

estos UCServer Business

7.4.1.5939

1	Welcome to estos UCServer	6
2	estos UCServer	7
3	The estos ProCall Client	8
4	Application scenarios	9
4.1	Application in a workgroup	9
4.2	Application in a Windows® Domain	9
4.3	Application with Roaming Users.....	9
5	Installation.....	10
5.1	Presence domain	10
5.2	Network interfaces	10
5.2.1	Network interface properties	11
5.3	Certificate	12
5.4	User database	13
5.5	User authentication.....	13
5.6	Global settings.....	14
5.7	Location	15
5.7.1	TAPI lines.....	15
6	Administration	18
7	General	19
7.1	User database.....	19
7.1.1	Advanced Active Directory® settings	19
7.2	User authentication.....	20
7.3	Events.....	21
8	Telephony.....	22
8.1	Lines.....	22
8.1.1	TAPI lines.....	22
8.1.2	SIP Softphone Lines	25
8.2	Initial Location Setup	30
8.3	Location	31
8.3.1	PBX system.....	31
8.3.2	Formatting rules	35
8.3.3	Least cost routing	36
8.3.4	Advanced	38
8.3.5	Projects	39
8.3.6	Check rules.....	40
8.3.7	Location concepts	41
8.4	Telephone journal	44
9	User management.....	46
9.1	User.....	46
9.2	Groups	48

9.3	Computer	50
9.4	Properties for a computer	52
9.5	User rights	52
9.6	Profile	53
9.7	Global settings	54
10	Services.....	56
10.1	Update server	56
10.2	E-Mail dispatch.....	56
10.3	Share content	57
10.4	STUN and TURN Server Settings	58
10.5	Push notifications.....	60
10.6	Domains authorization.....	60
11	Server status.....	61
11.1	Status monitor.....	61
11.2	Server events.....	62
12	Tools menu	63
12.1	Network interfaces	63
12.2	Certificate.....	64
12.3	Online services	64
12.4	Advanced.....	65
12.5	Connection	68
12.6	Info.....	68
12.7	Lines.....	69
12.8	Set up ECSTA	69
12.9	Connecting the telephone system via ECSTA.....	69
13	Set of rules for filtering out SIP lines	71
13.1	Set up telephone system.....	72
14	Installation of Clients.....	73
14.1	Installation at the workplace	73
14.2	Installation using group policies	74
14.3	MSI description.....	74
14.4	Software distribution	75
14.5	Update service.....	76
14.6	Active Directory® Objects.....	77
15	Technical notes.....	78
15.1	Configuration file location	78
15.2	Contact search.....	80
15.3	Regular expressions	80
15.4	User rights	82
15.5	User Authentication	83

16	Global permissions	84
16.1	Contact data	84
16.2	Presence and lines	85
16.3	Configure user account yourself	89
16.4	Automatic line binding	91
16.5	Server certificate	91
16.6	TAPI-driver	91
16.7	Configuration files	92
16.8	User database import and export	92
16.9	SIP Softphone(s)	93
16.10	SIP Response Codes	93
16.11	Creating SIP PCAP log files	96
17	Info about estos UCServer	97

1 Welcome to estos UCServer

You will find more detailed information about the supported functions and settings of estos ProCall on our web pages.




A guide for installation and initial setup is available in our support area.

This helptext will assist you in configuring the estos UCServer and installing the estos ProCall clients.

- An overview over the characteristics of the estos ProCall from the user perspective is provided by the page estos ProCall client.
- Before you instal, please get information about the typical Application scenarios.
- Help to the configuration dialogs of the estos UCServer can be found under Administration.
- Information about the installation of the estos ProCall 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 estos 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 estos 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.

What is estos UCServer?

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

estos 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 estos UCServer central log data and journals are kept and central databases are connected.

What is the estos ProCall client?

estos ProCall Client is the software at the user's workstation. estos ProCall 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 estos ProCall client](#).

Clients can be installed centrally or remotely.

In addition to an already available software administration, the estos 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 estos 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.

More can be found out about the client installation under [Installation of clients](#).

TAPI-driver

The estos ProCall client cannot be used on the desktop without a TAPI driver. If necessary, a client TAPI driver can be installed which allows third party applications to dial via TAPI.

3 The estos ProCall Client

The estos ProCall client is installed on the users PCs and offers the following important functions and performance features:

Contact search: Find information about the current contact.

estos ProCall automatically searches for the appropriate contact information based on the call number of an incoming or outgoing conversation (especially the call partner) and displays that information. 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 estos ProCall 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 estos ProCall 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.

Journal - tracking and planning communication

The journal in estos 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.

Audio/VideoChat - real-time communication with WebRTC

Der estos ProCall ermöglicht eine direkte Kommunikation mit anderen Benutzern per Audio-/VideoChat und Bildschirmfreigabe.

Softphone - Mit dem PC über eine Telefonanlage telefonieren

The UCServer can register SIP lines at a SIP-capable telephone system. As a result, the PC in combination with a headphone and the estos ProCall Client becomes a VoIP telephone.

4 Application scenarios

The estos 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 estos 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 estos UCServer if you have a Windows® network with domain server and Active Directory®.

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

4.1 Application in a workgroup

To use the estos UCServer in a workgroup without a domain server, first install the estos 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 estos UCServer account**. You can give all users mutual global rights. In a small workgroup usually most rights are valid globally for everybody.

4.2 Application in a Windows® Domain

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

1. Use Active Directory® as User databank.
2. Define the User registration. If all users are registered with the domain, use *Domain authentication*.
3. Define the options Global settings. In addition, you can give globally to all users mutual rights. It's recommended to give the right **View presence** to all users among each other.
4. After the server installation you can either install the workstations manually (directly on the workstation), via software distribution in the estos UCServer or via an Active Directory® group policy. You can also read Installation via Group Policy.

4.3 Application with Roaming Users

To use the estos 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.

- For information about the requirements regarding the operating system and TAPI drivers, go to the page [Link Website System Requirements](#).
- On the page [WEB PAGE - Best Practice Startup](#) you will learn which steps must be taken in which sequence.

