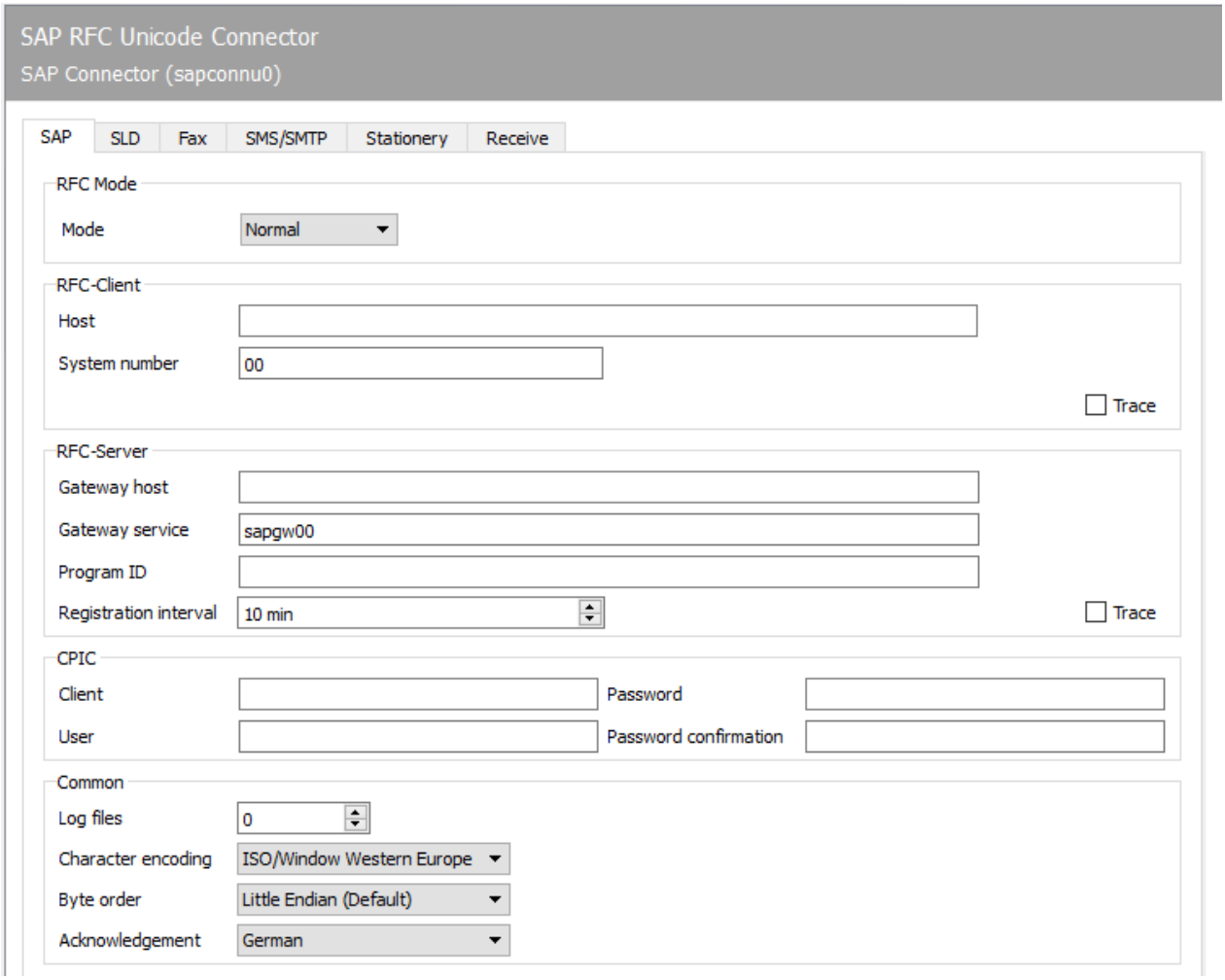
In order to send a test message from SAP, both the messaging server and the connectors must be started. You log on to R/3 with the *SAPgui*. A new message is now created in the Business Workplace (transaction *SBWP*). The recipient number must be entered in the syntax *<country code> number* (e.g. ***DE 0123456***, ***US 555-$^{456}/_{89}$***), which is automatically generated by the R/3 recognized as a fax number.

With the _Send_button from the toolbar, the document is saved as a send order in the office outbox. Here it waits for the ABAP program *RSCONN01* to transmit it to the connector. The current transmission status of the document can be read at any time on the *Recipient list* tab in the office exit. This tab is associated with the message.

The status of other SAP documents, such as B. Orders. The SAP applications use the Business Workplace as a transport medium and therefore store the fax jobs in the office outbox. A document has the following status messages in the course of sending:

R/3 release	**Version 6.x**
Before RSCONN01	Waiting
After RSCONN01 and before completion of sending by the fax server	Message passed from node ... to communication system
After successful completion of sending by the fax server	Delivery to ...
After the fax server failed to complete the transmission	No extradition

If the document cannot be sent, the R/3 sender also receives an express document, which draws his attention to this fact.



10.19.3. SAP

The first configuration steps for the *SAPCONNU* component relate to the direct connection to the SAP system and are carried out on the *SAP* tab.

RFC mode

The type of RFC connection is determined in the *RFC mode* area. The choice made here changes the input options of the tab:

Mode

*normal
In RFC mode *Normal*, both the RFC server and the RFC client connection take place without load balancing. This is the standard case, i. H. this setting applies to most of the installation.

- Load balancing
  In *RFC mode load balancing*, the RFC client connection is subject to load balancing. Since this setting only affects incoming messages and status messages, this option only makes sense for a very small number of installations.

*RFC-INI
The *RFC mode RFC INI* is only intended for experts who want to manually describe the RFC connection in the configuration file *saprfc.ini*.

> Note!
> For most installations, *Normal* is sufficient as the RFC mode.

RFC client

In this area, information about the RFC inbound connection from *SAPCONNU* to the R/3 system is made (depending on the *RFC mode*).

Host, system number *(normal in RFC mode)*

With RFC mode *Normal*, the TCP/IP address or the resolved name of the R/3 application server must be entered as *Host*. The two-digit system or instance number of the R/3 system is required as the *system number*. This number can e.g. read in the SAPlogon program.

Host, name, group (in RFC mode *load balancing*)

In the RFC mode *Load Balancing* the TCP/IP address or the resolved name of the R/3 application server that provides the load balancing must be entered as *Host*.

name is the name of the R/3 system and *group* is the name of the group of R/3 application servers with load balancing. If such systems are available, you can also find this information in the SAPlogon program of the SAPgui.

RFC section (in RFC mode *RFC INI*)

The section in *saprfc.ini* that describes the RFC connection to the R/3 System is specified (note the use of upper and lower case!).

Trace (all modes)

Regardless of the RFC mode, the RFC trace can be activated/deactivated with *Client-Trace*. The trace files are stored in the work directory of the SAPCONN connector. The work directory is in %ProgramFiles%\FFUMS\FMSRV\work\SAPCONN.

RFC server

Here the RFC outbound connection from the R/3 system to *SAPCONN* is configured. This information must be the same as the information in R/3, and must therefore be configured later in R/3 for the RFC destination (SM59).

Gateway host, gateway service (in RFC mode *normal* and *load balancing*)

The TCP/IP address or the resolved name of the R/3 application server (normal RFC mode) or the computer on which the SAP gateway is running (load balancing) must be specified as *Gateway host*. The resolved TCP/IP port over which the RFC connection is to run is specified under *Gateway service*. The gateway service name (e.g. *sapgw00*, *sapgw01*) may need to be resolved on the server in the *services* file.

Program ID (in RFC mode *normal* and load balancing)

A unique name is configured as the *program ID* under which SAPCONNU registers in R/3. R/3 uses this program ID to find the *SAPCONNU* connector. For this purpose, the same program ID is

stored in R/3 in the RFC destination assigned to the SAPconnect node (Note: upper and lower case letters!).

RFC section (in RFC mode *RFC-INI*)

In RFC mode *RFC INI*, the section in *saprfc.ini* that describes the connection from the R/3 system to SAPCONNU must be specified as *RFC-Dest.* (note the use of upper and lower case!).

Registration interval (all modes)

After the connector is started, *SAPCONNU* registers itself with the configured *program ID* on R/3. This registration allows transmission jobs to be transferred to the connector via the RFC server connection (SM59) configured in R/3. Since the R/3 system in some environments e.g. *SAPCONNU* repeats the registration in the *registration interval* set here. If the new registration were not carried out, the R/3 could not have a registered connector after the restart, which would lead to an RFC error for all send requests.

Trace (all modes)

Regardless of the RFC mode, the *Server Trace* can be activated/deactivated. The trace files are then in the work directory of *SAPCONNU* (as above).

CPIC

A *CPIC* or RFC user account, which must be created as a service account for *SAPCONNU* in R/3, is specified here.

Tenant, User, Password, Confirm Password:

To do this, enter the three-digit number of the R/3 client in *Mandant* in which the CPIC user account is created. The R/3 user name of the CPIC user account is specified as *user*. Finally, the password of the CPIC user account is stored in the fields *Password* and *Confirm password*.

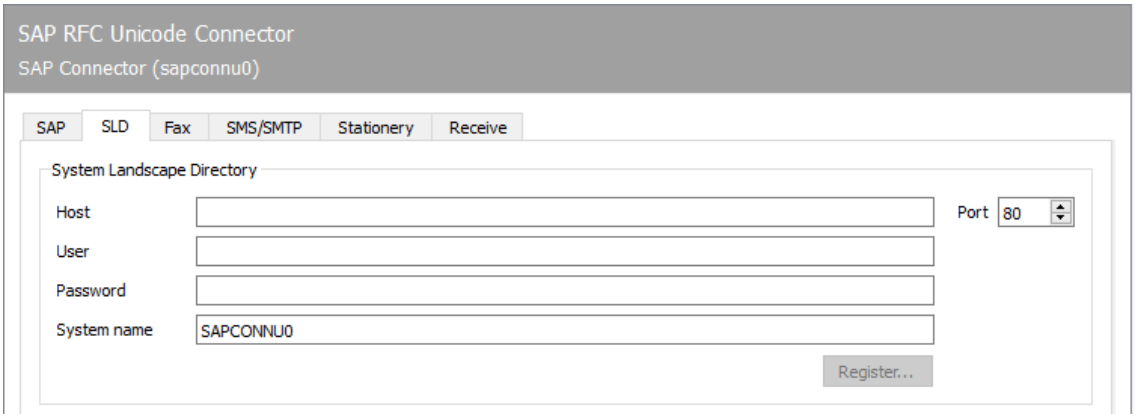
General

Log files

In addition, *SAPCONNU* can log the connection to R/3 daily in a so-called communication log. To do this, enter the number of days under *Log files* for how long a communication log should be kept. If all log files are to be saved, configure the value **0*.

Character encoding

If R/3 sends unformatted files as text (TXT or RAW), the *character encoding* cannot be taken from them. Since faxes are mostly sent as formatted files in PCL, PS or PDF, this mainly applies to short messages (SMS) and e-mails. If the character encoding of the file does not match the *SAPCONNU* setting, individual characters in the file may be converted incorrectly.



10.19.4. SLD

System Landscape Directory

All information about an IT system landscape in the SAP environment is stored in the System Landscape Directory (SLD). This information is used both to inform the employees responsible in SAP customer support and to provide the customer's employees with an overview of the installed system landscape and the communication channels.

Host

Name of the server that provides the System Landscape Directory in this environment.

User

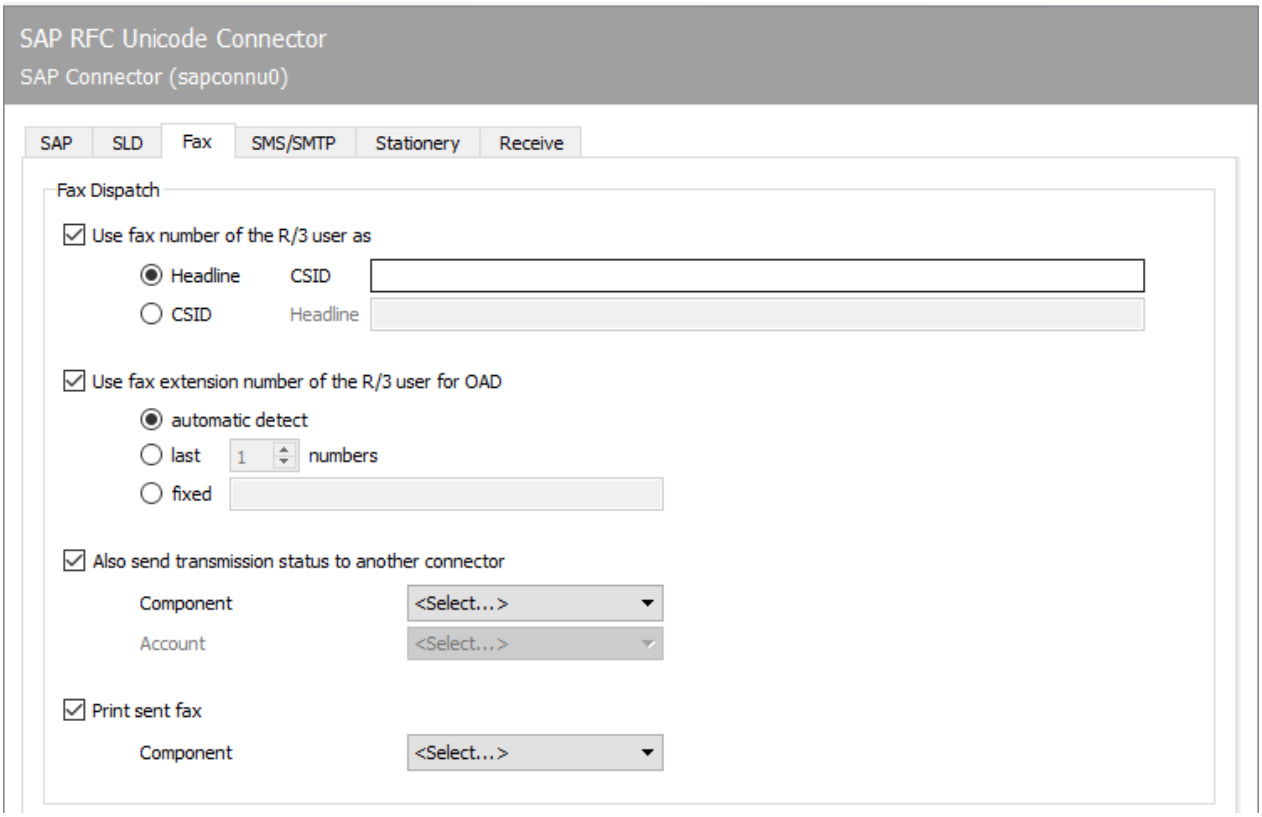
Name of a user who is authorized to make entries in the System Landscape Directory.

Password

User password for authentication in the System Landscape Directory.

System name

SLD name of the OfficeMaster Suite system under which the SLD entry is made.



10.19.5. Fax

Fax dispatch

Use fax number of R/3 user as ...

A separate fax identifier can be determined for each transmission process, which is communicated in the fax log and entered in the header. If no values are maintained for *Fax-ID* and *Header* for *SAPCONNU*, the default values configured in OMCUMS or in DirectSip are used.

Selection	ID	Header
(disabled)	as stored for OMCUMS/SIP	as stored for OMCUMS/SIP
Header	as defined for SAPCONNU	Fax number of the R/3 sender
identifier	Fax number of the R/3 sender	as defined for SAPCONNU

Use fax extension of R/3 user or fixed value for OAD

The connector supports two modes for determining the sender number or the *Originator Address Digit (OAD)*, which is communicated to the telephone system for send requests from *SAPCONNU* by *OMCUMS* or *SIP*:

- A fixed OAD is always transmitted (regardless of whether OMCUMS or SIP is used). Selection: ***fixed***

or

- The OAD is determined for each transmission depending on the fax number stored in R/3 for the sender.

In the latter case, the OAD can be *determined* ***automatically*** from the fax sender number or the ***last x digits*** of the fax sender number are used for this. The number that was stored in R/3 as the fax extension for the user is used for automatic determination.

Also transmit the transmission status to another gateway

In addition to the status message in R/3, the messaging server can send the final send status to the user via other components configured in the messaging server.

The user information that is forwarded to the selected connector consists of the fax number as assigned to the sender in the R/3 user master, including the country code - but in the normalized state.

The normalized fax number must be assigned to the user or object (database, distribution list, group) in Active Directory (for Exchange) or in the name and address book (for Notes) to which the send status is to be sent.

In the Active Directory, the assignment is made using an additional FAX address that is distributed to the user.

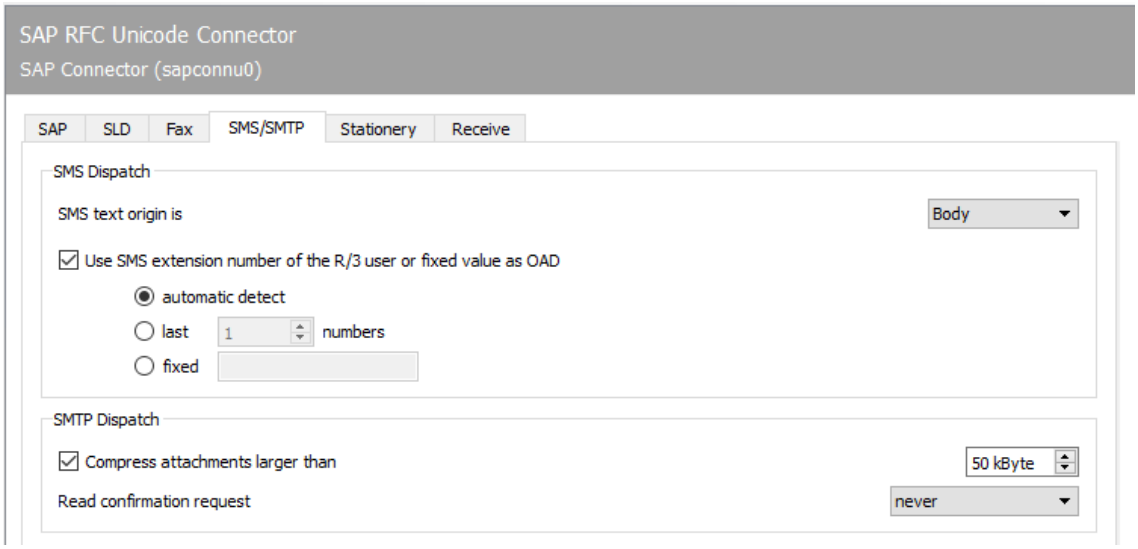
In the name and address book, the normalized number is usually entered as an additional alias for the user.

Normalization of phone numbers:

Country	Original value	Normalized value
Germany	03328-455-960	493328455960
Austria	01-23456-77	4312345677

Print sent faxes

OfficeMaster Messaging Server can optionally output the faxes sent by *SAPCONNU* to a network printer after they have been sent. To do this, a print component *PRINTGW* must first be set up in the messaging server. The corresponding *PRINTGW* is then selected as a *component* on the connector.



10.19.6. SMS/SMTP

Sending SMS

SMS text origin

While fax messages and e-mails consist of several pages or files, a short message/SMS is limited to text. In SAP documents, the subject line and/or the message text come into consideration for this text. Accordingly, either the text from the subject line, from the message text or from the subject line and message text can be used as the origin of the SMS text.

If the resulting SMS text exceeds the maximum number of 160 characters permitted for a short message/SMS, the message can be split into several short messages. The maximum number of short messages to which a message should be distributed can be specified under Extras > System settings.

Use the R/3 user's SMS extension or a fixed value for OAD

In the latter case, by ticking this checkbox, a number that differs from the ISDN or SIP configuration can be specified as the SMS sender number or OAD, which is communicated to the telephone system when the call is set up. The mobile phone number assigned to the SAP user in the R/3 user master is used as the SMS sender address. In general, two modes are possible:

- A fixed OAD is always transmitted (regardless of whether OMCUMS or SIP is used). Selection: ***fixed***

or

- The OAD is determined for each transmission depending on the mobile phone number stored in R/3 for the sender.

In the latter case, the OAD can be *determined* ***automatically*** from the fax sender number or the ***last x digits*** of the cell phone sender number are used for this. The number that was stored in R/3 as the mobile phone number for the user is used for automatic determination.

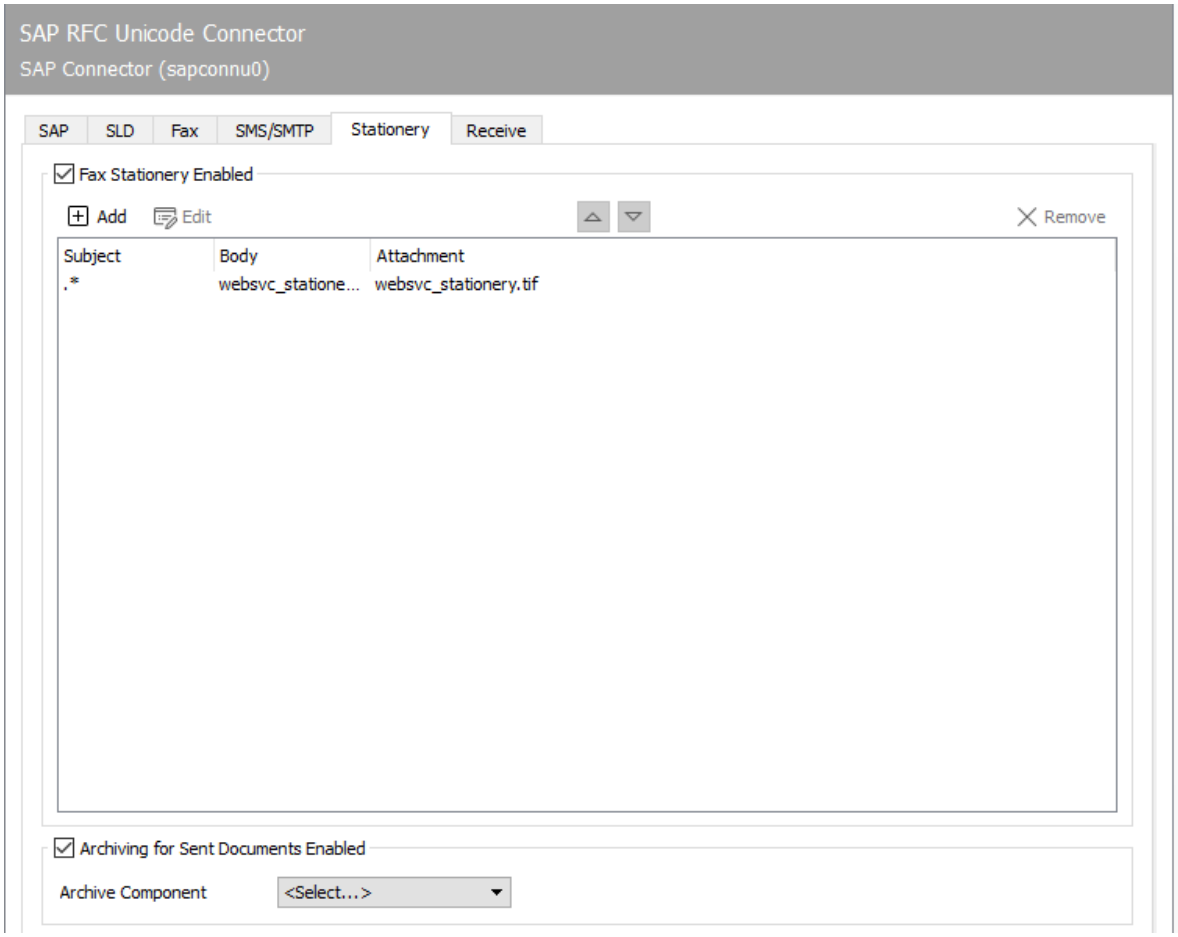
SMTP dispatch

Compress attachments larger than

For sending e-mail attachments, the size of file attachments in kByte can be specified with *Compress attachments larger than*, from which the OfficeMaster Messaging Server should automatically pack the file attachments in ZIP archives.

Request read receipt

- Never
- According to SAP order
- Always



10.19.7. Stationery, archiving

Enable fax stationery

Not all messages from R/3 are permanently provided with stationery or an electronic signature. These two functions can be activated via the *Stationery/Signature* tab, depending on the subject line contained in each transmission.

Archiving of sent documents enabled

An archiving interface can be selected for all documents sent via the RFC connector.

10.19.8. Stationery

If *fax stationery is activated*, different stationery can be stored. Clicking on *Add* opens a dialog in which the necessary settings can be made. A graphic file can be specified here, which is stored as stationery for outgoing messages and their file attachments. The stationery is stored on the messaging server in the %Programdata%\FFUMS\data\stationery\ subdirectory. The graphic must be saved as a TIF or as a DCX (multi-page PCX) in black and white with a width of 1728 pixels and a height of 2200 pixels (recommendation).

Filters

Regarding

Which stationery to use is decided based on the content of the subject line, which is applied in the form of regular expressions. The regular expression **.*** (dot + asterisk) stands for a subject line with any content.

Body/Attachments

Stationery

If documents with the subject line ***Offer 123xyz*** are to be assigned a special stationery, this stationery can be added to the list using a rule with the regular expression **Offer.***. For multi-

page stationery, a mode should be specified for how the stationery is to be used by the messaging server. The following modes are available:

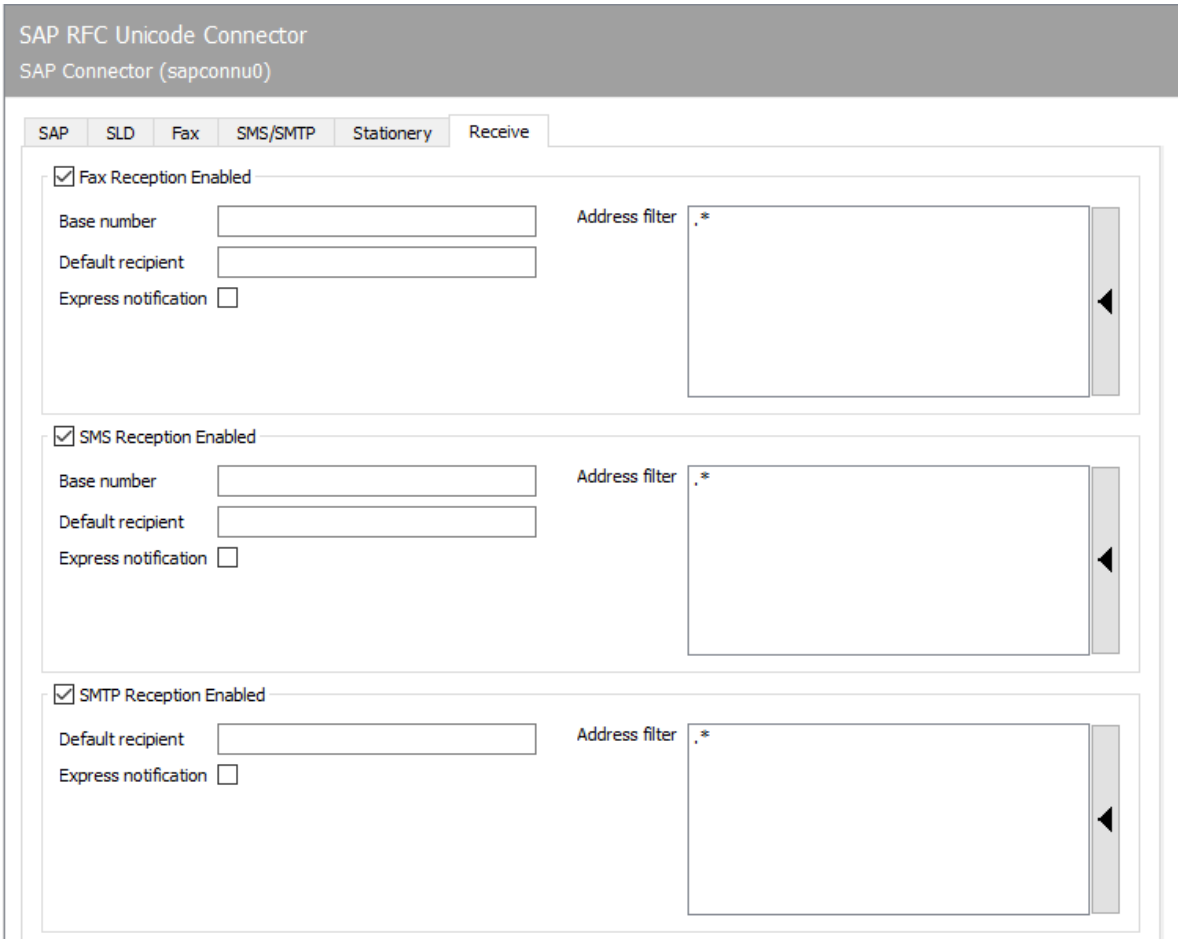
- No stationery
- Use first page only
- Use all pages
- Repeat first page,
- Repeat last page

The stationery configuration can be made differently for the first document and for subsequent documents.

Pixel Options

In addition, you can specify the *pixel operation* to be performed when using the stationery.

- With the pixel operation *or* (or; real stationery), a pixel is black as soon as the pixels that belong together in the send document or in the stationery are black (otherwise white).
- With the pixel operation *xor* (exclusive or fake stationery), a pixel is black in the result as soon as the pixels in the sending document or stationery are black. If both pixels are black, the result is that the pixel is white.



10.19.9. Reception

Fax reception activated

Base Number

If fax reception is activated, faxes are delivered to the corresponding R/3 user in the SAP Business Workplace (transaction *SBWP*). For fax reception, the trunk fax number with country code of the country specified for the users in R/3 must be configured as *Base Number* (e.g. $+^{493328}/_{455}$ - if the user in R/3 country information Germany and the fax number *03328 /455 960* was assigned to the user master). The country code must be specified with a *plus sign* (**+** , no double zero).

Default recipient

In addition to the base number, the full phone number of the R/3 user (master fax number plus extension or called party number) is required as the standard recipient, to whom all received faxes that cannot be assigned to an R/3 user are delivered. The input notation corresponds to the base number (see above).

Address filter

In addition, an address filter must be stored that specifies which faxes are to be reported from *SAPCONNU* to R/3. The address filter is maintained in the form of regular expressions. If fax reception is desired in R/3, the connector receives all faxes received from the messaging server with the entry **.*** (dot + asterisk). If the address filters of several connectors overlap, each applicable connector gets the incoming faxes.

SMS reception activated

Base number, default recipient

Similar to fax reception, SMS reception can be activated so that short messages received from the messaging server are also transferred to R/3. As with fax reception, you need the *base number* and a *standard recipient*. Both specifications are configured with the same notation as for fax (see previous section). However, the cell phone number stored for the user in the R/3 user master record is used for comparison when receiving SMS messages. Furthermore, an address filter in the form of regular expressions must be specified, which is applied to the addresses of the short messages (SMS) received.

SMTP reception enabled

Default recipient, address filter

E-mails received by the messaging server are delivered to the recipient in the *SAP Business Workplace*. For receipt, a user's e-mail address must be stored as the *standard recipient*, to which all messages are delivered whose recipient addresses are not maintained in R/3. In addition, *SAPCONNU* requires an address filter in the form of regular expressions, which is also applied here to the e-mail address of received messages.

