estos SIP Proxy

6.2.0.1055

1 Welcome to estos SIP Proxy

SIP Proxy makes the operation of several estos UCServers in the same SIP presence domain possible. This ability can be used to run UCServer at various sites or for load distribution. SIP Proxy will guarantee the connections between the various UCServers and the federation.

This help system will guide you through the installation and configuration process for estos SIP Proxy.

- Conditions relating to the operating system System Requirements.
- The network settings will be described on the Network Interface Configuration page.
- Configuration of the estos UCServer server connected to the SIP Proxys will be described in the UCUCServeronnection Configuration section.
- You will learn how to configure the federation from Federation Configuration.
- Static Routing Configuration will explain how to configure static routes.
- Starting and stopping the SIP Proxy service will be explained by Service Configuration.
- Contact information for the support department can be found in the Product Support Information section.
- Technical background information can be found under the headings: About Federation, about Creating DNS Service Resource Records and Server Certificates necessary for the federation in this help file.

The help system can be access at any time from the **Help** menu option on the SIP Proxy program window. As a rule, the help page for the topic corresponding to the feature you are using will be opened automatically.

In Help the following icons are used:

Icon	Meaning
	Note
	Warning, caution

1.1 System requirements

Supported operating systems for estos SIP Proxy:

- Windows® 7 SP1
- Windows® 8.1
- Windows® 10
- Windows Server® 2008 R2 SP1
- Windows Server® 2012
- Windows Server® 2012 R2
- Windows Server® 2016

	List is just a selection and there is no warranty of accuracy or completeness.
	Actual and complete versions are available on our Website.

1.2 WAN Settings

Configuration of network interfaces which are used for incoming connections.

- **Certificate**
  To use the secured TLS or MTLS network protocols, you will need a server certificate. This certificate must have been signed by a certification authority. Click on the "Certificate..." button to open a window for selecting a certificate. Then, select the appropriate certificate and confirm it by clicking the OK button. Information about the selected server certificate will then be displayed.

- **Use other public address**
  Activates, or deactivates, the use of the public IP address. This feature should be activated, when your server has connected with the public Internet through Network Address Translation (NAT) routing.

  - **Port / IP**
    Displays the port number and the IP address that should be sued as the public address. If you do not know your public address, click the Detect IP Address button. It will discover the appropriate IP address and make the corresponding entry.

  - **Detect IP**
    Click this button when you want the system to determine the IP address automatically for public address usage.

1.3 Network interfaces

1.3.1 List of the network interfaces

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

- **Activate**
  Activates or deactivates the network interface. You can carry out this setting directly. Click on the checkbox to activate the network interface. Click again on the checkbox to deactivate the network interface. If the network interface is deactivated, the checkbox is empty.

- **IP**
  Displays the IP address for the network interface. Together with the indicated port number, this setting uniquely identifies the interface. To change the IP address for the network interface, select the interface and then click on the Properties...button.

- **Port**
  Displays the port number for the network interface. The port number and IP address identify the interface uniquely. To change the port number for the network interface, select the interface and then click Properties... button.

- **Log**
  Displays the transport protocol of the network interface. Different protocols for network interfaces can be selected.
  - UDP (User Datagram Protokoll)
  - TCP (Transmission Control Protocol)
  - TLS (Transport Layer Security)
  - MTLS (Mutual Transport Layer Security)

  To change the type of protocol for a network interface, select the interface and then click on the Properties... button. For secured network protocols, you will also require a server certificate for using

secured network interfaces. Further information regarding certificates can be found under Server Certificates.

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

1.3.2 Configuration of network interfaces

You can configure the list of network interfaces. Click the Add... button to add another network interface to the list. Click the Delete button to remove one or more network interfaces for your list. Click the Properties... button to display the properties for the network interface and to make adjustments to that network interface.

- **Add...**
  Click this button to add another network interface to the list. A new dialog will be opened, from which you can set the properties for the new network interface. Further information about network interface properties and how to set them can be found in the Network Interface List section.

- **Remove**
  Click on this button to remove network interfaces from your list. You can only do this if at least one network interface was marked on the list. A message dialog will then request that you confirm the removal of the network interface you selected. Click the OK button to confirm the deletion. Click the Cancel button to stop the removal process.

