PBX Call Assist 5 UCServer

8.11.0.12763

1 Willkommen zum PBX Call Assist 5 UCServer 8
2 PBX Call Assist 5 UCServer 9
3 The PBX Call Assist 5 Client 10
4 Application scenarios 12
4.1 Application in a workgroup 12
4.2 Use in a Windows® domain 12
4.3 Use in a Windows® domain 12
4.4 Application with Terminal Server 13
4.5 Application with Roaming Users 13
5 Installation 15
5.1 System requirements 15
5.2 Preparation for installation 15
5.3 Active Directory® integration 16
5.4 Start installation 17
6 Setup 19
6.1 Login 19
6.2 Server name and server role 19
6.3 Presence domain 19
6.4 Network interfaces 20
6.4.1 Network interface properties 21
6.5 Certificate 22
6.6 Upgrade 22
6.7 Server reboot 23
6.8 Licenses 23
6.9 Database 24
6.10 User database 24
6.11 User authentication 25
6.12 Global settings 26
6.13 Location 28
6.13.1 TAPI lines 29
6.14 Remote Office 30
6.15 Setup finished 31
7 Administration 32
8 Server administration 33
9 General 34
9.1 Licenses 34
9.2 User database 35
9.3 Security 36
9.3.1 Advanced Active Directory® settings 36

9.4 User authentication ... 37
9.5 Database ... 38
9.6 Events ... 40
9.7 Online licenses ... 41
10 Telephony ... 43
10.1 Lines ... 43
10.1.1 TAPI lines ... 43
10.1.2 SIP Softphone Lines ... 46
10.1.3 SIP softphone via SIP trunk ... 53
10.2 Initial Location Setup ... 54
10.3 Location ... 55
10.3.1 Area code rules ... 55
10.3.2 Dialing prefix rules ... 56
10.3.3 PBX system ... 57
10.3.4 Formatting rules ... 62
10.3.5 Least cost routing ... 63
10.3.6 Advanced ... 65
10.3.7 Vanity ... 66
10.3.8 Projects ... 66
10.3.9 Remote - TAPI driver ... 68
10.3.10 Check rules ... 68
10.3.11 Location concepts ... 69
10.4 Telephone journal ... 72
10.5 Unanswered calls ... 73
10.6 Error handling ... 74
11 User management ... 76
11.1 User ... 76
11.2 Free additional fields ... 81
11.3 Voice Services - Users ... 81
11.3.1 Assign phone devices ... 81
11.4 Groups ... 82
11.5 PN_PBXVOICESERVICE_SHORT - Call groups ... 84
11.6 Ringing strategy ... 85
11.7 Timer ... 85
11.8 Hunt groups ... 86
11.8.1 SIP Softphone (in UCServer) ... 86
11.8.2 PN_PBXVOICESERVICE_SHORT ... 86
11.9 Computer ... 86
11.10 Properties for a computer ... 88

11.11 User rights ... 88
11.12 Profile ... 90
11.13 Global settings ... 91
12 Services ... 94
12.1 Update server ... 94
12.2 E-Mail dispatch ... 94
12.3 Notifications ... 95
12.4 SMS dispatch ... 97
12.5 Call recording ... 97
12.6 Share content ... 98
12.7 External servers ... 99
12.7.1 UCConnect ... 99
12.7.2 Local Web Service ... 99
12.8 STUN and TURN Server Settings ... 101
12.9 Push notifications ... 103
13 Integration in Microsoft® Teams ... 104
14 ChatGPT-Integration ... 105
15 Federation ... 106
15.1 SIP Federation ... 106
15.2 SIP Server ... 107
15.3 Network interfaces ... 108
15.4 SIP Static Routing ... 109
15.5 XMPP Federation ... 111
15.6 Domains authorization ... 113
15.7 Block domain ... 113
15.8 Diagnostics ... 114
16 Databases ... 116
16.1 MetaDirectory ... 116
16.2 Google integration ... 116
17 Server status ... 118
17.1 Status monitor ... 118
17.2 Server events ... 119
18 Tools menu ... 120
18.1 Network interfaces ... 120
18.2 Certificate ... 121
19 Installation of Clients ... 122
19.1.1 Installation at the workplace ... 122
19.1.2 License ... 122
19.1.3 service features ... 122

19.1.4 Connection to the server ... 123
19.2 Installation using group policies ... 123
19.3 MSI description ... 124
19.4 Software distribution ... 124
19.5 Update service ... 126
19.6 Active Directory® Objects ... 126
20 Technical notes ... 127
20.1 Configuration file location ... 127
20.2 Offline journal ... 129
20.3 Contact search ... 129
20.4 Regular expressions ... 130
20.5 Setup a DNS service resource record ... 131
20.6 Setup of DNS Service Resource Records for the federation ... 132
20.7 User rights ... 133
20.8 User Authentication ... 134
21 Global permissions ... 135
21.1 Contact data ... 135
21.2 Presence and lines ... 136
21.3 Configure user account yourself ... 140
21.4 Automatic line binding ... 142
21.5 Server certificate ... 142
21.6 TAPI-driver ... 143
21.7 XSL templates ... 143
21.8 XSLT for e-mail notification ... 143
21.9 Configuration files ... 144
21.10 User database import and export ... 144
21.11 SIP Softphone(s) ... 145
21.12 SIP Response Codes ... 146
21.13 Creating SIP PCAP log files ... 148
21.14 Creating an XMPP Federation ... 149
21.15 Creating a static routing entry between PBX Call Assist 5 UCServer and Microsoft® Lync® Server using TLS/MTLS ... 150
22 Core services ... 152
22.1 Restrictions ... 152
22.2 PN_PBXVOICESERVICE_LONG ... 152
22.3 Initial setup ... 152
22.3.1 Telephone system ... 153
22.3.2 Drop-off number ... 153
22.4 Telephone system ... 153
22.5 Interactive Voice Menu (IVR) ... 154

22.5.1 Basic settings 154
22.6 Add submenu 155
22.7 Timer 155
22.8 Devices 155
22.8.1 uaCSTA settings 156
22.8.2 Enter phone devices 156
22.8.3 Overview - phone devices 157
22.9 Signaling 158
23 Info about PBX Call Assist 5 UCServer 159

1 Willkommen zum PBX Call Assist 5 UCServer

The present help leads you to the installation and configuration of the PBX Call Assist 5 UCServer.

- An overview over the main characteristics is provided by the page PBX Call Assist 5 UCServer.
- An overview over the characteristics of the PBX Call Assist 5 from the user perspective is provided by the page PBX Call Assist 5 client.
- Before you instal, please get information about the typical Application scenarios.
- Information on how to instal the PBX Call Assist 5 UCServer can be found under Installation.
- Information on how to carry out the most important settings in the PBX Call Assist 5 UCServer set up can be found under Setup.
- Help to the configuration dialogs of the PBX Call Assist 5 UCServer can be found under Administration.
- Information about the installation of the PBX Call Assist 5 clients can be found under Installation of clients.
- Information about details and special topics are summarised under Technical notes.
- Links to software updates and support can be found on the page Product support.

Help is available at any time via the PBX Call Assist 5 UCServer program window **Help**. Usually is the help opened on the subject which corresponds to the function used at this moment.

In Help the following icons are used:

Icon	Meaning
	Note
	Warning, caution
	Change from earlier versions

2 PBX Call Assist 5 UCServer

What is Computer telephony integration?

Computer telephony integration (CTI) describes the connection of telephony and data processing. With CTI one is able to establish calls, pick up call and end phone calls out of a computer program. CTI allows the switching of calls and the establishing of conference calls. Typical CTI programs signal to a user all the states of his telephone terminals, regardless of whether it is corded or mobile DECT terminals. Different programs from the corporate and office environment can be connected via interfaces.

What is PBX Call Assist 5 UCServer?

PBX Call Assist 5 UCServer is the server component for PBX Call Assist 5. It's the middleware for your phone system. PBX Call Assist 5 UCServer is an efficient, scaleable 3rd-party CTI implementation which integrates with all VoIP, hybrid or classical phone systems, if these support CSTA or TAPI interfaces.
The PBX Call Assist 5 UCServer also supports the registration of SIP lines in order to make the PBX Call Assist 5 available as a softphone.

PBX Call Assist 5 UCServer monitors and controls the lines of the CTI-capable terminals. It can be used for user administration, manages permissions and offers security through authentication. In PBX Call Assist 5 UCServer central log data and journals are kept and central databases are connected. Different services can be connected via a development kit.

What is the PBX Call Assist 5 client?

PBX Call Assist 5 Client is the software at the user’s workstation. PBX Call Assist 5 enables users to manage their contacts, see the presence of other users, search for contacts and offers many other functions that make their daily work easier. Users can control their telephones and see who is calling.
More can be found out about the client on the page The PBX Call Assist 5 client.

3 The PBX Call Assist 5 Client

The PBX Call Assist 5 client is installed on the users PCs and offers the following important functions and performance features:

Contact search: Find information about the current contact.

PBX Call Assist 5 automatically searches in case of an incoming or outgoing call for the appropriate contact information, based on the phone number (particularly the call partner) and displays this information. Which contact data sources are searched and in which order, can be defined in the configuration of the PBX Call Assist 5 and (by the administrator) in the PBX Call Assist 5 UCServer. If more contacts are found from several data sources for that phone number, the contact data which was last used is displayed as active.

Conversely, the user is able to search in the search window of PBX Call Assist 5 for a person's contact data by entering the name or a part of it and then start the call or other action out of the contact detail window.

ActiveContacts - actively manage contacts

In addition to the contact data the ActiveContacts technology in PBX Call Assist 5 displays further information about the phone status of the user, e.g. from the calendar function of Microsoft Outlook®. The information is constantly updated in "real time". The user always knows, when and how and with which medium his or her contacts are accessible. The communication can be started or managed, depending on the available information, from the context menu.

Presence - to know the availability of contacts

Every user connected to the system has a status, their *Presence*. This information is formed according to defined rules, from the status of several services: Telephony status (telephony service), calendar status (calendar service), login-log off (system service) and the manually entered status, provided by the user.

Therefore, the presence always provides information about the current availability of communication partners.

Federation - The trustworthy network

A federation is a secured structure for the communication between members of different organisations (e.g. two companies, company and customer) with the aim to improve cooperation.

Within the federation, presence management permits the exchange of current information about the accessibility/availability of people, even beyond organisation boundaries. So, a suitable method of communication can be selected (e.g. phone, e-mail, chat, etc.).

Within the frame of the federation, every organisation defines which information is revealed and decides which services and systems are used for the exchange of this information.

Journal - tracking and planning communication

The journal in PBX Call Assist 5 UCServer provides information about all events around your communication, e.g. all phone calls, missed incoming calls and call partners who could not be reached. The information can be filtered and listed according to different criteria.

The journal entries can be processed, marked, annotated and be shared with other users.

Phone calls can be prepared right before or by setting schedules. Call related notices can be done anytime.

Audio/VideoChat - Real-time communication using WebRTC

The PBX Call Assist 5 client enables real-time peer-to-peer Audio/VideoChat and screen sharing communication with other users. This is supported within the internal network (LAN) and between enterprises using federation.

Softphone - Making phone calls with the PC via a PBX

The PBX Call Assist 5 can be registered via the UCServer at a SIP-PBX. The PC in conjunction with a headset turns to be a VoIP phone.

Computer Smartphone Integration via Bluetooth (CSPI)

The PBX Call Assist 5 client supports connecting cell phones with the PC using Bluetooth. This connection will make controlling and monitoring of the telephone possible. Furthermore a PC audio device can be used for conversations by cell phone.

4 Application scenarios

The PBX Call Assist 5 UCServer can be integrated in various ways into an existing IT infrastructure.

On the page Application in a workgroup you can find information about how to setup the PBX Call Assist 5 UCServer if you use a network without domain server in which every user has his/her own computer and his/her own phone.

On the page Application in a Windows® domain you can find information about how to setup the PBX Call Assist 5 UCServer if you have a Windows® network with domain server and Active Directory®.

On the page Application with a terminal server you can find information about how to setup the PBX Call Assist 5 UCServer for a terminal server scenario.

On the page Application with roaming users you can find information about how to setup the PBX Call Assist 5 UCServer if you have users who log on to different PC's.

4.1 Application in a workgroup

To use the PBX Call Assist 5 UCServer in a workgroup without a domain server, first install the PBX Call Assist 5 UCServer as described in Installation. Note the following here:

1. Use the integrated User databank.
2. Define the User registration Select UC password, because there is no central Windows® user administration.
3. Define the Global settings. If you want to involve the users in the configuration, select **Self configuration of the PBX Call Assist 5 UCServer account**. You can give all users mutual global rights. In a small workgroup usually most rights are valid globally for everybody.

4.2 Use in a Windows® domain

To use the PBX Call Assist 5 UCServer in a Windows® domain, first install the server as described in Installation. Note the following here:

1. Use Active Directory® as User databank. Decide before the installation whether you would like to extend the Active Directory® schema or not.
2. Optionally install Active Directory® SnapIn. If you want to extend the schema, you need to run the SnapIn installation.
3. Define the User registration. If all users are registered with the domain, use *Domain authentication*.
4. Define the options Global settings. If you want to involve the users in the configuration, select **Self configuration of PBX Call Assist 5 UCServer account**. In additon, you can give globally to all users mutual rights. It's recommended to give the right **View presence** to all users among each other.
5. After the server installation you can either install the workstations manually (directly on the workstation), via software distribution in the PBX Call Assist 5 UCServer or via an Active Directory® group policy. You can also read Installation via Group Policy.

4.3 Use in a Windows® domain

ProCall NEX can perform the user login against Microsoft® Entra ID. For use in a Windows® domain, the synchronization of the Windows® domain with Microsoft® Entra ID must be set up.

To use user management via Microsoft® Entra ID, you must make the settings in the Microsoft® Azure portal and then transfer the app registration(s) in PBX Call Assist 5 Administration under "User management with Microsoft® Entra ID" so that replication can be carried out correctly.

Information on setting up the Entra ID can be found on our support pages under:
https://support.estos.de/procall-nex/inbetriebnahme-und-einrichtung-von-procall-nex/benutzerverwaltung-mit-microsoft-entra-id-einrichten

1. Select "User management with Microsoft® EntraID" as the user database.
2. Under User login, the system automatically switches to "OAuth2 authentication".
3. Specify the options for the global settings. If you want to involve the users in the configuration, select **Configure PBX Call Assist 5 UCServer account yourself**. You can still assign rights to all users globally. It is recommended that you give the **View presence** permission to all users.

4.4 Application with Terminal Server

To use the PBX Call Assist 5 UCServer with a terminal server or Citrix® Metaframe, first install the server as described in Installation.



In contrast to TapiServer 2.x, with PBX Call Assist 5 UCServer no TAPI drivers are required for PBX Call Assist 5 in Terminal Server environments.
You only have to install the multi-line TAPI driver if other applications use TAPI.

If you have installed a further application which uses TAPI please observe the following instructions:

PBX Call Assist 5 UCServer is installed on the Terminal Server
If the PBX Call Assist 5 UCServer is installed on the terminal server, no remote TAPI driver is used. The lines which are made available to the telephone system by the TAPI driver can be viewed and used by all users. The PBX Call Assist 5 UCServer has the task to allocate lines to the users.

PBX Call Assist 5 UCServer is not installed on the Terminal Server
If the PBX Call Assist 5 UCServer is installed on another server, then the Multiline TAPI driver is installed on the terminal server. In the Computer configuration all lines are assigned to the Multiline TAPI driver which are needed by the terminal server users. These lines are then visible for all users and the right line is always used for the registered user.

Every user uses the terminal server from his permanent workstation
In this case every user can have his own phone assigned to them. Every user is the owner of his phone which stands next to his workstation.

Every user can use the terminal server from any workstation
Users do not have their own number:
In this case users are not assigned their own lines. Phones are assigned to the computers which they are standing next to. If a user logs on to the terminal server from a workstation they are assigned the phone standing next to that workstation.
Every user has his own number:
In this case every user can have his own phone assigned to him. The user can then either take his (cordless) phone with him to his workstation or log on to a phone so that their number is available there.

4.5 Application with Roaming Users

To use the PBX Call Assist 5 UCServer with roaming user, first install the server as described in Installation. Note the following here:

1. Roaming users definitely require a domain. User profiles are stored on the server. Roaming profiles are intended to allow users to log on to any workstation and access their software, their settings and their documents there.
2. To ensure that a user who logs onto a PC is also able to use the corded telephone next to it, the phones must be defined in the configuration Computer. This defines the location of phones.
3. With wireless telephones, the phone needs to be assigned to the user in the configuration of the Users.

5 Installation

You should already be informed about the Application scenarios and their meaning for the installation.

On the following pages you can find out how to install the PBX Call Assist 5 UCServer:

- About the requirements concerning operating system and TAPI driver the page System requirements informs.
- On the page Preparation for the installation you can learn what steps must be performed in which order.
- The Start of installation page provides information about the installation process.

Installation packages

The software is supplied as a zip file containing several Microsoft® Installer (*.msi*) packages.
Please unpack the ZIP file before you run the *.msi* files!

The various packages are containing a lowercase abbreviation for the language and a lowercase abbreviation for the region of the software in the file name. E.g. "en" stands for the language English and "US" stands for the region United States.
Example: *UCServer_en-US.msi* is the English server installation package for the region USA.
Below the abbreviation is given neutrally with *xx-XX*.

File name	Description
UCServer_xx-XX.msi	Installation package for the PBX Call Assist 5 UCServer. Administrator rights are required for installation on the server.
PBX Call Assist 5_xx-XX.msi	Installation package for the PBX Call Assist 5 workstation. Includes a standard TAPI driver.
Help files (PDF)	Documentation in PDF format for the modules listed above. After the installation of the software please use the integrated online help.
readme.txt	Installation guide

5.1 System requirements

For the operating systems supported by PBX Call Assist 5, please visit the website.
(https://support.estos.de/de/procall-enterprise/procall-8-enterprise-systemvoraussetzungen)

The supplied TAPI drivers are also fully available for 64-bit systems and are automatically installed in the respective versions.

5.2 Preparation for installation

With the PBX Call Assist 5 UCServer installation on the network, the drivers and data sources are installed and configured first, then the PBX Call Assist 5 UCServer and finally the workplaces.

Please also consider the notes in Application scenarios.

Run the installation steps in this order please:

1. **Installation of the TAPI driver for your telephone system**
   The TAPI-driver for your phone system must first be installed on the server. This driver makes all phone system extensions available as TAPI lines on the server.

2. **Optional: Install estos MetaDirectory**
   If you wish to use the MetaDirectory to make further databases for contact searching available for the PBX Call Assist 5 UCServer you should install this now.

3. **Installation of the server software**
   To start the installation please run the *UCServer_xx-XX.msi* installer. For more information please refer to Start the installation.

4. **Installation of the workstations**
   You can install the software on the workstations in several ways. An overview can be found on the client install page.

5. **Configuration of the workstations**
   The workstations were either already configured during the manual installation or can be configured any time centrally via the server administration. You can also hand over the responsibility to the users and allow them to enter their settings themselves (view Global settings).

5.3 Active Directory® integration

The Active Directory® can be connected to PBX Call Assist 5 UCServer for user administration. The following options are available:

- **Without schema extension**
  All information which the PBX Call Assist 5 UCServer stores is filed in the field **extensionName**.
- **With schema extension**
  PBX Call Assist 5 UCServer normally uses a schema extension which is, however, best set up in the appropriate schema master *before* the server is installed.

Setup without schema extension
If the PBX Call Assist 5 UCServer is used without schema extension, nothing must be set. Nevertheless, there may conflict with other software that also uses the data field **extensionName** in the Active Directory® to file data.



Parallel operation of version 2.2 and the newer version 3.0 (e.g. migration or to evaluate the new version) is only possible in this case if one of the two servers is running with schema extension!

Setup with schema extension
To use Active Directory® with schema extension the schema must be set up on the domain schema master before first use. A ZIP file that contains all the necessary programs is included in the installation package delivered PBX Call Assist 5 UCServer.

Schema administrator rights for the schema master are required for successful installation.

⚠	A schema extension cannot be revoked once it is installed!
➡	That PBX Call Assist 5 UCServer can use the sheme extension, writing rights are required for following objects: • User • Computer • Groups A detailed list of the fields which are described by these objects is given in the documentation which is included in the ZIP file.
➡	To guarantee the reliable, automatic synchronisation of contact data, the UCServer requires reading access to the list "Deleted Objects" of the connected ActiveDirectory.

Administration via the management console
To support administration in large environments there is a *snap-in* for the console which displays users, computers and groups. This *snap-in* then permits administration of the named elements directly in the Active Directory® environment.

5.4 Start installation

Performing the installation

1. Clicking on the *UCServer_xx-XX.msi* will start the server installation.
2. The version number is displayed on the welcome page. If an older installation already exists, this number is removed. You can select the application of existing settings later during the PBX Call Assist 5 UCServer setup.
3. Read and confirm the license agreement.
4. After a short period, you receive the message "The PBX Call Assist 5 UCServer was successfully installed". Click on **Complete**.
5. If you haven't removed the tick on **Start now PBX Call Assist 5 UCServer server setup**, the PBX Call Assist 5 UCServer setup automatically starts at he point where you can carry out the most important basic settings. The PBX Call Assist 5 UCServer setup can also be found on the Windows® start menu where you can check settings or change them. Help with the PBX Call Assist 5 UCServer setup dialogs can be found under Setup.

➡	The server may not be installed directly from the zip file supplied as otherwise the Windows® installer cannot find *PBX Call Assist 5_xx-XX.msi* which is required for installing or updating the workstations.

Notes for the installation with Microsoft® Installer on a terminal server

The following points should be borne in mind when running a *.msi* file on a Terminal Server:

- Administrators and non-administrators can run Windows® Installer Installations from the command line.
- A terminal server remote session allows only administrators to perform installations.
- Administrators can only perform Windows® Installer installations from a remote session if the EnableAdminTSRemote system policy is activated. This policy is only available from Windows® Installer version 1.1 upwards and Windows® 2000 and later Windows® versions.

- The Windows® Installer is started as a system service and therefore cannot access connected network drives. If you execute *.msi* from a network resource, use UNC paths (\\Server\Verzeichnis\produkt.msi).
- If you get an **Error 2755: Server returned unexpected error 3 attempting to install package** message the cause is usually that you have run the setup from a network drive and have not used UNC paths (the installer service cannot find the *.msi*).

6 Setup

The main server settings are made with the PBX Call Assist 5 UCServer setup.

The setup starts automatically after installation of the server. It can also be started anytime from the Windows® start menu.

Help for each dialog of the setup can be found on the following pages:

- Login
- Presence domain
- Database
- Network interfaces
- Upgrade
- Server reboot
- Licenses
- User database
- User authentication
- Global settings
- Share content
- UCConnect
- Location
- Lines
- Setup finished

6.1 Login

Enter the user name and the password for the PBX Call Assist 5 UCServer administrator here during installation.

You need this user name and password to change the PBX Call Assist 5 UCServer settings. You must enter this login every time the PBX Call Assist 5 UCServer administrator program is started.

You can change the password later in the Tools.

6.2 Server name and server role

If the computer name couldn't be determined automatically, enter in this dialog the name of the computer on which the PBX Call Assist 5 UCServer is installed. The computer name cannot be changed (under certain circumstances) but certainly not if the computer is a member of a domain.

The full name of the server is used to allocate a user to this server. Under this name the server must be accessible from the workstations.

6.3 Presence domain

The PBX Call Assist 5 UCServer needs an unequivocal address for every user for presence and Chat, the so-called "identity". The identity is composed from the username and the presence domain.

A presence domain is distinctly and permanently assigned to a PBX Call Assist 5 UCServer. The PBX Call Assist 5 UCServer is responsible for the transmission of the presence information of all users. This can be done, if required, via Federation also accross the company boundaries.

The same presence domain may never be used on multiple servers. The presence domain must not be changed anymore. Please note that with an alteration to the presence domain all users on the server are no longer accessible to external contacts, because the user's identities change with the presence domain.

The presence domain can be exclusively changed via the server setup, i.e. by a new installation, upgrade or update. Please note that by updating the presence domain all user profiles on the server are customized. Similarly, Setup will try to update all of the favorites and monitor content of workplace software to the changed user identities. After the upgrade, you will be prompted to check the user profiles, especially the user identities.

Ideally, the identity of each user should correspond with their e-mail address. This is important if you want to exchange your presence information and chat messages with external users beyond the boundaries of the enterprise network. The PBX Call Assist 5 UCServer can enable communication with external users via the e-mail address. To ensure that the identity and the e-mail address fit together, you should use the same presence domain for your e-mail addresses.

6.4 Network interfaces

The connection between the software on the workstations and PBX Call Assist 5 UCServer is made via *network interfaces*. The PBX Call Assist 5 UCServer provides several interface types on the server computer for this. Each network interface is bound to a combination of IP address and port number, shown in the field "Bound to IP" and "Port". If network interfaces are used encrypted the configured certificate is listed. The configuration is shown at the fields "Encryption" and "Certificate". A coloured symbol with tooltip help indicates the actual state of the related network interface.

Default settings

The following default settings are used for the network interface types:

Type	Bound to IP	Port	Encryption	Certificate
Administration	All available	7221	unencrypted	
Remote TSP (TAPI)	All available	7220	unencrypted	
UC Client	All available	7222	unencrypted	

By default, ports are bound to all IP interfaces on the computer. If necessary, they can be limited to be used with specific IP addresses only.

Changing the default port configuration is not recommended except the setting conflics with other software running on the system.
If a port conflict accurs an error event appears in the event log of the PBX Call Assist 5 UCServer.

With the button **Standard** settings can be reset to the default values.

The **Add** button allows you to set up a new network connection.

Using the button **Remove** a network interface can be deleted.

The **Properties** button allows you to change a network connection.

6.4.1 Network interface properties

The connection between the application software on the workstations and the PBX Call Assist 5 UCServer takes place across network interfaces.

Type

The following network interface types are available:

- The UC client is the PBX Call Assist 5 software on the workstations.
- The **Remote TSP** offers Tapi Service Providers (TSP) over the network.
- Administration is the application for configuring the PBX Call Assist 5 UCServer.

IP address and port

Each network interface is linked to its own combination of an IP address and port number. The IP address is set by default to "all available". It is however also possible to select one of the determined IP addresses. A summary of the pre-set port numbers can be found in the chapter Network interfaces.

Changing the default port configuration is not recommended except the setting conflics with other software running on the system.
If a port conflict accurs an error event appears in the event log of the PBX Call Assist 5 UCServer.

Encryption

The network interface can be configured in different security levels:

- **Unencrypted:** the PBX Call Assist 5 UCServer is using the network interface unencrypted.
- **Starttls optional:** the PBX Call Assist 5 UCServer is using the network interface encrypted, if available.
- **Starttls mandatory:** the PBX Call Assist 5 UCServer requires using the network interface encrypted.

Default

Check this box if all connections of the actual network interface type are using these interface as standard.

Certificate for TLS connections

If the network interfaces shall be used encrypted a **certificate** is required.

Using the button **Select certificate** a certificate can be configured to be used by the network interface for authentication. If no certificate is offered the network interface can be used unencrypted or a certificate needs to be installed at the system. A short guidance around certificates can be found at the chapter **certificate**.

More information about certificates can also be found at the online help of the *Microsoft® Management Console MMC* Snap-in for certificates "certmgr.msc".

Using the button **Delete certificate** a selected certificate can be removed out of the list.

DNS name for the network interface

Please specify the name how the network interface is resolved at the DNS (e.g. machinename.domain.com). With the initial usage of the software a name is proposed to the user.

6.5 Certificate

To increase security, the data traffic between PBX Call Assist 5 UCServer and PBX Call Assist 5 can be encrypted with TLS/SSL.
For the TLS/SSL encrypting of data a valid certificate has to exist and be selected, which was issued for the FQDN (Full Qualified computer name, e.g. "server.domain.com") of the computer on which PBX Call Assist 5 UCServer runs.

A short tutorial about certificates, how to get them and how to setup them can be found in the chapter Server certificate.
A detailed description can also be found in the online help *Microsoft® Management Console* Snap-Ins for certificates "certmgr.msc" .

Security level for connections with PBX Call Assist 5

- **Allow secure data transmission using TLS**
  If the TLS/SSL encrypting is activated, encrypted and unencrypted programmes in the PBX Call Assist 5 UCServer can be combined.
  PBX Call Assist 5 recognizes this possibility and is able to use it with the next login. Because of this, only clients who have the entire server name in their connection settings (as named in the certificate), e.g. "servername.domain.com" can login.
  Changes to the TLS/SSL settings will be taken over only for new incoming connections. Existing Client connections are not influenced by the new settings.
- **Reject unsecured connections**
  If the TLS/SSL encrypting is activated, insecure connections to the PBX Call Assist 5 UCServer can be rejected.

Certificate for SSL/TLS communication with PBX Call Assist 5
Here the certificate which was selected for the secured data transfer is displayed.

- **Delete certificate**
  Removes the certificate from the configuration. If no certificate is selected, the PBX Call Assist 5 is not able to connect with the UCServer anymore.
- **Choose certificate...**
  Opens up a dialog to display the certificates available on the computer and to select one of them for the data transfer.

6.6 Upgrade

In this dialog box, during the upgrade you can select whether existing chats are to be transferred or whether the data transfer is not to take place.

PBX Call Assist 5 UCServer uses a newer chat database schema than the previous version. Continued use of existing chats is only possible if they are converted to the new database schema.

Depending on the size of the database or system, the conversion can take several minutes and must

	not be canceled.
⚠	A subsequent conversion of the database is not possible.

6.7 Server reboot

The PBX Call Assist 5 UCServer has to be started to continue the setup. If the server setup is carried out when the system is in operation, a new start is necessary. Click on **Next**.

6.8 Licenses

PBX Call Assist 5 UCServer requires licence keys to operate. Basic properties of PBX Call Assist 5 UCServer are defined by the licence key.

Select license model
At this point there are the following possibilities:

Test 25 licenses free of charge (for 45 days)	Use the evaluation license. The PBX Call Assist 5 UCServer can be tested for 45 days with all available functions for 25 PC's. At the end of the test period the licences have to be purchased and entered.
Add license	To enter a new license please use the button **"Add"**.

➡	For the installation and operation of the PBX Call Assist 5 UCServer a connection to the Internet is required.

The PBX Call Assist 5 UCServer licenses are regularly checked online for a valid Software Assurance (SWA) contract. For extensions of the system additional licenses can be registered.

Licenses for the Mobility Services must be entered in the UCConnect and are displayed in the Online Licenses menu.

List of licenses used
This list shows the licenses entered and its properties.

Field	Description
Description	Description of licenses or its features
Amount	Amount of active licenses or its features
Used	Amount of actually used licenses or its featues
Valid until	Displays the license validity period
License	License key (35 digits)

PBX Call Assist 5 workstations	Number of users that can be used
Clients and devices (server connections)	Amount of server connections enabled to be active simultaneously
Lines	Number of lines and phones which can be used

Sum active licenses shows the summary of current valid licenses.

Add
This allows new licenses to be added to the list.
Any number of licenses can be entered.

Remove
Remove the marked license from the list

Hardware-ID
A hardware ID which is used to create a license bound to the hardware.

6.9 Database

PBX Call Assist 5 UCServer's various services such as telephony, calendar, scheduled calls and chat use a database. SQLite or Microsoft SQL Server® (from version 2000) can be used as database.
The use of existing Microsoft Access® databases is no longer supported.

For the conversion of the server database from SQlite to Microsoft SQL Server®, the general notes on SQL databases apply.
A data transfer does not take place during the conversion. The data of the previously used database remains completely intact.

For more information on converting Microsoft Access® databases or SQlite to Microsoft SQL Server®, see Server Database.

6.10 User database

Either user administration integrated into the PBX Call Assist 5 UCServer or an Active Directory® server can be used to administrate computers, users and groups.

PBX Call Assist 5 UCServer user management (file-based)
The PBX Call Assist 5 UCServer uses its own user administration, data is saved under Configuration files.

External user management using Active Directory® server
The users, computers and groups from the Active Directory® are used. All settings are stored directly in Active Directory®. The information is stored in Active Directory® either as per the standard with a schema extension or in a reserved field.
The users, computers and groups can be configured in the PBX Call Assist 5 UCServer administration.
Optionally the Active Directory® SnapIn can be installed. A maximum of 1,000 entries are displayed in the PBX Call Assist 5 UCServer administration under user, computer and groups. If you have more than 1,000 users,

you *have to* carry out the configuration with the Active Directory® Snap-In.

Active Directory® server

Enter the computer name of the server here if you want to establish a connection to a specific Active Directory® server.

You can also leave the field empty or enter a domain name. If the field is left blank, the domain name of the computer on which the PBX Call Assist 5 UCServer is running is used.

Automatic reconnection is activated by entering a domain name or leaving it blank. This means that if the connected Active Directory® server fails during use, an automatic attempt is made to reconnect to another Active Directory® server within the specified domain.

User name

Specify the user name that has write permission to the users, groups and computers (optional) of the Active Directory®. For example, this can be the Administrator Account. Specify the user name in the form *Administrator@mydomain.com*.

Password

Enter the user's password here.

Force LDAPS

When this option is activated, an encoded network connection to the Active Directory® Server is forced (LDAPS). The connection will be established on Port 636 (or on the port specified in the computer name). The connection will only be established if LDAPS can also actually be activated.

