estos XMPP Proxy

7·3·3·5345

1 Welcome to estos XMPP Proxy

XMPP Proxy makes operation of multiple instances of estos UCServer with the same XMPP presence domain possible. Together with estos SIP Proxy, it can be used to run UCServer at multiple sites or for load distribution.

⚠	At this time, communication between two people using different instances of estos UCServer in the same presence domain throguh XMPP Proxy is not possible. estos SIP Proxy is required to accomplish this.

This help will guide your through the installation and configuration of estos XMPP Proxy.

- Conditions relating to the operating system System Requirements.
- The Network Interface Configuration will explain the server-to-server interface settings required for federations.
- The configuration of estos UCServer in connection wtih XMPP Proxy will be described in the UCUCServeronnection Configuration section.
- The section certificate describes the configuration needed for TLS encryption server certificate.
- Starting and stopping the XMPP Proxy services will be explained under Service Configuration.
- Contact information for the support department can be found in the Product Support Information section.

This help file can be opened from the XMPP Proxy program window at any time by requesting **Help**. As a rule, the help page for the topic, which corresponds to the feature currently being used, will be displayed.

In Help the following icons are used:

Icon	Meaning
➡	Note
⚠	Warning, caution

1.1 System requirements

Supported operating systems for estos XMPP Proxy:

- Windows® 8.1
- Windows® 10
- Windows® 11
- Windows Server® 2012
- Windows Server® 2012 R2
- Windows Server® 2016
- Windows Server® 2019
- Windows Server® 2022

➡	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.

Other XMPP servers need to connect with the XMPP Proxy for a federation to function. The proxy's server-to-server interfaces can be configured as follows:

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

Be careful that the Windows® firewall for the computer running XMPP Proxy will not block the port chosen and setup an appropriate rule, if necessary.

Make sure that this interface can be accessed from the public Internet and that your presence domain can be resolved to an IP address through DNS. If a non-standard port has been chosen, a DNS SRV record (_xmpp-server._tcp.*domain*) can publish this information for_tcp.*domain*) use by other systems. Ideally, such a DNS SRV record should also exist, if the default port is used. A DNS SRV Record is not absolutely required, since other systems can generally establish a connection to your UCServer using a DNS A Record and the default port 5269.

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

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

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

either invalid or not signed by a reliable certification authority then the connection will fail. This type of encryption is recommeneded, does not however always work (for example, GoogleTalk does not support TLS encryption, many server certificates have expired or they have only been signed by the server itself).

⚠	TLS encryption is only possible with a valid server certificate. The configuration of a Server Certificate is described inconfiguration of the certificate.

1.3 LAN Settings

Settings for the connection of UCServers, which have configured their connections to other servers through the proxy service.

- **TCP Port**
  Enter the TCP port through which XMPP Proxy should expect incoming connections. The port can be set to 5275 by clicking the Default button.
- **Bind to IP address**
  Choose the IP address, which you would like to use for incoming connections, for your system.
- **Password**
  Enter the password that UCServer should use for logging onto the XMPP Proxy.

⚠	Be careful that the Windows® firewall for the computer running XMPP Proxy will not block the port chosen and setup an appropriate rule, if necessary.
⚠	Be careful that only one user is active for each UCServer. Otherwise, the message will be delivered to the last UCServer that logged into XMPP Proxy.
⚠	The connection between UCServer and XMPP Proxy can only be encrypted if, as described in Sectionconfiguration of the certificate a valid server certificate has been configured. If no certificate is selected, between UCServer and XMPP Proxy only an unencrypted connection can be established.

1.4 Certificate Configuration

If TLS encryption is required, select a valid certificate here.

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.

The configured certificate is also used for the encryption of the connection from the TLS UCServer to XMPP Proxy. If no certificate is selected, between UCServer and XMPP Proxy only an unencrypted connection can be established.

1.5 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.

1.6 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.

1.7 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**.

2 Info about estos XMPP Proxy

estos XMPP Proxy is a product of estos GmbH.

Copyright (C) 2021 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

Microsoft®, Windows Server®, Windows® are either registered trademarks or trademarks 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.