- **Properties...**
  Click on this button to display the properties and details of a network interface. You must select only one network interface on the list. You can also modify the network interface properties. Further information about network interface properites and how to adjust them (as needed) can be found in the Network Interface List section.

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

1.4 Network Interface Configuration

- **IP Address**
  Select the IP address that you would like to use for incoming connections from the list of available IP addresses. You may only select addresses that appear in the list. The selection options are determined by your system settings.

- **Port number**
  Enter the port number that you would like to use for incoming connections. The port number may be any value between 0 and 65535. Many SIP servers use Port 5060 over TCP or 5061 over TLS.

- **Log**
  Select the transport protocol that you would like to use for incoming connections. The following transport protocols may be used:
  - UDP (User Datagram Protocol)
  - TCP (Transmission Control Protocol)
  - TLS (Transport Layer Security)
  - MTLS (Mutual Transport Layer Security)

  For using the MTLS protocol, you will need a server certificate issued for your system. The server certificate must have been issued by a reliable certification authority. You can select an appropriate certificate from Network Settings.

⚠	Please note that UDP and TCP are unencrypted protocols, which have not been secured against

	eavesdropping. Using these protocols only in a local area network is recommended. The UDP protocol is not recommended because of the maximum packet size of 65,535 bytes.

-

1.5 SSL/TLS Communications Certificate

Selected Certificates Property List

Subject Name	The Signatory or Certificate Purposes entries must be fully qualified domain names (FQDNs).
Issuer	Source of the certificate
Valid From / Until	Time duration for the certificate

Choose certificate...
Click this button to select a certificate. A new dialog will be opened, from which you can select the certificate. Once selected, click the OK button to accept the selection. Click the Cancel button to reject the selection.

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

1.6 LAN Settings

Settings for UCServer's connection, which configured your connection to other servers through the SIP proxy service.

- **User name**
  Enter a unique user name that will be required for logging onto the SIP proxy service.

- **Password**
  Enter a unique password here. The entry is optional.

- **Bind to IP address**
  From the list of available network interfaces, select the interface through which UCServer should connect to the SIP proxy service.

- **Port number**
  Enter the number of the port through which UCServer should connect to the SIP proxy service.

- **Transport Protocol**
  Enter the transport protocol which will be used by UCServer. The following options are available:
  - UDP (User Datagram Protokoll)
  - TCP (Transmission Control Protocol)
  - TLS (Transport Layer Security)
  - MTLS (Mutual Transport Layer Security)

  You will need a server certificate for the MTLS protocol. You can specify the certificate from the Network Settings dialog.

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

1.7 Federation

Federations allow internal users to send instant messages and view the presence information of external users. A detailed description of the federation can be found on the page Introduction to federation.

- **Use Federation service**
  This service enables communication between different companies, who use estos UCServer and have all registered with the Federation service. To configure the federation, simply click on the "Configure..." button. A new dialog will be displayed, from which you can modify the Federation settings.

- **Use open federation**
  Connections to other presence domains will be created using standard SIP protocols. The accessibility of other servers will automatically be determined using special DNS service location records, which avoids the need for further configuration. To configure accessibility for your server, simply click on the "Configure..." button. A new dialog will be displayed, from which you can change the Open Federation Settings.

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

1.8 Federation Service Configuration

- **To use this service, you must have registered with the NGN21 Federation service.**

  - **User name**
    Enter your unique user name to login to the federation service here.

  - **Password**
    Enter your unique password, which will be needed for logging onto the Federation service.

  - **Network interface**
    Select the interface with which you would like to connect to the federation service from the list of available network interfaces.

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

1.9 Open Federation Configuration

You will require a valid server certificate, a DNS-SRV record with the public DNS server and a network interface for incoming connections in order to use Open Federation. Further information regarding the specification of a certificate can be found under server certificate.
Information about creating a DNS-SRV record can be found under Creating a DNS Service Resource Record for the Federation.

- **Certificate**
  You will need a server certificate to use Open Federation. This certificate must have been signed by a certificate authority. Click the "Certificate..." button to select a certificate. Select the appropriate certificate and then confirm your selection by clicking the OK button. Additional information about the selected server certificate will then be displayed.