PBX Call Assist 5 UCServer user management (SQL-supported, for special requirements only)

PBX Call Assist 5 UCServer uses its own SQL database for managing users, groups and computers. This setting is only visible for installations which wish to use user data from an external, write-protected data source.

6.11 User authentication

The computer login always uses the computer's name. The user login to the server can be done in several ways. Select carefully the method which is possible and sensible for your infrastructure.

Examples of useful application in different types of scenarios:

Description	Method
Workgroup without a server; each user is logged in as an administrator.	Integrated user administration, authentification with UC password. You must assign every workstation a unique login for the PBX Call Assist 5 UCServer so that users can be uniquely identified.
Workgroup, every user is logged in with his unique user name.	Integrated user administration with UC password. The user names are unique; no individual user names need to be set up. Every user receives his own password on the PBX Call Assist 5 UCServer.
Windows® Domain (also with Active Directory® Server)	Integrated user administration or Active Directory®, Windows® domain authentification. Users must also explicitly log in to the PBX Call Assist 5 UCServer with their domain login.
Windows® domain (all users are logged on to the domain)	Integrated user administration or Active Directory®, Windows® domain authentification. Users are automatically authentificated via their domain login at the PBX Call Assist 5 UCServer.

Authentication with UC password
Each user uses an individual UC password to log into the PBX Call Assist 5 UCServer. This UC password has nothing to do with the Windows® password and is configured in the user administration.

Windows® domain authentification
The Windows® user name and password are always used for authenticating CTI users. If the user is already logged into the domain on his workstation the user is authenticated directly with his Windows® login. If the user is not logged in to a domain he can still log in to the PBX Call Assist 5 UCServer with his Windows® login credentials.
This is the greatest possible security to prevent unauthorized users from using a phone for which they have no authorization. Caution: use this setting only if all computers and users are members of a domain.
Use this setting only if all computers and users are members of a domain.

More information about the technical background of the authentication methods can be obtained on page Authentication of users.

OAuth2 authentication
The login is used when the users are replicated from the Microsoft® Entra ID. The login data for Microsoft® Entra ID is always used for user authentication.

6.12 Global settings

Rights which apply globally on the server for all users can be configured here. If a right is configured here all users have this right regardless of the group or user configuration.

⚠	Changes of user rights are usually activated immediately for the entire system. Large installations possibly need longer because of changes made to user rights!
⚠	Globally assigned permissions cannot be revoked on the user object. The permissions can be extended on the user and group object.

Give users global permissions among themselves:
Global permissions can be defined here that all users have mutually. If a permission is granted here, this permission applies independently of the group or user configuration. The meaning of the permissions in detail can be found under Global permissions.

In the table, you can specify which software and features users are allowed to use. The users can use more functions than specified here through individual assignment on the user object or through membership in a group.

Field	Value
General features	
Configure user profile personally	If this option is set, all users are allowed to change their Personal settings in the user management itself.
Allow AudioChat	If this option is activated, the user is allowed to make AudioChats with other users.

Allow AudioChat and VideoChat	If this option is activated, the user is allowed to make AudioChats and VideoChats with other users.
Enable screen sharing rights via federation	If this option is set the screen sharing rights specified by the administator can also be used via SIP federation. Users across enterprises (different domains) may share their screen with other users. Users within the same enterprise (same domain) may also invite other users to share screens.
Accept screen sharing requests	If this option has been enabled, the user may only use the screen sharing features when other users have invited them to do so.
Initiate desktop sharing	If this option has been enabled, the user may independently share their screen with other users as well as invite other users to share their screens.
Enable access to the whole journal for all users	All users can be given access to the phone journals of all users here. This, however, only makes sense with installations which have a small number of users.
Users are allowed to delete journal entries	The journal entries can be subsequently changed by the user to a limited extent. For example, the user can subsequently change the note on the call or the call partner. If this option is activated, the user can delete journal entries.
All users have all users in the monitor	If this option is activated, a special group is set up for every system user in the client monitor in which the user can see all other UC software users. This option only makes sense for installations with a small number of users. For a large number of users (more than 20) such an administrative parameter can be set via the groups.
Assignment of rights to monitor groups	Permissions can be set for the monitor groups specified in the group objects. The permissions set here are valid for all administratively specified monitor groups. If users are added to the monitor via monitor groups or the above setting "All users have all users in the monitor", they have global permissions among themselves. If there are no assignments in the groups, you can additionally assign a minimum of rights here. This is useful, for example, not to send permission requests to the users.
Automatically provide phone numbers as lines which are configured in the user account.	Phone numbers, configured in the user account are automatically used by the server for the line binding. If the server finds a line for a user's phone numbers, then this line is automatically assigned to the user. If this automatism cannot be used in the existing environment, it can be deactivated via this option. View Automatic line binding.
Use apps	If this option is enabled, the user is allowed to use the mobile apps. The setting can be changed only if this right has not already been assigned in the global permissions.
Workstation	If this option is activated, users with selected PBX Call Assist 5 can log on to this

Client Login via the Internet	server via a public network without having to establish a VPN connection to the network. You need a UCConnect account and additional licences if necessary.
Share content	
Files	If this option is activated, users can transfer files in the chat. The service must be set up under Services – Share Content.
Other external services	
Integration in Microsoft® Teams	If this option is activated, the presence status will be synchronized between Microsoft® Teams and the PBX Call Assist 5 client. The prerequisite is to set up the Integration in Microsoft® Teams.
Profile page visible to anonymous users	If this option is enabled, the user contact data are visible via the business card of the Web service.

6.13 Location

The location settings are used to enable the right dailing and display of phone numbers.

Only with the right location settings it is possible that external phone numbers are dialed and displayed properly.

This section of the help file will describe the individual configuration parameters on the Location Settings dialog. If a location is depicted, the following pages will provide all information necessary for configuration. If several networked locations must be setup, all information for special configuration scenarios can be found in the Location Designs section.

Country/region:
Choose your country from this list.

Area code
Enter your local area dialing code here. This is for example 030 for Berlin or 44 for Zurich (Switzerland). The leading 0 is not necessary and is removed by the system when the settings are saved.

Display Advanced Settings
The location settings have many options that will only be needed in special cases. Settings that are not mandatory for normal operation will not be displayed by the wizard.

The advanced settings include:

- Rules for the detection of internal and external phone numbers
- Rules for formatting the line phone numbers
- Special formatting of phone numbers that will be registered by the telephone system
- Special formatting of phone numbers that will be transferred to the telephone system for dialing
- Least cost routing
- Vanity phone numbers

6.13.1 TAPI lines

Here you can select which extensions will be made available in the network.

A line usually corresponds to a phone. All lines are displayed in the list which are available on the computer. provided by TAPI drivers. If you add a new driver under Control Panel - add Phone and Modem Options and the lines are added here accordingly. With some TAPI-drivers it is necessary to reboot PBX Call Assist 5 UCServer.

Add a line (PBX)
PBX Call Assist 5 UCServer supports central connection to telephone system through the system manufacturer's CTI TAPI driver, through the supplied ECSTA connection or through SIP softphones. The TAPI driver and ECSTA connectors allow monitoring and remotely controlling telephones that will be operated with the system. The SIP Softphone Configuration will allow PBX Call Assist 5 Client users to use their PCs as softphones in order to make calls through the telephone system.

Line properties
You can change some line properties directly in the list. A dialog can be opened via *properties* after selecting and marking a line. A line has the following properties:

- **Use lines**
  The line is opened by the PBX Call Assist 5 UCServer. Then the line can be used and users can be added.
- **Trunk line**
  This line is treated specifically in PBX Call Assist 5 UCServer if it is an outside line.
- **Activate journal**
  All calls on this line are written to the database.
- **Private telephone**
  In the journal all of this phone's entries are automatically marked as "Private" and are treated according to the rules of the Telephone journal. Other users are not able to see connected numbers or contacts on this phone.
- **Line addresses**
  If the TAPI line has several addresses, you can define here whether incoming calls are notified to all addresses or only to one special address.
- **Internal phone number**
  This is the phone number with which the phone can be contacted internally. The number is normally determined automatically (either from the address or from the line name). A phone number may only occur once. This phone number is the unique key with which the phones are assigned to users and computers**. If you have dual phone numbers such as, for example, with parallel connection of terminal devices, you should use small letters to differentiate the phone numbers.** If you have two lines with the phone number 111, you should give one line the number 111 and the other the number 111b.
- **Location**
  Defines the Location of the line, if the location wasn't configured via the line group. The location defines, for example, the number formats and the dialing rules.
- **Call redirection**
  PBX Call Assist 5 UCServer supports server-side call redirection. Various call targets can be added to the list of redirections. How long a call remains at the relevant extension if it is not answered must be additionally configured. The list of the first line which rings applies. Configured call redirections on lines which are gone through as part of a call forwarding scenario do not apply. All targets in the list must be activated by the server in the line manager. If a target is not monitored, the forwarding is stopped at this number.

Line group properties
Lines are combined into groups. The properties of a group apply to all lines in the group. To display the

properties of a group, select the group and press *Properties*. The settings for the Line Group Properties for SIP Softphone and Line Group Properties for TAPI Driver differ in a few respects and therefore have separate help pages.

Line status
The line status, whether available or not, is displayed in the form of a colored icon. If a ECSTA driver is used, the tooltip schows detailed information on the status icon in case of en error (communication error, login error, license error etc.).

Icon	Statement
	This line could be opened.
	This line could not be opened. Check the functionality of the TAPI driver.
	This line is not in use. The terminal device has been physically disconnected and is therefore not connected to the TK system. This line cannot be used.
	Line has not yet been initialised.

6.14 Remote Office

Remote Office allows you to initiate calls from outside of the company using your business phone. The call will be identified using the business phone number, regardless of where you are. Remote Office will be activated from the PBX Call Assist 5 client through the line menu in the custom area. Also check the setting in UCServer in the line properties. When activating this feature, enter the number where you will actually be available, the so-called Remote Office Number (such as your cell phone number). Call forwarding will be setup from your business phone to the remote office number. If you place a call, such as through PBX Call Assist 5 Mobile, the telephone system will call the specified remote office number. As soon as this connection has been made, the target person will be called.
If the telephone system in use does not natively support the Remote Office feature, an attempt will be made to emulate it. To accomplish this, your business phone will briefly call the specified remote office number in hands-free mode. As soon as the connection has been made, the call will be transferred to the target person. Depending on the telephone system this will be implemented by means of a blind transfer or a callback, which will be immediately transferred.

So that you can use this feature, the telephone system in use must meet the following requirements:

- Native implementation of remote office (e.g. ECSTA for Broadsoft)
- Alternatively
    - Set to forward, delete and request calls through the PBX (lineForward)
    - Support for dialing in speaker phone mode and optionally:
        - Starting a conversation and transfer it in the ringing state (lineSetupTransfer with subsequent lineCompleteTransfer(LINETRANSFERMODE_TRANSFER), or
        - Transfer an existing conversation blindly (lineBlindTransfer)

If one of the indicated requirements has not been fulfilled, the telephone system will not be able to depict Remote Office.

6.15 Setup finished

Click on **Finish** to confirm the server setup. Then the PBX Call Assist 5 UCServer Administration is started and the configuration can be checked or changed.

7 Administration

The server settings are done with the program *PBX Call Assist 5 UCServer administrator*.
The program can be started on the server but also on any other computer. The program connects then via TCP/IP to the server. Please note that connecting remotely to the server may limit some minor functionality. Further, the *PBX Call Assist 5 UCServer administrator program* is not updated automatically if it runs on remote machines.

At the start of the program please select the Server connection.

Help for single dialogs of the configuration can be found in sections:

- General
- Voice Services
- Telephony
- User management
- Services
- Federation
- Databases

Help for server status and server protocols can be found in sections:

- Server status
- Server events

Help for the menu **Tools** of the administration can be found in sections:

- Tools menu

8 Server administration

When the PBX Call Assist 5 UCServer administrator starts, you are able to select which server you wish to administer:

- **Protocol only (server logs only)**
  Using this option no connection to the server will be established. You may only view the event log and the connection log.
- **Local server**
  This option connects to the server installed locally on this computer. You can also view the event log and the connection log.
- **Remote server**
  This option connects to the server which is not installed locally on this computer. You cannot view the event log and the connection log.
  The computer name or the IP address of the remote computer needs to be entered at the field "Server". A computer of the local network can be selected from a list by using the button "search". The corresponding port number of the remote server needs to be entered in the related field (default 7221). The connection may be used encrypted if the option "force TLS encrypted connection" is checked. In this case the remote server needs to be configured accordingly.

Login
To be able to administer the server, you need to login at the server. The login of the administrator was defined during the installation. It can be changed with Menu tools.

9 General

On the following pages the general settings are explained:

- Presence domain
- User database
- User authentication
- Database
- Events
- Online licenses

9.1 Licenses

PBX Call Assist 5 UCServer requires licence keys to operate. Basic properties of PBX Call Assist 5 UCServer are defined by the licence key.

Select license model
At this point there are the following possibilities:

Test 25 licenses free of charge (for 45 days)	Use the evaluation license. The PBX Call Assist 5 UCServer can be tested for 45 days with all available functions for 25 PC's. At the end of the test period the licences have to be purchased and entered.
Add license	To enter a new license please use the button **"Add"**.

For the installation and operation of the PBX Call Assist 5 UCServer a connection to the Internet is required.

The PBX Call Assist 5 UCServer licenses are regularly checked online for a valid Software Assurance (SWA) contract. For extensions of the system additional licenses can be registered.

Licenses for the Mobility Services must be entered in the UCConnect and are displayed in the Online Licenses menu.

List of licenses used
This list shows the licenses entered and its properties.

Field	Description
Description	Description of licenses or its features
Amount	Amount of active licenses or its features
Used	Amount of actually used licenses or its featues
Valid until	Displays the license validity period

License	License key (35 digits)
PBX Call Assist 5 workstations	Number of users that can be used
Clients and devices (server connections)	Amount of server connections enabled to be active simultaneously
Lines	Number of lines and phones which can be used

Sum active licenses shows the summary of current valid licenses.

Add
This allows new licenses to be added to the list.
Any number of licenses can be entered.

Remove
Remove the marked license from the list

Hardware-ID
A hardware ID which is used to create a license bound to the hardware.

9.2 User database

Either user administration integrated into the PBX Call Assist 5 UCServer or an Active Directory® server can be used to administrate computers, users and groups.

PBX Call Assist 5 UCServer user management (file-based)
The PBX Call Assist 5 UCServer uses its own user administration, data is saved under Configuration files.

External user management using Active Directory® server
The users, computers and groups from the Active Directory® are used. All settings are stored directly in Active Directory®. The information is stored in Active Directory® either as per the standard with a schema extension or in a reserved field.
The users, computers and groups can be configured in the PBX Call Assist 5 UCServer administration. *Optionally* the Active Directory® SnapIn can be installed. A maximum of 1,000 entries are displayed in the PBX Call Assist 5 UCServer administration under user, computer and groups. If you have more than 1,000 users, you *have to* carry out the configuration with the Active Directory® Snap-In.
Active Directory® server
Enter the computer name of the server here if you want to establish a connection to a specific Active Directory® server.
You can also leave the field empty or enter a domain name. If the field is left blank, the domain name of the computer on which the PBX Call Assist 5 UCServer is running is used.
Automatic reconnection is activated by entering a domain name or leaving it blank. This means that if the connected Active Directory® server fails during use, an automatic attempt is made to reconnect to another Active Directory® server within the specified domain.
User name
Specify the user name that has write permission to the users, groups and computers (optional) of the Active Directory®. For example, this can be the Administrator Account. Specify the user name in the form *Administrator@mydomain.com*.
Password
Enter the user's password here.

Force LDAPS
When this option is activated, an encoded network connection to the Active Directory® Server is forced (LDAPS). The connection will be established on Port 636 (or on the port specified in the computer name). The connection will only be established if LDAPS can also actually be activated.

PBX Call Assist 5 UCServer user management (SQL-supported, for special requirements only)
PBX Call Assist 5 UCServer uses its own SQL database for managing users, groups and computers. This setting is only visible for installations which wish to use user data from an external, write-protected data source.

9.3 Security

The PBX Call Assist 5 UCServer can monitor login attempts and block them if they are invalid.
The following are monitored:

- the local interface for registrations via PBX Call Assist 5 for Windows® and the Remote TAPI driver
- the web interface through which the mobile apps and PBX Call Assist 5 Web log in.

After a certain number of failed login attempts, users are deactivated or locked out in UCServer. This prevents, for example, accounts in Active Directory® from being locked due to failed login attempts.

Temporarily block a user
Specify the number of failed logins and the time window. Once this limit is reached, the account will be temporarily locked for the specified period.
The user receives a corresponding message on the PBX Call Assist 5 client.

Deactivate user
If the specified thresholds are reached, the user object is deactivated and must be reactivated by the administrator.

It is important to note that login attempts do not "accumulate." If a user is temporarily blocked, no further login attempts will be accepted, counted, or forwarded to the connected Active Directory® for the specified duration.
Once the registration has been approved, the count starts over at 0

The following applies to both fields: If a "0" is entered or the field contents are cleared, the monitoring function is disabled.

9.3.1 Advanced Active Directory® settings

BaseDNs
Here you may enter the basis which shall be searched for users, computers and groups. If nothing is entered here the BaseDN is set automatically.
Several BaseDNs may be indicated in each entry line. These are simply separated by ';' between each entry.



By indicating several BaseDNs for users, computers and groups, it is possible to filter objects of a domain (or a domain forest) for use in PBX Call Assist 5 UCServer.

With hte button "Filter..." you can also modify the **LDAP filters** that the PBX Call Assist 5 UCServer uses to read users, groups and computers. Please note: that the LDAP filter only affects the user manager, but not the number resolution of the PBX Call Assist 5 UCServer.

LDAP attribute allocation
Here you can view the LDAP attribute allocation. You are able to configure the phone number fields used for the Automatic line binding.
Some attributes can be deactivated server-side so that they'll no longer be visible (e.g. a user's private phone number).

LDAP phone number attributes
Of particular importance are the phone number attributes from the Active Directory® in connection with the PBX Call Assist 5 UCServer. Only if you permit writing access for the phone number attributes are you able to configure the phone numbers of the user in the PBX Call Assist 5 UCServer administration. These phone numbers are then written in the Active Directory® in the same way as they were entered in the administration. This is why you can preformat the phone numbers if you assign a line to a user. The phone number is then preformatted accordingly and transfered to the user account, if you have selected a line of the user. During reading the phone numbers from the Active Directory®, the phone numbers are converted again into full canonical format.

If the TAPI driver supplies phone numbers with a postfix, they will be attached unmodified to the pre-formatted phone number. These postfixes are absolutely necessary for the assignment of the line based on the phone number. If corresponding postfixes disrupt the Phone Number entries in Active Directory®, the postfixes will have to be either deleted manually from Line Phone Numbers or alternatively added to the user profile through additional lines.

9.4 User authentication

The computer login always uses the computer's name. The user login to the server can be done in several ways. Select carefully the method which is possible and sensible for your infrastructure.

Examples of useful application in different types of scenarios:

Description	Method
Workgroup without a server; each user is logged in as an administrator.	Integrated user administration, authentification with UC password. You must assign every workstation a unique login for the PBX Call Assist 5 UCServer so that users can be uniquely identified.
Workgroup, every user is logged in with his unique user name.	Integrated user administration with UC password. The user names are unique; no individual user names need to be set up. Every user receives his own password on the PBX Call Assist 5 UCServer.
Windows® Domain (also with Active Directory® Server)	Integrated user administration or Active Directory®, Windows® domain authentification. Users must also explicitly log in to the PBX Call Assist 5 UCServer with their domain login.
Windows® domain (all users are logged on to the domain)	Integrated user administration or Active Directory®, Windows® domain authentification. Users are automatically authentificated via their domain login at the PBX Call Assist 5 UCServer.

Authentication with UC password
Each user uses an individual UC password to log into the PBX Call Assist 5 UCServer. This UC password has nothing to do with the Windows® password and is configured in the user administration.

Windows® domain authentification
The Windows® user name and password are always used for authenticating CTI users. If the user is already logged into the domain on his workstation the user is authenticated directly with his Windows® login. If the user is not logged in to a domain he can still log in to the PBX Call Assist 5 UCServer with his Windows® login credentials.
This is the greatest possible security to prevent unauthorized users from using a phone for which they have no authorization. Caution: use this setting only if all computers and users are members of a domain.
Use this setting only if all computers and users are members of a domain.

More information about the technical background of the authentication methods can be obtained on page Authentication of users.

OAuth2 authentication
The login is used when the users are replicated from the Microsoft® Entra ID. The login data for Microsoft® Entra ID is always used for user authentication.

9.5 Database

PBX Call Assist 5 UCServer's various services such as telephony, calendar, scheduled calls and chat use a database. SQLite or Microsoft SQL Server® (from version 2000) can be used as database. Microsoft Access® databases are no longer supported.

General rules on SQL databases apply for converting server databases (especially from SQlite or Microsoft Access® to Microsoft SQL® Server).
A data transfer does not take place during the conversion. The data of the previously used database remains completely intact.

SQLite

SQLite databases are files created on the PBX Call Assist 5 UCServer computer.

- **Directory**
  The absolute path to the directory where the database has been stored. If this path will be changed and existing data should not be lost, the existing database must first be copied into the new directory. The path is an absolute path to the computer running the PBX Call Assist 5 UCServer service. If a connection should be made to a PBX Call Assist 5 UCServer remote computer using PBX Call Assist 5 UCServer Administration, access to the other computer's file system will not be available. In that case, the indicated path is a local path to the computer targeted by the connection.

Microsoft SQL Server®

The following configuration is required for operating SQL Server®:

- **Server name**
  Enter the name or the IP-address of the server here. If a named instance, such as an SQL Server® Express installation, should be used, the name of the instance must also be specified. Such names

will follow the pattern: HOSTNAME\INSTANCENAME.
For example: hostname\SQLExpress

- **Authentication**
  PBX Call Assist 5 UCServer supports the following options for authentication.
  - **Windows® Authentication using a Service Account**
    PBX Call Assist 5 UCServer will implicitly log onto the SQL Server® using the Windows® user account that started the PBX Call Assist 5 UCServer service. There will be no need to specify the user name and password in this case. For this authentication method, make sure that the service account running the PBX Call Assist 5 UCServer instance will have access to the necessary access rights on the SQL server. By default, the local system account will be used for logging the PBX Call Assist 5 UCServer installation on as a service account, which usually already has full access to a local instance of SQL Server® Express. PBX Call Assist 5 UCServer and the SQL Server® must run on the same machine when using the local system account. The PBX Call Assist 5 UCServer service must be converted from using the local system account to using a Windows® account with network permissions for using Windows® Authentication using a Service Account and an SQL Server® that will be accessed through the network. The service account can be converted by opening the service from the Control Panel and the Administrative Tools and setting the desired Windows® user account from the properties for the PBX Call Assist 5 UCServer entry.
  - **Windows® Authentication**
    If Windows® authentication has been selected, a Windows® user account with password must be explicitly specified, which the PBX Call Assist 5 UCServer service will use for logging onto SQL Server®. For this authentication method, make sure that the specified Windows® user account has the necessary access rights for the SQL Server®.
  - **SQL Server® authentication**
    If SQL Server® authentication has been selected, the user account setup in SQL Server® will be used to log onto the database. SQL Server® must have activated the setting for the so-called Mixed Mode for this. For this authentication method, make sure that the specified SQL Server® user account has the necessary access rights for the SQL Server®.
- **User name** and **Password**
  Enter the login information that PBX Call Assist 5 UCServer should use for logging onto SQL Server®. The user name and password cannot be entered for all types of authentication. For Windows® authentication enter the fully qualified user name as the user name, meaning for example "user@domain". Alternatively, the Windows® login notation ("domain\user") can also be used.
- **Database name**
  Enter here the database name where PBX Call Assist 5 UCServer should store its data. PBX Call Assist 5 UCServer will manage the necessary tables itself. The already existing databases will be provided for selection once the connection with the SQL Server® has been successfully setup. Setting up a dedicated database for PBX Call Assist 5 UCServer is recommended. If a database not in the list is specified, it will be created if the specified user has the required access rights.

Other notes regarding the SQL Server® or SQL Server® Express connection

Context	Solution
UCServer will start during system startup before the database service.	If SQL Server® has been installed on the same computer as UCServer, the database service must be started first. This can be controlled through the service dependences. To accomplish this, the SC.exe service control program can be run from the command line. For example, using the command: sc config eucsrv depend= MSSQL$SQLEXPRESS/TapiSrv/LmHosts set that the service "eucsrv" depends on the database service "MSSQL$SQLEXPRESS", the TAPI subsystem "TapiSrv" and the network layer and is started accordingly only if these are running.

	The *sc /?* command will provide additional help about sc.exe. Note: a space should be entered after the equals sign in the parameter "depend=".
Authentification and access rights	Apart from read and write access the PBX Call Assist 5 UCServer needs the following rights for accessing the database: • Create database When the server starts the configuration for the first time it attempts to create the database if it does not yet exist. If the database already exists the right is not used. • Create table When the server starts the configuration for the first time the required tables are created in the specified database if they do not yet exist. If the tables already exist the right is not used. • Change tables It is possible (although seldom) that the introduction of new features or improvements will make it necessary to change (add to) tables. At start-up the server analyzes the table structure and automatically makes extensions and changes. If such a procedure is necessary, the instructions will be noted in the release notes and the necessary changes will be described there. These rights are not required if the corresponding works or changes are done by hand.

9.6 Events

The PBX Call Assist 5 UCServer writes an event protocol in the installation list under *Logs*. Here you can define which kind of events should be protocolled. For usual operations **Protocol mistakes and warnings** should be set.

Directory
Here you can select the directory into which the logfiles are saved.

Maximum size of a log file
The maximal size (in MB) of log files can be specified here. Once the limit is reached a new log file is created additionally.

Keep old logs
PBX Call Assist 5 UCServer produces a new log file every day and deletes the old logs. If this option is activated, the old logs are no longer deleted and thus remain in the above directory.

Send errors as e-mail to administrator
If this option is activated, errors are sent by e-mail to the administrator. It has to be configured under E-Mail dispatch and an e-mail address for the administrator has to be provided.

Delete log files
By pressing this button the logfiles in this directory are deleted.

Collect log files
By pressing this button the created log files are packed into a ZIP archive. A window is opened prompting for

the target directory. These ZIP archives are often used by the technical support for understandig better customer's issues.

Windows® event log
Here you can define whether the errors and warnings should be additionally written to the Windows® event log. It is possible to select whether just errors or also warnings are included in the event log.

Media Server Events

To better support an analysis in case of problems with softphone and audio/video, additional recordings can optionally be created here.

Please note that enabling these logs can significantly increase the system load. Logging should only be enabled at the request of support.

9.7 Online licenses

estos UCConnect is an independent platform for the cloud. It offers various online services for companies that rely on the hybrid cloud concept and thus want to operate software components from the cloud in addition to their own hardware. Companies that do not want to carry out this installation themselves or do not have the necessary expertise usually benefit most from the offers provided by UCConnect since UCConnect dispenses with the need to configure the web service and the set up of STUN and TURN servers separately.

The setup and connection to estos UCConnect allows you to use the online services and UCConnect hybrid cloud modules. Online service in this case means that the corresponding clients are not in the local network, but connect to the UCServer via the Internet, e.g. from the home office. Mobile use of these applications therefore requires access to estos UCConnect from the Internet as well as the STUN server and the TURN server for using audio and video chat features.

The required port and firewall rules depend on the UCConnect services used. The following list shows what must generally be set up in the routers/firewalls. The routers/firewalls must be set up in such a way that a connection once established remains open and all additionally required/requested ports can be used.

Query license

Source	UCServer
Destination	*.ucconnect.de
Port	443, TCP

Push-Service

Source	UCServer
Destination	ucpush.ucconnect.de
Port	443, TCP

PBX Call Assist 5 Mobile Service

Source	UCServer and all PBX Call Assist 5 Clients
Source port	all
Destination	*.ucconnect.de
Port	3478 und 443, UDP and TCP

Existing licenses for the estos UCConnect services must be entered in the server account in UCConnect. Test licenses for the available online services can be requested for each server account in the UCConnect. The licenses entered in the UCConnect and their scope are displayed here.
You can get the licenses for all UCConnect services from your usual sources or our Online Shop.

Use estos UCConnect

The UCServer must be connected to a server account in the UCConnect. Click on "Log in to UCConnect" and enter the Server ID with the corresponding password.
If you have not yet created a server account in UCConnect, go to the web pages of the estos UCConnect portal.

For information on creating and setting up accounts in UCConnect, see the Support pages:
https://support.estos.de/de/ucconnect

Under **Connection**" is shown if the UCServer is connected with UCConnect and which services are available.

In the table **Licenses** the licenses stored in the UCConnect are displayed. With additional licenses you can use different online services.

Under the table **Licenses** you can activate, set up and invite users for using PBX Call Assist 5 Mobile using wizard.

- **Configure and invite users to use the mobile apps**

If users are to use Mobility Services, they can be selected, set up and informed here.

- **1st step**
  Start the wizard by clicking the "Invite users to use mobile apps" button.
- **2nd step**
  Select the users who should be invited to use the app and click "Send emails".
- **3rd step**
  The users retrieve the email on their smartphones and download the app from the respective store, the link to the store is included in the email.
- **4th step**
  The mail contains another link with all user-specific login information. The user only needs to retrieve this from the smartphone with the app installed and log in with his password only. The password corresponds to that of the UCServer user.

10 Telephony

The telephony setup is explained on the following pages:

- Lines
  - Tapi lines
  - SIP softphone lines
- Location
- Phone journal
- Unanswered calls
- Error handling

10.1 Lines

Here you can select which extensions will be made available in the network.

A line usually corresponds to a telephone or a PBX Call Assist 5 as a softphone. The list displays all lines that are available on the computer. The lines are made available by SIP Line Registrations or as TAPI lines.

The TAPI drivers should already be installed on the system. If you add a new driver under Control Panel - add Phone and Modem Options and the lines are added here accordingly. With some TAPI-drivers it is necessary to reboot PBX Call Assist 5 UCServer.

The configuration of the lines and line groups depends on the type of line.

- TAPI lines
- SIP Lines

The configuration of the lines and line groups depends on the type of line.

- ECSTA Lines
- SIP lines

10.1.1 TAPI lines

Here you can select which extensions will be made available in the network.

A line usually corresponds to a phone. All lines are displayed in the list which are available on the computer. provided by TAPI drivers. If you add a new driver under Control Panel - add Phone and Modem Options and the lines are added here accordingly. With some TAPI-drivers it is necessary to reboot PBX Call Assist 5 UCServer.

Add a line (PBX)
PBX Call Assist 5 UCServer supports central connection to telephone system through the system manufacturer's CTI TAPI driver, through the supplied ECSTA connection or through SIP softphones. The TAPI driver and ECSTA connectors allow monitoring and remotely controlling telephones that will be operated with the system. The SIP Softphone Configuration will allow PBX Call Assist 5 Client users to use their PCs as softphones in order to make calls through the telephone system.

Line properties
You can change some line properties directly in the list. A dialog can be opened via *properties* after selecting and marking a line. A line has the following properties:

- **Use lines**
  The line is opened by the PBX Call Assist 5 UCServer. Then the line can be used and users can be added.
- **Trunk line**
  This line is treated specifically in PBX Call Assist 5 UCServer if it is an outside line.
- **Activate journal**
  All calls on this line are written to the database.
- **Private telephone**
  In the journal all of this phone's entries are automatically marked as "Private" and are treated according to the rules of the Telephone journal. Other users are not able to see connected numbers or contacts on this phone.
- **Line addresses**
  If the TAPI line has several addresses, you can define here whether incoming calls are notified to all addresses or only to one special address.
- **Internal phone number**
  This is the phone number with which the phone can be contacted internally. The number is normally determined automatically (either from the address or from the line name). A phone number may only occur once. This phone number is the unique key with which the phones are assigned to users and computers**. If you have dual phone numbers such as, for example, with parallel connection of terminal devices, you should use small letters to differentiate the phone numbers.** If you have two lines with the phone number 111, you should give one line the number 111 and the other the number 111b.
- **Location**
  Defines the Location of the line, if the location wasn't configured via the line group. The location defines, for example, the number formats and the dialing rules.
- **Call redirection**
  PBX Call Assist 5 UCServer supports server-side call redirection. Various call targets can be added to the list of redirections. How long a call remains at the relevant extension if it is not answered must be additionally configured. The list of the first line which rings applies. Configured call redirections on lines which are gone through as part of a call forwarding scenario do not apply. All targets in the list must be activated by the server in the line manager. If a target is not monitored, the forwarding is stopped at this number.

Line group properties
Lines are combined into groups. The properties of a group apply to all lines in the group. To display the properties of a group, select the group and press *Properties*. The settings for the Line Group Properties for SIP Softphone and Line Group Properties for TAPI Driver differ in a few respects and therefore have separate help pages.

Line status
The line status, whether available or not, is displayed in the form of a colored icon. If a ECSTA driver is used, the tooltip schows detailed information on the status icon in case of en error (communication error, login error, license error etc.).

Icon	Statement
	This line could be opened.
	This line could not be opened. Check the functionality of the TAPI driver.
	This line is not in use. The terminal device has been physically disconnected and is therefore not connected to the TK system. This line cannot be used.

