estos SIP Proxy

8.2.3.8086

1 Willkommen zum estos SIP Proxy 4
1.1 Systemvoraussetzungen 4
1.2 WAN Einstellungen 5
1.3 Netzwerk Schnittstellen 5
1.3.1 Liste der Netzwerk Schnittstellen 5
1.3.2 Konfigurieren von Netzwerk Schnittstellen 6
1.4 Konfiguration Netzwerk Schnittstelle 6
1.5 Zertifikat für SSL-/TLS-Kommunikation 7
1.6 LAN Einstellungen 7
1.7 Federation 8
1.8 Konfiguration Open Federation 8
1.9 Statische Routen 10
1.9.1 Liste aller Statischen Routen 10
1.9.2 Konfigurieren von Statischen Routen 11
1.9.3 Konfiguration Statische Route 12
1.10 Diagnose 13
1.11 Proxy Dienst 13
2 Technische Hinweise 14
3 Einführung in Federation 15
3.1 Server-Zertifikat 16
3.2 Einrichten eines DNS Service Resource Records für die Federation 17
4 Info über estos SIP Proxy 18

1 Willkommen zum estos SIP Proxy

Der SIP Proxy ermöglicht es, mehrere estos UCServer innerhalb derselben SIP-Präsenzdomäne zu betreiben. Dies kann zum Betrieb von UCServer an verschiedenen Standorten oder zur Lastverteilung genutzt werden. Der SIP Proxy sorgt dabei für die Verbindung der UCServer untereinander und die Federation.

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

- Über die Voraussetztungen bezüglich Betriebssystem informiert die Seite Systemvoraussetzungen.
- Die Netzwerkeinstellungen werden auf der Seite Konfiguration der Netzwerkschnittstellen beschrieben.
- Die Konfiguration der an den SIP Proxy angeschlossenen estos UCServer wird im Abschnitt Konfiguration der UCServer Verbindung beschrieben.
- Wie Sie die Federation konfigurieren erfahren Sie unter Konfiguration der Federation.
- Der Abschnitt Konfiguration der Statischen Routen erklärt die Konfiguration statischer Routen.
- Starten und Stoppen des SIP Proxy-Dienstes wird unter Konfiguration des Dienstes erklärt.
- Kontaktaddressen für den Support finden sie im Abschnitt Informationen zur Produktunterstützung.
- Weiterhin finden Sie in dieser Hilfe technische Hintergrundinformationen zur Federation, zur Einrichten eines DNS Service Resource Records sowie zu den für die Federation notwendigen Serverzertifikaten.

Die Hilfe lässt sich jederzeit aus den SIP 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 SIP Proxy:

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

	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.

- **Zertifikat**
  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.

- **Abweichende öffentliche Adresse verwenden**
  Schaltet die Verwendung der öffentlichen Adresse ein oder aus. Aktivieren Sie diese Funktion, falls Ihr Server über NAT-Routing (Network Address Translation) mit dem öffentlichen Internet verbunden ist.

  - **Port / IP**
    Zeigt die Portnummer und die IP Adresse an, die als öffentliche Adresse benutzt werden soll. Sollte Ihnen Ihre öffentlichen Adresse nicht bekannt sein, klicken Sie auf die Schaltfläche IP ermitteln. Es wird darauf hin die entsprechende IP Adresse ermittelt und in das Feld eingetragen.

  - **IP ermitteln**
    Klicken Sie auf diese Schaltfläche, wenn Sie bei Verwendung der öffentlichen Adresse die IP Adresse automatisch vom System bestimmen lassen wollen.

1.3 Netzwerk Schnittstellen

1.3.1 Liste der Netzwerk Schnittstellen

Listet die Netzwerk Schnittstellen auf, die für eingehende Verbindungen genutzt werden. Jede Netzwerk Schnittstelle verfügt über Eigenschaften und zusätzliche Informationen, die in der Tabelle zusammengefasst werden. Folgende Eigenschaften einer Netzwerk Schnittstelle werden angezeigt:

- **Aktiviert**
  Schaltet die Netzwerk Schnittstelle ein oder aus. Sie können diese Einstellung direkt vornehmen. Klicken Sie auf das Kontrollkästchen, um dieses zu markieren und die Netzwerk Schnittstelle zu aktivieren. Klicken Sie erneut auf das Kontrollkästchen, um die Netzwerk Schnittstelle zu deaktivieren. Im Falle einer deaktivierten Netzwerk Schnittstelle ist das zugehörige Kontrollkästchen nicht markiert.

- **IP**
  Zeigt die IP Adresse der Netzwerk Schnittstelle an. Zusammen mit der angegebenen Portnummer bestimmt sie die Schnittstelle eindeutig. Um die IP Adresse der Netzwerk Schnittstelle zu ändern, selektieren Sie die Zeile und klicken anschließend auf die Schaltfläche Eigenschaften....