5.1 Presence domain

The estos 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 uniquely and permanently assigned to a estos UCServer. The estos UCServer is thus responsible for transmitting the presence information of all its users. Ideally, the identity of each user should match their email address.

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.

5.2 Network interfaces


The connection between the software on the workstations and estos UCServer is made via *network interfaces*. The estos 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 conflicts with other software running on the system.

If a port conflict occurs an error event appears in the event log of the estos UCServer.

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

Using the button **Add** a new network interface can be created.

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

Using the button **Properties** the configuration of a network interface can be changed.

5.2.1 Network interface properties

The connection between the application software on the workstations and the estos UCServer takes place across network interfaces.

Type

The following network interface types are available:

- The **UC client** is the estos ProCall application software on the workstations.
- The **Remote TSP** offers Tapi Service Providers (TSP) over the network.
- The **Administration** is the application to configure the estos UCServer.

IP address and port

Network interfaces are bound to a combination of IP address and port number. The default configuration is set to "All available" IP addresses. It is also possible to select specific IP addresses found by the configuration program. An overview of the default port numbers can be found in the section **network interface**.



Changing the default port configuration is not recommended except the setting conflicts with other software running on the system.
If a port conflict occurs an error event appears in the event log of the estos UCServer.

Encryption

The network interface can be configured in different security levels:

- **Unencrypted:** the estos UCServer is using the network interface unencrypted.
- **Starttls optional:** the estos UCServer is using the network interface encrypted, if available.
- **Starttls mandatory:** the estos 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.

5.3 Certificate

To increase security, the data traffic between estos UCServer and estos ProCall 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 estos 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 estos ProCall

- **Allow secure data transmission using TLS**
If the TLS/SSL encrypting is activated, encrypted and unencrypted programmes in the estos UCServer can be combined.
estos ProCall 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 estos UCServer can be rejected.

Certificate for SSL/TLS communication with estos ProCall

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 ProCall 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.

5.4 User database

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

estos UCServer user administration (file-based)

The estos 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 the Active Directory®. The information is stored in the Active Directory® in the "extensionName" field.

The account entered for the connection requires write permission for the objects in the Active Directory®.

The configuration of users, computers and groups is performed in the estos UCServer Administration.

Active Directory® server

Enter the server's computer name here.

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.

5.5 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, authentication with UC password. You must assign every workstation a unique login for the estos 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 estos UCServer.
Windows® Domain (also with Active Directory® Server)	Integrated user administration or Active Directory®, Windows® domain authentication. Users must also explicitly log in to the estos UCServer with their domain login.
Windows® domain (all users are logged on to the domain)	Integrated user administration or Active Directory®, Windows® domain authentication. Users are automatically authenticated via their domain login at the estos UCServer.

Authentication with UC password

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



Windows® domain authentication

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 into a domain he can still log in to the estos 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.

5.6 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 all users the following rights against each other

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
Softphone, audio chat	If this option is activated, the user is allowed to use audio chat and softphone with other users.
Softphone, audio/video chat	If this option is activated, the user is allowed to use softphone, audio chat and video chat with other users.
Enable screen sharing rights via federation	If this option is set the screen sharing rights specified by the administrator 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.
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.
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.
Share contents	If this option is activated, users can transfer files in the chat. The service must be set up under Services – Share Content.

5.7 Location

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

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

Open the "Default" location and configure the connection to the telephone system or the exchange access.

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.

5.7.1 TAPI lines

You can set up the connection to your telephone system here and select which extensions are to be made available in the network.

The connection to the telephone system is displayed as "Line group". If an ECSTA is set up, you can select "Configure driver" in the context menu of the line group to enter the connection data to your telephone systems.

If the TAPI driver of the manufacturer is used, the setup is done via the Windows® control panel "Phone and Modem".

After successful connection and line setup in the TAPI driver, the lines are displayed under the line group. For information on setting up a supplied ECSTA for your telephone system, please refer to Connecting the telephone system via ECSTA.

Line group properties

The properties of the line group apply for all lines of the group. To display the properties of the group, highlight the group and select *Properties* in the context menu. The configuration options are explained in line group properties for TAPI drivers.




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 estos UCServer. Then the line can be used and users can be added.
- **Trunk line**
This line is treated specifically in estos 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**
estos 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 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 shows detailed information on the status icon in case of an 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 Administration

The server settings are done with the program *estos UCServer administrator*. The program can be started on the server.

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

- General
- Telephony
- User management
- Services

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

7 General

On the following pages the general settings are explained:

- Presence domain
- User database
- User authentication
- Events
- Online services

7.1 User database

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

estos UCServer user administration (file-based)

The estos 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 the Active Directory®. The information is stored in the Active Directory® in the "extensionName" field.

The account entered for the connection requires write permission for the objects in the Active Directory®.

The configuration of users, computers and groups is performed in the estos UCServer Administration.

Active Directory® server

Enter the server's computer name here.

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.

7.1.1 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 estos 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 estos 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 estos 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 transferred 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 preformatted 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.

7.2 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, authentication with UC password. You must assign every workstation a unique login for the estos 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 estos UCServer.
Windows® Domain (also with Active Directory® Server)	Integrated user administration or Active Directory®, Windows® domain authentication. Users must also explicitly log in to the estos UCServer with their domain login.
Windows® domain (all users are logged on to the domain)	Integrated user administration or Active Directory®, Windows® domain authentication. Users are automatically authenticated via their domain login at the estos UCServer.

Authentication with UC password

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

Windows® domain authentication

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 estos 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.

7.3 Events

estos ProCall writes all log files for the estos UCServer server, the contact data replication and the ECSTA to the installation directory under *logs*. You can specify here what type of events should be logged for the estos UCServer server and the contact data replication.

For normal operation, you should leave **Log errors and warnings** set.

If errors occur in the function of the software, the log level must be set to "Debug" until the error has occurred again.

To evaluate the logs for the contact data import and the ECSTAs, the files in the log directory must be opened.

You can activate logging for the ECSTA directly in the configuration of the respective ECSTA.