●	Line has not yet been initialised.

10.1.1.1 Tapi line group properties

The lines are aggregated in groups. The properties of the group apply to all of the lines in the group. To display the properties of the group, highlight the group and choose *Properties* in the context menu. The settings described here apply for TAPI and ECSTA line groups.

In the properties only settings are shown which are supported by the TAPI or ECSTA used.

- **Use all the group's lines**
  If this option is active all the group's lines are switched on.
- **Automatically use line**
  If you have activated this option, the lines will be opened automatically once somebody shows an interest in this line (users, computer, remote TAPI driver, etc.)
- **Create line automatically as required**
  This option is only available for ECSTA drivers.
  If you have activated this option, the lines will be set up and opened automatically once somebody shows an interest in this line (user, computer, remote TAPI driver, etc.). This means that computers can no longer select from the list of available lines, but must enter the respective number when a line is assigned to a user. The PBX Call Assist 5 UCServer will instruct the ECSTA driver to open and provide the line in the telephone system. As soon as the driver offers the line, it will become operative automatically.
- **Activate journal for all lines**
  Every call is written to the journal database for all the line group's lines.
- **Set phone numbers automatically**
  If this option is set the lines' phone numbers are always automatically read out. This option should be deactivated if the phone numbers are not correctly recognized. The numbers for each line can then be entered manually.
- **Use the TAPI-line name**
  As a rule, the phone number is displayed as the name of a line which is currently without an owner. If you wish to display the names supplied by the TAPI-driver for lines you should activate this option.
- **Group location**
  Defines a location for all lines in the line group. In addition to selecting a location, the following options can be configured:

  <Ignore>
  Permits assignment of different locations in the line properties for each line.

  <Automatically>
  The UCServer automatically determines the location of the line based on the phone number. This setting only works if the line can be assigned to a location via the extension number. The line numbers must be taken over by the driver, i.e. they must be set automatically (no manual assignment of the line number).

Characteristics of the line group - CTI functions
Here, you can configure extended settings for certain CTI functions.

- **Activate/deactivate CTI functions:**
  You can activate or deactivate certain CTI functions here. For example, you can hide certain functions that are not correctly supported by the telephone system.
  -If you deactivate a function, it will never be offered irrespective of the status of the call.
  - If you activate a function, it will be offered accordingly if permitted by the status of the call.

- **Remote Office:**
  Remote Office can be activated, or deactivated for all lines in the line group.

Characteristics of the line group - CTI feature codes
Here you can configure advanced settings for certain CTI functions.

- **CTI feature codes**
  Here is where you can store the telephone system's CTI feature codes which are offered in the PBX Call Assist 5 line menu if no telephone calls are being made on the corresponding line. If a call is produced from a selected feature code, it will only be displayed in the client only if the peer rings or the call is connected.
  Each feature code consists of a name which is displayed in the line menue and a code dialed on the telephone system as sson as the user has clicked on the feature code.
- **Pickup facility code**
  Permits configuration of a facility code to carry out a pickup if the driver of the telephone system does not provide this via TAPI. Primarily, it will be attempted to realise a pickup via TAPI. If this fails, the facility code deposited will be used. The code must contain **<NUMBER>**for the number of the line which a call is to be picked up from. Example: ***59<NUMBER>**
- **Always executive a pickup as a pickup (no LineRedirect)**
  In the event of a pickup, the PBX Call Assist 5 UCServer will always try to forward the call from the extension called to the user carrying out the pickup. Only if forwarding fails will a pickup be carried out. By setting this option, you can make sure that a pickup is always carried out right away.
- **Reverse call direction in case of a pickup**
  Some telephone systems report pickup calls as outgoing. This will result in a false display in the journal. This option permits reversal of the call direction.

10.1.2 SIP Softphone Lines

This chapter describes how to add and configure SIP softphone lines. The line can be used by the PBX Call Assist 5 client to make phone calls via a SIP PBX by assigning the line number to a user.

Add and configure new lines

In the Lines dialog, press the *Add telephone system* button and select your system from the list of known telephone systems. Softphone lines can be configured using classic SIP registration be connected to the telephone system. Pressing *Add* calls up an SIP wizard which will guide you through the configuration. If you want to modify an existing line, you can right-click on the corresponding line or line group and modify *Properties*.

Configure the location settings in the Line Group.

Registrar

- **Name of the Line Group**
  Choose a unique name as desired for the group of lines. If multiple telephone systems should be integrated into UCServer, a name that identifies the telephone system used will be helpful.
- **Registrar/IP Address** (of the PBX)
  Enter the DNS name (FQDN) or the IP address of the registrar of the telephone system. Enter the port that the telephone system uses for SIP messages (usually 5060).
  If the telephone system is to be connected via a proxy, the IP address or the FQDN of the proxy server is configured here. In most cases, the setting of the registrar domains is also required (see below).

- **Domain**
  If the registration at the telephone system is to take place via a proxy, the setting of the registrar domain is usually required. In this case, deactivate the *Apply registrar as logon domain* field and enter the desired value in the *Domain* field. If, for example, a Session Border Controller (SBC) is to be placed as a proxy between the telephone system and the UCServer, the SBC can be addressed with the parameter "Registrar/IP address" and the domain of the telephone system with the parameter "Domain". This menu item is only available for certain telephone systems.
- **Register expires**
  UCServer will send a SIP REGISTER notification to the telephone system so that the softphones will be made available for calls. If necessary, choose the time period that should be entered for cyclical SIP REGISTER notifications in accordance with RFC3261 using the *Expires* entry. The value should be greater than or equal to the corresponding setting of the registrar. A value that is too small can lead to logon errors. If the telephone system answers with a different value, this is automatically taken over by UCServer. This menu item is only available for telephone systems with registrar.
- **Register delay**
  UCServer can insert a delay between SIP REGISTER messages. This makes it possible, in large installations with many registrations, to avoid overloading the telephone system when starting UCServer. If necessary, deviate from the default value and select an appropriate value.
- **Failover Delay**
  During redistribution following a server failure, the UCServer waits for the SIP registration of the lines to complete until the time specified here has elapsed. A value of 0 disables this waiting period. Select a value at least equal to the telephone system's SIP registration or session timeout. This setting is independent of the registration delay, which serves only for load balancing during startup.
- **NAT Refresh**
  The UCServer can send cyclical "NAT Refresh" messages to the SIP registrar, in case the SIP registrar is located behind a NAT Device. This is the case e.g. if a UCServer located in the internal LAN has to log on to an SIP registrar of a SIP provider in the public internet (WAN). In many cases, the time between two SIP registrations is sufficient (see menu item *Reregister after*) to keep the ports on the NAT open for incoming calls. Then cyclical NAT Refreshes can be deactivated by setting *0 s*. However, if there is not enough time, a corresponding value may be selected. The value does not depend on the set SIP provider, but rather depends on the used NAT Device. This menu item is only available for specified telephone systems (e.g. SIP provider).
- **SIP Transport**
  In some cases it is desirable to set a different value for the SIP Transport Protocol than the default. However, it is recommended to leave the default settings, since they have been tested for proper function. If you make changes to the settings, you are doing so at your own risk. The UDP, TCP and TLS/sRTP transport protocols are offered. If TLS (in the signaling) is set, sRTP (for Media) will automatically be used. Please also make certain to use a port suitable for the transport protocol, which is set at the Registrar (e.g., for UDP usually Port 5060 and for TLS Port 5061, depending on the setting of the telephone system).
- **SIP Options Refresh**
  The UCServer sends SIP OPTIONS messages to the PBX cyclically to maintain the connection state to the PBX. If necessary, select the maximum time period that should elapse between SIP OPTIONS messages. This menu item is only available for telephone systems with SIP trunk and fixed IP address.

Softphone registrations and lines

Softphone registrations an der PBX oder Nummern aus dem Rufnummernbereich eines SIP-Trunks entsprechen den Softphone-Leitungen im UCServer.

For a SIP trunk with registrar, registering *one* number (e.g. the first number of the number range) activates the entire SIP trunk on the PBX. The remaining numbers of the number range must be added during the configuration in the wizard by "configure more softphones" or in the line group in the tab "Softphone lines". In the "Softphone lines" tab, the number registering the SIP trunk is marked with a "Register".

In the case of a SIP trunk with a fixed IP address, on the other hand, a "Refresher" is marked in the "Softphone lines" tab, which uses cyclic SIP OPTIONS to maintain the connection state with the PBX.

- **User name(s)**
  Enter the user name for logging on to the SIP Registrar here. The user name usually corresponds to the call number of the SIP-Softphone line. If you wish to register several call numbers at the PBX, which have the same password, you can also define several call numbers (e.g.e.g. *123* or *100-120* or also *150;177;200-220*). If the user name does not match the call number of the line, a call number can be manually assigned to the line.
  If multiple phone numbers should be registered with the PBX, activate the *Configure Additional Softphones* option. Doing so will list all registrations from that group of lines. The registrations can be changed, deleted or others added. New registrations can also be added by importing softphone lines.
- **Password**
  Enter the password for SIP authentication, if present.
- **Auth. user name**
  If you have to configure an authentication user name please uncheck *Take authentication user name from user name*. Enter the value into the field *Auth. user name*. If you enter multiple numbers and these are a part of the authentication user name you may use the place holder <*>. At the appropriate place in the Authentication user name, <*> is replaced by the number entered in the User name field.
- **Phone number**
  Some telephone systems require a manual configuration of the call numbers when the user name of the Softphone registration does not match the extension number of the line. For manual configuration, deactivate the *Apply Call Number from User Name* field. Enter the desired value in the *Call number* field. This can be the extension or the canonically formatted number (e.g., +49123456781). The number must correspond to the location settings. This menu item is only available for specified telephone systems (e.g., SIP providers). However, it is also visible when the parameter Automatically set call numbers is deactivated in the Settings of the line group.
- **SIP Options Refresher**
  The number or line for the SIP Options Refresh can be changed by activating the corresponding checkbox for a different number. This menu item is only available for SIP trunk connections with a fixed IP address.

Import of Softphone lines

In the case of a large number of Softphone lines, manually entering the user name, password and call number via dialog box is rather time-consuming. For this reason, there is an import function available for importing the line information from a CSV formatted file. In the dialog box for Softphone registrations the *Add* button can be expanded by the *Import* option. The import file can be selected there.
The data records to be imported must be present in the import file in the CSV format (values separated by commas). For each Softphone line to be imported, one line must be provided containing the required parameters.

The sequence of the parameters is strictly defined. Missing values must be marked with a comma.

Value: User name (mandatory field),
Value: Auth.User name (optional),
Value: Password (optional),
Value: Call number deviating from user name (optional).

Example of data records to be imported with non-used Auth. User name:

abc_xxx,,asdfghjklö,+49123456781
abc_yyy,,asdfghjklö,+49123456782

abc_zzz,,asdfghjklö,+49123456783
...

The Import function only allows new user name entries to be added. Existing user name entries are skipped over in the list of Softphone registrations, even if parameters in those entries have been changed. An import also cannot be used to delete user names from the list.

Export of softphone lines

Im Dialog für Softphone-Registrierungen kann die Schaltfläche *Bearbeiten* um die Option *Exportieren* erweitert werden. Dort kann die Exportdatei ausgewählt werden. In einem Optionsdialog kann eingestellt werden, dass nur aktive Leitungen exportiert werden sollen.
The exported data records are saved in CSV format (see import of softphone lines) and are in the same format as the import function. The password is not exported for security reasons (the value is set empty).

The passwords are not included in the exported data records. If the lines are to be imported again at a later date, the passwords can be added to the export file beforehand or added in the *PBX Call Assist 5 UCServer administration* after importing.

Line group name (defined under Registrar)

- **Line group properties**

PCAP-Log

- **SIP PCAP log files**
  You can find more information in the chapter Creating SIP PCAP Log Files.

Setup SIP Softphone lines

Once the SIP softphone line appears as a line in the group(s) of lines, the line can be activated by checking the left checkbox and clicking the *Accept* button at the top. A colorful icon symbolizes the line status or the success of the SIP registration with the telephone system. *Green* indicates successful registration. A mouse tooltip will provide additional indicators about the current status (such as *Line is functional*). To see the SIP notifications, the corresponding line can be right-clicked and *Display SIP Events* selected from the context menu to inspect them more precisely and track the SIP notifications in an event window. To reset the line (send a new SIP registration message), right-click on the corresponding line and re-start by selecting *Reset Line* on the context menu.

Once registration is successful (the icon is *green*), the line can be assigned to a User (see User Administration - Users). Right-clicking on the corresponding user and selecting *Properties* from the context menu will display the *Telephone Numbers* tab page where the line can be selected from the *Business* entry or the *First Telephone* entry using the button on the right. Alternatively, the number that corresponds to the line number can be entered manually.

10.1.2.1 Line group properties for SIP softphone

The lines are grouped together. The properties of the group apply to all lines in the group.

Settings for declining calls

In many cases, the wide variety of configurations possible for telephone systems necessitates settings in UCServer which determine whether or not calls should be declined, and if so, how.
Note: The SIP responses and numbering in parentheses (e.g. "Decline (603)") listed below correspond to the RFC3261 definition for SIP (Session Initiation Protocol) and are therefore not translated in menus.

- **Client not logged on**
  If no client is logged on to the UCServer, calls are answered automatically on the server side. This option offers a selection of SIP responses with which the UCServer should answer incoming calls. The default setting is "Busy Here (486)" and signals "busy". Other possible settings include "Temporarily Unavailable (480)", "Decline (603)" and "Ringing (180)", i.e. instead of being declined, the call is placed in a "Ringing" state until the caller hangs up or the call is forwarded or "picked up" by another participant.
  This setting only takes effect if no call forwarding is set for the called line on the PBX Call Assist 5 client and if no administrative call forwarding is set up.
- **Client on do not disturb**
  If the line is set to *Do not disturb (DND)* on a client, calls are answered automatically on the server side. This option offers a selection of SIP responses with which the UCServer should answer incoming calls.
  The default setting is "Busy Here (486)", "Busy" is signaled. Further selection options are "Temporarily Unavailable (480)" (currently unavailable), "Decline (603)" (reject) and "Ringing (180)", i.e. instead of being rejected, the call is set to ringing status until it is hung up or forwarded or another subscriber "picks up". This setting only takes effect if no call forwarding is set for the called line on the PBX Call Assist 5 client and if no administrative call forwarding is set up.
- **Reject calls by clients**
  If calls are being declined by clients, this selection of SIP responses can determine how they are declined, or how a decline is emulated.
  The default setting is "Busy Here/Decline (486/603)". Depending on the situation, the client can choose to decline the call using either "Busy Here" or "Decline".
  Fixed selection options are "Busy Here (486)", "Temporarily Unavailable (480)", "Decline (603)" and "Ringing (180)", i.e. instead of being declined, the call is placed in a "Ringing" state until the caller hangs up or the call is forwarded or "picked up" by another participant. The client is "unaware"of this; it is normally separate from the call, while the "Ringing" state is maintained on the server.
  The server setting is used for fixed selection options, regardless of the client. For example, if the client sends a "Decline" to decline a call and the server is set to "Busy Here", the call is answered with "Busy Here" as well.
- **Hide Decline button in client**
  Depending on each case, it may make sense not to give a client user the ability to reject the call via the Decline button. If this option is set, the Decline button is hidden when calls are made to the client (default: option not set).

Administrative call forwarding

- **With logged off client, forward calls to 'voice mailbox'**
  If a phone number is assigned to the 'voice mailbox' field of the user, all calls are forwarded there if no client is logged on to UCServer. In this case no phone calls are automatically declined server-side, since the configuration setting for declining calls if no client is logged on is not applied.

Settings for call forwarding

This menu item is not displayed if a telephone system has the SIP feature '302 Removed' (also known as 'Call Deflection').

- **Forward calls through**
  If incoming calls should be forwarded before the call is accepted (e.g. in case of call forwarding) even though the telephone system does not support this, this functionality can be provided through UCServer.

  <*Forward calls by making new call*>
  In case of an incoming call, UCServer places a new call to the called party and remains active during the call (Call Bridge).
  In this type of forwarding, many telephone systems do not display the caller's telephone number to the party being called, but rather the number of the party being forwarded. In such cases, the option <*Forward calls by answering, holding and transferring*> can help.

  <*Forward calls by answering, holding and transferring*>
  The incoming call is being answered, held and transferred via SIP refer (Blind Transfer).
  Until the called party accepts the call, the caller will hear the on-hold music configured in the telephone system as the call is being forwarded.
  Please note with this selection that if a forwarded call is refused by the client, the caller stays on hold until he or she hangs up. However, this behavior is also dependent on settings and on the type of telephone system.

Journal

- **Activate journal for all lines**
  Every call is written to the journal database for all the line group's lines.

Line phone numbers and names

- **Set phone numbers automatically**
  Phone numbers are automatically generated from the SIP Registration. If this option is deactivated you can configure the phone numbers manually in the line details properties.

Location settings

- **Location of the group:**
  Defines a Location for all lines in a line group. In addition to location selection, the following options may also be configured:

  <*Ignore*>
  Allows the assignment of different locations in the line properties of each line.

  <*Automatic*>
  The UCServer automatically determines the line's location based on the phone number. This setting only works if the line can be assigned to a location via the extension number. Line phone numbers here must be transferred from the SIP Registration, i.e. automatically set (no manual assignment of line phone number).

Line group properties - Functions
Here you can configure advanced settings for certain functions.

- **Activate/deactivate functions:**
  -If you deactivate a function, it will never be offered irrespective of the status of the call.
  - If you activate a function, it will be offered accordingly if permitted by the status of the call.

Line group properties - Feature codes
Here you can configure advanced settings for certain functions.

- **Feature codes**
  Here is where you can store the telephone system's CTI feature codes which are offered in the PBX Call Assist 5 line menu if no telephone calls are being made on the corresponding line.
  Every Feature Code consists of a name, displayed in the line menu, and a code which is dialed on the telephone system when the user clicks the Feature Code. If a PBX Call Assist 5 Feature Code is clicked, a softphone conversation window opens. Many telephone systems acoustically signal (e.g. via the headset) the success or failure of an action. Other telephone systems just hang up with no acoustic feedback after dialing the feature code. Please refer to your telephone system manual for available feature codes and acoustic signals.
- **Pickup feature code**
  Allows a feature code to be configured in order to perform a pickup. The code must contain "<NUMBER>" for the number of the line from which a call is to be picked up. Example: *59<NUMBER>.
  Clicking on the PBX Call Assist 5 pickup function will open a softphone conversation window to carry out the pickup conversation.
- **Execute pickup of SIP lines in UCServer**
  This option enables executing the pickup internally in the UCServer. This allows a PBX Call Assist 5 softphone subscriber to pick up a call from another softphone subscriber without the telephone system having to be involved. If the call picked up does not belong to the softphone line group, e.g. if it is a Tapi line, the pickup is sent to the telephone system unchanged with the configured pickup feature code.

Line group properties - Media
Here you can configure advanced media settings for Softphone. The UCServer contains a media server that connects the PBX on one side and the PBX Call Assist 5 client on the other. The media server converts the data (media streams) into the correct format (e.g. codecs, encryption). The active audio codecs are listed from the top according to their priority if more than one codec is to be offered. To change the priority of a selected codec, move the order using the corresponding buttons.
This setting is available depending on the connected telephone system and should only be changed after consulting with the PBX Call Assist 5 Support.

- **Audio codecs towards PBX**
  The Media Server supports the following codecs: G.711 (8kHz sampling rate), G.722 (16kHz sampling rate), Opus (up to 48kHz sampling rate). Several codecs can be activated at the same time.
  The priority of the codecs should correspond to the settings in the PBX. The codecs with the highest quality would have to be sorted at the top and those with the lowest quality at the bottom in the PBX and in the UCServer. Telephone systems typically offer at least one G.711 codec (with the variants aLaw PCMA or uLaw PCMU). Therefore, the G.711 aLaw codec is always active and cannot be deselected. Many telephone systems also offer HD telephony. The codecs for HD telephony offer a broader frequency spectrum than with the usual G.711 codec thanks to higher sampling rates. As a result, the sound transmission is better and the conversation is easier to understand. A widely used codec for HD telephony is G.722, which can be used for internal and external calls in many cases (depending on the remote station, telephone system and exchange). A very modern, but not so widespread codec is Opus. If the telephone system supports Opus, the best call quality can be used for internal calls with softphones or compatible telephones.
  If a specific telephone system type has been successfully tested with G.722, the codec is activated by default when a new softphone line group is created. In all other cases, the desired codec can also be activated afterwards. If the telephone system has not been tested with G.722, activation is at your

own risk. Information on the status of the tests can also be found by searching the Internet for "Auerswald Connection instructions for telephone systems".

- **Audio codecs towards WebRTC**
  The PBX Call Assist 5 client always communicates with the media server in a WebRTC-compatible format (e.g. encryption via DTLS-SRTP).
  The media server requires the least computing power if the same setting (e.g. 'G.711 aLaw' in each case) is used for the PBX and correspondingly for WebRTC (i.e. for the PBX Call Assist 5 client). However, this does not have to be the case; with activated HD telephony, for example, the G.722 codec can be active towards the PBX, while the Opus codec is active towards the PBX Call Assist 5 client. If an HD codec has been activated for the audio codecs in the PBX direction, an HD codec (Opus) must also be used in the PBX Call Assist 5 client direction. If this has been forgotten in a configuration, it will be adjusted automatically. The Opus codec also has the property that it can achieve good audio quality even at low bandwidths (e.g. 20kBit/s) and is therefore very well suited for PBX Call Assist 5 mobile apps.
- **Media port range (min/max)**
  The media server automatically occupies free system ports for the media streams from the entire range between 1024 and 65535 (internal default setting). In some cases, however, it is necessary to restrict the range. The entered value range applies to all softphone line groups in UCServer and the connected Windows® PBX Call Assist 5 clients. For these clients, the media port range also applies to other WebRTC-based services such as audio/video chat and screen sharing.

10.1.3 SIP softphone via SIP trunk

The SIP softphone can be connected to the telephone system via a SIP trunk. Two different connection types are supported. Depending on the selected telephone system type, the telephone system expects a registration or a fixed IP address when connecting to the UCServer. The SIP GW Listener is used when using a fixed IP or the checkbox is checked or unchecked when using a registrar. If necessary, you can change the default settings on your own responsibility to try other configurations.

- **SIP trunk with fixed IP address**
  The telephone system does not provide a registrar, but requires a fixed IP address (and port) with which the UCServer SIP interface can be reached. This is provided by a network interface through the SIP GW Listener in the UCServer. Create the network interface with the configuration of the SIP GW Listener and enter the data at the PBX. Thus the telephone system can deliver new SIP messages (e.g. calls) to the UCServer.
  The UCServer also needs a setting on which IP address (and port) the telephone system can be reached. Enter the data in the UCServer configuration of the SIP trunk connection to the PBX. This allows the UCServer to deliver new SIP messages to the PBX.
- **SIP trunk with registration**
  The PBX provides a registrar where the UCServer can register with its IP address (and port). The SIP GW Listener must be deactivated. Configure the SIP trunk connection to the PBX at the UCServer.

10.1.3.1 SIP-GW Listener

The SIP GW Listener can provide a UCServer network interface with fixed IP address and port. The transport protocols UDP, TCP and TLS can be set.

Use SIP GW Listener
The check box switches the use of the SIP GW Listener on or off. To use the connection to a PBX with a SIP trunk with a fixed IP address, the SIP GW Listener must be enabled. Create a network interface where the PBX can reach the UCServer.
If you disable the SIP GW Listener, a connection to a PBX with a SIP trunk with registrar can be made.

- **Network interfaces**
  Press "add" at Network interfaces and select a configuration on which the telephone system should

reach the UCServer. A status lamp signals "green" if the port is not yet occupied by another network interface. Determine a still free port in the range between 1024 and 65535 (e.g. 5080).

- **Certificate**
  To use the secured network protocols TLS and MTLS, you can configure a server certificate. This must be signed by a certificate authority. Click on the "Certificate:" button to open the window for selecting a certificate. Select the appropriate certificate and then confirm your entry with "OK". Information about the selected server certificate is additionally displayed.

10.2 Initial Location Setup

The location settings are used to enable the right dailing and display of phone numbers.

Only the right location settings grants external phone numbers to be dialed and displayed correctly.

This section of the help file will describe the individual configuration parameters on the Location Settings dialog. If a location is depicted, the following pages will provide all information necessary for configuration. If several networked locations must be setup, all information for special configuration scenarios can be found in the Location Designs section.

Location name
Enter a name for the new location to be setup. The name will be used for display in the system.

Country/region:
Choose your country from this list.

Area code
Enter your local area dialing code here. This is for example 030 for Berlin or 44 for Zurich (Switzerland). The leading 0 is not necessary and is removed by the system when the settings are saved.

Location is using a PBX
Activate this option, if the location has a telephone system.

Public line type
Please select the type of the public line: DDI trunk line (for Direct Dial-In) or a Multipoint connection line. Sometimes DDI lines are also referred to as DID lines (for Direct Inward Dialing). A DDI line enables external parties to call internal phones directly using phone number ranges. DDI numbers comprise of a PBX base number (addressing the PBX) plus a number range (or several ranges) to address internal phones from outside.
A Multipoint connection typically is used for smaller offices or for home usage. One or more phone numbers (Multi Subscriber Number = MSN) are used in this case. The MSNs may be totally different, e.g. they don't have to use numbering ranges.

PBX base number (only with a PBX using a DDI line)
If you have a DDI line you should enter the PBX base number here. For example if you have the number +1 (30) 12345-222, the PBX base number is 12345.

Extension numbers range
Please enter here the extension number range (DDI range or space) that is allocated by the phone company for the related PBX. For example, if you have the DDI number range from +1 30 12345 30 to +1 30 12345 69, enter "from 30 to 69". Or for example using three-digit extensions while the entire range is available for DDI enter "from 100 to 999". All internal phone numbers in this numbering range will automatically be displayed as external, international phone numbers.

External access prefix
This is a number you have to dial for an external telephone call. Even if an outside line is automatically requested by a telephone, it may be necessary to enter this number in PBX Call Assist 5. This number will be automatically deleted for dialing as well as for the telephone numbers (default value is 0).

Determine external access prefix...
The wizard will provide support in determining the external access prefix (also known as "external dialing code", "trunk access code" or "outside line access code"). Access to a telephone at the location and an external telephone (cell phone) will be needed. If there is uncertainty about the external dialing code, start the wizard and follow its instructions. All settings for the external dialing code will be set automatically.

Phone number format of an extension
Displays the international phone number of an extension number at the current location (PBX usage only).

Details...
The Complete Location Settings will be displayed. The dialog can be opened at any time after initial installation using the Location List in the administrator interface.

10.3 Location

The location settings are used to enable the right dailing and display of phone numbers.

Only with the right location settings it is possible that external phone numbers are dialed and displayed properly.

This section of the help file will describe the individual configuration parameters on the Location Settings dialog. If a location is depicted, the following pages will provide all information necessary for configuration. If several networked locations must be setup, all information for special configuration scenarios can be found in the Location Designs section.

Country/region:
Choose your country from this list.

Area code
Enter your local area dialing code here. This is for example 030 for Berlin or 44 for Zurich (Switzerland). The leading 0 is not necessary and is removed by the system when the settings are saved.

Display Advanced Settings
The location settings have many options that will only be needed in special cases. Settings that are not mandatory for normal operation will not be displayed by the wizard.

The advanced settings include:

- Rules for the detection of internal and external phone numbers
- Rules for formatting the line phone numbers
- Special formatting of phone numbers that will be registered by the telephone system
- Special formatting of phone numbers that will be transferred to the telephone system for dialing
- Least cost routing
- Vanity phone numbers

10.3.1 Area code rules

These settings are only required for countries in North America.

The area code rules determine which dialing rules must be used for dialing a number in the North American Numbering Plan (NANP). The number must be dialed differently depending on how far the number you wish to dial is from your own location. For example, a free call must be dialed differently to a chargeable call.

The target number to be dialed decides which dialing rules are used. The number's area code and the three digits which follow it are decisive.

Own area code
Calls within the local area can be free and chargeable. Configure which dialing rules must be used.

- All calls in the local area are free.
  Phone numbers with the same area code as your own location are always dialed with the *local call* dialing rule.
- There are calls within the local area which are chargeable.
  If there are chargeable phone numbers with your own area code, select the dialing rule *local call (chargeable)*.
    - Configure chargeable phone numbers
      Configure the Prefix rule for which phone numbers wit the dialing rule *Local call (costs involved)* have to be selected. All other phone numbers in the local area are dialed with the dialing rule*Local call*.
    - Configure free phone numbers
      Configure the Area code rule for which phone numbers with the dialing rule *Local call* have to be selected. All other phone numbers in the local area are dialed with the dialing rule *Local call (costs involved)*.

Other area codes
Calls to other area codes may be free. Configure which dialing rules must be used.

- All calls to other area codes are long-distance calls.
  Phone numbers with a different area code are always dialed with the *long-distance call* dialing rule.
- There are calls to other area codes which are free.
  Switch on this option, if there are cost free phone numbers with a different area code and which have to be dialed with the rule *local call other area code*. Configure for every area code area code rule for which phone numbers with the rule *local call other area code* have to be selected.

Automatic configuration
You can access these rules automatically on the internet. For this purpose, the supplier http://www.localcallingguide.com is used. Please always check the accuracy of the imported data, no guarantee is accepted for completeness. If this service is not available, you need to configure the rules yourself.
Information as to which phone numbers must be dialed as local calls from your location is available from your phone company.

10.3.2 Dialing prefix rules

These settings are only required for countries in North America.

A dialing code rule defines a series of phone numbers which must be dialed with a certain dialing rule.

A phone number consists of an area code and a (subscriber) phone number. The first digits of the phone number are known here as a prefix.

Area code
Enter the area code which is to apply for this rule.

List of prefixes
Here you can enter a list of prefixes. If one of these prefixes matches the number to be dialed this rule applies.

Example
A phone number which fulfils this rule reads: +1 (202) 333-5678
Enter 202 as the area code
Enter 333 as the prefix

10.3.3 PBX system

Location is using a PBX
Activate this option, if the location has a telephone system.

Public line type
Please select the type of the public line: DDI trunk line (for Direct Dial-In) or a Multipoint connection line. Sometimes DDI lines are also referred to as DID lines (for Direct Inward Dialing). A DDI line enables external parties to call internal phones directly using phone number ranges. DDI numbers comprise of a PBX base number (addressing the PBX) plus a number range (or several ranges) to address internal phones from outside.
A Multipoint connection typically is used for smaller offices or for home usage. One or more phone numbers (Multi Subscriber Number = MSN) are used in this case. The MSNs may be totally different, e.g. they don't have to use numbering ranges.

PBX base number (only with a PBX using a DDI line)
If you have a DDI line you should enter the PBX base number here. For example if you have the number +1 (30) 12345-222, the PBX base number is 12345.

Extension Numbers (DDI - Direct Dialing In) (only with a PBX using a DDI line)
If all extension numbers have the same length configure an extension number space. If extensions are used with different lengths configure extension number prefix.

Extension number space
Please enter here the extension number range (DDI range or space) that is allocated by the phone company for the related PBX. For example, if you have the DDI number range from +1 30 12345 30 to +1 30 12345 69, enter "from 30 to 69". Or for example using three-digit extensions while the entire range is available for DDI enter "from 100 to 999".
All internal phone numbers available in this range are displayed automatically as external, international phone numbers.

Extension numbers prefix
Please specify the lowest and the highest first digit of the extension numbers. If e.g. the internal numbers 20, 300-499 and 5000 are used please configure '2' as the first prefix and '5' as the second prefix. The length of the internal numbers are set to '2' to '4' in this case. Depending on the length of the internal numbers the program calculates the numbers to be used as external and international types.

Length of internal phone numbers
Enter the length of longest and shortest internal phone numbers. If all extensions are the same length, for example 121 (three digits), both entries should be "3".

Extension phone number format:
External phone numbers: displays the international phone number for the location (only for a system connection).
Internal phone numbers: displays the internal phone numbers for the location

10.3.3.1 Dialing prefixes

Outgoing PC dialing:
An external access prefix (also referred as external dialing code) is the number on the telephone that must be used to make an external call. The entry of this number will be required for dialing from PBX Call Assist 5 even for automatic external access on the telephone. Normally, the following external dialing codes are identical (default value: 0).

- **Local access code:**
  Enter the access code you need for calls to destinations in your own area.
- **National access code:**
  Enter the access code you need for calls to national destinations.
- **International access code:**
  Enter the access code you need for calls to international destinations.
- **Private call external dialing code:**
  Enter the access code required for placing private phone calls. The placeholders: e, E, u or U (see Projects); may also be used.
- **Number for an outside line required to activate call forwarding:**
  Here, enter the number for an outside line which you require for call forwarding.

Determine external access prefix...
The wizard will provide support in determining the external access prefix (also known as "external dialing code", "trunk access code" or "outside line access code"). Access to a telephone at the location and an external telephone (cell phone) will be needed. If there is uncertainty about the external dialing code, start the wizard and follow its instructions. All settings for the external dialing code will be set automatically.

10.3.3.2 Formatting

These rules are applied to all phone numbers that are signaled by the TAPI driver or via the SIP connection.

In all fields you can specify several trunk codes, separated by commas. Normally the ones to be truncated are identical (default value: 0).