- **Port**
  Zeigt die Portnummer der Netzwerk Schnittstelle an. Portnummer und IP Adresse bestimmen die Schnittstelle eindeutig. Um die Portnummer der Netzwerk Schnittstelle zu ändern, markieren Sie die Zeile und klicken anschließend auf die Schaltfläche Eigenschaften....

- **Protokoll**
  Zeigt das Transport Protokoll der Netzwerk Schnittstelle an. Für Netzwerk Schnittstellen stehen verschiedene Protokolle zur Auswahl.
  - UDP (User Datagram Protokoll)
  - TCP (Transmission Control Protocol)
  - TLS (Transport Layer Security)

- MTLS (Mutual Transport Layer Security)

Um den Protokoll Typ einer Netzwerk Schnittstelle zu ändern, markieren Sie die Zeile und klicken anschließend auf die Schaltfläche Eigenschaften.... Für abgesicherte Netzwerk Protokolle benötigen Sie zusätzlich ein Server Zertifikat für die Verwendung der gesicherten Netzwerk Schnittstellen. Weiterführende Informationen hinsichtlich Angabe eines Zertifikates finden Sie unter Server Zertifikat.

- **Status**
  Zeigt den Status der Netzwerk Schnittstelle an. Sie können diese Darstellung nicht editieren.

1.3.2 Konfigurieren von Netzwerk Schnittstellen

Sie können die Liste Ihrer Netzwerk Schnittstellen konfigurieren. Klicken Sie auf die Schaltfläche Hinzufügen..., um eine weitere Netzwerk Schnittstelle der Liste hinzuzufügen. Klicken Sie auf die Schaltfläche Entfernen, um eine oder mehrere Netzwerk Schnittstellen aus Ihrer Liste zu entfernen. Klicken Sie auf die Schaltfläche Eigenschaften..., um die Eigenschaften einer Netzwerk Schnittstelle anzuzeigen und um gegebenenfalls Anpassungen an dieser Netwerk Schnittstelle vorzunehmen.

- **Hinzufügen...**
  Klicken Sie auf diese Schaltfläche, um eine weitere Netzwerk Schnittstelle in die Liste aufzunehmen. Es öffnet sich ein neues Fenster, in dem Sie die Eigenschaften der neuen Netzwerk Schnittstelle festlegen. Weiterführende Informationen über die Eigenschaften einer Netzwerk Schnittstelle und wie Sie diese bestimmen können, entnehmen Sie bitte dem Abschnitt Liste der Netzwerk Schnittstellen.

- **Entfernen**
  Klicken Sie auf diese Schaltfläche, um Netzwerk Schnittstellen aus Ihrer Liste zu entfernen. Sie können diese Aktion nur dann ausführen, wenn mindestens eine Netzwerk Schnittstelle in der Liste von Ihnen markiert wurde. Sie werden anschließend über ein Meldefenster dazu aufgefordert, das Löschen Ihrer markierten Netzwerk Schnittstellen zu bestätigen. Klicken Sie auf die Schaltfläche "OK", um die Aufforderung zum Löschen zu bestätigen. Klicken Sie auf die Schaltfläche "Abbrechen", um den Löschvorgang abzubrechen.

- **Eigenschaften...**
  Klicken Sie auf diese Schaltfläche, um sich Eigenschaften und Details zu einer Netzwerk Schnittstelle anzeigen zu lassen. Sie können diese Aktion nur dann ausführen, wenn Sie genau eine Netzwerk Schnittstelle in der Liste gewählt haben. Sie können zusätzlich die Eigenschaften der Netzwerk Schnittstelle anpassen. Weiterführende Informationen über die Eigenschaften einer Netzwerk Schnittstelle und wie Sie diese gegebenenfalls anpassen können, entnehmen Sie bitte dem Abschnitt Liste der Netzwerk Schnittstellen.

Um Ihre Einstellungen zu bestätigen, klicken Sie auf die Schaltfläche "OK". Klicken Sie auf die Schaltfläche "Abbrechen", um Ihre Angaben zu verwerfen.

1.4 Konfiguration Netzwerk Schnittstelle

- **IP Adresse**
  Wählen Sie hier aus der Liste verfügbarer IP Adressen diejenige aus, die Sie als Netzwerkschnittstelle für eingehende Verbindungen verwenden möchten. Sie können nur aus der vorgegebenen Liste eine Auswahl treffen. Die Auswahlmöglichkeiten sind von den Einstellungen Ihres Systems abhängig.

- **Portnummer**
  Geben Sie hier die Portnummer an, die Sie für eingehende Verbindungen verwenden möchten. Der Wert der Portnummer darf zwischen 0 und 65535 angegeben werden. Viele SIP Server verwenden die Portnummer 5060 mit TCP oder 5061 mit TLS.