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

estos 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 understanding 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.

8 Telephony

The telephony setup is explained on the following pages:

- Lines
 - TAPI lines
 - SIP softphone lines
- Location
- Phone journal

8.1 Lines

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

A line usually corresponds to a telephone or a ProCall 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.

estos UCServer supports the connection to a PBX. A table with the released PBXs can be found on the web pages.

With the button "Select telephone system" you can set up the connection to your telephone system to control the telephones via ProCall and/or to use ProCall as softphone.

To control the phones a TAPI or CSTA connection is needed. The ECSTA supplied by estos ProCall can be set up when added. For information on the requirement in your telephone system and how to set up the ECSTA, see "Setting up ECSTA".

Manufacturer supplied TAPI drivers must already be installed on the system. If you add a new driver under Control Panel - Phone and Modem Options, the lines are added here accordingly. With some TAPI drivers a restart of the estos UCServer is necessary for this.

To use the ProCall as a softphone, the connection must be set up via SIP.

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

- TAPI lines
- SIP Lines

8.1.1 TAPI lines

You can set up the connection to your telephone system here and select which extensions are to be made available in the network.

The connection to the telephone system is displayed as "Line group". If an ECSTA is set up, you can select "Configure driver" in the context menu of the line group to enter the connection data to your telephone systems.

If the TAPI driver of the manufacturer is used, the setup is done via the Windows® control panel "Phone and Modem".

After successful connection and line setup in the TAPI driver, the lines are displayed under the line group. For information on setting up a supplied ECSTA for your telephone system, please refer to Connecting the telephone system via ECSTA.

Line group properties

The properties of the line group apply for all lines of the group. To display the properties of the group,

highlight the group and select *Properties* in the context menu. The configuration options are explained in line group properties for TAPI drivers.




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 estos UCServer. Then the line can be used and users can be added.
- **Trunk line**
This line is treated specifically in estos 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**
estos 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 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 shows detailed information on the status icon in case of an 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.

8.1.1.1 *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.)
- **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.

Characteristics of the line group - CTI functions

Here, you can configure extended settings for certain CTI functions.

- **Activate/deactivate CTI functions:**
Certain CTI features can be activated, or deactivated, from here. For example, features not properly supported by the telephone system can be hidden.
-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.

Characteristics of the line group - CTI feature codes

Here, you can configure extended 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 estos ProCall 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 menu and a code dialed on the telephone system as soon as the user has clicked on the feature code.
- **Pickup feature 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 estos 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.

8.1.2 SIP Softphone Lines

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

Add and configure new lines

The connection to the telephone system is displayed as "Line Group". In the Context menu of the line group you can choose "Settings" to enter the connection data for your telephone system. After successfully establishing a connection and setting up the lines, the lines will be displayed under the line group. For information about setting up the SIP connection for your telephone system, please consult the instructions on the web pages at Connection Instructions for Telephone Systems.

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.
- **Registrar/IP Address** (of the PBX)
Please enter here the FQDN or the IP address of the PBX registrar. Enter the port number (typically e.g. 5060). The UCServer requires access via LAN using a local IP address of the PBX registrar. The registrar is also be used as proxy.
- **Domain**
Some telephone systems require a distinction between Registrar and Domain. In this case, deactivate the *Apply Registrar as Login Domain* field and enter the desired value in the *Domain* field. This menu item is only available for specified telephone systems (e.g., SIP Provider).
- **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 equal or greater than the related configuration at the PBX registrar. A value too small may lead to registration problems. In case of the PBX registrar responds with a different value during the registration process, it is being used by the UCServer automatically.
- **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.
- **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).

Softphone registrations

Softphone registrations at the PBX correspond to the Softphone lines in UCServer.

- **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.

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.

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.

Activation of the 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.

8.1.2.1 Line group properties for SIP softphone

Lines are combined into groups. The properties of a 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 or on Call Protection**
If no client is logged into UCServer or the line is set to *Do Not Disturb (DND)*, calls are automatically answered server-side. This option offers a choice of SIP responses for the UCServer to 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 applies only when no call forwarding of the type "Forward calls on logged off ProCall" is set for the called line at the ProCall client and when no administrative call forwarding is assigned.

- **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

- **Group location**
The dialing and call number rules defined under "Location" for SIPAV are applied for this line group.

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 estos ProCall 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 ProCall 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 ProCall pickup function will open a softphone conversation window to carry out the pickup conversation.

Line group properties - Media

Here is where you can configure advanced media settings for softphones. UCServer includes a media server, which is connected to the PBX on one side and to the ProCall client on the other side. The media server is used to convert data (media streams) into the correct format (e.g. codecs, encryption). Active audio codecs are listed at the top based on their priority, if more than one codec should be provided. To change the priority of a selected codec, change its order using the appropriate keys.

This setting is available depending on the connected telephone system and should only be changed after consulting with the estos ProCall Support.

- **Audio codecs - PBX direction**
Codec priority should correspond to the settings in the PBX. PBXs typically offer at least one G.711 codec (default, aLaw or uLaw variant). G.711 has a constant bit rate of 64 kBit / s and provides good call quality. The uLaw variant is generally preferred by the PBX in North America and Japan, and aLaw is generally preferred in the rest of the world.

- **Audio codecs - WebRTC direction**

The ProCall client normally communicates with the media server in a WebRTC-compatible format (e.g. encryption via DTLS-SRTP).

The media server requires the least computing power when the same setting (e.g. 'G.711 aLaw') is used to the PBX and correspondingly towards the WebRTC (i.e. to the ProCall client).

- **Media Port range (min/max)**

The Media Server automatically occupies free ports of the system from the entire range between 1024 and 65535 for the media streams (internal default setting). However, in some cases it is necessary to restrict the range. The entered value range is valid for all Softphone line groups in UCServer and for all connected Windows® ProCall clients. For these clients, the Media Port range is also valid for other WebRTC based services such as audio/video chat and screen sharing.

8.2 Initial Location Setup

The location settings are used to enable the right dialing 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.