Remove trunk access code from numbers

- **reported as incoming:**
  Enter the extension numbers to be deleted from the phone number in case of incoming calls.
- **reported as outgoing:**
  Enter the extension numbers to be deleted from the phone number in case of outgoing calls.
- **reported as a forwarded call:**
  Enter the extension numbers which must be removed from the phone number in case of forwarded calls.

Remove trunk access code from connected IDs

- **reported as incoming**
  Enter the extension numbers which should be removed from the number for incoming connected calls.
- **reported as outgoing**
  Enter the extension numbers which should be removed from the number for outgoing connected calls.
- **Ignore ConnectedID**
  If the driver for the telephone system reports inconsistent number formats for ConnectedID (different forms of numbers to get an outside line for incoming, outgoing or connected calls), you

must ignore the ConnectedID. As a result, you will not see the actual number of the person at the other end, but only the number of the person called or calling.
This option is the last chance to catch inconsistent numbers from the driver. Please try first to make the reported numbers consistent by configuring the driver or the telephone system. **Only activate this feature when it is absolutely necessary**.

10.3.3.3 External rules

External phone numbers:
If a telephone system is used, a difference must be made between internal and external phone numbers. Normally, internal phone numbers are recognized based on the extension range and the length of an internal phone number that has been configured for the telephone system. Deviating from this, it may be necessary to classify certain numbers that would normally be understood as internal phone numbers as external phone numbers.

The rules permit detection of phone numbers based on Regular Expressions or direct comparison. Each entry can be configured individually. If the Replace With column has been entered, the phone number will be replaced automatically. Subsequently, the phone numbers will not be formatted further, but should however be transferred in international format. The configured rules will be processed from top to bottom, until a match has been found.

Check:
The rules can be checked immediately. Enter the corresponding expression in the Phone Number field. If the phone number was detected and how it has been implemented can be seen in the output row. The rule used for recognizing and formatting will be highlighted.

Specific Examples for the Use of Special External Rules:

- Detection of external phone numbers that would normally be understood as internal phone numbers (emergency numbers that are within the internal phone number range, but have not been assigned an extension (110, 112 and 911).

If a comprehensive set of rules should be established, the list can be maintained outside the administrator's utility. Existing rules can be exported as XML or CSV files, adjusted correspondingly and then re-imported.

10.3.3.4 Internal rules

Internal phone numbers
If a telephone system is used, a difference must be made between internal and external phone numbers. Normally, internal phone numbers are recognized based on the extension range and the length of an internal phone number that has been configured for the Telephone systeme. Deviating from this, it may be necessary to classify certain numbers as internal .

The rules permit detection of phone numbers based on Regular Expressions or direct comparison. Each entry can be configured individually. If the Replace With column has been entered, the phone number will be replaced automatically. Subsequently, the phone numbers will not be formatted further, but should however be transferred in international format. The configured rules will be processed from top to bottom, until a match has been found.

Check:
The rules can be checked immediately. Enter the corresponding expression in the Phone Number field. If the phone number was detected and how it has been implemented can be seen in the output row. The rule used for recognizing and formatting will be highlighted.

	Specific Examples for the Use of Special Internal Rules: • Detection of internal phone numbers not covered by the rules configured in the Telephone System. • Conversion of internal phone numbers to external, when internal phone numbers and extensions (DDI) are different. • Detection of internal phone numbers in system groupings with substitution through their representation in international format.
	If a comprehensive set of rules should be established, the list can be maintained outside the administrator's utility. Existing rules can be exported as XML or CSV files, adjusted correspondingly and then re-imported.
	Entries that cannot be edited were automatically created by UCServer for the determination of phone numbers from other locations. These rules will be recorded as Generated Expressions. A tooltip will indicate the location for which this rule was determined. Additional information can be found under Advanced Location Settings. These rules are currently only applied to phone numbers that either come from the telephone system or from the search for contacts in PBX Call Assist 5, given a corresponding configuration in the Advanced Location Settings.

10.3.3.5 Emergency numbers

	The rules for emergency numbers are applied exclusively to softphone lines.
	The phone numbers defined here do not go through any further dialing rules.

Some telephone systems support the specification of call-back location-based numbers for dialing an emergency number.
Depending on the prefix in front of the dialed emergency number (110, 112), the telephone system signals a callback phone number stored in the telephone system in the SIP P-Asserted-Identity (PAI) field or in the FROM field.

If PBX Call Assist 5 with Softphone is used at different and varying locations, no fixed prefix can be assigned per client. With the "Rules emergency numbers", the required prefixes can be prefixed to the emergency number, depending on the IP address of the logged-in client.

After activating the rules for emergency numbers, subnets, emergency numbers and prefixes can be defined.

Description	A name / designation can be specified for each entry. The entry may only contain letters and numbers.

Subnet	The subnet must be specified in CIDR notation. Example: 10.12.13.0/24 or fe80::c91b:d632:2a35:89df%3/60
Emergency numbers	Specification of the emergency numbers. Several numbers can be entered separated by commas. The specified emergency numbers must not be assigned as internal extension numbers!
Prefix	Specifies the prefix which is to be prefixed to the emergency number and signaled to the PBX. The prefix can consist of numbers, #, *.

To prevent the prefix from being displayed on the PBX Call Assist 5 client, it must be removed by means of a rule under "Formatting rules - Outgoing".

The specified emergency numbers must not be assigned as internal extension numbers!

10.3.3.6 Line phone numbers

The Lines will be assigned to the users in the easiest manner based on the phone number configured in the user profile. For this, the line phone numbers should be in international format. If the lines do not have an internationally formatted phone number, the line phone number will be transferred in international format with the location of the line. This will only work when the phone number exists in the DDI range for the location. If the line phone numbers cannot be transferred in international format with the location information, they can be adjusted using rules. Doing so will be necessary when the phone numbers are not in agreement with the DDI phone numbers (numbers outside of the phone number range, cross-network identifiers and so forth).

The rules permit detection of phone numbers based on Regular Expressions or direct comparison. Each entry can be configured individually. If the Replace With column has been entered, the phone number will be replaced automatically. The phone number should be formatted using international notation after the formatting process. The configured rules will be processed from top to bottom until the first match has been found.

Check:
The rules can be checked immediately. Enter the corresponding expression in the Phone Number field. If the phone number was detected and how it has been implemented can be seen in the output row. The rule used for recognizing and formatting will be highlighted.

Specific Examples for the Use of Rules for Adjusting Line Phone Numbers:

- Phone Numbers with Cross-network Identifiers (Cisco)
- Internal and external phone numbers outside of the base number range (lines do not carry the DDI phone numbers, but rather internal line identifiers).

If a comprehensive set of rules should be established, the list can be maintained outside the administrator's utility. Existing rules can be exported as XML or CSV files, adjusted correspondingly and then re-imported.

10.3.4 Formatting rules

You can change and individually format phone numbers with special rules. This can be done using Search/Replace or Regular expressions. Besides the formatting rules, phone numbers can also be changed internally/externally via those rules. Depending on whether the phone number has been registered by the telephone system or sent for dialing to the telephone system, the sequence of processing the rules will be changed. Additional information about the sequence in which the rules will be applied are described in the sections Phone Number Formatting and Dialing Rules.

The rules permit detection of phone numbers based on Regular Expressions or direct comparison. Each entry can be configured individually. If the Replace With column has been entered, the phone number will be replaced automatically. The configured rules will be processed from top to bottom until the first match has been found.

Formatting Phone Numbers that have been registered by the Telephone System
Note the order of the Phone number formatting.

- **Incoming**
  Phone numbers for incoming calls which are reported to the PC by the phone system are formatted with these rules.
  These phone numbers come directly from the phone system as dialable digits. They consist exclusively of digits and also * and #.
  The phone number may include an external dialing code and, optionally, be an international, national, local or internal phone number.
- **Outgoing**
  Numbers for outgoing calls which are reported to the PC by the phone system are formatted with these rules.
  These phone numbers come directly from the phone system as dialable digits. They consist exclusively of digits and also * and #.
  The phone number may include an external dialing code and, optionally, be an international, national, local or internal phone number.

Formatting Phone Numbers before They are transferred to the Telephone System for Dialing:
The sequence in which phone numbers will be adjusted for Dialing has to be observed.

- **PC dialing**
  Phone numbers for outgoing calls which are to be dialed.
  These rules will be applied after the phone number has been transferred in International Format.
  At networked locations, this list will show generated expressions, given a corresponding configuration in the Advanced Location Settings, in order to convert long phone numbers from other locations into DDI phone numbers.
- **PC dialing final**
  Phone numbers for outgoing calls which are to be dialed.
  These rules are applied directly before the phone number is sent to the phone system.
  The phone has already been formatted for dialing (with the External Dialing Code).



Specific Examples for Formatting Phone Numbers:

- Removing cross-network identifiers for registered phone numbers.
- Setting the cross-network identifier when a call should not go through the external telecommunications provider but rather through the internal location network.
- Replacing phone numbers when they should not be visible for other users at the application

	layer level.
	If a comprehensive set of rules should be established, the list can be maintained outside the administrator's utility. Existing rules can be exported as XML or CSV files, adjusted correspondingly and then re-imported.
	Entries that cannot be edited were automatically created by UCServer for the determination of phone numbers from other locations. These rules will be recorded as Generated Expressions. A tooltip will indicate the location for which this rule was determined. Additional information regarding this will be found under Advanced Location Settings.

10.3.5 Least cost routing

Least cost routing is the automatic selection of the cheapest call-by-call provider for a call. You must configure rules in order to make this choice for a call. For the server to be able to offer LCR, there have to be rules setup. These kann be setup manually oder implemented from different web services.

- **Provider**
  The list Provider contains all Call-by-Call providers which can be used, with their respective dialing code.
- **Zones**
  The list Zones contains the different zones for the Least Cost routing.
- **Assignment of zones to providers**
  With the Allocation of providers the systems knows when to use which provider. According to the time you can specify the weekday seperately (Monday to Friday), Saturday or Sunday Allocation to the provider zones.

Reset
Deletes all LCR settings.

Import and export
You can import and export all LCR settings. The following formats are supported:

- Own LCR-data format (**.lcrxml*)
- Agfeo LCR-data format (**.lcr*)
  For Germany you can obtain LCR-data in this format from several providers in the Internet.

10.3.5.1 Provider

A provider is a provider of call-by-call telecommunications services. In order to use a provider for a phone call the provider's network dialing code is dialed before the phone number.

Examples for Germany

Provider	Pre-selection network prefix
Arcor	01070

Tele2	01013

10.3.5.2 Zones

A zone represents a list of phone numbers which can be called for a certain tariff. You can assign a provider to every zone accoring to date and time.

Zone name
Enter a name for for the zone, e.g. longis distance or mobile.

Area code list
All phone numbers which start with digits provided in the list belong to this zone. The phone numbers are compared during processing the Dialing rules. The phone numbers must be entered in the super canonical format (e.g. "+1171").

Examples:

Area code	Meaning
+1	All numbers which begin with +49, in other words all phone numbers in Germany (apart from special numbers).
+1905	All phone numbers which begin with +1905, in other words all numbers in Toronto, Canada.
+117	All phone numbers which begin with +4917, in other words all mobile phone numbers in Germany with a 017x dialing code.

Instructions
You typically configure zones for local calls, long-distance calls and mobile phone networks and several zones for other countries.

Priority of longer dialing codes
If there are several dialing codes configured in different zones which fit the phone number, the zone which has the greater number of digits in its dialing code is used.
Example: the number +4917123456789 is dialed. If *+4917* is entered in zone 1 and *+49171* in zone 2, zone 2 is used because more digits match.

Priority of zones without providers
If there are several dialing codes configured in different zones which are identical and one zone has no provider assigned to it the zone without a provider has priority.

10.3.5.3 Least cost routing assignment

Every zone can be assigned to a provider. This assignment is separate for Monday to Friday, Saturday and Sunday. Different providers can be used at different times for each of these days.

The time (in 48 half-hours) is plotted to the right of the table. The configured zones are listed at the bottom. Each line of the table shows which provider is used for the zone at the respective time.

Select the provider which you wish to assign. Next, click on the cells date and time in the table where the provider is to be used.

10.3.6 Advanced

Core services

Phone number format, PC dialing
This option determines the phone number format for outgoing calls. Phone numbers are transfered in this format to the phone system.

- Apply dialing rules (standard)
  Phone numbers are always formatted according to the dialing rules.
- Always international super-canonical/E164
  Phone numbers are always converted into the super-canonical phone number format (e.g. +1891234567, also known as international E.164 format) before they are sent to the phone system. Only activate this option, if your phone system and the TAPI driver supports this phone number format.

Always use the area code when dialing in local area
If the area code must be dialed for calls in the local area, this option must be enabled. In some cases, IP Centrix providers require the call to be dialed with the corresponding area code. This relates to both the outbound dialing as well as the formatting of phone numbers that are reported by the telephone system. Phone numbers in databases must be provided with the local area code in order to be dialed. Enable this option only if your telephone provider requires dialing the local area code in their own local network!

Automatically re-dialing extensions
If a number to be dialed is longer than the maximum phone number length allowed in the corresponding target country, the number will be divided into sections and the first section dialed and then the remaining section dialed as a DTMF number after the connection has been made. This currently applies for countries like the United States, Russia and Taiwan. The maximum phone number length is defined in the countries.xml and cities.xml files. If the option has been deactivated, the telephone system will have to emulate this behavior.

Cross-location Settings
If several locations that have consistent, non-overlapping phone numbers have been integrated into one UCServer, the server can determine rules, which will allow for calls to be sorted by locations. The DDI phone numbers may not overlap. Each phone numbers can only exist at one location.

Enable Location Integration
This location will be activated for the rules for location integration. Only activated locations will be used for the determination of the rules.

Detect phone numbers from other locations
By activating this option, the server will determine the rules for this location in order to generate the international format for the abbreviated DDI phone numbers from other locations. They will be stored in the Internal Rules. When the feature is activated, it will check if the current location settings exhibit a unique phone number range. Any occuring errors will be displayed.
Only DDI phone numbers registered in the system will be expanded to their international format.

Search for phone numbers across locations
Allows to search for abbreviated phone numbers at other locations in PBX Call Assist 5. The internationally formatted phone number will be used for searching the associated databases.

Abbreviate Phone Numbers before Dialing
Long phone numbers from other locations will be abbreviated to the DDI phone numbers before dialing. The rules to be determined for this will be displayed under PC Dialing. If dialing between locations requires cross-network identifiers, the rules will have to be configured manually from PC Dialing.

10.3.7 Vanity

Letters marked on the phone's keypad makes it possible to apply for numbers whose alphameric conversion corresponds to a certain name or concept. These are phone numbers which can be written as a text. Vanity phone numbers can be used in different areas (0700, 0800, 0180...). For example: 0800HANSMEIER.

Resolve vanity numbers
Here you can define phone numbers for which you wish to use vanity numbers. Enter the dialing code without the national identifier number, e.g. 700, 800.

10.3.8 Projects

PBX Call Assist 5 UCServer permits the user to assign calls to previously defined projects, to send certain code numbers to the phone or the phone system when dialing or to mark calls explicitly as private.

Parameters are, for example, used with targeted MSN assignment, the initiation of private calls in phone systems or for dialing project parameters. You can define several parameters here and give them names. They can then be used in the call window. The parameters are always saved in the journal on the PBX Call Assist 5 UCServer.

Parameters have two functions:

- Parameters for dialing. These are sent to the phone system and activate specific features before making the call.
- Parameters for the Journal. These are included in the journal (server-side) and are subsequently used for invoicing by project parameters.

Define projects

1. Enter a readable name for the project in field **name**. This name appears later in the call window and the journal.
2. Enter the **parameter** which is dialed before the actual number in the column of the same name.

   The following rules apply:

Character	Deployment
0-9 * #	Digits which are dialed normally
C	Here you wait for the remote station to accept the call.
e, E	Place-holder for entering a PIN. With E, the number of digits for entry is not important. With e, the number of digits is defined by the number of letters (eee for three digits).
u, U	Place-holder for entering a user ID. With U, the number of digits to be entered is not important. With u, the number of digits is defined by the number of letters (uuu for three figures).

p, P	Dialing pause: p for 0.5 seconds, P for 1 second
N	Place-holder for the number to be dialed. If the place-holder is not specified the number is automatically added to the end.
J	Defines, if available, that the user login and pin number entered by the user is noted in the journal.
X	Defines, if present, that the number to be dialed should be dialed with an external code. If the 'X' is missing the number is dialed in national format (03012345678).

3. Select one of the following **options** which is to apply for the project:
   Journal entry only: The parameter is not sent to the phone but just saved in the journal.
   Dialing and journal entry: This parameter is used for outgoing dialing is saved in the journal entry.
   Dial only: This parameter is only used for dialing.
   Dial Private Call: The Access Code for Private Calls option is used for this (see Dialing Prefixes). Doing so may be necessary in order place private calls, depending on the telephone system and configuration. Phone numbers used for private calls will not be visible to others and will be additionally flagged in the journal.

Examples of use

- For the journal only:
  You wish to assign project parameters to calls. Create an entry and name it e.g. Project Test and give the parameter 12345. Select the Journal entry only option. The parameters are logged on the server side only.
- Selective external dialing code:
  Assume you have have a normal external dialing code of '0' and a further external dialing code which is '80'. Create an entry and name it 'External2'. Enter '80' as the phone number. Select the 'Dial only' option.
- Select project parameter:
  Assume you can dial the project parameter '4444' on the phone with the combination *604444#. Create an entry and name it 'Current Project'. Enter *604444# as the phone number. The X means that an external dialing code must be added after the project parameter. You can then also make internal calls with this project parameter.
- Private call 1. Example:
  Assuming you can dial a private call on the phone with your personal PIN '1234' by means of the combination *601234#: create an entry and name it 'Private'. Specify the number as *60eeee#X. The 'X' means that an external code must follow the parameter. You can then also make internal calls with this parameter. The 'eeee's mean that you still have to enter a four-digit PIN. If you then dial in the call window with this setting you are asked to enter this PIN. You can, of course, enter the PIN for private calls here directly, in other words *601234# (if no other person has access to your computer).
- Private call 2. Example:
  Assuming you can dial a private call on the phone with your personal PIN ,1234' by means of the combination 51234: after entering the PIN you no longer have to dial an external code. Create the entry and name it 'Private'. Enter 5eeee as the phone number. This time, no X is used (no external code after the parameter). The 'eeee's mean that you still have to enter a four-digit PIN. If you then dial in the call window with this setting you will be required to enter the PIN. You can, of course, also enter the PIN for the private call directly here: 51234.
- Example of a calling card provider:
  With the rules you can deal with dialing a calling card provider for private conversations. Enter the phone number format required by the calling card provider in the project parameters field.

E.g.: 0080012345678CP#eeeeeeeee#uuuu#N#
The calling card provider is dialed via the number 0080012345678. After the call has been answered there is a one-second delay; the 8-digit user ID and then the four-digit password is subsequently transmitted, followed by the number to be dialed. The placeholders for ‘e’ and ‘u’ were queried by the user in the client. User recognition and the PIN can be saved on the client if desired.
The subsequent dialing of digits after a pause or waiting for an answer from the remote station is realised with DTMF tones. This is only possible if your TAPI driver supports this feature.

10.3.9 Remote - TAPI driver

Here you can set up the remote and Multiline TAPI-driver phone number formats.

PC dialing

- **Dial without formatting**
  The phone number is only adapted by the rules in "PC dial final" in Formatting rules, all other formatting rules are ignored.
- **Format phone numbers before dialing**
  All rules for outgoing dialing stored in the location are applied.

Phone number format:

- **Without formatting**
  Phone numbers are passed to the remote TAPI-driver without formatting. The application which uses TAPI receives the numbers as if they had been reported directly by the phone system.
- **Pre-formatted, without external dialing code**
  The phone number is preformatted, i.e. with all rules applied but not presented super-canonically.
- **Formatted, super-canonical**
  The phone number is formatted with all rules and presented super-canonically.

10.3.10 Check rules

Here you can check the configured rules. Enter a phone number and check if the phone number si used correctly for displaying or dialing.

Format for dialing
Formats a phone number that will be transferred to the telephone system for dialing. The formatting process will perform the following steps:

Formatting for call forwarding
Formats a phone number that will be transferred to the telephone system for call forwarding. The formatting process will perform the following steps:

Format for display
Formats a phone number for display.

ConnectedID outgoing
Formats the outgoing ConnectedID reported by the driver. The formatting process will perform the following steps:

ConnectedID incoming
Formats the incoming ConnectedID reported by the driver. The formatting will perform the following steps.

CallerID
Formats the CallerID reported by the driver. The formatting process will perform the following steps.

CalledID
Formats the CalledID reported by the driver. The formatting process will perform the following steps.

Call forwarding
Formats the phone number for call forwarding reported by the driver. The formatting process will perform the following steps.

10.3.11 Location concepts

Configuration options for systems with several locations are displayed in the locations designs. If the telephone system to be set up involves a single location, it should be configured based on the Location Settings. An attempt should be made to include the following issues in the system design:

- **Consistent Phone Number Range:**
  - Internal phone numbers corresponding to DDI
  - Internal phone numbers that have not been assigned multiple times
  - Location phone numbers can be assigned in blocks
  - Extensions can be quickly dialed across locations (in connection with or without a cross-network identifier)

  - Configure the individual locations based on the key performance indicators for the respective location.
  - In Advanced Location Settings, enable *Enable Location Integration* and *Determine Phone Numbers from Other Locations*.
  - To the extent that direct dialing of an abbreviated phone number across locations is possible, also enable *Abbreviate Phone Numbers before Dialing*. If dialing through cross-network identifiers is available, corresponding rules should be configured under PC Dialing. Alternatively, the telephone system can take over the conversion of the phone numbers to be dialed.

- **Arbitrary Phone Number Range:**
  - Internal phone number does not correspond to DDI
  - Internal phone numbers can be assigned multiple times
  - Location phone numbers cannot be grouped into blocks

  The internal phone numbers must be converted to fully canonical external phone numbers for arbitrary phone numbers ranges and for phone numbers outside phone number range (DDI/internal). For this, enter the transformations in Internal Rules. In this manner, the fully canonical representation can be sought from the internal phone numbers in the associated databases and, vice versa, the fully canonical phone numbers can be abbreviated before dialing the internal extension numbers. The rules necessary for this should be entered under PC Dialing.

10.3.11.1 Phone number formatting

A phone number which is sent from the phone system to the PC has to be formatted accordingly before further processing. The server always uses Super-canonical phone numbers.

The phone number is formatted in this order:

1. **Formatting**
   All digits apart from + * # 0 1 2 3 4 5 6 7 8 9 are removed.

2. **Application of the formatting rules**
   The rules of the Formatting rules are applied. For further processing, the modified (if necessary) phone number is used.
3. **Removal of the external dialing code**
   External dialing codes are removed if present. If an external dialing code is found the phone number is treated as an external number.
4. **Recognition of internal numbers**
   Provided that no dialing prefix was removed, it is decided by the length and rules for internal phone numbers whether it is an internal phone number.
   - Detection of Special External Phone Numbers, when the phone number is external
   - Phone numbers in the DDI Phone Number Range, when the phone number is internal
   - Detection of Special Internal Phone Numbers, when the phone number is internal (the phone number may have been modified)
   - Detection of Phone Numbers from Other Locations, when the phone number is internal (phone number will be given the appropriate long distance dialing codes).
   - If the length of the phone number corresponds to the specifications for an Internal Phone Number, when the phone number is internal
   - Phone number is external
5. **Removal of call-by-call dialing codes (only outgoing phone numbers)**
   Existing CallbyCall prefixes are removed for outgoing phone calls. The used prefixes are saved in a Configuration file *providers.xml*.
6. **Standardization of the number**
   The phone number is now converted in a super-canonical phone number.

10.3.11.2 Dialing rules

The dialing rules influence the formatting of phone numbers when dialing from a PC.

The phone number is formatted in this order:

1. **Formatting**
   All characters apart from + * # 0 1 2 3 4 5 6 7 8 9 a b c d e f g h i j k l m n o p q r s t u v w x y z are removed. All letters are turned into capitals.
2. **Vanity phone number recognition**
   If the number contains one of the configured vanity numbers and if the letters following it are valid according to the ITU E.161 rules the number is first converted into dialable digits.
3. **Further formatting**
   All digits apart from + * # 0 1 2 3 4 5 6 7 8 9 are removed.
4. **Recognition of specific numbers**
   A decision is made based on specialnumbers.xml as to whether it is an special number (normally emergency numbers). If the number is stored in the xml file it is dialed externally without further formatting.
5. **Recognition of specific external numbers**
   The decision will be made based on the rules for External Phone Numbers about whether an external phone number is involved or not. If an external phone number is detected, it will be dialed externally without additional formatting.
6. **Recognition of internal numbers**
   A decision is made by means of the internal numbers as to whether it is an internal number in the system. If an internal number is recognized it is dialed without further formatting.
7. **Phone number standardisation**
   The phone number will be converted to the international numbering plan.
8. **Transfer of Project Settings**
   If dialing has been initiated in connection with a Project Identifier to be dialed through the telephone system, it will now be applied to the phone number to be dialed.

9. **Using least cost routing**
   If configured, the rules for the least cost routing process will be applied.
   Least Cost Routing (LCR) will not be used, if:
   - the phone number to be dialed involves a special external or an internal phone number
   - Call Forwarding has been configured (the applied call forwarding number will be considered independent of the time of day or week and will therefore not be considered by LCR).
10. **Transformation of external phone numbers into internal numbers**
    If you have configured a system phone number (system line) a check is made as to whether the phone number is an internal number. If an internal number is recognized the number is shortened.
11. **Using the PC dialing rules**
    The phone number runs through the special rules for PC dialing.
12. **Abbreviation of long Phone Numbers from Other Locations**
    To the extent that the Location Networking has been configured so internationally formatted phone numbers from other locations will be abbreviated to their DDI phone numbers, the phone number will now be abbreviated accordingly
13. **Transformation into a dialable number**
    The phone number is reformatted according to the rules of the configured country in a dialable phone number. The dialing rules of countries are saved in the Configuration file *countries.xml*.
14. **Using external dialing codes**
    The appropriate external dialing code(s) is/are added if the number has not been identified as internal yet.
15. **Using the PC final dialing rules**
    The PC final dialing rules are applied directly before the phone number is sent to the phone system.
16. **Dialing the number**
    The number is sent to the phone system.



Dialing Phone Numbers directly without using Dialing Rules
By prefixing a **!** can suppress the use of dialing rules. The phone number will then only be transferred directly to the telephone system driver without any formatting.

10.3.11.3Telephone number formats

Supercanonical number
A phone number format which allows the unique international identification of the participant. The PBX Call Assist 5 UCServer and PBX Call Assist 5 exclusively use the super-canonical phone number format for all phone numbers. For the display the simplified number is sometimes used (if available). Phone calls are carried out with the shortened phone number.
Supercanonical phone numbers always begin with a + and have the following format: **+Country City Number**
But no spaces are used. e.g. +49301234567
The number should only contain digits and +.

Service numbers
are special public phone numbers which cannot be given in international number format. These are for example emergency numbers (110) or directory enquiries (118xx). In order to be able to dial these numbers from a PC they must either be longer than the internal phone numbers or configured as external rules. these numbers are specified directly as dialable numbers:

DDI Phone number
Direct Dialling In phone number. External phone number of a participant in the system. This phone number can be displayed in its short form as well as in the international form bconsisting of country, dialing code and

DDI. DDI numbers will be shown in short form for the same location, the system uses the international form internally.

Phone number
No spaces are used. Example: 11833

Dialable phone numbers
are always kept in the format required by the phone system in order to reach the subscriber. The number is formatted according to the rules in PBX Call Assist 5 UCServer.
Examples:
Phone number internal extension number
Phone number external dialing code Number of subscriber 12345 in the local area network
External dialing code Country Area code Phone number Number of a subscriber in a different country
The above examples apply for Germany and depend to a large extent on the regions. You can see which dialing rules apply for your location in the location settings.

Phone numbers for display
are used by PBX Call Assist 5 insofar as this form consisting of the country code and the area code can be determined.
+Country (area code) number
Example:
+49 (30) 123456 Phone number of subscriber 123456 in Berlin, Germany

10.4 Telephone journal

The telephone journal will be stored in a server database, which will be centrally created on the server for all users. The users will have access to the journal entries belonging to them.

10.4.1.1 Private call

PBX Call Assist 5 UCServer supports special treatment of private telephone conversations. Conversations will be considered private when the user explicitly flags the call as private. All conversations made on a line flagged as private will be flagged as private by default.

- **Don't handle private calls separately**
  With this option, private calls are written to the journal along with all other calls.
- **Store private calls with a shortened number.**
  In this case, the last digits of the phone number will be replaced with XXX. The name of the caller will not be stored in the journal.
- **Store private calls without the number.**
  In this case phone numbers and names are not stored.

10.4.1.2 Journal

The journal records all telephone events in a database. How long certain records remain stored in the database before they are archived or deleted can be set from here.

Record archiving is only possible using Microsoft Access® databases.

The time interval for maintenance is between 1 AM and 4 AM.

- **Permanently Keep Journal Records**
  Select this option if all phone calls (internal and external) will not be archived or deleted.

- **Archive Journal Records Every X Days**
  This option was available up to PBX Call Assist 5 8.0 in conjunction with Microsoft Access® as the database system.
  If you have connected a **Microsoft SQL Server®** as a database system, the administrator of your chosen RDBMS can set up regular archiving.

- **Delete Journal Entries**
  - **Delete Internal Phone Calls without Notes after X Days**
    Select this option, if internal phone calls should be deleted after a certain period of time.
  - **Delete External Phone Calls without Notes after X Days**
    Select this option, if external phone calls should be deleted after a certain period of time.
  - **Delete All Phone Calls with Notes after X Days**
    Select this option, if all phone calls with saved notes should be after a certain period of time.
  - **Delete chat messages after X days**
    Activate this option if you want to delete chat messages after a certain amount of time.

Apply rules now
Thereby, the journal and offline journal maintenance will be performed immediately.

A maintenance cycle may take a long time in some cases and the journal database will be blocked during that time. For this reason, Apply Rules Now should not be executed during normal operating hours.

10.4.1.3 Offline journal

In addition to the journal, an offline journal will be kept, in which all telephone calls are saved when the client is not connected with the server.

- **Delete offline journal**
  Obsolete entries can be automatically deleted from the offline journal after a preset number of days using this feature.
  Important: If the automated journal database maintenance has been activated, the storage period for offline journal entries must be shorter than the shortest storage period configured in the journal.

10.5 Unanswered calls

With these rules it's defined which phone calls should be marked as unanswered in the journal. It will be distinguished between missed calls or calls which were forwarded and then answered. For both scenarios it can be defined seperately which user receives the call marked as unanswered.

Unanswered calls deposited to ...

- **no participant**
  No participant who has been called receives the call marked as a missed call in the journal.
- **the first subscriber who has not answered the call**
  The participant whose phone has rung first receives this phone call marked in the journal as unanswered.
- **the last participant with an unanswered call**
  The participant whose phone has rung last receives this phone call marked in the journal as unanswered.
- **all subscribers**
  All participants whose phone has rung receive this phone call marked in the journal as unanswered.

Forwarded and answered phone calls deposit to ...

- **no participant**
  No participant who has been called receives the call marked as a missed call in the journal.
- **the first subscriber who has not answered the call**
  The first participant who has not answered the phone call receives it marked as unanswered in the journal.
- **the last subscriber who has not answered the call**
  The last participant who has not answered the phone call receives it marked as unanswered in the journal.
- **all subscribers with unanswered calls**
  All participants who have not answered the phone call receive it marked as unanswered in the journal.

Special cases

Some scenarios are treated differently:

- **The call is answered by pickup on another (possibly not monitored) extension**
  If the TAPI driver reports a call disconnected per LINEDISCONNECTMODE_PICKUP, the call is logged as 'answered' because a 'pickup call' changes the call state always to 'connected'. Regardless if the answering party is monitored or not, the disconnect cause of a call can be found in a TAPI trace (e.g. using 'TAPICaps' of the support tools). The Journal logs the connected party if the party is monitored by the UCServer.
- **The user forwards the call to another party using the PBX Call Assist 5. The other party may not be monitored.**
  If a user forwards a call via PBX Call Assist 5 to another party the server logs the call as 'answered', regardless if the other party is monitored or not. For example, if a user forwards all calls to his mobile phone all incoming calls are logged as 'answered'.

	In the journal entry it's noted who has answered the call.
	A phone call is logged as unanswered by the PBX Call Assist 5 UCServer once the call ended. If the option "Report unanswered phone calls to the first participant who hasn't answered the call" is valid but the call is still in the system (e.g. in a cyclic call distribution), then logging is done once the caller has finished the call. It is possible that users receive journal entries which are marked with a delay as not processed. For answered calls applies the same: The information who has answered the phone call is noted in the journal only at the end of the telephone call.

10.6 Error handling

Settings for special situations which only occur under special circumstances and with certain phone systems can be set up here.

Tapi LINE_REINIT report
How PBX Call Assist 5 UCServer reacts to a LINE_REINIT message is defined here. This message can be triggered by a TAPI-driver if it has no automatic error handling implementation e.g. for when the connection to the phone system is lost.