- **Protokoll**
  Wählen Sie hier das Transport Protokoll, das Sie für eingehende Verbindungen verwenden möchten. Folgende Transport Protokolle sind möglich:
  - **UDP** (User Datagram Protocol)
  - **TCP** (Transmission Control Protocol)
  - **TLS** (Transport Layer Security)
  - **MTLS** (Mutual Transport Layer Security)

  Für das Protokoll MTLS benötigen Sie ein für Ihr System ausgestelltes Server Zertifikat. Das Server Zertifikat muss von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt sein. Ein geeignetes Zertifikat können Sie in den Netzwerk Einstellungen auswählen.

  ⚠ Beachten Sie, dass es sich bei UDP und TCP um unverschlüsselte Protokolle handelt, die nicht abhörsicher sind. Es wird empfohlen, diese Protokolle nur innerhalb eines LANs zu verwenden. Das UDP Protokoll wird aufgrund der Beschränkung der maximalen Paketgröße von 65.535 Bytes nicht empfohlen.

-

1.5 Zertifikat für SSL-/TLS-Kommunikation

Übersicht der Eigenschaften des ausgewählen Zertifikats.

Subjekt Name	Signator bzw. Verwendungszweck des Zertifikats muss hier ein FQDN(fully qualified domain name) sein.
Aussteller	Herausgeber des Zertifikats.
Gültig vom / bis	Gültigkeitsdauer des Zertifikats.

Zertifikat auswählen...
Klicken Sie auf diese Schaltfläche, um ein Zertifikat auszuwählen. Es öffnet sich ein neues Fenster, in dem Sie die Auswahl des Zertifikats vornehmen können. Klicken Sie anschließend auf die Schaltfläche "OK", um die Auswahl zu übernehmen. Klicken Sie auf die Schaltfläche "Abbrechen", um die Auswahl zu verwerfen.

Um Ihre Einstellungen zu bestätigen, klicken Sie auf die Schaltfläche "OK". Klicken Sie auf die Schaltfläche "Abbrechen", um Ihre Angaben zu verwerfen.

1.6 LAN Einstellungen

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

- **Benutzername**
  Geben Sie hier einen eindeutigen Benutzernamen an, der für die Anmeldung am SIP Proxy Dienst benötigt wird.

- **Passwort**
  Geben Sie hier ein eindeutiges Passwort an. Die Angabe eines Passwortes ist optional.

- **Auf IP-Adresse binden**
  Wählen Sie aus der Liste verfügbarer Netzwerkschnittstellen, die Schnittstelle aus, über die sich UCServer mit SIP Proxy Dienst verbinden sollen.

- **Portnummer**
  Geben Sie hier die Portnummer an, über die sich UCServer mit SIP Proxy Dienst verbinden sollen.

- **Transport Protokoll**
  Stellen Sie hier ein, welches Transport Protokoll von den UCServern verwendet wird. Folgende Möglichkeiten stehen zur Auswahl:
  - UDP (User Datagram Protokoll)
  - TCP (Transmission Control Protocol)
  - TLS (Transport Layer Security)
  - MTLS (Mutual Transport Layer Security)

  Für das Protokoll MTLS benötigen Sie ein Server Zertifikat. Angaben zum Zertifikat können Sie in den Netzwerk Einstellungen vornehmen.

Um Ihre Einstellungen zu bestätigen, klicken Sie auf die Schaltfläche "OK". Klicken Sie auf die Schaltfläche "Abbrechen", um Ihre Angaben zu verwerfen.

1.7 Federation

Die Federation ermöglicht internen Benutzern das Versenden von Instant Messaging Nachrichten und die Ansicht der Präsenzinformation externer Benutzer.
Eine ausführliche Beschreibung der Federation finden Sie auf der Seite Einführung in Federation.

- **Open Federation verwenden**
  Die Verbindungen zu anderen Präsenz Domänen werden über Standard SIP Protokolle hergestellt. Die Erreichbarkeit anderer Server wird automatisch über spezielle DNS Service Location Records ermittelt, so dass in diesem Fall keine weitere Konfiguration erforderlich ist. Um die Erreichbarkeit Ihrer Server zu konfigurieren, klicken Sie einfach auf die entsprechende Schaltfläche "Konfigurieren...". Es öffnet sich ein neues Fenster, in dem Sie die Einstellungen zur Open Federation vornehmen können.

Um Ihre Einstellungen zu bestätigen, klicken Sie auf die Schaltfläche "OK". Klicken Sie auf die Schaltfläche "Abbrechen", um Ihre Angaben zu verwerfen.