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 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 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 ProCall. 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.

Extension phone number format

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.

8.3 Location

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

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

Open the "Default" location and configure the connection to the telephone system or the exchange access.

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.

8.3.1 PBX system

The location settings enable error-free dialing and display of phone numbers.

Only correct location settings ensure that external phone numbers can be dialed and phone numbers are displayed correctly.

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 number 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

8.3.1.1 Dialing prefixes

The signaling of the phone numbers for TAPI and SIP connections may differ. Enter the exchange codes for both connections and define the required formatting.

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 ProCall 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.
- **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.

8.3.1.2 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 access code from phone 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 access code in case of ConnectedID:

- **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.**

8.3.1.3 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.

➔	<p>Specific Examples for the Use of Special External Rules:</p> <ul style="list-style-type: none"> • 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).
➔	<p>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.</p>

8.3.1.4 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 system. 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.

	<p>Specific Examples for the Use of Special Internal Rules:</p> <ul style="list-style-type: none"> • 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.
	<p>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.</p>
	<p>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 ProCall, given a corresponding configuration in the Advanced Location Settings.</p>

8.3.1.5 Emergency numbers



	<p>The rules for emergency numbers are applied exclusively to softphone lines.</p>
	<p>The phone numbers defined here are not subject to any further dialing rules.</p>

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 ProCall 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 ProCall 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!

8.3.2 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.

8.3.3 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.

Information about current rates of Call-by-Call providers can be found on the internet under www.estos.de/produkte/unified-communications/procall4plusenterprise/lcr.html.

- **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.

8.3.3.1 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.

Examply for Germany

Provider	Pre-selection network prefix
Arcor	01070
Tele2	01013

8.3.3.2 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.

8.3.3.3 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.

8.3.4 Advanced

Core services

Phone number format, PC dialing

This option determines the phone number format for outgoing calls. Phone numbers are transferred 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 enter the area code for local phone numbers.

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.

8.3.5 Projects

estos 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 estos 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 'o' and a further external dialing code which is '8o'. Create an entry and name it 'External2'. Enter '8o' 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#eeeeeeee#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.

8.3.6 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.

8.3.7 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.

8.3.7.1 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.

8.3.7.2 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 a 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:

- o the phone number to be dialed involves a special external or an internal phone number
- o 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

Prefixing the phone number with an exclamation point ! will avoid the use of dialing rules. The phone number will then only be transferred directly to the telephone system driver without any formatting.

8.3.7.3 Telephone number formats

Supercanonical number

A phone number format which allows the unique international identification of the participant. The estos UCServer and estos ProCall 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 estos 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 estos ProCall 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

8.4 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.

8.4.1.1 Journal

The journal gathers all telephone events in one database. You can make settings here for how long specified entries will remain stored in the database, before they are deleted.

- **Permanently Keep Journal Records**
Activate this option, if you do not want to delete any journal entries for calls (internal and external).
- **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.

9 User management

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

- Global settings
- Profile
- Groups
- User
- Computer

9.1 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 estos UCServer . It corresponds to the Windows® login name if Active Directory® is being used.
Identity	Identity of the user, with which he can be unambiguously addressed. The address of the identity ideally corresponds to the email address of the user.
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	The "Default" profile is displayed here. If settings have been made at Profiles, those settings are valid.
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 active	User profile is active. The user can log on and use estos UCServer services.

Telephone numbers

The telephone numbers of a user are displayed as call numbers of his contact. estos UCServer searches the lines to the call numbers when loading user accounts. The user automatically gets the lines that belong to him without further configuration.

In the case of an integrated user administration, the telephone numbers of a user must be entered in the supercanonical format. Call numbers from the Active Directory® are displayed here as they are stored in the Active Directory®. When loading user accounts in estos UCServer, these are converted into supercanonical notation.

Regardless of whether the users are created in the Active Directory® or locally, a line set up under "Lines" can be assigned to the user via the "Browse button".

Field	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).

Contact address

The contact address shows all relevant contact details of the user. These are visible for estos UCServer users (depending on 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 estos ProCall. 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.

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
Start chat	If this option is activated the user may send text messages to other users.

Softphone, AudioChat	If this option is enabled, the user is allowed to make softphone calls and audio chats with other users.
Softphone, audio/video chat	If this option is enabled, the user is allowed to make softphone calls, audio chats and video chats 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 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 estos ProCall settings whether they want to use this feature.
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.

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.

The user can also change this setting via the authorization levels in estos ProCall.

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.

9.2 Groups

User groups are used to group users and for granting mutual rights.

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
Start chat	If this option is activated the user may send text messages to other users.
Softphone, audio chat	If this option is activated, the user is allowed to use audio chat and softphone with other users.
Softphone, audio/video chat	If this option is activated, the user is allowed to use softphone, audio chat and video chat with other users.
Accept screen sharing requests	If this option has been enabled, the group users may only use screen 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.
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.
The group's journal will be visible to the group leader.	If this 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	If this option is activated, all members can view the journal of all group

be visible to the whole group.	members, except calls marked as "private".
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.

Members

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

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.

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 ProCall) of the registered group are shown automatically in a "ProCall 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.

9.3 Computer

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

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 estos 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 ProCall 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 estos ProCall 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 ProCall. If more detailed information is desired, open the Properties dialog for the computer and switch to the Status tab page.

9.4 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 estos ProCall version or update service software version.

9.5 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 an authorization is granted for global rights, it applies for all system users. These rights are configured exclusively by the administrator.
- **User rights.** 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.

9.6 Profile

The profile consists of a list of optional settings for the users and is assigned to each user object. Hence, the settings are valid for all users. These settings are loaded from estos ProCall by the server and applied. If a setting is defined in the profile, this setting is write-protected in estos ProCall.

Fax

In this area the fax client side integration for estos ProCall can be configured. By entering the fax domain at "Exchange Gateway", the fax messages received as e-mail at estos ProCall can be displayed in the speech bubble.