- **With the certificate matching DNS SRV record**

Depending on the selected server certificate an IP address and port number is detected by a DNS request. If nothing is displayed after selecting the certificate the DNS-SRV record may not match the certificate or it may not be present.

- **DNS host IP**
  Returned IP address of the DNS request using a Certificate Subject Name.

- **DNS port**
  Returned port number of the DNS request using a Certificate Subject Name.

- **Network interface for incoming connections**

  Select a network interface that you would like to use for incoming interfaces from the Open Federation. After a network interface has been selected and its subsequent configuration, it will automatically be added to the network interfaces for incoming connections.

  - **Bind to IP address**
    From the list of available network interfaces, select the interface through which servers should connect with the SIP proxy service.

  - **Port**
    Please enter the port number to be used for open federation.

- Public IP address and Network Address Translation (NAT) type automatically determined by the Simple Traversal of User Datagram Protocol (UDP) through NAT (STUN) server. With the help of the STUN server, clients can determine the public IP address and port, which NAT devices shielding the clients use externally and which have been assigned to a certain local port per NAT.
  - **Use the public address**
    Activates, or deactivates, the use of the public IP address. This feature should be activated, when your server has connected with the public Internet through Network Address Translation (NAT) routing.

  - **NAT Type**
    NAT type determined by STUN request

    - **Full Cone**
      Full cone NAT represents all requests from the same internal IP address and port to the same external IP address and port. Furthermore, each external host may send a packet to the internal host, since external addresses are also assigned to internal addresses.

    - **Restricted Cone**
      In contrast to full cone NAT, an external host (using a given IP address) may send a packet only to the internal host, if that internal host has previously sent a packet to that same IP address.

    - **Port Restricted Cone**
      Port restricted cone NAT is similar to restricted cone NAT, however the restriction also includes the port number. In other words, an external host (using a given IP address and given port) may only send a packet to the internal host, if the internal host has previously send a packet to that same combination of IP address and port number.

    - **Symmetric NAT**
      Symmetric NAT is similar to full cone NAT, however different assignments are used when the same host (using the same IP address and port) sends a packet to a

different target. Furthermore, only the external host, which has received a packet, may send a UDP packet back to the internal host.

- **Open Internet**
  NAT will not be used.

- **Firewall blocking UDP**
  UDP packets have been blocked by a firewall.

- **Symmetric UDP Firewall**
  A firewall permits the replacement of the transmission of UDP packets without IP addresses.

- **Unknown**
  An error occurred during the determination of the NAT type.

- **Public IP Address**
  The public IP address determined by STUN request

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

1.10 Partner Domain configuration

From here, you can gather and configure the static routing list, which should be used for outgoing connections.

1.10.1 List of all static routes

- **Use static routes**
  Activate or deactivate the functionality of the static routes included in your list here. If you deactivate "use static routes", all your static routes are deactivated and you can't carry out any adaptations in your existing configuration.

- **Partner Domain configuration**
  Shows the list of the registered and configured static routes. Every line in the list represents a static route with individual settings. The following properties of a static route are displayed.

  - **Activate**
    Activates, or deactivates, the static routing entry. You can change this setting directly. Click the checkbox to enable or disable the static routing entry. Additional information can be found under Static Routing Configuration.

  - **Trustworthy**
    Indicates if the static routing entry has been categorized as reliable. You can change this setting directly. Click the checkbox to enable or disable this categorization. Additional information can be found under Static Routing Configuration.

  - **Domain**
    Displays the domain name that should be used for the static routing entry. The domain name establishes the context for the hierarchical system and must be unique in your displayed list. Additional information can be found under Static Routing Configuration.

  - **Access server**
    Displays the server's IP address used for accessing the domain. This value may also be a symbolic name, which will be converted into an IP address as part of operations. Additional information can be found under Static Routing Configuration.

- **Port**
  Displays the port used by the selected access server. Values between 0 and 65535 may be entered for the port number. Many SIP servers use Port 5060 over TCP or 5061 over TLS. Additional information can be found under Static Routing Configuration.

- **Log**
  Displays the transport protocol for the selected access server. Various protocols are available for static routing. Information regarding transport protocol settings and additional information can be found under Static Routing Configuration.

