UCServer für ProCall Enterprise 6 - Mobile Apps einrichten

Best Practice

Rechtliche Hinweise / Impressum

Die Angaben in diesem Dokument entsprechen dem Kenntnisstand zum Zeitpunkt der Erstellung. Irrtümer und spätere Änderungen sind vorbehalten.

Die estos GmbH schließt jegliche Haftung für Schäden aus, die direkt oder indirekt aus der Verwendung dieses Dokumentes entstehen.

Alle genannten Marken- und Produktbezeichnungen sind Warenzeichen oder Eigentum der entsprechenden Inhaber.

Die derzeit gültigen Allgemeinen Geschäftsbedingungen finden Sie auf unserer Webseite unter http://www.estos.de/agb.

estos GmbH
Petersbrunner Str. 3a
82319 Starnberg, Deutschland
info@estos.de
www.estos.de

Dokumentvorlage 5/2015

Dokumentenhistorie

Version	Datum	Autor	Änderungen
7	21.11.2018	KAB	Skizzen tlw. angepasst
6	08.11.2018	BK,MB	Inhaltskontrolle
5	21.09.2018	DL	Änderungen und Ergänzungen
4	17.09.2018	MB	Weitere Änderungen
3	12.09.2018	MB	Änderungen/Ergänzungen
2	07.09.2018	BK	Ergänzung Fehlersuche
1	30.08.2018	BK	Initiale Erstellung

Inhaltsverzeichnis

1. Einführung

ProCall Enterprise kann Plattform-unabhängig und Geräte-übergreifend genutzt werden und bietet neben dem Windows Clients auch native Clients für MacOS, iOS und Android.

Mit ProCall Mobile, den nativen Apps für iPad, iPhone und Android, können Anwender auch mobil auf ausgewählte und bewährte Leistungsmerkmale der Unified Communication & CTI Software Suite ProCall Enterprise zurückgreifen.

Die Funktionen können in zwei grundsätzliche Bereiche eingeteilt werden:

1.1. UCServer-eigene Funktionen

- Präsenz
- Text Chat
- Kontaktdaten/-Suche
- Steuerung der Telefone (Rufumleitung, Remote Office ...)

1.2. Sprach- und Bildübertragung

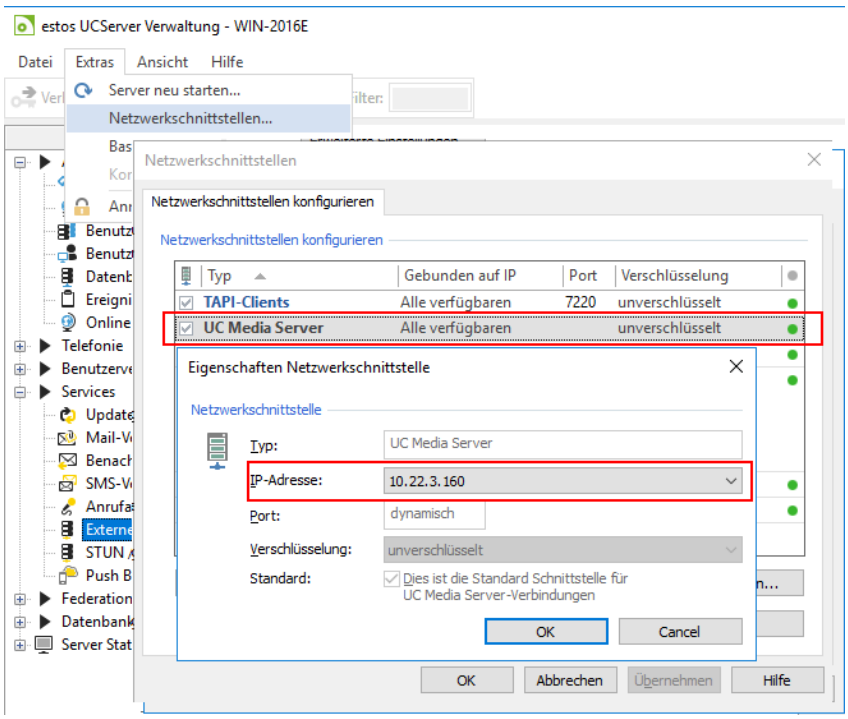
- Audio- und Video-Kommunikation
- Softphone-Funktionen (SIP)

Abhängig davon, welche Funktionen in den Mobile Apps genutzt werden sollen und ob die Mobile Apps nur im internen Netzwerk oder auch von extern über das Internet genutzt werden sollen, sind unterschiedliche Schritte zur Einrichtung erforderlich.

Diese Anleitung beschreibt einige Möglichkeiten zur Einrichtung des UCServer und enthält Hinweise zur Einrichtung ggf. zusätzlich benötigter Komponenten für die Nutzung der Mobile Apps im lokalen Netzwerk und über das Internet.

Weiterführende Informationen und Erklärungen zu den benötigten Netzwerk-Komponenten und –Funktionen finden Sie im Anhang.

Unabhängig von den dargestellten Szenarien, beachten Sie bitte Folgendes:



Wenn Sie Audio-/Video-Chat und/oder Softphone-Funktionen benutzen möchten, benötigt die zuständige UCServer-Komponente eine fest zugewiesene IP-Adresse zur Kommunikation.

Hat der Rechner, auf dem der UCServer installiert ist, mehr als eine IP-Adresse und/oder mehrere Netzwerk-Karten, **muss** dem *UC Media Server* eine IP-Adresse **für die Kommunikation mit der Telefonanlage** zugewiesen werden.

Öffnen Sie im *UCAdmin* das Menü *Extras – Netzwerkschnittstellen*. Öffnen Sie per Doppelklick die Einstellungen zum *UC Media Server* und wählen Sie die gewünschte IP-Adresse aus.

Speichern Sie die Einstellung und starten Sie den UCServer Dienst neu.

2. Mobile Apps nur im internen Netzwerk nutzen

Alle oben genannten Funktionen sind nach der Installation und Einrichtung des UCServer im internen Netzwerk sowohl für die ProCall Clients als auch für die ProCall Mobile Apps verfügbar.

Damit Nachrichten und Anrufe auch dann am Handy angezeigt werden, wenn sich die App im Hintergrund befindet oder das Handy gesperrt ist, müssen die Mobile Apps, unabhängig von den genutzten Funktionen, über eingehende Nachrichten und Anrufe mittels *Push-Nachrichten* informiert werden.

Push-Nachrichten werden vom UCServer zum estos Push-Server im Internet gesendet, welcher die Benachrichtigungen an die entsprechenden Dienste von Apple (iOS) bzw. Google (Android) übermittelt.

Von dort werden die Push-Nachrichten an das jeweilige Zielgerät gesendet.

2.1. Einrichten der Push-Benachrichtigung

Für diese Funktion ist zwingend erforderlich, dass der UCServer eine Verbindung zum Internet hat. Eine zusätzliche Lizenz ist nicht erforderlich.

2.1.1. Firewalls einrichten

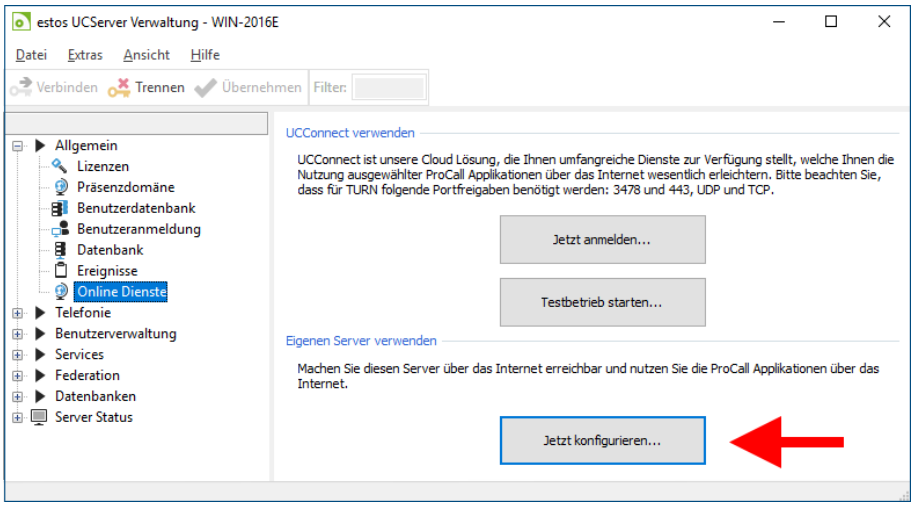
Die Firewall am UCServer Rechner und auf dem Gateway zum Internet muss so eingerichtet werden, dass der UCServer die Push-Nachrichten versenden darf an:

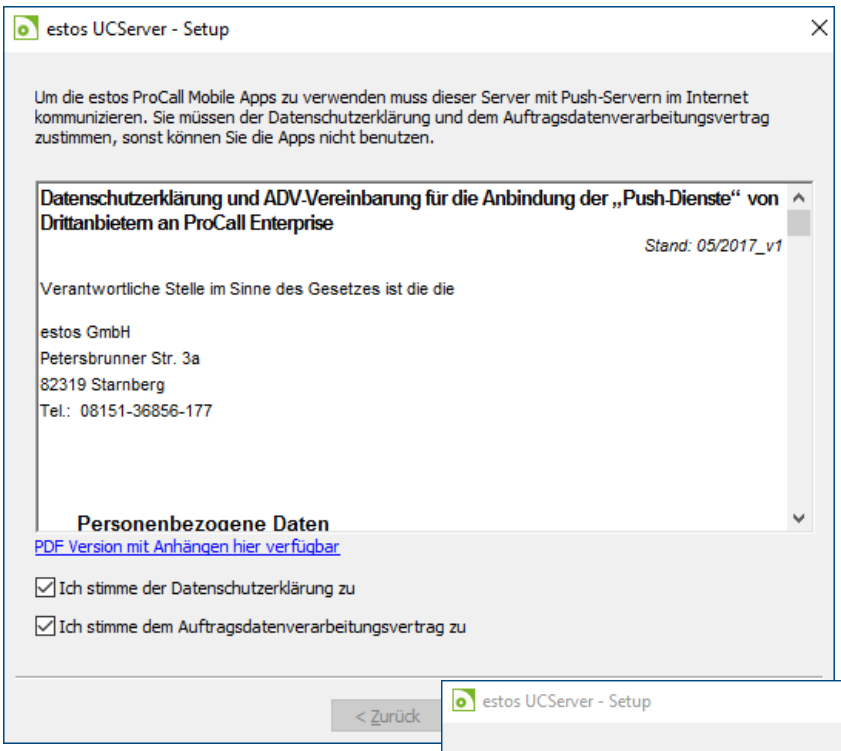
ucpush.ucconnect.de auf Port 443

Ein Empfang von Daten aus dem Internet ist nicht erforderlich.

2.1.2. UCServer zum Versand von Push-Nachrichten einrichten

Starten Sie den UCServer Admin und öffnen Sie *Allgemein – Online Dienste*. Starten Sie unter *Eigenen Server verwenden* den Einrichtungs-Wizard über den Button *Jetzt konfigurieren...*



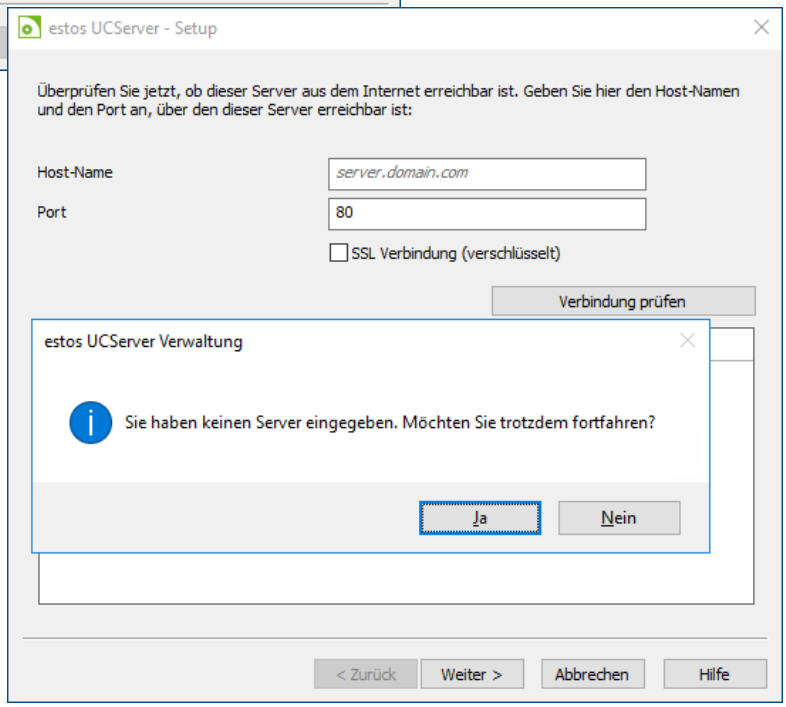


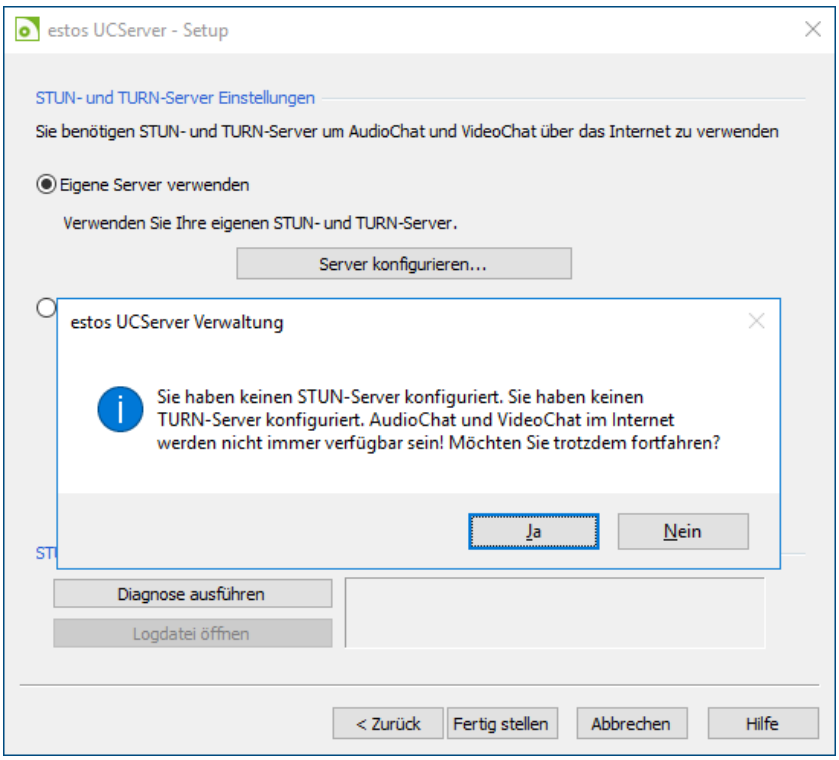
Wird der Wizard das erste Mal gestartet, werden Datenschutzerklärung und ADV-Vereinbarung angezeigt.

