estos XMPP Proxy

6.4.11.3356

1 Willkommen zum estos XMPP Proxy 4
1.1 Systemvoraussetzungen 4
1.2 WAN Einstellungen 5
1.3 LAN Einstellungen 6
1.4 Konfiguration des Zertifikats 6
1.5 Diagnose 7
1.6 Proxy Dienst 7
1.7 Server-Zertifikat 7
2 Info über estos XMPP Proxy 8

1 Willkommen zum estos XMPP Proxy

Der XMPP Proxy ermöglicht es, mehrere estos UCServer innerhalb derselben XMPP-Präsenzdomäne zu betreiben. Dies kann zusammen mit dem estos SIP Proxy zum Betrieb von UCServer an verschiedenen Standorten oder zur Lastverteilung genutzt werden.

⚠	Zur Zeit ist die Kommunikation zweier Benutzer auf verschiedenen estos UCServer in der gleichen Präsenzdomäne über den XMPP Proxy noch nicht möglich. Dafür wird der estos SIP Proxy benötigt.

Die vorliegende Hilfe führt Sie durch Installation und Konfiguration des estos XMPP Proxy.

- Über die Voraussetztungen bezüglich Betriebssystem informiert die Seite Systemvoraussetzungen.
- Der Abschnitt Konfiguration der Netzwerkschnittstelle erklärt die Einstellungen der Server-zu-Server-Schnittstelle, die für die Federation benötigt wird.
- Die Konfiguration der an den XMPP Proxy angeschlossenen estos UCServer wird im Abschnitt Konfiguration der UCServer Verbindung beschrieben.
- Der Abschnitt Zertifikat beschreibt die Konfiguration des für die TLS Verschlüsselung benötigten Server Zertifikats.
- Starten und Stoppen des XMPP Proxy-Dienstes wird unter Konfiguration des Dienstes erklärt.
- Kontaktaddressen für den Support finden sie im Abschnitt Informationen zur Produktunterstützung.

Die Hilfe lässt sich jederzeit aus den XMPP Proxy Programmfenstern über **Hilfe** aufrufen. In der Regel wird die Hilfe zu dem Thema geöffnet, das der gerade von Ihnen genutzten Funktion entspricht.

In der Hilfe werden die folgenden Symbole verwendet:

Symbol	Bedeutung
	Hinweis
⚠	Warnung, Vorsicht

1.1 Systemvoraussetzungen

Unterstützte Betriebssysteme für estos XMPP Proxy:

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

	Liste ist lediglich ein Auszug und es besteht kein Anspruch auf Richtigkeit und Vollständigkeit.
	Vollständige und aktuelle Versionen finden Sie auf unserer Website.

1.2 WAN Einstellungen

Konfiguration von Netzwerk Schnittstellen, die für eingehende Verbindungen genutzt werden.

Für die Federation ist es notwendig, dass sich andere XMPP-Server zum XMPP-Proxy verbinden können. Die Server-zu-Server-Schnittstelle des Proxys wird wie folgt konfiguriert:

- **TCP Port**
  Geben Sie hier den TCP Port für die XMPP Server-to-Server Schnittstelle an. Mit der Schaltfläche "Standard" können Sie den Standard-Port 5269 einstellen.
- **Auf IP-Adresse binden**
  Wählen Sie hier eine IP-Adresse Ihres Systems, auf die die XMPP Server-to-Server Schnittstelle gebunden werden soll.

Achten Sie auch darauf, dass die Windows®-Firewall des Rechners, auf dem der XMPP-Proxy läuft den eingestellten Port nicht blockiert und richten sie gegebenenfalls eine entsprechende Regel ein.

Stellen Sie sicher, dass diese Schnittstelle über das öffentliche Internet erreichbar ist und dass Ihre Präsenzdomäne über DNS zu einer IP-Adresse auflösbar ist. Wenn Sie einen vom Standard-Port abweichenden Port konfigurieren kann dieser über einen DNS SRV Record (_xmpp-server._tcp.*domäne*) anderen Systemen bekannt gemacht werden. Idealerweise sollte auch ein solcher DNS SRV Record existieren, wenn Sie den Standard-Port verwenden. Dieser DNS SRV Record ist aber nicht zwingend notwendig, da andere Systeme in der Regel auch über einen DNS A Eintrag und den Standard-Port 5269 eine Verbindung zu Ihrem UCServer aufbauen können.