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

9.7 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 all users the following rights against each other

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
Softphone, audio chat	If this option is activated, the user is allowed to use audio chat and softphone with other users.
Softphone, audio/video chat	If this option is activated, the user is allowed to use softphone, audio chat and video chat with other users.
Enable screen sharing rights via federation	If this option is set the screen sharing rights specified by the administrator 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.
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.
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.
Share contents	If this option is activated, users can transfer files in the chat. The service must be set up under Services – Share Content.

10 Services

The setup of the different services of the estos UCServer is described on the following pages:

- Update server
- E-Mail dispatch
- Share contents
- Push notifications

10.1 Update server

estos 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 the estos UCServer the current client is copied to the *ClientInstall* directory. If a new client is to be distributed, the msi package must be copied to the folder. The directory is monitored by the server for changes, which means you do not have to restart the server if you want to provide new installation packages. Just copy the packages into the directory, they will be detected and offered automatically.

In the administrator you can see the settings for the update server and the available installation packages. The most important settings:

- **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.
- **Available packages 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.

10.2 E-Mail dispatch

estos 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 addresses 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.

10.3 Share content

To be able to use the "Share contents" feature and thereby to enable users to transfer files in the chat, make the following configuration settings.

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
	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 users to be able to use the "Share Contents" function, this service must be enabled in the Global Settings.

10.4 STUN and TURN Server Settings

estos UCServer make central configuration of STUN and TURN possible for estos ProCall clients. The estos ProCall 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 estos UCServer for that reason. The settings that describe how STUN and TURN servers located on the Internet can be accessed can be made on estos 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).

estos 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.
 - **Using 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. estos 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 estos 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 estos 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 relays media streams between the endpoints 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 symmetric 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.

10.5 Push notifications

Push notifications are required for the use of the mobile apps. When there is an incoming call or message, the estos ProCall sends a push message to the device.

Whether the estos UCServer can establish a connection to the push service is displayed in the menu item "Online services". Under *Push notification diagnosis* a diagnosis can be executed if necessary.

In the list you can see the clients that have signed up 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".

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.

10.6 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.

11 Server status

You will find information about the current status of the estos UCServer on the following pages.

- Status monitor
- Server events

11.1 Status monitor

The status monitor provides an overview of the services and client software connected with the estos UCServer.

Type:	Description:
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.
Active audio/video chats	Number of currently running audio/video and softphone calls.
Active Calls	Number of currently conducted telephone conversations.
Calls on an outside line	Number of currently conducted telephone conversations on an outside line.
Clients	Displays the number of currently logged in ProCall clients, the number of available licenses and the opened port by UCServer for the client log in.
Lines	Number of active lines.
Mobile Access Clients	Number of logged-in and licensed Mobile Clients via estos UCConnect.
UC Media Server	Displays the status of the locally installed UC Media Server. This service must be connected for softphone calls.
UC Web Server	Displays the status of the locally installed UC Web Server for the unencrypted network interface.
UC Web Server SSL	Displays the status of the locally installed UC Web Server for the encrypted network interface.
Update server	Status of the update server.

11.2 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.

Icons used:

	Error
	Warning
	Information
	Debug information

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

12 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.

Change administrator password

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

12.1 Network interfaces


The connection between the software on the workstations and estos UCServer is made via *network interfaces*. The estos 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 conflicts with other software running on the system.
If a port conflict occurs an error event appears in the event log of the estos UCServer.

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

Using the button **Add** a new network interface can be created.

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

Using the button **Properties** the configuration of a network interface can be changed.

12.2 Certificate

To increase security, the data traffic between estos UCServer and estos ProCall 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 estos 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 estos ProCall

- **Allow secure data transmission using TLS**
If the TLS/SSL encrypting is activated, encrypted and unencrypted programmes in the estos UCServer can be combined.
estos ProCall 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 estos UCServer can be rejected.

Certificate for SSL/TLS communication with estos ProCall

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 ProCall 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.

12.3 Online services

UCConnect is estos's own platform for the cloud, which also provides online services for estos ProCall. Since the license for estos ProCall is stored in estos UCConnect, UCServer needs a permanent connection to UCConnect.

Online Services also allows you to use the ProCall Mobile Apps, provided you have a valid service agreement. 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.

The online service means that the access required for ProCall Mobile to the UCServer from the Internet and STUN and TURN servers for the use of audio and video chat is provided.

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


ProCall Mobile Service

Source	UCServer and all ProCall clients
Source port	All
Destination	*.ucconnect.de
Port	3478 and 443, UDP and TCP

Connection

Es wird angezeigt ob der UCServer mit UCConnect verbunden ist und welche Services verfügbar sind.

The login data for UCConnect were specified during installation. If these are to be changed, you must log out of UCConnect and log in again. If an "alias" is stored in UCConnect, it will be entered automatically during a new logon.

 The server ID or "alias" is required for the apps to log in to UCConnect. You should define a simple alias and inform the users.

The **Services** and **Licenses** tables display the licenses stored in UCConnect.

Using the button under the **Services** table, you can activate, set up and invite users to use ProCall Mobile using a wizard.

12.4 Advanced

Telefonanlagen unterstützen unterschiedliche Optionen und Funktionen. Abhängig von der angebotenen Telefonanlage können nachfolgende Funktionen/Optionen beeinflusst werden. Es werden Ihnen nur die Möglichkeiten angeboten, die von der Telefonanlage und dem ECSTA unterstützt werden.