Beiden muss zugestimmt werden, bevor die Push-Dienste genutzt werden können

Klicken Sie auf *Weiter,* um den Wizard fortzusetzen.

Da die Mobile Apps nicht aus dem Internet auf den UCServer zugreifen sollen, kann das nächsten Fenster ohne Angabe des Host-Namens mit *Weiter* und die Hinweis-Meldung mit *Ja* übersprungen werden.





Wenn auch kein Audio-/Video-Chat oder Softphone-Funktionen zum Einsatz kommen sollen, kann auch das letzte Fenster ohne Angabe von Informationen mit *Fertig stellen* geschlossen und die Hinweis-Meldung mit *Ja* übersprungen werden.

Die Einrichtung von UCServer für den Versand von Push-Nachrichten ist abgeschlossen.

Das Vorgehen zum Einrichten und Verwalten der Benutzer und Mobile Apps wird in Kapitel 4 erklärt.

3. Mobile Apps von extern nutzen

Soll der Zugriff per Mobile App auch von außerhalb des lokalen Netzwerks möglich sein, müssen die entsprechenden Dienste/Schnittstellen von UCServer aus dem Internet erreichbar sein.

Zu unterscheiden ist auch hier die Nutzung von:

- **Präsenz, Text Chat, Steuerung der Telefonleitung und Kontaktsuche**
  Hierfür müssen die mitinstallierten UCServer Web Services auch aus dem Internet erreichbar sein.
- **Sprach- und Video-Übertragungen (Audio/Video und Softphone)**
  Zusätzlich zu den UCServer Web Services müssen ein STUN- und ein TURN-Server von intern und extern erreichbar sein.

In beiden Fällen wird zusätzlich der Versand von Push-Nachrichten (siehe 2.1) benötigt.

3.1. Voraussetzungen

Unabhängig davon, in welchem Umfang die Dienste von UCServer für die Nutzung von extern zur Verfügung gestellt werden sollen, müssen die folgenden Voraussetzungen zur Veröffentlichung von UCServer erfüllt sein.

3.1.1. Öffentliche IP-Adresse und DNS

Öffentliche IP Adresse

Ihr Internetzugang muss über eine öffentliche IP Adresse verfügen. Bevorzugt solle es sich um eine statische (feste) IP-Adresse handeln.

DNS Eintrag

Für die leichtere Konfiguration der Verbindung in den Mobile Apps ist ein DNS Eintrag sinnvoll, es kann aber auch die IP-Adresse zur Konfiguration genutzt werden.

UCServer

Der Name des **UCServer** (z. B. *ucws.domain.com*) sollte sowohl im internen Netzwerk als auch im Internet über DNS aufgelöst werden können, da ansonsten die Mobile Apps unterschiedliche Verbindungsdaten benötigen würden.

Im Internet muss die öffentliche IP Adresse, im LAN die lokale IP-Adresse zurückgegeben werden.

Eigener STUN/TURN-Server

Kommt ein **eigener STUN/TURN-Server** zum Einsatz**,** muss auch dieser Name sowohl von intern als auch von extern aufgelöst werden können. Hier muss in beiden Fällen die **externe** IP-Adresse zurückgegeben werden.

Fügen Sie jeweils einen DNS A Record zu Ihrer Domain hinzu (z. B. *ucws.domain.com* und/oder *turn.domain.com*).

Steht keine feste IP-Adresse zur Verfügung, **MUSS** im *DynDNS* im Internet ein entsprechender DNS Eintrag eingetragen werden, z. B: *ucws.domain.com* -> externe IP-Adresse.

Optional: Serveradresse in den Mobile Clients automatisch konfigurieren

Sie können Ihren Benutzern das Einrichten ihres ProCall Mobile Clients erleichtern. Der Mobile Client kann die zum Login benötigte öffentliche Adresse Ihres UCServer automatisch über einen DNS-Server-Eintrag abfragen. Der Benutzer muss damit nur noch Benutzername und Passwort eingeben.

DNS-SRV Eintrag

Richten Sie zusätzlich zu dem A-Record für den UCServer folgenden DNS-SRV Eintrag für Ihre Domain ein:

Name:	_ctiwebserver
Protokoll:	TCP
Target-Domain:	Öffentliche Domain oder IP Adresse des UCServer (z.B. ucws.domain.com)
Target-Port:	Öffentlicher Port des UCServer (HTTPS Port: 443 bzw. 7225)
Beispiel:	_ctiwebserver._TCP.domain.com

Informationen zu den benötigten Ports entnehmen Sie Kapitel 3.1.3 Benötigte Port- und Firewall Regeln

3.1.2. Verschlüsselung und SSL Zertifikat

Es ist empfehlenswert, die Verbindung von externen Teilnehmer zu verschlüsseln.

estos empfiehlt dringend den Einsatz von https mit einem vertrauenswürdigen SSL Zertifikat. Das Zertifikat sollte von einer öffentlichen Zertifizierungsstelle (*Certificate Authority / CA*) ausgestellt sein, die von den gängigen Browsern und Betriebssystemen als vertrauenswürdig eingestuft ist. Falls notwendig, beantragen Sie ein SSL Zertifikat für Ihren DNS-Namen bei einer öffentlichen Zertifizierungsstelle.

Falls Sie mit einem selbst signierten Zertifikat (*Self Signed Certificate*) arbeiten, ist die Verbindung verschlüsselt, aber nicht abhörsicher und die Nutzung von Browser Applikationen ist ggf. nicht möglich.

Im Falle von Port Forwading werden alle Anfragen aus dem Internet direkt von den UCServer Web Services entgegengenommen. Damit ist dieser auch für die Verschlüsselung der Verbindung verantwortlich. Das Zertifikat muss im UCServer hinterlegt werden.

Werde die UCServer Web Services über einen Reverse Proxy veröffentlicht, werden alle Anfragen aus dem Internet zuerst vom Proxy entgegengenommen und danach an den UCServer Web Services weitergeleitet. Damit ist der Proxy auch für die Verschlüsselung der Verbindung verantwortlich.

In diesem Fall muss das SSL-Zertifikat in dem Reverse Proxy eingetragen werden.

Achtung

Ein vertrauenswürdiges Zertifikat ist für die Nutzung der Browser-Applikationen zwingend notwendig.

3.1.3. Benötigte Port- und Firewall Regeln

Die benötigten Port- und Firewall-Regeln sind abhängig von der Topologie des Netzwerkes und den zu veröffentlichenden Diensten des UCServer bzw. den genutzten estos Diensten im Internet. Die nachfolgende Aufstellung zeigt, was generell in den Routern/Firewalls einzurichten ist.

Generell müssen die Router/Firewalls so eingerichtet werden, dass eine einmal aufgebaute Verbindung offen bleibt und alle zusätzlich benötigten/angeforderten Ports genutzt werden können.

Nur Push-Service:

Ausgehend:	
Quelle:	UCServer
Ziel:	ucpush.ucconnect.de
Port:	443, TCP

UCServer Web Services:

Veröffentlichung des Servers per NAT

Eingehend:	
Quelle:	alle
Ziel:	UCServer
Ziel-Port:	http: 7224 TCP und/oder https: 7225, TCP

estos UCConnect:

Ausgehend:	
Quelle:	UCServer und alle ProCall Clients
Quell-Port:	alle
Ziel:	*.ucconnect.de
Ziel-Port:	3478 und 443, UDP und TCP

estos STUN/TURN Server:

Veröffentlichung des Servers per NAT

Eingehend:

Quelle:	alle
Ziel:	estos STUN/TURN-Server
Ziel-Port:	3478, UDP und TCP

Freigabe der lokalen Teilnehmer

Ausgehend:

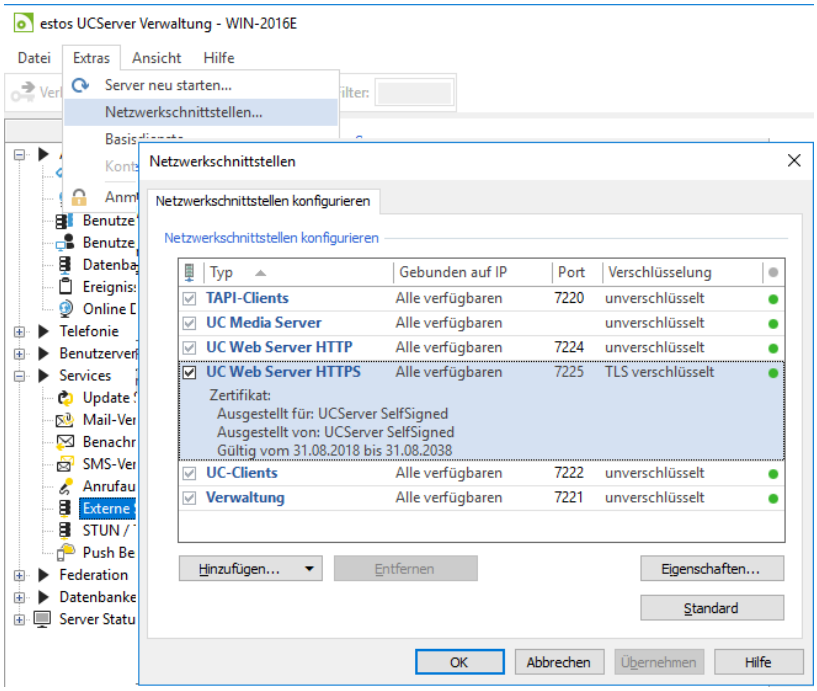
Quelle:	UCServer und alle estos Clients
Quell-Port:	Alle
Ziel:	estos STUN/TURN-Server
Ziel-Port:	3478, UDP und TCP

3.2. Web Services Schnittstelle in UCServer konfigurieren

Sollen einige oder alle Funktionen von UCServer von extern erreichbar sein und es wird nicht UCConnect eingesetzt, müssen die Web Services von UCServer über das Internet erreichbar sein.

3.2.1. IP-Adresse und Port

Die IP-Adresse und den für die Web Services festgelegten Port können Sie im Menü des *UCServer Admin* unter *Extras – Netzwerkschnittstellen* einsehen und ändern. Die Mobile Apps müssen von extern/aus dem Internet auf die hier eingetragene IP-Adresse/Port Kombination zugreifen können.

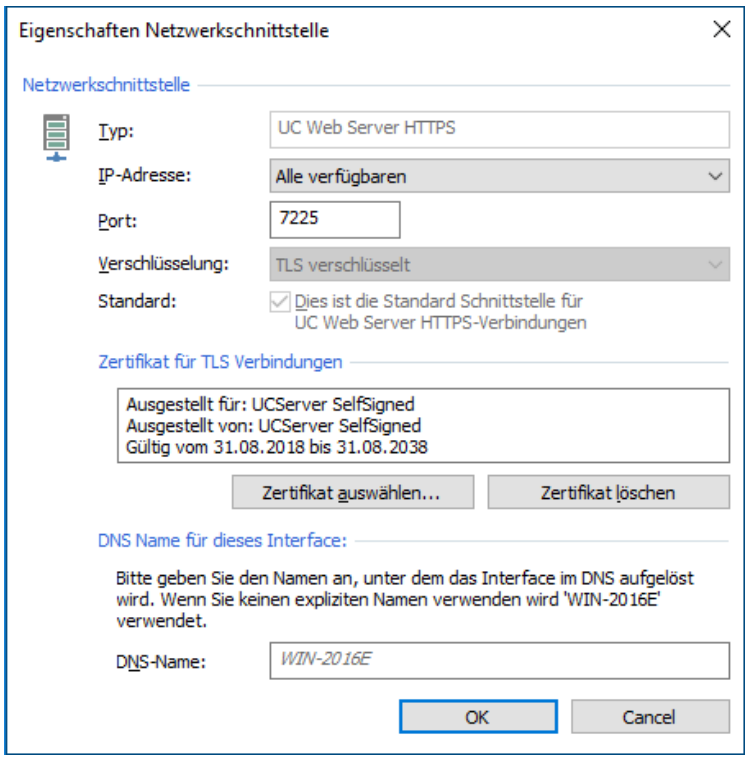


In der Standardeinstellung beantwortet der UCServer Anfragen über http auf Port 7224 und https auf Port 7225.

Wird der UCServer über einen anderen Port veröffentlicht, sollte dieser Port hier auch eingetragen und genutzt werden.

3.2.2. Zertifikat eintragen

Die Verbindung der Mobile Apps mit dem UCServer über das Internet sollte immer verschlüsselt erfolgen.



Wird die Veröffentlichung ohne Einsatz eines http Proxy gemacht, muss im UCServer ein gültiges Zertifikat hinterlegt sein.

Beachten Sie die Hinweise unter 3.1.2 Verschlüsselung und SSL-Zertifikat

Um ein Zertifikat zu hinterlegen machen Sie einen Doppelklick auf den Eintrag *UC Web Server HTTPS* und klicken auf *Zertifikat auswählen…*.

3.3. Mobile App ohne Audio/Video und Softphone

3.3.1. Veröffentlichen der UCServer Web Services

Zusammen mit dem UCServer wird immer ein Web Service installiert, welcher dauerhaft mit dem UCServer verbunden ist. Diese UCServer Web Services ermöglichen Ihnen die Nutzung der Funktionen:

- Präsenz
- Text Chat
- Steuerung der Telefonleitung
- Kontaktsuche

Um diese Dienste in der ProCall Mobile App und den Web Anwendungen nicht nur im lokalen Netzwerk, sondern auch über das Internet nutzen zu können, müssen die UCServer Web Services im Internet verfügbar sein.

Bei der Veröffentlichung unterscheiden wir grundsätzlich 2 verschiedene Szenarien.

Die Veröffentlichung ohne DMZ

- Der UCServer hat eine öffentliche IP Adresse, d.h. er ist direkt mit dem Internet verbunden (nicht empfohlen und nicht erläutert)
- Der UCServer hat keine öffentliche IP Adresse, d.h. er befindet sich hinter einem NAT-Device, und *Port Forwarding* wird verwendet.