Line cannot be initialized
How PBX Call Assist 5 UCServer reacts if a line cannot be initialized when PBX Call Assist 5 UCServer is started

is defined here. Either the line is then not available until after rebooting or another attempt is made to initialize the line.

Delay after lineOpen
Here the time span can be preset for how long the PBX Call Assist 5 UCServer waits after every opening of a line.

11 User management

On the following page is the setup of users, groups and computers explained:

- User
- Groups
- Computer
- Profile
- Global settings

11.1 User

Here you can set all users relevant settings. This includes the user's contact information, Numbers and line assignments, Services that can be used, group memberships and user rights. Depending on the user management not all the settings can be configured. Settings which can not be configured here must be edited in the leading user management.

General

Field	Description
User name (login)	This is the user name the user logs in with onto the PBX Call Assist 5 UCServer . It corresponds to the Windows® login name if Active Directory® is being used.
Identity	The identity of the user, in order for them to be clearly addressed in the Federation scenario. The address of the identity corresponds idealy with the e-mail address of the user, because then the user is also accessible from outside of the company via the federation.
First name	The user's first name (e.g. Arthur).
Last name	The user's last name (e.g. Dent).
Displayed name	This is the user's full name (e.g. Arthur Dent). This can occur several times and is only used for display purposes. If the field is empty, a suggestion is automatically shown when the first and last name are entered.
User profile	Here a user can be assigned to a user profile if more profiles than the 'default' profile exist.
E-mail address	This is the e-mail address of the user. Among other things, it will be used for notifying the user about missed calls and voice-mail messages.
UC Password	Usually the authentication of the users is carried out via the Windows® domain authentication. Alternatively a password can be defined here and the user login configured for the usage of a password User login.
User profile	User profile is active. The user can log on and use PBX Call Assist 5 UCServer services.

active	

Telephone numbers

The telephone numbers of a user are displayed as the telephone numbers of their contact. This applies both to PBX Call Assist 5 UCServer users and to Federation contacts. The PBX Call Assist 5 UCServer searches for the lines to the phone numbers when loading user accounts. The user automatically receives the lines belonging to them without any further configuration. The behavior can be configured via global settings. and via user database-specific settings configure. See Automatic line binding.

Phone numbers and a user's line numbers have to be entered in super-canonical format, when using integrated user administration. Phone numbers from the Active Directory® are displayed as they are saved in the Active Directory®. During the loading of user accounts in the PBX Call Assist 5 UCServer the numbers are converted into super-canonical notation. If you use several locations, the phone numbers have to be entered in the Active Directory® in super-canonical notation!

You are able to select the lines of the user via a button, as well as the business phone numbers and the other phones. The phone number of the line is then transfered into the respective field. Next to the button is displayed how many lines were found for the phone number. The user can use and control as many phones as they like (with the right licences), to a particular phone number.

Property	Description
Business	The user's primary business phone number
Business 2	Another business phone number of the user
Private	The user's private phone number
Mobile	The mobile phone number of the user. This phone number is used, for example, for the automatic setup of call diversions and to send SMS text messages.
Pager	The user's pager phone number. The attribute can be used to store a user's private mobile phone number.
Voice mailbox	The user's mailbox phone number. The mailbox is the user's personal answering machine. This number is used for automatically setting up call redirections. It should be entered as an internal phone number (e.g. 147).
Recording server	The phone number of an external call recording server. This field is only required if you use an external server instead of the integrated call recording server. If this field is filled, the entered phone number is used for the Call recording. If no number is entered, then the centrally configured number is used.

Other, for phones that cannot be seen by other users

Permits the allocation of phones which are not in the contact details of the user. The user can use these phones as usual. The line identifiers are always used if via the number of the user a linebinding isn´t

possible. The line identifiers are not formatted by site rules and point directly to a line in the routing list. The user can use these phones normal.See Automatic line binding.

Property	Description
First phone	This is the user's personal phone's internal number. A phone can only have one owner. This assignment is also used for the offline journal.
Second phone	You can specify a second personal phone for the user here.

Contact address

The contact address shows all contact relevant details of the user. They can be viewed by PBX Call Assist 5 UCServer users as well as by Federation contacts (depending on the authorization).
A contact picture can be assigned to every user when using the integrated user administration. This picture is then displayed at different places in the PBX Call Assist 5. This photo is used (thumbnailPicture) if the Active Directory® user administration is used. The picture is scaled to the size of 96x96 pixels when it's saved or added.
In addition, you can also allocate a large profile picture for every user. This profile picture will be used by clients who are logged on via web services. During import, the profile picture will be automatically scaled to a width of 400 pixels.

Services
Enter here which software and functions the user is allowed to use. The user can obtain more rights through membership in a Group as mentioned here.

Field	Value
General features	
Configure user account yourself	If this option is activated the user may change server-related settings themselves.
Start chat	If this option is activated the user may send text messages to other users.
Allow AudioChat	If this option is activated, the user is allowed to make AudioChats with other users.
Allow AudioChat and VideoChat	If this option is activated, the user is allowed to make AudioChats and VideoChats with other users.

Accept screen share prompts	If this option is enabled, the user may only use the screen sharing functions when prompted to do so by another user.
Initiate desktop sharing	If this option is enabled, the user may independently share his screen with other users as well as request other users to share the screen.
Send SMS	If this option is activated, the user may dispatch text messages as SMS. For that the SMS text message dispatch must be configured in UCServer.
Send missed calls as an e-mail	If this option is activated, the user receives e-mails for missed phone calls. For this the E-mail dispatc has to be configured in the UCServer. The user decides in the PBX Call Assist 5 settings whether they want to use this feature.
Deliver unanswered phone calls as SMS text messages.	If this option is activated, the user receives SMS text messages for missed phone calls. For this the SMS text message dispatch has to be configured in the UCServer. The user decides in the PBX Call Assist 5 settings whether they want to use this feature.
Record calls	If this option is activated the user may use the call recording function. The call recording must also be configured.
Use phone books	If this option is activated, the user is allowed to use phone books as a contact data source. The usage regulations of the respective manufacturer are to be followed. Phone books are linked via estos MetaDirectory.
Use phone books	If this option is enabled, the user may use phone books as a contact data source. The terms of use of the respective manufacturer must be observed. Phone books are connected via estos MetaDirectory.
Use apps	If this option is enabled, the user is allowed to use the mobile apps. The setting can be changed only if this right has not already been assigned in the global permissions.
Workstation Client Login via the Internet	If this option is activated, users with selected PBX Call Assist 5 can log on to this server via a public network without having to establish a VPN connection to the network. You need a UCConnect account and additional licences if necessary.
Share content	
Files	When this option is enabled, users can share documents and other contents via the Chat function. In order to do this, the functions 'Chat' und 'Share Contents' must be configured and activated in the UCServer.

Other external services	
Profile page visible to anonymous users	If this option is enabled, the user contact data are visible via the business card of the Web service.
Integration in Microsoft® Teams	If this option is activated, the presence status is synchronized between Microsoft® Teams and the PBX Call Assist 5 client. The prerequisite is the setup of Integration in Microsoft® Teams.
PBX Call Assist 5 Voice Services	This setting is only available if the user is activated for the PBX Call Assist 5 Voice Services.
Use Voice-Mailbox	The Voice-Mailbox is set up for each user with the initial setup and can be deactivated here.

Additional lines
Here, additional lines can be made available to a user. These lines are then displayed on the Client in Favourites within a specific group that cannot be changed by the user. From there, these lines may be copied into other groups or into the monitor.

Field	Value
Display outgoing calls	If this option is activated the user may see the phone numbers and names with which this extensions makes calls if the calls are initiated from here.
Display incoming phone numbers	If this option is activated the user may see the phone numbers and names with which this extensions makes calls if this extension is called.
Forward/pick up calls	If this option is activated the user may pick up calls from this extension.

Authorizations
Which users have authorizations for the user just opened and what the authorizations are can be specified here.
User rights can also be granted through group membership and global allocation. These are, however, not visible.
This setting can also be changed by the user themselves via PBX Call Assist 5. For federation contacts these settings can only be changed in PBX Call Assist 5

Authorizations are always cumulative, i.e. if the authorization is given in one place it cannot be removed again at another.

Member of
Here you can enter which Groups this users belongs to.
If Active Directory® is being used as the user management system, the P flag in the Type column will indicate that this group is the primary group of users. The primary group assignment cannot be configured here.

Status
This page displays when the user last logged in, which computer they used and what their current status is. In addition, an overview is included, which shows currently used devices or programs of the user logged on to UCServer. It also contains the information whether the device shows active or inactive state.

11.2 Free additional fields

This selection is only available with a LiveChat license.

This dialog allows you to create your additional custom fields with contact data for UCServer users. To do this, you define possible field identifiers and their display names. Customized content can be assigned to these additional fields within the user configuration.

	You need an appropriate client to display these additional contact data.
	Please note these contact data may also be sent to any anonymous users from the Internet.

11.3 Voice Services - Users

If the user object for "PN_PBXVOICESERVICE_SHORT" is activated, lines/call numbers from this area and registered end devices can be assigned to the user.

By activating the user for the "PN_PBXVOICESERVICE_SHORT" a voice mailbox is set up for the user. The user can set up the voice mailbox on the PBX Call Assist 5 client for Windows® and activate call forwarding to the voice mailbox.
The messages left by the caller are delivered to the user via email.
If no Voice-Mailbox is to be available to the user, this can be deactivated on the Services tab.

	A valid, externally accessible e-mail address must be entered for the user.

After assigning a PN_PBXVOICESERVICE_SHORT line, the use for softphone can be activated. The SIP line is created automatically and the user can use the line immediately on the PBX Call Assist 5 client.

11.3.1 Assign phone devices

After the end devices have been entered on the PBX Call Assist 5 UCServer, they can be assigned to the user on the "Phones" tab.

Select the desired device via the "Add" button. In the next step, you can assign the terminal device to the phone numbers assigned to the user.
Save the selection and (re)start the terminal after applying the settings.
The assigned phone numbers are automatically assigned to the phone device.

	Softphone and phone devices can be activated and used together for one phone number.

Please also refer to the notes on the Auerswald GmbH web pages: https://support.estos.de/de/procall-voice-services

11.4 Groups

User groups are used to group users and to assign rights together.
The administrator defines which authorizations the group members have against each other. In addition, they can define a group leader and optionally a deputy who can have additional authorizations.

General

- **Group name**
  In addition to displaying the group name, it is possible here to define a group line and its rights towards the group members,
- **Head of group / deputy**
  The group leader and their (optional) deputy have a superior role in the group but only in that they can be granted extended authorizations to the group members.
  The users entered here do not have to be group members.
  If a group leader is defined, the authorization field in which the authorizations can be defined appears.
- **Group settings active**
  If the group settings are active, all settings apply for the members of the group. The group settings have no influence if they are deactivated. This setting does not change the status of the user profiles (active / inactive).

Services
Which software and functions the group users may use is defined here. If you allow a function in the group it applies for all group members. If you do not allow a function in the group this does not mean it is disabled for all group users - the user's individual settings are then used.

Field	Value
General functions	
Configure user profile personally	If this option is activated the user may change settings relevant for the server themselves from within PBX Call Assist 5
Start chat	If this option is activated the user may send text messages to other users.
Allow AudioChat	If this option is activated, the user is allowed to make AudioChats with other users.
Allow AudioChat and VideoChat	If this option is activated, the user is allowed to make AudioChats and VideoChats with other users.
Accept screen sharing requests	If this option has been enabled, the group users may only use scree sharing features when they have been invited to do so by other users.

Initiate screen shares	If this option has been enabled, the group users may independently share their screen with other users as well as invite other users to share screens.
Send SMS	If this option is activated the user may send text messages as a SMS. The SMS dispatch must also be configured.
Record calls	If this option is activated the user may use the call recording function. The call recording must also be configured.
Use phone books	If this option is activated, the user is allowed to use phone books. The respective license regulations of the phone book manufacturers are to be followed. Phone books are linked via the estos MetaDirectory.
Use apps	If this option is enabled, the user is allowed to use the mobile apps. The setting can be changed only if this right has not already been assigned in the global permissions.
Workstation Client Login via the Internet	If this option is activated, users with selected PBX Call Assist 5 can log on to this server via a public network without having to establish a VPN connection to the network. You need a UCConnect account and additional licences if necessary.
Journal access within the group	
The group’s journal will be visible to the group leader.	If this is option is activated, the group leader (and his deputy) can view the journal of all group members, except calls marked as "private".
The group’s journal will be visible to the whole group.	If this option is activated, all members can view the journal of all group members, except calls marked as "private". Unanswered calls or changes to entries are only sent to clients whose users are also allowed to change the journal entries.
Journal entries may be modified	If group members are allowed to see the each other’s journal entries, they will also be allowed to modify the entries with this additional option.
Share content	
Files	If this option is activated, users can transfer files in the chat. The service must be set up under Services - Share content.
Other external services	
Business card visible for	If this option is enabled, the user contact information is visible via the business

anonymous users	card of the webservice.
Portal group	If this option is enabled, members of the group can be displayed in the Portal of the web service.
Integration in Microsoft® Teams	If this option is enabled, the presence status is synchronized between Microsoft® Teams and the PBX Call Assist 5 client. The prerequisite is that the integration in Microsoft® Teams has been set up.

Members
The group members are listed here and can added to or removed.

If the group is set up as a collective group with the option "SIP softphone (in UCServer)" and the option "Use as agent group" is activated, the "Agent" column is displayed with the login status of the members.

	The user is logged in to the group. The user can be logged out via the context menu.
	The user is logged out of the group.
	The user is logged in to the group, but all PBX Call Assist 5 are logged out. The user can be logged out via the context menu.
	All PBX Call Assist 5 sessions have been terminated and logged out of the group.

Authorizations
Here the authorizations can be set for the group members to each other. A predefined menue simplifies the authorizations settings into several levels. Depending on the authorisation level for the group a predefined rights setting is given regarding access to information like presence, calendar, primary and secondary lines states. The predefined settings can be changed by checking or un-checking rights-related checkboxes. In this case the authorisation level is set to 'special'.

Monitor groups
The contents of the Monitor and the Favorites can be specified here. Thus to each member of the group the members (activated for PBX Call Assist 5) of the registered group are shown automatically in a "PBX Call Assist 5 group" of the Monitor and/or the Favorites. For the user, the administrative groups are marked with a padlock symbol and cannot be custom-populated with contents.

Keys
Here, the members of this group can be given "keys" with phone numbers and speed dials in the montitor and/or the favorites.

11.5 PN_PBXVOICESERVICE_SHORT - Call groups

If a group available in PBX Call Assist 5 UCServer is activated on the "General" tab as "call group for PN_PBXVOICESERVICE_SHORT", the "Collective group" tab is switched active.
On this must the phone number **from the range of the PN_PBXVOICESERVICE_SHORT line group** is entered under which the group is to be reachable.

An incoming call is signaled to all group members logged on to the group, on **all terminals and phone numbers** in each case.

For group members, the PBX Call Assist 5 client for Windows® expands with a new function. The user can log in and out of the group.

If the "Switchboard" menu item is activated, an additional telephone number that can only be reached externally **can** be entered for the call group. Here you can enter single-digit phone numbers. e.g.: +498151368560

11.6 Ringing strategy

You can choose between 2 ring strategies:

Parallel	An incoming call is signaled to all registered group members at the same time
Sequential	The incoming call is only forwarded to one group member at a time. If the call is not answered by this user within 15 seconds, the call is forwarded to the next active member of the group and so on. The order in which they are passed on corresponds to the member list in the Members tab of a group and can also be changed there.
Witing Queue	Incoming calls are accepted and put on hold immediately. The calls are forwarded to the registered agents in a sequence to be defined. The queue is configured exclusively in the WebAdmin of the telephone system.

11.7 Timer

As an option, **off-hours** can be defined. This allows you to specify whether and when incoming calls are only answered with an "After hours" announcement or redirected to a voice mailbox.
By adding multiple entries, different times can be set for the days.

Example:
The company's opening hours are:
Monday to Thursday: 8:00 a.m. - 5:30 p.m
Friday: 8:00 a.m. - 3:00 p.m

The following entries must be defined as closing times:
Mon, Tue, Wed, Thu: 5:30 p.m. - 8:00 a.m
Fri: 15:00 - 23:59
Sat, Sun: All day - All day

If the **Voice mailbox** is activated, the announcement must contain a reference to this. No additional announcement is played.

The voice-messages left by the caller are sent by e-mail to the specified recipients.

	A valid, externally accessible e-mail address must be entered for the selected users.

All announcements for PN_PBXVOICESERVICE_LONG must be WAV files in the following format: Mono, 8kHz, 16 bit, PCM

11.8 Hunt groups

If the "Collection group" option is activated on the "General" tab, the "Collection group" tab is activated. Depending on which option is selected, different options are displayed on the "Collection group" tab.

11.8.1 SIP Softphone (in UCServer)

Incoming calls on this line are delivered to all members of the group who have assigned a **SIP line** and use PBX Call Assist 5 as a softphone.
The call is not displayed for members who only have a TAPI line.
The group must be assigned the phone number of a **SIP line** under which the group should be reachable.

If the **option "Use as agent group"** is activated, the group members must log in to the group in order to be signaled calls. If a member is logged in to the group, this is indicated on the PBX Call Assist 5 clients in the favorites and in the monitor by the icon displayed.
The status of the group members can be viewed in the member list on the "Members" tab.

The call group is managed exclusively in UCServer. No information is passed on to the telephone system.

Since the PBX Call Assist 5 UCServer manages the hunt group itself and no information is passed to the PBX, members can have SIP lines from different number ranges and PBXs. The availability of additional switching functions depends on the configuration of the telephone system.

11.8.2 PN_PBXVOICESERVICE_SHORT

See Voice Services for more information.

11.9 Computer

The computer settings are used to permanently assign lines to a (computer) location.

In the computer settings you can enable or disable the computer account, as well as you can see information about the update service, installed client version on the computer and the last logon date.

If Active Directory® has been selected under User Database, all computers managed from Active Directory® will be displayed here. If the user management system is manually managed using UCServer, all computers will have to be manually added from there.At least, add all of the computers whose clients should be remotely installed or administered. Optionally, add all of the computers which should always provide

notifications about their most recent activities.
The Add... and Delete... buttons are available for this purpose.

Actions from Buttons

Action	Description
Add...	Here, the desired computer name can be specified or searched in the network (if the computer is powered on).
Remove	Deletes the selected computer from the list.
Properties... (or double-click the desired computer)	Displaying and configuring the Properties for a computer.
Begin updating the client	If a new version of the client has been copied to the update directory, its distribution can be forced. Otherwise, it may take a day for the new version to be installed.

Actions through Context Menu

Additional features are available from the context menu (by right-clicking on the computer).

Action	Description
Install Software	With this action, the update service can be copied and started, which will then automatically download the current version of PBX Call Assist 5 UCServer and install it. Software components can also be uninstalled here.
Update Installation Status	First runs the Reset Installation Status action. Afterwards, the update service will be asked to re-send its data. This feature is helpful for checking if both program components can successfully communicate with each other.If not, check the firewall settings first. Furthermore, the display can be manually updated when a version of PBX Call Assist 5 has been manually updated and there is no desire to wait for the display to update automatically.
Reset Installation Status	The data about the installed version and the last contact between either the update service or clients and UCServer will be deleted.
Open Log File	An additional window will open here, in which all individual steps have been logged. An error code will also be displayed for errors and problems. This display can be used, when information about each action is desired or problems need to be narrowed down.

Remove	Deletes the selected computer from the list.
Properties...	Displaying and configuring the Properties for a computer.

Column Description

Description	Description
Computer name	Assign the computer name in the network as well as in Microsoft® Windows®
Own extension	Primary assigned line
Second extension	Secondary assigned line
Update server	Version of the update services on the workstation or terminal server
Client software	Version of PBX Call Assist 5 on the workstation or terminal server
Last logon	The most recent date when which components last registered themselves will be displayed here. The component may either be the update server or a successful login by PBX Call Assist 5. If more detailed information is desired, open the Properties dialog for the computer and switch to the Status tab page.

11.10 Properties for a computer

General
Two phones which always stand next to this computer can be assigned to it here (as a rule, these are not mobile phones). When a user logs into this computer they can use the phones even if they are not the owner of the phones.See also use with roaming users.

Status
It is displayed here when a computer last logged on with the server and with which PBX Call Assist 5 version or update service software version.

11.11 User rights

There are individual authorizations between system users. A user can acquire authorizations for another user in various ways. These authorizations contain both rights to see information about another user and rights to control their phones or to set their presence status.

A user can acquire authorizations for another user in the following ways:

- **Global rights**. If an authorization is granted in the global rights it applies for all system users. These rights are configured exclusively by the administrator.
- **Group rights**. If authorization is granted in the group rights, this applies to all users who are members of this group. The rights are configured exclusively by the administrator.
- **User permission**. Every user can grant individual rights to themselves to other users. These rights can also be viewed and configured by the administrator.



Rights always apply additively. If the user has acquired a certain right via superior rules this cannot be taken away in subordinate rules.

The following authorizations are available:

Authorization	Description
See presence	The other user may see the presence status (present, absent…).
Set presence	The other user may alter the presence status. This right should only be set for special trust relationships.
See private appointments	The other user may see the appointments marked as private in the calendar. This right should only be set for special trust relationships.
See public appointments	The other user may see the appointments marked as public in the calendar.
See outgoing numbers (primary/secondary line)	The other user may see who the user is currently calling with their primary/secondary phone. This right should only be set for special trust relationships.
See incoming numbers (primary/secondary line)	The other user may see who is currently calling the user on their primary/secondary line.
See the number of a set redirection (primary/secondary line)	The other user may see to which target number a redirection in the phone is activated. This right should only be set for special trust relationships.
See call redirection (primary/secondary line).	The other user may see that call redirection is activated on the phone.
Pick up calls to the user (primary/secondary line).	The other user may pick up incoming calls on the primary/secondary line. This right should only be set for special trust relationships.

11.12 Profile

A profile consists of a list of optional settings for users. These settings are loaded and applied by te PBX Call Assist 5. The settings, defined in the profile, overrule the corresponding Registry settings from HKEY_CURRENT_USER in the client. If a setting is preset in the profile, this setting is write protected in the PBX Call Assist 5.

A profile can be assigned to every user. If no profile is assigned to a user, the standard profile with the name "Default" is used. This also applies if the assigned profile for the user was deleted.

The settings of the profiles offers a similar functionality as the administrative templates of the Active Directory® group guideline. The settings are applied with the following priority:

1. HKEY_LOCAL_MACHINE - Group guideline
2. HKEY_CURRENT_USER - Profile
3. HKEY_CURRENT_USER - Group guideline
4. HKEY_CURRENT_USER – User settings

Profile name
Every profile must have an unique name. A description of the profile can be optionally entered.

General
You can make individual adjustments to contact details and conversation windows for the selected profile. To configure the fields, start the editor via the link.

Custom Tabs
In this section, addresses of websites can be configured which are shown in the PBX Call Assist 5 as tabs in the main window. This allows you to integrate web based applications in PBX Call Assist 5.

Provide a title each which names the tab and URL (e.g. http://intranet) which is displayed.

Some web applications imply a certain (newer) Internet Explorer® version. You may set the needed emulation mode in the registry for this purpose. With the following registry entry PBX Call Assist 5 will use the Internet Explorer® 9 compatible mode:

HKEY_LOCAL_MACHINE\SOFTWARE\(Wow6432Node)\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_BROWSER_EMULATION\ECtiClient.exe = [DWORD] = 9000

In order to use the Internet Explorer® 11 emulation mode set this DWORD value to 11000. More information and adaptabilities for embedded Internet Explorer® controls may be found on the Microsoft® web pages.

Fax
This section allows you to configure the client-side fax integration for PBX Call Assist 5. The application offers you two different integrations from which you must select one. If you select "Exchange Gateway", both your incoming and outgoing fax messages are displayed by Outlook® as emails or By choosing WebService, both incoming and outgoing faxes will be displayed, recorded and sent through custom tab pages in PBX Call Assist 5.

Settings
Each line can concern one or more functions. The line can be edited with **Edit**. Three settings are possible:

- Not configured
  No specifications are given by the server for this setting.

- Activated:
  This setting is preset by the server.
- Disabled:
  This setting is deactivated by the server. This status is not available for all settings.

11.13 Global settings

Rights which apply globally on the server for all users can be configured here. If a right is configured here all users have this right regardless of the group or user configuration.

⚠	Changes of user rights are usually activated immediately for the entire system. Large installations possibly need longer because of changes made to user rights!
⚠	Globally assigned permissions cannot be revoked on the user object. The permissions can be extended on the user and group object.

Give users global permissions among themselves:
Global permissions can be defined here that all users have mutually. If a permission is granted here, this permission applies independently of the group or user configuration. The meaning of the permissions in detail can be found under Global permissions.

In the table, you can specify which software and features users are allowed to use. The users can use more functions than specified here through individual assignment on the user object or through membership in a group.

Field	Value
General features	
Configure user profile personally	If this option is set, all users are allowed to change their Personal settings in the user management itself.
Allow AudioChat	If this option is activated, the user is allowed to make AudioChats with other users.
Allow AudioChat and VideoChat	If this option is activated, the user is allowed to make AudioChats and VideoChats with other users.
Enable screen sharing rights via federation	If this option is set the screen sharing rights specified by the administator can also be used via SIP federation. Users across enterprises (different domains) may share their screen with other users. Users within the same enterprise (same domain) may also invite other users to share screens.
Accept screen sharing requests	If this option has been enabled, the user may only use the screen sharing features when other users have invited them to do so.
Initiate desktop sharing	If this option has been enabled, the user may independently share their screen with other users as well as invite other users to share their screens.

Enable access to the whole journal for all users	All users can be given access to the phone journals of all users here. This, however, only makes sense with installations which have a small number of users.
Users are allowed to delete journal entries	The journal entries can be subsequently changed by the user to a limited extent. For example, the user can subsequently change the note on the call or the call partner. If this option is activated, the user can delete journal entries.
All users have all users in the monitor	If this option is activated, a special group is set up for every system user in the client monitor in which the user can see all other UC software users. This option only makes sense for installations with a small number of users. For a large number of users (more than 20) such an administrative parameter can be set via the groups.
Assignment of rights to monitor groups	Permissions can be set for the monitor groups specified in the group objects. The permissions set here are valid for all administratively specified monitor groups. If users are added to the monitor via monitor groups or the above setting "All users have all users in the monitor", they have global permissions among themselves. If there are no assignments in the groups, you can additionally assign a minimum of rights here. This is useful, for example, not to send permission requests to the users.
Automatically provide phone numbers as lines which are configured in the user account.	Phone numbers, configured in the user account are automatically used by the server for the line binding. If the server finds a line for a user's phone numbers, then this line is automatically assigned to the user. If this automatism cannot be used in the existing environment, it can be deactivated via this option. View Automatic line binding.
Use apps	If this option is enabled, the user is allowed to use the mobile apps. The setting can be changed only if this right has not already been assigned in the global permissions.
Workstation Client Login via the Internet	If this option is activated, users with selected PBX Call Assist 5 can log on to this server via a public network without having to establish a VPN connection to the network. You need a UCConnect account and additional licences if necessary.
Share content	
Files	If this option is activated, users can transfer files in the chat. The service must be set up under Services – Share Content.
Other external services	
Integration in Microsoft® Teams	If this option is activated, the presence status will be synchronized between Microsoft® Teams and the PBX Call Assist 5 client. The prerequisite is to set up the Integration in Microsoft® Teams.

Profile page visible to anonymous users	If this option is enabled, the user contact data are visible via the business card of the Web service.

12 Services

The setup of the different services of the PBX Call Assist 5 UCServer is described on the following pages:

- Update server
- E-Mail dispatch
- Notifications
- SMS dispatch
- Call recording
- Share content
- External servers
- TURN/STUN server
- Push notifications

12.1 Update server

PBX Call Assist 5 UCServer provides an automatic Update service, as well as central Software distribution. Both services need the update server. The update server provides its services via the CTI client port.

The update server is the counterpart to Update service on the PCs. The installation packages are provided in the installation list under "ClientInstall" for the update and installation service. When you install PBX Call Assist 5 UCServer the current matching client version to the server version is copied into the *ClientInstall* folder in the same language as the server. If you wish to provide further languages for software distribution and the update service you must copy the appropriate installation packages into the folder manually.
The folder is monitored by the server for changes; in other words, you do not have to restart the Server when you wish to offer new installation packages. Simply copy the packages into the folder. They will be recognized and offered automatically. (The files must be entered in *UpdateDefinitions.xml*. The various language versions with different names for the installation files are, however, already defined here.)

In the administrator, you can see the update server settings and the available installation packages in the appropriate versions and languages. The most important settings are:

- **Limit availability by time**
  If you wish to limit the installation of updates by time you can define a time frame here in which update services receive installation packages from the server.
- **Behavior with active media connections**
  During an update, all active softphone, audio and video calls as well as screen shares are terminated. Define whether a client should be updated immediately or only when there is no longer an active call.
- **Packets available for the update server**
  List of the installable update packages present on the server.

If you deactivate the update server you cannot use central software distribution.

12.2 E-Mail dispatch

PBX Call Assist 5 UCServer supports sending email. This transmission feature is used for administrator error notifications and events, as well as for notifying users of unanswered calls.

SMTP server
Host name, or IP address and port number, for the mail server. By default, the port number will either be 25 (for SMTP) or 587 (for Message Submission).

Login name (optional)
User name for the SMTP connection (SMTP AUTH)

Password (optional)
Password for the SMTP connection (SMTP AUTH)

Sender's e-mail address
The sender's e-mail address.

Recipient's e-mail address
The administrator's e-mail address for the delivery of error messages.
You may enter multiple adresses separated by a semi-colon.

Allow e-mails with UTF-8 (UNICODE) contents
Allows the server to send e-mails in UTF 8 code. If you deactivate this option, e-mails can send only characters known in the ISO Latin code page of the operating system.

Force TLS
Activates forced TLS encryption. If the server does not provide any encryption, transmission will fail.

Validate...
A test message will be sent, which may take a few minutes. A pop-up dialog will then appear, which will report on the success or failure (including potential error message) of the test.

12.3 Notifications

PBX Call Assist 5 UCServer supports message dispatch for unanswered calls.



There are an array of new features for unanswered phone calls compared with PBX Call Assist 5 UCServer 3.0. E-mails that were previously sent for missed phone calls from the client or server are now sent centrally via the server. It is configured in the server in which cases e-mails for missed phone calls are dispatched. The single user decides for himself whether he would like to receive them or not. Settings for missed phone calls are now configured separately for the journal and the e-mail dispatch.

The message is always sent to the line owner's address. This is identified via User administration

The contents of a notification can be customized with a template. The content of e-mails can be adapted with the help of XSL generate templates as html. View XSL templates.

Recipient

- **Do not deliver**
  No e-mail notifications for missed phone calls are dispatched.
- **first participants, who have not answered the call**
  The first participant whose phone has rung receives the notification about the missed phone call.
- **last participants, who have not answered the call**
  The last participant whose phone has rung receives the notification about the missed phone call.

- **all subscribers who have not answered the call**
  All participants whose phone has rung receive a notification about the unanswered phone call.

PBX Call Assist 5 UCServer supports the recognition of parallel switchings, group calls, cyclic call distribution and redirection in the call phase. This helps prevent dual delivery of unanswered calls, even if the call rang on several phones.

Send an email even if the call is accepted by another party
If this option is enabled an Email is sent to the called party even if the call is accepted by another party (e.g. per pickup).

Use the caller's email address as the sender
If this option is active, the e-mail notification has the caller as a sender. With this option you permit a direct contact with the caller.

If you use a Groupware solution for absence notifications, the caller receives a message with the absence note you provided. With this the caller is informed when the person can be contacted again or if specified in the absence note they can contact a colleague.

Attach caller contact details to the email as a vCard
Contact information which was established via the Contact search can be automatically attached as vCard to the e-mail. This also permits access to all the caller's contact data if you are not in the office.

Give telephony links the following prefix
Activate this option, if a phone number should be formatted as a link when sending notifications of missed calls through email. The reference line will take the place of the HRef attribute of the introductory <a> tag. This reference line may be standardized with the help of a prefix. The following prefixes may be preset by you.

- **tel:** (default settings for Android, Blackberry and iOS, for example)
- **phone:**
- **callto:**

Furthermore, you have the option of assigning an individualized prefix (up to 9 characters plus terminator). Please note that the prefix must be terminated by a **colon**. If you do not want to use prefixes then deactivate this option. In that case, phone numbers will not be formatted as links in notification messages.

Exceptions

- **With internal calls**
  No notifications are generated for internal calls.
- **Calls with hidden phone number**
  No notifications are generated for calls with hidden numbers.
- **If no contact data could be found**
  No notifications are generated for callers in which contact data couldn't be found.
- **With repeated phone calls on the same day**
  If the caller phones more then once in the same day no notifications are generated.
- **For phone calls repeated without user login**
  If the caller calls repeatedly and the user doesn't log onto the system, for example, because he is on vacation.

- **If the call rang for less than 2 seconds**
  If the caller rang for less than 2 seconds and you don't return calls from colleagues or customers who accidentally dialed your number.
- **If the calling number has been stored in this list**
  then you will be allowed to excluded certain extensions and phone numbers from the notification process. For example, the doorman's office may be stored in the list.

Use this language
You can set the language in which the e-mails are sent. The languages for which files exist in the *languages* directory are available.