12.4.1.1 Alcatel OXO Connect

- **Snapshot for active calls**
The driver can validate existing calls. This prevents that calls are displayed on the PC that do no more exist in the PBX system.
Enter a time interval in seconds.
The higher this value, the longer it can take for the driver to detect a false call. The lower this value, the higher the load on the telephone system.
- **Emulate blind transfer**
If the PBX system does not offer blind transfer the driver can emulate this feature. The driver will setup a consultation transfer which is merged as soon as the called destination is rings.
- **Blind transfer timeout**
Timeout for the blind transfer emulation. The consultation call must be answered within this timeout. Otherwise the consultation call is canceled and the initial call is retrieved.
- **Rules for detecting SIP lines**
Choosing "Edit Rules" takes you to a dialog box that allows you to specify whether SIP lines should be detected by the ECSTA automatically or via a set of rules, filtered out and thus forwarded to the TAPI's line management or not. When automatically filtering out SIP lines, all lines that have been configured in the system for the "SIP" device type are filtered out. When filtering out SIP lines via a set of rules, the administrator must create a set of rules (see set of rules for filtering out SIP lines) for the phone numbers, names or IDs that determine which lines are filtered out.
- **Snapshot for active calls**
The driver checks in the given time interval whether the currently displayed calls still exist in the telephone system
You can enter a time interval in seconds here.
- **Retry MonitorStart**
In the event that the driver cannot start monitoring an extension because, for example, the extension has not been connected to the PBX, the driver will attempt to start monitoring at periodic intervals.
Enter a time interval in seconds.

12.4.1.2 Avaya IP Office Connect

- **Back to the held contact when ending a consultation call**
When ending a consultation call, you can select whether the held call party should be reconnected automatically or remain on hold.
- **Rules for detecting SIP lines**
Choosing "Edit rules" takes you to a dialog box that allows you to specify whether SIP lines should be detected by the ECSTA via a set of rules, filtered out and thus not forwarded to the TAPI's line management (see set of rules for filtering out SIP lines).
- **Format line names**
The TAPI line names can be changed by this setting.
Default = Line number / Name
Call number = line number
Name = Name
- **Snapshot for active calls**
The driver checks in the given time interval whether the currently displayed calls still exist in the telephone system
You can enter a time interval in seconds here.

12.4.1.3 Mitel MiVoice Office 400

- Back to the held contact when ending a consultation call
When ending a consultation call, you can select whether the held call party should be reconnected automatically or remain on hold.
- Rules for detecting SIP lines
Choosing "Edit Rules" takes you to a dialog box that allows you to specify whether SIP lines should be detected by the ECSTA automatically or via a set of rules, filtered out and thus forwarded to the TAPI's line management or not. When automatically filtering out SIP lines, all lines that have been configured in the system for the "SIP" device type are filtered out. When filtering out SIP lines via a set of rules, the administrator must create a set of rules (see set of rules for filtering out SIP lines) for the phone numbers, names or IDs that determine which lines are filtered out.
- Phone Number Format
You can use rules to change the phone numbers that are reported by the driver to the application. You can also change the phone numbers that are sent from the PC to the telephone system.
- Format line names
The TAPI line names can be changed by this setting.
Default = Line number / Name
Call number = line number
Name = Name
- Snapshot for active calls
With the given interval, the driver checks whether the currently displayed calls still exist in the telephone system. Enter a time interval in seconds.

12.4.1.4 Panasonic

- Readout line names
If this option is active, the names of the telephones from the telephone system are requested.
- Read active lines only
Only lines on which a telephone is in operation are read.
- Snapshot for active calls
With the given interval, the driver checks whether the currently displayed calls still exist in the telephone system. Enter a time interval in seconds.
- Retry MonitorStart
In the event that the driver cannot start monitoring an extension because, for example, the extension has not been connected to the PBX, the driver will attempt to start monitoring at periodic intervals. Enter a time interval in seconds.

12.4.1.5 Unify OpenScape Business

- Feature Code FlexCall
The feature code configured in the telephone system for the FlexCall function is entered here. This is used for the CLIP No Screening feature. CLIP No Screening only allows you to set other extension numbers within the company. You cannot use this to transfer any number to the exchange.
- Report incoming calls on busy extension
If call waiting is not configured for subscribers in the telephone system, the driver can still signal a short incoming call on these lines. The user can thus recognize that he has been called.

- Offer CLIP no screening
If this option is active, the driver can transfer an individual phone number with outgoing calls. See also Feature Code FlexCall.
- Recognition of existing calls
If enabled, the phone system can recognize existing call while opening the line. Please note that not all call parameters are discovered!
- Fees
The charge multiplier allows you to adjust the charge information reported by the PBX to the driver.
- Rules for detecting SIP lines
With "Edit rules" you get to a dialog where you can define if SIP lines should be detected by ECSTA via a set of rules, filtered out and thus not forwarded to the line management of Tapi (See set of rules for filtering out SIP lines).
- Snapshot for active calls
The driver can validate existing calls. This prevents that calls are displayed on the PC that do no more exist in the PBX system.
Enter a time interval in seconds.
The higher this value, the longer it can take for the driver to detect a false call. The lower this value, the higher the load on the telephone system.
- Retry MonitorStart
In the event that the driver cannot start monitoring an extension because, for example, the extension has not been connected to the PBX, the driver will attempt to start monitoring at periodic intervals.
Enter a time interval in seconds.

12.5 Connection

The information for connecting the telephone system must be specified. Enter the IP address of the telephone system and specify the port. Depending on the telephone system, you must enter further details:

Option	Description
Encryption	If an encrypted connection is supported by the telephone system, it can be activated
Login	If the ECSTA has to log on to the telephone system, enter the user data of the user who has been set up in the telephone system for CSTA access. If multiple interfaces are supported, you can select which interface should be used to access the telephone system.

12.6 Info

Hier werden die Informationen zur installierten Version und dem angebunden Telefonsystem ausgegeben.

The log for the ECSTA can be activated under "Diagnostics". A log file is created for each line in which, among other things, the signaling on the line is logged. In addition, a "General_xxx.log" and an "asndata_XXX.log" are created.


The "General_xxx.log" contains messages concerning the driver, e.g. connection status and access to the lines.

The "asndata_XXX.log" contains information about the interface and is only interesting for the inspection by the support.

12.7 Lines

Once the connection to the telephone system has been established, the lines available in the telephone system can be entered in ECSTA.

Depending on the telephone system, different options are available for this:

Option	Description
Manual input	The "Add" button can be used to enter the phone numbers (extension) of the phones as well as a name.
Load Lines	This option is recommended. Start the process from the "Extras" menu. The available lines are determined automatically from the telephone system. Options for reading out the lines can be set in a separate dialog.
Import lines	Using the "Extras" menu, you can import a list of lines from a text file. The file must start with the phone number in each line. Optionally, the name can also be included, separated by commas.
	After setting up the driver, the lines may not be available until the PC is restarted.