10.20. Connector for SAP

The connection to SAP takes place via the SAPconnect interface.

- SAPconnect has been delivered in R/3 Basis since R/3 version 3.1G and is based on *Remote Function Calls (RFC)*.
- Since R/3 version 4.7 with *Web Application Server (WAS)* version 6.10, SAPconnect can alternatively be operated on the basis of *Simple Mail Transfer Protocol (SMTP)*.

The concept behind SAPconnect is independent of RFC and SMTP. The individual SAP applications (MM, SD, FI, CO) create send requests that are transferred from SAPconnect to OfficeMaster via RFC or SMTP. After OfficeMaster has processed the send request, the final send status is also reported back to R/3 via RFC or SMTP. In order to be able to operate the two SAPconnect technologies, OfficeMaster includes the RFC connector SAPCONN, SAPCONNU, SAPCONNW and the SMTP gateway SAPSMTP.

SAPconnect can be connected in two ways:

- With RFC
- Via SMTP

Both RFC and SMTP support the sending of documents by fax, SMS and e-mail, but the RFC variant offers a larger range of functions and better integration than the SMTP variant.

The status and trace function of the RFC variant allows the system status of the messaging server and detailed log files to be viewed in the SAPconnect administration, which is not possible with SMTP due to the concept.

Various settings are required for commissioning, both in the R/3 system and in the messaging server. The required settings and the recommended sequence can be found in the table below.

Configuration step	**RFC connector(SAPCONN)**	**RFC connector(SAPCONNU)**	**RFC connector(SAPCONNW)**	**SMTP Connector(SAPSMTP**
Set up CPIC users	X	X	X	-
Setting up SAPconnect via RFC	X	X	X	-
Creating and configuring	X	X	X	-

Configuration step	RFC connector(SAPCONN)	RFC connector(SAPCONNU)	RFC connector(SAPCONNW)	SMTP Connector(SAPSMTP
RFC connectors				
Setting up SAPconnect via SMTP	-	-	-	X
Creating and configuring SAPSMTP gateways	-	-	-	X
Set up mail receiving and sending	optional (only for email)	optional (only for email)	optional (only for email)	X
User Management	X	X	X	X
Schedule messaging	X	X	X	X
Test message with SAP Business Workplace	X	X	X	X

10.20.1. Set up SAPconnect via RFC

Depending on the SAPconnect connection via RFC or SMTP, SAP must be configured to use a SAPconnect node for fax, SMS and e-mail. This is used to reach either OfficeMaster's RFC connector (SAPCONN, SAPCONNU, SAPCONNW) or OfficeMaster's SMTP gateway (SAPSMTP).

> **Note!**
> Further information on the SAPconnect configuration can be found in SAP Note 17194 Telefax in various SAP releases.

OfficeMaster's SAPCONNW connector must be set up in each client of an SAP system. In R/3, it represents a SAPconnect node to which the document to be sent with the associated recipient list is transferred via RFC. For the sake of clarity, the necessary "customizing" for SAP ECC 6 is described in this chapter.

A **CPIC** user is required to operate the RFC connector, the configuration of which is described in the following section.

Create CPIC/system user

Transaction: SU01

The RFC-SAPCONN connector requires a CPIC user account under which it can log on to R/3 and transmit status messages and received documents. This user account is created in the R/3 user administration SU01 as follows:

The user account, such as B. _FERRARI*CPIC*, is specified and confirmed with *Create* in the toolbar. The _last*name* of the user can be chosen arbitrarily, e.g. **OfficeMaster**.

Logon data tab

Password: A password for the user is assigned here. The assigned password will later be assigned to the SAPCONNConnector.

User type: The *User type* is changed to **System** or **CPIC**.

Authorization profile S_A.SCON: With _authorization profile S*A.SCON* the required rights are given to the user account on the index card *Profile*.

Now the user account is secured. If there is already a user account with the above settings, it can be shared. Several connectors of a client can also share a CPIC user account.

RFC communication

The SAPconnect interface between R/3 and communication systems uses RFC connections for data exchange. Remote Function Call (*RFC*) is the SAP implementation of the Remote Procedure Call (*RPC*) concept. This concept describes the execution of subprograms on remote computers including the transfer of parameters and return values.

An RFC connection always has two sides. On the one hand, the RFC server offers the execution of functions for other processes. On the other hand, the RFC client calls these functions. Since an RFC connection consists of a server and a client, function calls can only be made in one direction. Therefore, two RFC connections are required for communication between R/3 and communication systems.

- The first RFC connection transfers the data to be sent from R/3 to the communication system. Here the R/3 system is the RFC client and calls functions of the communication system, which the RFC server represents.
- The second RFC connection returns feedback about the success of the communication. It transports received messages from the communication system to the R/3 System. As an RFC client, the communication system calls functions in the R/3 system, which is the RFC server here.

These two directions of communication are considered separately below.

From R/3 to the communication system

A communication system is represented in the R/3 database by a SAPconnect node. A so-called RFC destination is assigned to this node. The attributes of this RFC destination are the information that R/3 needs to set up an RFC connection to a communication system. RFC destinations can be viewed and edited using transaction *SM59*.

If you start transaction *SM59*, you will find a large number of RFC destinations of different types. If an RFC destination is to be used for the SAPconnect interface, it must be of the *TCP/IP* type. This type is available in variants

- *Start*: When executing an RFC, R/3 starts an external program and waits for it to end.
- *Registration*: must be selected for SAPconnect. An external program registers with R/3 and waits for remote function calls.

Such RFC destinations have three attributes:

- Gateway host
- Gateway service
- Program ID

Example:
Gateway here is an R/3 process that handles communication with an external component. Gateway host is the network name or TCP/IP address of the R/3 application server through which communication is to run. Gateway service is the TCP/IP port to be used for this communication. Here you can either enter the port number directly (***3300-3399***) or the name defined by SAP (***sapgw00-sapgw99***). Usually the last two digits of the gateway service correspond to the system number of the R/3 system. Finally, the program ID is a unique name that is used to distinguish between different RFC partners that register on the same application server at the same port.

These three parameters are also sufficient for the other side of the RFC connection (*SAPCONNW*-Connector from OfficeMaster) to register with the SAP gateway. It must be ensured that the network and port names are also known on the computer on which the *SAPCONNW* connector is running. If you have configured the same gateway host, gateway service and program ID on the R/3 and *SAPCONNW* side and started the *SAPCONNW* connector, it is already possible to transfer fax jobs from the R/3 system to *SAPCONNW*.

In transaction **SM59** you can check the existence of this RFC connection with the function *test connection*. Alternatively, each registered system can be displayed via the menu sequence Go to > Registered Systems in the Gateway Monitor (transaction **SMGW**).

From the communication system to the R/3

In the opposite direction of communication, OfficeMaster transfers information to the R/3 system. The network name of the application server and the system or instance number of the system for which the message is intended are required to establish the connection. Normally, the application server here is the same computer that was specified as the gateway host for the RFC connection from the R/3 system to the communication system. Since exceptions are possible, both computer names can be configured separately in the configuration of the *SAPCONNW* connector.

If status messages for fax jobs or received faxes are to be transferred to the R/3 System, data in the R/3 System must be changed. This requires rights that can only be assigned to users. The communication system must identify itself as an R/3 user. To do this, a so-called CPIC or RFC user is created in R/3 with the rights required by the communication system. The communication system must transfer the logon data of this user to the R/3 system with every communication. The login data includes the name and password of the CPIC user and the name of the client for which the CPIC user was created.

Configuration Files

It may happen that the TCP/IP configuration of the computer on which the *SAPCONNW* connector is running needs to be adjusted. This is done by editing the hosts file and the services file.

The hosts file contains a mapping of names to TCP/IP addresses. On Windows, it is located in the %systemroot% \system32\drivers\etc directory and is named *hosts*. So if the name of the R/3 server cannot be resolved on the machine running the *SAPCONNW* connector, a line containing the name and IP address of the R/3 server is added to the hosts file.

The Services file contains a mapping of names to TCP/IP ports. It is located in the %systemroot%\system32\drivers\etc directory (on Windows) and is named *services*. If you use names of the form *sapgwXX* instead of the port numbers *33XX* in the _SAPCONNW_Connector configuration, add a line with the name and port number to the services file for each name used. These settings are made automatically by installing a SAPgui.

Create RFC destination

Transaction: SCOT or SM59

The *SAPCONNW* connector of the messaging server is represented in R/3 as a SAPconnect node. An RFC destination is assigned to this node, to which the requests are sent after conversion. The RFC destination can also be created during the installation of the node.

You can maintain the RFC destination with transaction *SM59* or with the node assistant of the SAPconnect administration. An RFC destination is created with *Create* in the toolbar.

RFC destination: Maintaining the RFC destinations involves system-wide settings. Since the RFC destination will later be linked to client-related settings of the SAPconnect node, a name with client number (e.g. _fercon*100* for SAPCONN connector for *client 100*) should be selected.

Connection type: The connection is made via TCP/IP, select **T** for this.

Activation type: The activation type must be set to “Registered server program”. Depending on the selection, the associated program ID can then be entered. To ensure clarity, the name of the destination (in the example: _fercon*100*) can be used (capital - & note lower case!).

Gateway options: The host name of the R/3 server is entered under Gateway host. The gateway service is the TCP port that SAPconnect uses to set up the RFC call to the SAPCONN connector. Enter **sapgwXX** here, where **XX** stands for the two-digit system or instance number of the R/3 system (e.g. *sapgw00*). Finally, the RFC destination is saved.

Create SAPconnect node

Transaction: SCOT, Menu: View > Node

Each SAPconnect node in SAP is created with the help of an R/3 wizard. In the *SCOT* transaction under the menu item View > Node, select the *Create Node* button from the toolbar.

First you will be prompted to enter the node name (e.g. *FERCON*) with description and the node type.

So that the RFC node can transfer send requests to the SAPCONNW connector via RFC, it needs an RFC destination. This can be entered in the subsequent dialog. It is created with the *RFC Destination* button. Then select the RFC destination and click *Next*.

Fax with SAPconnect via RFC

The creation of a node of the address type *Fax* is described below. The descriptions for *Internet-Mail* and *SMS* follow afterwards.

Address range:

In the next dialog, a fax address range for this node is specified so that outgoing fax messages are routed to it. This routing can be set using the recipient fax number. To set up only one SAPconnect node or SAPCONNW connector, “*” is entered in the address area.

If there are several SAPCONNW connectors (and thus several nodes), the address ranges for the individual nodes are divided (e.g. **CH*** for the node _FAX*Z* or **DE 030*** for the node _FAX*B*).

Document formats: In the next step, the document formats that can be processed by the messaging server are specified. The following document formats are possible for fax communication with SAP: *PCL* or *PS* (mutually exclusive), PDF, RAW and TIF (for forwarded faxes).

> **Note!**
> The converter component of the messaging server must be configured accordingly. If *PS* is used as the file format, *Ghostscript* must be installed as the conversion software.

The *PCL* and *TIF* formats are preferred, since the internal PCL converter can be used for them.

Documents in the R/3 internal document format (such as *ALI*, *SCR*) are converted to PCL or PS format in the R/3 spool. Depending on the previously configured document format, the printer driver *HPLJ5* (for PCL) or *POST2* (for PS) is specified as the device type. Optionally, the transmission times for the three different priority levels can be specified in the following dialog.

Configuration of the location: This is followed by the configuration of the location. The country code (e.g. *DE*) indicates the location of the OfficeMaster Messaging Server. This input is required for controlling the country code of the fax numbers (like *+49*).

After clicking on *Next* you can either add further address types (Internet mail and SMS) to the node or exit the configuration wizard.

If no further address types are to be added, settings for all address areas of the node can be made by selecting *No* in the following dialog.

Maximum waiting time for resend attempts: The interval for resend attempts (see Figure 10.10) is entered as the first setting for the entire node if an RFC error occurs during the transfer from R/3 to SAPCONNW.

Node can resolve path references/node should be monitored by the alert monitor: The checkboxes *Node can resolve path references* and *Node should be monitored by the alert monitor* should not be checked.

Node is operational: Finally, the *Node is operational* check box is checked.

Result:

The SAPconnect node *FERCON* was set up for the *SAPCONNW* connector. The node can be reconfigured if necessary.

Internet mail with SAPconnect via RFC

Equivalent to fax, a (further) address range is created for the node for sending Internet e-mails. The dialogs are adjusted accordingly. If only this SAPconnect node with Internet mail functionality is to be specified in the R/3 client, the entry * (asterisk) in the address area is sufficient.

The transmission of e-mails is usually not limited to any specific document format. Therefore, all document formats are generally supported.

If orders and lists in the *OTF*, *SCR*, *ALI* and *INT* formats are to be converted into externally understandable formats beforehand using SAPconnect, these formats should be excluded. To do this, select the option *All formats except the following* and add the above formats to the list by clicking the *SAP internal formats* button. In addition, the formats PCL and PS should be excluded from mailing.

The previous step presumably converts all internal SAP formats to PDF or HTM, depending on the conversion rules set. Thus, no device type is required.

All the settings required for e-mail have now been made. If desired, paging/SMS can be configured. Otherwise *No* is selected.

Paging/SMS with SAPconnect via RFC

Since R/3 Version 4.5, SAPconnect has supported the sending and receiving of short messages/SMS. A prerequisite is a configured SMS communication interface on the OfficeMaster Messaging Server. Under these conditions, *Pager* (=SMS) is selected as the address type.

When configuring the address range for this node, the short messages are routed to the node. If only this SAPconnect node is to be addressed with SMS functionality, * is entered in the address area. Pager subtypes such as *E+.** or *02:017** can be specified for a more precise specification.

RAW data (ASCII) are supported for the transmission of short messages. In order to convert the R/3 internal data (e.g. SCR) into RAW, ASCIIPRT is required as the device type.

Configure SAPconnect node (optional)

Since SAP 4.7, external formats must be set for the four internal SAP formats, depending on the service. There is no need to configure conversion rules, output devices or supported document formats. The following table provides an overview of the recommended target formats.

SAP internal formats	**Fax**	**SMS/Pager**	**Internet Mail**
SAPscript/Smart Forms	PCL or PS	TXT	PDF
ABAP list	PCL or PS	TXT	HTM
Business Object/Reference	TXT	TXT	HTM
RAW Text	TXT	TXT	TXT

10.20.2. RFC connector (SAPCONN)

The connection of an R/3 system to the messaging server takes place via the gateway component SAPCONNW with a Netweaver connection. At least one gateway component must be created, configured and operated as a connector for each SAP client. To do this, select in the quick launch bar > SAP > RFC in the messaging server configuration.

All created connectors are displayed on the left side. The selected SAPCONNW connector can be configured on the right side. If no connector is displayed, the corresponding SAPCONNW connectors must be created using the *Add* button.

Create RFC connector

A new component of type SAPCONNW is created for the messaging server. A SAPCONN connector is set up for each SAP client or for each SAPconnect node.

Since the connectors are numbered consecutively by name, it is advisable to use descriptive display names in order to simplify administration later. For example, the SAP system abbreviation and the SAP client number can be used in the display name, resulting in names like *SAP DEV 100*. Once the component has been created, it can be configured.

Test sending faxes via SAP GUI

R/3 user administration

Transaction: SU01 or SU51

R/3 users should be assigned fax numbers, radio numbers and e-mail addresses in the R/3 user master for the following reasons:

- Only users with a sender address in the desired communication type are allowed to send messages in this way, i.e. only users with a fax number are allowed to fax.
- The maintained sender number or e-mail address is also communicated to the recipient as the sender address.
- Received faxes, short messages and e-mails are assigned via the phone numbers or e-mail addresses maintained in the R/3 user master.
- In the log files of the SAPCONN connector, the operations of a specific R/3 user are identified by their sender address in the R/3 user master.

Of course, the fax number can also be maintained in transaction SU51 (System > User settings > User address).

Messaging

Transaction: SCOT, in the menu sequence View > Jobs

The R/3 internal program *RSCONN01* is responsible for transferring the messages from R/3 to OfficeMaster via RFC. In order for this to happen, a job is scheduled that starts the program every 10-15 minutes. Depending on how sensitively communication is handled in a company, the interval for program execution should be selected. It should not be less than 5 minutes.

The process is activated with *Schedule sending process* in the toolbar of the SAPconnect administration and the input of a name for the job is expected.

Then the variant *FAX* is selected with the cursor and confirmed with *Schedule*.

The time interval for the program starts of *RSCONN01* can be entered via *Schedule periodically*. The first start date is generally one hour in the future. After saving these settings, the job is scheduled.

The procedure is analogous with Internet mail and pagers/SMS.

To test the configuration, the transmission of faxes, short messages and e-mails can also be started manually and not job-controlled. This is also possible in the SAPconnect administration. The *Start send process* button is available for this. *FAX*, *Pager*, *INT* or "*" is selected as the address type. Alternatively, the transfer program (*RSCONN01*) can be started in transaction *SE38*.

> Note!
> Another very useful R/3 program is *RSCONN05*. It allows faxes with errors to be resent without having to recreate the documents using the R/3 applications (such as MM, SD, etc.). This program can be accessed via transaction *SOST* or the menu sequence Utilities > Overview of send requests. More information is available in SAP note number *92287*.

Test message with SAP Business Workplace

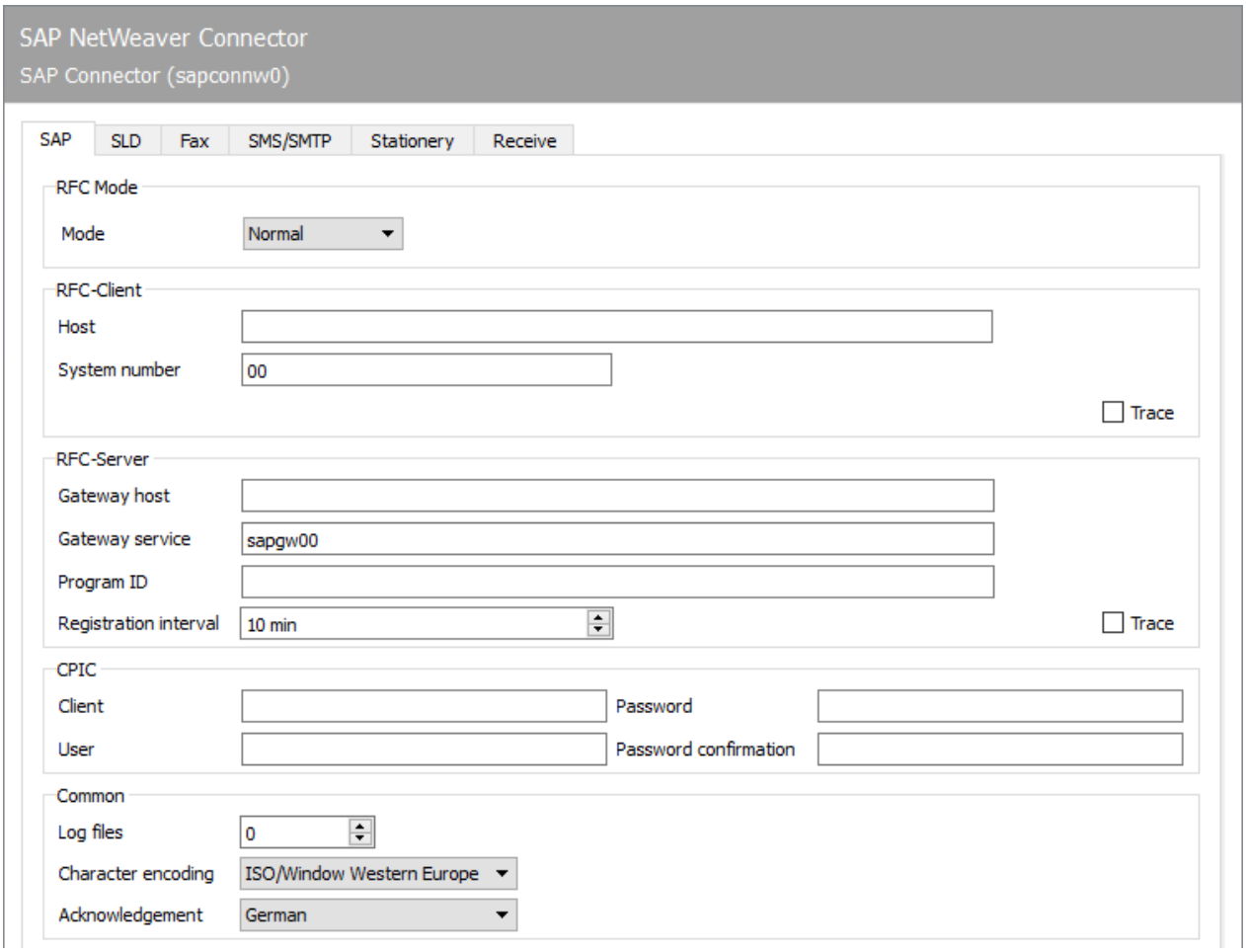
In order to send a test message from SAP, both the messaging server and the connectors must be started. You log on to R/3 with the *SAPgui*. A new message is now created in the Business Workplace (transaction *SBWP*). The recipient number must be entered in the syntax *<country code> number* (e.g. ***DE 0123456***, ***US 555-$^{456}/_{89}$***), which is automatically generated by the R/3 recognized as a fax number.

With the _Send_button from the toolbar, the document is saved as a send order in the office outbox. Here it waits for the ABAP program *RSCONN01* to transmit it to the connector. The current transmission status of the document can be read at any time on the *Recipient list* tab in the office exit. This tab is associated with the message.

The status of other SAP documents, such as B. Orders. The SAP applications use the Business Workplace as a transport medium and therefore store the fax jobs in the office outbox. A document has the following status messages in the course of sending:

R/3 release	**Version 6.x**
Before RSCONN01	Waiting
After RSCONN01 and before completion of sending by the fax server	Message passed from node ... to communication system
After successful completion of sending by the fax server	Delivery to ...
After the fax server failed to complete the transmission	No extradition

If the document cannot be sent, the R/3 sender also receives an express document, which draws his attention to this fact.



10.20.3. SAP

The first configuration steps for the *SAPCONNW* component relate to the direct connection to the SAP system and are carried out on the *SAP* tab.

RFC mode

The type of RFC connection is determined in the *RFC mode* area. The choice made here changes the input options of the tab:

Mode

*normal
In RFC mode *Normal*, both the RFC server and the RFC client connection take place without load balancing. This is the standard case, i. H. this setting applies to most of the installation.

- Load balancing
  In *RFC mode load balancing*, the RFC client connection is subject to load balancing. Since this setting only affects incoming messages and status messages, this option only makes sense for a very small number of installations.

*RFC-INI
The *RFC mode RFC INI* is only intended for experts who want to manually describe the RFC connection in the configuration file *saprfc.ini*.

> Note!
> For most installations, *Normal* is sufficient as the RFC mode.

RFC client

In this area, information about the RFC inbound connection from *SAPCONNW* to the R/3 system is made (depending on the *RFC mode*).

Host, system number *(normal in RFC mode)*

With RFC mode *Normal*, the TCP/IP address or the resolved name of the R/3 application server must be entered as *Host*. The two-digit system or instance number of the R/3 system is required as the *system number*. This number can e.g. read in the SAPlogon program.

Host, name, group (in RFC mode *load balancing*)

In the RFC mode *Load Balancing* the TCP/IP address or the resolved name of the R/3 application server that provides the load balancing must be entered as *Host*.

name is the name of the R/3 system and *group* is the name of the group of R/3 application servers with load balancing. If such systems are available, you can also find this information in the SAPlogon program of the SAPgui.

RFC section (in RFC mode *RFC INI*)

The section in *saprfc.ini* that describes the RFC connection to the R/3 System is specified (note the use of upper and lower case!).

Trace (all modes)

Regardless of the RFC mode, the RFC trace can be activated/deactivated with *Client-Trace*. The trace files are stored in the work directory of the SAPCONNW connector. The work directory is in %ProgramFiles%\FFUMS\FMSRV\work\SAPCONN.

RFC server

Here the RFC outbound connection from the R/3 system to *SAPCONNW* is configured. This information must be the same as the information in R/3, and must therefore be configured later in R/3 for the RFC destination (SM59).

Gateway host, gateway service (in RFC mode *normal* and *load balancing*)

The TCP/IP address or the resolved name of the R/3 application server (normal RFC mode) or the computer on which the SAP gateway is running (load balancing) must be specified as *Gateway host*. The resolved TCP/IP port over which the RFC connection is to run is specified under *Gateway service*. The gateway service name (e.g. *sapgw00*, *sapgw01*) may need to be resolved on the server in the *services* file.

Program ID (in RFC mode *normal* and load balancing)

A unique name is configured as the *program ID* under which SAPCONNW registers itself in R/3. R/3 uses this program ID to find the *SAPCONNW* connector. For this purpose, the same program

ID is stored in R/3 in the RFC destination assigned to the SAPconnect node (Note: upper and lower case letters!).

RFC section (in RFC mode *RFC-INI*)

In RFC mode *RFC INI*, the section in *saprfc.ini* that describes the connection from the R/3 system to SAPCONNW must be specified as *RFC-Dest.* (note the use of upper and lower case!).

Registration interval (all modes)

After the connector is started, *SAPCONNW* registers itself with the configured *program ID* on R/3. This registration allows transmission jobs to be transferred to the connector via the RFC server connection (SM59) configured in R/3. Since the R/3 system in some environments e.g. *SAPCONNW* repeats the registration at the *registration interval* set here. If the new registration were not carried out, the R/3 could not have a registered connector after the restart, which would lead to an RFC error for all send requests.

Trace (all modes)

Regardless of the RFC mode, the *Server Trace* can be activated/deactivated. The trace files are then in the work directory of *SAPCONNW* (as above).

CPIC

A *CPIC* or RFC user account, which must be created as a service account for *SAPCONNW* in R/3, is specified here.

Tenant, User, Password, Confirm Password:

To do this, enter the three-digit number of the R/3 client in *Mandant* in which the CPIC user account is created. The R/3 user name of the CPIC user account is specified as *user*. Finally, the password of the CPIC user account is stored in the fields *Password* and *Confirm password*.

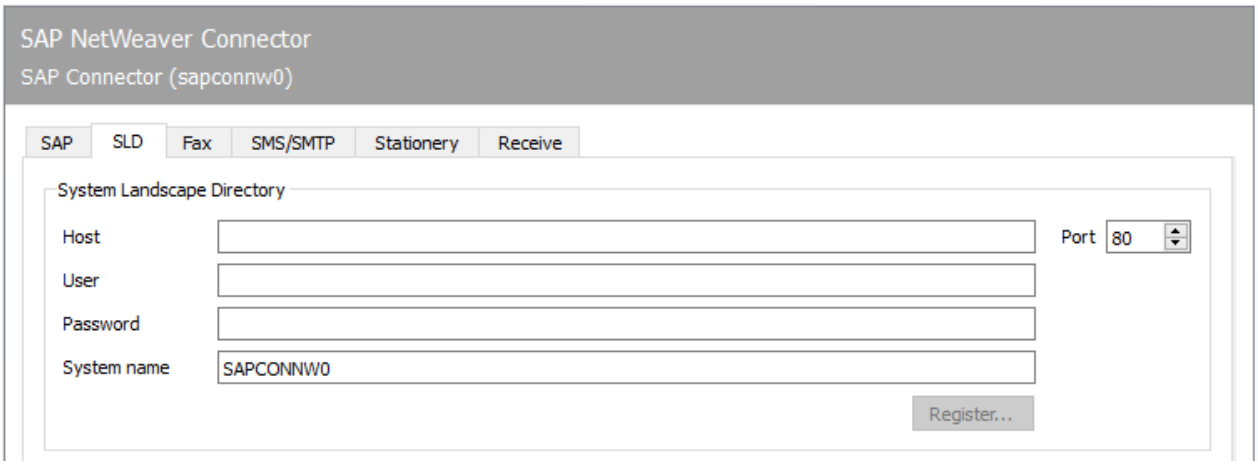
General

Log files

In addition, *SAPCONNW* can log the connection to R/3 daily in a so-called communication log. To do this, enter the number of days under *Log files* for how long a communication log should be kept. If all log files are to be saved, configure the value **0*.

Character encoding

If R/3 sends unformatted files as text (TXT or RAW), the *character encoding* cannot be taken from them. Since faxes are mostly sent as formatted files in PCL, PS or PDF, this mainly applies to short messages (SMS) and e-mails. If the character encoding of the file does not match the *SAPCONNW* setting, individual characters in the file may be converted incorrectly.



10.20.4. SLD

System Landscape Directory

All information about an IT system landscape in the SAP environment is stored in the System Landscape Directory (SLD). This information is used both to inform the employees responsible in SAP customer support and to provide the customer's employees with an overview of the installed system landscape and the communication channels.

Host

Name of the server that provides the System Landscape Directory in this environment.

User

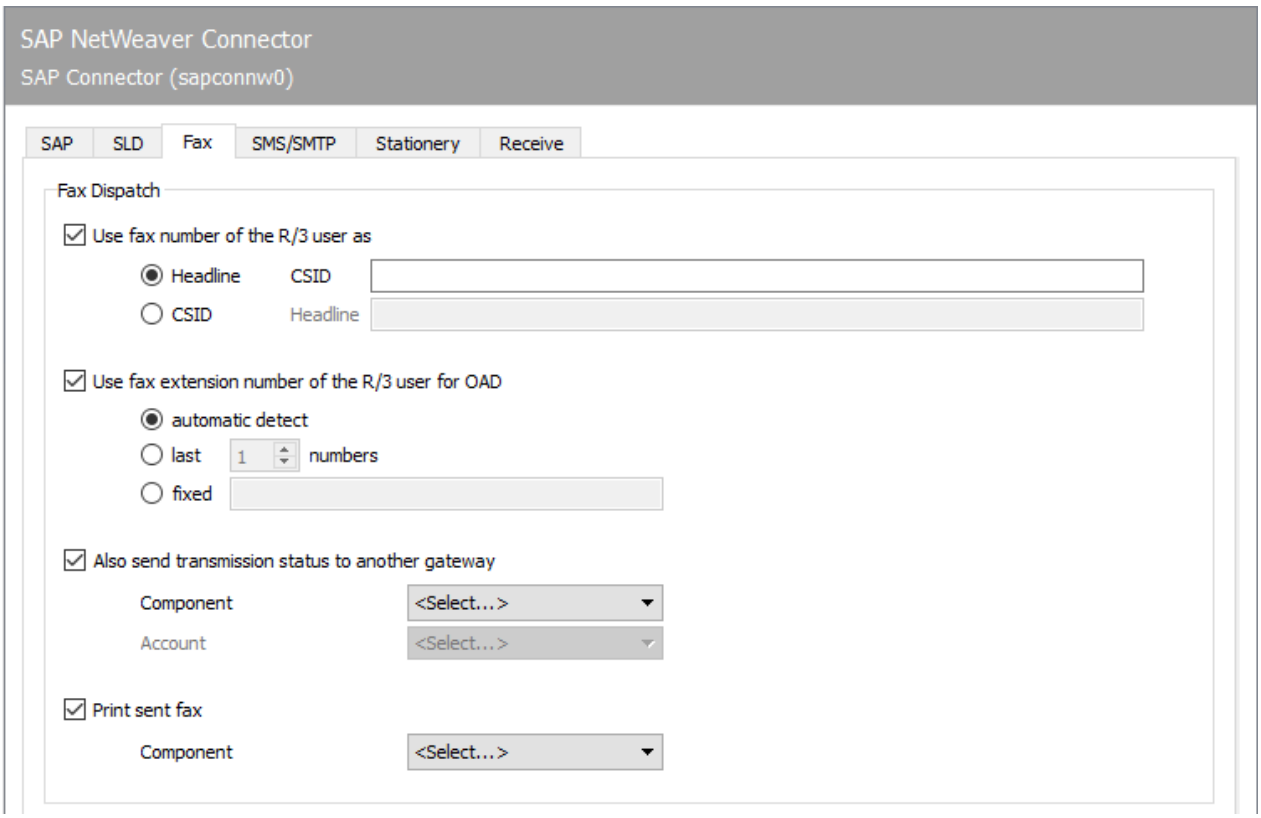
Name of a user who is authorized to make entries in the System Landscape Directory.