Die Veröffentlichung mit DMZ

- Der UCServer hat keine öffentliche IP Adresse, d.h. er befindet sich hinter einem NAT-Device, und *http Reverse-Proxy* in einer DMZ wird verwendet.

  Beachten Sie, dass der UCServer im lokalen Netzwerk und Internet unter demselben Namen erreichbar sein sollte.

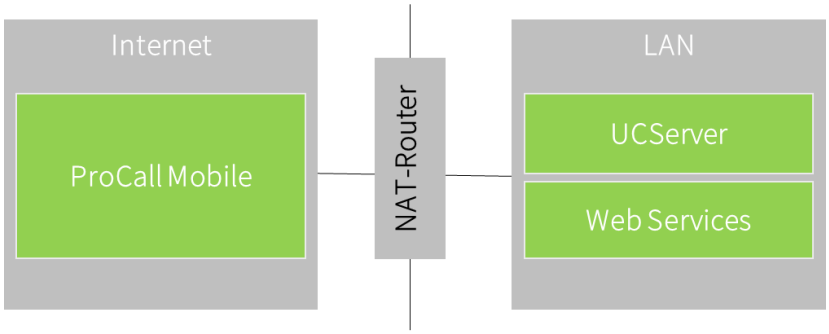
  Sehen Sie hierzu: Voraussetzungen - Öffentliche IP-Adresse und DNS

  Zusätzlich sollten die Push-Nachrichten an die Mobile Apps gesendet werden. Der Dienst wird bei der Konfiguration des UCServer automatisch mit eingerichtet.

  Die Firewall am UCServer Rechner und auf dem Gateway zum Internet muss so eingerichtet werden, dass der UCServer die Push-Nachrichten an ***ucpush.ucconnect.de:443*** versenden darf.

3.3.2. Veröffentlichung ohne DMZ

In dem Szenario ist der UCServer durch eine Firewall/Router vom Internet getrennt.



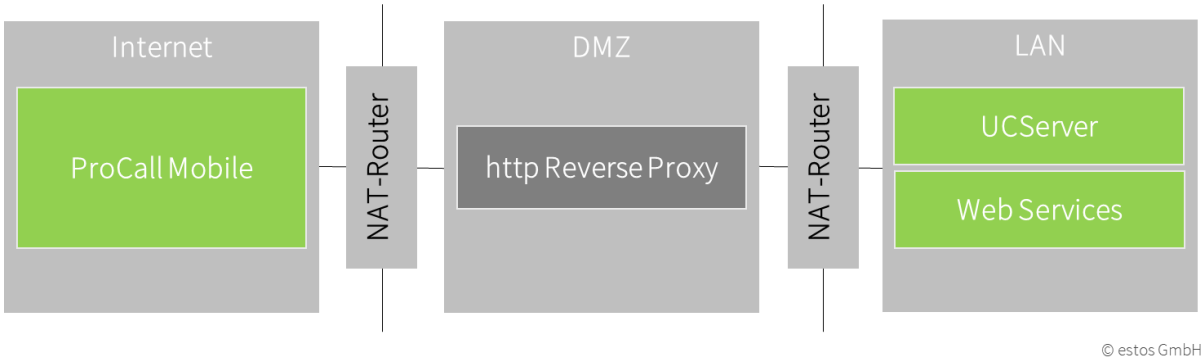
Konfigurieren Sie an Ihrem NAT-Router ein Port Forwarding. Leiten Sie die (auf Ihrer öffentlichen IP-Adresse z. B. auf Port 443 TCP) eingehenden Verbindungen auf den https-Port der UCServer Web Services (Standard: 7225) weiter.

SSL-Zertifikat

Achten Sie darauf, in den UCServer Web Services ein gültiges Zertifikat zu hinterlegen um die Verbindungen verschlüsseln zu können. Beachten Sie die Hinweise unter 3.1.2 Verschlüsselung und SSL-Zertifikat

3.3.3. Veröffentlichung mit DMZ

Sollen die UCServer Web Services über eine DMZ hinweg veröffentlicht werden, muss ein *http Reverse Proxy* eingesetzt werden. Darunter versteht man einen Server, der http(s) Anfragen entgegennimmt und an einen Server im privaten Netz weiterleitet.



SSL Zertifikat

In diesem Fall muss das SSL-Zertifikat **im Reverse-Proxy** eingetragen werden.

Im Falle eines http Reverse-Proxy werden alle Anfragen aus dem Internet zuerst vom Proxy entgegengenommen und danach an UCServer Web Services weitergeleitet, damit ist der Proxy auch für die Verschlüsselung der Verbindung verantwortlich.

Beachten Sie die Hinweise unter 3.1.2 Verschlüsselung und SSL-Zertifikat

Je nach Anforderung können Sie die Anfragen innerhalb Ihres LAN

- über **unverschlüsseltes http**
- oder **mit TLS Verschlüsslung**

weiterleiten.

http Reverse-Proxy

Es können alle standardkonformen http Reverse-Proxy Server verwendet werden, die http GET und POST und Websocket Verbindungen (RFC 6455) ermöglichen.

Der Proxy-Server muss so eingerichtet werden, dass er die von der öffentlichen IP-Adresse eingehenden Anfragen an die UCServer Web Services weiterleitet.

Die benötigten Informationen zu IP-Adresse und Port für UCServer Web Services finden Sie in der UCServer Verwaltung (siehe 3.2 Web Services Schnittstelle konfigurieren).

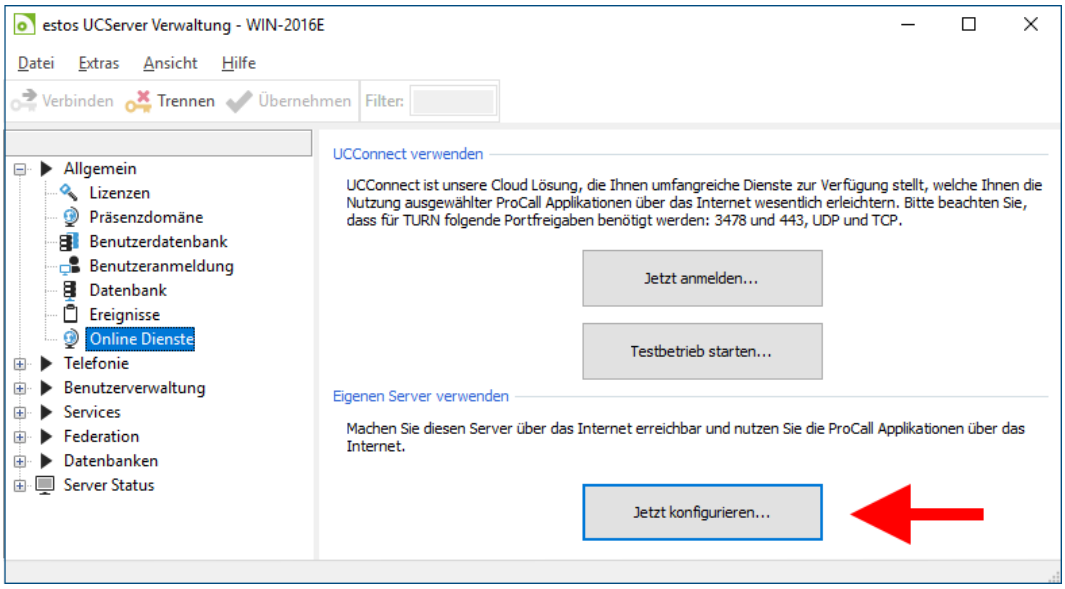
Im Anhang dieses Dokumentes wird konkret auf die Einrichtung von den folgenden Proxy Servern eingegangen:

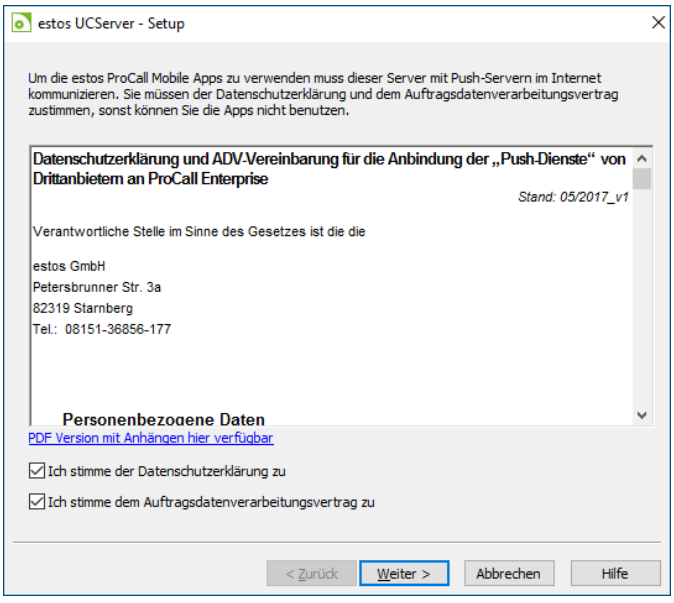
- Microsoft Internet Information Services (IIS)
- Nginx (Linux)

3.3.4. Einrichten von UCServer

Die Einrichtung von UCServer ist unabhängig davon, ob er über NAT oder einen http-Reverse Proxy frei gegeben werden soll.

Starten Sie den *UCServer Admin* und öffnen Sie *Allgemein – Online Dienste*. Starten Sie unter *Eigenen Server verwenden…* den Einrichtungs-Wizard über den Button *Jetzt Konfigurieren…*



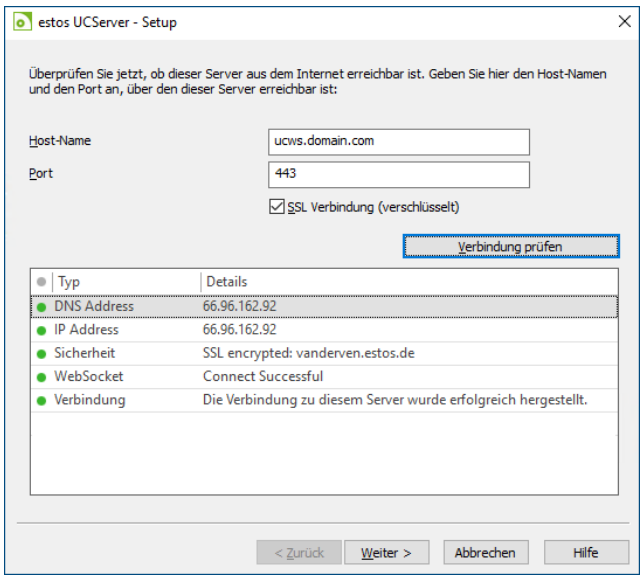


Wird der Wizard das erste Mal gestartet, werden Datenschutzerklärung und ADV-Vereinbarung angezeigt.

Beiden muss zugestimmt werden, bevor die Push-Dienste genutzt werden können.

Klicken Sie auf *Weiter*, um den Wizard fortzusetzen.

Geben Sie den (im Internet und im lokalen Netzwerk) im DNS eingetragenen Hostnamen an und legen Sie den Port fest.

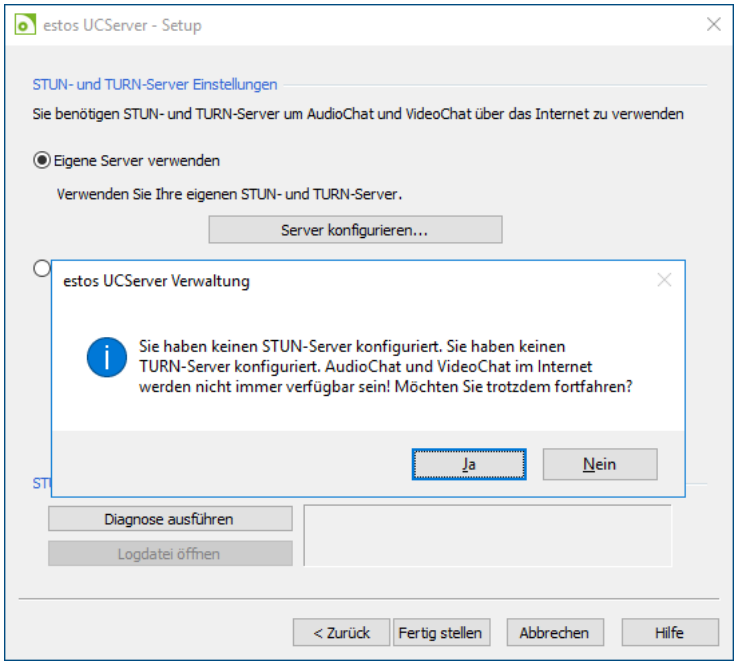


Über *Verbindung prüfen* wird ein Testprogramm gestartet, das folgendes ausführt:

- Verbindungsaufbau ins Internet
- Überprüfung der DNS-Auflösung
- Verbindung mit dem gefundenen Server

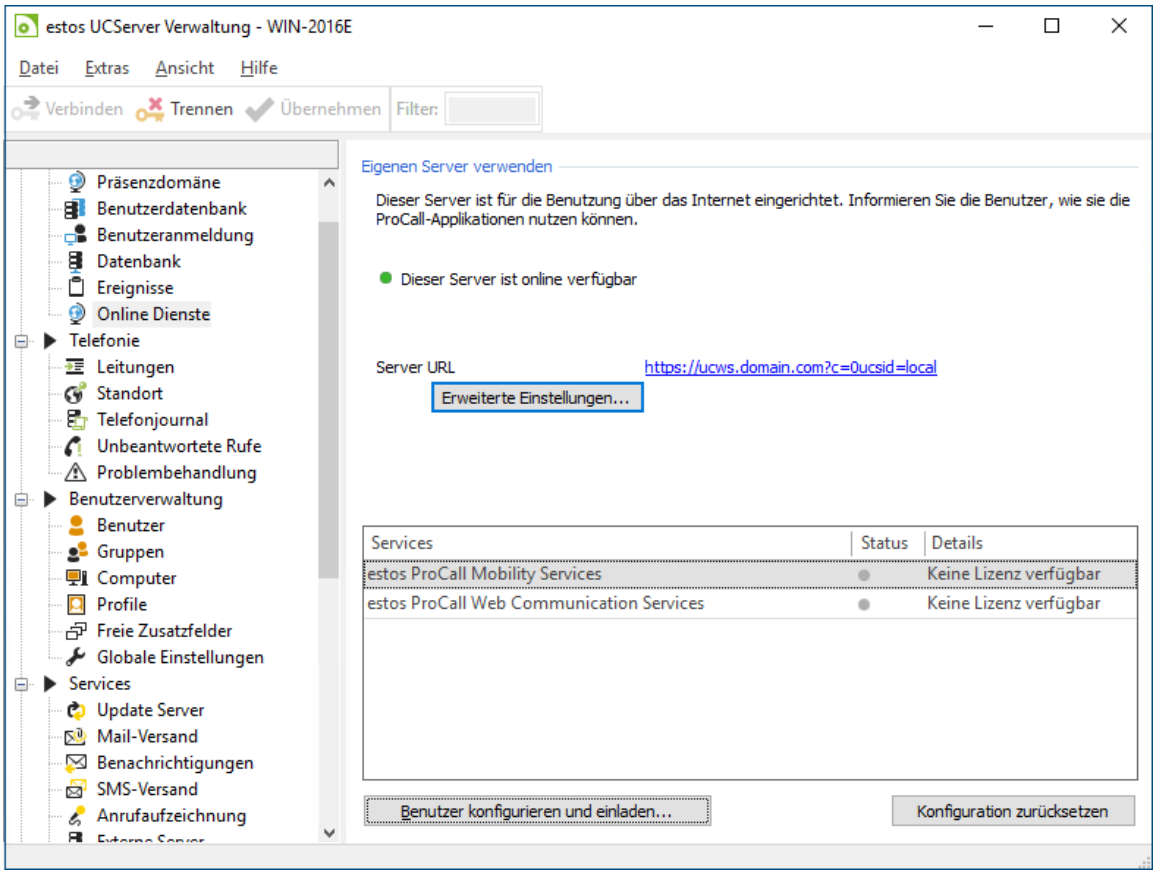
Alle Tests müssen erfolgreich sein, damit die Funktion sichergestellt werden kann. Im Fehlerfall können Sie auch den Wizard über *Weiter* fortführen und das Problem später analysieren.