12.8 Set up ECSTA

The configuration of the ECSTA is started when a telephone system is added and can be opened at any time in the UCServer management interface. To do this, select "Configure driver" in the context menu of the line group to open the configuration interface of the ECSTA.

The configuration of the ECSTA contains the following menu items:

- Connection: Enter the connection and login data for the telephone system.
- Lines: Readout/entry of the telephone lines to be monitored
- Advanced: Editing of telephone system specific settings
- Info: Information about ECSTA and log setting

To ensure error-free operation, please observe the settings required in the telephone system:

- Alcatel-Lucent OXO Connect
- Avaya IP Office Connect
- Mitel MiVoice Office 400
- Panasonic KX-, NS Series
- Unify OpenScape Business

12.9 Connecting the telephone system via ECSTA

To operate this software a TAPI or CSTA driver for your telephone system is necessary if you want to control your telephone.

A TAPI driver is a system component made available by the manufacturer of your telephone system or another provider (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.

With estos ProCall a CSTA driver is supplied for some telephone systems which communicates with the CSTA interface of the telephone system. The setup of the connection to the respective telephone system as well as the requirements in the telephone system for the use of the CSTA driver differ from manufacturer to manufacturer. For the drivers supplied with estos ProCall, please refer to the notes for your telephone system:

- Alcatel-Lucent OXO Connect
- Avaya IP Office Connect
- Mitel MiVoice Office 400
- Panasonic KX-, NS-Serie
- Unify OpenScape Business

For instructions on setting up ECSTA, see [Setting up ECSTA](#).



estos ProCall supports connection to a telephone system and hence the creation of an instance.

13 Set of rules for filtering out SIP lines

You can enter rules that determine whether lines should be filtered out during readout or not. If "no detection of SIP lines" is selected, all read-in lines will be included in the line management. If "Rules for recognizing SIP lines" is selected, a set of rules is applied when the lines are read in, which determines whether a line should be included in the line management or not. This set of rules consists of individual entries created by the user.

Each entry has one of four possible entry types and a corresponding string to search for. The following entries for a rule are possible:

- **String in name**
When lines are read in, only those lines are included in the line management whose line name does not contain the character string entered in the "Search for:" column.
Example:

- **String in the phone number**
When lines are read in, only those lines are included in the line management whose phone number does not contain the string entered in the "Search for:" column.
Example:

- **Regular expression in name**
The string in the "Search for:" column must be a regular expression. When the lines are read in, only the lines for which the search using the regular expression in the line name was unsuccessful are included in the line management.
Example:

- **Regular expression in the call number**
The string in the "Search for:" column must be a regular expression. When lines are read in, only those lines are included in the line management for which the search using the regular expression in the phone number was unsuccessful.
Example:

Here is a short overview of the syntax of regular expressions:

String	Description
^	The beginning of the phone number or name. The regular expression "^o" or the regular expression "^Max" finds the search character 'o' or the search string "Max" only at the beginning of the phone number or name.
\$	The dollar sign (\$) indicates the end of the phone number or name. The regular expression "152\$" finds the string "152" only at the end of the phone number or name.
	The () character allows both characters between which it is located. The expression "8 9" allows '8'

	or 'g'.
.	The dot (.) allows any character (or any digit).
*	The asterisk (*) indicates that the character to its left must be present 0 times or more.
+	The Plus sign (+) is similar to the asterisk, only the character to the left must be present at least once.
?	The question mark (?) indicates that the character to the left must be present 0 or 1 times.
[]	The square brackets ([and]) signal a set of characters that are allowed at this point.

Check:

You can directly check your set of rules in the "Rules for detecting SIP lines" dialog box. Enter a character string in the Search Text field that you want to test with the set of rules. In the "Detected as SIP line:" field, you can see whether a rule for filtering was successfully applied to the search text.


See also Advanced Settings.

13.1 Set up telephone system

The setup of the connection to the respective telephone system as well as the prerequisite in the telephone system for the use of the CSTA driver differ from manufacturer to manufacturer. For the drivers supplied with estos ProCall, please refer to the notes for your telephone system:

- Alcatel-Lucent OXO Connect
- Avaya IP Office Connect
- Mitel MiVoice Office 400
- Panasonic KX-, NS-Serie
- Unify OpenScape Business

For instructions on setting up ECSTA, see Setting up ECSTA.


estos ProCall supports the connection to a telephone system and thus the creation of an instance

14 Installation of Clients

After the installation of the estos UCServer, the estos ProCall 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 estos 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 estos 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

14.1 Installation at the workplace

For the installation on the PC, the MSI file has to be double clicked. Then the Windows® installer starts and guides through the installation process. During that process, different information is shown to the user and options are offered for the configuration. They are explained here:

	The estos client TAPI driver for dialing from third party applications via a phone is automatically installed as well.
---	--

Version Information

The exact version number is displayed on the homepage.

If estos ProCall is installed on a 64-bit operating system, a note is displayed here on this page that the 64-bit variations of the TAPI driver have to be installed.

License

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

Connection to the server

The server with which the estos ProCall should connect to is entered here.

The server name or its IP address must be entered in the input field.

The server can be searched for and selected in the local network with **Search server....** The list displayed contains the following information about the servers found:

Computer name	The computer name of the server
Version	Information about the installed version of the estos UCServer

After the final entry of the target folder for the program installation, the software is installed and the installation is completed.
Tick to open the base configuration.

14.2 Installation using group policies

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

12. 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. `msiexec /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 estos UCServer.
 13. 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.

14.3 MSI description

The workstation software for estos ProCall 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 ProCall_de-DE.msi /q CTISERVER=ctiserver.mydomain.de`
- Default installation with client TSP, basic user interface, hostname is `ctiserver.mydomain.de`
`msiexec.exe /i ProCall_de-DE.msi /qb CTISERVER=ctiserver.mydomain.de CLIENTTSP=edial`
- Prepare administrative installation for distribution with group policy
`msiexec.exe /a ProCall_de-DE.msi`
- De-installation
`msiexec.exe /x ProCall_de-DE.msi`

Special MSI properties

All of the following properties are listed in `AdminProperties` and thus also available for an administrative installation.