Password

User password for authentication in the System Landscape Directory.

System name

SLD name of the OfficeMaster Suite system under which the SLD entry is made.



10.20.5. Fax

Fax dispatch

Use fax number of R/3 user as ...

A separate fax identifier can be determined for each transmission process, which is communicated in the fax log and entered in the header. If no values are maintained for *Fax-ID* and *Header* for *SAPCONNW*, the default values configured in OMCUMS or in DirectSip are used.

Selection	ID	Header
(disabled)	as stored for OMCUMS/SIP	as stored for OMCUMS/SIP
Header	as defined for SAPCONNW	Fax number of the R/3 sender
identifier	Fax number of the R/3 sender	as defined for SAPCONNW

Use fax extension of R/3 user or fixed value for OAD

The connector supports two modes for determining the sender number or the *Originator Address Digit (OAD)*, which is communicated to the telephone system for send requests from *SAPCONNW* by *OMCUMS* or *SIP*:

- A fixed OAD is always transmitted (regardless of whether OMCUMS or SIP is used). Selection: ***fixed***

or

- The OAD is determined for each transmission depending on the fax number stored in R/3 for the sender.

In the latter case, the OAD can be *determined* ***automatically*** from the fax sender number or the ***last x digits*** of the fax sender number are used for this. The number that was stored in R/3 as the fax extension for the user is used for automatic determination.

Also transmit the transmission status to another gateway

In addition to the status message in R/3, the messaging server can send the final send status to the user via other components configured in the messaging server.

The user information that is forwarded to the selected connector consists of the fax number as assigned to the sender in the R/3 user master, including the country code - but in the normalized state.

The normalized fax number must be assigned to the user or object (database, distribution list, group) in Active Directory (for Exchange) or in the name and address book (for Notes) to which the send status is to be sent.

In the Active Directory, the assignment is made using an additional FAX address that is distributed to the user.

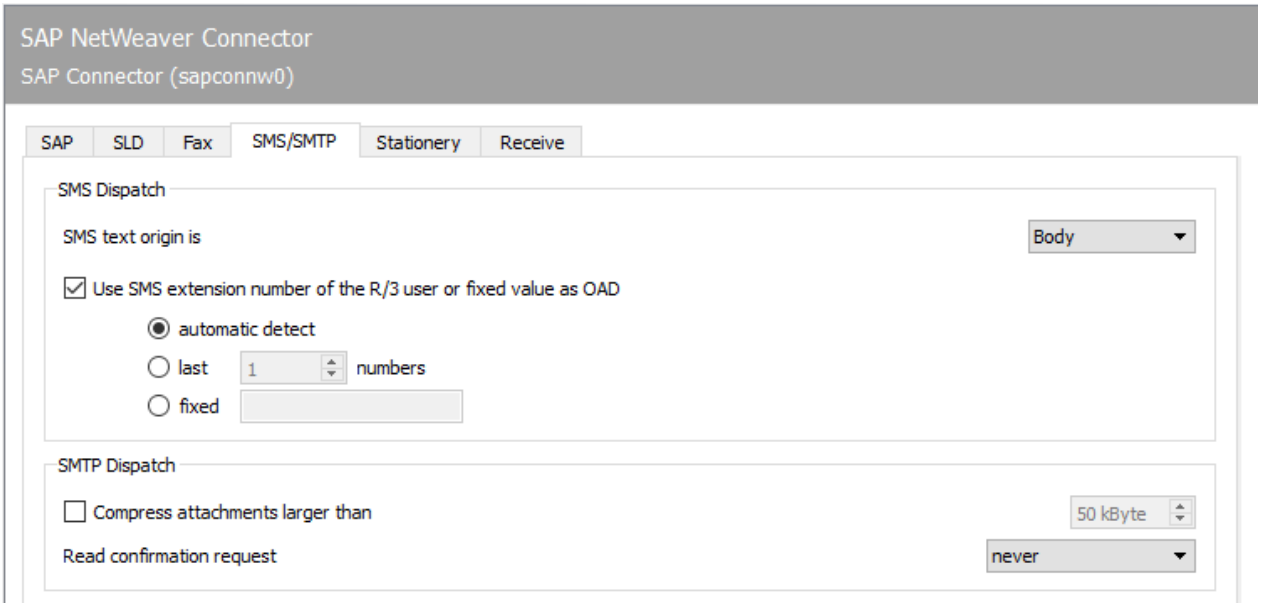
In the name and address book, the normalized number is usually entered as an additional alias for the user.

Normalization of phone numbers:

Country	Original value	Normalized value
Germany	03328-455-960	493328455960
Austria	01-23456-77	4312345677

Print sent faxes

OfficeMaster Messaging Server can optionally output the faxes sent by *SAPCONNW* to a network printer after they have been sent. To do this, a print component *PRINTGW* must first be set up in the messaging server. The corresponding *PRINTGW* is then selected as a *component* on the connector.



10.20.6. SMS/SMTP

Sending SMS

SMS text origin

While fax messages and e-mails consist of several pages or files, a short message/SMS is limited to text. In SAP documents, the subject line and/or the message text come into consideration for this text. Accordingly, either the text from the subject line, from the message text or from the subject line and message text can be used as the origin of the SMS text.

If the resulting SMS text exceeds the maximum number of 160 characters permitted for a short message/SMS, the message can be split into several short messages. The maximum number of short messages to which a message should be distributed can be specified under Extras > System settings.

Use the R/3 user's SMS extension or a fixed value for OAD

In the latter case, by ticking this checkbox, a number that differs from the ISDN or SIP configuration can be specified as the SMS sender number or OAD, which is communicated to the telephone system when the call is set up. The mobile phone number assigned to the SAP user in the R/3 user master is used as the SMS sender address. In general, two modes are possible:

- A fixed OAD is always transmitted (regardless of whether OMCUMS or SIP is used). Selection: ***fixed***

or

- The OAD is determined for each transmission depending on the mobile phone number stored in R/3 for the sender.

In the latter case, the OAD can be *determined* ***automatically*** from the fax sender number or the ***last x digits*** of the cell phone sender number are used for this. The number that was stored in R/3 as the mobile phone number for the user is used for automatic determination.

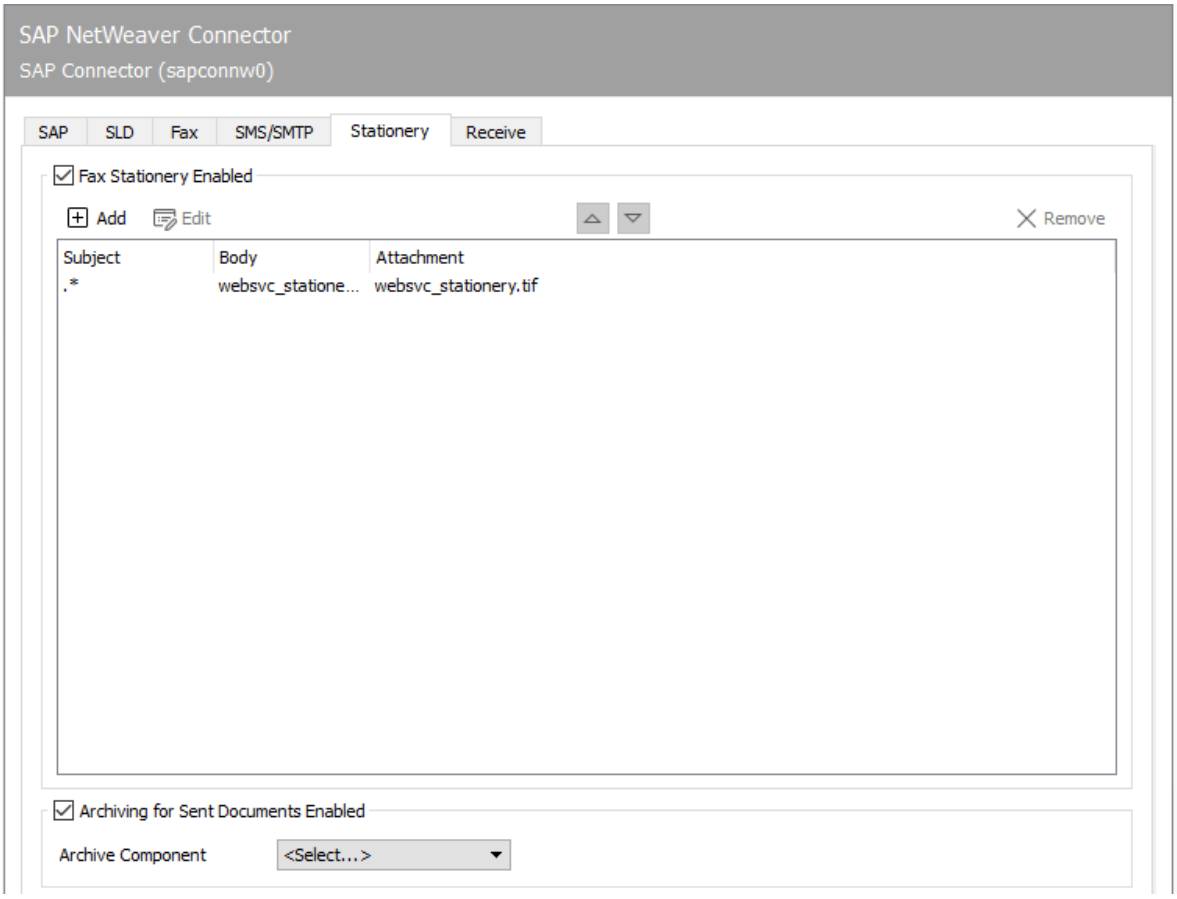
SMTP dispatch

Compress attachments larger than

For sending e-mail attachments, the size of file attachments in kByte can be specified with *Compress attachments larger than*, from which the OfficeMaster Messaging Server should automatically pack the file attachments in ZIP archives.

Request read receipt

- Never
- According to SAP order
- Always



10.20.7. Stationery, archiving

Enable fax stationery

Not all messages from R/3 are permanently provided with stationery or an electronic signature. These two functions can be activated via the *Stationery/Signature* tab, depending on the subject line contained in each transmission.

Archiving of sent documents enabled

An archiving interface can be selected for all documents sent via the RFC connector.

10.20.8. Stationery

If *fax stationery is activated*, different stationery can be stored. Clicking on *Add* opens a dialog in which the necessary settings can be made. A graphic file can be specified here, which is stored as stationery for outgoing messages and their file attachments. The stationery is stored on the messaging server in the %Programdata%\FFUMS\data\stationery\ subdirectory. The graphic must be saved as a TIF or as a DCX (multi-page PCX) in black and white with a width of 1728 pixels and a height of 2200 pixels (recommendation).

Filters

Regarding

Which stationery to use is decided based on the content of the subject line, which is applied in the form of regular expressions. The regular expression **.*** (dot + asterisk) stands for a subject line with any content.

Body/Attachments

Stationery

If documents with the subject line ***Offer 123xyz*** are to be assigned a special stationery, this stationery can be added to the list using a rule with the regular expression **Offer.***. For multi-

page stationery, a mode should be specified for how the stationery is to be used by the messaging server. The following modes are available:

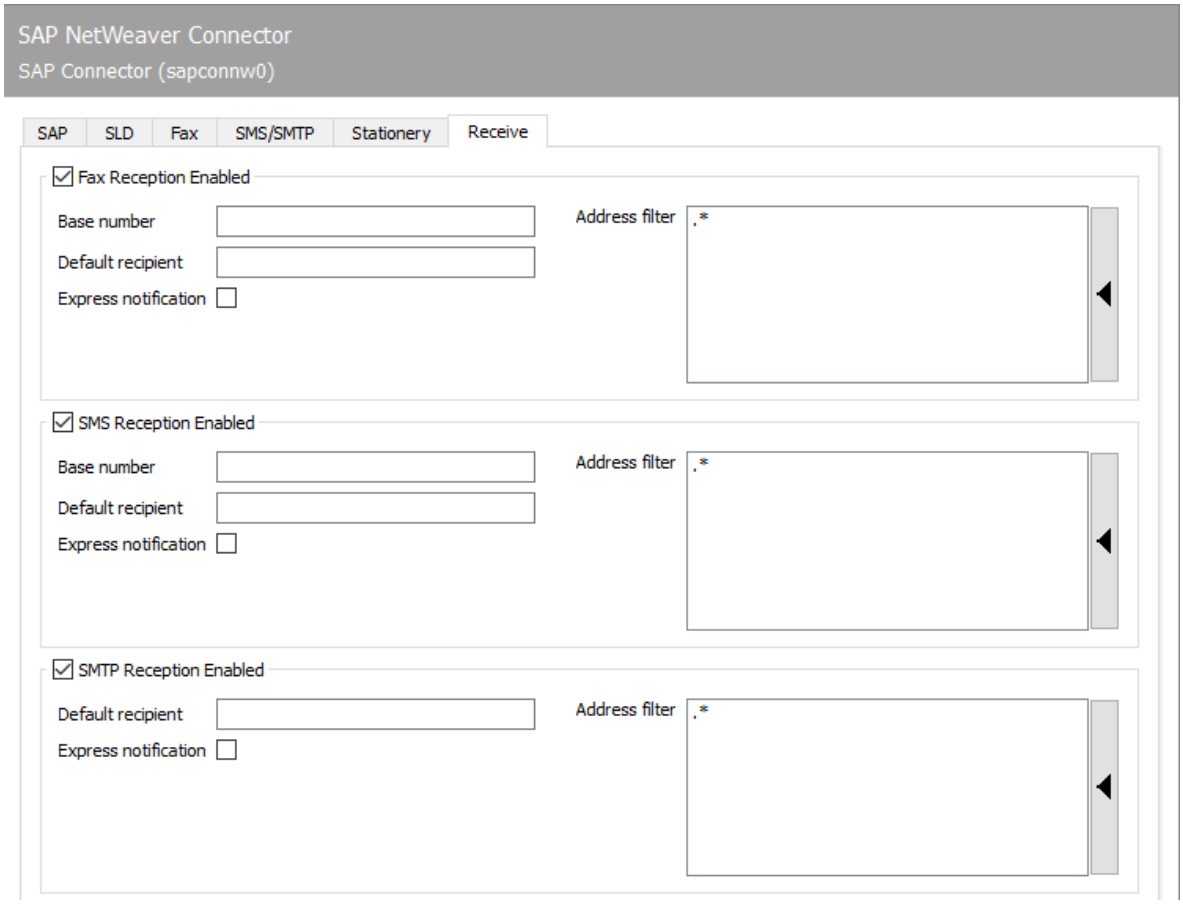
- No stationery
- Use first page only
- Use all pages
- Repeat first page,
- Repeat last page

The stationery configuration can be made differently for the first document and for subsequent documents.

Pixel Options

In addition, you can specify the *pixel operation* to be performed when using the stationery.

- With the pixel operation *or* (or; real stationery), a pixel is black as soon as the pixels that belong together in the send document or in the stationery are black (otherwise white).
- With the pixel operation *xor* (exclusive or fake stationery), a pixel is black in the result as soon as the pixels in the sending document or stationery are black. If both pixels are black, the result is that the pixel is white.



10.20.9. Reception

Fax reception activated

Base Number

If fax reception is activated, faxes are delivered to the corresponding R/3 user in the SAP Business Workplace (transaction *SBWP*). For fax reception, the trunk fax number with country code of the country specified for the users in R/3 must be configured as *Base Number* (e.g. $+^{493328}/_{455}$ - if the user in R/3 country information Germany and the fax number *03328 /455 960* was assigned to the user master). The country code must be specified with a *plus sign* (**+** , no double zero).

Default recipient

In addition to the base number, the full phone number of the R/3 user (master fax number plus extension or called party number) is required as the standard recipient, to whom all received

faxes that cannot be assigned to an R/3 user are delivered. The input notation corresponds to the base number (see above).

Address filter

In addition, an address filter must be stored that specifies which faxes are to be reported from *SAPCONNW* to R/3. The address filter is maintained in the form of regular expressions. If fax reception is desired in R/3, the connector receives all faxes received from the messaging server with the entry **.*** (dot + asterisk). If the address filters of several connectors overlap, each applicable connector gets the incoming faxes.

SMS reception activated

Base number, default recipient

Similar to fax reception, SMS reception can be activated so that short messages received from the messaging server are also transferred to R/3. As with fax reception, you need the *base number* and a *standard recipient*. Both specifications are configured with the same notation as for fax (see previous section). However, the cell phone number stored for the user in the R/3 user master record is used for comparison when receiving SMS messages. Furthermore, an address filter in the form of regular expressions must be specified, which is applied to the addresses of the short messages (SMS) received.

SMTP reception enabled

Default recipient, address filter

E-mails received by the messaging server are delivered to the recipient in the *SAP Business Workplace*. For receipt, a user's e-mail address must be stored as the *standard recipient*, to which all messages are delivered whose recipient addresses are not maintained in R/3. In addition, *SAPCONNW* requires an address filter in the form of regular expressions, which is also applied here to the e-mail address of received messages.

10.21. SAP connect via SMTP

10.21.1. Transaction: *SCOT*, Menu: View > Nodes

In contrast to the RFC variant, no separate SAPconnect node has to be created when connecting via SMTP. Since fax and SMS send orders are sent to OfficeMaster's SMTP gateway by e-mail, the SAPconnect node that already exists for e-mail is used.

> **Note!**
> The use of the SMTP-based SAPconnect variant requires profile settings on the SAP Web Application Server (*WAS*) used. Details on these settings can be found in SAP Note *455140* "*Configuration email, fax, paging/SMS via SMTP*".

For configuration, switch to the SAPconnect administration using transaction *SCOT* and select the menu sequence View > Nodes. All existing SAPconnect nodes are displayed here.

Since SAP R/3 version 4.7, the node *SMTP* is initially supplied. Via this node, e-mail send orders are transmitted to the company's internal mail server via SMTP. To configure, double-click the node.

SMTP connection

Mail Host, Mail Port

The fully qualified name or the IP address of the company's internal mail server to which SAPconnect forwards the mails via the *WAS* is specified as the mail host. In addition to the IP address, the port number is required on which e-mails are received by the mail server. This is usually the standard port 25 for receiving mail.

The fax and SMS send orders are first sent by SAPconnect by mail to the configured mail host, which then forwards them to OfficeMaster. Forwarding is based on the computer and domain information to which the emails are sent. For configuration, select the button *Set fax* or *Set SMS*.

Address ranges

Regardless of whether it is an RFC or SMTP node, each node is assigned an address range. This address range refers to the recipient's address, i.e. the fax number or the email address of the recipient.

If SAPconnect has several active nodes in a client that support a communication service (e.g. several nodes for fax), the send areas must be divided. For this purpose, all relevant addresses are stored in a list. “*” (asterisk) can be used as a wildcard within the list.

> **Example:**
> If the node is to send all faxes to Germany and Austria, for example, the two address ranges *DE** and *AT** must be specified in the list. If a node is only to process faxes to Berlin, enter *DE030** as the address range. In most cases, however, all faxes should be sent to the same node so that its address range can be reduced to the entry “*” (asterisk).

Output formats for SAP documents (only for fax)

Before being handed over, documents in SAP’s internal format are converted into a format that can be further processed externally. OfficeMaster Messaging Server has its own converters for PCL and TXT. The following formats should be set by default:

Document form	**Format**
SAPscript / Smart Forms	PCL
ABAP list	PCL
Business Object / Reference	TXT
RAW Text	TXT

If necessary, SAPconnect can also convert documents of the type SAPscript / Smart Forms and ABAP list to PDF or PS.

> **Note!**
> The transfer format should only be changed to PS or PDF if there are significant layout differences between the PCL generated by SAPconnect and the PDF/PS generated for the same document.

Translation of the internet address

So that the mail server can distinguish between e-mails and faxes and short messages and forward them to OfficeMaster, SAPconnect sends these send requests to a specific mail domain that is stored as a domain in the *Translation of the Internet address* area.

Mail routing for this address must be set in the mail server so that all mails for this domain are routed to OfficeMaster.

Example:
The domain *SAPSMTP_DEV_100.company.local* was specified in the configuration example (see Figure 10.23). SAPconnect sends
Faxes to the address *fax=rufnummer@SAPSMTP_DEV_100.company.local* und
SMS to _sms=rufnummer@SAPSMTP_DEV*100.company.local*.

Attention!
The domain stored here must also be used for the email address configured for the SMTP gateway of the messaging server.

10.22. SAPSMTP gateway (for SAP via SMTP)

In SAP version 4.7 with SAP Web Application Server from version 6.10, *SAPconnect* can be operated on an SMTP basis. The associated gateway on the part of OfficeMaster is provided by the SAPSMTP component. The configuration is done in the *Messaging Server Configuration* via the quick launch bar > SAP > SMTP.

> Note!
> The SMTP gateway for SAP requires that the messaging server has correctly configured components for sending and receiving mail (*SMTPTX*, *SMTPRX*).

10.22.1. Create SAPSMTP gateway

An SMTP gateway is created in the quick launch bar of the messaging server > SAP > SMTP -> via the *New SAP connector* button from the SAPSMTP configuration. With the help of the starting assistant, a SAPSMTP gateway is set up for each SAP client or for each SAPconnect node.

Since the SAPSMTP gateways are numbered consecutively by name, it is advisable to use descriptive display names to simplify administration later. For example, the SAP system abbreviation and the SAP client number can be used in the display name, resulting in names like ***SAP_DEV_100***.

Test sending faxes via SAP GUI

R/3 user administration

Transaction: SU01 or SU51

R/3 users should be assigned fax numbers, radio numbers and e-mail addresses in the R/3 user master for the following reasons:

• Only users with a sender address in the desired communication type are allowed to send messages in this way, ie. H. only users with a fax number are allowed to fax.

• The maintained sender number or e-mail address is also communicated to the recipient as the sender address.

• Received faxes, short messages and e-mails are assigned using the phone numbers or e-mail addresses maintained in the R/3 user master.

• In the log files of the SAPCONN connector, the processes of a specific R/3 user are identified by their sender address in the R/3 user master.

Of course, the fax number can also be maintained in transaction SU51 (System > User settings > User address).

Messaging

Transaction: SCOT, in the menu sequence View > Jobs

The R/3 internal program *RSCONN01* is responsible for transferring the messages from R/3 to OfficeMaster via RFC. In order for this to happen, a job is scheduled that starts the program every 10-15 minutes. Depending on how sensitively communication is handled in a company, the interval for program execution should be selected. It should not be less than 5 minutes.

The process is activated with *Schedule sending process* in the toolbar of the SAPconnect administration and the input of a name for the job is expected.

Then the variant *FAX* is selected with the cursor and confirmed with *Schedule*.

The time interval for the program starts of *RSCONN01* can be entered via *Schedule periodically*. The first start date is generally one hour in the future. After saving these settings, the job is scheduled.

The procedure is analogous with Internet mail and pagers/SMS.

To test the configuration, the transmission of faxes, short messages and e-mails can also be started manually and not job-controlled. This is also possible in the SAPconnect administration. The *Start send process* button is available for this. *FAX*, *Pager*, *INT* or "*" is selected as the address type. Alternatively, the transfer program (*RSCONN01*) can be started in transaction *SE38*.

> Note!
> Another very useful R/3 program is *RSCONN05*. It allows faxes with errors to be resent without having to recreate the documents using the R/3 applications (such as MM, SD, etc.). This program can be accessed via transaction *SOST* or the menu sequence Utilities > Overview of send requests. More information is available in SAP note number *92287*.

Test message with SAP Business Workplace

In order to send a test message from SAP, both the messaging server and the connectors must be started. You log on to R/3 with the *SAPgui*. A new message is now created in the Business Workplace (transaction *SBWP*). The recipient number must be entered in the syntax <*country*

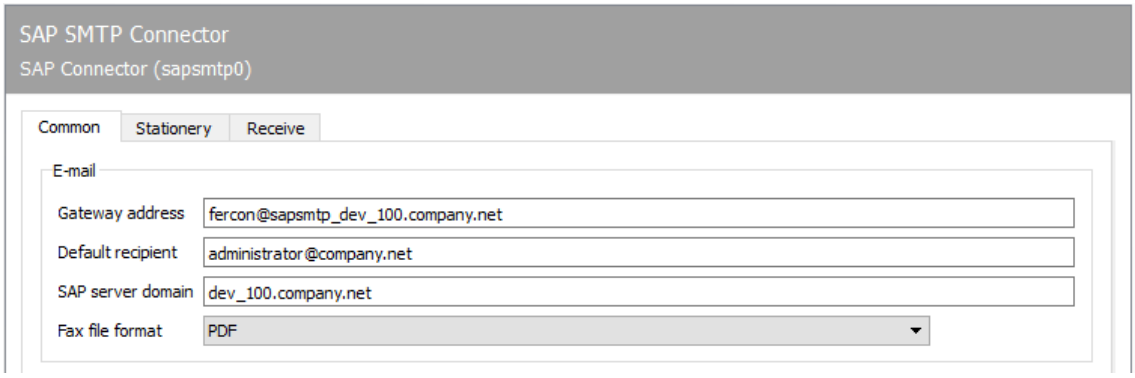
code> number (e.g. ***DE 0123456***, ***US 555-$^{456}/_{89}$***), which is automatically generated by the R/3 recognized as a fax number.

With the _Send_button from the toolbar, the document is saved as a send order in the office outbox. Here it waits for the ABAP program *RSCONN01* to transmit it to the connector. The current transmission status of the document can be read at any time on the *Recipient list* tab in the office exit. This tab is associated with the message.

The status of other SAP documents, such as B. Orders. The SAP applications use the Business Workplace as a transport medium and therefore store the fax jobs in the office outbox. A document has the following status messages in the course of sending:

R/3 release	**Version 6.x**
Before RSCONN01	Waiting
After RSCONN01 and before completion of sending by the fax server	Message passed from node ... to communication system
After successful completion of sending by the fax server	Delivery to ...
After the fax server failed to complete the transmission	No extradition

If the document cannot be sent, the R/3 sender also receives an express document, which draws his attention to this fact.



10.22.2. General

email

Gateway address

Receipt processes and status messages are sent to SAP by the SMTP gateway as an e-mail. With these SMTP mails, the value configured for the SMTP gateway is used as the sender address.

> Note!
> In addition, the domain specified for the SMTP gateway after the asterisk (in the example "_sapsmtp_dev*100.company.local*") is used to assign e-mails received from the SMTPRX component of the messaging server to the SMTP gateway. The domain specification must must therefore be the same as the fax domain used in the SAPconnect node.

Default recipient

All processes that were created by unauthorized users or that cannot be assigned to a user are forwarded to the e-mail address specified as the default recipient.

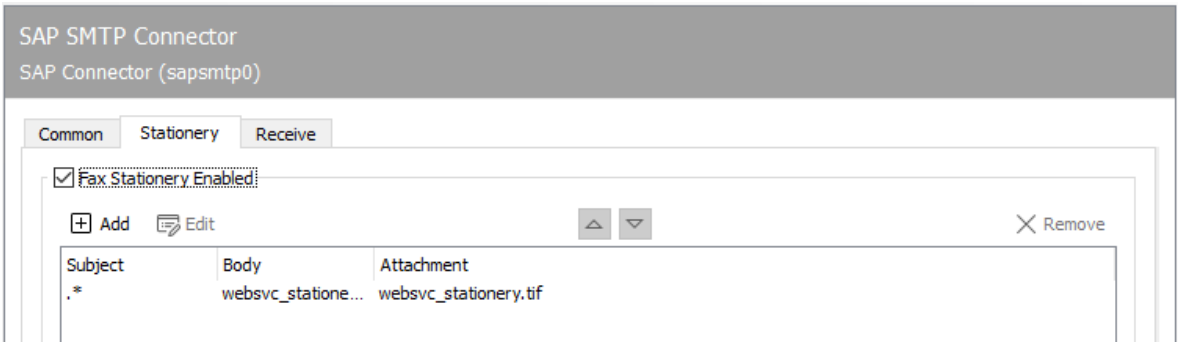
SAP server domain

Name of the SAP server domain.

File format for fax

Faxes that have been received or sent are delivered to the user as a file attachment to an e-mail. The fax file can be delivered in the following file formats:

- TIF (G4 or MH),
- PDF (not searchable) and
- PDF-OCR, provided the messaging server has a licensed *OfficeMaster OCR* installation *OCR (Optical Character Recognition)*"



10.22.3. stationery

Enable fax stationery

Not all messages from R/3 are permanently provided with stationery or an electronic signature. These two functions can be activated via the *Stationery/Signature* tab, depending on the subject line contained in each transmission.

10.22.4. Stationery

If *fax stationery is activated*, different stationery can be stored. Clicking on *Add* opens a dialog in which the necessary settings can be made. A graphic file can be specified here, which is stored as stationery for outgoing messages and their file attachments. The stationery is stored on the messaging server in the %Programdata%\FFUMS\data\stationery\ subdirectory. The graphic must be saved as a TIF or as a DCX (multi-page PCX) in black and white with a width of 1728 pixels and a height of 2200 pixels (recommendation).

Filters

Regarding

Which stationery to use is decided based on the content of the subject line, which is applied in the form of regular expressions. The regular expression .* (dot + asterisk) stands for a subject line with any content.