1.8 Konfiguration Open Federation

Zur Verwendung der Open Federation, benötigen Sie ein gültiges Serverzertifikat, ein DNS-SRV Eintrag im öffentlichen DNS und eine Netzwerkschnittstelle für eingehende Verbindungen. Weiterführende Informationen hinsichtlich der Angabe eines Zertifikates finden Sie unter Server Zertifikat.
Informationen zum Einrichten eines DNS-SRV Eintrag finden Sie unter Einrichten eines DNS Service Resource Records für die Federation.

- **Zertifikat**
  Zur Verwendung der Open Federation 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.

- **Mit dem Zertifikat übereinstimmender DNS-SRV Eintrag**

Abhängig vom ausgewählten Server Zertifikat, wird über eine DNS Abfrage, die ermittelte IP Adresse und Port angezeigt. Sollte nach Auswahl eines Zertifikats nichts angezeigt werden, haben Sie möglicherweise keinen oder einen nicht mit der Zertifikat übereinstimmenden DNS-SRV Eintrag.

- **DNS Host IP**
  Ermittelte IP Adresse aus der DNS Abfrage mit Zertifikats-Subjekt Namen.

- **DNS Port**
  Ermittelte Portnummer aus der DNS Abfrage mit Zertifikats-Subjekt Namen.

- **Netzwerkschnittstelle für eingehende Verbindungen**

  Wählen Sie hier eine Netzwerkschnittstelle, die Sie für eingehende Verbindungen der Open Federation verwenden wollen. Nach Auswahl einer Netzwerkschnittstelle und abschließen der Konfiguration, wird diese automatisch den Netzwerkschnittstellen für eingehende Verbindungen hinzugefügt.

  - **Auf IP Adresse binden**
    Wählen Sie aus der Liste verfügbarer Netzwerkschnittstellen, die Schnittstelle aus, über die Open Federation verfügbar sein soll.

  - **Port**
    Geben Sie hier die Portnummer für die Open Federation an.

- Automatisch über STUN (Simple Traversal of User Datagram Protocol [UDP] Through Network Address Translators [NATs]) Server ermittelter NAT-Typ und öffentliche IP-Adresse. Mit Hilfe des STUN-Servers können Clients ihre öffentliche IP-Adresse, das NAT-Gerät, hinter dem sie sich befinden, und den nach außen veröffentlichten, Internet-seitigen Port ermitteln, dem per NAT ein bestimmter lokaler Port zugewiesen wurde.
  - **Öffentliche Adresse verwenden**
    Schaltet die Verwendung der öffentlichen Adresse ein oder aus. Aktivieren Sie diese Funktion, falls Ihr Server über NAT-Routing (Network Address Translation) mit dem öffentlichen Internet verbunden ist.

  - **NAT-Typ**
    Ermittelter NAT-Typ durch STUN Abfrage.

    - **Full Cone**
      Ein Full Cone NAT bildet alle Anfragen von der gleichen internen IP-Adresse und Port auf die gleiche externe IP-Adresse und Port ab. Darüber hinaus kann jeder externe Host ein Paket an den internen Host senden, da auch externe Adressen zu internen Adressen zugeordnet werden.

    - **Restricted Cone**
      Im Gegensatz zu einem Full Cone NAT, kann ein externer Host (mit IP-Adresse X) ein Paket nur an den internen Host senden, wenn der interne Host zuvor ein Paket an die IP-Adresse X gesendet hatte.

    - **Restricted Port Cone**
      Ein Port beschränkter Cone-NAT ist wie ein Restricted-Cone-NAT, wobei die Beschränkung auch Port-Nummern umfasst. Genauer gesagt, kann ein externer Host ein Paket, mit Quell-IP-Adresse X und Quell-Port P, nur an den internen Host senden, wenn der interne Host zuvor ein Paket an die IP-Adresse und den Port X P. gesendet hatte.

    - **Symmetric**
      Ein Symmetric NAT ist wie ein Full Cone-NAT, wobei andere Zuordnungen

verwendet werden, wenn der gleiche Host ein Paket mit der gleichen Quelle-Adresse und Port an ein anderes Ziel sendet. Desweiteren kann nur der externe Host, der ein Paket empfangen hat, ein UDP-Paket zurück an den internen Host senden.

- **Open Internet**
  NAT wird nicht verwendet.

- **Firewall blocks UDP**
  UDP Pakete wurden durch eine Firewall blockiert.

- **Symmetric UDP Firewall**
  Eine Firewall, erlaubt das Versenden und Empfangen von UDP Paketen ohne IP-Adressen zu ersetzen.

- **Unbekannt**
  Fehler beim ermitteln den NAT-Typs.

- **Öffentliche IP Adresse**
  Ermittelte öffentliche IP-Adresse durch STUN Abfrage.

Um Ihre Einstellungen zu bestätigen, klicken Sie auf die Schaltfläche "OK". Klicken Sie auf die Schaltfläche "Abbrechen", um Ihre Angaben zu verwerfen.