12.4 SMS dispatch

PBX Call Assist 5 UCServer can offer SMS dispatch using several providers. To use these services, you must be registered with one of the providers listed who will invoice you for this service.
Fees may vary depending on the provider. With some providers you have to have a static IP in order to use the service. Simply compare the various providers and pick out the most favourable one for you.

Configuration

- Select one of the SMS providers listed.
- Enter the data specified by the provider into the field user name and password.
- Various providers allow the use of gateways to take advantage of certain features. A short text describes the individual gateways and their features.
- Depending on the provider, you can also include the return address with the query. If this option is offered by the provider, you can choose between three different ways of defining the return address. If you choose to use the mobile phone No. configured in the user profile, only those users having a mobile phone number may use the SMS function.
- Send a test SMS permits you to test the configuration.

	The service User account has to be activated so that a user is able to use the SMS text message dispatch.
	In principle, every service provider can be connected if it has a HTTP GET or POST interface. For this the configuration file has to be adapted accordingly in the installation list *config\smsprovider.xml*. The template can be found under *config\default\smsprovider.xml*.

12.5 Call recording

A function for recording calls is integrated into PBX Call Assist 5 UCServer. Call recording is realised via a three-way conference with an ISDN card (with a CAPI driver). If a user makes a call and initialises recording, a three-way conference with the ISDN card is commenced on the user's phone. The PBX Call Assist 5 UCServer recognizes the user with the help of the phone number and records the conversation. At the end of the conversation the recording is sent as a file attachment by e-mail to the user. For this purpose the users in the configuration need to have an e-mail address configured and the e-mail dispatch has to be setup.

- **MSN(s) of the ISDN adapter**
  Enter a phone number here with which the ISDN controller can be contacted within the phone system. You may also enter multiple phone numbers seperated by a semi-colon. At least entering one phone number is required even if the option "Accept all calls" is set. The phone number is used to accept calls and to establish the conference call for the recording service.

- **Maximum number of simultaneous connections**
  Enter here the maximum possible number of simultaneous connections to the ISDN controller.
- **Location for phone number formatting:**
  In order for the incoming call on the ISDN card to be assigned to a user the phone number reported by the CAPI driver must be formatted. Enter the location under which the ISDN card is connected to the phone system.
- **Use audio compression**
  The call is recorded either as a *wav*file (PCM 8 Bit, 8kHz, mono) or in a compressing audio format. To enable the support for compressed audio formats additional software is required to be installed. It is recommended to use the Lame MP3 Encoder because of its simplicity.
  Please copy the program 'lame.exe' and the related DLLs to the UCServer installation directory. Afterwards the audio compression feature can be enabled by using the administrator program.
- **Accept all calls**
  If you activate this option all calls will be accepted by the CAPI device regardless of the called number. You should use this option only if your device does not process the CAPI information properly. Do not activate this option if the CAPI device is used by different applications (fax, voice, etc.).

12.6 Share content

In order to use the feature Share Contents and make it possible for users to transfer files in Chat, the following configuration settings should be made. In the UCServer Manager in the Services menu under Share Contents you can activate and configure the use of the function Share Contents for the entire system.

Function	Description
Activate	Activates the function Share Contents for the overall system
File location	Here you can define the directory where UCServer places the files in temporary storage for the file transfer.
Define total capacity (specification in MB)	Capacity that is permitted to be used in its entirety for the storage of files before a low space warning message is displayed. You can activate the warning message in the UCServer in the General Menu under Events.
Maximum file size (specification in MB)	Limits the size for an individual file
Blocked file extensions	Manage blacklist for files not authorized for dispatch. You can exclude individual file extensions from dispatch or receipt here.
Delete files	Automatic deletion of files in temporary storage after a specified time interval

You can administer individual users or groups in the UCServer manager in the menu item User Management. The authorizations for users or user groups can be granted there.

	The files to be sent are temporarily stored on UCServer. In this way, the files can also be preserved for users who are not currently logged on. The files are stored in externally non-readable format in the file system and thus protected from unwanted access. Manual cleaning of this intermediate storage is not recommended. Instead, use the "Delete Files" function of the UCServer Manager.
	The maximum size for a file to be transferred is restricted by the system to 25MB.
	In order for a user to be able to use the function Share Contents, this service must be enabled in his/her User Account.

12.7 External servers

External servers will provide additional services for this UCServer installation. These services include:

- **Web services**
  Web services permit access to UCServer through HTTP or HTTPS. This will permit communication with clients located on the Internet using UCServer.
- **Audio Relay Server**
  Audio relay servers are required in order to make it possible to use SIP softphones (audio chat) with telephone systems that are not compatible with WebRTC.

12.7.1 UCConnect

If this UCServer installation has been registered with UCConnect, UCServer will connect with one or more external servers. They can provide the Web Services and STUN and TURN Servers features.

12.7.2 Local Web Service

A web service, which is continuously connected with UCServer (inbound), will be installed on the local machine by UCServer. This local web service will provide the Web Services and Audio Relay Servers features.

This service also has its own web interface and the web applications "Multimedia Business Card" and "Portal".

The web interface
The links specified refer to localhost and HTTP. If the pages are retrieved on another computer and/or if HTTPS (default setting on Port 7225) is to be used, they must be adapted accordingly.

- Main page
  http://localhost:7224
  This page contains references to the other pages of the WebService.
- Installation support for the mobile apps
  http://localhost:7224/ws/appconfig
  These pages, provided they are accessible via the Intranet or Internet, help users to quickly set up the mobile apps for PBX Call Assist 5 UCServer.
  Users are guided through the configuration.
- The Portal
  http://localhost:7224/apps/contactportal/
  Users can be contacted from web pages via the Portal and the associated multi-media business card. For more information, see below.



To be able to use the Portal and the business card productively, the WebService requires Internet access. This ensures that the version adapted to the current browser versions is always available.

- Administration interface
  http://localhost:7224/ws/admin/login
  The local WebService has an administration interface that enables users to see the current connection status to UCServer, the clients currently connected via the interface and the current WebService logfile.

Multimedia Business Card
Multimedia Business Card (referred to in the software as simply ‘business card’) allows any PBX Call Assist 5 UCServer user to be available over Internet-based real time communication. To this end, every approved user receives his personal contact page with presence and contact information as well as the possibility for direct, simple contact via links. The link to this page can be added easily in the Email footer or printed profile page, enabling a rapid contact via the intranet or Internet.

An approved user's business card can be accessed via a link starting with
`http://localhost:7224/apps/contactportal/` and attached identity of the desired user.

Example:
`http://localhost:7224/apps/contactportal/frau.mustermann@domain.de`

Users can be specifically enabled in the user settings under "Services" with "Business card visible for anonymous users". In addition, all users of a Portal group are approved for the business card.



It is recommended that users are enabled specifically on an individual or group basis, since with global settings potential user contact details may become visible that should not be public.

All users can be activated with the global setting "Business card visible to anonymous users".

If a user is approved for the business card, new buttons are displayed to him in PBX Call Assist 5 above the search input line that he can use to control his availability in the web application.

The button "Start post-processing" allows users to set "Occupied - In post-processing" in order to indicate to other users of the web application the non-availability by means of the presence state "Occupied". Pressing the button again resets the state.

The additional keys map all the Portal groups configured by the administrator, including the business card, to which the user can log on or off. If the key is activated, the user is "logged on" and his availability is displayed on the web pages. If the key is not activated, the user appears on the pages as "not available" and can only be reached via e-mail or a phone call.

Portal
All the users of the Portal Group are listed in Portal. The Portal enables visitors of the website to find the appropriate contact themselves and get in touch with them directly. Presence management automatically controls the availability of individual contacts.

As shipped, the user group named "Contactportal" is considered as the Portal group. The user group must be created manually. All members of the group will be listed in the Portal. In addition, the user group must be enabled for use in the Portal via the setting "Portal Group", which can be found in the "Services" group tab.

For further information, in particular regarding the definition of additional Portal groups, please refer to the online Help **(not available in the field test!)**.

Availability over the Internet
The web applications can be used automatically on the local server, but maximum benefit is achieved if the users, clients or partners also have access to these pages via the Internet.

You can make the UCServer available to PBX Call Assist 5 clients via UCConnect or provide own servers.
You can find instructions on how to make UCServer accessible from the Internet on our support pages.

12.8 STUN and TURN Server Settings

PBX Call Assist 5 UCServer make central configuration of STUN and TURN possible for PBX Call Assist 5 clients. The PBX Call Assist 5 client will require these settings if the audio or video chat features should be used. A STUN and TURN server will always be required if at least one client is outside of the local network. In particular, this will affect the apps and browser applications. STUN and TURN servers are typically found on the Internet and are not components of PBX Call Assist 5 UCServer for that reason. The settings that describe how STUN and TURN servers located on the Internet can be accessed can be made on PBX Call Assist 5 UCServer's configuration page (under services -> STUN & TURN). The configuration parameters will be provided by the operators of the STUN and TURN servers.
The STUN and TURN servers may be located on identical systems or use the same URLs or IP addresses, however, they may also be located on different systems or use different URLs or IP addresses (and ports).

PBX Call Assist 5 UCServer supports multiple options for using STUN and TURN servers.

- **Using an internal server**
  Customer internal STUN and TURN server(s) may be used. To do so, configure the following parameters:
  - **STUN URI**
    Enter the STUN server's name here. The default STUN port is 3478. Valid STUN URI's include:
    - stun:my.server.com
    - stun:stun.l.google.com:19302
  - **TURN URI**
    Enter one or more URIs for the internal server(s) here. The standard TURN port is 3478. Valid TURN URIs include:
    - turn:my.server.com
    - turn:my.server.com:3478
    - turn:my.server.com:3478?transport=udp
    - turn:my.server.com:443?transport=tcp
  - **TURN Authentication**
    Access to a TURN server always requires authentication to prevent unauthorized usage. Since the media channels passed through as well as computer performance will use Internet bandwidth for the TURN service, the TURN service must be protected against uncontrolled, mass usage. The following authentication methods are supported.
    - **Authentication using User Name & Password**
      Enter the user name and password. Note: if client applications are used in the browser through the Internet, the access data will not be protected against access.
    - **Shared Secret (TURN REST API)**
      The Shared Secret is a key that is known to both the TURN server as well as UCServer. UCServer will generate valid access data every 24 hours based on the shared secret, which will be transferred to the clients.

  - **Use UCConnect**
    Log into UCConnect in order to use STUN and TURN servers automatically.
- **Use External Provider**
  There are several providers who operate STUN and TURN servers. To do so, log into a provider. Enter the necessary access data received from the provider on the Configure Provider dialog. PBX Call Assist 5 UCServer will periodically retrieve new access data for the TURN server from the respective provider and make it available to the clients. The access data will typically be valid for 24 hours.

STUN / TURN diagnostics
The actual settings described above can be verified by pressing the "Start diagnostics" button. The test result appears in the text field near the button, for example "STUN test passed, TURN test passed".
Once a log file has been created and PBX Call Assist 5 UCServer has access to the file, the Open Log File button can be clicked. The diagnostics will be created with the help of a utility, ICE-Test2.exe. The Execute Diagnostics button will remain gray if the utility is not available to the PBX Call Assist 5 UCServer Administration program.

What is a STUN server?
STUN (Session Traversal Utilities for NAT) is a client-server protocol which returns the public IP address to the client. It allows a client to discover its public IP address at the internet if the client is located in a LAN behind a NAT. Additional information is provided enabling the client to make conclusions about the type of NAT. Thus a STUN server shall not be accessible via internal IP addresses of a LAN, for example if the STUN server resides in the DMZ of an enterprise network. The STUN server need to be addressed by the client always by using IP addresses of the public address space.

What is a TURN server?
TURN (Traversal Using Relays around NAT) servers are used when direct peer-to-peer communication is disabled by a firewall. A TURN server relayes media streams between the endpoinds avoiding such direct peer-to-peer communication.
Such requirements are frequently required in particular for connections from a mobile network, meaning that a mobile client on a cell phone will attempt to create audio-video communication through the Internet. Similarly, especially restrictive NAT devices (the transition point between an internal LAN and the external Internet) may require the use of a TURN server.

What is a NAT device?
NAT stands for "Network Address Translation" and translates the "internal" IP addresses (and ports) to the external IP addresses (and ports). A NAT device is for example a router connecting a LAN with the public internet.

What is a symmetric NAT?
A remote station at the internet may reply data back to a client only if the remote station replies from the same system (using the same IP address and port number). If the remote station answers from a different location it fails because the NAT device opens a new NAT table entry. Using symmetric NAT devices no VoIP connection can be established without using a TURN server.

When do I need STUN or TURN servers?
All Audio/VideoChat clients are at the same local network (LAN): there is no need for configuring STUN and TURN servers.
The Audio/VideoChat clients are using also the internet to communicate to each other. No symmteric NAT is used: a STUN server configuration is required, configuring a TURN server is optional.
The audio/video chat clients must also communicate with each other through the Internet. The environment is unknown. Someone is using a symmetric NAT or cell phone to communicate through the public Internet. STUN and TURN server settings will be required.

Are there any public STUN and TURN servers?
There are several public STUN servers, such as stun:stun.l.google.com:19302.

There are no publicly available TURN servers. There is a TURN server provider from whom this service can be rented. UCConnect can also make STUN and TURN servers available.

Which software should I use to run my own STUN and TURN server(s)?
The coturn software supports all of the required features required to run WebRTC applications. See https://github.com/coturn/coturn also.

12.9 Push notifications

Push notifications can be used by the mobile apps and web applications. The list displays clients that have registered for Push notifications.

The registration is deleted when the user logs off from the application. If an application is not used for a period of 30 days, it is automatically logged off. To log off from an application manually, highlight the corresponding line and press "Delete".

Mobile apps that are logged on via UCConnect require a Mobility Services license. This is displayed in the list.

A valid service contract is required to use the mobile apps.

Status Online means that the user is currently connected to the application. For example, this is the case if the Mobile App is currently open.

13 Integration in Microsoft® Teams

The integration of PBX Call Assist 5 UCServer in Microsoft® Teams enables mutual reconciliation of presence and call status. For example, if a call is received via PBX Call Assist 5 UCServer during a meeting in Microsoft® Teams, it is rejected - depending on the setting.
Conversely, a call in PBX Call Assist 5 UCServer also influences the presence status and activity in Microsoft® Teams.

Information about the function and startup can be found here: https://support.estos.de/procall-enterprise/procall-integration-in-microsoft-teams

14 ChatGPT-Integration

As version 8.3.0, PBX Call Assist 5 supports the integration of ChatGPT via the interface of the providers OpenAI and Microsoft® with Azure OpenAI Service.

By setting up the chat application centrally on the UCServer users are offered a seamless and smooth process as they do not have to worry about technical aspects such as setup, costs or API keys.
This enables companies to provide this service to their users without any additional effort or technical knowledge.

The central setup on the UCServer requires the so-called API key, for which an account must be set up with the AI platforms (third-party providers). The terms and conditions of the third-party provider apply to the account.

Informationen zur Funktion und Inbetriebnahme finden Sie in unserem Support-Portal:
https://support.estos.de/procall-enterprise/chat-in-procall-8-enterprise/chatgpt-integration-in-procall

15 Federation

PBX Call Assist 5 UCServer supports using the SIP, SIMPLE AND XMPP protocols for federations. A detailed description can be found under Introduction to Federations.

Der vom PBX Call Assist 5 UCServer unterstützte Funktionsumfang ist abhängig von der Art der Federation. Generell wird der Austausch von Präsenzinformationen und Chatnachrichten unterstützt.
Wird der UCServer (mit aktiviertem SIP-Server) über eine statische Route direkt mit einem anderen PBX Call Assist 5 UCServer verbunden, werden auch Audio- und Video-Chat sowie die Bildschirfreigebe unterstützt.

The following pages will describe how to setup the SIP and XMPP services for PBX Call Assist 5 UCServer.

- SIP Federation
- SIP Server
- SIP Static Routing
- XMPP Federation
- Domains authorisation
- Block domain
- Diagnostics

15.1 SIP Federation

SIP federations allow internal users to send chats and view the presence information of external users.
A detailed description of the federation can be found on the page Introduction to federation.

15.1.1.1 Use federation

To activate federation, different configuration possibilities can be selected.

- **Direct (Open Federation)**
  The connection with servers in other presence domains is carried out **directly** from this server. The connections to other presence domains are established via standard SIP protocols. The servers are automatically located via special DNS service location records, so no other configuration is necessary.
- **Message Window**
  This window shows status reports and additional information about your selected configuration. Every entry has a time stamp - format: (date time) at the beginning of a line. The time stamp informs on when the notification has arrived. Only the last 30 entries are shown.

15.1.1.2 Configuration of open federation

For using open federation it is required to have a valid server certificate, a public DNS-SRV record and a network interface for incoming connections. Please find more information regarding certificates at server certificates. Further information regarding DNS-SRV records can be found at 'Setting up DNS Service Resource Records for federation'.

- **Certificate**
  For using open federation a valid server certificate is required. The certificate must be signed by a Certificate Authority (CA) and it need to be installed on the system. Please press the button *Certificate* to open the dialog. Select the signed certificate and press the button 'OK'.
- **A DNS-SRV record of a public DNS corrosponding with the certificate**
  Depending on the selected server certificate an IP address and port number is detected by a DNS request. If nothing is displayed after selecting the certificate the DNS-SRV record may not match the certificate or it may not be present.

    - **DNS host IP**
      Returned IP address of the DNS request using a Certificate Subject Name.
    - **DNS port**
      Returned port number of the DNS request using a Certificate Subject Name.
- **Network interface for incoming connections**
  Please select a network interface to be used with incoming connections of open federation. By finishing the configuration the network interface is added automatically to the network interfaces for incoming connections.
    - **Bind to IP address**
      Please select the network interface to be used for open federation.
    - **Port**
      Please enter the port number to be used for open federation.

To accept the new settings please press the button "OK". Press the button "Cancel" to discard the settings.

15.2 SIP Server

Configuration of network interfaces to be used for incoming connections.

- **Use SIP Server**
  Activates or deactivates the SIP services. The SIP server must have been activated and the corresponding network interfaces configured in order to be able to use the SIP Proxy, Open Federation and Static routing federation services. If you deactivate the SIP server, you cannot carry out other settings to SIP based services and network interfaces.
- **Certificate**
  To use the secured network protocols TLS and MTLS, you need a Server certificate. This has to be signed by a certification authority. Click on the button "Certificate..." to open the window for the certificate selection. Select the suitable certificate and afterwards confirm the information with "OK". Information about the selected server certificate is also shown.
- **Use SIP registrar**
  Activates, or deactivates the usage of the SIP Registrar service. SIP Registrar allows SIP user agents to be registered. SIP messages will only be accepted from authorized user agents when the SIP Registrar has been activated. This service can only be activated if the SIP Server has been activated.
- **Use other public address**
  Activates or deactivates the use of the public address. If it's necessary that your server is connected with the internet via NAT-Routing (Network address translation) then activate this function.
    - **Port / IP**
      Shows the port number and the IP address which should be used as a public address. The port number can range from 0 to 65535. Certain applications use port numbers which are specially assigned and are generally known. They usually lie between 0 and 1023. Therefore, it is best to select a port number between 1024 and 65535. If you enter no port number or if you do not know the port number of your access server, try to enter the standard port number of 5060. If you have activated the Use Public Address option, you should also enter the appropriate IP address. You can enter this value manually. If you do not know it then click the Determine IP button. The appropriate IP address will then be determined and the entry will be automatically set.
    - **Detect IP**
      Click this button if the system should automatically determine the IP address when the Use Public Address feature has been enabled.

15.3 Network interfaces

15.3.1.1 List of the network interfaces

Lists the network interfaces which are used for incoming connections. Every network interface has certain properties and additional information which is summarised in the index. The following properties of a network interface are displayed:

- **Activate**
  Activates or deactivates the network interface. You can carry out this setting directly. Click on the checkbox to activate the network interface. Click again on the checkbox to deactivate the network interface. If the network interface is deactivated, the checkbox is empty.
- **IP**
  Displays the network interface's IP address. Together with the specified port number, it will uniquely identify the interface. Select the line and click the Properties... button to change the network interface's IP address.
- **Port**
  Displays the network interface's port number. The port number and the IP address will uniquely identify the interface. Select the line and click the Properties... button to change the network interface's port number.
- **Log**
  Displays the transport protocol of the network interface. Different protocols for network interfaces can be selected.
  - UDP (User Datagram Protokoll)
  - TCP (Transmission Control Protocol)
  - TLS (Transport Layer Security)
  - MTLS (Mutual Transport Layer Security)

  Select the line and click the Properties... button to change the protocol type for the network interface. You will also need a server certificate for the use of secured protocol over secured network interfaces. Additional information regarding certificate specifications can be found under Server Certificates.

- **Status**
  Displays the status of the network interface. You are not able to edit this design.

15.3.1.2 Configuration of network interfaces

You can configure the list of your network interfaces. Click the Add... button to add additional network interfaces to the list. Click the Delete button to remove one or more network interfaces from your list. Click the Properties... button to display the network interface's properties and adjust them, if necessary.

- **Add...**
  Click this button to add an additional network interface to the list. A new window will be opened, where the network interface's Properties can be set. Additional information about the network interface's properties and how you can determine them can be found in the Network Interface List section.
- **Remove**
  Click on this button to remove network interfaces from your list. You can only do this if at least one network interface was marked on the list. Afterwards, you are asked to confirm the removal of the marked network interfaces. Click on the button "OK" to confirm the removal. Click on the button "Cancel" to stop this action.
- **Properties...**
  Click on this button to display the properties and details of a network interface. You must select only one network interface on the list. You can also adjust the network interface's properties. Additional

information about the network interface's properties and how they can be adjusted can be found in the Network Interface List section.

15.4 SIP Static Routing

Please gather and configure here your list of static routing entries used for outgoing connections. An introduction describing the creation of static routing entries for Microsoft® Lync® Server can be found at Creating a Static Route between PBX Call Assist 5 UCServer and Microsoft® Lync® Server using TLS/MTLS.

15.4.1.1 List of all static routes

- **Use static routes**
  Activate or deactivate the functionality of the static routes included in your list here. If you deactivate "use static routes", all your static routes are deactivated and you can't carry out any adaptations in your existing configuration.
- **Partner Domain configuration**
  Shows the list of the registered and configured static routes. Every line in the list represents a static route with individual settings. The following properties of a static route are displayed.
  - **Activate**
    Activates, or deactivates, the static routing entry. You can make this setting directly. Click the checkbox to enable or disable the static routing entry. Additional information regarding this can be found under Static Routing Entry Properties.
  - **Trustworthy**
    Indicates if the static routing entry has been categorized as trustworthy. You can make this setting directly. Click the checkbox to enable or disable its function. Additional information can be found under Static Routing Entry Properties.
  - **Domain**
    Displays the domain name that should be used for the static routing entry. The domain name establishes the context for the hierarchical system and must be unique in your displayed list. Additional information can be found under Static Routing Properties.
  - **Access server**
    Displays the server's IP address used for accessing the domain. This value may also be a symbolic name, which will be converted into an IP address as part of operations. Additional information can be found under Static Routing Properties.
  - **Port**
    Displays the port used by the selected access server. Values between 0 and 65535 may be entered for the port number. Many SIP servers use Port 5060 over TCP or 5061 over TLS. Additional information can be found under Static Routing Properties.
  - **Log**
    Displays the transport protocol for the selected access server. Various protocols are available for static routing. Information regarding transport protocol settings and additional information can be found under Static Routing Properties.
  - **Linked on**
    Displays the selected IP address, if the system has been bound to an IP address. Additional information can be found under Static Routing Properties.

15.4.1.2 Configuring static routes

You can modify your static routing list. Click the Add... button to add another entry to the static routing list. Click the Delete button to remove one or more static routing entries from the list. Click the Properties... button to display the static routing properties and change them, if necessary.

- **Add...**
  Click this button to add additional static routing entries to the list. A new window will be displayed, from which you will be able to change the property settings for the new static routing entry.

Afterwards, click Ok to add the new entry to the list. Click Cancel to reject the new static routing entry.

- **Remove**
  Click on this button to remove static routes from your list. You are only able to carry out the removal, if at least one static route is marked in the list. Afterwards you are asked to confirm the removal. Click on the button "OK" to confirm. Click on the button "Cancel" to abort.
- **Properties...**
  Click on this button to get the properties and details of a static route displayed in another window. You need to have marked exactly one static route on the list to do so.

15.4.1.3 Adapt the properties of the static routes

- **Domain name**
  Displays the domain name that should be used for the static routing entry. The domain name establishes the context for the hierarchical system and must be unique in your displayed list.
- **Access server**
  Shows the IP address of the server under which the domain is accessible. It can also be a symbolic name which was converted into an IP address.
- **Port**
  Enter the port number for the selected access server. Values between 0 and 65535 may be entered for the port number. Many SIP servers use Port 5060 over TCP or 5061 over TLS. The port number and the transport protocol must correspond to a network interface for incoming connections from the access server.
- **Bind to IP address**
  Select the IP address from the list of available IP addresses, which you would like to use for the static routing entry. You may only select from the entries in the list. The selection options will depend on your system settings.
- **Transport Protocol**
  Choose the transport protocol for the access server. The transport protocol and port number must correspond to a network interface for incoming connections from the access server. The following transport protocols are available for static routing:

  - UDP (User Datagram Protocol)
  - TCP (Transmission Control Protocol)
  - TLS (Transport Layer Security)
  - MTLS (Mutual Transport Layer Security)
  For using the MTLS protocol, you will need a server certificate issued for your system. The server certificate must have been issued by a reliable certification authority. You can select an appropriate certificate from Network Settings.

  ⚠ Please note that UDP and TCP are unencrypted protocols, which have not been secured against eavesdropping. Using these protocols only in a local area network is recommended. The UDP protocol is not recommended because of the maximum packet size of 65,535 bytes.

- **Activate static route**
  Activates, or deactivates, static routing. Click the checkbox to activate static routing. In this case, the checkbox will be checked. Click on the checkbox again to deactivate static routing. In that case, the checkbox will not be checked. The setting of this property will correspond to the Enabled column in the static routing list.
- **Classify route as trustworthy**
  Mark this checkbox if you classify the static route as trustworthy. Click on the checkbox to activate the functionality. The checkbox is then marked. Click on the checkbox again to deactivate the feature. In that case, the checkbox will not be checked. A static route entry marked as unreliable will

require the use of the SIP registrar for the authorization of incoming SIP messages. Static routing entries that use the MTLS protocol for transport will automatically be considered reliable.

For reasons of security, using this option only for static routing entries in a LAN is recommended.

- **Network interface for incoming connections**
  Select a network interface for incoming server connections. The network interface is added to the list of Network interfaces for incoming connections by finishing the configuration.
  - **IP interface**
    Select the network interface to be used with connections to the UCServer.
  - **Port**
    Please specify the port number to be used with connections to the UCServer.

To confirm your settings of a static route, click on the button "OK". Click on the button "Cancel" to abort. Should the system reject the information of a static route, first check if the information is complete and there is no typing mistake. Then change the properties of the static route and try again.

15.5 XMPP Federation

XMPP Federation enables users exchanging chat messages and presence information with external users accross enterprise network boundaries.
A detailed description of federations can be found on the Introduction to Federations page. Step-by-step instructions for creating an XMPP federation can be found on the Creating an XMPP Federation page.

15.5.1.1 Using XMPP Federation

Check the Use XMPP Federation checkbox to activate XMPP Federation.

In order to enable the PBX Call Assist 5 UCServer to contact a domain through XMPP, a corresponding domain authorization with a public business, team member or personal authorization level is required. The protocol type must be set to "XMPP". Domain authorizations for popular XMPP domains (such as gmail.com) were configured as part of the PBX Call Assist 5 UCServer installation process.

Determine how the connection to other servers should be created:

- **Direct**

  The connection to servers in other XMPP presence domains should be **direct** from this server. An XMPP server-to-server interface will be opened to allow other servers to connect to PBX Call Assist 5 UCServer:

  - **TCP Port**
    Enter the TCP port for the XMPP server-to-server interface. The default port, 5269, can be set by clicking the Default button.
  - **Bind to IP address**
    Select an IP address for your system, through which the XMPP server-to-server interface should connect.

Make sure that this interface can be reached through the public Internet and that your presence domain can be resolved to an IP address by DNS. If you configure a different port than the default, a DNS SRV Record (_xmpp-server._tcp.*domain*) can inform other systems about this. Ideally, such a DNS SRV Record should also exist, when the default port is used. However, this DNS SRV Record is not mandatory, since other systems can also generally connect to your PBX Call Assist 5 UCServer using a DNS A Record and the default port, 5269.

The certificate used for server-to-server connections as well as other options for encrypting the connection can be set by means of the "Advanced..." button. However, only the connection to the XMPP server in those domains, which encrypt messages and forward them to remote users, will be encrypted. *End-to-end* encryption is not used.

A server certificate will be required for using the secured TLS and MTLS network protocols. The certificate must have been signed by a certification authority. Click the Certificate button to open the window for selecting a certificate. Select the appropriate certificate and confirm it by clicking the OK button. Information about the selected server certificate will also be displayed. If you do not specify a certificate, but a SIP server certificate exists, an attempt will be made to use that certificate.

The settings for TLS encryption may either be set globally for all domains or locally for each individual domain. The global settings will apply for all domains, when other settings have not been made. In order of accessibility and trustworthiness, the following categories can be assigned:

  - **No encryption**
    TLS encryption will not be used for connections with remote domains. This setting should only be selected when the *TLS Encryption Optional* setting will not work.
  - **TLS encryption optional**
    An attempt will be made to use TLS encryption with connections to remote domains, if that domain makes such possible and a local certificate is available. If the other domain does not offer TLS support (which is the case with GoogleTalk, for example) then message exchanges will not be encrypted. Otherwise, the attempt will be made to ensure the highest possible level of reliability. This settings will almost always work, but does not guarantee the reliability of the messages.
  - **TLS encryption required, ignore certificate errors**
    The attempt will be made to use TLS encryption with connections to remote domains. If a local certificate is not available or the other domain does not support TLS, the connection will fail. If certificate errors occur (for example, because the other domain's certificate has expired or has not been signed by a reliable certification authority), they will be ignored. Connections will offer reliability, however not strong authentication in the other domain.
  - **TLS encryption with valid certificate**
    The attempt will be made to use TLS encryption with the connections to remote domains. If a local certificate is not available, the other domain does not support TLS or the other domain's certificate is either invalid or not signed by a reliable certification authority then the connection will fail. This type of encryption is recommeneded, does not however always work (for example, GoogleTalk does not support TLS encryption, many server certificates have expired or they have only been signed by the server itself).

- **XMPP Proxy**

The connection to servers in other XMPP presence domains will be made through XMPP Proxy.

  - **Proxy TCP Port**
    Enter the TCP port to which PBX Call Assist 5 UCServer will connect the XMPP Proxy. The port can be set to the default port, 5275, for the proxy connection by clicking the Default button.

- **Proxy Address**
  Enter the address for XMPP Proxy.
- **Password**
  Specify a password, which PBX Call Assist 5 UCServer should use for logging onto XMPP Proxy.

15.6 Domains authorization

Define which presence and contact information is transferred from UCServer users to external federation contacts by using authorization levels.
The authorization levels can be determined either for every domain explicitly or for all domains globally. The global setting is valid for all domains for which no explicit authorization level was defined.

- **Maximum global authorization level**
  This option determines the set authorization for all domains without an extra authorization level in the settings. This setting is valid for all domains not explicitly named in the list. The following levels are possible (in order of restriction).
  - Blocked
  - Open
  - Business
  - Team member
  - Personal

  More details can be found under Authorizations.

- **Explicit authorization levels**
  List of domains with explicit authorization levels. It concerns the listing of explicitly named domains with an appropriate authorization level. For all other domains which are not named in this list, the globally set authorization level applies.
  If the placeholder *. is entered in front of a domain, then the domain (including all subdomains) receives the explicit authorization.

  More details can be found under Authorizations.

- **Log**
  - SIP SIMPLE: The connection to the domain will be created through the SIP SIMPLE protocol.
  - XMPP: The connection to the domain will be created through the XMPP protocol.

⚠	If no configuration exist for the domain the protocol SIP SIMPLE is used.

15.7 Block domain

Define which domains should be explicitly excluded from federation here.

- **Blocked domains**
  List of the domains to be blocked for communication. No explicit authorizations are valid for blocked domains. Explicit authorizations are done in the Domain authorizations settings. If a domain has the placeholder *. in front, the domain is blocked (including all subdomains).

15.8 Diagnostics

If you cannot establish a successful federation to other servers, the reason can be a misconfiguration or physical connecting problems. According to the configuration, different diagnostics options are available.

Diagnostics available

- **Network interfaces**
  If the SIP server is used, then it can be checked whether the configured network interfaces were correctly opened.
- **Open Federation**
  It is tested whether the requirments for Open Federation are fulfilled and the necessary DNS entries exist.
- **SIP Proxy**
  Problems with the SIP proxy server can be detected with this test. If the connection to the SIP proxy server could be established and login was successful will be tested. Login errors will be displayed as SIP response codes.
- **Partner Domain configuration**
  It trys to estabish a network connection with the access server. Please note that only an outgoing connection is established. Please check the conncetion for a complete test of a static route on the SIP level.
- **XMPP**
  The prerequisites for XMPP federation will be tested for fulfillment.
- **Connection test**
  Here it can be tested if a SIP connection can be established between a local user (sender) and a user on another server (receiver). The sender subscribes the presence of the receiver for a short time. Connecting test errors at SIP level are shown as SIP responses code.