Body/Attachments

Stationery

If documents with the subject line ***Offer 123xyz*** are to be assigned a special stationery, this stationery can be added to the list using a rule with the regular expression **Offer.***. For multi-page stationery, a mode should be specified for how the stationery is to be used by the messaging server. The following modes are available:

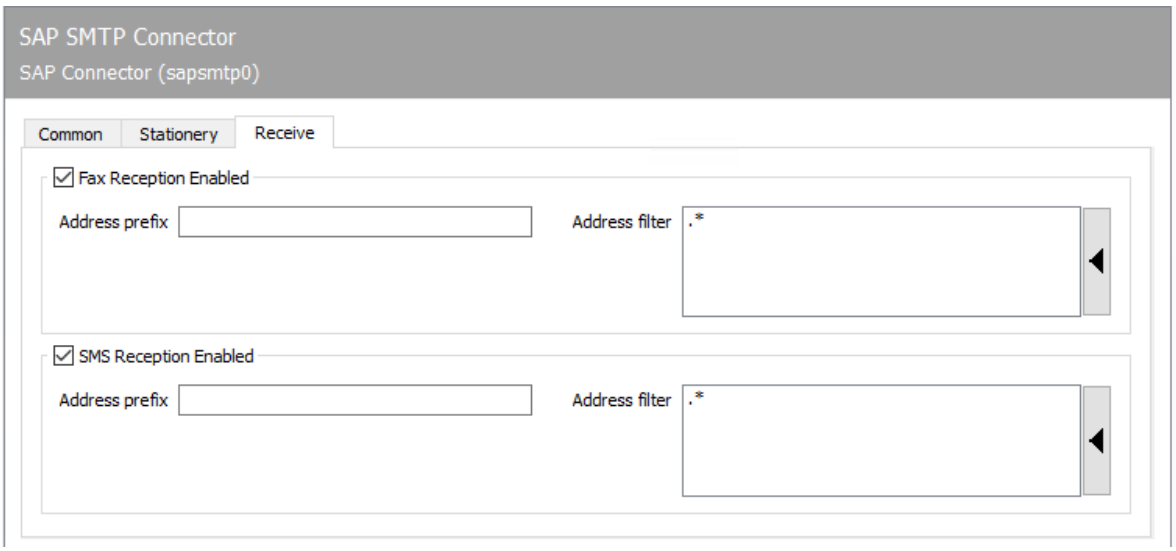
- No stationery
- Use first page only
- Use all pages
- Repeat first page,
- Repeat last page

The stationery configuration can be made differently for the first document and for subsequent documents.

Pixel Options

In addition, you can specify the *pixel operation* to be performed when using the stationery.

- With the pixel operation *or* (or; real stationery), a pixel is black as soon as the pixels that belong together in the send document or in the stationery are black (otherwise white).
- With the pixel operation *xor* (exclusive or fake stationery), a pixel is black in the result as soon as the pixels in the sending document or stationery are black. If both pixels are black, the result is that the pixel is white.



10.22.5. Reception

The parameters relating to reception are configured on the *Reception* tab.

Activate fax reception; Activate SMS reception

In general, fax and SMS reception can be activated and deactivated independently of one another. All phone numbers that are relevant for the SMTP gateway are specified for receiving messages.

Address prefix

In most installations where faxes and/or short messages (SMS) are received in SAP via the SMTP gateway, it is essential to configure an address prefix. Since the phone numbers are stored complete (e.g. 03328/455-960), i.e. with the area code etc. as a fax number with the R/3 user, SAPconnect will not find the user in R/3 because only the extension number is available in ISDN 960 is communicated to OfficeMaster. The receiving prefix +49 (3328) 455 for fax and SMS must be entered here, as SAP stores the fax numbers internally in the so-called canonical number format. If the receive prefix has already been stored on the ISDN connection, it applies to all gateways in the messaging server and does not have to be set again for the SMTP gateway.

Address filter

In the simplest case, an address filter consists of a list of the numbers intended for the SMTP gateway. If faxes to the numbers 305, 306, 307 and 308 are to be processed by the SMTP gateway, these numbers are entered one below the other as an address filter. If there are a large number of phone numbers, the phone number entry can be summarized and simplified using regular expressions (for the example above: 30[5-8]). In the default configuration, the address filter consists of a period followed by an asterisk (.*). The period is also a regular expression and stands for any character. The asterisk gives the previous character the meaning any number of times. In this way, the reception processes are forwarded to any phone number (i.e. all) to the SMTP gateway.

> Note!
> If the address filter is restricted, receipt processes that were received on phone numbers that are not maintained are no longer sent to the SMTP gateway and its administrator, but are stored by the Undeliverable (UNDLVRBL) component of the messaging server. It is important to configure the Undeliverable component so that no received messages are lost unnoticed.

10.23. SIP trunk

The SIP component is available for connection to SIP trunks and IP telephone systems. Fax and NGDX transmission, landline SMS and voicemail are supported via the SIP trunk.

For configuration, open the OfficeMaster Suite configuration and select *Telephony > SIP Trunk* from the quick launch bar.

10.23.1. Create new component

Directly after the installation you will not find any created SIP components. To create a new component, please select *New SIP Trunk component*. An installation wizard will then open.

After you have confirmed or adjusted the default settings such as *Component name*, *Display name* and *Server*, the special wizard for the SIP component starts, which leads through several dialogs to the setup.

1. Choose the type of connection

In the first step, select the type of connection to be connected. This preselection makes the following dialog with the currently predefined remote stations clearer.

The templates are constantly being expanded and the OfficeMaster Suite is updated accordingly. If the remote station you are using is not listed, select *Common Profile* and continue to follow the wizard.

> **Note!**
> If you have made an adjustment for an existing profile or you have carried out a connection that has not yet been made? - we look forward to your feedback and would be happy to add it for further releases of the OfficeMaster Suite.

1. Connection Settings

Enter the connection information here, such as the IP address and port of the remote station.

1. Line configuration

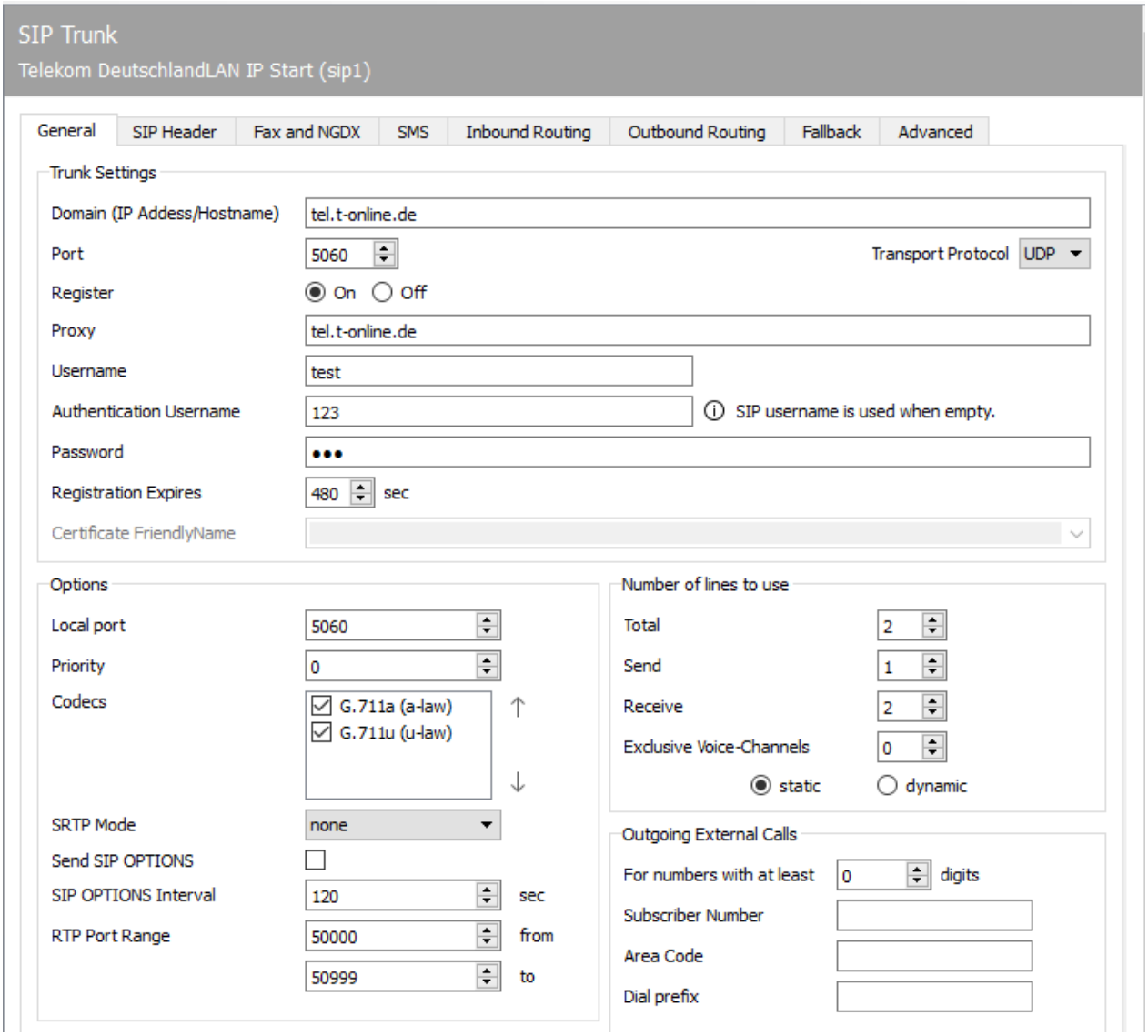
Depending on the existing licenses and the desired priority of incoming and outgoing messages, you can configure the available lines here.

Finally, when using the fax function, enter the basic information for fax communication.

After you have gone through the wizard, you will see the newly created component (named sip0, sip1, ...) in the overview of the available SIP components.

You can access the complete settings for the connection by left-clicking on the component in the quick start bar or by right-clicking in the main field.

Now you can make further settings, e.g. NGDX or number corrections based on the dialed numbers.



10.23.2. General

SIP trunk

General settings for connecting the SIP trunk.

> **Note!**
> If you've created the sip trunk out of a template, the wizard fullfilled the settings with all necessary parameters.

Domain (IP address/DNS)

Enter the IP address or the DNS of the PBX system, the session border controller or the IP Provider here.

Port

Enter the port on which the remote station can be reached.

Transport Protocol

Specification of the transport protocol to be used for SIP: UDP, TCP or TLS.

Register

If registration is required at the remote station, select *On* here, otherwise *Off*.

Proxy

If a proxy is needed, please enter the proxy here.

User name

The username for identification at the remote station.

Authentication user

Enter the user name required for authentication here. If you don’t enter a name, the SIP user name will be used.

Password

A password is expected here if required.

Registration expires

Here you can specify the time period for a valid *register*.

Certificate (Friendly Name)

If you have selected *TLS* as the transmission protocol, please select the appropriate computer certificate for MTLS (mutual TLS) here.

Alternatively, enter the name of your certificate here and the OfficeMaster Suite then searches for the certificate in the certificate administration of the local computer using the display name (CNAME, canonical name or FriendlyName).

The following search order applies:

1. In the PKI directory there is a file in PFX format with the specified name.
2. In the PKI directory there is a .crt.pem and a .key.pem PEM file with the specified name x as “x.crt.pem” and “x.key.pem”.
3. In the PKI directory there is a .crt and a .key PEM file with the specified name x as “x.crt” and “x.key”.
4. In the “Windows User Certificate” store there is a certificate with certificate and key **(exportable)** with Friendly Name equal to given name or CNAME equal to given name.
5. In the “Windows Local Machine Certificate Store” there is a certificate with certificate and key **(exportable)** with Friendly Name equal to the given name or CNAME equal to the given name.
6. The domain certificate in the “Windows Local Machine Certificate Store” can **not** be used due to the lack of an exportable private key.

Open SIP server port

In the case of TLS or TCP as the transmission protocol, no SIP server port is generally required for communication with the trunk since there is a pure client-server connection from direct SIP to the trunk. In the case of TLS, no certificate needs to be specified. In the case of MTLS (mutual TLS), however, a certificate is still required.

Options

Local port

Enter the local port for SIP communication of the SIP component here.

Note!
When using multiple SIP components, you must specify a separate port for each component, e.g. sip0 5060 , sip1 5061, ...

Priority

Specify the priority routing rules take placed within the global rouitng list in the controller component. This is necessary if multiple sending components for the same number range and deterministic job routing are required. If all priority values are equal, the rules of the component launched first are interpreted first. In this case, the job routing depends on the start sequence of the components.

Codecs

Here you select the codecs supported by the remote station for transmitting the data streams.

SRTP mode

Should Secure RTP (encrypted media stream) be used?

Send SIP OPTIONS

SIP OPTIONS are used to periodically check if the remote station (SIP Proxy, SBC or IP PBX System) is fully functional. The SIP remote station has to support SIP OPTIONS, otherwise this setting shouldn't be activated.

If the remote station no longer responds to SIP OPTIONS, a fault in the SIP trunk is detected and the the corresponding SIP component no longer accepts outgoing jobs.

SIP OPTIONS Interval

Specifies the time interval between sending the individual SIP OPTIONS here. Default value is 120s.

RTP port range

DirectSIP RTP ports are selected from the specified range. The area should be at least as large as the number of simultaneous connections. If a firewall is used, it is necessary to define this area in the firewall too.

Number of lines to be used

Enter the lines to be used in the *Total* (allocation of line licenses to the components) and separately according to *Send* and *Receive*. Channels can be reserved exclusively for *Voice-Mail*. Please notice the total number of line licenses you have available. Especially in solutions with multiple sending components (*SIP*/*OMCUMS*), all components should always have a number of licenses and lines adapted to the desired configuration.

The lines are requested and distributed dynamically up to the upper limit defined here, they are still available and not used by another sending component.

Outgoing External Calls

For numbers with at least ... digits

This parameter specifies the minimum phone number length for outbound calls without using the *Dial Prefix*.

Subscriber Number

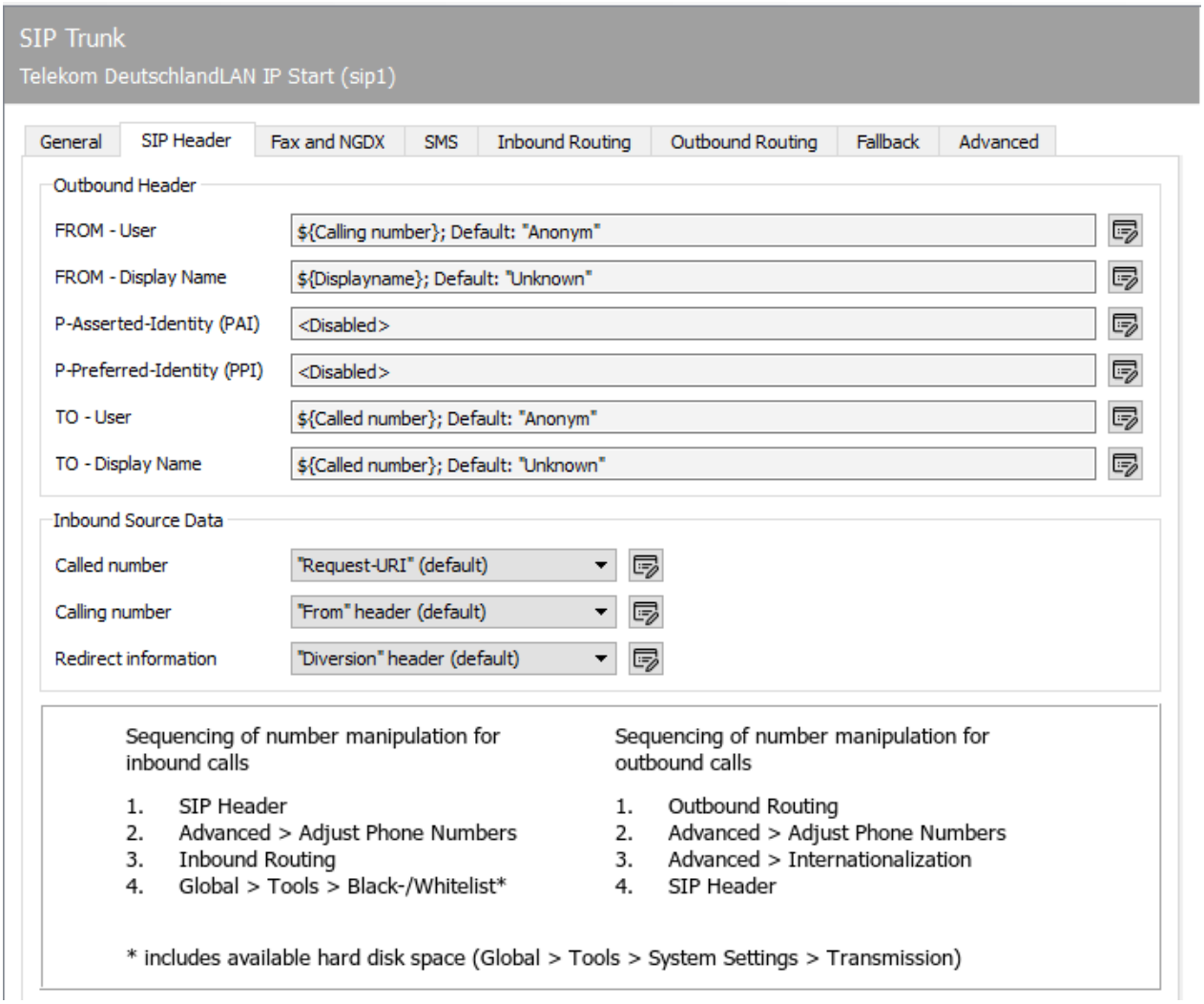
Specifies the phone number of the PBX or subscriber.

Area Code

Specification of the area code of the local network in which the connection is located.

Dial Prefix

When connecting to a PBX, the outbound line access can be entered here (usually 0 or 00). This part of the number is put in front of the number to be dialed in order to reach external participants.



10.23.3. SIP header

Outgoing calls - SIP header

For outbound calls, it can be necessary to specify which fields of the outbound data source match to the various SIP headers. The following fields are available as data sources: - Calling number / number of the caller - Called number / number of the person to be called - Redirecting Number / number which redirects the call - Called Subscriber (CSID) - Displayname / caller name - Callee Name / Callee Name - SIP Username / name of the user on the SIP trunk - SIP Username (Auth) / Name of the user on the SIP trunk, authenticated

FROM - Users

Field for the SIP\ sender address.

FROM - Display name

Field for the clear text name of the sender.

P-Asserted-Identity (PAI)

The P-Asserted-Identity header is used between two trusted SIP Nodes transmitting the user's authenticated identity.

P-Preferred-Identity (PPI)

With the P-Preferred-Identity header, a SIP user agent communicates the identity that the reliable SIP node (e.g. proxy) should enter in the P-Asserted-Identity header.

TO - User

Field for the destination SIP address.

TO - Display name

Field for the plain text name of the called party.

Incoming calls - source data

For inbound calls, it can be specified from which SIP headers the information for the phone numbers of the caller, the called party and any redirection should be taken.

Called number

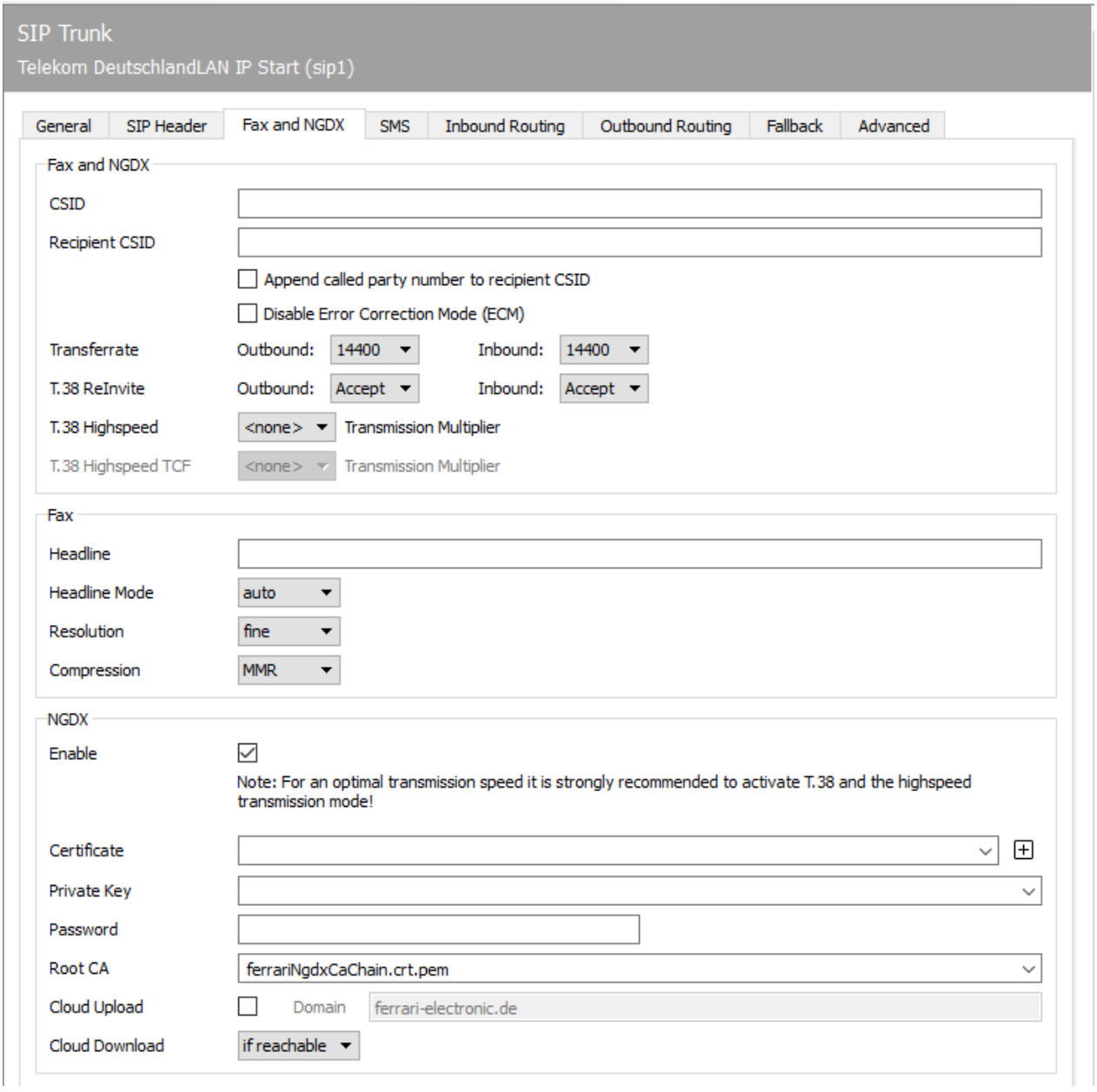
The destination phone number can be delivered within the *Request-URI*, the *To* header or the *P-Called-Party-Id* header.

Calling number

The caller's number can be entered in the *From* header, the *P-Asserted-Identity* header, or the *P-Preferred-Identity* header.

Redirect information

The number that rerouted the call can be delivered in the *Diversion* header (default) or the first or last *History-Info* header.



10.23.4. Fax and NGDX

Fax and NGDX

CSID

According to the ITU standard *T.30*, the fax identifier to be used is derived from the international telephone number of the telephone connection, i.e. from the country code, area code and telephone number. Only digits, plus signs and spaces may be used in the fax identifier. The area codes are to be entered without a leading zero.

Recipient CSID

Here you can specify the CSID shown during the transmission process on the remote fax device.

Append called party number to recipient CSID

If a different fax ID is to be communicated for the reception of the sending party, a special receiving ID can be configured. Optionally, the function “Append called party number to recipient CSID” can be activated. This has the effect that, i.e. when sending a fax to the number 348, the reception ID +49 3328 455 will be appended to it, the fax ID +49 3328 455 348 will be indicated in the sending confirmation for the sending party. If one or more number correction rules are configured, the correction of the incoming number will take place before the addition.

Disable Error Correction Mode (ECM).

Here you can disable automatic error correction. We only recommend doing this if the remote station does not support ECM and the training phase should be shortened.

Transfer rate

You should leave the default settings here. In some cases with poor line quality it can make sense to throttle the speed by default (default: 14400).

T.38 Reinvite

T.38 fax connections start as normal telephone connections with the G.711 codec. One of both endpoints (calling or called fax machine) begins the renegotiation to T.38 via SIP ReInvite with media type Image T.38 instead of audio. If both endpoints are renegotiating at the same time, there may be a problem. In the T.38 mode *Send* DirectSIP sends the T.38 ReInvite automatically. In *Accept* mode, an incoming ReInvite is accepted and switched to T.38. The *Decline* setting prevents T.38 renegotiation.

> Note:
> Depending on the selected SIP trunk profile, the various *T.38* modes are configured by the installation wizard.

For optimal speed of document transmission (including fax) we recommend setting T.38 “Initiate” for sending and receiving whenever possible.

T.38 Highspeed

Increase the data rate of the T.38 data stream in steps of 64kbit/s (rate of a G.711 telephony voice channel).

T.38 Highspeed TCF

Increase the transmission speed for the T.38 training information in steps of 64kbit/s (rate of a G.711 telephony voice channel).

Fax

Headline

Headline configures the default header text (e.g. company name) for outgoing faxes. This header text also contains the fax identifier. It is printed on the remote document at the top of the page.

According to the ITU standard *T.30*, the fax identifier to be used is derived from the international telephone number of the telephone connection, i.e. from the country code, area code and telephone number. According to the standard, only digits, plus signs and spaces may be used in the fax ID. The area codes are to be entered without a leading zero. In practice, you will also find texts or organization names in the Headline.

The standard parameters configured for *Headline* and *Fax ID* are only used for sending if no order-specific settings, e.g. the *Exchange*, *Notes* or *SAP* user.

Headline Mode

- *Off* : No header information is transmitted
- *Merge* : Header information is integrated into the document to be sent. Under certain circumstances, this can lead to information in the document being “superimposed”.
- *Extend* : Header information is prepended to the document. Lines are added to the actual fax document (the page is lengthened) and, if in doubt, also scaled so that the maximum page size is not exceeded at the end. *Auto (default setting)* : Based on the document to be sent, OfficeMaster Suite tries to automatically recognize whether the first lines are empty and thus merging is possible or whether an extension (*extend*) has to be made.

Resolution

- *Standard* : 100dpi
- *Fine* : 200 dpi (default)

Compression

- *MH* : Modified Huffman, RLE (run length encoding) based
- *MR* : Modified Read, Fax Group 3
- *MMR* : Modified Modified Read, Fax Group 4 (default)

NGDX

NGDX stands for Next Generation Document Exchange and describes a series of processes that improves the fax protocol. The individual methods are:

- *T.434 file transfer* for exchanging PDF documents via G.711 and T.38 telephony links. This conforms to the ITU standard, the Ferrari electronic implementation also checks the content lexically for PDF conformity in order to rule out malware.
- *T.38 Speed-Up* for pure IP routes (end-to-end T.38). If no T.38 media gateway is used, the data rate of classic analogue modems can be ignored and the T.38 data can be sent more quickly. This allows the transmission speed to be increased by a factor of up to 100. This also works with T.38-capable remote stations from other manufacturers.
- *Encryption and authentication*: T.30 defines an encryption method for ECM data, which is unusable from today’s perspective (40-bit key). As a proprietary extension, the files transmitted via T.434 can be encrypted with AES256. The key exchange uses RSA and X.509

certificates. X.509 certificates with SAN Tel-URI are used for optional authentication of the remote station.

- *Cloud Relay Mode*: The transmission of large (several MByte) files via telephony modem takes a long time. In cloud relay mode, the files are divided into pieces (shards, max 256KB) and these shards are individually encrypted with their own keys. After that, the shards are uploaded from the sender to a cloud server. The sender creates a list of URLs, cryptographic keys and file metadata and transmits this to the recipient using encrypted T.434. This downloads the shards, decrypts them and assembles the documents and, after a successful hash check, confirms receipt over the telephony route. For example, a 50MB PDF file can be transferred in just over a minute.
- *URL Break-Out*: This is a future NGDX procedure based on the use of the T.30 fields CIA and ISP.

Enable

Activate document exchange. Whenever a remote station can receive documents via NGDX, this transmission is used. If NGDX is not possible, the automatic fallback to fax takes place.

Certificate, Private Key, Password, Root CA

If the documents are to be encrypted and transmitted via NGDX with a trustworthy certificate, please enter the relevant information here.

Ferrari electronic delivers a root certificate, which should be entered under Root CA. If you have a certification authority (Root CA) yourself you can transfer the root certificate. However, you should only do this if you want to communicate in a closed user group.

If you click the “plus” in the interface behind the input field, you can create a self-signed NGDX certificate. This creates a private key, a certificate signing request (Certificate Signing Request/ CSR) and a self-signed certificate. These can now be used for encryption, but do not have a signature from the certification authority (CA).

Note:
NGDX certificate with wildcard on a number block
The phone number to be stored here in the SAN Tel-URI can contain a wildcard character. By putting one Asterisks (*) at the end of the phone number ensure that the certificate for a block of phone numbers ends with “any”.

As soon as you confirm the entry, the private key and the certificate are automatically stored by the configuration. Afterwards the certificates are also visible as NGDX certificates in the certificate management.

- Self-signed certificate with phone number but without signature of the root CA can be created any time and allows encrypted transmission via NGDX. However, the authenticity of the remote station cannot be checked.
- NGDX certificates

You can email the generated CSR file to “pmc@ferrari-electronic.de”. A fax with a “secret” is sent to the Tel-URI specified in the certificate. If received and confirmed the fax (feedback to ferrari), the correctness of the Tel/URI in the certificate has been checked and Ferrari electronic AG will sign the certificate with an intermediate certificate derived from its root certificate.

Afterwards you have to store the received certificate in the *C:\ProgramData\FFUMS\fmsrv\data\pki\ngdx* folder and replace the self-signed certificate. Now the chain of trust (trust chain) is intact and you can use the encrypted and authenticated document transmission (Secure NGDX).

The password field is required if the private key you generated is secured with a password. The certificates and keys generated by the OfficeMaster Suite currently do not use a password.

Cloud upload, domain, cloud download

The parameters are used to configure the cloud relay mode. The PDF documents to be sent are

- split in file pieces (shards),
- these are individually encrypted,
- the encrypted shards are uploaded to the cloud relay server via HTTPS and
- then the download URLs and cryptographic keys are sent to the recipient via T.434 over the telephone line.

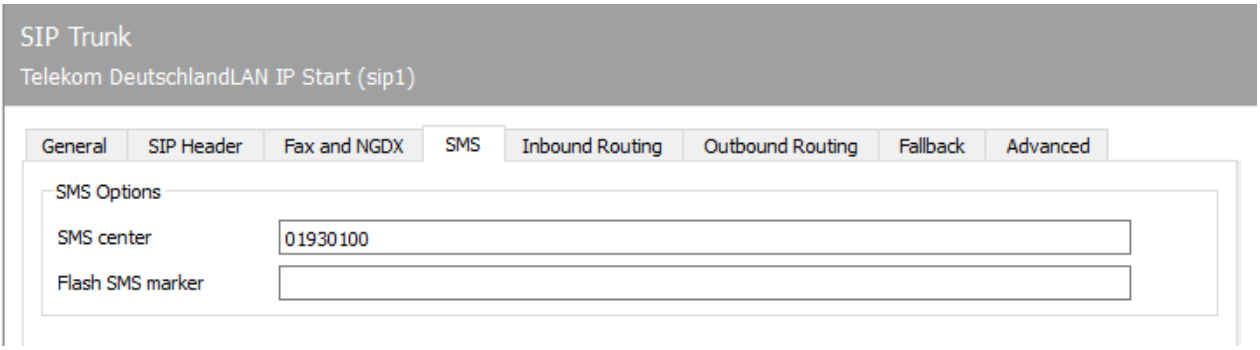
The recipient

- receives the URL list with keys,
- downloads the shards,
- decrypts these and puts the documents back together,
- checks the hashes to ensure the correctness of the transmission and
- confirms receipt via telephone line.