Da Audio-/Video-Chat sowie Softphone nicht zum Einsatz kommen sollen, kann das letzte Fenster ohne Angabe von Informationen mit *Fertig stellen* abgeschlossen und die Hinweis-Meldung mit *Ja* übersprungen werden.



Die Veröffentlichung der UCServer Web Services und die Konfiguration für den Versand von Push-Nachrichten ist abgeschlossen.

Nach der Konfiguration wird die Verfügbarkeit des Servers angezeigt.



Als letzten Schritt müssen die Benutzer eingerichtet und optional per E-Mail benachrichtigt werden.

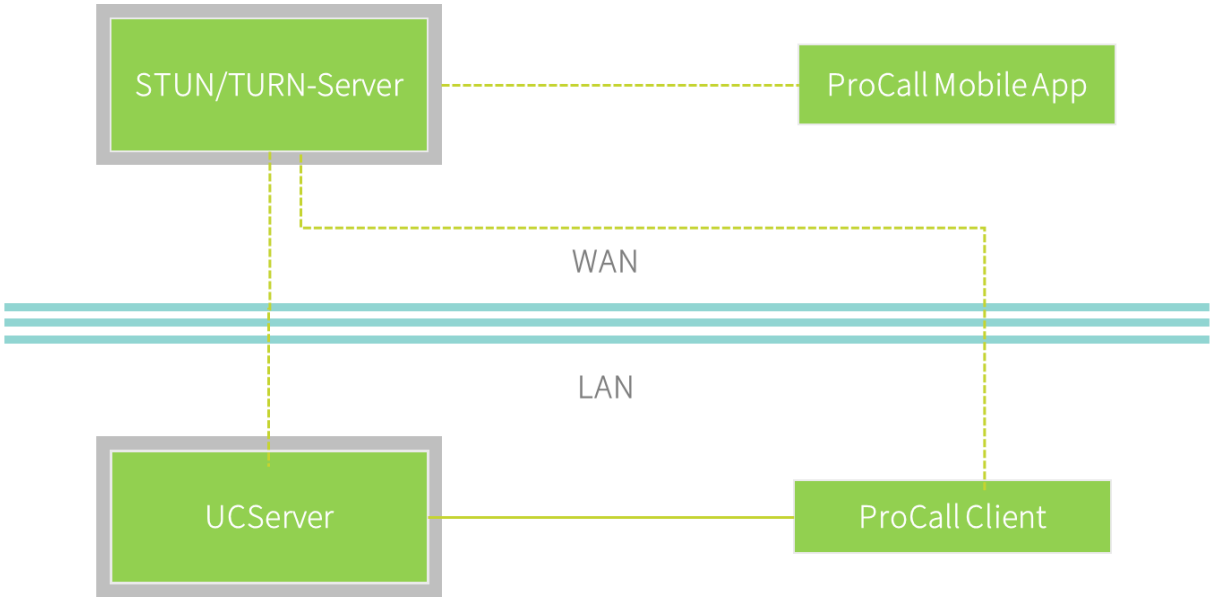
Das Vorgehen zum Einrichten und Verwalten der Benutzer und Mobile Apps wird in Kapitel 4. erklärt.

3.4. Mobile App mit Audio/Video und Softphone von extern nutzen

Werden die Sprachdienste von den Clients (Windows ProCall, Mobile App) nur im lokalen Netzwerk genutzt, können die Clients eine direkte Verbindung zum UCServer und untereinander aufbauen, um die Sprachpakete auszutauschen.

Wenn die an der Kommunikation beteiligten Clients keine direkte Verbindung zueinander und/oder zum UCServer aufbauen können, werden für die Übertragung von Sprachdaten ein STUN- und ein TURN-Server benötigt.

In diesem Fall benötigen alle an der Kommunikation beteiligten Clients eine Verbindung zu diesen Servern. Der STUN/TURN-Server muss also aus dem Internet erreichbar sein.



Grundsätzlich gibt es zwei Möglichkeiten, einen STUN/TURN Server zu nutzen:

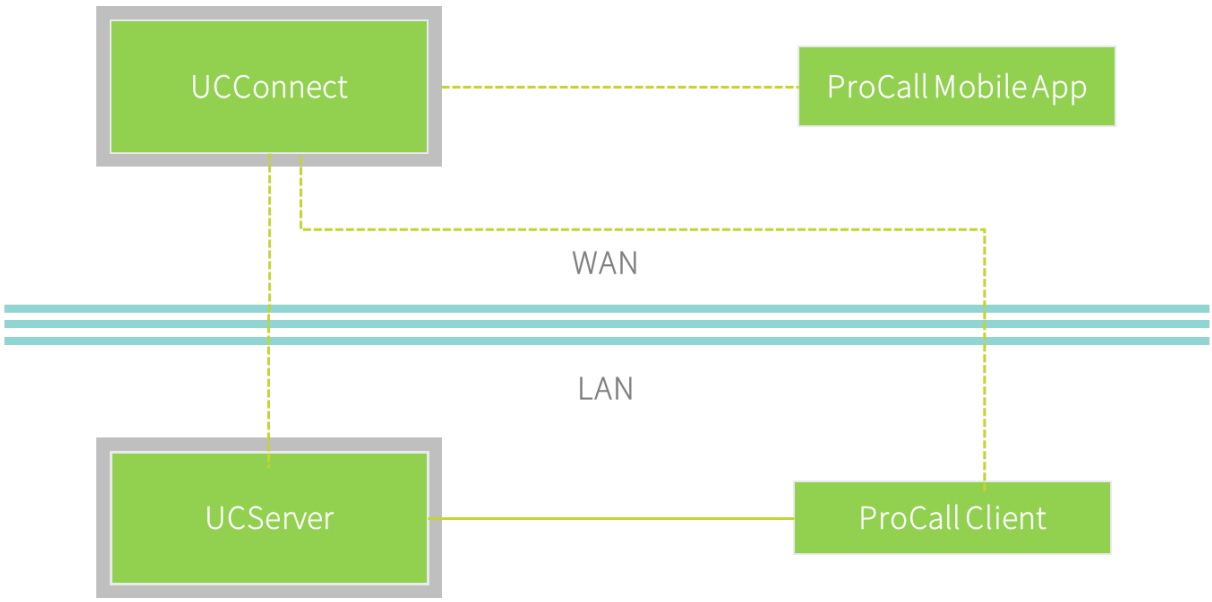
- **estos UCConnect**
  - Cloud Dienst der Firma estos -> im Internet verfügbar
  - leicht einzurichten
  - geringe Anforderungen an die Netzwerkkonfiguration
  - für kleine und mittlere Umgebungen empfohlen
- **separater estos STUN/TURN Server**
  - muss selbst zur Verfügung gestellt werden
  - STUN/TURN Server muss aus dem Internet erreichbar sein
  - UCServer Web Services müssen aus dem Internet erreichbar sein
  - relativ leicht einzurichten
  - geringe Anforderungen an die Netzwerkkonfiguration
  - für mittlere und große Unternehmen

Ausführliche Information über die Funktionsweise von STUN/TURN und ICE, sowie Erklärungen zu den weiteren, benötigten Funktionen und Komponenten finden Sie im Anhang unter „Informationen zu STUN/TURN“.

3.4.1. UCConnect

Mit UCConnect bietet estos einen einfachen Weg, den Mobile Apps alle Funktionen inklusive Audio-/Video-Chat und Softphone zur Verfügung zu stellen.

UCConnect stellt unter anderem die benötigten Funktionen für die Sprachübertragung zwischen den Teilnehmern zur Verfügung.



Informationen zu Kosten und Nutzungsbedingungen erhalten Sie im estos Vertrieb.

Grundsätzliche Vorbereitung

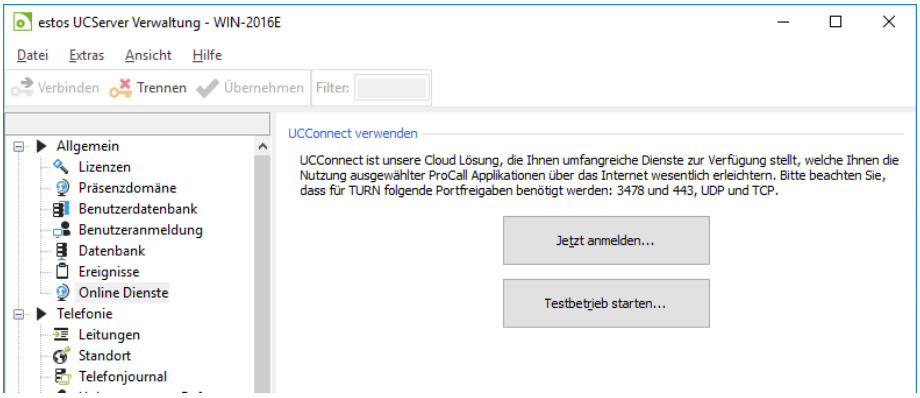
Die Firewalls/Router müssen so eingerichtet werden, dass alle internen ProCall Clients und der UCServer eine Verbindung zu UCConnect aufbauen können.

Außerdem muss der UCServer Daten an den Push-Dienst senden können.

Beachten Sie die Hinweise unter: 3.1.3 Benötigte Port- und Firewall Regeln

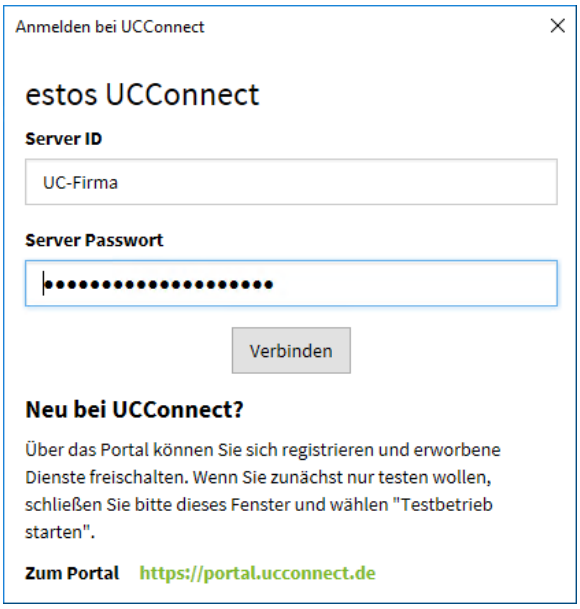
Die Veröffentlichung der UCServer Web Services (siehe 3.3) und das Einrichten des Push-Dienstes sind **nicht erforderlich**.

Starten Sie den UCServer Admin und öffnen Sie unter *Allgemein - Online Dienste*.



Sie können jetzt einen Testbetrieb starten oder sich mit der Server-ID bei UCConnect anmelden.

Ihren Server und die benötigten Lizenzen verwalten Sie über die Webseite https://portal.ucconnect.de im UCConnect Portal.



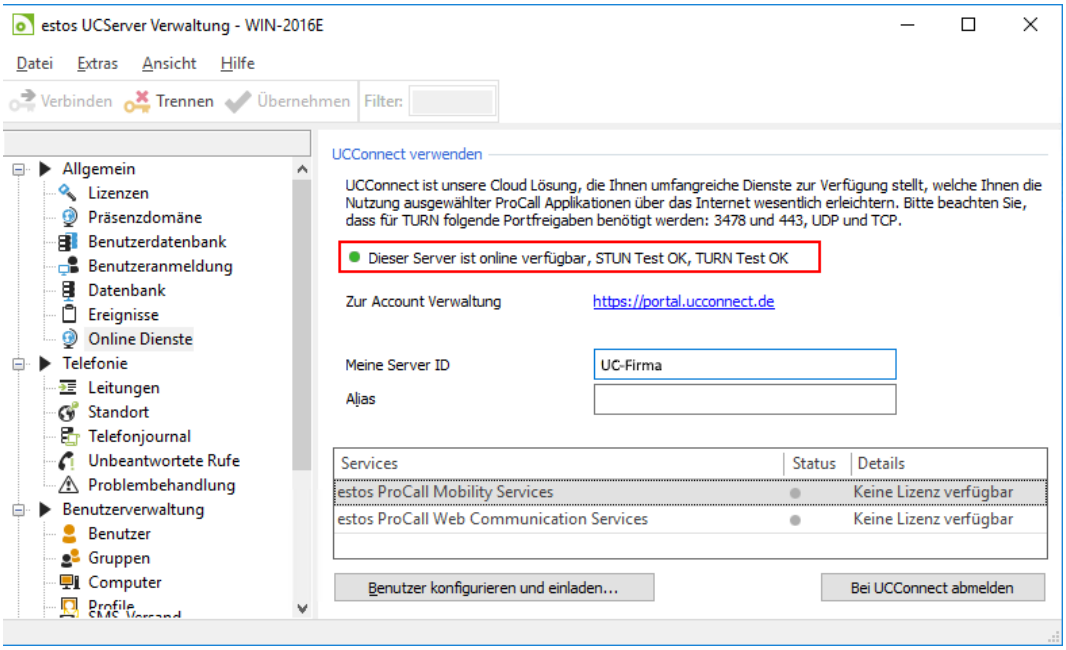
Haben Sie noch kein Konto im UCConnect Portal angelegt, können Sie die Webseite des Portals direkt aufrufen und sich registrieren oder den Testbetrieb nutzen.