⚠	Please note that during the brief subscribtion of the presence for the connecting test under circumstances an authorization inquiry (receiver) can take place.

Diagnostics results

Diagnostic results are divided into three categories:

✔	The test was completed successfully.
ⓘ	The lines show the information that was determined by the test steps and should be rechecked. Discrepancies can often be detected here. Example: The name (Host) is determined by an IP address. Should this name contain no named parts of the desired device (that you would like to connect to), you should recheck the IP address. An incorrect number sequence is often the cause.
✖	An expected prerequisite was not found or the test was stopped because of an error.

Load

Old test results can be restored with this button. This functionality is used primarily by our support to restore your saved reports and to be able to give you the best advice.

Save

Save the results in a file if you cannot solve the problem and would like to have the help of our supports. Your personal consultant needs this file for an ideal consultation.

16 Databases

The various pages for connecting the contact databases to PBX Call Assist 5 UCServer are described in this section.

- MetaDirectory
- Google Integration

16.1 MetaDirectory

The estos MetaDirectory is a meta-directory which permits central collection of employee and customer information. Organizations can thus merge their existing, distributed data into a global information service based on the Lightweight Directory Access Protocol (LDAP). The automatic synchronization caused by the replication process merges existing employee and customer data from different information sources. The advantage of the meta-directory over databases is the very high access speed and the high availability even during the synchronisation phase.

The special feature in connection with the PBX Call Assist 5 UCServer is that the MetaDirectory standardizes the phone numbers during replication into (Super-canonical phone number). This allows an extremely quick search. If a MetaDirectory is entered here, the phone numbers of callers are transfered by the PBX Call Assist 5 UCServer in names and are then available as e-mails via "unanswered phone calls".

If you connect estos MetaDirectory to PBX Call Assist 5 UCServer you can decide whether just the server itself or also the clients connected are allowed to use the contact data. You can also separately configure access for phone books and further contact data here.

If you are using a estos MetaDirectory with user management (from estos MetaDirectory version 3.5), you will need a user ID with password which is required for server-side search (esp. reverse call lookup). Please note that the specified user need full access to all data records at the Base DN in order to search on behalf of all users. You can specify here the user name and the password for the login with the MetaDirectory administrator program. A server side search is always executed in the context of the related user. The MetaDirectory returns contact data only according to the related user rights, for example by searching contacts during an incoming call. The PBX Call Assist 5 logs in with the PBX Call Assist 5 client related credetials. The login at the estos MetaDirectory is not done with administrative rights.



For better scalability, telephone books in PBX Call Assist 5 UCServer are linked via estos MetaDirectory. Use of the telephone books does not require an additional license for the estos MetaDirectory.

16.2 Google integration

PBX Call Assist 5 UCServer can permit clients to access contacts and appointments for your account using the Google API. To do this, PBX Call Assist 5 UCServer must be authenticated with Google and allow PBX Call Assist 5 UCServer users access to their data.
An OAuth2 ClientID must be generated for authentication with Google, which is done through the Google Developer Console.
The following settings are important:

Type of application:	Miscellaneous

Activated APIs:	Google Calendar API Contacts API

If a ClientID has been generated, download the associated JSON file and copy its contents to the entry provided. PBX Call Assist 5 UCServer will extract the necessary data from it and send it to the clients as needed. The clients will then be requested to permit access to your account when the program will next be started. Afterwards, contacts and appointments will be available in PBX Call Assist 5.

17 Server status

You will find information about the current status of the PBX Call Assist 5 UCServer on the following pages.

- Status monitor
- Server events

17.1 Status monitor

The status monitor provides an overview of the status of the available services, as well as licenses in use and registered clients

Service:	Description:
Licenses	
PBX Call Assist 5 User	Displays the number of currently ***logged in*** PBX Call Assist 5 users and the number of available licenses.
Windows® PBX Call Assist 5	Shows the number of currently logged in PBX Call Assist 5 clients for Windows®, the number of available licenses and the port opened by UCServer for client login.
Lines	Number of lines activated and available/usable in UCServer.
PBX Call Assist 5 Meetings User	Displays the number of users ***activated*** for PBX Call Assist 5 meetings and the number of available licenses.
Mobility Services Users	Number of PBX Call Assist 5 clients registered via estos UCConnect. (Mobile App, PBX Call Assist 5 for Windows®, PBX Call Assist 5 APP)
Active Calls	
TAPI/Active calls	Number of currently conducted telephone conversations.
Active audio/video chats	Number of currently running audio/video and softphone calls.
Calls on an outside line	Number of currently conducted telephone conversations on an outside line.
Interfaces	
Remote Tapi Clients (Standard)	This is the "extended remote TAPI driver" on the client (TapiServer Standard Tapi driver). The active connections and the port defined for the connection are displayed.

Admin Clients	Displays the number of currently logged in UCServer administrative clients and the open port from UCServer for the connections to UCServer administrative clients.
Push-Notifications	Status whether the "Push Service" is activated.
SIP Proxy	Status of the connection to a SIP Proxy.
SIP Server	Status of the open SIP ports.
XMPP Proxy	Status of the connection to a XMPP Proxy.
XMPP Server2Server	Status of the XMPP Server2Server Port.
Update server	Status and port of the update server.
PBX Call Assist 5 Web Server	Displays the status of the locally installed PBX Call Assist 5 Web Server for the unencrypted network interface.
PBX Call Assist 5 Web Server SSL	Displays the status of the locally installed PBX Call Assist 5 Web Server for the encrypted network interface.
PBX Call Assist 5 Media Server	Displays the status of the locally installed PBX Call Assist 5 Media Server. This service must be connected for softphone calls.
Active Directory® objects	If the entry appears, adjust the ADMaxRead value in the registry.

17.2 Server events

The event protocol of the server is displayed here. How to define which events are protocolled can be found on the page Events.

Symbols used

	Error
	Warning
	Information
	Debug information

The events can be searched and narrowed down with the filter toolbar.

18 Tools menu

The **Extras** menu offers you certain features which assist you with administration.

Reboot server
You can also reboot the server remotely. The connection must be subsequently restored. Depending on the number of lines it can take several minutes before the server is available again.

Network interfaces
This menu item opens a dialog to change the configuration of the settings of the server Network interfaces. Certificates for a secure communication can be configured under Certificate.

Core services
For specific scenarios some core services can be restricted.

Synchronize contact data
If the ActiveDirectory user administration is used, the contact data buffer can be updated here when you do not want to wait for the automatic cycle.

Change administrator password
You can change the administrator login for the server here. A connection to the server is required.

Select language
You can select the language in which you wish to run the program. More than one language DLL must be present in the installation folder for this. You must restart the program if you have changed the language.

18.1 Network interfaces

The connection between the software on the workstations and PBX Call Assist 5 UCServer is made via *network interfaces*. The PBX Call Assist 5 UCServer provides several interface types on the server computer for this. Each network interface is bound to a combination of IP address and port number, shown in the field "Bound to IP" and "Port". If network interfaces are used encrypted the configured certificate is listed. The configuration is shown at the fields "Encryption" and "Certificate". A coloured symbol with tooltip help indicates the actual state of the related network interface.

Default settings

The following default settings are used for the network interface types:

Type	Bound to IP	Port	Encryption	Certificate
Administration	All available	7221	unencrypted	
Remote TSP (TAPI)	All available	7220	unencrypted	
UC Client	All available	7222	unencrypted	

By default, ports are bound to all IP interfaces on the computer. If necessary, they can be limited to be used with specific IP addresses only.

Changing the default port configuration is not recommended except the setting conflics with other software running on the system.
If a port conflict accurs an error event appears in the event log of the PBX Call Assist 5 UCServer.

With the button **Standard** settings can be reset to the default values.

The **Add** button allows you to set up a new network connection.

Using the button **Remove** a network interface can be deleted.

The **Properties** button allows you to change a network connection.

18.2 Certificate

To increase security, the data traffic between PBX Call Assist 5 UCServer and PBX Call Assist 5 can be encrypted with TLS/SSL.
For the TLS/SSL encrypting of data a valid certificate has to exist and be selected, which was issued for the FQDN (Full Qualified computer name, e.g. "server.domain.com") of the computer on which PBX Call Assist 5 UCServer runs.

A short tutorial about certificates, how to get them and how to setup them can be found in the chapter Server certificate.
A detailed description can also be found in the online help *Microsoft® Management Console* Snap-Ins for certificates "certmgr.msc" .

Security level for connections with PBX Call Assist 5

- **Allow secure data transmission using TLS**
  If the TLS/SSL encrypting is activated, encrypted and unencrypted programmes in the PBX Call Assist 5 UCServer can be combined.
  PBX Call Assist 5 recognizes this possibility and is able to use it with the next login. Because of this, only clients who have the entire server name in their connection settings (as named in the certificate), e.g. "servername.domain.com" can login.
  Changes to the TLS/SSL settings will be taken over only for new incoming connections. Existing Client connections are not influenced by the new settings.
- **Reject unsecured connections**
  If the TLS/SSL encrypting is activated, insecure connections to the PBX Call Assist 5 UCServer can be rejected.

Certificate for SSL/TLS communication with PBX Call Assist 5
Here the certificate which was selected for the secured data transfer is displayed.

- **Delete certificate**
  Removes the certificate from the configuration. If no certificate is selected, the PBX Call Assist 5 is not able to connect with the UCServer anymore.
- **Choose certificate...**
  Opens up a dialog to display the certificates available on the computer and to select one of them for the data transfer.

19 Installation of Clients

After the installation of the PBX Call Assist 5 UCServer, the PBX Call Assist 5 client software can be installed on the PCs.

Clients can be installed centrally or remotely and updated.
In addition to an already available software administration, the PBX Call Assist 5 UCServer offers its own technology for the automatic and central installation of workstations. Furthermore, an automatic update service is available which supplies all workstations from the PBX Call Assist 5 UCServer with the latest software.
It is possible to automatically install the network workstations with the help of group guidelines.
Wizards ensure an easy installation for remote installation and initial configuration for the workstation.
Find out more on the following pages:

- Installation at the workplace
- Installation using group policies
- MSI description
- Software distribution
- Update service
- Update server

19.1.1 Installation at the workplace

The *.msi* file is double-clicked for installation at the workstation. The Windows® Installer will then start and guide you through the installation process. Various information is displayed to the user and configuration options are offered:

Version Information
The exact version number is displayed on the homepage.

If PBX Call Assist 5 UCServer is installed on a 64-bit operating system, a message appears on this page that the 64-bit version of the TAPI driver must be installed if required.

19.1.2 License

The licence agreement has to be read and accepted by the user before the installation can be continued.

19.1.3 service features

If the UCServer is installed in the local network, it can be specified:

- **Install PBX Call Assist 5 Workstation**
  Select this option to completely install the PBX Call Assist 5 application.
- **Install only the advanced Remote TAPI driver**
  Select this option if you no longer require the PBX Call Assist 5 application. Only the advanced Remote TAPI driver will be installed. With the help of this driver it is possible for third-party software to use all of the functions via TAPI with the PBX Call Assist 5 UCServer.

Automatic Software Updates
You can specify whether the PBX Call Assist 5 should be kept up to date by the PBX Call Assist 5 UCServer. If this is the case, a local Windows® service is set up that is connected to the PBX Call Assist 5 UCServer and

downloads and installs the latest client software as required. However, this requires the software update service to be activated on the PBX Call Assist 5 UCServer.

Tapi driver installation options
If you install the complete PBX Call Assist 5 application, you can also select here which Tapi driver is be installed.

- **Do not install a Tapi driver**
  The latest version of PBX Call Assist 5 doesn't need a TAPI driver anymore for communication with the PBX Call Assist 5 UCServer. All functions are now available via direct communication. This simplifies the installation and servicing of the software, especially on terminal servers.
- **Install the Client TAPI driver**
  The client TAPI driver allows third parties the dialing via TAPI. The driver uses PBX Call Assist 5 as a connection with the PBX Call Assist 5 UCServer to carry out the dialing process. No additional TCP/IP connection is required and the installation and servicing of terminal servers are considerably easier than with TAPI.
- **Install the advanced Remote TAPI driver**(only for installations with PBX Call Assist 5 UCServer in the internal network)
  With the help of this driver, third party manufacturer's software can use all functions via TAPI and the PBX Call Assist 5 UCServer. Nevertheless, this driver needs another TSP/IP connection with the server.

19.1.4 Connection to the server

The server to which PBX Call Assist 5 UCServer is to connect is specified here.
The server name or its IP address is entered in the input field when using static configuration.
The server can be searched with **Search server...** in the local network and then selected. The displayed list contains the following information about the servers found:

Computer name	The computer name of the server
Version	Information about the installed version of the PBX Call Assist 5 UCServer
Method of localization	**"Broadcast"** means, that the server has answered a search inquiry on the local network. **"DNS Service Record"** means, that the server was setup in the DNS as a service provider.

If the DNS Service Location Record is used for the server configuration, no user input is required as the software automatically searches for and configures the PBX Call Assist 5 UCServer in this case.

After finally entering the destination folder for the program installation, the software is installed and the installation is completed.

Then start the basic configuration by activating the checkbox and selecting *Complete*.

19.2 Installation using group policies

You can install workstations automatically by using group policies. Proceed as follows:

1. Define which components are to be installed on the workstations. Use the Windows® Installer in administrator mode. In a command prompt start*msiexec /a* followed by the name of the installation package, e.g. *msiexe /a client.msi*. You have the option of specifying a directory where the prepared installation is to be stored. This must be a network-enabled directory. Then select which software components should be installed on the workstation and which computer is the PBX Call Assist 5 UCServer.
2. Run the *Active Directory® user and computer management* console to configure the domain users. Assemble the users (or computers) in groups to form organizational units. You can create group policies for each organizational unit which also automatically manage software installation.
   Open an organizational unit's properties dialog. Go to the group policies. Add a new group policy. Open the group policy by choosing Edit.
   Add new packages either in **Computer Configuration - Software Settings - Software Installation** or in **User Configuration - Software Settings - Software Installation**.
   Now choose the installation package previously prepared by the administrative installation. See also the relevant documentation about Windows Server®, Active Directory® and group policies.

19.3 MSI description

The workstation software for PBX Call Assist 5 is installed with a Microsoft® Installer package. This msi can be directly executed, started with msiexec or distributed via a group policy.

Languages
The msi user interface is available in one language. The software installed with msi is installed in all available languages.

Command line under Windows®
If you run setup with msiexec.exe and use the option /q (quiet without interface), it must be started from a shell with administrator rights (elevated).

Examples of the command line

- Default installation without user interface, hostname is ctiserver.mydomain.de
  msiexec.exe /i PBX Call Assist 5_de-DE.msi /q CTISERVER=ctiserver.mydomain.de

- Default installation with client TSP, basic user interface, hostname is ctiserver.mydomain.de
  msiexec.exe /i PBX Call Assist 5_de-DE.msi /qb CTISERVER=ctiserver.mydomain.de CLIENTTSP=edial

- Prepare administrative installation for distribution with group policy
  msiexec.exe /a PBX Call Assist 5_de-DE.msi

- De-installation
  msiexec.exe /x PBX Call Assist 5_de-DE.msi

Special MSI properties
The valid parameters for the installation are constantly being expanded. The currently available properties can be found on our website at:
https://help.estos.com/help/de-DE/procall/8.5/ucserver/dokumentation/tech/sc_installmsiproperties.htm

19.4 Software distribution

Software distribution

PBX Call Assist 5 UCServer provides central software distribution. With software distribution the administrator can install PBX Call Assist 5 on the workstations automatically and centrally from the server after the PBX Call Assist 5 UCServer has been successfully installed.

The installation requires administrator rights on the client. This can be either a local administrator account on the client computer or a domain administrator account.

For installation on workstations, you must add the appropriate computers to the computer list. Change to the **Computer** view in the PBX Call Assist 5 UCServer administrator. With **Add** you can enter a computer name manually or comfortably add the computers visible in the Windows® network.

Afterwards, select the computers on which the software should be installed or removed. Select in the menu **Install software**. A wizard guides you through this process.

- **Step 1 of 4 - Summary of the selected computers**
  You see here the list of computers on which you wish to distribute software.
- **Step 2 of 4 - Select action**
  You can choose between three installation or deinstallation options.
  - Remove installation service and software packages
    Use this option to install software on a computer. The computer must be running and accessible in the network.
    The installation service will be installed by this process. An administrator account will be necessary on the target computer to be able to perform this step successfully.
  - Manage Software Package
    Use this option to install or remove software packages on this computer. The installation service must have already been installed on the computer.
    Note: Modifying functional scope of a software package only possible through de-installation and subsequent re-installation.
  - Remove installation service and software packages
    Use this option to remove all software packages and the installation service from a computer.
- **Step 3 of 4 - Specify user account for access**
  If you install the installation service you must now specify an administrator account with which you can access the computers.
- **Step 4 of 4 - Select software package**
  Now you must specify which software packages you wish to install on or remove from the target computers. You can make further installation settings via the **Details** button.
- When you have finished with the wizard, PBX Call Assist 5 UCServer performs the appropriate actions automatically. With an installation, the client must now be available. With a configuration change or a deinstallation, the server remembers this until the next time the client logs in.

	Remote installation on Windows® 7 Starter/Home Basic/Premium or Windows® 8 Standard-Edition is not possible as the necessry administrator rights are not available on these systems.
	The TAPI driver may be changed only after deinstalling and reinstalling the client software.

Update service

The PBX Call Assist 5 UCServer provides an automatic update service. More information can be found under Update service.

Update server

The software distribution and the update service need the update server. More information can be found under Update Server.

19.5 Update service

The update service can be installed on the workstation with PBX Call Assist 5.

This system service checks regularly whether a new version of PBX Call Assist 5 is available on the PBX Call Assist 5 UCServer. If a new verison is found it is automatically installed on the workstation.

The update service consists of two applications:

- ***EACuSrv.exe***
  Checks at regular intervals whether a new software version is available on the server, loads it on to the client and starts the update process.
  The application is registered as a system service and also runs without users logged in.
- ***EClnSet.exe***
  Auxiliary application which installs the update.
- ***EClnProg.exe***
  Auxiliary applications which inform the user about an upcoming update and the update progress. Is started in the context of the logged-in user in order to be able to display the information in their session.



If you deploy PBX Call Assist 5 workstations in different languages you must keep the corresponding languages available in the client update folder. During server installation, only the server language is installed by default. You must copy further client installation packages manually into the update folder.

19.6 Active Directory® Objects

By default, replication of the Active Directory® objects will be restricted to 2000 objects in PBX Call Assist 5 UCServer for reasons of performance.
In this context, a special understanding of the term Objects as Users will be required. In addition to Users, this includes groups, contacts and other things.

If Active Directory® contains 2000 objects and the next (2001) object is a user no longer present in PBX Call Assist 5 UCServer, it will no longer be replicated. Check the number of objects stored in Active Directory®.
If the number of objects is found to exceed 2000, or if PBX Call Assist 5 UCServer indicates a potential excess in the server status, the restrictions implemented in PBX Call Assist 5 UCServer can be increased by adding the following registry key.

Registry Key:	HKEY_LOCAL_MACHINE\Software\(Wow6432Node\)estos\UCServer4\Server\ADMaxRead
Type:	[REG_DWORD]
Value:	5000
Minimum:	100

20 Technical notes

Information about details and special topics are summarized in this section, referenced from other help pages.

- Telephone number formats
- Configuration file location
- Offline journal
- Contact search
- Regular expressions
- Setup a DNS service resource record
- Setup of DNS Service Resource Records for the federation
- User rights
- User Authentication
- Automatic line binding
- Server certificate
- TAPI-driver
- XSL templates
- XSLT for e-mail notification
- Configuration files
- User database import and export
- SIP Response Codes
- SIP PCAP log files
- Creating an XMPP Federation
- Creating a static routing entry between PBX Call Assist 5 UCServer and Microsoft® Lync® Server using TLS/MTLS
- Core services
- Active Directory® objects

20.1 Configuration file location

Location configuration
The configuration of the locations is always stored in an *xml* file. The file is in *config\locations.xml*.

Country dialing rules
The dialing rule table contains the country dialing rules. These are stored in the *countries.xml* file. It contains the names of the countries and the appropriate dialing rules for local, national and international calls.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<countries xmlns="http://www.w3.org/2001/XMLSchema.xsd">
<country ID="49">
 <countryCode>49</countryCode>
 <name>Germany</name>
 <SameAreaRule>G</SameAreaRule>
 <LongDistanceRule>0FG</LongDistanceRule>
 <InternationalRule>00EFG</InternationalRule>
</country>
</countries>
```

Icon	Meaning

E	Country code
F	Area code
G	Local number
I	Optional dialing code
N	Optional long distance provider

Call-by-call country dialing codes
The *providers.xml*l file contains the known call-by-call dialing codes for individual countries.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<providers xmlns="http://www.w3.org/2001/XMLSchema.xsd">
 <provider ID="10???" countryID="41">
 <name>General</name>
 </provider>
 <provider ID="10703" countryID="41">
 <name>Smartphone</name>
 </provider>
 <provider ID="01090" countryID="49">
 <name>O2</name>
 </provider>
</providers>
```

Day	Meaning
countryID	ID of the country in countries.xml
ID	Provider prefix (*?* is a placeholder for any digit)

Dialing codes and place names
The *cities.xml* file contains the known place names for the country dialing codes.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<cities xmlns="http://www.w3.org/2001/XMLSchema.xsd">
 <city ID="+1201" countryID="1">
 <name>New Jersey</name>
 </city>
 <city ID="+4989" countryID="49">
 <name>München</name>
 </city>
</cities>
```

Day	Meaning

countryID	ID of the country in *countries.xml*
ID	Area code

Special phone numbers
The *specialnumbers.xml* file contains the known country special phone numbers. These are numbers which are not internationally dialable, e.g. emergency or information numbers. No dialing code is added to these numbers during formatting.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<specialnumbers xmlns="http://www.w3.org/2001/XMLSchema.xsd">
 <specialnumber ID="110" countryID="49">
 <name>Notruf</name>
 </specialnumber>
</specialnumbers>
```

Day	Meaning
countryID	ID of the country in countries.xml
ID	Phone number

20.2 Offline journal

The offline journal is a server-based database which temporarily saves missed calls before delivering them to the users.

If the PBX Call Assist 5 software is running on the workstation of the user, the call is registered directly at the workstation of the user and delivered as an unanswered call. If the PBX Call Assist 5 software has not been started or the PC is shut down, the call is flagged on the server as unanswered. If the user now starts the PBX Call Assist 5 software, the incoming calls in the meantime are delivered to the client which processes them as usual.

In addition to the off-line journal, there is also the possibility to send these missed calls directly by e-mail from the server. It is sometimes possible that not all names of callers are found here. The server processes phone numbers only with the user administration and the MetaDirectory.

20.3 Contact search

With an incoming or outgoing call, PBX Call Assist 5 automatically searches for the dialog partner for the displayed phone number in various locations. Parts of the contact search are implemented both on the server and on the client. PBX Call Assist 5 UCServer searches for a suitable contact and presents them to the client. PBX Call Assist 5 searches in client-side connected data sources and expands the individual contact into a list of contacts. After the search is complete, PBX Call Assist 5 checks whether the user has already ever selected one of the contacts found. If a contact has ever been selected, this contact is set as the active dialog partner; otherwise, the first contact found (server or client contact) is displayed as the active dialog partner.

- Contact search in PBX Call Assist 5 UCServer:
  The server searches synchronously for a contact. The client therefore only displays the call window

for an incoming or outgoing call when the contact search is finished.
The server searches in the connected data sources in the sequence specified here. The first hit ends the search.
Server search sequence:
- Cache for contacts already found
- Internal user administration
- Active Directory®
- estos MetaDirectory databases
- EDBCon (SDK component)
- estos MetaDirectory Phonebooks

- Contact search in PBX Call Assist 5:
  The client searches asynchronously for a contact. The call window is initially displayed with the contact found on the server. The client searches through the contact data sources configured and specified by the administrator in PBX Call Assist 5.

20.4 Regular expressions

Regular expressions are patterns with which strings can be searched. It is thus possible to determine whether the string fulfils specific parameters (length, begins with certain numbers, etc.) or to replace certain parts of the string.

Search for
This expression is used on the string. If a match is found, the string is replaced with the *replace with* expression.
Hint: The caret (^) key can be found at the upper left of a keyboard with German layout.

A brief overview of the permitted expressions:

Character	Description
^	The beginning of the digit chain. The expression "^0" finds "0" only at the beginning of the phone number.
^	The caret directly after the left bracket ([) has another meaning. It is used to exclude the other characters within the bracket. The term "[^0-8]" permits digits from 0 to 8 only.
$	The dollar character labels the end of the character string. The term "152$" is valid for phone numbers which end with "152" only.
|	The slash allows both digits each side of it. The expression "8|9" allows "8 or "9".
.	The dot (.) permits any character (or any digit).
*	The asterisk (*) shows that the characters to its left must be present 0 times or more.
+	The plus sign (+) is similar to the star except that the character to its left must be present at

	least once.
?	The question mark (?) shows that the character to its left must be present 0 or 1 times.
()	The round bracket marks the expressions which are available in the **replace with** field.
[]	The square bracket ([and]) marks a number of characters which are permitted at this location.

Replace with
Insofar as a match with the string was found, the string is replaced by the expression entered here. Parts of the found string can be inserted here:
\1 reads out the first expression marked with '()' in the *search for* field.
\2 reads out the second, etc..

Examples:

Effect	**Search for**	**Replace with**
Removal of a leading 0	^0(.*)	\1
Replacing a 80 at the beginning of a number (e.g. targeted external dialing code) with 0	^80(.*)	0\1
Removal of a private PIN which is added to the beginning of a phone number as 50xxx	^50[0-9][0-9][0-9](.*)	\1
Suppression of all numbers which are signalled internally (3 digits)	^[0-9][0-9][0-9]$	
Add an external dialing code code (leading 0) for all numbers with more then 3 digits	^([0-9][0-9][0-9].+)	0\1
Add the phone system base number (03012345) to all internal numbers (1 to 3 digits in length)	^([0-9][0-9]?[0-9]?)$	03012345\1
Add your own area code to all numbers which do not start with 0 and are at least 4 digits long (and thus not internal numbers).	^([^0][0-9][0-9][0-9].*)	08151\1

20.5 Setup a DNS service resource record

A service (SRV) resource record can be entered in a DNS to make IP-based services in a domain easier to find. Additional information on a service can also be made available (e.g. server on which the service is running, priorities, etc.)

Such a Service Resource Record can be created as follows:

```
_ctiserver Service Location (SRV) [1][0][7222] ucserver.domain.com.
```

_ctiserver	Name of the service under which it can be found in the DNS. For PBX Call Assist 5 this must be _ctiserver.
Service Location (SRV)	The type of record contained by these lines.
[1]	Priority of the service. This permits prioritisation of the different, similar entries.
[0]	Weighting of the entry. Is used to make a pre-selection of the DNS entry when the client setup is run. The following values are of particular significance: 0 - DNS entry exists but the static configuration is still pre-selected in the client setup **Note:** Entry 0 is not valid for the individual installation of the "Extended RemoteTSP" 1 - 99 DNS entry is pre-selected in the client setup 100 - DNS entry is pre-selected; static configuration is not available.
[7222]	The port number under which the service provides the service is specified here. For PBX Call Assist 5, the default setting is normally client port 7222.
ucserver.domain.com	Computer which provides the service. Here PBX Call Assist 5 expects the computer on which PBX Call Assist 5 UCServer runs.

More details about the numeric values (special priority and weighting) are documented accordingly in the RFC-2782.

How and where the Service Resource Records are created for specific DNS servers can be found in the corresponding manufacturer's documentation.

20.6 Setup of DNS Service Resource Records for the federation

A Service (SRV) Resource Record can be created on a Domain Name Server (DNS) for making IP-based services easier to find in a domain. Additional information about a service may be made available (such as the server running the service, priority and so forth).

Such a Service Resource Record can be created as follows:

```
_sipfederationtls Service Location (SRV) [1][0][5061] ucserver.domain.de.
```

_sipfederationtls	The name of the services which are found in the DNS. For the federation, the name must be _sipfederationtls.
Service Location (SRV)	The type of record contained by these lines.

[1]	The priority of the service so that different, similar records can be prioritized. Not in use.
[0]	Emphasizes the entry. It is not used
[5061]	Here the port number is provided from which the service provides the service. For the federation the default is generally valid: standard SIP on port 5061.
ucserver.domain.com	The computer which offers the service. Here, the federation expects the computer on which the UCServer runs.

How and where the Service Resource Records are created for specific DNS servers can be found in the corresponding manufacturer's documentation.

20.7 User rights

There are individual authorizations between system users. A user can acquire authorizations for another user in various ways. These authorizations contain both rights to see information about another user and rights to control their phones or to set their presence status.

A user can acquire authorizations for another user in the following ways:

- **Global rights**. If an authorization is granted in the global rights it applies for all system users. These rights are configured exclusively by the administrator.
- **Group rights**. If authorization is granted in the group rights, this applies to all users who are members of this group. The rights are configured exclusively by the administrator.
- **User permission**. Every user can grant individual rights to themselves to other users. These rights can also be viewed and configured by the administrator.



Rights always apply additively. If the user has acquired a certain right via superior rules this cannot be taken away in subordinate rules.

The following authorizations are available:

Authorization	Description
See presence	The other user may see the presence status (present, absent…).
Set presence	The other user may alter the presence status. This right should only be set for special trust relationships.
See private appointments	The other user may see the appointments marked as private in the calendar. This right should only be set for special trust relationships.

See public appointments	The other user may see the appointments marked as public in the calendar.
See outgoing numbers (primary/secondary line)	The other user may see who the user is currently calling with their primary/secondary phone. This right should only be set for special trust relationships.
See incoming numbers (primary/secondary line)	The other user may see who is currently calling the user on their primary/secondary line.
See the number of a set redirection (primary/secondary line)	The other user may see to which target number a redirection in the phone is activated. This right should only be set for special trust relationships.
See call redirection (primary/secondary line).	The other user may see that call redirection is activated on the phone.
Pick up calls to the user (primary/secondary line).	The other user may pick up incoming calls on the primary/secondary line. This right should only be set for special trust relationships.

20.8 User Authentication

The user login on the PBX Call Assist 5 UCServer requires authentification. This can be done either via a UC password or via a Windows® application. The combination of user database and user login configuration dictates the process used. The technical background is described in the following.

Active Directory® user management, domain authentication

The user names come from the Active Directory®. Only users who are configured in Active Directory® can log on. The users will be authenticated at the Active Directory® implicitly or explicitly with their Windows® login with NTLM. The PBX Call Assist 5 UCServer does not have to be member of the domain, the authentication at the Active Directory® takes place using LDAP. The password of the user will never be transmitted via the network.

Integrated user management, UC password

The user names come from the integrated user database. Only users who are configured in the PBX Call Assist 5 UCServer can log on. The UC password is specially configured for the user and stored in the user database. The user's UC password is transmitted over the network in encrypted form.

Integrated user management, domain authentication

The user names come from the integrated user database. Only users who are configured in the PBX Call Assist 5 UCServer can log on. The users are authenticated either implicitly or explicitly via NTLM directly on the PBX Call Assist 5 UCServer. The user's password is not transmitted over the network under any circumstances.

21 Global permissions

With the authorization levels you set which presence and contact information is transferred to the users within the UCServer at least. You also use the level to set the minimum permissions users receive on other users' lines.
Users can increase the permission level, but cannot revoke a right assigned here.
There are 4 predefined levels for the permissions.

➡	The authorization levels restrict only the contact details exchanged through presence information. The authorization level does not affect the contact search function. Contact details such as mobile phone numbers are still visible via a contact search regardless of the authorization levels.
➡	These authorizations are only effective within the UCServer service responsible for the user. Federation contacts or contacts of other UCServer services do not see this data! The permissions for federation are set separately under "Federation - Domain Permission".

21.1 Contact data

The information displayed in the contact details depends on the user management used. If Active Directory® Integration is used as the user management, additional fields are displayed.

Information	Public	Business	Team	Personal
Contact image	X	X	X	X
Display name	X	X	X	X
Title	X	X	X	X
Company	X	X	X	X
Department (Active Directory® only)		X	X	X
Office		X	X	X
Business address		X	X	X
Work phone	X	X	X	X
Business phone 2	X	X	X	X
Mobile number	X	X	X	X
Pager		X	X	X

Private phone				X
additional phone numbers (Active Directory® only)				X
Business fax number		X	X	X
E-mail address	X	X	X	X
SIP address	X	X	X	X
SharePoint/Website		X	X	X

21.2 Presence and lines

The following permissions are granted to users among themselves on presence information and lines in the Favorites and Monitor.