- **Linked on**
  Displays the selected IP address, if the system has been bound to an IP address. Additional information can be found under Static Routing Configuration.

1.10.2 Configuring static routes

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

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

- **Remove**
  Click on this button to remove static routes from your list. You are only able to carry out the removal, if at least one static route is marked in the list. Afterwards you are asked to confirm the removal. Click on the button "OK" to confirm. Click on the button "Cancel" to abort.

- **Properties...**
  Click on this button to get the properties and details of a static route displayed in another window. You need to have marked exactly one static route on the list to do so.

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

1.10.3 Static Routing Configuration

- **Domain name**
  Displays the domain name that should be used for the static routing entry. The domain name establishes the context for the hierarchical system and must be unique in your displayed list.

- **Access server**
  Shows the IP address of the server under which the domain is accessible. It can also be a symbolic name which was converted into an IP address.

- **Port**
  Enter the port number for the selected access server. Values between 0 and 65535 may be entered for the port number. Many SIP servers use Port 5060 over TCP or 5061 over TLS. The port number and the transport protocol must correspond to a network interface for incoming connections from the access server.

- **Bind to IP address**
  Select the IP address from the list of available IP addresses, which you would like to use for the static

routing entry. You may only select from the entries in the list. The selection options will depend on your system settings.

- **Transport Protocol**
  Choose the transport protocol for the access server. The transport protocol and port number must correspond to a network interface for incoming connections from the access server. The following transport protocols are available for static routing:
  - UDP (User Datagram Protocol)
  - TCP (Transmission Control Protocol)
  - TLS (Transport Layer Security)
  - MTLS (Mutual Transport Layer Security)

  For using the MTLS protocol, you will need a server certificate issued for your system. The server certificate must have been issued by a reliable certification authority. You can select an appropriate certificate from Network Settings.

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

-

- **Activate static route**
  Activates, or deactivates, static routing. Click the checkbox to activate static routing. In this case, the checkbox will be checked. Click on the checkbox again to deactivate static routing. In that case, the checkbox will not be checked. The setting of this property will correspond to the Enabled column in the static routing list.

- **Classify route as trustworthy**
  Mark this checkbox if you classify the static route as trustworthy. Click on the checkbox to activate the functionality. The checkbox is then marked. Click on the checkbox again to deactivate the feature. In that case, the checkbox will not be checked. A static route entry marked as unreliable will require the use of the SIP registrar for the authorization of incoming SIP messages. Static routing entries that use the MTLS protocol for transport will automatically be considered reliable.

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

-

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

1.11 Diagnostics

You configure the log files for the diagnosis of problems from this dialog.

Log Level
Enter how much information should be written to the log file here.

Maximum size of a log file
Several log file files will be written. Each log file will be sequentially re-created, when the size entered in megabytes here has been exceeded.

Delete Log Files Daily
If this option has been activated then all log files will be deleted each day.

Log File Directory
The log files will be stored in this directory. Note that the service will require appropriate write rights for this directory.

1.12 Proxy Service

Displays the status of the proxy service.

- **Start the service**
  Click this button to start the proxy service.

- **Stop the service**
  Click this button to stop the proxy service.

2 Technical notes

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

- Federation
- Server certificate
- Setup of DNS Service Resource Records for the federation

3 Federation

What is a federation?

A federation is a special trusted network for the users of IT and telecomunication systems, which creates a secure structure for the communication between organisations, with the aim of improving the cooperation between its members.

Within the frame of this structure, every organization, for example, a company, defines on one hand the quality of the information which it would like to reveal and on the other hand, decides which services and systems for the exchange of information may be used.

This definition originates from technical literature, in particular on ECMA (European association for standardizing information and communication systems – former European Computer Manufacturers' Association) documents which talk about federation, federated solutions and federated services. A German notation hasn't been established yet, which is why this document generally uses English terms. Typical communication services which can be used today within the frame of a federation are a presence management and Instant Messaging (Chat). Other services are also imaginable in the future. Audio services and video services could also be provided in future within the framework of a federation.

The presence management within a federation enables the exchange of presence information between organisations and also beyond organisational borders. The technology provides information regarding a person's accessibility so that a suitable means of communication can be chosen depending on the person's status. The user receives information about a person's status or makes this information available to others.