Bitte beachten Sie:

Beim ersten Starten/Einrichten der UCConnect Verbindung werden die Lizenzinformationen angezeigt. Die UCConnect Dienste inkl. der Apple/Google-Push-Dienste können vollständig nur genutzt werden, wenn Sie die angezeigten Bedingungen akzeptieren.

Nach Angabe der UCServer ID und des Passwortes klicken Sie auf *Verbinden*.

Der UCServer prüft automatisch die Verbindung zu UCConnect und gibt das Ergebnis aus.



Konnte keine Verbindung aufgebaut werden, prüfen Sie bitte Ihre Firewall/Router Konfiguration.

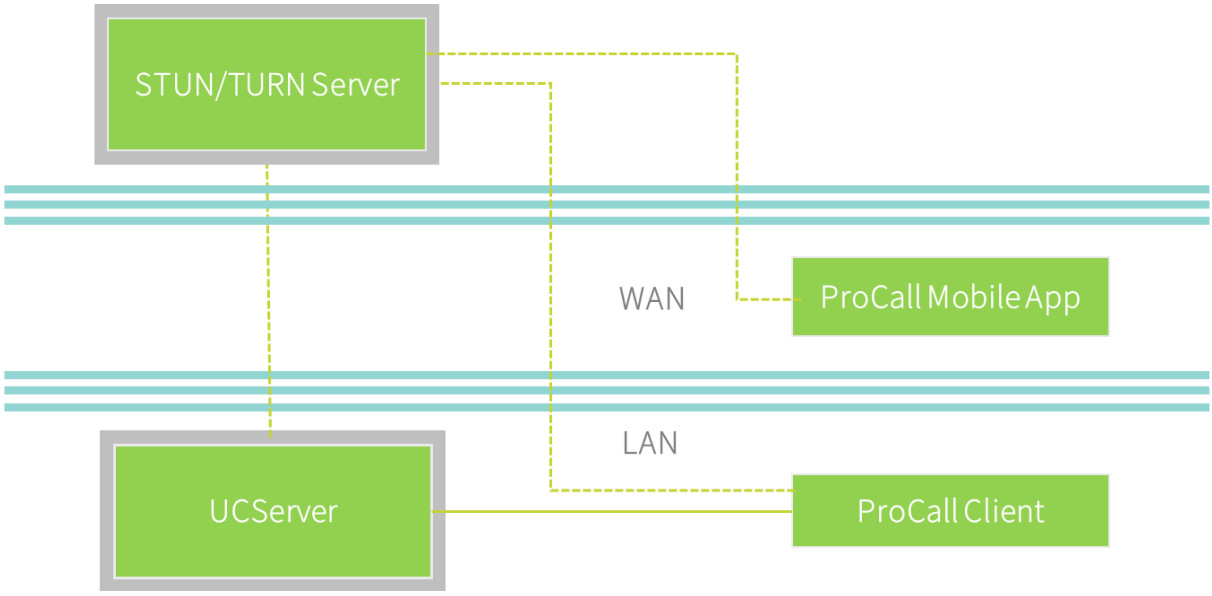
Im unteren Bereich können Sie Ihre Lizenzen überprüfen. Eingetragen und gelöscht werden diese über das UCConnect Portal.

Als letzten Schritt müssen die Benutzer eingerichtet und optional per E-Mail benachrichtigt werden.

Das Vorgehen zum Einrichten und Verwalten der Benutzer und Mobile Apps wird in Kapitel 4. erklärt.

3.4.2. estos STUN/TURN-Server nutzen

Wenn Sie einen STUN/TURN Server für Ihr Unternehmen selbst betreiben und zur Verfügung stellen möchten, müssen Sie den estos STUN/TURN Server installieren und im Internet zur Verfügung stellen.



Alle beteiligten Komponenten (UCServer, Clients im LAN, Mobile Apps) müssen eine Verbindung zu diesem Server aufbauen können.

Der estos STUN/TURN Server wird im Download von ProCall Enterprise mitgeliefert, die Lizenz ist bei ProCall Enterprise mit enthalten.

Anmeldefunktionen müssen weiter vom UCServer zur Verfügung gestellt werden. Dafür müssen die UCServer Web Services zusätzlich aus dem Internet erreichbar sein. Sehen Sie hierzu auch 3.3: Mobile App ohne Audio/Video und Softphone (Veröffentlichen des UCServer)

Voraussetzungen

- Der estos STUN/TURN Server muss so installiert werden, dass er aus dem Internet (also über eine externe IP-Adresse) erreichbar ist.
- Er kann per NAT veröffentlicht oder direkt auf eine öffentliche IP-Adresse gebunden werden.
- Der estos STUN/TURN Server muss aus dem lokalen Netzwerk heraus und aus dem Internet unter demselben Namen z. B. *turn-uc.domain.com* und derselben **EXTERNEN** IP-Adresse erreichbar sein.
  Sehen Sie hierzu unter 3.2.1 Öffentliche IP-Adresse und DNS
- Der UCServer und die internen ProCall Clients müssen eine Verbindung zum estos STUN/TURN Server im Internet aufbauen können.

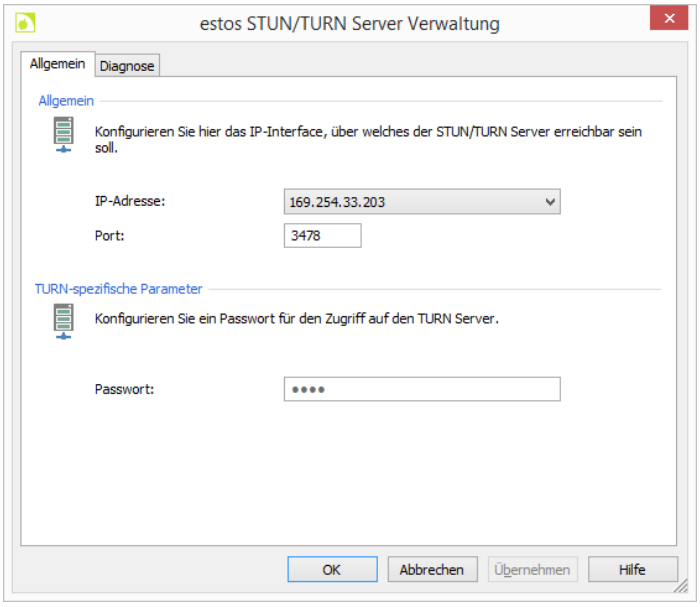
Die Installation und Einrichtung eines estos STUN/TURN Servers wird einfach durch Doppelklick auf das Installationspaket „STUN_TURN_Server_6.x.x.xxx.msi“ gestartet. Anschließend startet der Konfigurationsassistent, der durch die einzelnen notwendigen Einrichtungsschritte führt. Danach ist der Dienst einsatzbereit.

Für den Betrieb des estos STUN/TURN Servers sind einige Einstellungen notwendig. Um diese Einstellungen vorzunehmen, wird das Administrationsprogramm des estos STUN/TURN Servers verwendet.

Die benötigten Einstellungen sind abhängig von der Umgebung und dem gewünschten Szenario. Empfohlen wird die Veröffentlichung des Servers per NAT.

Allgemein

An die hier festgelegten Verbindungsdaten müssen die aus dem Internet eingehenden Verbindungen weitergegeben werden.



IP-Adresse und Port

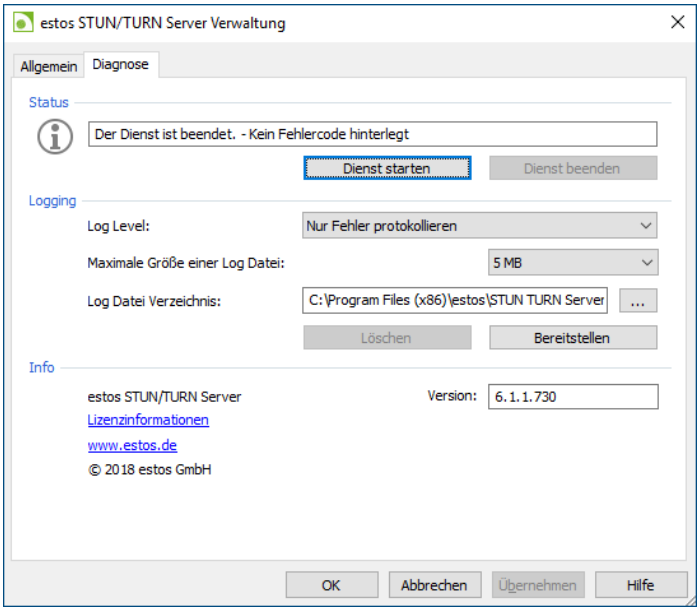
Wählen Sie eine der lokalen IP-Adressen des Rechners aus.

Der Default TCP Port für den Server ist Port 3478. Dieser sollte nicht geändert werden.

Passwort

Da der Transfer der Mediadaten zwischen den Clients hohe Bandbreitenanforderung an die Schnittstelle stellt, ist der Zugriff Passwort-geschützt. Dieses muss im UCServer ebenfalls eingegeben werden. Das Passwort sollte keine Umlaute enthalten.

Diagnose



Status

Hier kann der Dienst gestartet und beendet werden.

Logging

Stellen Sie den Log Level nur zur Fehlersuche in den Debug-Modus.

Bei Bedarf kann die Größe der Logdatei geändert werden.

Info

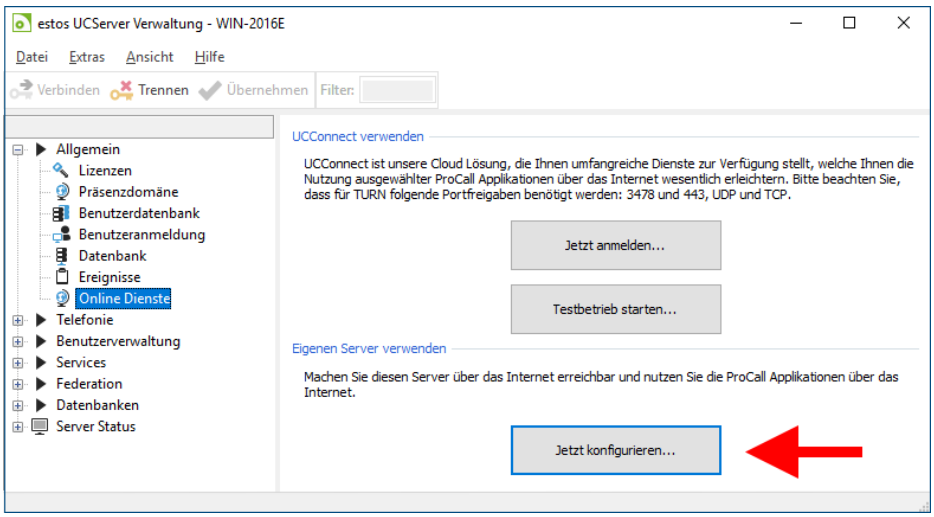
Die Version von STUN/TURN Server und installiertem UCServer sollten übereinstimmen.

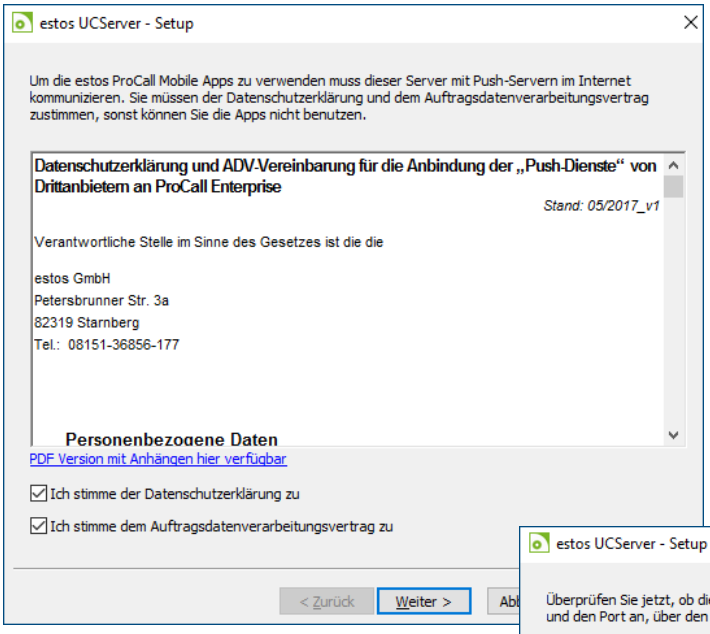
Starten Sie den Dienst und beenden Sie die Konfiguration mit *OK*.

Ab jetzt steht der STUN/TURN Server zur Verfügung

Konfiguration von UCServer

Starten Sie den *UCServer Admin* und öffnen Sie *Allgemein – Online Dienste*. Starten Sie unter *Eigenen Server verwenden* den Einrichtungs-Wizard über den Button *Jetzt konfigurieren…*

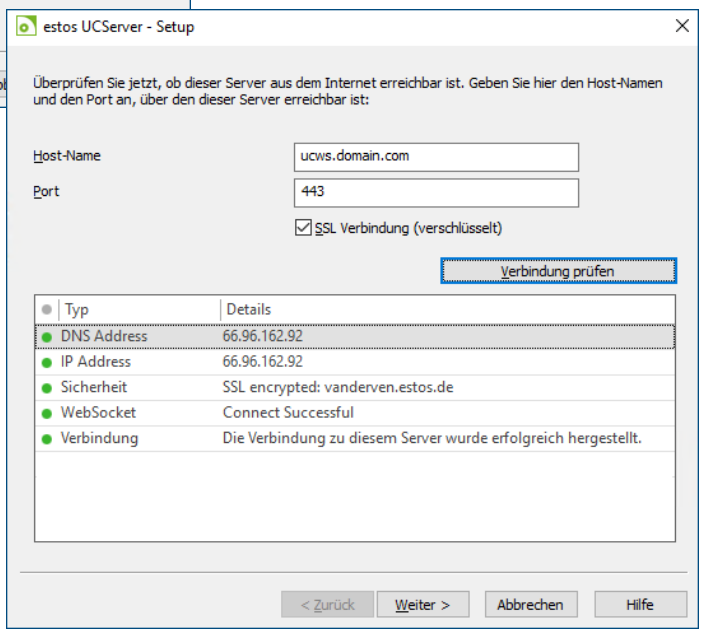




Wird der Wizard das erste Mal gestartet, werden Datenschutzerklärung und ADV-Vereinbarung angezeigt.