The *Cloud upload* checkbox activates the process for sending documents. The *Cloud Download* combo box activates the cloud relay for receiving documents. Cloud relay is used if both the receiving and sending fax terminals have activated the procedure and both sides have Internet access.

The *domain* specifies the address of the cloud relay server to be used. This is typically the Ferrari electronic cloud relay server, which is resolved under the name _ngdx._tls.ferrari-electronic.de via SRV record. Customers can operate their own cloud relay servers if they set up the corresponding SRV record in their domain.

It is recommended to set up a NGDX certificate in order to be able to encrypt the transmission of the shard URLs.



10.23.5. SMS

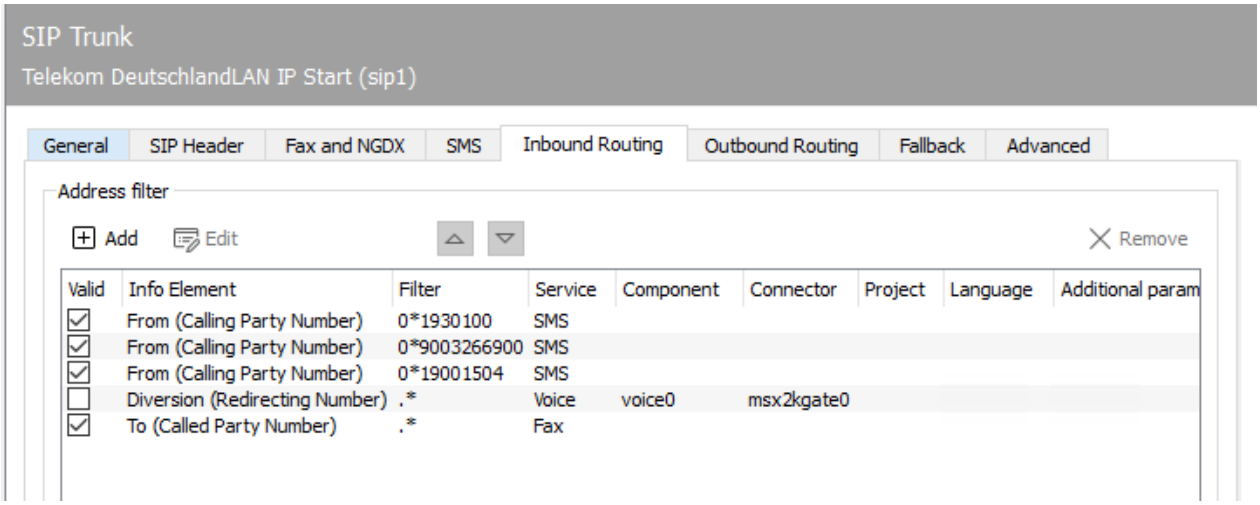
DirectSIP supports the transmission of SMS via V.23 modem over telephony routes (landline SMS according to ETSI standard ETSI ES 201 912). To do this, an SMS center is called via the SIP trunk.

- Deutsche Telekom SMS Center: 01930100
- Materna (www.sms-im-festnetz.de) SMS Center: 090032669000

This type of SMS transmission is suitable for applications with a low SMS volume (e.g. Admin Alert SMS). The SMPP component (Short Message Peer to Peer Protocol) is more suitable for a higher volume of SMS.

SMS center: Enter the phone number of the landline center to be addressed here.

Flash SMS marking: If your provider supports Flash SMS, enter the appropriate syntax here, which will activate it.



10.23.6. Inbound Routing

Address filter

By creating rules in an address filter list, you can specify which service and which component is selected for specific phone numbers or phone number blocks. A filter expression is applied to a selectable SIP header and, if this applies, routed to the appropriate component. The rules will be processed from top to bottom. If one rule matched, no further rules will be checked.

Add to

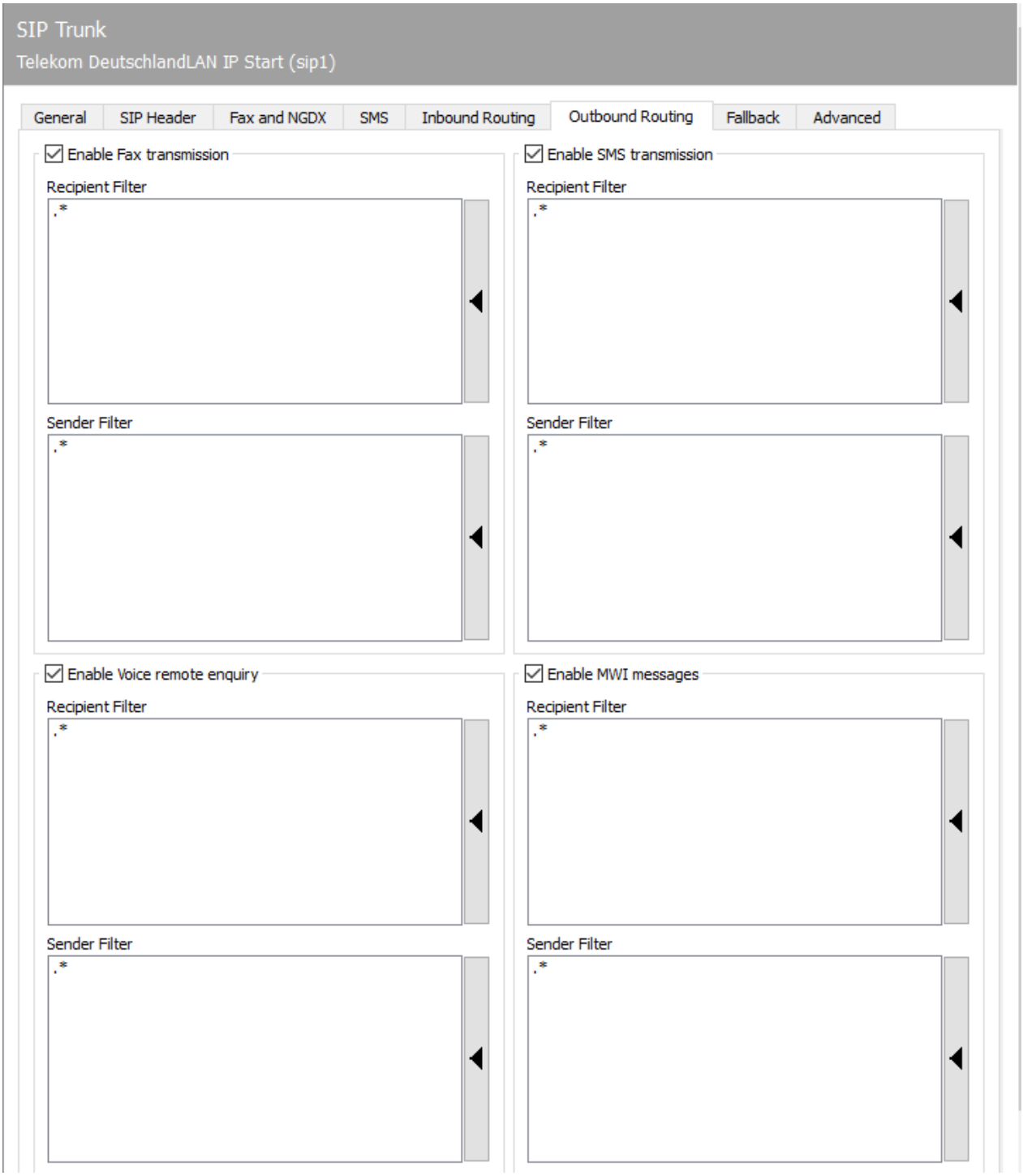
With *Add* a new rule can be created and added to the list.

To edit

An already existing rule can be edited with *Edit*.

Up or Down

This allows you to move the selected rule and to change the order of the rules. This is relevant because the routing decision is made with the first applicable rule.

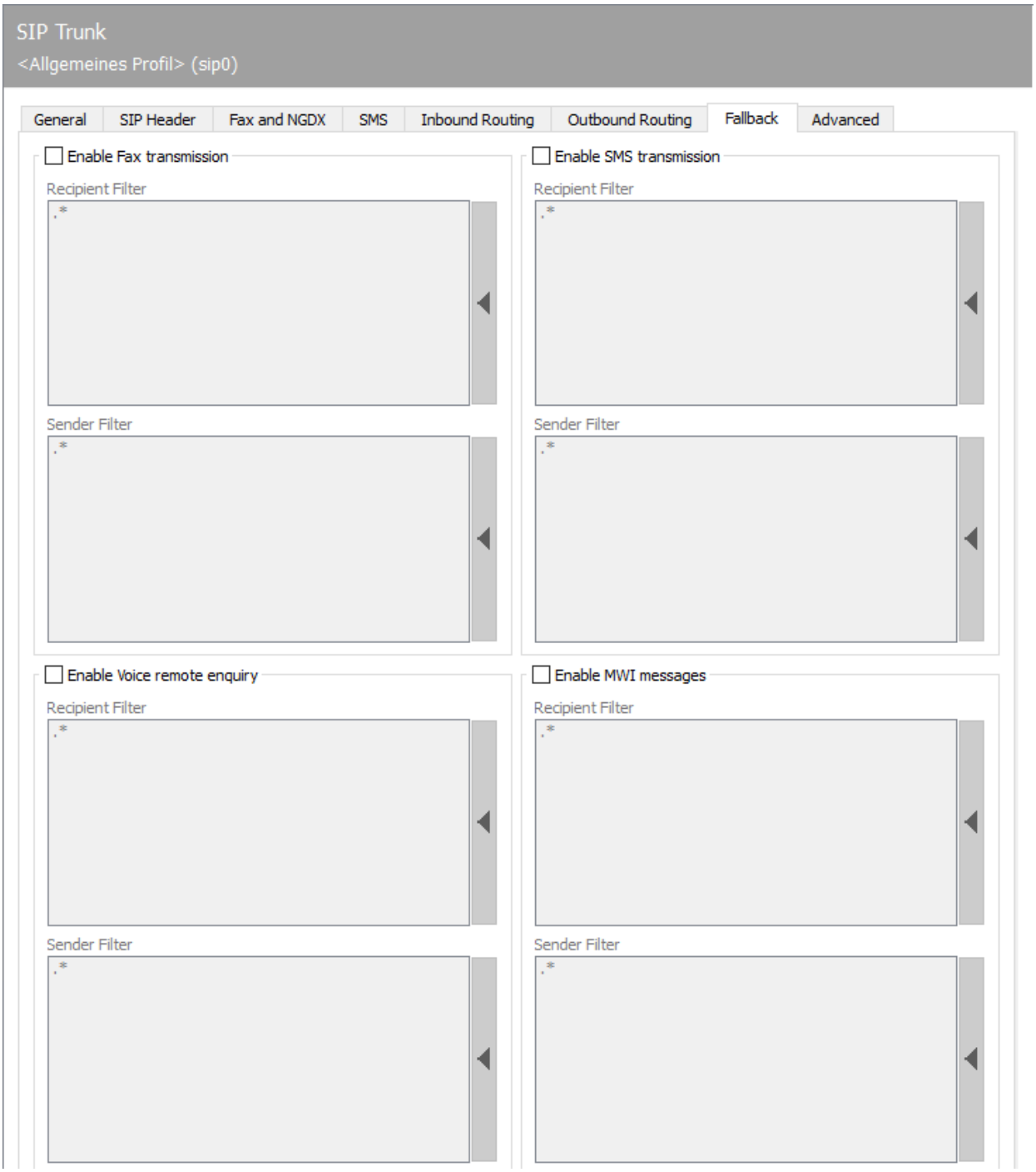


10.23.7. Outbound Routing

It can be specified for the four different service types (Fax, SMS, voicemail and MWI/message waiting indication) which of the currently configured SIP component should process the corresponding outgoing job. Regular expressions are specified for the destination phone number (*Recipient Filter*) and the sender number (*Sender Filter*). In the case of a match, the SIP component is the outgoing routing target.

The filters made for all available send components are used for the routing decision of a send job. This makes it possible, for example, to send specific orders to specific target phone numbers on the appropriate SIP trunks.

Clicking on the right sidebar of a list allows entering a regular expression. Syntax examples are also given. The regular expression syntax is based on the PCRE2.



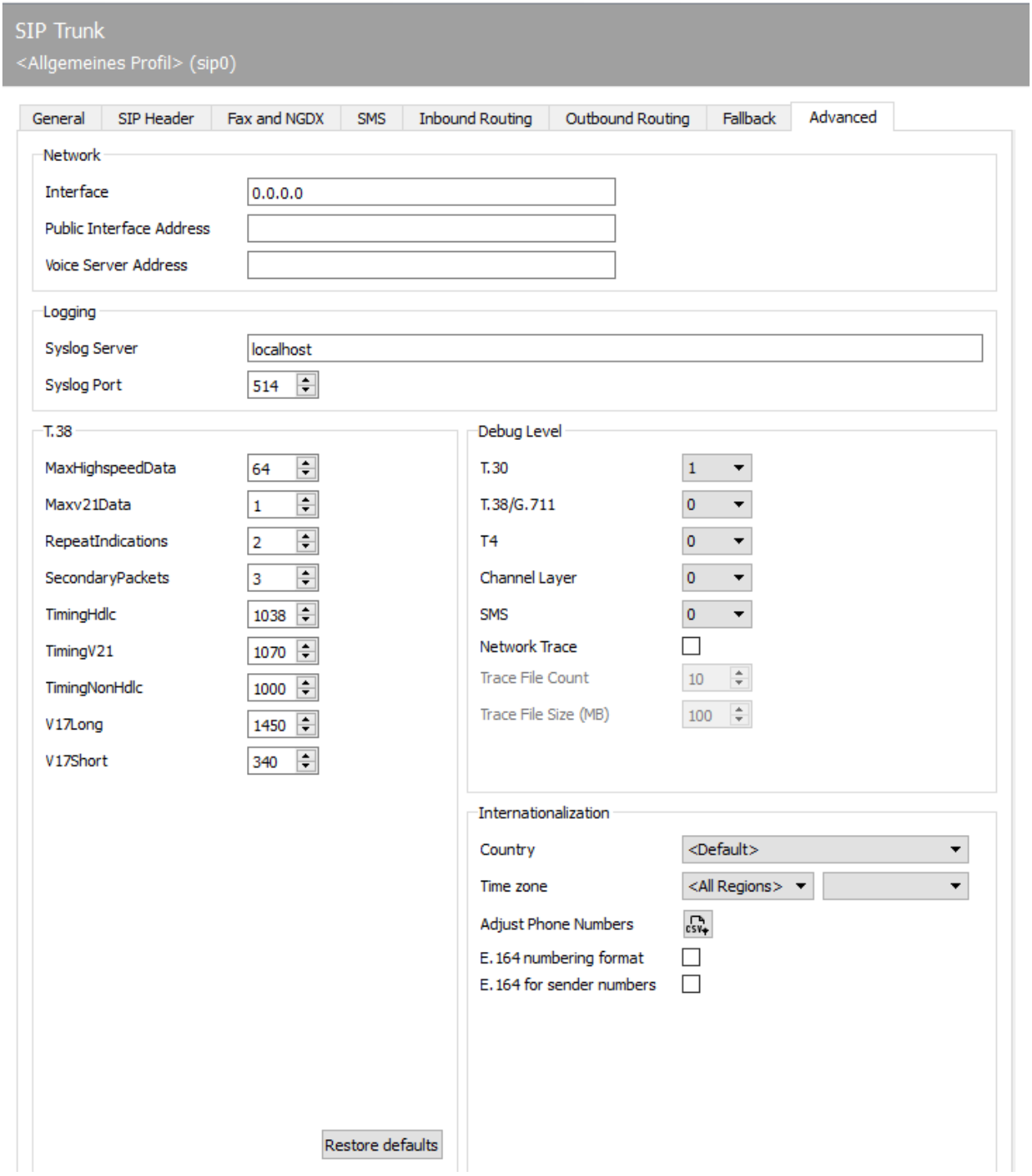
10.23.8. Fallback Routing

Fallback routing is used if a certain number of redial attempts did not lead to a successful transmission. To do this, fallback routing must be activated under Tools menu > System settings > Common by enabling *Enable fallback Processing*. Afterwards, on the *Error processing* tab, you can set the number of redials per error type (e.g. SIP error > Auto Resend) that are carried out before the messaging server switches to fallback routing and selects a different send component for the job. The actual set of rules is similar to *Outbound Routing*.

It can be specified for the four different service types (Fax, SMS, Voicemail and MWI/message waiting indication) which of the currently configured SIP component will process the corresponding outgoing job. Regular expressions are specified for the destination phone number (*Recipient Filter*) and sender number (*Sender Filter*). In the case of a match, the SIP component is the outgoing routing target.

The filters of all send components are used for the routing decision of a send job. This makes it possible, for example, to send specific orders to specific target phone numbers on the appropriate SIP trunks.

Clicking on the right sidebar of a list allows entering a regular expression. Syntax examples are also given. The regular expression syntax is based on the PCRE2.



10.23.9. Advanced

The options on the *Advanced Settings* tab are essentially intended for the following use cases:

- For phone number correction - to correct and redirect incorrect recipient phone numbers. You can find more information on this in the Call Routing chapter.
- For fine adjustment of T.38 parameters (this should not be necessary in normal operation).

- To set log levels that are requested by the support team for support cases.
- To adjust the network settings in the case of multi-homing or firewall operation for the corresponding sip component.
- To specify the address of the syslog server.

Network

Interface

Please enter the network interface to be used here. If all available interfaces are to be used, leave this value at *0.0.0.0*

Public Interface Address

The public IP address of any existing firewall may be necessary under certain circumstances for the operation of DirectSIP. If yes, you can enter it here. In all other cases the value should be left blank.

Voice Server Address

The voice server address can be specified here.

Logging

The SIP component sends its log messages to a syslog server via UDP. When installing the OfficeMaster Suite, the OfficeMaster SyslogServer is installed as a service. If you use a different syslog server, you can specify it here (FQDN or IP Address).

> Note!
> If the syslog server is installed by the OfficeMaster Suite (this happens by default), the following path is used for the log files: %ProgramData%\ffums\syslog\. If you want to change this path, please call up the OfficeMaster Syslog configuration program and edit the path according to your requirements.

T.38

You should only change the settings for the T.38 fax transmission protocol if you are a T.38 professional or after consulting the Ferrari electronic support team.

Debug level

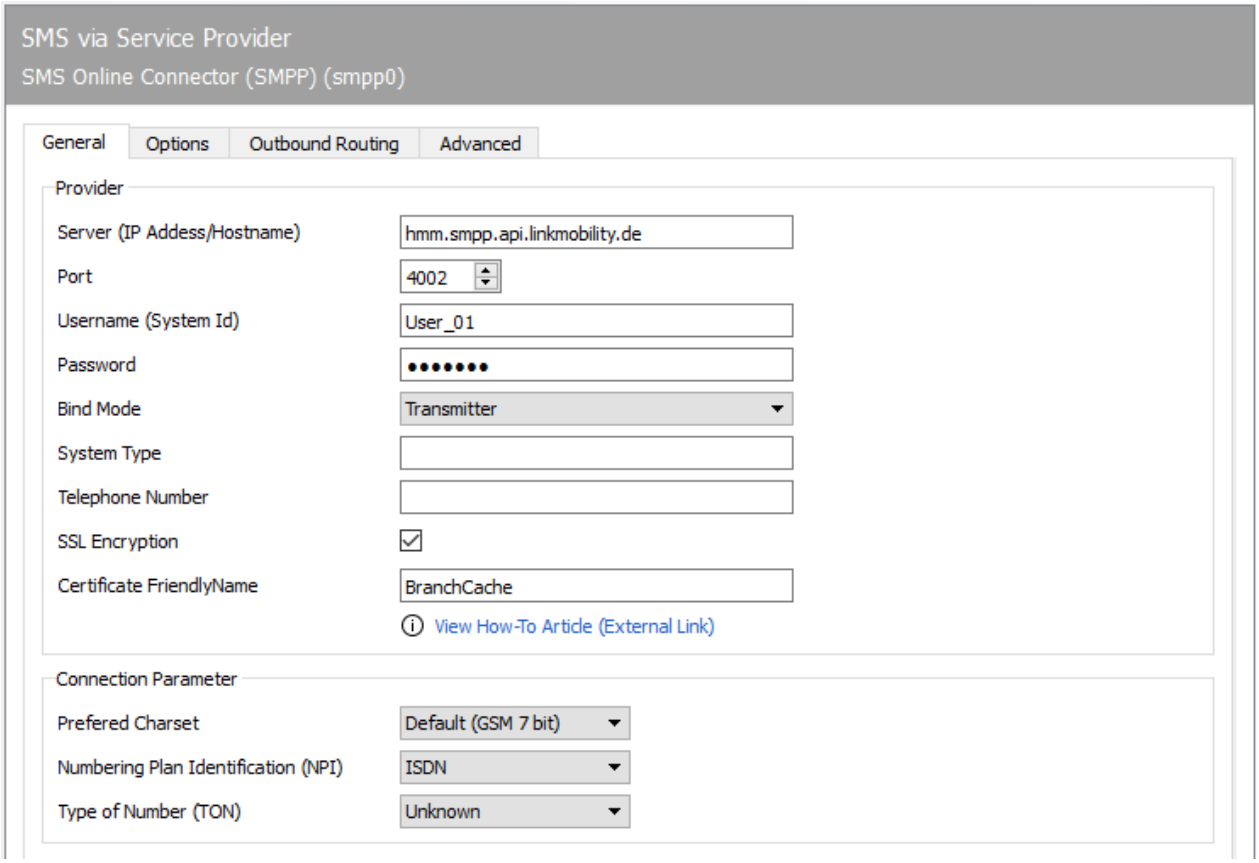
The sensitivity of the log behavior can be set to different levels for different software subcomponents. By activating the *Network Trace* option, it is possible to analyze so-called *Pcaps* via Wireshark. However, this requires the installation of *Pcap* (such as *WinPcap*). The installation for *WinPcap* can be found by default under C://ProgramData/FFUMS/FMSRV/... .

10.24. SMS via Service Provider (SMPP)

The SMPP send/receive component of the OfficeMaster Suite is responsible for sending and receiving short messages (SMS) via an SMS service provider. It communicates with an SMS provider available on the Internet.

Providers can be connected flexibly with this component. Open the configuration under SMS > SMS via IP Provider (SMPP) in the left quick launch bar.

SMPP is short for Short Message Peer-to-Peer. If your provider uses this protocol, the SMPP component can be used. Protocol details are available at smpp.org.



10.24.1. General

The most important account information is to be stored on the first tab.

Providers

Server (IP Address/Host)

Enter the URL specified by your provider here

Port

Enter the destination port according to your provider's information.

Username (System ID) and Password

User name assigned by the provider with the associated password.

Type of component

Fill in after specifying the provider (sender, recipient or both)

Type of system

Only fill out this field if required by your provider.

Phone number

Enter the phone number here that is to be used as the sender phone number when sending. If no value is configured here, the sender phone number is derived from the job properties.

If you store an alphanumeric value here, you must select "Alphanumeric" for TON below.

SSL encryption and certificate

Specify, whether the connection is to be encrypted or not. Optionally, you can also specify a client certificate from the server's certificate store.

Connection settings

Character set

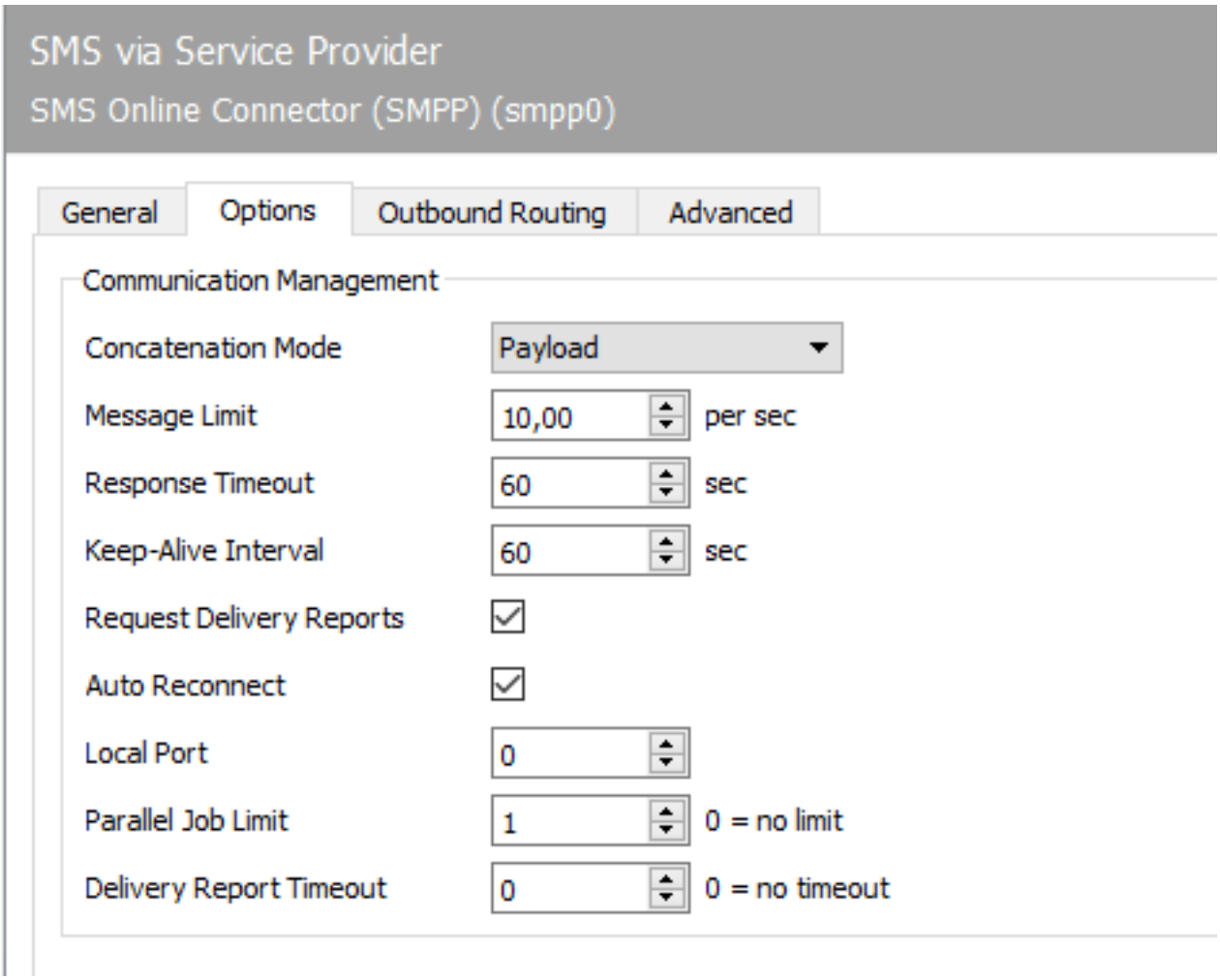
The character set to be used varies depending on the provider. In most cases, use the default “GSM 7 bit”.

Numbering Plan Identification (NPI)

Please select the appropriate numbering plan from the selection box.

Type of Number (TON)

Set the number type here depending on your sender phone number.



10.24.2. Options

Most of the settings to be made here depend on the connected provider and should only be adjusted in coordination.

Communication management

Concatenation mode

- A long SMS is sent with Payload.
- Short message.
- Short message with SAR.

Message limit

Enter the throughput limit for sending and receiving short messages here. This value is specified by the provider.

Response timed out

Value specified by the provider, maximum value until a response is expected from the SMPP provider.

Keep alive interval

Value specified by the provider, interval between keep-alive messages.

Request shipping confirmation

Turn shipping confirmation on or off. If switched off, only the transfer to the provider is confirmed in the feedback to the connector or the user, but not the successful SMS\ dispatch. If switched on, the feedback to the connector or the user only occurs when a delivery confirmation has been received from the provider. It is also necessary that “Transmitter”, “Receiver” or “Transmitter and Receiver” is stored as the component type under *General*.

> Note!
> In the case of bulk mailing, it may be advisable not to wait for the shipping

confirmation, as the counter for processing only counts down the maximum number of orders after feedback to the connector.

AutoReconnect

The setting specified by the provider is to automatically establish a new connection after the network connection has been disconnected.

Local port

Here you specify the local port on which the component communicates via TCP. If no value is stored, the defaults apply:

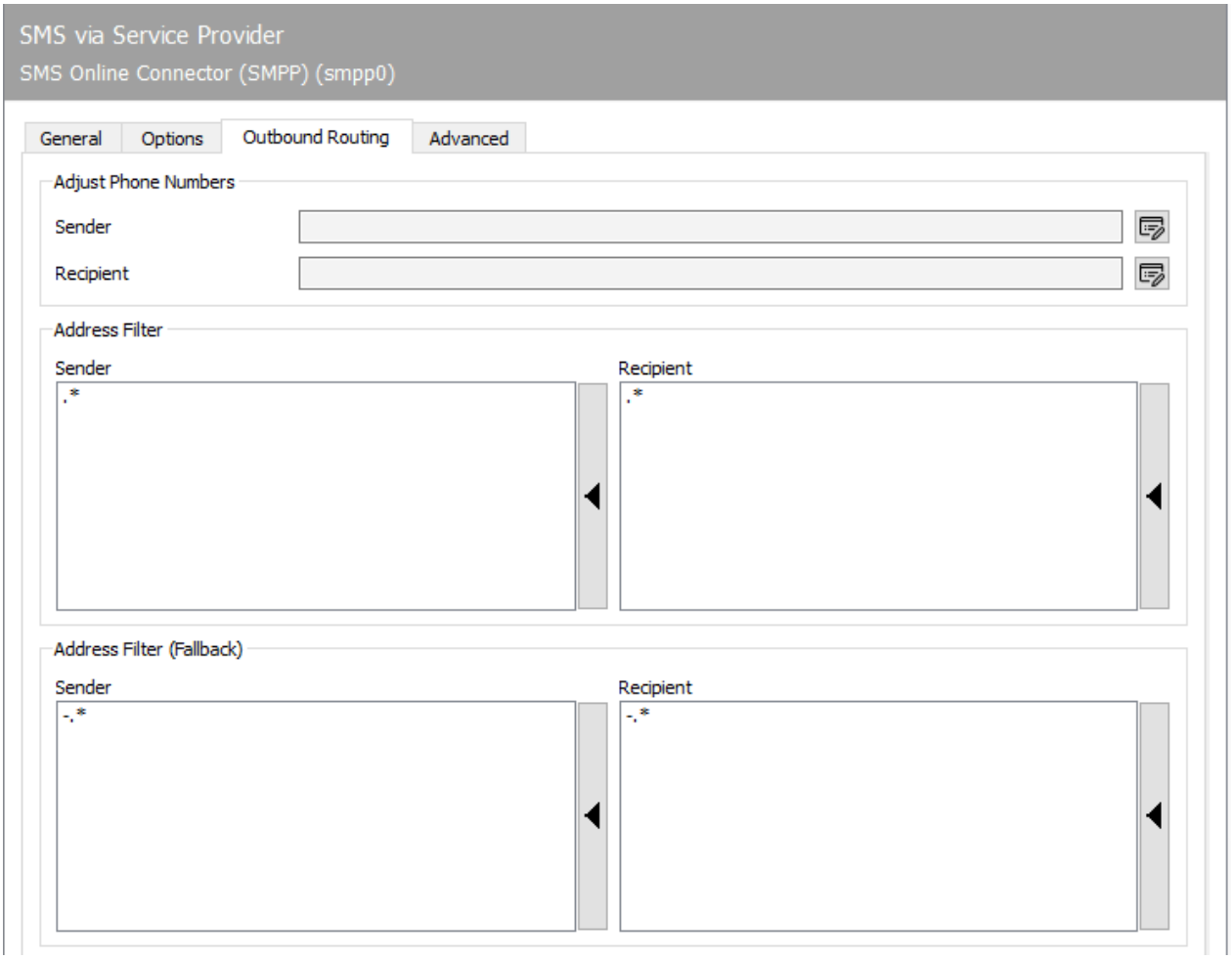
- 3550 when using SSL or TLS
- 2775 when using TCP without encryption

Limitation of parallel orders

Regardless of the provider, a limit on the number of jobs can be specified for the OfficeMaster Suite. An order is considered active as long as the feedback to the connected connector has not yet been handed over again. If a “0” is specified, there is no limit to the parallel jobs.