1.9 Statische Routen

Erfassen und konfigurieren Sie hier Ihre Liste von statischen Routen, die für ausgehende Verbindungen genutzt werden sollen.

1.9.1 Liste aller Statischen Routen

- **Statische Routen verwenden**
  Aktivieren oder deaktivieren Sie hier die Funktionalität der in Ihrer Liste erfassten Statischen Routen. Wenn Sie "Statische Routen verwenden" ausschalten, sind alle von Ihnen erfassten Statischen Routen deaktiviert und Sie können des Weiteren keine Anpassungen an Ihrer bestehenden Konfiguration vornehmen.

- **Statische Routen**
  Zeigt die Liste der von Ihnen eingetragenen und konfigurierten Statischen Routen an. Jede Zeile in der Liste repräsentiert eine Statische Route mit jeweils individuellen Einstellungen. Folgende Eigenschaften einer Statischen Route werden angezeigt.

  - **Aktiviert**
    Schaltet die Statische Route ein oder aus. Sie können diese Einstellung direkt vornehmen. Klicken Sie auf das Kontrollkästchen, um die Statische Route ein- oder auszuschalten. Weiterführende Information hierzu finden Sie unter den Konfiguration Statische Route.

  - **Vertrauenswürdig**
    Zeigt an, ob die Statische Route als vertrauenswürdig eingestuft wird. Sie können diese Einstellung direkt vornehmen. Klicken Sie auf das Kontrollkästchen, um die Funktionalität ein- oder auszuschalten. Weiterführende Information hierzu finden Sie unter den Konfiguration Statische Route.

  - **Domäne**
    Zeigt den Namen der Domäne an, der für die Statische Route genutzt werden soll. Der Domänenname ist der zusammenhängende Teilbereich des hierarchischen Systems und

muss in Ihrer angezeigten Liste eindeutig sein. Weiterführende Information zum Domänennamen finden Sie unter den Konfiguration Statische Route.

- **Zugangs Server**
  Zeigt die IP Adresse des Servers an, unter der die Domäne erreichbar ist. Hierbei kann es sich auch um einen symbolischen Namen handeln, der im Laufe des Betriebs in eine IP Adresse umgewandelt wird. Weiterführende Information zum Zugangsservers finden Sie unter den Konfiguration Statische Route.

- **Port**
  Zeigt den verwendeten Port des von Ihnen gewählten Zugangsservers an. Der Wert der Portnummer darf zwischen 0 und 65535 angegeben werden. Viele SIP Server verwenden die Portnummer 5060 mit TCP oder 5061 mit TLS. Weiterführende Information hierzu finden Sie unter den Konfiguration Statische Route.

- **Protokoll**
  Zeigt das Transport Protokoll des von Ihnen gewählten Zugangsservers an. Für Statische Routen stehen verschiedene Protokolle zur Auswahl. Einstellungen zum Transport Protokoll und weiterführende Informationen hierzu finden Sie unter den Konfiguration Statische Route.

- **Gebunden auf**
  Zeigt die Auswahl der IP Adresse, falls die Route auf eine IP Adresse Ihres Systems gebunden wurde. Weiterführende Information hierzu finden Sie unter den Konfiguration Statische Route.

1.9.2 Konfigurieren von Statischen Routen

Sie können die Liste Ihrer Statischen Routen anpassen. Klicken Sie auf die Schaltfläche Hinzufügen..., um eine weitere Statische Route der Liste hinzuzufügen. Klicken Sie auf die Schaltfläche Entfernen, um eine oder mehrere Statische Routen aus der Liste zu entfernen. Klicken Sie auf die Schaltfläche Eigenschaften..., um sich die Eigenschaften einer Statischen Route anzeigen zu lassen und um gegebenenfalls Änderungen an diesen Eigenschaften vorzunehmen.

- **Hinzufügen...**
  Klicken Sie auf diese Schaltfläche, um eine weitere Statische Route in die Liste aufzunehmen. Es öffnet sich ein neues Fenster, in dem Sie die Einstellungen zu den Eigenschaften Ihrer neuen Statischen Route vornehmen können. Klicken Sie anschließend auf die Schaltfläche "OK", um die Statische Route als neuen Eintrag in die Liste aufzunehmen. Klicken Sie auf die Schaltfläche "Abbrechen", um die Statische Route zu verwerfen.

- **Entfernen**
  Klicken Sie auf diese Schaltfläche, um Statische Routen aus Ihrer Liste zu entfernen. Sie können diese Aktion nur dann ausführen, wenn mindestens eine Statische Route in der Liste von Ihnen markiert wurde. Sie werden anschließend über ein Meldefenster dazu aufgefordert, das Löschen Ihrer Auswahl zu bestätigen. Klicken Sie auf die Schaltfläche "OK", um die Aufforderung zum Löschen zu bestätigen. Klicken Sie auf die Schaltfläche "Abbrechen", um den Löschvorgng zu verwerfen.