Mittels des Buttons "Erweitert..." lassen sich Optionen für die Verschlüsselung der Server-zu-Server-Verbindungen einstellen. Es wird hierbei jedoch nur die Verbindung zum XMPP-Server der anderen Domäne verschlüsselt, der die Nachrichten entschlüsselt und an die entfernten User weiterleitet. Es erfolgt keine *Ende-zu-Ende-Verschlüsselung*.

Die Einstellungen für die TLS-Verschlüsselung können entweder global für alle Domänen oder für jede Domäne einzeln eingestellt werden. Für alle Domänen, für die keine explizite Einstellung eingetragen wurde, gilt die globale Einstellung. Folgende Stufen geordnet nach dem erreichbaren Grad der Vertraulichkeit sind möglich:

- **Keine Verschlüsselung**
  Es wird keine TLS Verschlüsselung für die Verbindungen mit der entfernten Domäne verwendet. Diese Einstellung sollte nur gewählt werden falls die Einstellung *TLS Verschlüsselung optional* nicht funktioniert.
- **TLS Verschlüsselung optional**
  Es wird versucht, TLS Verschlüsselung für die Verbindungen mit der entfernten Domäne zu verwenden, sofern dies von der Gegenseite möglich ist und lokal ein Zertifikat vorhanden ist. Bietet die Gegenseite kein TLS an (was zum Beispiel bei GoogleTalk der Fall ist), so erfolgt der Nachrichtenaustausch ohne Verschlüsselung. Andernfalls wird versucht, ein Höchstmaß an Vertraulichkeit zu gewährleisten. Diese Einstellung wird nahezu immer funktionieren, bietet jedoch keine Garantien bezüglich der Vertraulichkeit der Nachrichten.
- **TLS Verschlüsselung erforderlich, Zertifikatfehler ignorieren**
  Es wird versucht, TLS Verschlüsselung für die Verbindungen mit der entfernten Domäne zu verwenden. Ist lokal kein Zertifikat vorhanden oder bietet die Gegenseite kein TLS an schlägt die Verbindung fehl. Treten Zertifikatfehler auf (beispielsweise weil das Zertifikat der Gegenseite abgelaufen ist oder nicht von einer vertrauenswürdigen Zertifizierungsstelle unterzeichnet wurde) so werden diese ignoriert. Die Verbindungen bieten Vertraulichkeit, jedoch keine starke Authentifizierung der Gegenseite.

- **TLS Verschlüsselung mit gültigem Zertifikat**
  Es wird versucht, TLS Verschlüsselung für die Verbindungen mit der entfernten Domäne zu verwenden. Ist lokal kein Zertifikat vorhanden, bietet die Gegenseite kein TLS an oder ist das Zertifikat der Gegenseite nicht gültig und von einer vertrauenswürdigen Zertifizierungsstelle unterschrieben schlägt die Verbindung fehl. Diese Art der Verschlüsselung wird empfohlen, funktioniert aber leider nicht immer (z.B. bietet GoogleTalk keine TLS-Verschlüsselung an, viele Zertifikate anderer Server sind abgelaufen oder nur selbst signiert).

⚠ TLS Verschlüsselung ist nur mit einem gültigen Server Zertifikat möglich. Die Konfiguration eines Server Zertifikats wird in Abschnitt Konfiguration des Zertifikats beschrieben.

1.3 LAN Einstellungen

Einstellungen für die Verbindung von UCServern, die ihre Verbindung zu anderen Servern über den Proxy Dienst konfiguriert haben.

- **TCP Port**
  Geben Sie hier den TCP Port an, auf dem der XMPP Proxy eingehende Verbindungen erwartet. Mit der Schaltfläche "Default" können Sie den Default-Port 5275 einstellen.
- **Auf IP-Adresse binden**
  Wählen Sie hier eine IP-Adresse Ihres Systems, die Sie für eingehende Verbindungen verwenden möchten.
- **Passwort**
  Geben Sie hier das Passwort ein, mit dem sich der UCServer am XMPP Proxy anmelden soll.

⚠ Achten Sie auch darauf, dass die Windows®-Firewall des Rechners, auf dem der XMPP Proxy läuft den eingestellten Port nicht blockiert und richten sie gegebenenfalls eine entsprechende Regel ein.

⚠ Es ist darauf zu achten, dass ein Nutzer nur auf einem UCServer aktiv ist. Ansonsten wird die Nachricht an den letzten UCServer ausgeliefert, der sich am XMPP Proxy angemeldet.