Transmission report timed out

Maximum interval in which the transmission confirmation is expected. After the waiting time has expired, it is assumed that the transmission has failed and a corresponding response is generated.



10.24.3. Routing (outgoing)

This section is divided into three sections. On the one hand the phone number correction for outgoing short messages and on the other hand in the two routing rules. Here it is determined for which orders the component registers in the normal case and in the fallback scenario on the controller of the OfficeMaster Suite and takes over the dispatch accordingly.

Telephone number correction

Behind the fields for sender and recipient you can open another dialog by clicking on the edit field. All relevant fields for the transmission of a message via SMPP can be adjusted here using regular expressions or fixed values. Only one rule is possible.

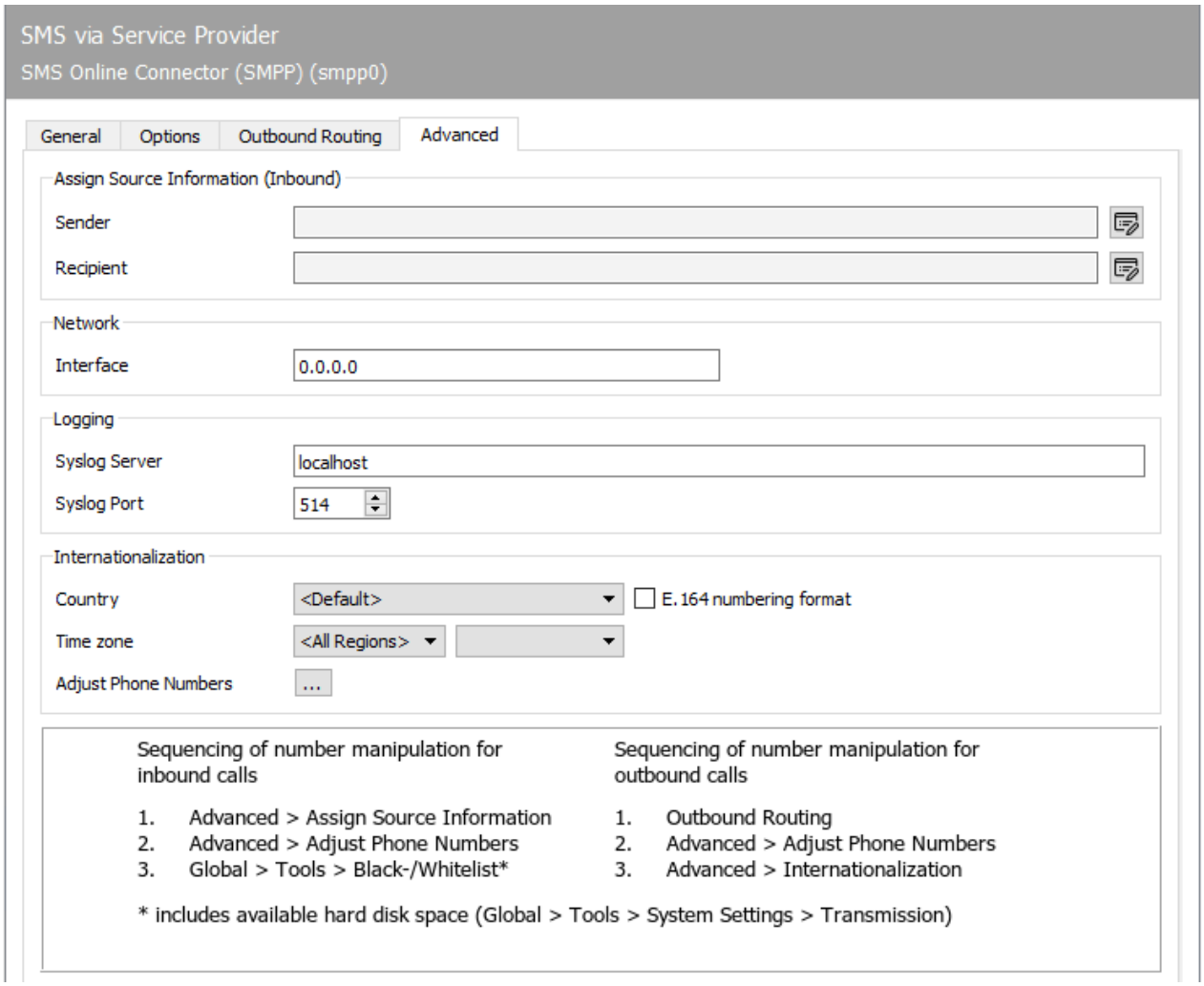
Address filter

Sender

One or more regular expressions define which SMS jobs should be sent by this component.

Address filter (fallback)

One or more regular expressions define which SMS jobs are to be sent by this component in the case of repetitions in the event of an error (fallback routing).



10.24.4. Advanced

In the *Advanced* tab you can specify additional settings that are not essential for the pure function. You can adjust the phone numbers and also select a different network interface.

Assign Source Information (Inbound)

If incoming short messages are processed, they are often not in the same numbering scheme as the users are stored in the local directory. For this purpose there is the possibility of phone number manipulation. The procedure is the same as in the SIP component.

Network

The IP number in the *Interface* field determines the local ip address of the network interface. If the host has multiple IP Adresses please specify the one which should be used by the smpp component.

Logging

The SMPP component sends log messages to a syslog server. The address and port of this server can be specified here. The default setting is logging to the local Syslog server installed with the OfficeMaster suite.

Internationalization

Country

The automatic number correction adds or removes national and international area codes depending on the configured location of the SIP component or the phone numbers of transmissions. In addition of controlling the area codes, incorrectly entered phone numbers are also corrected, e.g. +49*0*3328....

Time zone

The time zone is responsible for the time stamp of the SMS messages. If you have configured the operating system to an other time zone than the zone that makes sense for the messages, you have to specify the appropriate setting here. It will override the time zone of the host.

In the case of an international distributed user solution (across multiple time zones), the correct time zone can be selected here for the SMPP component.

Adjust phone numbers (replacement rules)

Replacement rules can be entered here, which replace the characters in a telephone number with other characters or delete them. This is particularly useful in the following situations:

1. To make internal calls to an internal number even if the complete telephone number is specified (03328455 > <nothing>).
2. For choosing a provider for calls to certain countries (0081 > 010780081).
3. For call by call scenarios (3U > 01078; if supported by the gateway).
4. To close eventualities and gaps in the automatic correction.

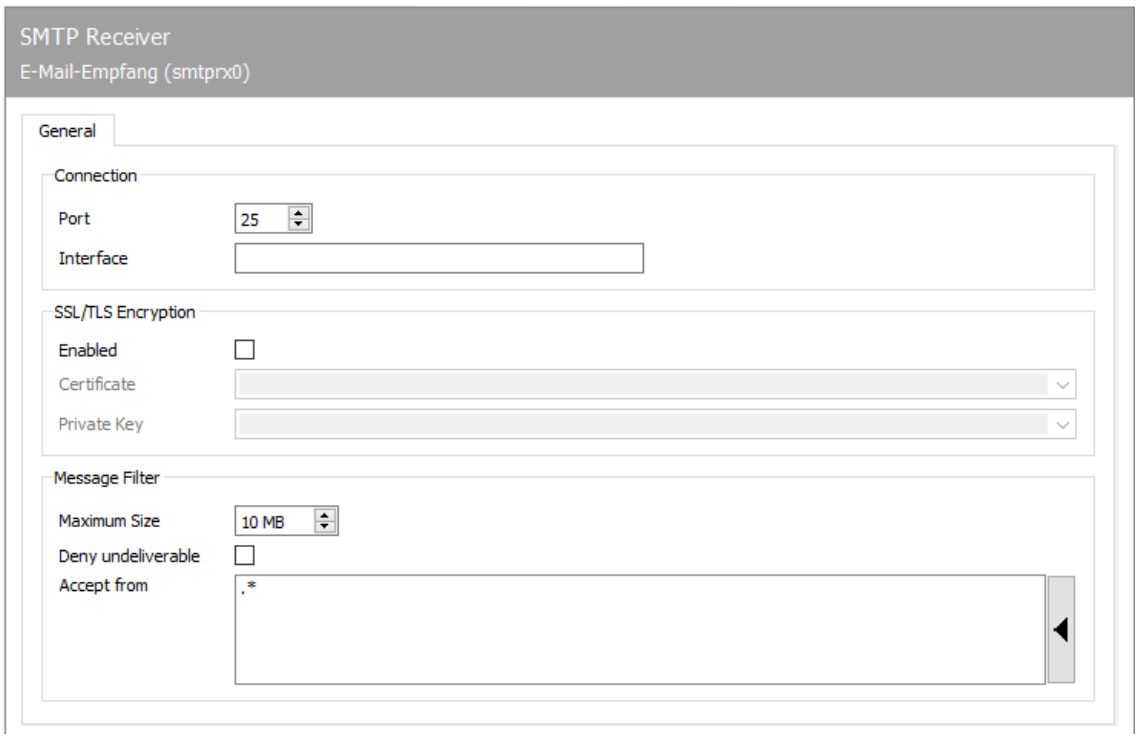
The [...] button takes you to the setup dialog. There you have the option to *add*, *edit*, *remove* and *copy* rules.

You can find a detailed description of the process of phone number manipulation for incoming and outgoing calls in the manual. This history is the same for SIP and SMPP. Regular Expressions will be used.

10.25. SMTP recipient

Incoming mails are forwarded to *SMTPRX* by the company's internal mail server. The *SMTPRX* component is automatically created with OfficeMaster 8 when setting up an *MSX2kGATE* or *MAILGW*.

In the event that the components have not been created, they can be created manually via the quick launch bar > E-mail > Reception > New SMTP recipient component.



10.25.1. General

The standard configuration can usually be accepted. Changes are required, among other things, if:

- The receiving port on the computer is occupied by another (mail) server, such as Microsoft Exchange, Lotus Notes, Sendmail,
- E-mail receipt should be regulated, i.e. *SMTPRX* should not process all e-mails,
- A whitelist procedure for e-mails should be activated, in which e-mails to addresses unknown to the messaging server should not even be accepted.

Connection

Ports

For email reception, *SMTPRX* binds to a port of one or all IP addresses and waits for incoming connections. In the delivery state it is port **25**; the default port for receiving SMTP. If a third-party mail server with the same port and interface configuration is running on the *SMTPRX* server (which is standard under Linux, for example), the start of *SMTPRX* may be aborted. Conversely, the receiving component of the third-party mail server may not start. In this case, all emails are received by *SMTPRX* and routed by the messaging server to existing gateways (*MAILGW*, *SAPCONN*, *FILEGW*) or to the default recipient *Undeliverable*.

To solve this, different ports and/or interfaces or IP addresses for receiving mail are configured for SMTPRX and the third-party mail server.

Interfaces

By default, emails from *SMTPRX* are received on all IP addresses or network cards assigned to the server. If the server has multiple IP addresses or network cards, _SMTPRX can be configured so that emails are only accepted on one IP address.

This allows the computer to perform a router function between several networks and may only receive e-mails from one of the networks. This IP address must be stored as an interface. When delivered, **0.0.0.0** is configured as the interface, so that *SMTPRX* waits for e-mails on all available IP addresses.

SSL/TLS encryption

Activate

This enables TLS encryption for the SMTP transport.

Certificate

Selection of the certificate for the TLS encryption of the local SMTP server port.

Private key

Selection of the private key (matching the certificate) for TLS encryption of the local SMTP server port.

Message filter

Maximum size

In addition to the port and the interface, e-mail reception can also be regulated based on the data volume. The maximum message size up to which e-mails should be accepted is set in megabytes.

Reject undeliverables

If the messaging server has one or more gateway components that process received emails (such as *FILEGW*, *MAILGW* or *SAPCONN*), an address filter for receiving emails can be stored for each gateway. This controls the distribution of the received e-mails and, in the standard configuration (.*), causes each gateway to receive every e-mail received. If the address filter has been adjusted for each gateway, i.e. if a list has been maintained for each gateway that includes all e-mail addresses to be assigned to the gateway, *SMTPRX* can reject undeliverable messages from the outset, since the OfficeMaster Messaging Server knows all valid addresses.

Accept from

In order to further reduce the probability of hacker and spam attacks on *SMTPRX* or on OfficeMaster Messaging Server, a list of permissible and impermissible sender addresses can be stored in the form of regular expressions.

Alternatively, this function can also be used to carry out the authorization check with regard to the services provided by the mail gateway (*MAILGW*) of the messaging server (e.g. *Who is allowed to transmit fax jobs by e-mail?*).

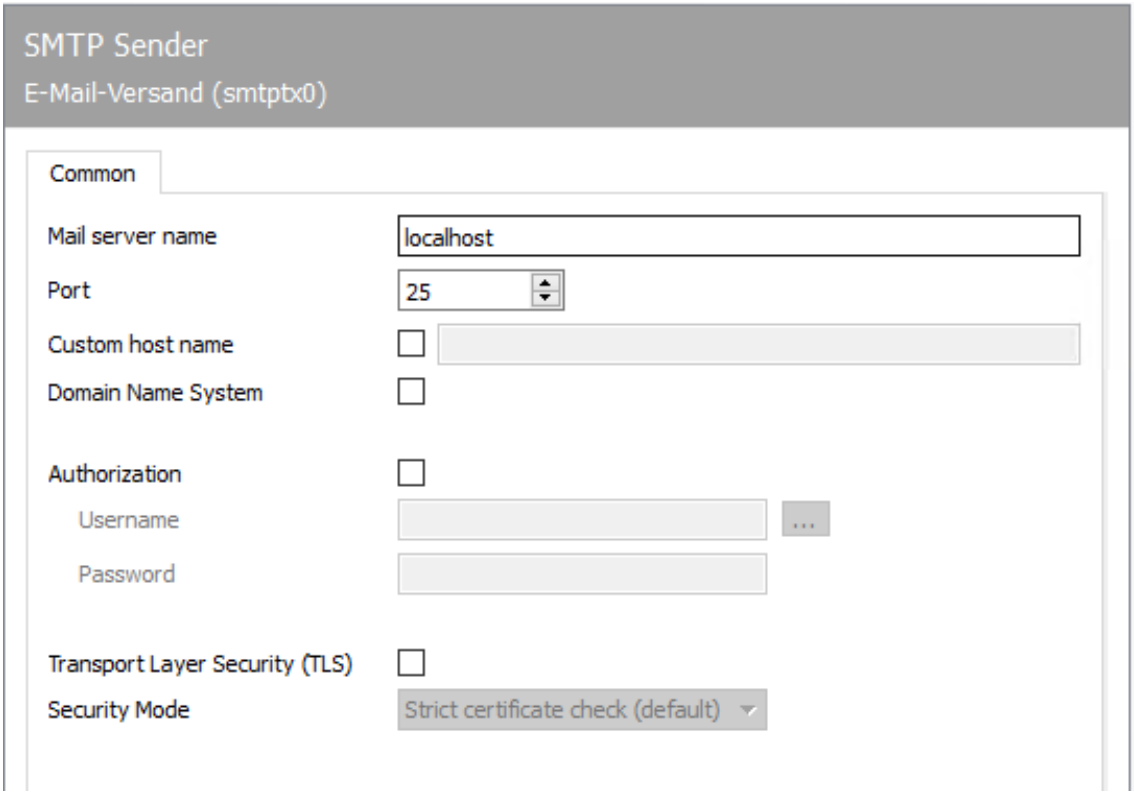
The list can be edited via the context menu or right-click menu. When delivered, *SMTPRX* accepts all addresses (.*).

> Note!
> In order for e-mails to be received, they must be forwarded from the company's internal mail server to the computer on which *SMTPRX* is running. This routing can be set up at various points (mail server, network router) in the network. In practice,

sub-domains such as “*sap.firma.de*” (for SAPCONN) or “*fax.local*” or “*sms.local*” (for MAILGW) have proven useful as routing criteria. E-mails to these sub-domains are forwarded from the network to OfficeMaster Messaging Server.

10.26. SMTP sender

OfficeMaster Messaging Server requires the mail sender SMTPTX for e-mail communication. It forwards all e-mails to the company's internal mail server (relaying server), which sends the e-mails to the Internet. This mail server can be any SMTP-based mail server such as Lotus Domino, Microsoft Exchange, Sendmail, etc. The configuration of SMTPTX is reached under *Edit > Other senders/receivers > E-mail dispatch...*.



10.26.1. General

Mail server name; port

The IP address or the resolved name of the company's internal mail server is required as the name of the mail server (e.g. mail.company.local). In addition, the port on which e-mails are to be sent must be set for SMTPTX, i.e. the port on which the relaying server expects the e-mail to be received. This is usually port 25; the standard port for e-mail reception (Well Known Port).

Custom host

When sending mail, SMTPTX communicates the name of the host on which SMTPTX is running to the configured mail server. Alternatively, the name configured as Custom Host can be communicated to the mail server. This is necessary if the mail server requires the specification of the fully qualified name to send the mail. For example, if the host of SMTPTX is called faxsrv and this name is not accepted by the mail server, faxsrv.company.com can be configured as a custom host.

If Internet mails are to be sent via OfficeMaster Messaging Server (e.g. from SAP or via LPD gateway), the company's internal mail server must allow mail relay for the server computer on which the mail sender SMTPTX of the messaging server is running. You can see the successful or unsuccessful attempts to send email in the SMTPTX log files (View > Log files...). Mail relay is disabled by default on most mail servers.

Domain Name System

If DNS usage is activated, the email addresses of the recipients are resolved as MX or A/AAAA records and the connection is made directly to the SMTP server of the target domain (no mail relay).

If DNS is not activated, the mail server specified above is used as a mail relay.

Authorization

If the mail server expects a login, it can be activated here and the **username** and the **password** can be stored.

Transport Layer Security (TLS)

If the mail server requires secure communication, TLS can be activated and one of 3 modes can be selected.

- Full certificate check (default)
- Accept self-signed certificates
- Accept any certificate

10.27. Redial and dispatch control (SPLIT)

The configuration of the handling of faulty transmissions takes place under the menu sequence *Extras > System settings > Error processing* in the messaging server configuration. This is where the central dispatch control for errors in the ISDN protocol and in the fax protocol is located. The number of redials and the pauses between them can be configured for the individual error codes.

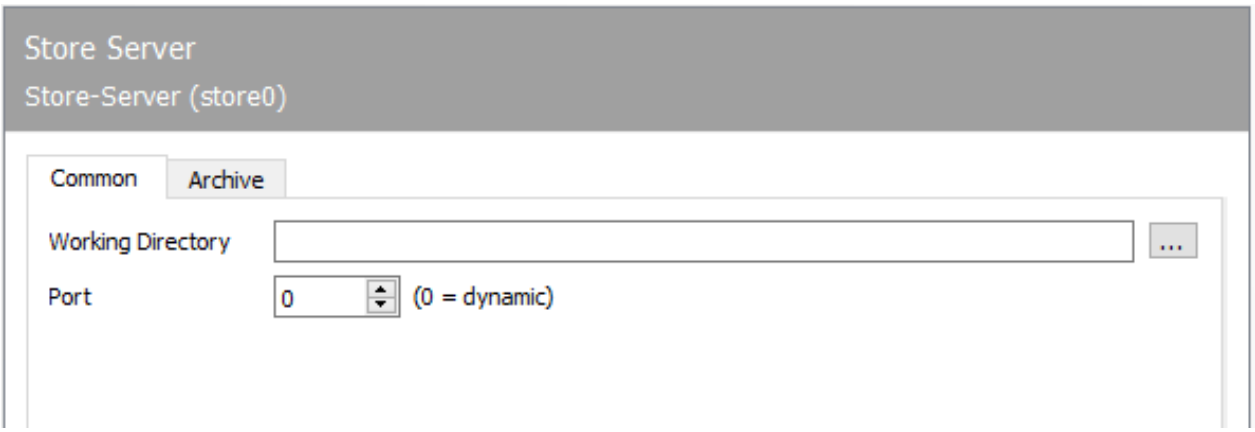
10.28. store servers

The voice messages are stored in the store server if *Store Native* or *SMTP/OfficeMaster Store* is selected in the *UNIVOICE* component on the General tab under *Delivery/access method*. If you select the last option, the voice messages are saved in the store server and then also sent to the corresponding mail system via SMTP. The corresponding SMTP settings are also set in the *UNIVOICE* component in the SMTP tab.

> **Note!**
> If voice messages are deleted via the phone, these are also automatically removed at file level.

By default, there is no existing store server in the OfficeMaster Suite.

To create the component, select > Voice Server > Store - Server > New Store Server component in the quick launch bar.



10.28.1. General

Working directory

A directory can be specified here, where the *STORE* component should store the voice messages.

> **Note!**
> No directory is specified in the delivery state. The voice messages are then saved in the directory %programdata%\ffums\fmsrv\work\store0\ and there in the respective subfolder of the corresponding voice box.

Ports

TCP/IP port for connection to the mail server. **0** stands for dynamic (delivery status).

10.28.2. Archive

Enabled

Target directory

Directory to which the voicemails are moved.

Items older than

Which voice messages to move in relation to age.

Time of day

When to move the voice messages on the system.

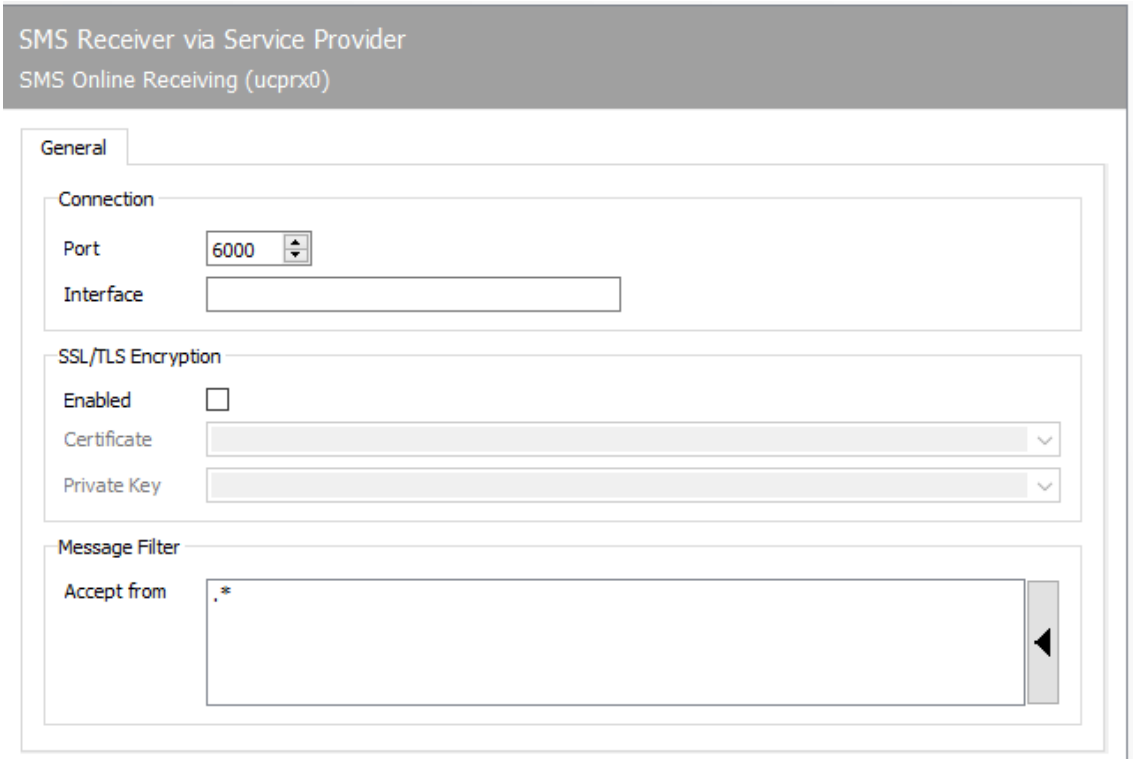
10.29. SMS reception via UCP

Obsolete

With the UCPRX component, SMS messages can be received via the UCP protocol.

Create component

The component is created via the quick start bar in the folder SMS > SMS reception via UCP and then via new *SMS recipient component*.



10.29.1. General

Connection

Ports

TCP/IP port on which the messages are received.

Interfaces

A special network adapter interface can be entered here. With the standard **0.0.0.0** all interfaces are “listened” to.

SSL/TLS encryption

Activate

If the encryption of the communication is to be used, then this checkbox must be selected.

Certificate

Private key

Message filter

Accept from:

The message filter has a direct influence on the incoming SMS messages. SMS messages from certain senders (calling party number) can be blocked here. With the default setting (.*), all SMS messages received via the UCPRX component are accepted and processed via the corresponding connector (msx2kgate, msxbcsgate, mailgw, etc.).

In the simplest case, an address filter consists of a list of numbers. For example, if SMS messages from mobile phone numbers starting with ***0152*** and ***0172*** are to be rejected, the two required rules could look like this:

-0172.* and -0152.*

The entries must be one below the other in the list. The minus sign must be specified explicitly so that the messages are rejected.

Entries in this list can also be summarized with regular expressions. The default value (.*) for the address filter is also a regular expression. The dot (.) stands for any character. The asterisk gives the character in front of it the meaning as often as you like. At this point, only one address can be specified per line. It is not possible to combine several expressions in one line using OR (|) or AND (&).

> **Note!**
> Entries that should explicitly match certain phone numbers must always be at the top of the list (above the **.*** entry).

10.30. Send SMS via UCP

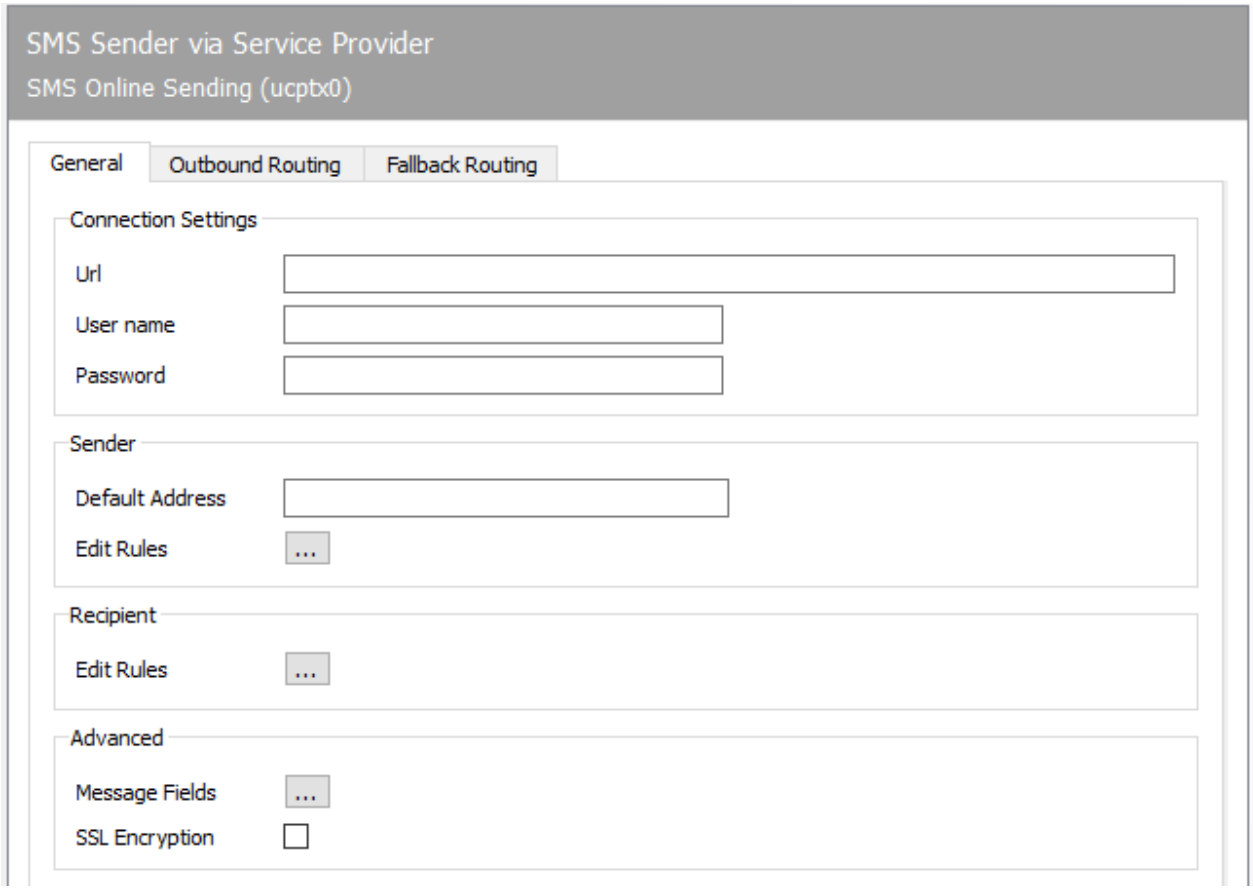
The UCPTX component can send SMS messages via the UCP protocol.

Obsolete

UCP is only offered to maintain backwards compatibility. For new setups please use the *SMS via IP component/SMPP*

Create component

The component is created via the quick start bar in the folder SMS > SMS dispatch via UCP and then via new *SMS dispatch component*.



10.30.1. General

Connection settings

URL

The URL of the UCP API is specified here. This information is provided by the UCP provider.

User name

A user name is required to log in to the UCP-API. Please take this information from your account at a UCP provider.

Password

A password is required to log in to the UCP-API. Please take this information from your account at a UCP provider.

Sender

Default address

If no sender address is specified in the order, this default address will be used.

Edit Rules

These rules govern the transformation of the sender address from orders into the sender format desired by the provider. Certain patterns are found in the address and then replaced accordingly.