Authorization	Description	Public	Business	Team	Personal
See contact image	A contact image stored for the user is visible.	X	X	X	X
See presence	The other user is allowed to see the presence (Present, Absent...).	X	X	X	X
Set presence	The other user is allowed to change the presence. This right should be set only in the case of special positions of trust.			X	X
See note	The other user is allowed to see the note.	X	X	X	X
Set note	The other user may enter a note.			X	X
See private appointments	The other user is allowed to see the		x with the	x with the	X with

		appointments marked as private from the calendar, if the user has released his appointments. This right should be set only in the case of special positions of trust.		indication "Private	indication "Private	subject and place
See public appointments		The other user is allowed to see the appointments marked as public from the calendar, if the user has released his appointments.		X	X	X
Phone:						
See existing phone numbers		The phone numbers assigned to the user are displayed when you move the mouse over the prefix (phone number/extension of all lines).	X	X	X	X
See line status (free/busy)		The other user can see if the phone line is free or busy		X	X	X
First line (Business 1)	See outgoing phone numbers	The other user is allowed to see who the user is calling on their primary phone. This right should be set only in the case of special positions of trust.		X	X	X
	See incoming phone numbers	The other user is allowed to see who the user is currently being called by on their primary phone.		X	X	X

	See diversions	The other user is allowed to see that call forwarding is enabled on the phone.	X	X	X	X
	See the number of a set call forwarding	The other user is allowed to see to which destination number call forwarding is enabled on the phone. This right should be set only in the case of special positions of trust.		X	X	X
	Set diversions	The other user is allowed to set up call forwarding on the line.				X
	Retrieve call	The other user is allowed to pick up incoming calls on the first line.			X	X
Second line (Business 2)	See outgoing phone numbers	The other user is allowed to see who the user with his second phone is calling. This right should be set only in the case of special positions of trust.			X	X
	See incoming phone numbers	The other user is allowed to see who the user with his second phone is currently being called by.			X	X
	See diversions	The other user is allowed to see that call forwarding is	X	X	X	X

		enabled on the phone.				
	See the number of a set call forwarding	The other user is allowed to see to which destination number call forwarding is enabled on the phone. This right should be set only in the case of special positions of trust.			X	X
	Set diversions	The other user is allowed to set up call forwarding on the line.				X
	Retrieve call	The other user is allowed to pick up incoming calls on the second line.				X
additional lines	See outgoing numbers	The other user is allowed to see who the user with his second phone is calling. This right should be set only in the case of special positions of trust.			X	X
	See incoming phone numbers	The other user is allowed to see who the user is currently being called by on their phone.			X	X
	See call forwarding	The other user is allowed to see that call forwarding is enabled on the phone.	X	X	X	X
	See the	The other user is			X	X

	number of a set call forwarding	allowed to see to which destination number call forwarding is enabled on the phone. This right should be set only in the case of special positions of trust.				
	Set call forwarding	The other user is allowed to set up call forwarding on the line.				
	Pickup call	The other user is allowed to pick up incoming calls.				
Audio/Video:						
See line status (free/busy)		The other user can see if the AV line is free or busy	X when busy, the AV icon is grayed out	X when busy, the AV icon is grayed out	X when busy, the AV icon is red	X when busy, the AV icon is red
see Conversation participants		The other user can see with whom the AV is conducted.			X	X

21.3 Configure user account yourself

Users may configure their profiles personally
When installing the workstations, you can give users ownership. The users are then prompted to enter their own settings. The server is thus configured by the help of the users. You can undo this setting at any time when the server has finished configuring.
If this option is set, all users can change their personal settings in the user administration themselves. The user can make these settings with the workplace settings. The following settings are possible (see also Users):
Depending on the selected user management, the users with the right to manage their user account themselves can change the following settings:

Setting	Active Directory®	Integrated user database

First name	-	X
Last name	-	X
Displayed name	-	X
E-mail address	-	X
Password	X	X
Company	X[2]	X
Job title	X[2]	X
Office	X[2]	X
Street house no.	X[2]	X
Zip code / Place	X[2]	X
State	X[2]	X
Country	X[2]	X
Website	X[2]	X
Business phone number	X[2]	X
Business phone number 2	X[2]	X
Private phone number	X[2]	X
Mobile number	X[2]	X

Mailbox phone number	X	X
Recording server phone number	X	X
1. phone	X	X
2. phone	X	X
Services	X	X
Own phones	X	X
Computer phones	X	X
Contact address / Image	-	X

[2]Can be edited by the user if Active Directory® write access has been configured.

21.4 Automatic line binding

The phone numbers configured in the user account are automatically used by the PBX Call Assist 5 UCServer for the line binding. If the server is able to find a line for the phone numbers of a user, then the line is automatically assigned to the user. The phone number in the user account has to match the phone number of a line. The user automatically receives the lines belonging to him without further configuration.

If users are maintained in the Active Directory®, it can be separately defined whether automatic line binding should be used for the first and second business phone number.

If this automatism cannot be used in the available field, then it can be deactivated via Global settings. In this case the lines have to be configured for every user manually. In the user configuration, use the fields **1st phone** and **2nd phone** to assign the lines to the user. Enter the phone numbers under which the user is available in the business phone number fields.

21.5 Server certificate

A server certificate is required for encrypted communication via TLS (Transport Layer Security) and MTLs (Mutual MTLS).

Server certificate
A server certificate uniquely identifies a server. The certificate must be issued on the server's FQDN (full qualified domain name) . The server certificate must be issued by a trustworthy instance. Certificates are configured in the Microsoft® Management Console (MMC) certificate snap-in.

Certificate store
The certificates used must be stored under Local Computer/Own Certificates and contain a private key. The Local Computer certificate store can be opened with the MMC console.

- Select **Run...** from the Windows® Start menu and enter mmc.exe. `mmc.exe`.
- Select **File** - **Add/Remove snap-in...**
- Select **Add**. Select **Certificates** from the list of available snap-ins. Select **Computer account**, **Local computer** and click **Finish**.
- In the list, go to **Certificates (Local computer)** - **Own certificates**.

21.6 TAPI-driver

Your telephone system requires a TAPI driver to operate this software, if you wish to control your telephone.

A TAPI-driver is a system component that is provided by the manufacturer of your telephony device (either free of charge or for a fee).

The TAPI-driver connects the CTI software to the telephony terminal device. Each TAPI-driver supports different functions depending on the implementation. Not all functions which you can perform on the phone itself are always available on the PC.

TAPI-drivers are installed in Settings - Control Panel - **Phone and Modem Options - Advanced**.

Open phone and modem settings:

21.7 XSL templates

The PBX Call Assist 5 UCServer uses XSL Templates (short: XSLT) for the display of XML data as html sites. The XSL Template files are in the *Templates* or *Templates/default* directory. See Configuration files.

Template	Deployment
unanswered.xslt	E-mail notification of unanswered or forwarded phone calls. View XSL templates for e-mail notification

XSLT processor
PBX Call Assist 5 UCServer provides the data as XML files. These XML files are processed into an HTML page with the help of an XSL template and an XSLT processor. Either Sablotron or the Microsoft® XML Parser are used as an XSLT processor.

Development of own templates
You can develop and use your own templates. You should familiarise yourself with XSLT syntax for this. You can find help on the subject at SelfHTML or the Microsoft® MSDN pages.
If you wish to use templates you have developed yourself these should be stored in the *config* directory. Your changes will then not be lost if an product update is installed.

21.8 XSLT for e-mail notification

The *unanswered.xslt* file is used for e-mail notification of unanswered or forwarded calls.

The XML files on which the template is used are created by the server. File *sample_unanswered.xml* contains example files for an unanswered call. File *sample_redirected.xml* contains example files for a forwarded call. The files are to be found in the *templates/default* directory.

You can use the *msxlt.exe* program supplied to apply an XSLT to an XML file. Open a command line in the installation directory:

```
msxsl.exe templates\default\sample_unanswered.xml
templates\default\unanswered.xslt -o unanswered.htm
```

If the logLevel is set under Events on debug, a XML file is provided in the list *logs* for every unanswered phone call. You can use this for the development of your own XSL templates.

21.9 Configuration files

All important parts of the PBX Call Assist 5 UCServer configuration are stored in files. The only exception is the software licences, which are stored in the registry. All files are in the *config* directory below the installation directory.

Directory	Deployment
config	Configuration files which are created at run time. These are preserved in case of an update. You should also save files you have changed in this directory should you wish to change one of the files supplied in config/default.
config/default	Configuration files which were installed with the product. These are overwritten if the product is updated.
config/users	Settings for users for file-based PBX Call Assist 5 UCServer user management
config/computers	Settings for the computers with PBX Call Assist 5 UCServer user administration
templates	You should save files you have changed in this directory if you wish to change one of the files supplied in templates/default
templates/default	Configuration files which were installed with the product. These are overwritten if the product is updated.
database	All databases created by PBX Call Assist 5 UCServer using MS Access databases (default path). User database in case of SQL supported user administration (view User data base).

21.10 User database import and export

To be able to save and restore the current configuration of databases, users, groups and computers, use the **Data Export** and **Data Import** features on the **File** menu.

Data export
The current configuration data, databases (non-SQL Server) and the configured users (including Favorites),

groups and computers can be backed up in a ZIP file using the Data Export option. Exportation of inactive elements can also be selected for users, groups and computers.
If this feature is selected, a wizard will appear to guide the export process. Follow the wizard's instructions to create the export file.

Data import
Exported data can be restored to the system in this manner. Depending on the data to be imported, the server may need to be re-started in some cases. The wizard will import the data and issue a notification if the server must be restarted.

	Data import into an internal user management system overwrites all currently existing information.
	Users, groups and computers cannot be imported into an Active Directory® Administrator.
	If the directory for file-based databases cannot be created in the configuration to be imported, e.g. because the drive does not exist, the configuration is automatically adjusted and the default directory ([installation directory UCServer]\database) is used.

Data import from the previous version 2.2 or 3.0
Importing data from Versions 2.2 or 3.0 is not supported. Export the data from Versions 2.2 or 3.0 and import it into a Version 4.0 installation. Afterwards, the current 5.0 Version will be able to accept the data directly during installation.

	The latest version of the TapiServer service must be installed to permit its data to be exported.

21.11 SIP Softphone(s)

Many telephone systems (PBXs) make the operation of telephones possible that have been implemented according to the SIP standard. PBX Call Assist 5 UCServer supports the central integration of such telephone systems. This integration allows PBX Call Assist 5 client users to use their PCs as softphones in order to make telephone calls through the telephone system. To do this, the PBX Call Assist 5 client gets one or more lines, that respectively correspond to one telephone from UCServer.

To configure UCServer, one such line that is respectively responsible for registration of a certain telephone number must first be added. Afterwards, the line will be assigned to a user with the help of this telephone number. Thereby, the PBX Call Assist 5 client users can use the telephone system for making telephone calls through UCServer.

UCServer already has the SIP modules necessary for PBX integration, which assume control of the call signals. In addition, UCServer contains a media server that binds the PBX on the one hand and the PBX Call Assist 5 clients on the other hand with each other. By using the media server, the media streams will respectively be converted into the correct format. On the client side, the media streams are encrypted (DTLS-SRTP), even when the PBX does not provide encryption. The telephonic accessibility of the users located on the Internet is another job of the media server. If a PBX Call Assist 5 Mobile client is outside of the reach of the internal WLAN or, for example, a PC client is in a home office, the central PBX can continue to be used for making telephone calls.

Technical Information

The telephone system must allow registrations through a LAN interface in accordance with the SIP standard (RFC 3261). UCServer does not need a SIP-specific license. However, some telephone systems need licenses in order to register SIP softphones with the telephone system.

Connection to telephone systems via SIP trunk or via classic SIP registration
Softphone lines can be connected to the telephone system via a classic SIP registration or via a SIP trunk. The classic SIP registration registers one line per registration with the telephone system. With a SIP trunk, multiple lines are controlled by a signaling connection. A SIP trunk can be addressed by a fixed IP address, whereby all predefined lines are immediately available without registration. However, depending on the telephone system, a SIP trunk can also put a bundle of lines into operation through a single register. In this case, the UCServer registers with the SIP trunk of the telephone system.

Media Server
The media server offers the audio codecs G.711 (PCMU, PCMA), G.722 and Opus for the PBX. Opus is mostly used towards PBX Call Assist 5 Client. This offers good audio quality even with little LAN/WAN bandwidth. With encryption using the DTLS/SRTP method, the Media Server uses the highest security standard that is currently common in VoIP products.

Accessibility on the Internet
Accessibility on the Internet via the Media Server is achieved by using TURN/STUN Server services. These can be provided by your own infrastructure or by estos UCConnect services. If no TURN/STUN servers are configured, communication within the local LAN is possible.

21.12 SIP Response Codes

This page gives a short overview about the SIP response codes for errors. A detailed description of the SIP response code can be found in "RFC 3261 - SIP: Session Initiation Protocol".

SIP Response Codes, Class 4: Request error

Code	Description
400	Bad Request
401	Unauthorized
402	Payment Required
403	Forbidden
404	Not Found
405	Method Not Allowed
406	Not Acceptable
407	Proxy Authentication Required

408	Request Timeout
410	Gone
413	Request Entity Too Large
414	Request-URI Too Long
415	Unsupported Media Type
416	Unsupported URI Scheme
420	Bad Extension
421	Extension Required
423	Interval Too Brief
480	Temporarily Unavailable
481	Call/Transaction Does Not Exist
482	Loop Detected
483	Too Many Hops
484	Address Incomplete
485	Ambiguous
486	Busy Here
487	Request Terminated
488	Not Acceptable Here
491	Request Pending
493	Undecipherable

SIP response codes, class 5: server-error

Code	Description

500	Server Internal Error
501	Not Implemented
502	Bad Gateway
503	Service Unavailable
504	Server Time-out
505	Version Not Supported
513	Message Too Large

SIP response codes, class 6: globale-error

Code	Description
600	Busy Everywhere
603	Decline
604	Does Not Exist Anywhere
606	Not Acceptable

21.13 Creating SIP PCAP log files

PCAP (packet capture) is an open API designed to log network data. These data can then be read by network analysis tools (e.g. Wireshark) providing powerful system-independent options for display and analysis. PBX Call Assist 5 UCServer allows you to collect SIP softphone signaling network data in PCAP files.
Since PCAP log files are created in PBX Call Assist 5 UCServer, it is not necessary to install the Wireshark Win-pcap option (driver for recording on network interface cards). In addition, TLS-encrypted SIP messages can only be written to UCServer in readable form, since UCServer saves these messages in unencrypted form.

Configuration
Configuration takes place using the properties of the Line Group. The "PCAP Log" tab allows you to select either all lines in that group, or specific lines.
If a PCAP log is active, a blue "status icon" is displayed for this line group.

Check of PCAP log files
The name of the log file begins with sipav_[date_time] and ends with .pcapng. The generated file is processed according to the settings in Event with regard to directory, log file size and overwrite option ("Archive Old Logs"). The buttons "Delete log files" and "Collect log files" also work on the PCAP log files.

Analysis of PCAP log files
You can use the Wireshark analytical tool to display, filter and analyze any PCAP log files which were created.

The tool provides extensive filtering options, including the tracking of specific calls as well as a graphical display of flowcharts.

Line group status
The status of the Line Group is displayed with a color icon only when PCAP log has been activated.

Symbol	Statement
	Line group is PCAP log activated.

21.14 Creating an XMPP Federation

The creation of an XMPP federation for the "example.com" presence domain will be described step by step.

1. Start the *PBX Call Assist 5 UCServer administrator program* and connect it with your PBX Call Assist 5 UCServer.
2. Open the pages, Configuration -> Federation -> XMPP Federation.
3. Activate the XMPP federation by checking the Use XMPP Federation checkbox.
4. Select the Direct option from the options for connecting to other servers.
5. Set the TCP port to the default, 5269, by clicking the Default button.
6. Choose a server certificate. Without it, connection to other XMPP domains will not be encrypted using Transport Layer Security (TLS). See the Server Certificate section for more information.
7. Open the pages Configuration -> Federation -> Domain Authorization.
8. Click the "Add..." button, enter "example.com" for Domain Name on the subsequently appearing dialog or the name of the presence domain, to which you want to connect. Choose the desired presence authorization. Choose XMPP for Protocol. Select the desired type of encryption for the Encryption Type. The various types of encryption will be explained under domain authorizations. Complete the entries by clicking the OK button.
9. Click the Apply button to activate the settings just made.
10. If PBX Call Assist 5 UCServer is in a private network connected with the public Internet through a router and firewall then, depending on the circumstance, it may be necessary to have the router and firewall forward port 5269 to PBX Call Assist 5 UCServer. Precise information about this can be found in the documentation for the firewall and router. Make sure that the Windows® firewall running on the computer that is running PBX Call Assist 5 UCServer is not blocking port 5269 and setup a corresponding rule, if necessary.
11. So that "example.com" can connect to PBX Call Assist 5 UCServer, DNS must be able to resolve the name of the presence domain to a public IP address through which PBX Call Assist 5 UCServer can be accessed. If such a DNS record does not yet exist, it should be created. As a rule, a DNS A Record will suffice, since external XMPP servers will attempt to access PBX Call Assist 5 UCServer through the default port, 5269. If an external XMPP server does not support this, A DNS SRV Record will be required as will be described in the next step.
12. Creating a DNS SRV Record for XMPP Server-to-Server Connections:

    A Service (SRV) Resource Record can be created on a Domain Name Server (DNS) for making IP-based services easier to find in a domain. Additional information about a service may be made available (such as the server running the service, priority and so forth).

    Such a Service Resource Record can be created as follows:

    ```
    _xmpp-server Service Location (SRV) [1][0][5269] ucserver.domain.de.
    ```

_xmpp-server	The name of the service through which it will be found on the DNS. The name must be _xmpp-server for XMPP Federation.
Service Location (SRV)	The type of record contained by these lines.
[1]	The priority of the service so that different, similar records can be prioritized. Not in use.
[0]	Emphasizes the entry. It is not used
[5269]	The port number through which the service provided is made available is specified here. The pre-defined Port 5269 generally applies for XMPP Federation in accordance with the XMPP standard.
ucserver.domain.com	The computer providing the service. XMPP Federation will expect to find the computer running UCServer.

How and where the Service Resource Records are created for specific DNS servers can be found in the corresponding manufacturer's documentation.

21.15 Creating a static routing entry between PBX Call Assist 5 UCServer and Microsoft® Lync® Server using TLS/MTLS

Set up static routes in PBX Call Assist 5 UCServer

1. Start the *PBX Call Assist 5 UCServer Administration* program and connect it to the UCServer.
2. Open the page Configuration -> Federation -> SIP Server.
   - Activate Use SIP Server
   - Select a certificate that is valid for your server by means of the "Certificate..." button.
   - Add a TLS or MTLS interface (the default port for TLS or MTLS is 5061) by means of the "Add..." button.
3. Open the page Configuration -> Federation -> SIP Static Routing
   - Add a static routing entry with domain, access server and port (the default port for TLS or MTLS is 5061) for the Lync® Server by means of the "Add..." button.

Creating Static Routing in Microsoft® Lync® Server

A **Fully Qualified Domain Name** (FQDN) must be used in static routing for TLS communication.

A static routing entry for PBX Call Assist 5 UCServer is added in this manner

1. Login to the Lync® Server computer as a member of the **RTCUniversalServerAdmins** group.
2. Start the **Lync® Server Topology Builder** to define a **Trusted Application Pool**.
   - Right-click on **Trusted Application Servers** and click **New Trusted Application Pool**.
     - Enter the network address for the computer providing the PBX Call Assist 5 UCServer services for the FQDN pool. The network address must be in agreement with the FQDN for the server certificate.
   - Finally, the changes to the topology must be published.
     - Right-click on **Trusted Application Servers** and click **Topology** and then **Publish**.

3. Start the **Lync® Server Management Shell**.
    - Create static routing to PBX Call Assist 5 UCServer and add it to the global routing list.
        - First, adjust the following commands to your specifics. Afterwards, enter the adjusted commands through the shell.

          ```
          $x = New-CSStaticRoute -TLSRoute -Destination FQDN -Port
          PORT -UseDefaultCertificate $True -MatchUri URI
          ```

            - Where FQDN is the network address for the computer running PBX Call Assist 5 UCServer.
            - Where PORT is the port, 5061 is the default port for TLS and MTLS. IF another port has been configured for PBX Call Assist 5 UCServer, enter that port.
            - Where URI is the SIP URI for PBX Call Assist 5 UCServer after the at-sign (@).
        - Afterwards, enter the following commands through the shell to add the routing entry to the global routing list.

          ```
          Set-CsStaticRoutingConfiguration -Identity global -Route
          @{Add=$x}
          ```

    - Define Trusted Application
        - First, adjust the following commands to your specifics. Afterwards, enter the adjusted commands through the shell.

          ```
          New-CsTrustedApplication -ApplicationId NAME -
          TrustedApplicationPoolFqdn FQDN -Port PORT
          ```

            - Where NAME is any desired name for the application. The name must be unique in the pool.
            - Where FQDN is the network address for the computer running PBX Call Assist 5 UCServer.
            - Where PORT is the port, 5061 is the default port for TLS and MTLS. IF another port has been configured for PBX Call Assist 5 UCServer, enter that port.
    - Add Trusted Application to the Trusted Application Pool.
        - First, adjust the following commands to your specifics. Afterwards, enter the adjusted commands through the shell.

          ```
          Set-CsTrustedApplicationPool Identity
          TrustedApplicationPool:FQDN -OutboundOnly $False
          ```

            - Where FQDN is the network address for the computer running PBX Call Assist 5 UCServer.
    - Activate Settings.
        - Enter the following command in the shell to activate the settings.

          ```
          Enable-CsTopology
          ```

Note that the settings for static routing will first take effect after Lync® Server has been re-started.

22 Core services

22.1 Restrictions

Very specific basic services of the UCServer can be deactivated here for special deployment scenarios.

These basic services include:
Presence Management
- Presence
- Assignment of rights

Collaboration
- Chat
- Chat logging

It should be taken into consideration that this action will cause significant restrictions for the product features.

Presence Management
The accessibility of presence and the comfortability features can be affected by these settings.
Presence can be deactivated globally for the entire system. With that, the presence display in the clients will be grayed out and comfortability features like Inform About Status Changes or Set Rights will also no longer be available.

The assignment of rights from user to user in the entire system can be turned off using Users May Not Assign Rights, however without having to forego the presence display.

Collaboration
The text message features between users can be restricted here.
"Globally Suppress Text Chat" allows you to completely disable text messages globally.

"Do not save chat history in database" prevents chat messages from being stored in a server-side database. Chat messages are saved in main memory for 3 hours. If a message recipient is offline and does not log onto the server within 3 hours after the message was sent, the chat message is lost. All chat messages in main memory are likewise lost when the server is restarted.

22.2 PN_PBXVOICESERVICE_LONG

The Auerswald telephone system is activated by licensing and setting up the "PN_PBXVOICESERVICE_LONG" in the estos UCConnect portal.
If the PN_PBXVOICESERVICE_SHORT is licensed, the menu for configuring the telephone system is displayed in the UCServer administrator. Users and groups are enabled for acivation of the "PN_PBXVOICESERVICE_SHORT".

The settings are explained on the following pages:
Initial setup
Update the telephone system
Interactive Voice Menu (IVR)
Set up terminals
Signaling
Setup of users
Setup of groups

22.3 Initial setup

The system must be set up once for each exchange head using the "Initial setup".

22.3.1 Telephone system

If the exchange line ordered is available in the system, the line number is displayed in the "Initial setup" menu and can be selected for setting up the system.
Until the exchange line ordered is available, a test line with 10 extensions is provided for the PN_PBXVOICESERVICE_SHORT.

For the initial setup, the desired Telephone exchange connection must be selected and then "Set up system" selected.
You can also specify how users are set up with a phone number from the selected area:

- The users are activated for the Voice Services (required)
  A voice-mailbox is created for the activated users. This can be deactivated on the user object
- The users are activated for PBX Call Assist 5 (optional)
- A SIP line is created for the users and provided as a softphone. (opional)

The following actions are carried out with "Set up system":

- The location is created
- Users with a phone number from the selected range are activated for the PN_PBXVOICESERVICE_LONG and a Voice-Mailbox is set up for each user.
- SIP lines are created in UCServer for the phone numbers assigned to a user. (optional)
- The corresponding softphone line is assigned to these users. (optional)

Users with phone numbers from a different number range or users without a phone number must be updated manually.

The process must be carried out for each external number range.

After setting up the system, the groups/hunt groups can be created and an Interactive Voice Menu (IVR) can be set up.

22.3.2 Drop-off number

A "drop number" can be specified for calls to numbers that are not assigned to a user or no terminal device is registered. It should be ensured that a terminal device is always active on this number or that valid call forwarding is set up.

22.4 Telephone system

Further configurations can be made in the cloud telephone system. The prerequisite for using new functions is that the telephone system is up to date.

22.4.1.1 Advanced configuration

In the web administration, you can set up your own SIP trunks and queues, set call forwarding for groups and define telephone keys.
Instructions on the available configurations can be found in the support portal at:
https://support.estos.de/procall-voice-services/procall-voice-services-verwalten-web-admin

The web-based configuration interface can be opened in the standard browser via the link displayed.

An exception is the use on Windows Server® 2016, where the link must be copied via "right mouse click" and pasted into the browser.

The link contains an authentication token, which is renewed regularly. The link is therefore only valid for a limited time and cannot be saved as a favorite in the browser.

22.4.1.2 Update the telephone system

The PN_PBXVOICESERVICE_SHORT are constantly being further developed. When updating the PBX Call Assist 5 UCServer, it may also be necessary to update the cloud telephone system in order to be able to use the new functions.

22.4.1.3 Versions

Whether a new version of the telephone system is available is displayed here.

22.4.1.4 Update

The telephone system update can take up to 30 minutes. During this time, the PN_PBXVOICESERVICE_SHORT is not available.

You can specify the date and time at which the update is to be carried out.

22.5 Interactive Voice Menu (IVR)

An interactive voice menu (IVR) can be set up in the PN_PBXVOICESERVICE_LONG.
The stored announcement is played to the caller and he can select the desired transfer destination by pressing a button on the telephone.

22.5.1 Basic settings

The phone number for the IVR must be specified. This phone number is then no longer available for assignment to a user or group.
The desired phone number can be selected using the ... button or entered in the format +49.
The PN_PBXVOICESERVICE_LONG can only manage multi-digit extensions. If the central phone number has 1 digit, e.g. +49 8151 36856-0, it must be entered manually in full form without spaces.
Example:+498151368560
Then the destination numbers for selecting the digits 0 - 9 can be entered.

For switching to internal extensions, the selection should be made using the ... button. Otherwise **the extension** must be entered.
For transfers to external extensions, the phone number must be specified in full canonical format.
If another menu is to be selected, the submenu must be created first. (see below)
After creating the submenu, the assigned extension can be selected.
To activate the IVR, an announcement must be stored that contains all the options.



All announcements for PN_PBXVOICESERVICE_LONG must be WAV files in the following format: Mono, 8kHz, 16 bit, PCM

A **drop number** can be defined. The caller is connected to this number if they make no selection or an invalid selection.
Specify the number of seconds after which the caller should be connected without entering a number and select the destination number.

To specify the alternative phone number, the selection should be made using the ... button. Otherwise **the extension number** must be entered.

22.6 Add submenu

If a caller is to be able to select an additional menu, this must be created before the assignment.
Click on "Add submenu....
The extensions 99990 to 99999 are offered as line numbers for the submenu.
Selecting a phone number creates a new tab. Further settings can be made on this tab.

The information for the waiting time and the alternative destination is taken from the main menu, but can be changed.

22.7 Timer

As an option, **off-hours** can be defined. This allows you to specify whether and when incoming calls are only answered with an "After hours" announcement or redirected to a voice mailbox.
By adding multiple entries, different times can be set for the days.

Example:
The company's opening hours are:
Monday to Thursday: 8:00 a.m. - 5:30 p.m
Friday: 8:00 a.m. - 3:00 p.m

The following entries must be defined as closing times:
Mon, Tue, Wed, Thu: 5:30 p.m. - 8:00 a.m
Fri: 15:00 - 23:59
Sat, Sun: All day - All day

If the **Voice mailbox** is activated, the announcement must contain a reference to this. No additional announcement is played.

The voice-messages left by the caller are sent by e-mail to the specified recipients.



A valid, externally accessible e-mail address must be entered for the selected users.

22.8 Devices

The devices must be set up and provisioned in the Auerswald GmbH telephone system. After the device has been set up, it can be assigned to a user.
When the phone device is restarted, it is provisioned and automatically receives the assigned phone number.

Basically, autoprovisioning automatically gives the phones the following features:

- SIP account (registration of the phone with the PBX)
- Access data to protect the telephone configuration
- Function keys
- Language files
- STARFACE user menu for the phone display
- Firmware updates

Please also refer to the Auerswald GmbH web pages for the latest information on setting up the endpoints.

22.8.1 uaCSTA settings

If you have installed an Auerswald ECSTA for SIP Phones, you can enter the required connection data for the phones with provisioning.
Please note that the "Server" must be an address that can be reached from all phone devices. The password for the login, which you have defined in ECSTA for SIP phones, must be entered here.

22.8.2 Enter phone devices

Click "Add" to register a new device.

Name
The name of the device can be freely selected and is displayed when it is assigned to a user object. **The name cannot be changed after adding the device.**

Typ
Select the type of terminal device. Depending on the selection, the data required for registration will be requested.

MAC address	For registering snom and Yealink terminals. The MAC address of the end device must be entered
Gigaset DECT Master	To register a Gigaset DECT Master . The MAC ID must be entered
DECT handset	To register a Gigaset DECT terminal. The IPUI must be specified. This option is only available after successful provisioning of a Gigaset Master. If the handset is successfully entered, it is visible in the web interface of the DECT system.
Grandstream Analogadapter	To register a Grandstream analog adapter The MAC address of the station must be specified. After clicking the OK button, a URL is output, which must be entered in the analog adapter.

DECT Master
This option is only displayed when adding a DECT handset. If several DECT systems are entered, the correct

master must be selected here.

Provision desk phones
By "accepting" the entered devices, the information is transferred to the provisioning service and the phone device can be assigned to a user object.

After entering the snom and Yealink endpoints, accepting the entries (sending them to the provisioning service) and assigning them to a user, the endpoints must be (re)started.
The end devices receive new firmware and the software to use the available settings.

Please note:
The following requirements must be met so that the end devices can be used with PN_PBXVOICESERVICE_LONG and all PN_PBXVOICESERVICE_SHORT functions are available:

- The phone device must be set up in the UCServer.
- The phone device must be assigned to a user object.
- At least 1 phone number must be assigned to the terminal.
- The phone device must be (re)started.

Make sure that the new firmware is installed on the device. Otherwise, the PN_PBXVOICESERVICE_LONG functions will not be available.

Set up DECT system
The DECT master must be restarted once after entering in UCServer.
After successful provisioning, the handsets can be entered in UCServer using "Add" - DECT Handset".
The handsets added in this way are automatically entered in the DECT master and managed there.

In the next step, the handsets must be registered in the DECT system. Via the context menu in UCServer you can start the "Logon mode" in the master.

Set up Grandstream analog adapter
After entering the analog adapter, the URL displayed by the UCServer has to be entered in the configuration of the Grandstream analog adapter under "Advances Settings - Config Server Path".
After saving the input and restarting the analog adapter, the ports are displayed in the UCServer.
The ports can be changed and defined for fax or telephone.

22.8.3 Overview - phone devices

The overview shows to which user the device has been assigned and the status of the device.

Status	Meaning
Online	The device has been successfully provisioned and registered with the telephone system.
Offline	The device has been provisioned successfully, but has not been

	registered with the telephone system.
Provisioning	The Mac® address / UID has been successfully sent to the provisioning server.
MAC address already registered	The MAC address entered already exists on the provisioning server. To provision the end device again, it must first be deleted.
Error received from phone provider	MAC address / UID could not be passed to the provisioning server. contact Auerswald GmbH support.
Error registering device	Error registering the terminal device to the PBX.If re-registering the terminal device is not successful, contact Auerswald GmbH support.
No provider mapping for this device	There is no provider for the provisioning of the terminal.
unknown	The status is unknown. The status is displayed if the terminal device is not entered in the telephone system (offline, online). Errors during provisioning are currently only displayed as long as the "End Devices" window is open. After switching windows, the status cannot be displayed again.
Registration	This status is displayed on a Gigaset DECT Master when it is in registration mode so that the DECT terminals can register with the station.

Please also refer to the notes on the Auerswald GmbH web pages.

22.9 Signaling

If this option is activated, a phone number can be entered for each user, which is signaled to the remote station for outgoing calls.
The phone number entered here is signaled externally for all outgoing calls, regardless of whether the call is made with an assigned terminal or via softphone.

	The user cannot change the phone number.

Click on "Add" to generate a new entry and select the desired user. In the second column, enter the phone number in +49 format (without spaces) that is to be signaled to the remote station for an outgoing call.

By "Apply", the settings are saved in the telephone system and are immediately valid.

Please also see the notes on the Auerswald GmbH web pages. (https://support.estos.de/de/procall-voice-services)

23 Info about PBX Call Assist 5 UCServer

PBX Call Assist 5 UCServer is a product of Auerswald GmbH.

Copyright (C) 2026 estos GmbH.

For product updates visit https://www.auerswald.de

Frequently asked questions and answers and also support are available at https://www.auerswald.de

Support via e-mail is available from info@auerswald.de

Active Directory®, Lync®, Microsoft®, Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Google is either a registered trademarks or trademark of Google Inc. in the U.S. and/or other countries.

All brands and product names used in this document are for identification purposes only and may be trademarks or registered trademarks of their respective owners.