- **Eigenschaften...**
  Klicken Sie auf diese Schaltfläche, um sich Eigenschaften und Details einer Statischen Route in einem weiteren Fenster anzeigen zu lassen. Sie können diese Aktion nur dann ausführen, wenn Sie genau eine Statische Route in der Liste markiert haben.

Um Ihre Einstellungen zu bestätigen, klicken Sie auf die Schaltfläche "OK". Klicken Sie auf die Schaltfläche "Abbrechen", um Ihre Angaben zu verwerfen.

1.9.3 Konfiguration Statische Route

- **Domänen Name**
  Zeigt den Namen der Domäne an, der für die Statische Route genutzt werden soll. Der Domänenname ist der zusammenhängende Teilbereich des hierarchischen Systems und muss in Ihrer angezeigten Liste eindeutig sein.

- **Zugangs Server**
  Zeigt die IP Adresse des Servers an, unter der die Domäne erreichbar ist. Hierbei kann es sich auch um einen symbolischen Namen handeln, der im Laufe des Betriebs in eine IP Adresse umgewandelt wird.

- **Port**
  Geben Sie hier die Portnummer des von Ihnen gewählten Zugangsservers an. Der Wert der Portnummer darf zwischen 0 und 65535 angegeben werden. Viele SIP Server verwenden die Portnummer 5060 mit TCP oder 5061 mit TLS. Die Portnummer sowie Transport Protokoll, muss einer Netzwerk Schnittstelle für eingehende Verbindungen des Zugangs Servers entsprechen.

- **Auf IP Adresse binden**
  Wählen Sie hier aus der Liste verfügbarer IP Adressen diejenige aus, die Sie für die Statische Route verwenden möchten. Sie können nur aus der vorgegebenen Liste eine Auswahl treffen. Die Auswahlmöglichkeiten sind von den Einstellungen Ihres Systems abhängig.

- **Transport Protokoll**
  Wählen Sie hier das Transport Protokoll des Zugangsservers. Das Transport Protokoll sowie Portnummer, muss einer Netzwerk Schnittstelle für eingehende Verbindungen des Zugangs Servers entsprechen. Folgende Transport Protokolle sind mit Statischen Routen möglich:
  - **UDP** (User Datagram Protocol)
  - **TCP** (Transmission Control Protocol)
  - **TLS** (Transport Layer Security)
  - **MTLS** (Mutual Transport Layer Security)

  Für das Protokoll MTLS benötigen Sie ein für Ihr System ausgestelltes Server Zertifikat. Das Server Zertifikat muss von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt sein. Ein geeignetes Zertifikat können Sie in den Netzwerk Einstellungen auswählen.

  ⚠ Beachten Sie, dass es sich bei UDP und TCP um unverschlüsselte Protokolle handelt, die nicht abhörsicher sind. Es wird empfohlen, diese Protkolle nur innerhalb eines LANs zu verwenden. Das UDP Protokoll wird aufgrund der Beschränkung der maximalen Paketgröße von 65.535 Bytes nicht empfohlen.

-

- **Statische Route aktivieren**
  Schaltet die Statische Route ein oder aus. Klicken Sie auf das Kontrollkästchen, um die Statische Route einzuschalten. In diesem Fall ist das Kontrollkästchen markiert. Klicken Sie erneut auf das Kontrollkästchen, um die Statische Route auszuschalten. In diesem Fall ist das Kontrollkästchen nicht markiert. Die Einstellung dieser Eigenschaft entspricht der Spalte Aktiviert in der Liste Statischer Routen.

- **Route als vertrauenswürdig einstufen**
  Markieren Sie dieses Kontrollkästchen, wenn Sie die Statische Route als vertrauenswürdig einstufen. Klicken Sie auf das Kontrollkästchen, um die Funktionalität einzuschalten. In diesem Fall ist das Kontrollkästchen markiert. Klicken Sie erneut auf das Kontrollkästchen, um die Funktionalität auszuschalten. In diesem Fall ist das Kontrollkästchen nicht markiert. Eine nicht als vertrauenswürdig eingestufte Statische Route erfordert die Verwendung des SIP Registrars, um eintreffende SIP

Nachrichten autorisieren zu können. Statische Routen die als Transport Protokoll MTLS benutzten sind automatisch vertrauenswürdig eingestuft.

> ⚠ Aus Sicherheitsgründen wird empfohlen, diese Option nur für statische Routen innerhalb eines LANs zu verwenden.