Property	Value	Description
CTISERVER		Hostname or IP address of the server
CTISERVERUSEDNS		DNS Service Location Record Option
	0	Disabled - 'CTISERVER' is used (default)
	1	Enabled - Use DNS, 'CTISERVER' will be ignored
CLIENTCTIMAIN		Install ProCall application
	0	Do not install ProCall UI application, only the advanced Remote Tapi driver will be installed
	1	Install ProCall application as normal (default)
CLIENTTSP		Which Tapi driver is being installed
	none	Do not install a Tapi driver
	edial	Install the client Tapi driver (default)
	eclient	Install enhanced remote Tapi driver
OUTLOOKADDIN		Install Outlook® AddIn
	0	Do not install Outlook® AddIn
	1	Install Outlook® AddIn (default)
ACUSERVICE		The service for automatic updates is installed
	0	Do not install service for automatic updates
	1	Install service for automatic updates (default)

14.4 Software distribution

Software distribution

estos UCServer provides central software distribution. With software distribution the administrator can install estos ProCall on the workstations automatically and centrally from the server after the estos 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 estos 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 - Overview 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 deinstallation 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, estos 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.

Update service

The estos 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.

14.5 Update service

The update service is installed at the workstation with estos ProCall.

This system service checks regularly whether a new version of estos ProCall is available on the estos UCServer. If a new version 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.
- **EInSet.exe**
Auxiliary application which installs the update.
- **EInProg.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.

14.6 Active Directory® Objects

By default, replication of the Active Directory® objects will be restricted to 2000 objects in estos 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 estos 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 estos UCServer indicates a potential excess in the server status, the restrictions implemented in estos 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

15 Technical notes

Information about details and special topics are summarized in this section, referenced from other help pages.

- Telephone number formats
- Contact search
- User rights
- User Authentication
- Server certificate
- TAPI-driver
- Configuration files
- User database import and export
- SIP Response Codes
- SIP PCAP log files
- Active Directory® objects

15.1 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>oFG</LongDistanceRule>
<InternationalRule>ooEFG</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* 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 dialing prefix (? is a place-holder 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 <i>countries.xml</i>
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

15.2 Contact search

With an incoming or outgoing call, estos ProCall 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. estos UCServer searches for a suitable contact and presents them to the client. estos ProCall searches in client-side connected data sources and expands the individual contact into a list of contacts. After the search is complete, estos ProCall 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 estos 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
 - estos MetaDirectory Phonebooks

- Contact search in estos ProCall:

The client searches asynchronously for a contact. The call window is initially displayed with the contact found on the server.

15.3 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 than 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

15.4 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 an authorization is granted for global rights, it applies for all system users. These rights are configured exclusively by the administrator.
- **User rights.** 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)	The other user may see who the user is currently calling with

line)	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.

15.5 User Authentication

The user login on the estos UCServer requires authentication. 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 administration, 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 estos 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 administration, UC password

The user names come from the integrated user database. Only users who are configured in the estos 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 administration, domain authentication

The user names come from the integrated user database. Only users who are configured in the estos UCServer can log on. The users are authenticated either implicitly or explicitly via NTLM directly on the estos UCServer. The user's password is not transmitted over the network under any circumstances.

16 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".

16.1 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

16.2 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 appointments marked as private from the calendar, if the user has released his		x with the indication "Private	x with the indication "Private	X with subject and place

		appointments. This right should be set only in the case of special positions of trust.				
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	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	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 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			X	X

		special positions of trust.				
	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 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 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	

16.3 Configure user account yourself

Users are allowed to configure their user account themselves

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	X	X

phones		
Contact address / Image	-	X

²Can be edited by the user if Active Directory® write access has been configured.

16.4 Automatic line binding

The phone numbers configured in the user account are automatically used by the estos 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.

16.5 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 storage

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**.

16.6 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:

16.7 Configuration files

All important parts of the estos 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
<i>config</i>	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.
<i>config/default</i>	Configuration files which were installed with the product. These are overwritten if the product is updated.
<i>config/users</i>	Settings for users for file-based estos UCServer user management
<i>config/computers</i>	Settings for the computers with estos UCServer user administration
<i>templates</i>	You should save files you have changed in this directory if you wish to change one of the files supplied in templates/default
<i>templates/default</i>	Configuration files which were installed with the product. These are overwritten if the product is updated.
<i>database</i>	All databases created by estos UCServer using MS Access databases (default path). User database in case of SQL supported user administration (view User data base).

16.8 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.

16.9 SIP Softphone(s)

Many telephone systems (PBXs) make the operation of telephones possible that have been implemented according to the SIP standard. estos UCServer supports the central integration of such telephone systems. This integration allows estos ProCall client users to use their PCs as softphones in order to make telephone calls through the telephone system. To do this, the ProCall 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 ProCall 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 ProCall 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 ProCall 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.

The media server provides the G.711 (PCMU, PCMA) audio codecs in the direction of the PBX. In the direction of the ProCall clients, Opus is generally used. This also provides good audio quality using little LAN/WAN bandwidth. By encrypting according to the DTLS/SRTP procedure, the media server uses the highest security standard that is currently normal in VoIP products.

Availability on the internet via the Media Server is achieved by using the estos "UCConnect" services.

16.10 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

16.11 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. estos UCServer allows you to collect SIP softphone signaling network data in PCAP files. Since PCAP log files are created in estos 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.

Icon	Statement
●	Line group is PCAP log activated.

17 Info about estos UCServer

estos UCServer is a product of estos GmbH.

Copyright (C) 2022 estos GmbH.

For product updates visit <https://www.estos.de/>

Frequently asked questions and answers and also support are available at <https://support.estos.de>

Active Directory® is either a registered trademark or trademark of Microsoft Corporation in the United States 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.