⚠ Die Verbindung zwischen UCServer und XMPP Proxy kann nur dann verschlüsselt werden, wenn wie unter Abschnitt Konfiguration des Zertifikats beschrieben ein gültiges Server Zertifikat konfiguriert wurde. Falls kein Zertifikat ausgewählt wurde, kann zwischen UCServer und XMPP Proxy nur eine unverschlüsselte Verbindung aufgebaut werden.

1.4 Konfiguration des Zertifikats

Falls Sie TLS Verschlüsselung wünschen, wählen Sie hier ein gültiges Zertifikat aus.

Zur Verwendung der abgesicherten Netzwerkprotokolle TLS und MTLS benötigen Sie ein Server Zertifikat. Dieses muss von einer Zertifizierungsstelle signiert sein. Klicken Sie auf die Schaltfläche "Zertifikat...", um das Fenster zur Auswahl eines Zertifikates zu öffnen. Wählen Sie das geeignete Zertifikat aus und bestätigen Sie anschliessend Ihre Angabe mit "OK". Informationen zum ausgewählten Server Zertifikat werden zusätzlich angezeigt.

Das hier konfigurierte Zertifikat wird auch für die TLS Verschlüsselung der Verbindung vom UCServer zum XMPP Proxy verwendet. Falls hier kein Zertifikat ausgewählt wird, kann zwischen UCServer und XMPP Proxy nur eine unverschlüsselte Verbindung aufgebaut werden.

1.5 Diagnose

In diesem Dialog konfigurieren Sie die Log Dateien zur Diagnose von Problemen.

Log Level
Stellen Sie hier ein, wie viel Information in die Log Dateien geschrieben wird.

Maximale Größe einer Log Datei
Es werden mehrere Log Dateien geschrieben. Jede Log Datei wird zyklisch neu angelegt, wenn die hier eingestellte Größe in MB überschritten ist.

Log Dateien täglich löschen
Ist diese Option aktiv, so werden täglich alle Log Dateien gelöscht.

Log Datei Verzeichnis
In diesem Verzeichnis werden die Log Dateien abgelegt. Beachten Sie, dass der Dienst entsprechende Schreibrechte auf dieses Verzeichnis benötigt.

1.6 Proxy Dienst

Zeigt den Status des Proxy Dienstes.

- **Dienst starten**
  Klicken Sie auf diese Schaltfläche, um den Proxy Dienst zu starten.

- **Dienst beenden**
  Klicken Sie auf diese Schaltfläche, um den Proxy Dienst zu beenden.

1.7 Server-Zertifikat

Für die verschlüsselte Kommunikation über TLS (Transport Layer Security) und MTLS (Mutual TLS) wird ein Server-Zertifikat benötigt.

Server-Zertifikat
Ein Server-Zertifikat dient zur eindeutigen Identifizierung eines Servers. Das Zertifikat muss auf den FQDN (fully qualified domain name) des Servers ausgestellt sein. Das Server Zertifikat muss von einer vertrauenswürdigen Instanz ausgestellt sein. Zertifikate werden in dem Zertifikat-SnapIn der Microsoft® Management Console (MMC) konfiguriert.

Zertifikat-Speicher
Die verwendeten Zertifikate müssen im Speicher "Lokaler Computer" - "Eigene Zertifikate" abgelegt sein, und einen privaten Schlüssel enthalten. Den Zertifikatspeicher "Lokaler Computer" öffnen Sie mit der MMC-Konsole:

- Aus dem Windows® Start Menü, wählen Sie **Ausführen...** und geben `mmc.exe` ein.
- Wählen Sie **Datei** - **SnapIn hinzufügen/entfernen...**
- Wählen Sie **Hinzufügen**. Aus der Liste der verfügbaren SnapIns wählen Sie **Zertifikate**. Wählen Sie **Computerkonto**, **Lokaler Computer** und klicken Sie **Fertig stellen**.
- In der Liste gehen Sie zu **Zertifikate (Lokaler Computer)** - **Eigene Zertifikate**.

2 Info über estos XMPP Proxy

estos XMPP Proxy ist ein Produkt der estos GmbH.

Produkt Updates finden Sie unter https://www.estos.de/

Häufig gestellte Fragen und Antworten, sowie Support erhalten Sie unter https://support.estos.de