-

Um Ihre Einstellungen zu einer Statischen Route zu bestätigen, klicken Sie anschließend auf die Schaltfläche "OK". Klicken Sie auf die Schaltfläche "Abbrechen", um Ihre Angaben zu verwerfen. Sollte das System Ihre Angaben zu einer Statischen Route ablehnen, so prüfen Sie zunächst, ob Ihre Angaben vollständig sind oder ob sich vielleicht ein Tippfehler eingeschlichen haben könnte. Ändern Sie dazu die Eigenschaften der Statischen Route und probieren Sie es erneut.

1.10 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.

1.11 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.

2 Technische Hinweise

In diesem Abschnitt sind Informationen zu Details und speziellen Themen zusammengefasst, auf die aus anderen Hilfeseiten verwiesen wird.

- Einführung in Federation
- Server-Zertifikat
- Einrichten eines DNS Service Resource Records für die Federation

3 Einführung in Federation

Was ist Federation?

Eine Federation (Föderation) ist ein besonderer Vertrauensrahmen oder ein besonderes Vertrauensnetz für die Nutzer von IT- und TK-Systemen, das eine gesicherte Struktur für die Kommunikation zwischen Organisationen schafft, mit dem Ziel, die Zusammenarbeit (Kollaboration, engl. Collaboration) ihrer Mitglieder zu verbessern.

Im Rahmen dieser Struktur legt jede Organisation, beispielsweise ein Unternehmen, für sich einerseits die Qualität der Information fest, die es preisgeben möchte, und entscheidet andererseits, welche Dienste und Systeme für den Austausch dieser Informationen genutzt werden dürfen.

Diese Begriffsdefinition orientiert sich an technischer Literatur, insbesondere an ECMA (European association for standardizing information and communication systems – früher European Computer Manufacturers' Association)-Dokumenten, in denen von federation, federated solutions und federated services die Rede ist. Eine deutsche Schreibweise hat sich noch nicht etabliert, weshalb in diesem Dokument generell der englische Begriff verwendet wird. Typische Kommunikationsdienste, die heute im Rahmen einer Federation genutzt werden können, sind Präsenz-Management und Instant Messaging (Chat). Darüber hinaus sind in Zukunft auch andere Dienste denkbar. So könnten in Zukunft auch Audio- und Videodienste im Rahmen einer Federation bereitgestellt werden.

Das Präsenz-Management innerhalb einer Federation ermöglicht es, Präsenz-Informationen zwischen Organisationen auch über die Organisationsgrenze hinweg auszutauschen. Die Technologie liefert Informationen zur Erreichbarkeit einer Person, so dass, abhängig von deren Status, ein geeignetes Kommunikationsmittel gewählt werden kann. Der Anwender erfährt also etwas über den aktuellen Status einer Person bzw. stellt solche Informationen anderen zur Verfügung.

Ist jemand online und gerade erreichbar, kann man ad hoc Kontakt über das Telefon aufnehmen, eine Kurznachricht senden und sofort eine Antwort erwarten (Instant Messaging, Chat). Diese Funktionen zählen zur Gruppe der synchronen Medien. Ist der gewünschte Partner momentan nicht erreichbar, so wählt man in der Regel die E-Mail als (asynchronen) Kommunikationsweg. Präsenz-Management fördert somit die Agilität der Nutzer. Darüber hinaus bieten solche Systeme in der Regel erweiterte Funktionalitäten: Oft besteht zum Beispiel auch die Möglichkeit, sich über die Präsenzstatus-Änderung einer bestimmten Person informieren zu lassen (Tagging). Eine äußerst hilfreiche Funktion, wenn man sehnsüchtig auf die Rückkehr einer Person an den Arbeitsplatz wartet, weil man eine dringende Information benötigt.

Um das langfristige Potenzial des Einsatzes von Federation-basierter Kommunikation zu verdeutlichen, macht es Sinn sich noch etwas genauer mit den Diensten Präsenz-Management und Instant Messaging zu beschäftigen.

Was ist Präsenz-Management?

In der Welt klassischer Computer Telefonie Integrations (CTI)-Konzepte, den Vorläufern vieler Unified Communications (UC, vereinheitlichte Kommunikation)-Lösungen, standen nicht die Benutzer, sondern ihre Telefonleitungen und die dort stattfindenden Ereignisse im Mittelpunkt („leitungszentrierte Architektur"). Hier hieß es „Leitung 177 – Franz Müller – besetzt". In der Welt moderner SIP-basierter Unified Communications-Anwendungen wird eine neue „personenzentrierte Architektur" möglich: „Natürlich" steht hier die Person als kommunizierendes Wesen an erster Stelle! Konsequenterweise heißt es daher nun: „Franz Müller – beschäftigt – im Gespräch" oder „Franz Müller – beschäftigt – im Termin bis 12:00". Wenn man dabei noch berücksichtigt, dass auch neue Dienste und Medien in das Kommunikationsnetz integriert sein können, ergeben sich aus diesem Kontext zahlreiche neue Fragen: Ist die Person, mit der ich kommunizieren möchte, erreichbar? Über welches Medium kann ich Kontakt aufnehmen? Die entscheidenden Antworten hierzu liefert ein Präsenz-Management System.