Beiden muss zugestimmt werden, bevor die Push-Dienste genutzt werden können

Klicken Sie auf *Weiter,* um den Wizard fortzusetzen.

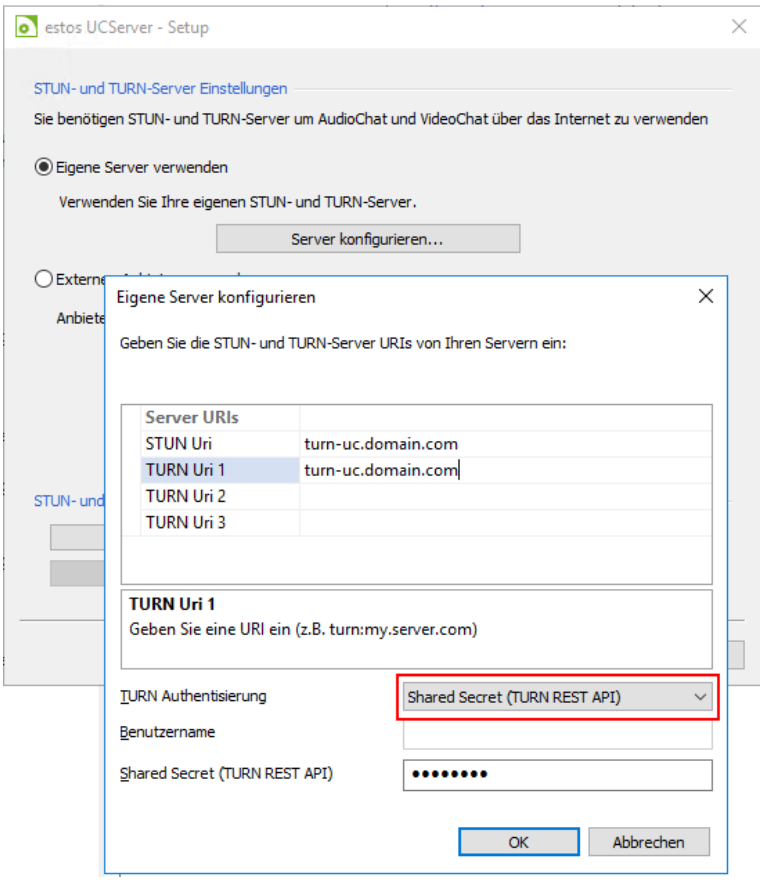


Geben Sie den (im Internet und im lokalen Netzwerk) im DNS eingetragenen Hostnamen an und legen Sie den Port fest.

Über *Verbindung prüfen* wird ein Testprogramm gestartet, das folgendes ausführt:

- Verbindungsaufbau ins Internet
- Überprüfung der DNS-Auflösung
- Verbindung mit dem gefundenen Server

Alle Tests müssen erfolgreich sein, damit die Funktion sichergestellt werden kann. Im Fehlerfall können Sie auch den Wizard über *Weiter* fortführen und das Problem später analysieren.



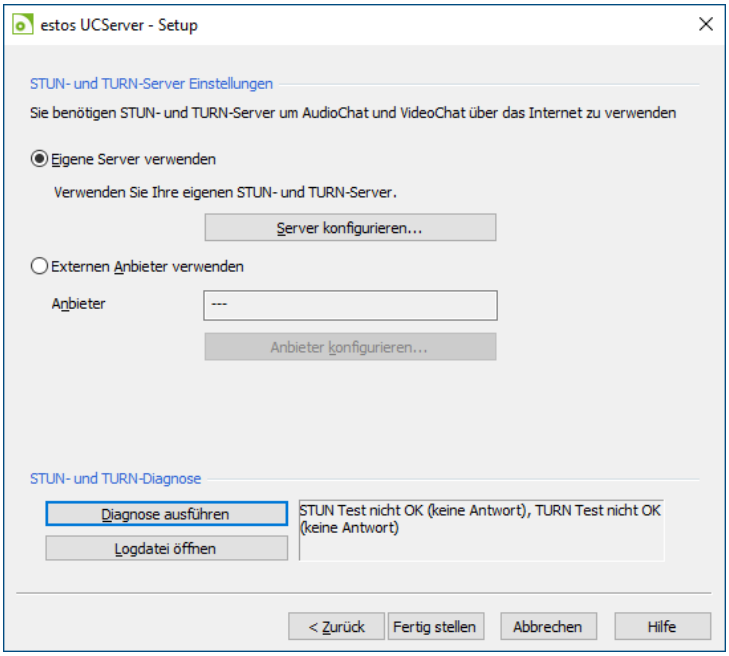
Danach muss in der Auswahl *Eigener Server verwenden – Server konfigurieren* der DNS-Name des estos STUN/TURN Servers angegeben werden.

Der Name muss sowohl als STUN Uri als auch als TURN Uri eingetragen werden.

Wählen Sie für die TURN Authentisierung *Shared Secret (TURN REST API)* aus.

Geben Sie unten das Kennwort ein, welches Sie auf der Karte *Allgemein* in der estos STUN/TURN Server Konfiguration vergeben haben.

Beenden Sie Eingabe mit OK



Zum Abschluss können Sie über *Diagnose ausführen* überprüfen ob der UCServer den estos STUN/TURN Server erreichen kann.

Die Konfiguration des UCServer für die Nutzung der Mobile Apps ist nun abgeschlossen.

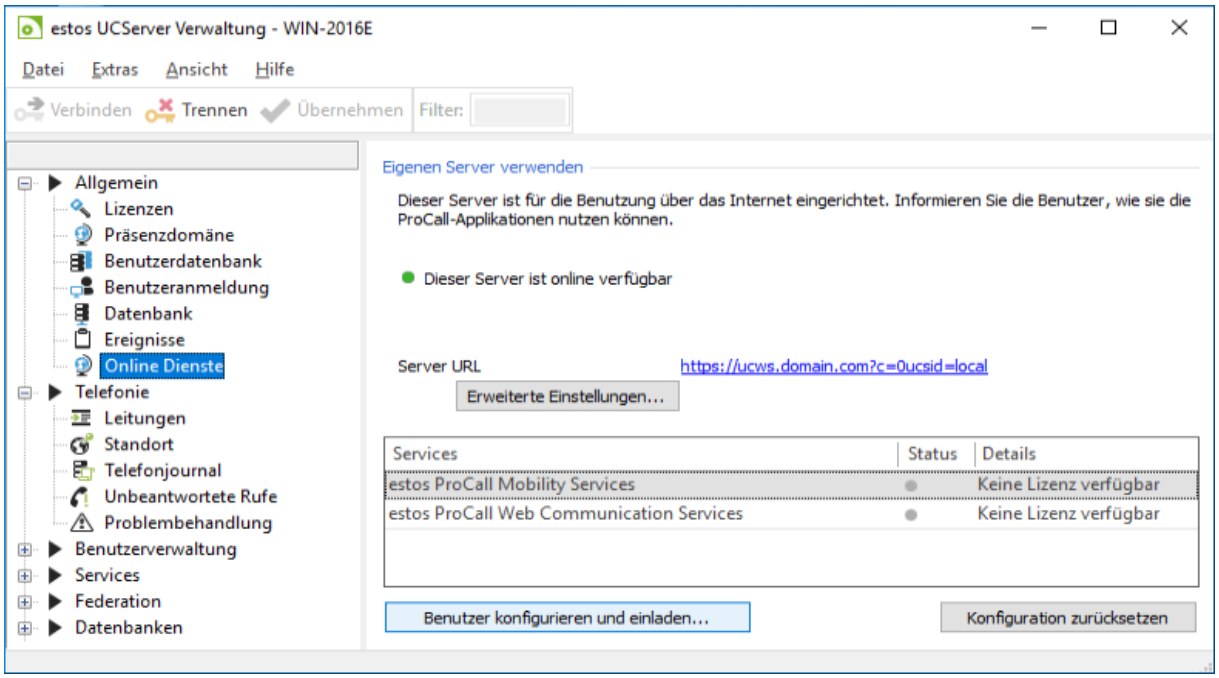
Als letzten Schritt müssen die Benutzer eingerichtet und optional per E-Mail benachrichtigt werden.

Das Vorgehen zum Einrichten und Verwalten der Benutzer und Mobile Apps wird in Kapitel 4. erklärt.

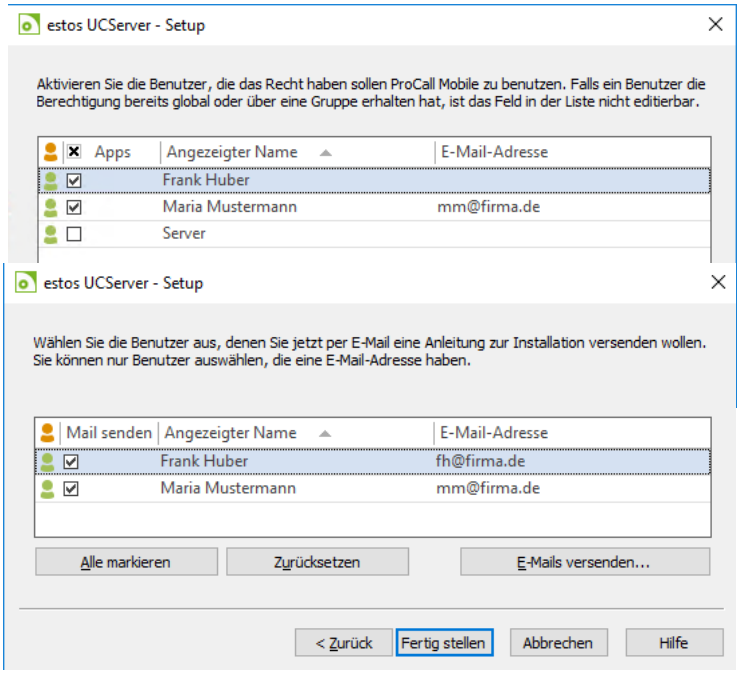
4. Benutzer und Mobile App einrichten und verwalten

Standardmäßig hat jeder ProCall Benutzer die Berechtigung, die Mobile Apps zu nutzen. Diese Berechtigung wird über die *Globalen Einstellungen* und/oder direkt am Benutzerobjekt vergeben.

Nach Konfiguration des UCServer für UCConnect oder Einrichten des estos STUN/TURN Server können die Benutzer im Bereich *Online Dienste* über einen Wizard eingerichtet und benachrichtigt werden.



Starten Sie den Wizard über den Button *Benutzer konfigurieren und einladen*



Zunächst können noch nicht berechtigte Benutzer aktiviert werden.

Im nächsten Schritt können Sie über den Button *E-Mails versenden* an die per Haken ausgewählten Benutzer eine E-Mail gesendet werden, die die Links zum Download der Mobile Apps und eine Anleitung für die Einrichtung enthält.

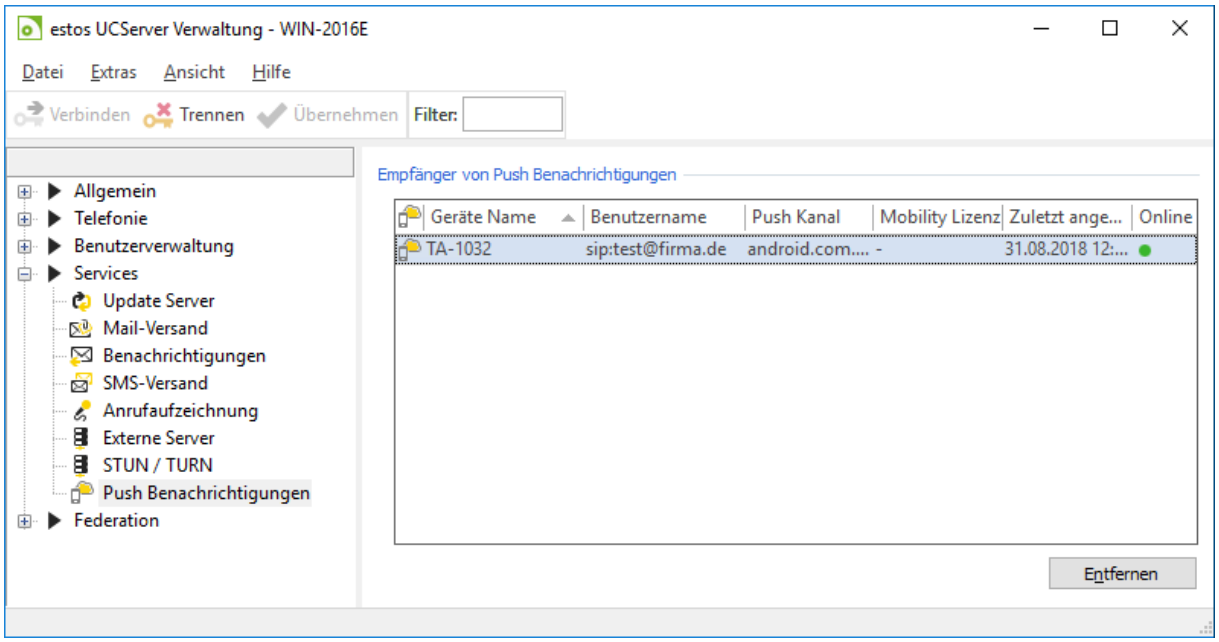
Sie können dazu noch eine zusätzliche Nachricht eingeben.

Beenden Sie den Wizard mit *Fertig stellen*.

Die Konfiguration, um die Mobile Apps mit Präsenz, Text Chat, Steuerung der Leitungen und Kontaktsuche auch im Internet nutzen zu können, ist nun abgeschlossen.