If somebody is online and available then one can get in touch ad hoc via the phone, send a text message and can expect an immediate answer (Instant Messaging, Chat). These functions belong to the group of synchronous media. If the call partner is currently unavailable, an e-mail is usually chosen as the means of (asynchronous) communication. Therefore presence management promotes the user's agility. Moreover, such systems generally offer enhanced functionality, for example, there is often the opportunity to learn about the presence status change of a particular person (tagging). This is an extremely helpful function if you are waiting for a person to return to their workplace because you need information urgently.

To emphasize the long-term potential of the use of federation-based communication, it makes sense to look into presence management and instant messaging services more closely.

What is presence management?

In the world of classical Computer Telephony Integrations (CTI) concepts, which is the forerunner of a lot of Unified Communications (UC, standardised communication) solutions, the user's telephone lines and the events taking place there were the center of attention but the user himself was less important ("line-centered architecture"). Before it was "Line 177 – Franz Mueller – engaged". In the world of modern SIP-based Unified Communications applications, a new form of "person centered architecture" becomes possible:"Of course" the person comes first with regard to communication! Therefore what's said now is: "Franz Mueller – busy – in a call" or "Franz Mueller – busy – in an appointment till 12:00". In consideration that new services and media can be integrated into the communication network, numerous new questions arise from this context: Is the person with whom I would like to communicate available? With which media can I get in touch? A presence management system answers these crucial questions.

With every person (user, identity) a system links a defined state, the so-called presence information. This is composed in real-time according to defined rules from the status of several services. Examples of this are telephone status (telephony service), calendar status (calendar service) and a logged in/off status (system service). The presence information gives dynamic information about the availability of a communication partner, according to the current state of the different services.

What is instant messaging?

In today's typical office work environment, two forms of media dominate: the telephone - to communicate in real-time, a synchronous medium, and e-mail - as the predominant form of correspondence, a asynchronous medium for a less urgent form of communication. Other asynchronous media, for example, the fax, is less important now due to the rise of e-mail commuinication.

Because of continuous optimization of networks and the rising acceptance from users, another relatively new method for written correspondence has been established: the instant messaging (IM, Chat). With this method two or several users communicate via text messages.

Messages are exchanged on a real-time basis via a push method. Users work with a special client application, e.g., estos ProCall or Microsoft® Office Communicator. The clients are connected via a server or service with each other. The usage is as uncomplicated as e-mail, with the advantage that it allows to react spontaneously and a immediate response can be expected. Exactly the right thing for short inquiries.

Both presence management and Instant Messaging services complement the telephone and e-mail very well. They allow the user to address the contact in a way appropriate to the situation.

Who benefits from the federation?

People working together in organizations or in a regular business connection profit from a federation. This includes colleagues as well as business partners, suppliers and customers. Simliar to how the standardized electronic data interchange (EDIFact) channels and structures trade between the involved partners, a federation allows structured communication between organizations. Technical directives and accepted general conditions form the base which can be defined on an administrative level. In the end, it is up to the user to decide whether and how he wants to use the technological possibilities.

3.1 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**.

3.2 Setup of DNS Service Resource Records for the federation

A Service (SRV) Resource Record can be created on a Domain Name Server (DNS) for making IP-based services easier to find in a domain. Additional information about a service may be made available (such as the server running the service, priority and so forth).

Such a Service Resource Record can be created as follows:

```
_sipfederationtls Service Location (SRV) [1][0][5061] ucserver.domain.de.
```

_sipfederationtls	The name of the services which are found in the DNS. For the federation, the name must be _sipfederationtls.
Service Location (SRV)	The type of record contained by these lines.
[1]	The priority of the service so that different, similar records can be prioritized. Not in use.
[0]	Emphasizes the entry. It is not used
[5061]	Here the port number is provided from which the service provides the service. For the federation the default is generally valid: standard SIP on port 5061.
ucserver.domain.de	The computer which offers the service. Here, the federation expects the computer on which the UCServer runs.

How and where the Service Resource Records are created for specific DNS servers can be found in the corresponding manufacturer's documentation.

4 Info about estos SIP Proxy

estos SIP Proxy is a product of estos GmbH.

For product updates visit http://www.estos.de/

Frequently asked questions and answers and also support are available at http://support.estos.de