Recipient

Edit Rules

These rules govern the transformation of the recipient address from the format supplied by the provider into the recipient address format used internally in orders. Certain patterns are found in the address and then replaced accordingly.

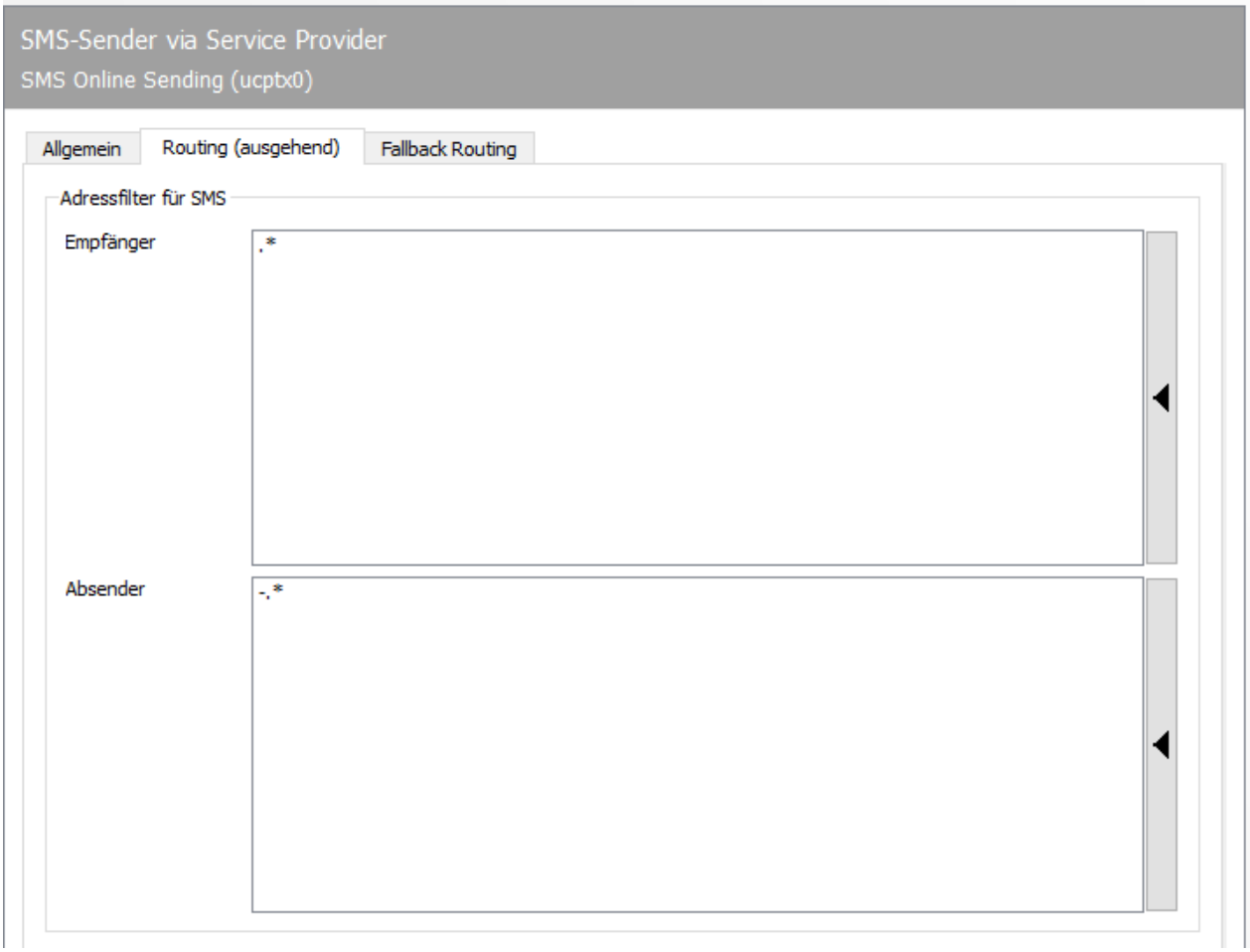
Extended

Message fields

The field names on the UCP API can be adjusted here in order to compensate for differences between providers. Normally this should not be changed.

SSL encryption

If the check box is activated, the connection to the UCP provider is established via TLS.



10.30.2. Routing (outgoing)

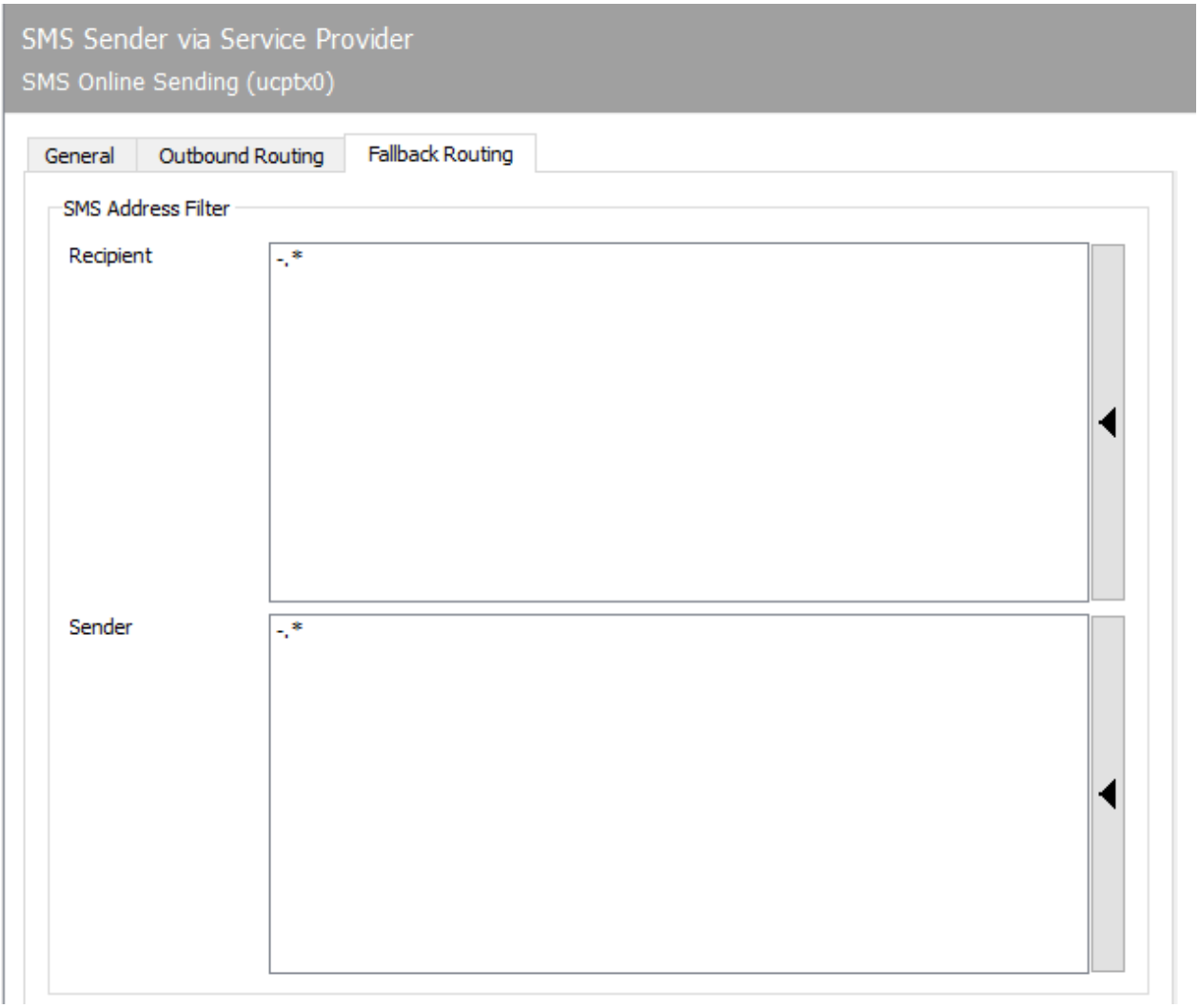
Address filter for SMS

Recipient

Here it is defined which destination number is routed via this component. By default, all destination phone numbers are routed via this component when an SMS is requested.

Sender

By default, all senders who are authorized to send SMS are routed via this component.



10.30.3. Fallback routing

Note!
Enable fallback mechanism must be activated in the *System settings* of the OfficeMaster Suite for the fallback settings to work.

Address filter for SMS

Recipient

Here it is defined which destination number is routed via this component in the event of a fallback. By default, all destination phone numbers are routed via this component when an SMS is requested.

Sender

By default, all senders who are authorized by SMS are routed via this component in the event of a fallback.

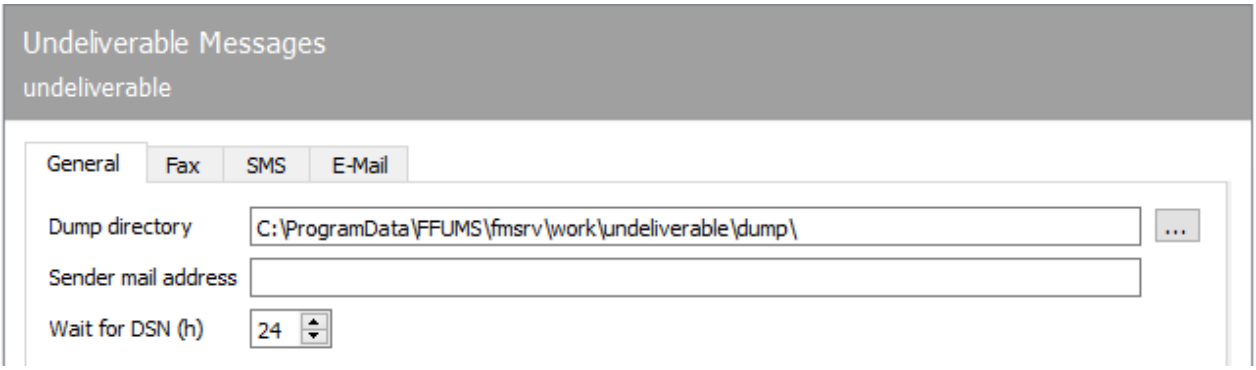
10.31. Undeliverable messages

Incoming messages (fax, SMS and e-mail) that cannot be assigned to a gateway within the messaging server are forwarded to the *Undeliverable* component.

The *Undeliverable* component has four different modes for handling incoming undeliverable messages:

- Mode *Dump*:
  The incoming message is stored in a directory on the server.
- Mode *Print* (only for fax):
  The incoming message is printed using a PRINTGW component and then filed.
- Mode *Forwarding*:
  The incoming message is forwarded to another address of the same type within the messaging server.
- Mode *Notification*:
  The incoming message is sent via SMTP to any internal or external mail recipient.

To configure *Undeliverable* choose Edit > Other Basic Components > Undeliverable Messages.



10.31.1. General

The framework parameters for the modes mentioned above are configured on the *General* tab.

Dump Directory

The undeliverable messages (fax, SMS, e-mail) are stored in the *Dump Directory*. Default value on Windows machines: **%ProgramData%\FFUMS\FMSRV\work\undeliverable\dump**

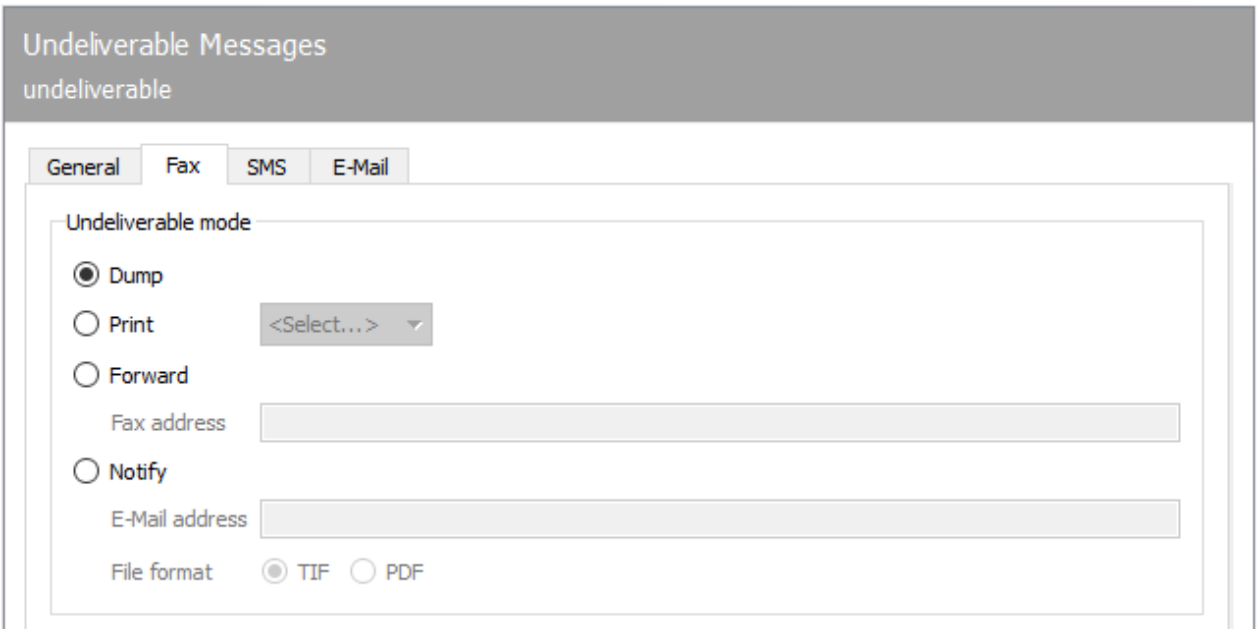
Sender email address

The *Sender email address* is used for the notification e-mail.

Wait for DSN (h)

The number of hours configured here determines how long *Undeliverable should wait for DSN* (Delivery Status Notification), which may follow a previous notification email, before the undeliverable message is deleted. The default value is **24** hours

> Note!
> So that DSN can be received by the messaging server, it must also be accessible externally under the configured *sender email address*. The desired mode for each individual message type (fax, SMS and e-mail) is configured on the following tabs.



10.31.2. Fax

Undeliverable Mode

Dump

After installation, *Undeliverable* runs in *Delivery* mode by default. All messages received and undeliverable in the messaging server are stored in the filing directory configured on the

General tab, along with all messages for which *Forwarding* or *Notification* failed. Two files are generated for each undeliverable message:

- A job file (recognizable by the file extension FMJ, contains all information about the process, including the file name of the document file).
- The document file (actual message).

Since the files in the dump directory are not processed by the messaging server, they remain stored there until they are deleted by the network administrator.

Print

The *Print* mode is only available for faxes. To do this, a configured PRINTGW component must be selected to which the document is to be delivered.

Forward

In the *Forwarding* mode, the undeliverable message is forwarded to a new address of the same type within the messaging server. The sender information is retained. A forwarding address must be stored for *forwarding*. This is an internal address of the same type (fax for fax, e-mail for e-mail). Forwarded documents that are undeliverable again are stored in the filing directory.

A fax is received from +49 123 456 on number 999. This number is not associated with any connector, so the operation is routed to Undeliverable. Forwarding to the internal fax address 960 is configured here for undeliverable fax messages. Undeliverable now generates a new incoming fax message to the forwarding number 960. However, the sender information of the remote station remains +49 123 456. The process is thus assigned to the connector responsible for 960, such as NOTESCONN, SAPCONN and MSX2KGATE.

Notify

If undeliverable incoming messages are to be sent by email, the *Notification* mode is the right choice. However, this also requires the operation of the messaging server components SMTPTX (for the notification mail) and SMTPRX (for any incoming status mails).

Furthermore, a sender address must be set on the *General* tab, which *Undeliverable* communicates with the e-mail notification (such as undeliverable@officemaster.firma.de). This e-mail address must be accessible externally so that *Undeliverable* is informed of any transmission errors via DSN (Delivery Status Notification).

For the notification mode, an external or internal e-mail address must be stored as a *notification address* to which undeliverable received messages are sent. For undeliverable fax messages, you can also choose between TIF and PDF as the file format for the fax attachment.

10.31.3. SMS

Non-delivery mode

Take off

After installation, *Undeliverable* runs in *Delivery* mode by default. All messages received and undeliverable in the messaging server are stored in the filing directory configured on the *General* tab, along with all messages for which *Forwarding* or *Notification* failed. Two files are generated for each undeliverable message:

- A job file (recognizable by the file extension FMJ, contains all information about the process, including the file name of the document file).
- The document file (actual message).

Since the files in the storage directory are not processed by the messaging server, they remain stored there until they are deleted by the network administrator.

Redirect

In the *Forwarding* mode, the undeliverable message is forwarded to a new address of the same type within the messaging server. The sender information is retained. A forwarding address must be stored for *forwarding*. This is an internal address of the same type (fax for fax, SMS for

SMS, e-mail for e-mail). Forwarded messages that are undeliverable again are stored in the filing directory.

An SMS is received on number 998 from +4917277777. This number is not associated with any connector, so the operation is routed to Undeliverable. Forwarding to the internal SMS address 961 is configured here for undeliverable SMS messages. Undeliverable now generates a new incoming SMS message to the forwarding number 961. However, the sender information of the remote station remains +4917277777. Thus, the process is assigned to the connector responsible for 961, such as NOTESCONN, SAPCONN and MSX2KGATE.

Notification

If undeliverable incoming messages are to be sent by email, the *Notification* mode is the right choice. However, this also requires the operation of the messaging server components SMTPTX (for the notification mail) and SMTPRX (for any incoming status mails).

Furthermore, a sender address must be set on the *General* tab, which *Undeliverable* communicates with the e-mail notification (such as undeliverable@officemaster.firma.de). This e-mail address must be accessible externally so that *Undeliverable* is informed of any transmission errors via DSN (Delivery Status Notification).

For the notification mode, an external or internal e-mail address must be stored as a *notification address* to which undeliverable received messages are sent. For undeliverable fax messages, you can also choose between TIF and PDF as the file format for the fax attachment.

10.31.4. email

Non-delivery mode

Take off

After installation, *Undeliverable* runs in *Delivery* mode by default. All messages received and undeliverable in the messaging server are stored in the filing directory configured on the *General* tab, along with all messages for which *Forwarding* or *Notification* failed. Two files are generated for each undeliverable message:

- A job file (recognizable by the file extension FMJ, contains all information about the process, including the file name of the document file).
- The document file (actual message).

Since the files in the storage directory are not processed by the messaging server, they remain stored there until they are deleted by the network administrator.

Redirect

In the *Forwarding* mode, the undeliverable message is forwarded to a new address of the same type within the messaging server. The sender information is retained. A forwarding address must be stored for *forwarding*. This is an internal address of the same type (fax for fax, SMS for SMS, e-mail for e-mail). Forwarded messages that are undeliverable again are stored in the filing directory.

Notification

If undeliverable incoming messages are to be sent by email, the *Notification* mode is the right choice. However, this also requires the operation of the messaging server components SMTPTX (for the notification mail) and SMTPRX (for any incoming status mails).

Furthermore, a sender address must be set on the *General* tab, which *Undeliverable* communicates with the e-mail notification (such as undeliverable@officemaster.firma.de). This e-mail address must be accessible externally so that *Undeliverable* is informed of any transmission errors via DSN (Delivery Status Notification).

For the notification mode, an external or internal e-mail address must be stored as a *notification address* to which undeliverable received messages are sent. For undeliverable fax messages, you can also choose between TIF and PDF as the file format for the fax attachment.

10.31.5. LDAP connector for voicemail

For receiving voicemails in the *Cyrus IMAP Server* from *SuSE, Open-Xchange* and *Netline Open-Xchange* or in *Novell GroupWise*, OfficeMaster Suite includes the voice connector *UNIVOICE*, which forwards received voicemails to the mail recipients via SMTP and accesses user mailboxes via IMAP for remote access.

UNIVOICE can be used as a voice gateway in environments without Microsoft Exchange Server or Lotus Domino. The table below shows the differences between each voice gateway.

Use of the various connectors for voicemail:

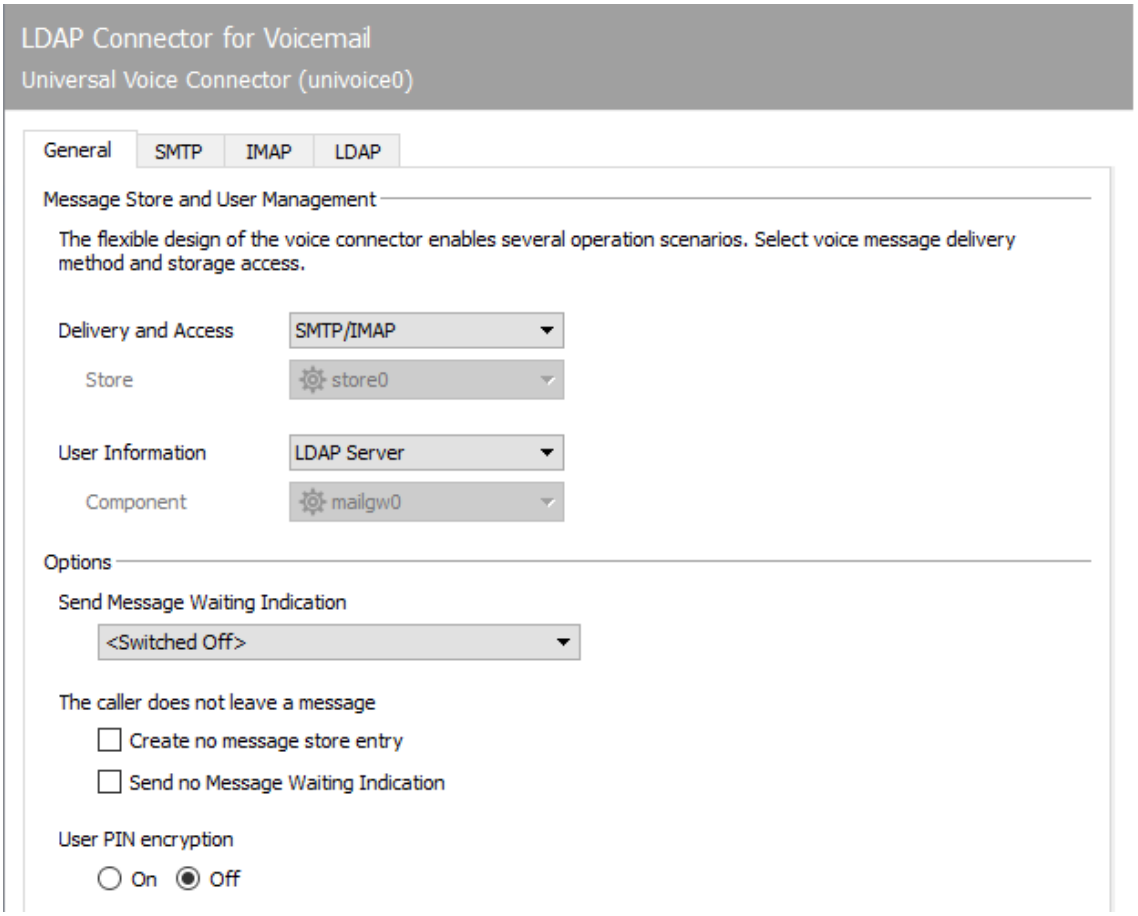
Voice Connector	**UNIVOICE**	**NOTESCONN**	**MSX2KGATE**	**CLIENTGW**
Environment	SMTP mail server	Notes/ dominoes	Microsoft Exchange	Web Connector
Supported mail servers/locations	Cyrus IMAP Sever, Novell GroupWise, Store Server	Notes/Domino Server	Microsoft Exchange	SQL
Deliver received voicemails	SMTP, Proprietary	Notes Mail	MAPI	Web Services
User management and access to user master data	LDAP, Proprietary	Notes API (name and	ADSI	SQL
Access to user mailboxes	IMAP, Proprietary	Notes API (User Mailbox)	MAPI	SQL

The following settings are required to operate the *UNIVOICE* connector:

- Access to user data (LDAP authorizations, field mapping),
- Access to user mailboxes (permissions) and
- E-mail dispatch via SMTP (relay server)

Create voice connector

To create a new Univoice connector, either select the *new component* option under LDAP/IMAP of the Voice folder in the quick start bar or switch directly to the component table via the *Edit* menu and then use the *Create component* option. *Universal Voice Gateway (UNIVOICE)* is selected as *Component Type*.



10.31.6. General

Message storage and user management

When using UNIVOICE you can combine different scenarios. To do this, configure the delivery/access method to the message store and set the component to be used for local storage. In addition, you select the type of user data storage.

Delivery/Access Method

- OfficeMaster Store Native
- SMTP/IMAP

If you activate this option, the SMTP and IMAP tabs become active and you can make the necessary settings there.

Store

The possible options vary depending on the chosen delivery method. The corresponding store server, which has already been created, would have to be selected here.

Access to user mailboxes and user data

If the voice user data is to be administered in an LDAP-enabled directory service, access to the directory server must be configured using the _User Information _button. The LDAP connection itself is configured under the *LDAP* tab.

User information

When selecting the *Users* tab, the user management mode can be selected. Configuration options are offered depending on the storage location of the user (LDAP or Mailgw) and must then be configured separately using the corresponding tab.

Component

The possible options vary depending on the selected user information source (LDAP, Mailgw, etc.)

Options

Send message waiting indication

Choose between the different options to activate and deactivate message waiting.

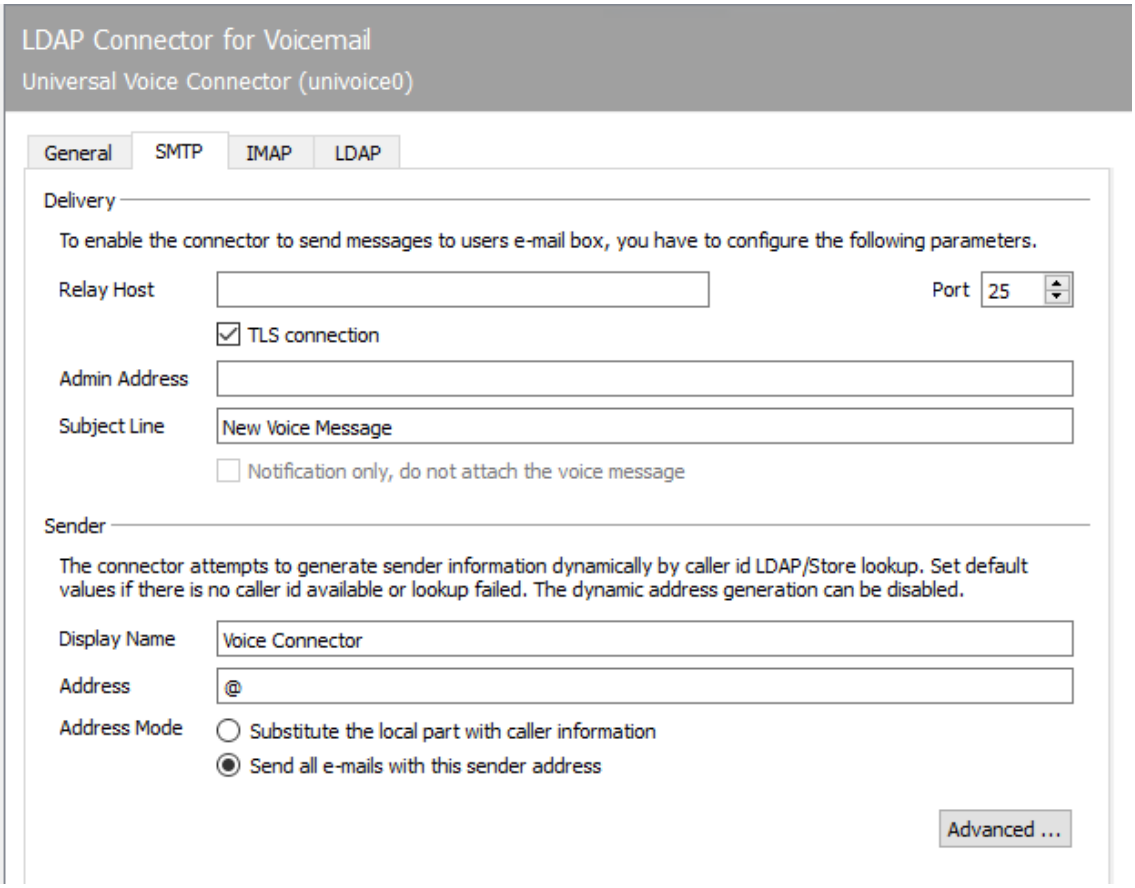
The caller does not leave a message

Here you configure the behavior for calls where the caller has not left a message. In many cases, it makes sense not to send a notification either, since missed calls may have already been recorded via the CTI solution.

- Do not create an entry in the message store.
- Do not send Message Waiting.

PIN encryption

Activate this option if the PIN is to be stored in encrypted form.



10.31.7. SMTP

If you select the *SMTP* tab, the settings for the SMTP delivery of voice mails to the user mailbox can be made in the user interface.

Delivery

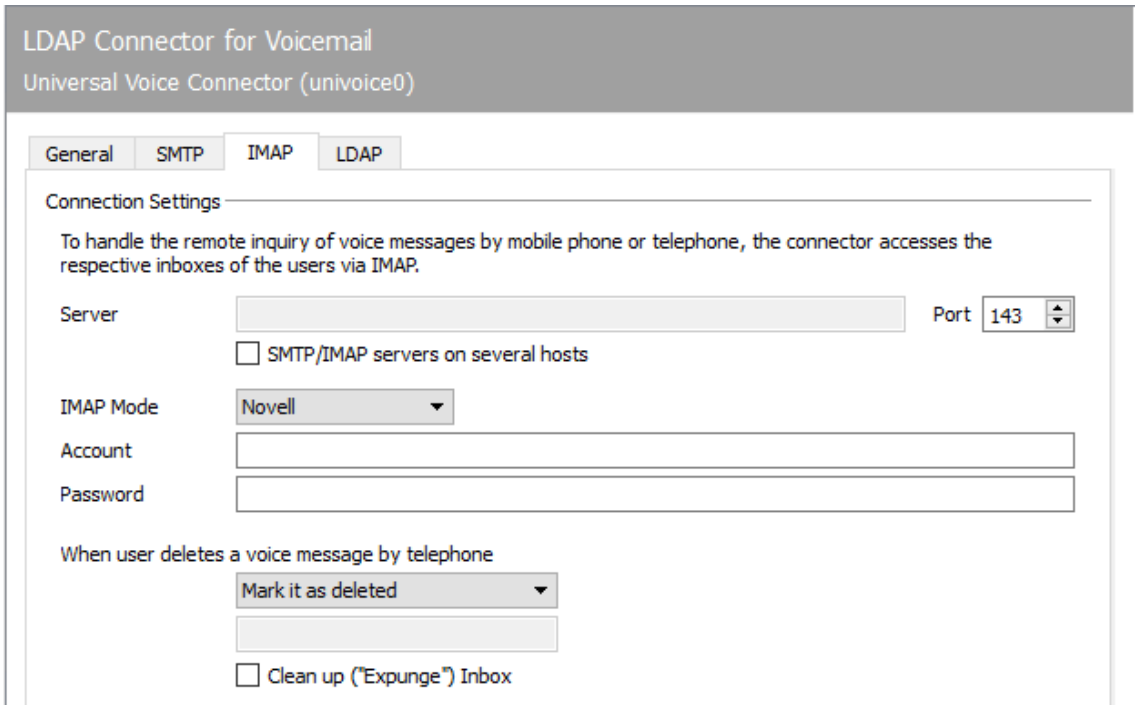
The e-mail server for sending the data and a destination address for undeliverable messages must be entered in the *Delivery* area.