4.1. Registrierte Mobile Apps

Nach Neustart der Mobile Apps werden die am UCServer angemeldeten Geräte unter *Services – Push-Benachrichtigung* angezeigt



4.2. Einrichten der Mobile App

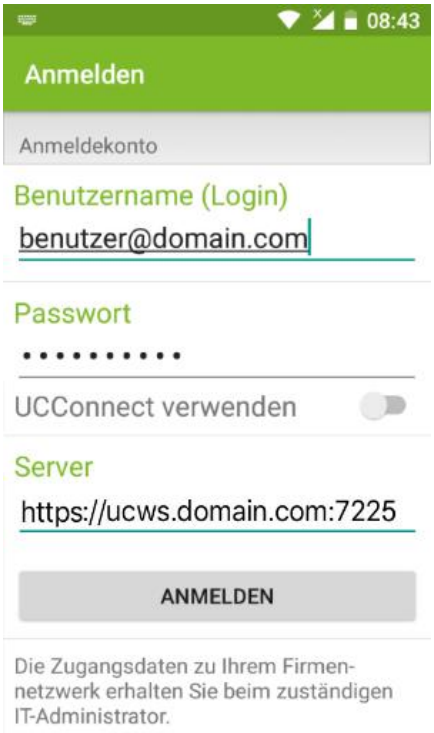
Nach Installation der Mobile App muss diese gestartet und die Verbindungsdaten eingegeben werden. Die Oberflächen der Apps bei Android und iOS sind ähnlich:

4.2.1. Anmeldekonto / Login

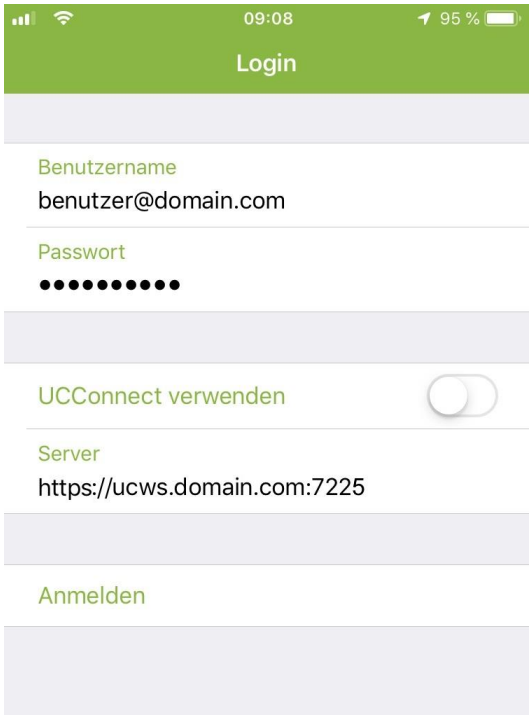
Geben Sie den Benutzernamen und das Passwort für die Anmeldung am UCServer an.

Konfiguration:

Android



iOS



UCConnect verwenden

Ist der UCServer mit UCConnect verbunden, aktivieren Sie diese Option. Die App wird sich automatisch mit dem UCConnect Servern verbinden.

Nutzen Sie den estos STUN/TURN Server, deaktivieren Sie *UCConnect verwenden*

Server

Wird UCConnect verwendet, geben Sie die *Server ID* an.

Wird der estos STUN/TURN Server verwendet, muss die IP-Adresse oder der Name des UCServer angegeben werden.

Nach Eingabe aller Daten drücken Sie *Anmelden*

5. Anhang

Nachfolgende Beispiele für Einrichtung und Konfiguration betreffen nicht die estos Software und sind daher ohne Gewähr und ohne Support durch die estos GmbH.

5.1. http-Reverse Proxy

Nachfolgend finden Sie Konfigurationsbeispiele zu den *http Reverse Proxys*:

- Microsoft Internet Information Services (IIS) - *Microsoft Windows kompatibel*
- Nginx - *Linux kompatibel*

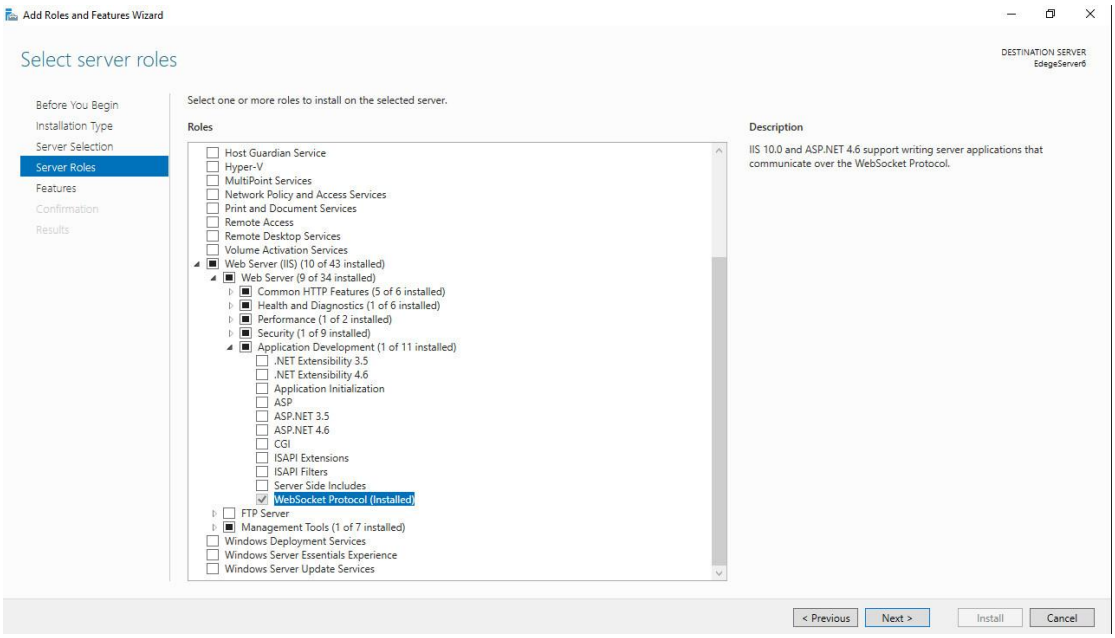
5.1.1. Microsoft Internet Information Services (IIS)

Voraussetzungen

- Microsoft Internet Information Services (IIS) ab Version 10
- WebSocket Protocol Feature für IIS
- Application Request Routing (ARR) ab Version 3 (https://www.iis.net/downloads/microsoft/application-request-routing)
- URL Rewrite Modul für IIS ab Version 2 (https://www.iis.net/downloads/microsoft/url-rewrite)

Installation und Vorbereitung Microsoft Internet Information Services (IIS)

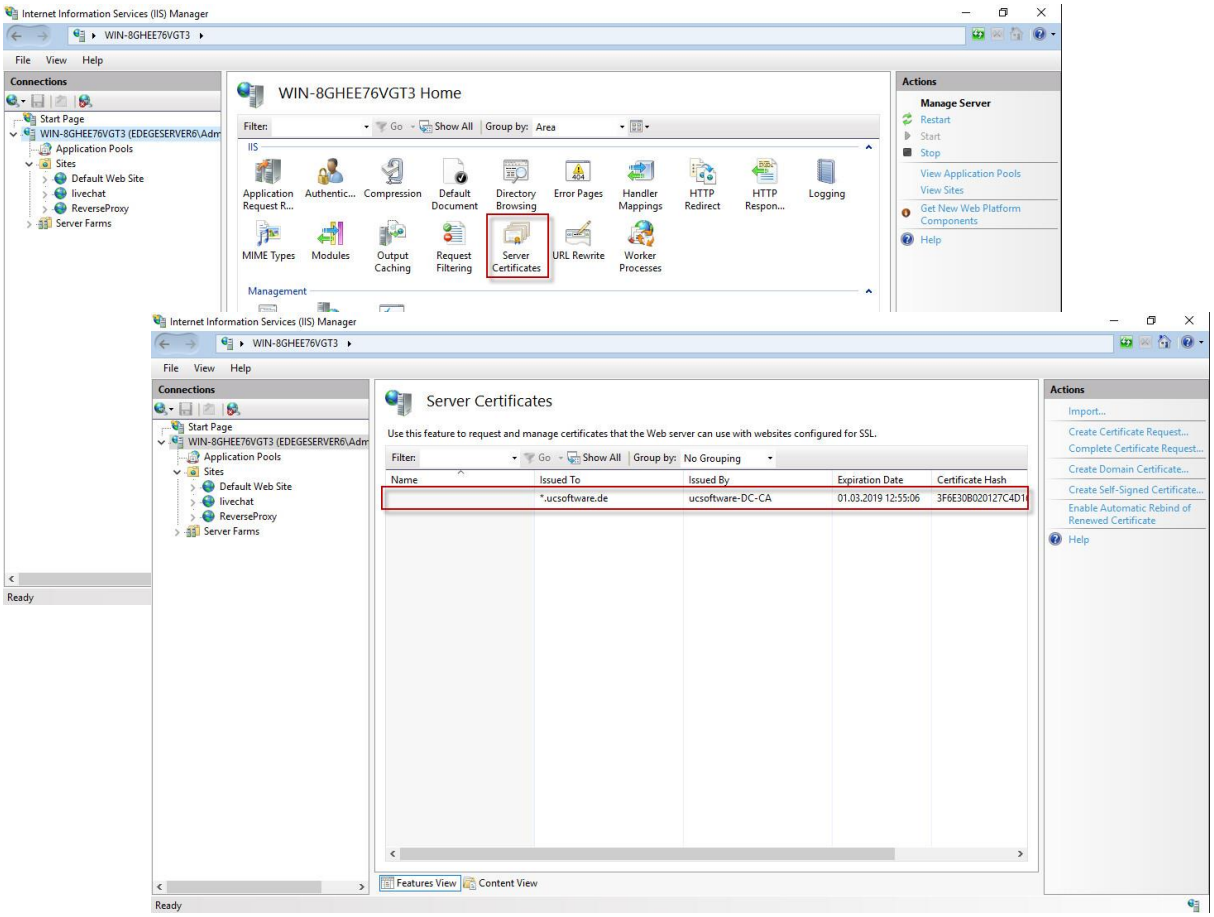
1. Installieren Sie den Microsoft Internet Information Services (IIS) auf dem gewünschten Server. Laden Sie dazu entweder das Installationspaket herunter oder fügen Sie die Rolle über die Serververwaltung hinzu.
2. Fügen Sie das Feature WebSocket Protocol hinzu.



3. Installieren Sie das Application Request Routing (ARR) Paket.
4. Installieren Sie das URL Rewrite Modul.
5. Konfiguration Microsoft Internet Information Services (IIS)
6. Um die Proxy-Funktion herzustellen, müssen im nächsten Schritt alle beteiligten Komponenten eingerichtet und entsprechend Ihrer Infrastruktur konfiguriert werden.

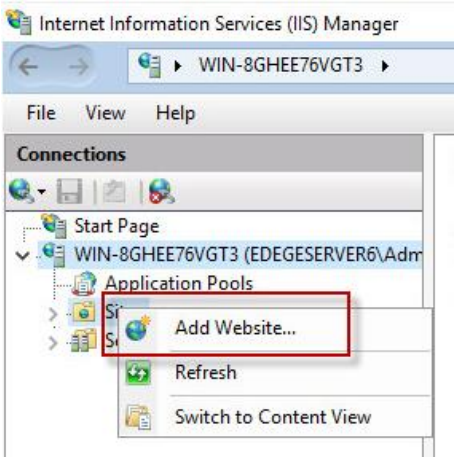
SSL Zertifikat konfigurieren

Es wird empfohlen, ein vertrauenswürdiges SSL-Zertifikat zu verwenden. Richten Sie ein Server Zertifikat für den IIS ein, gehen Sie dabei wie von Microsoft vorgeschlagen vor: https://technet.microsoft.com/en-us/cc731977

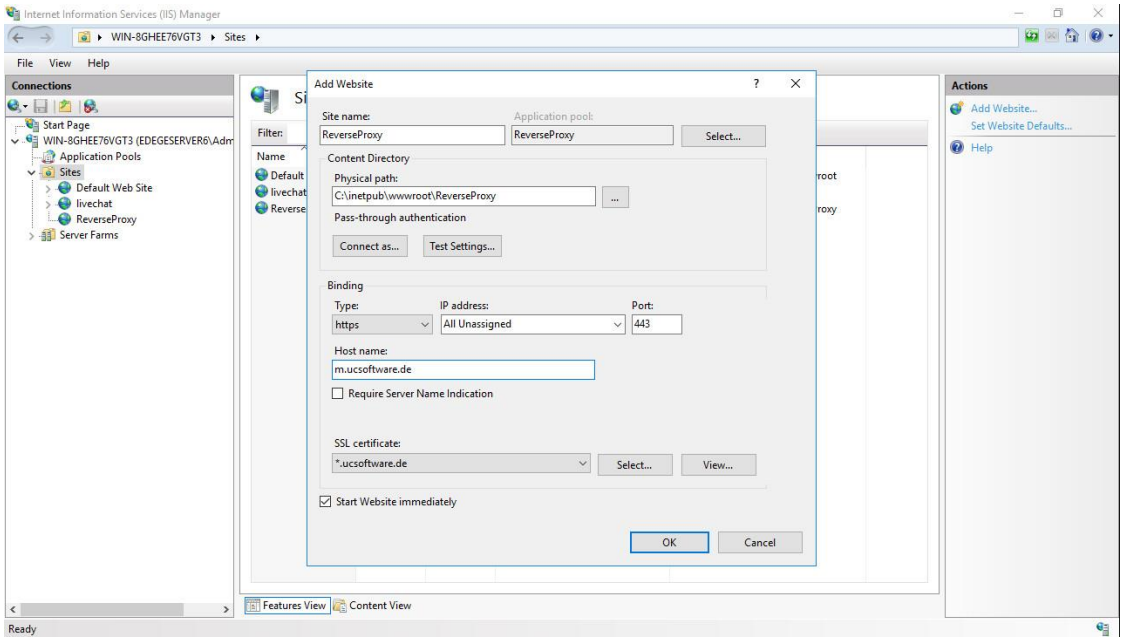


Einrichten einer Reverse Proxy Webseite

1. Fügen Sie eine neue Webseite hinzu



2. Füllen Sie die notwendigen Felder aus (siehe Beispiel unterhalb)



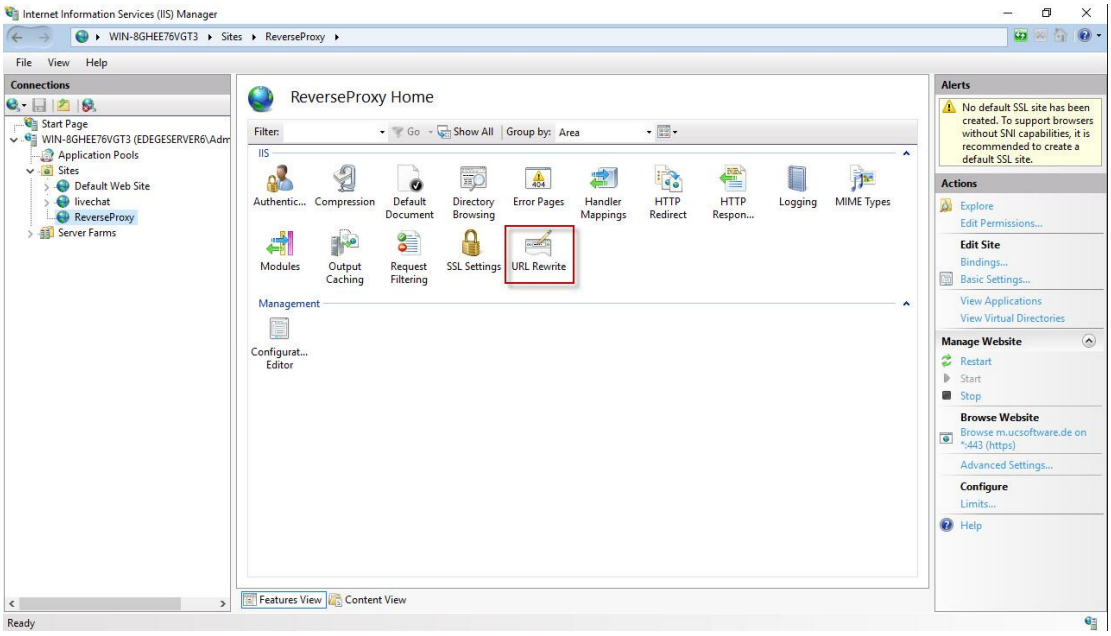
a) Die Pfad-Angabe ist nicht sonderlich relevant, da keine Webseite ausgeliefert wird. Der IIS wird dennoch trotzdem eine web.config Datei anlegen. estos empfiehlt den Pfad: C:\inetpub\wwwroot\ReverseProxy