Mit jeder Person (Benutzer, Identität) verknüpft ein System einen definierten Zustand, die sogenannte Präsenz-Information. Diese wird in Echtzeit nach definierten Regeln aus den Stati mehrerer Dienste gebildet. Beispiele dafür sind Telefoniestatus (Telefonie-Dienst), Kalenderstatus (Kalender-Dienst) und ein An-Abgemeldet-Status (System-Dienst). Die Präsenz-Information gibt daher dynamisch über die Erreichbarkeit eines Kommunikationspartners Auskunft, je nach aktuellem Zustand der verschiedenen Dienste.

Was ist Instant Messaging?

Am heutigen typischen Büroarbeitsplatz dominieren zwei Medien: das Telefon zur Kommunikation in Echtzeit, ein synchrones Medium, und die E-Mail für den überwiegenden Teil des Schriftverkehrs, ein asynchrones Medium für die weniger zeitkritische Kommunikation. Andere asynchrone Medien, wie z.B. das beliebte Fax, treten in den Hintergrund, weil Sie zunehmend im E-Mail-Format aufgehen.

Durch die laufende Optimierung der Netzwerke und die steigende Akzeptanz bei den Nutzern etabliert sich dazu eine weitere, relativ junge Konversationsmethode, bei der schriftlich kommuniziert wird: das Instant Messaging (IM, Chat). Bei dieser Methode kommunizieren zwei oder mehrere Nutzer mittels Textnachrichten.

Die Nachrichten werden dabei in Echtzeit mittels eines Push-Verfahrens ausgetauscht. Die Nutzer bedienen sich dazu einer speziellen Clientanwendung, z.B. estos ProCall oder Microsoft® Office Communicator. Die Clients wiederum sind über einen Server oder Dienst miteinander verbunden. Die Handhabung ist so unkompliziert wie die E-Mail, mit dem Vorteil, dass man spontan reagieren, und auch sofort eine Reaktion erwarten kann. Für kurze Rückfragen oft genau das Richtige.

Die beiden Dienste Präsenz-Management und Instant Messaging ergänzen das Telefon und die E-Mail hervorragend. Sie ermöglichen den Nutzern eine situationsgerechte Kontaktaufnahme und Ansprache.

Wer profitiert von der Federation?

Von einer Federation profitieren Menschen in Organisationen, die zusammenarbeiten oder in einer regelmäßigen Geschäftsbeziehung stehen. Dazu gehören Kollegen genauso wie Geschäftspartner, Lieferanten und Kunden. Ähnlich wie der standardisierte elektronische Datenaustausch (EDIFact) den Handel zwischen den beteiligten Partnern kanalisiert und strukturiert, ermöglicht eine Federation eine strukturierte Kommunikation zwischen den Organisationen. Die Basis dafür bilden technische Richtlinien und gemeinsam akzeptierte Rahmenbedingungen, die auf einer administrativen Ebene festgelegt werden können. Die Technologie lässt aber letztendlich dem Nutzer die Freiheit selbst zu entscheiden, ob und wie er die Möglichkeiten nutzen möchte.

3.1 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**.

3.2 Einrichten eines DNS Service Resource Records für die Federation

Ein Service (SRV) Resource Record kann in einem DNS eingetragen werden um IP-basierte Dienste in einer Domäne leichter auffindbar zu machen. Dabei können zu einem Dienst noch zusätzliche Informationen bereitgestellt werden (z.B. Server auf dem der Dienst läuft, Priorität etc.).

Eingetragen wird ein solcher Service Resource Record wie folgt:

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

_sipfederationtls	Name des Dienstes unter dem er im DNS gefunden wird. Für die Federation muss dieser _sipfederationtls lauten.
Service Location (SRV)	Welcher Typ von Eintrag diese Zeile beinhaltet.
[1]	Priorität des Dienstes. Damit kann eine Priorisierung der verschiedenen, gleichartigen Einträge erreicht werden. Wird nicht verwendet
[0]	Gewichtung des Eintrages. Wird nicht verwendet
[5061]	Hier wird die Portnummer angegeben, unter der der Service den Dienst zur Verfügung stellt. Für die Federation gilt im allgemeinen die Voreinstellung nach SIP Standard auf Port 5061.
ucserver.domain.de	Rechner, der den Dienst anbietet. Die Federation erwartet hier den Rechner, auf dem der UCServer läuft.

Wie und wo man die Service Resource Records für bestimmte DNS-Server einrichtet, entnehmen Sie bitte der entsprechenden Dokumentation des Herstellers.

4 Info über estos SIP Proxy

estos SIP 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