Sender

The appearance of the subject, the sender address and the displayed sender name can be set under *Sender*.

Advanced settings

In the case of an incomplete e-mail address in LDAP, an additional suffix can be specified for *E-Mail Address Modification*.



10.31.8. IMAP

Communication with the IMAP server can be determined on the *IMAP* tab.

Connection settings

The access mode to the IMAP server, which determines the login behavior of the gateway, is to be selected under *Connection settings*. With some IMAP servers, the selection of the authentication mode is necessary for the full range of functions of the connector.

Server and port

The name or IP address of the IMAP server must be entered in the *Server* field. In addition, it is possible to specify a different TCP port for the connection than the standard port **143** in the *Port* field.

IMAP mode

Currently *Novell*, *Cyrus*, *Apple* and *UserLogin* modes are supported.

UserLogin is a generic mode and works with all common IMAP servers. The gateway logs on to the IMAP server with the respective username and password of the target mailbox.

Special modes are provided for *Novell Groupwise* and the *Cyrus IMAP Server* to allow access to the message store. The voice system can be accessed without specifying user passwords.

Account and password

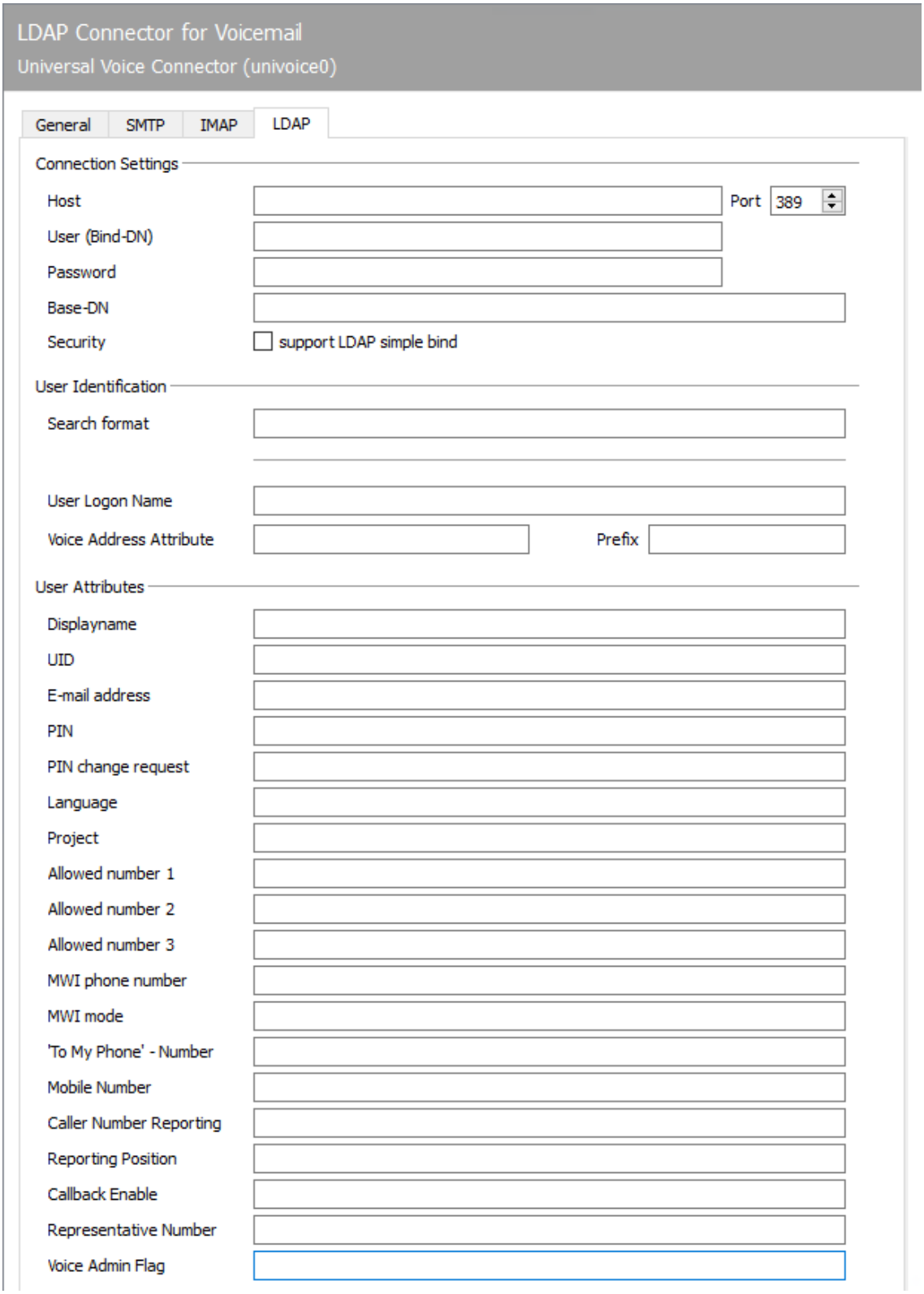
The *Account* and *Password* fields are assigned differently depending on the mode. The fields are deactivated for *UserLogin* because the information for the login is taken from the user administration. In the *Novell* mode, you write the name of the trusted application in the Account_ field and the appropriate key in the *Password* field. This information can be determined with the *OfficeMaster Trusted Application Wizard* program. When connecting to a *Cyrus IMAP server*, the username and password of an authorized user who has access to all mailboxes concerned must be entered in the fields.

When user deletes a voice message by telephone

If the message is deleted during remote inquiry, one of the following behavior can be selected:

- Move to “Trash” folder
- Mark as deleted
- Move to a folder <FolderName>

Note!
If you select the ***Clean up inbox*** checkbox, all voice messages that have already been marked as deleted are irrevocably deleted.


LDAP Connector for Voicemail
Universal Voice Connector (univoice0)
General
SMTP
IMAP
LDAP
Connection Settings
Host
Port
389
User (Bind-DN)
Password
Base-DN
Security
support LDAP simple bind
User Identification
Search format
User Logon Name
Voice Address Attribute
Prefix
User Attributes
Displayname
UID
E-mail address
PIN
PIN change request
Language
Project
Allowed number 1
Allowed number 2
Allowed number 3
MWI phone number
MWI mode
'To My Phone' - Number
Mobile Number
Caller Number Reporting
Reporting Position
Callback Enable
Representative Number
Voice Admin Flag

10.31.9. LDAP

Connection settings

Host; Port; User (Bind DN); Password; Base DN:

Access to user data via LDAP is suitable for avoiding duplicate user maintenance. Under the connection settings, all LDAP server connection information must be specified. This includes the *host* and *port* at which the server can be reached, the bind DN, a user and password for accessing the LDAP server, and a *base DN* to limit the search scope.

User identification

Search format

A phone number is assigned to a user using a formula that is stored under *Search format*. Here is the placeholder for the incoming phone number **%s**.

Login Name

The field in the LDAP scheme that supplies the user's login name is specified here. This can be used to map a user name to a phone number.

Voice address attribute

The field in the LDAP scheme that supplies the user's extension or phone number is specified here. This can then be used to map phone numbers to user names.

Prefix

If only parts of the phone number (e.g. only extension) are maintained in the LDAP, a complete (e.g. E.164) phone number can be generated from this with this prefix.

User Attributes

In the *User Attributes* area, the fields in the LDAP schema that contain information relevant to voice can be specified.

Useful pre-assignments can be chosen using the “Load Template” button in the actions-panel on the right side. There you can load LDAP values according to the target system. Changes already made will be lost after selecting this option!

10.32. Voicemail server

With the license *Extension for Voicemail* the functions of the voicemail server contained in the OfficeMaster Suite are activated. The general relationships are explained below.

10.32.1. Overall process of voice communication

In contrast to faxes, with voice calls a decision must be made as soon as the call is accepted for which user the call is intended and what behavior should occur. When the call is accepted, it must be decided which project, which announcement and which language are to be used. Accordingly, an incoming voice call is significantly more time-critical than a fax, to which the entire IT infrastructure must be adapted.

Sequence of a voice call

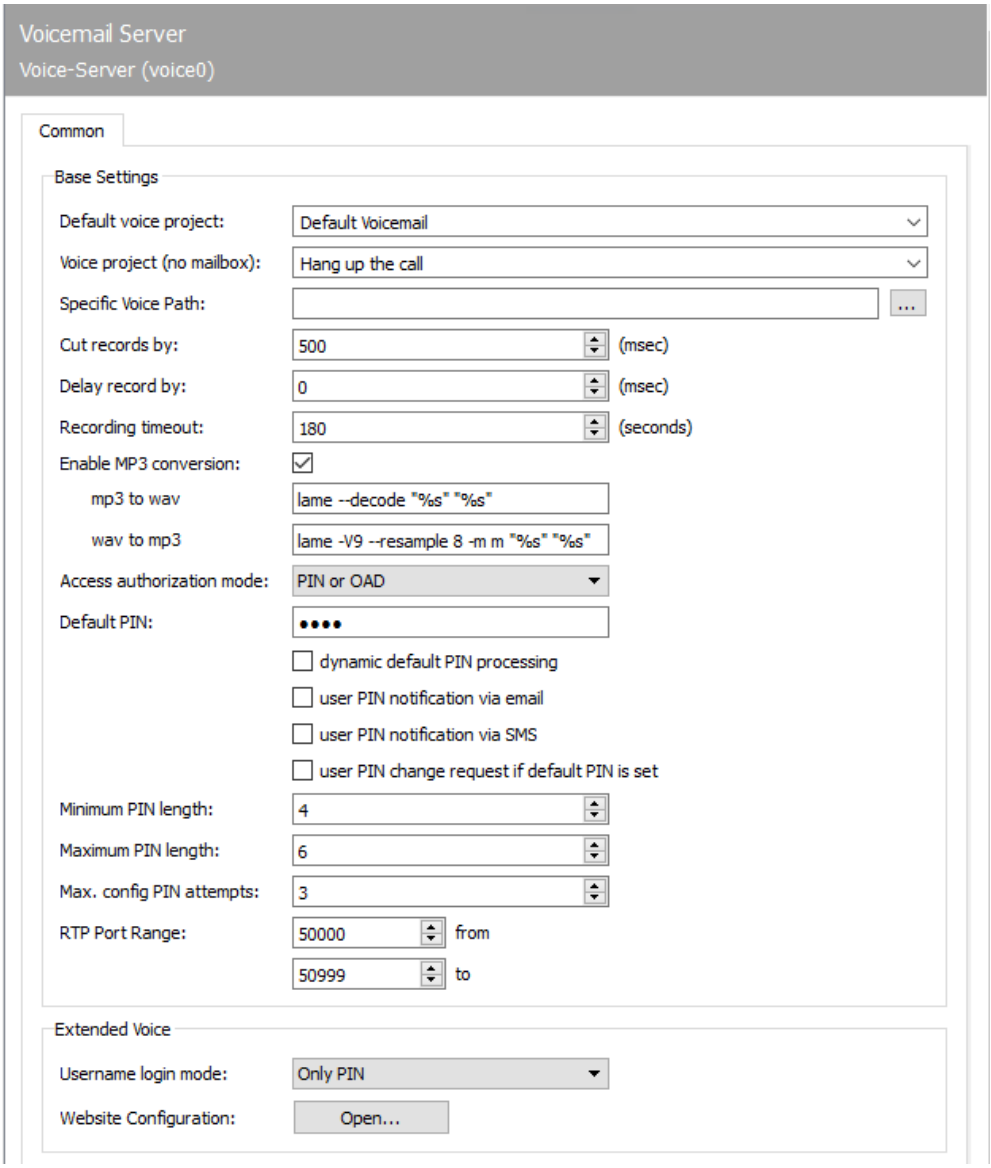
- The call is established from a SIP trunk and thus the SIP component or an OfficeMaster Gate in the direction of the hardware controller of the messaging server.
- The hardware controller or the SIP component determine the voice connector associated with this call (e.g. *msx2kgate*) and the corresponding voice server (usually *voice0*). All transmitted phone number elements can be used for this determination (called/to, calling/from, redirected /diversion/history, etc.).
- The voice server establishes a UDP connection to the IPMedia process or OfficeMaster Gate and handles direct communication.

  Note!
  A corresponding rule may have to be set up in the Windows Firewall for the outgoing connection from the voice server. A clear sign of firewall problems is when the fax signal can be heard during test calls to fax numbers, but not the corresponding standard announcement for calls to voice boxes.

10.32.2. Creation of the component

A new voicemail component is created via the Voice > Voicemail Server > *New Voicemail Component* quick launch bar.

Note!
This component must also be created if the Univoice component is used.



10.32.3. General

Base settings

Default Voice Project

If no voice project is stored for a called and identified mailbox, the project specified here is used.

Voice project (no mailbox)

Defines the voice project if no user mailbox was found.

Alternative project tree path

Change this path if the projects and the personal announcements should be in a different path. This means that even after updates, any individually adapted query menus remain up to date. This setting can also be used for redundant and failover systems.

Trim recording, delay recording

After the caller leaves a message, hanging up the phone may end the call. Since loud noises are still transmitted with some telephones when you hang up, the voice server can shorten the recording. In addition, the voice server can delay the recording. Both specifications are given in milliseconds.

Maximum recording time

It is possible to prolong the recording time to accept longer voice messages.

MP3 conversion active

By default, all voicemails are delivered to the user in MP3 format. Since MP3 is a less memory-intensive audio format compared to WAV, it is recommended to keep the default setting. The MP3 format requires only a tenth of the storage capacity of a WAV file with the same content to store the same audio data. The voicemail message is converted into MP3 format using an external converter.

> Note!
> The OfficeMaster Suite also supplies the “*Lame*” (freeware) program as a converter.

Access Permission

The phone number of the caller (*Calling Party Number*) or the PIN code can be used for the authorization check for remote inquiry. By default both methods are allowed. That means: A caller can use the remote inquiry either by calling from an authorized telephone or by entering the PIN code.

Alternatively, the authorization can be reduced to one of the two features centrally on the voice server, so that only those callers who are either calling from an authorized number or who know the PIN can access the voice box remotely. “PIN and OAD” means that both criteria apply.

Default PIN

If no PIN was set for the User and the Connector, the default PIN can be changed here.

- Dynamic PIN generation:
  If you choose this option, a static standard PIN is not used. Each user without their own PIN initially receives a dynamic PIN.
- PIN will be emailed to user:
  This option is automatically “forced” on as soon as a dynamic default PIN is generated and used.
  The first time the voice mailbox is called up by the user or by a caller, the mailbox owner receives the corresponding message.
- PIN will be sent to user via SMS:
  In addition, the PIN can also be sent to the user via SMS.
- User must change the PIN if this is the default PIN:
  The first time the voice mailbox is checked, the user must change the PIN.

Minimum and maximum PIN length

The permitted PIN length is defined with these parameters.

Max. config PIN attempts

Defines the number of failed attempts during PIN authentication.

RTP Port Range

Defines the default Port range used for audio signals inside the network.

Script parameters

In some cases it can be useful to enlarge or shorten the timer for announcements. Here you can define the timers in detail. All timers are displayed in seconds. If you don’t know the appropriate timer – please contact our support team.

10.32.4. Supplied projects in the voice system

After installation, OfficeMaster provides several projects that can be used without major administrative effort and provide various basic functions. These projects are created in "..\data\voice" of the messaging server in the form of subfolders with a description file and LUA script.

The voice system consists of several projects connected one after the other, between which one constantly switches. These projects are to be understood as individual states in a state graph. There are often multiple entry and exit points.

In order to maintain a certain overview, not all projects can be selected as start projects. Which is loadable or not is defined in the respective *.ini* file by the *loadable* flag.

Voicebox via Pilot ID

- projectvoxdidcpn
  The calling party number is set to the called party number, after which the jump to the Extended Voicemail project (*eVoice_projectStart*) takes place.

Extended Voice

The individual projects take on the following tasks:

- eVoice_projectStart
  Entry point with setting the individual values for the variables.
- eVoice_projectrecord
  Recording a voice message
- eVoice_projectPlayAudio
  If the recording is deactivated for a period of time or a voice box, only the desired announcement is played and then hung up.
- eVoice_projectAnnouncementFromPhone
  Recording of your own announcements controlled via the web interface.
- eVoice_projectAnnouncementToPhone
  Playback of your own announcements controlled via the web interface.

Recording function

- projectrecordcall
  When this project is called, a short message is given that the call is being recorded and then the recording is started. After the end of the call, a message with the corresponding recording is sent to the user.

  For reasons of storage space, it is strongly recommended to activate the audio conversion to .mp3!

Selection of the Voicebox to be called

- projectvoxdid, projectdid
  The caller is prompted to select which voice box he wants to be connected to by pressing a button.

“Recording Studio”

- projectrecstudio
  Recording an announcement especially for creating announcements for IVRs. Generates an audio file in the valid file format for further use in the system.

IVR templates

Example of scripting your own IVR with the most important functions.

- ivrExample_start
  Entry point with timetable, public holidays, etc.
- ivrExample_normal
  The company is open, the caller can choose to connect to another subscriber or leave a message.
- ivrExample_closed
  The company is closed, the caller is played an announcement.

10.32.5. Basic configuration of Webvoice

The OfficeMaster Suite setup lays the foundations for the interaction between the voice server and the components of the web services. The *Internet Information Service* (*IIS*) is created and activated as a feature of the Windows server.

The corresponding web pages for the IIS are made available under %Program Files% \FFUMS\fmsrv\Webservice. The user login mode must first be configured so that the user can later log in to the website with his created name.

Username login mode

- PIN: this means the PIN of the voicemail box.
- PIN or user password: PIN of the voice mailbox or password of the user.
- User password: User's password.

To configure the web services, various configuration files of the IIS and OfficeMaster would normally have to be called up. With the tool *FClientGwCfgPrg* (can be called up via the configuration of the component *VOICE* via *Web Page Configuration*) access to these files is much easier.

Start of the configuration program website configuration

- The address of the website to be configured is entered here. If the standard address was not changed manually on the IIS after installation, this is either *http://SERVERNAME/ums* or *http://SERVERNAME/fax*.

configuration password

- In the delivery state, access to the configuration is protected by the password *OfficeMaster!*.

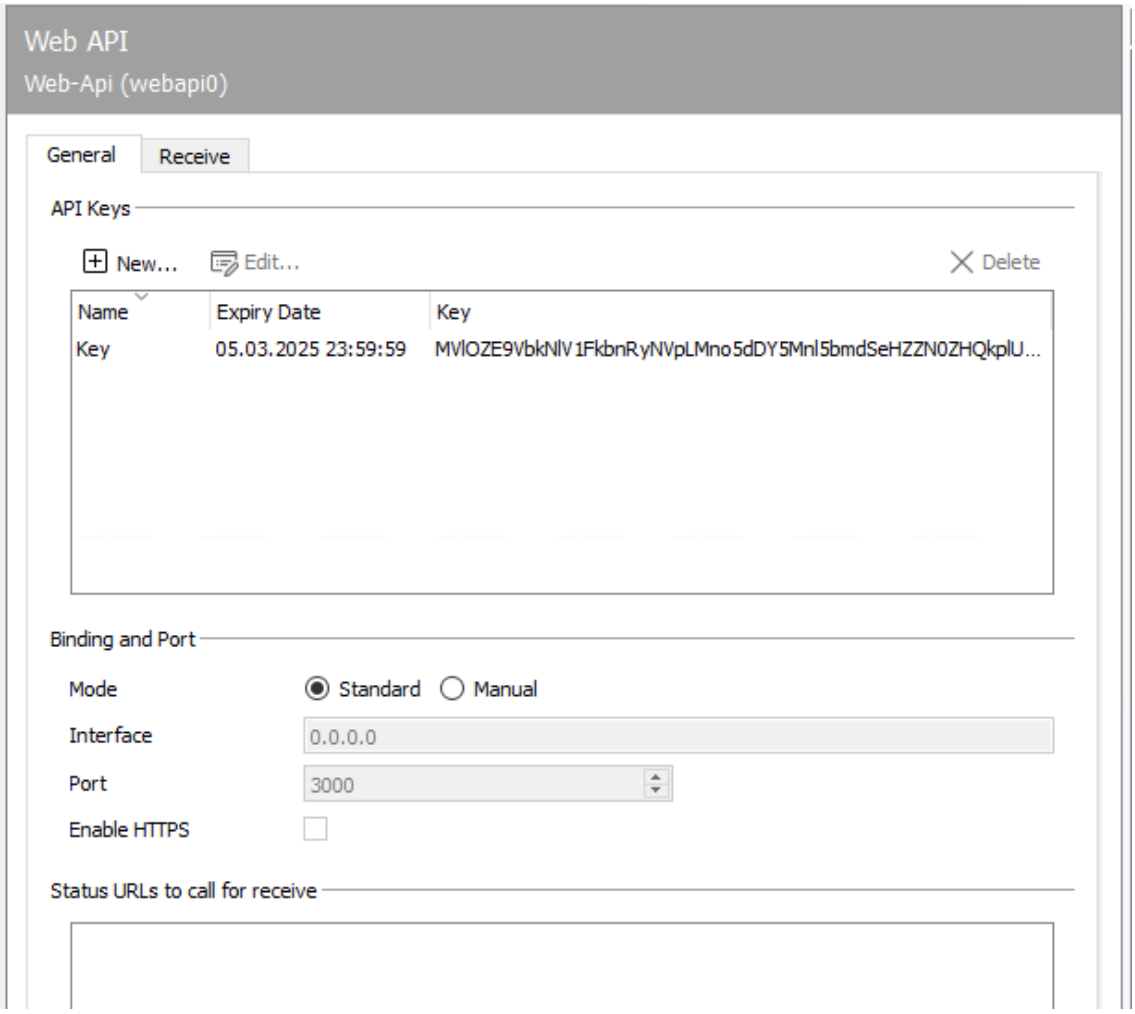
After successfully logging on to the server, the operating mode of the website, the voice server and the corresponding connector for the user information must be configured.

10.33. Web API

The Web API component provides an API via HTTPS. The API documentation is available at https://{host}:3216/webapi/v2/doc/. For older applications, there is still the API v1, which is not recommended for new developments. A Web API component must be set up and started to access the documentation.

The component can be used to transfer orders to the messaging server via the REST API and receive status messages using the response URI. This enables integration into existing software applications such as CRM systems.

Fax, SMS, print, e-mail and X-invoice orders can be created.



10.33.1. General

API keys

Authentication at the Web-API takes place via API keys. These are displayed in the list of API keys (name, expiration date, key). New API keys can be created by clicking on the '+' symbol; when creating a key, a comment and optionally an expiration date can be entered. By clicking on the '-' symbol, the selected API key is deleted. This means that access to the Web-API is no longer possible with this key.

Binding and port

In the default setting, the Web-API component is bound to the localhost address and is addressed by a reverse proxy in the GateKeeper. The local port number is assigned dynamically by the controller of the messaging server. This operating mode is active if the mode is set to "Standard". In this case, the component is accessible via a dynamic port under both IPv4 and IPv6.

However, it may also be desirable to run the Web-API component on any static port. To do this, the mode must be set from "Standard" to "Manual". As the mechanism with the reverse proxy then no longer works, in this case it must also be bound to an externally accessible IP address (e.g. 0.0.0.0 or :: or the address of a network interface).

Status URLs to call for feedback messages

Status URLs can be entered here which are called up for status confirmations of send orders. These URLs are only used if no separate status URLs have been specified in the order itself.

10.33.2. Reception

A feature of the Web-API is that incoming jobs can be delivered via HTTP POST. To deliver jobs, you must first register, whereby a distinction is made between static and dynamic receive status URLs:

- Static receive status URLs:
  - Are registered via the component configuration
  - Do not have an expiry time
- Dynamic receive status URLs:
  - Are registered by a client via the API interface (`/webapi/v2/receive`)
  - Expire after a configurable time (default: 5 minutes)

- Must be renewed regularly

To ensure the delivery of jobs, undeliverable receive notifications are repeated regularly until they can be delivered or the maximum number of send attempts (see `Receivestatus send retry count`) has been reached. The failed attempt counter is reset when the receive status URL is registered again.

The documentation of the API interface can be found at `https://<ip-address>:3216/webapi/v2/doc`.

Note! The component must be started to access the documentation.

Feedback URLs to call for matching receive jobs

Static Receive Status URLs

Static URLs can be entered here that are called up by the Web-API component as soon as a job has been received that matches the receive filters.

Keepalive Timeout

Determines the time after which the registration of receive notifications expires. If the receive filter and receive status URLs are not re-registered within this period, they are discarded. Permanent entries can only be achieved via the static receive status URLs and corresponding receive filters.

Number of send attempts for receive status messages

Specifies the number of retries for a receive status message. A receive status message is only repeated if the web server cannot be reached. A status message is only considered received if the web server responds with the status code `OK (200)` or `Accepted (202)`.

Fax

Fax reception activated

If fax reception is enabled, received jobs are sent to the specified static receive status URLs if the address filter applies to the job.

Address filter

Address filters can be specified here using regular expressions, which restrict which jobs reach the Web-API and are delivered to the static receive status URLs accordingly.

Document type filter

The document type filter restricts that only jobs containing the specified file types are delivered.

Sms

SMS reception activated

If SMS reception is enabled, received jobs are sent to the specified static receive status URLs if the address filter applies to the job.

Address filter

Address filters can be specified here using regular expressions, which restrict which jobs reach the Web-API and are delivered to the static receive status URLs accordingly.

Document type filter

The document type filter restricts that only jobs containing the specified file types are delivered.

10.34. XRechnung eInvoice Send Component

Since November 27, 2020, contractors from the federal, state, municipal and public institutions may only send them the invoice electronically in XRechnung format.

The XRechnung is the German variant of the UBL invoice (universal business language) and contains invoice data with a standardized schema in XML format. XRechnung is version 2.0.0 (version of June 30, 2020) and conforms to the European standard EN 16931-1. The XRechnung standard has been operated by the Coordination Office for IT Standards (KoSIT) since January 1, 2019. The currently valid version can be found on the KoSIT website

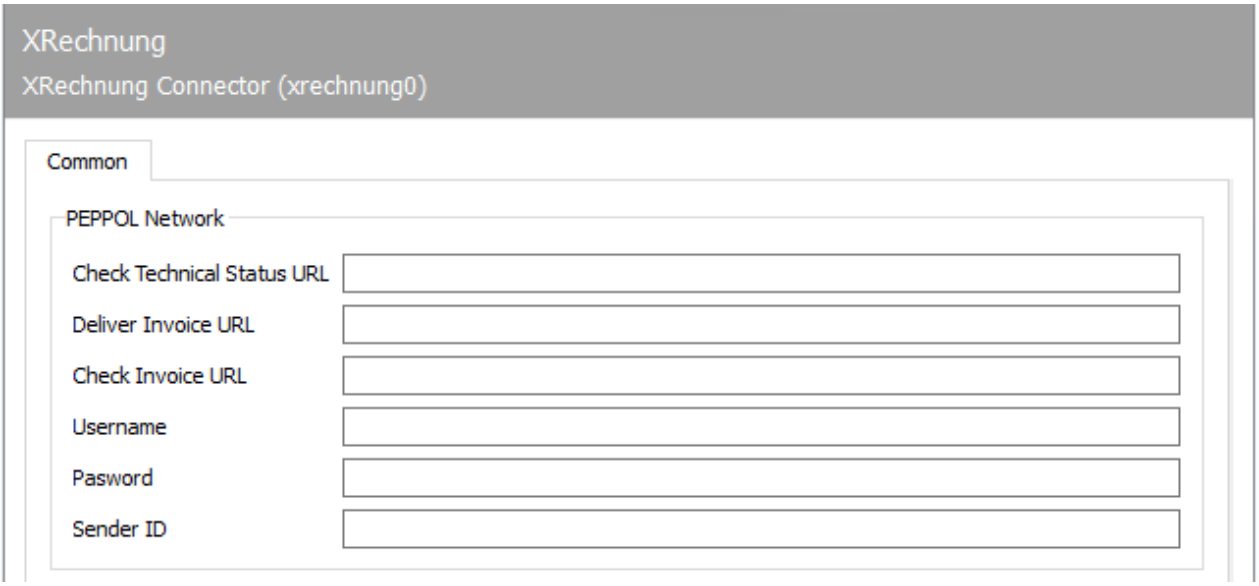
Peppol (Pan-European Public Procurement OnLine) is an originally European and now international consortium. It enables companies and government agencies to exchange standards-based electronic documents via the Peppol network. Peppol Access Points (Access Points) connect users to the Peppol network and exchange electronic data based on the PEPPOL specification. Participants can choose their preferred provider to exchange data with all Peppol participants.

The routing ID enables the electronic invoice to be addressed and forwarded to the downstream invoice processing systems. The route ID consists of 2...12 digits for general addressing, up to 30 digits for detailed addressing and 2 check digits. The rough addressing consists of two digits for federal/state, one digit for the administrative district, two digits for the district and 3, 4 or 7 digits for the municipality. The first two digits (federal/state addressing) have the following values:

- 01 Schleswig Holstein
- 02 Hamburg
- 03 Lower Saxony
- 04 Bremen
- 05 North Rhine-Westphalia
- 06 Hesse
- 07 Rhineland-Palatinate
- 08 Baden-Württemberg
- 09 Bavaria
- 10 Saarland
- 11 Berlin
- 12 Brandenburg
- 13 Mecklenburg-Western Pomerania
- 14 Saxons

- 15 Saxony-Anhalt
- 16 Thuringia
- 99 frets
    - 991 - direct federal administration or a constitutional body and receives electronic invoices via the ZRE.
    - 992 - indirect federal administration or federal state and receives electronic invoices via the OZG-RE.
    - 993 - indirect federal administration and receives electronic invoices via its own solution (neither ZRE nor OZG-RE).

The XRechnung component of the OfficeMaster Suite can send invoices to a Peppol Access Point. This will deliver the invoice to the actual invoice recipient in the Peppol network using the route ID. To do this, a provider for a Peppol Access Point must be selected and the corresponding access data must be stored in the configuration of the component.



10.34.1. General

URLs of the Peppol provider

There is a large number of providers connected to the Peppol network (https://www.e-rechnung-bund.de/peppol/). A list of providers can be found at https://peppol.eu/who-is-who/peppol-certified-aps/ . The URLs under which the provider's Peppol API can be reached is entered here.

- Check Technical Status URL: URL to qeury status information of the Peppol provider
- Deliver Invoice URL: Used to send XRechnung invoices via the Peppol provider.
- Check Invoice URL: Query if any invoices can be received from the Peppol provider.

Username

The username is assigned by the Peppol provider and is used for identification and authentication.

Password

The password is a user's secret key.

Transmitter ID

With this value, the user is identified as a participant in the Peppol network.