b) Verwenden sie https als Binding Type

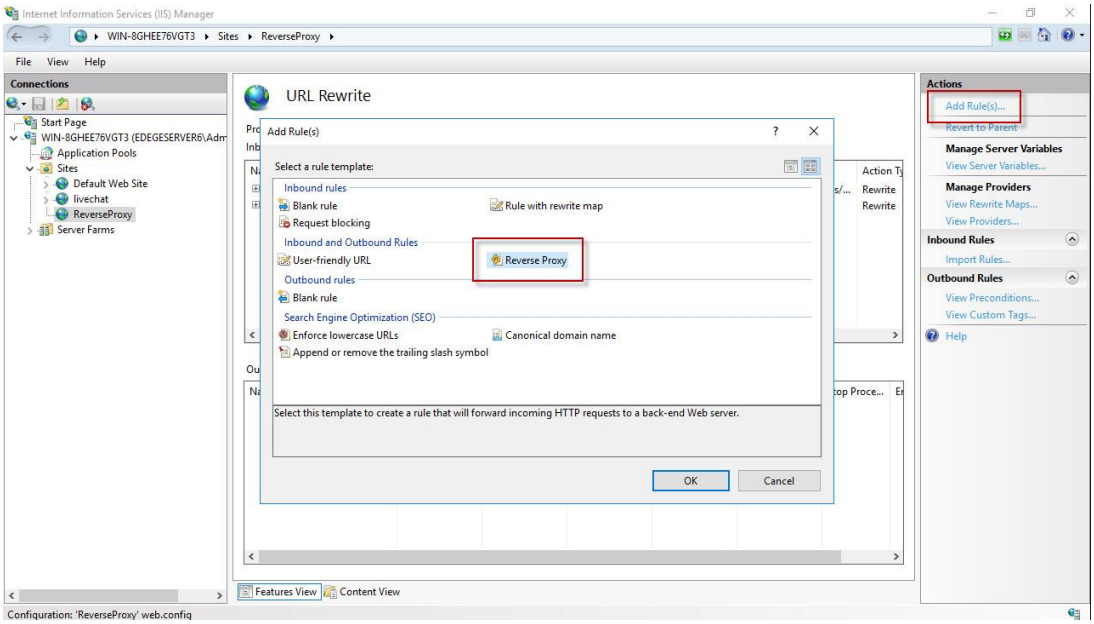
c) Hinterlegen Sie den Host Name, der Ihrem DNS-Eintrag und Zertifikat entspricht.

d) Wählen Sie das vorher hinterlegte Zertifikat aus.

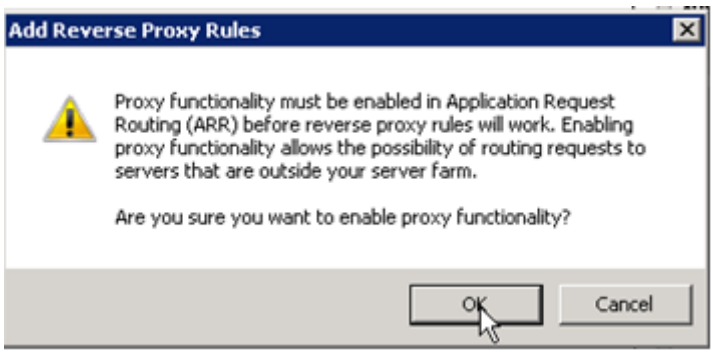
1. URL- Doppel-Klicken Sie auf die neu angelegte Webseite und öffnen Sie *URL Rewrite*



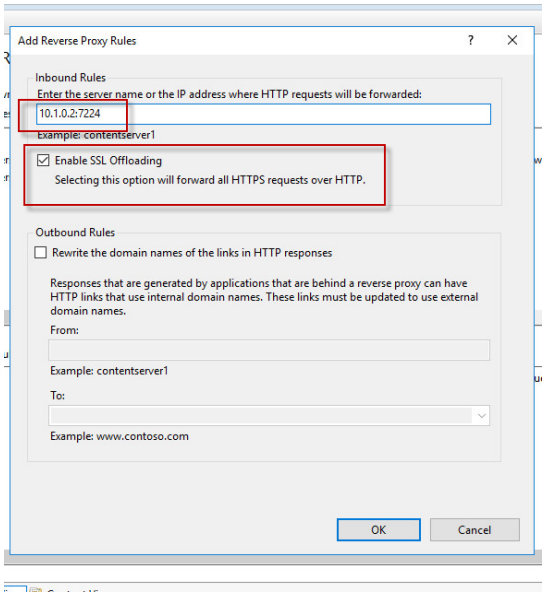
2. Klicken Sie *Add Rule(s)…* und wählen Sie *Reverse Proxy*



3. Wenn Sie folgende Warnung erhalten bestätigen Sie mit Ok



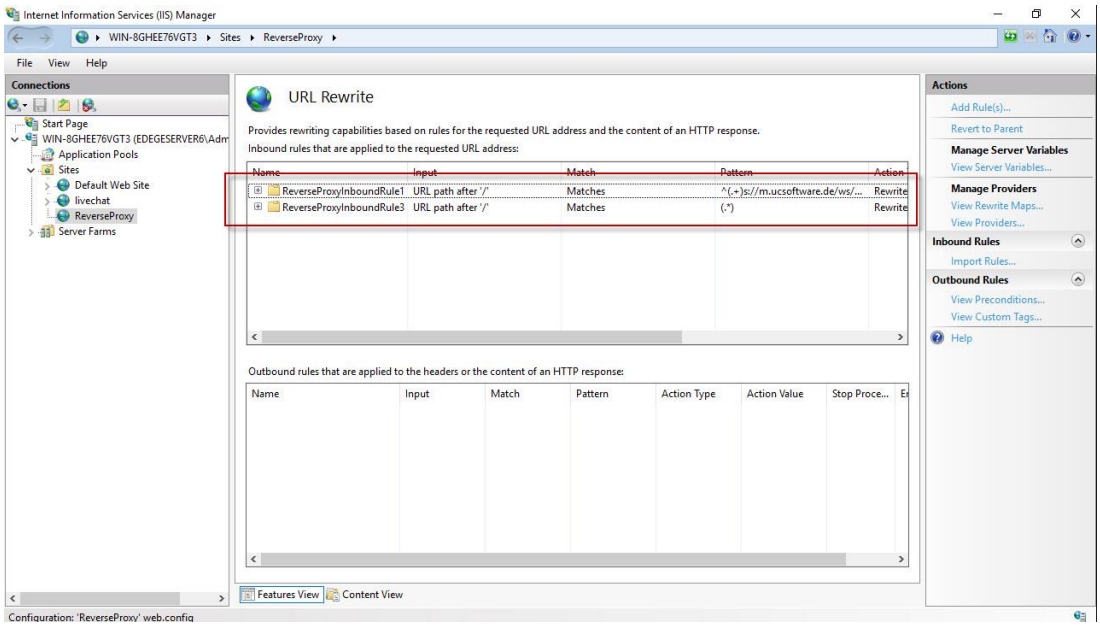
4. Machen Sie im nächsten Dialog Angaben, wohin die Anfragen umgeleitet werden sollen.



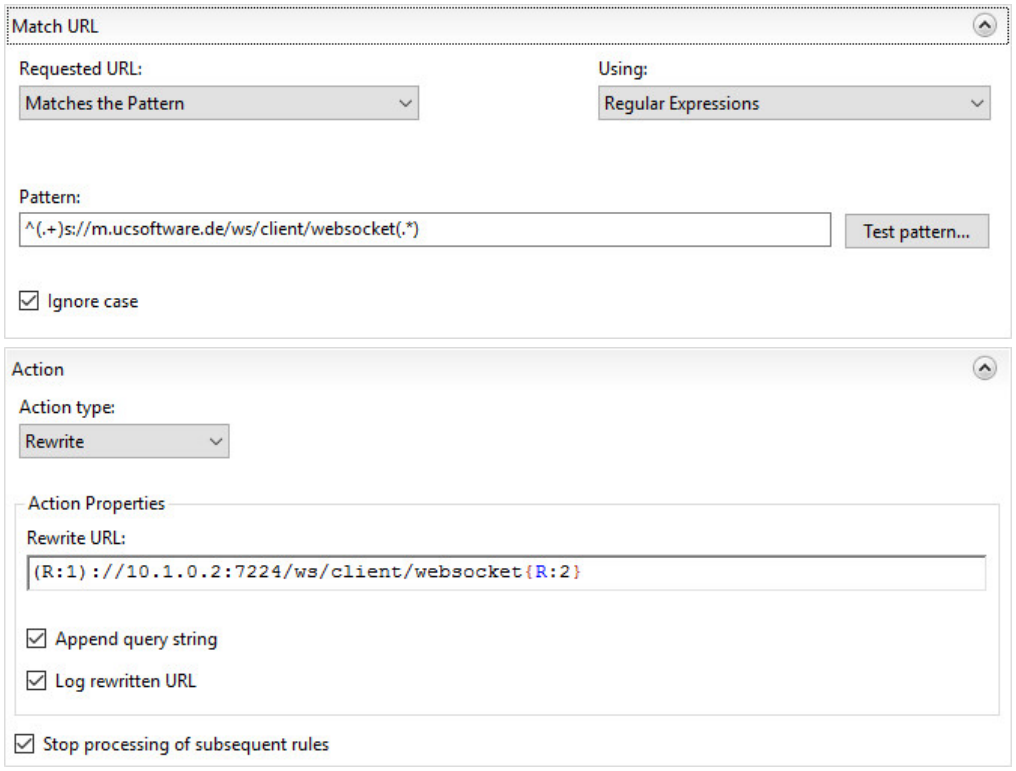
a. Tragen Sie unter *Inbound Rules* den DNS-Namen oder die IP-Adresse ein, auf die die Anfragen umgeleitet werden sollen (z. B. UCServer, Firewall). Ergänzen Sie außerdem den gewünschten Port.

b. Wenn Sie *SSL Offloading* aktivieren, werden die Anfragen unverschlüsselt weitergeleitet. Im Rahmen der weiteren Ausführungen wird davon ausgegangen, dass die Option aktiviert wurde.

5. Fügen Sie auf diesem Weg zwei identische Regeln hinzu:



6. Öffnen Sie die oberste Regel mit einem Doppel-Klick und editieren Sie *Match URL und Action*

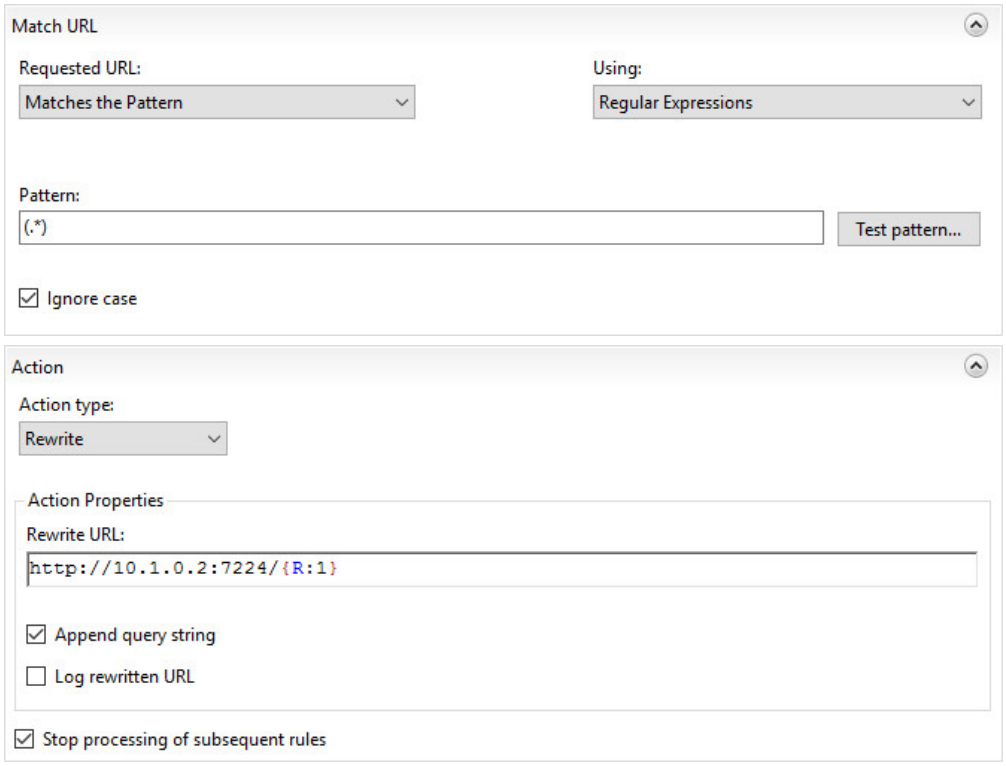


a. Unter *Match URL* muss ein Regulärer Ausdruck hinterlegt werden, um den Upgrade der http(s) auf eine ws(s) Verbindung abzubilden. Tauschen Sie bei folgender Vorlage `<DNS NAME>` mit Ihrem DNS Eintrag aus.
`^(.+)s://<DNS NAME>/ws/client/websocket(.*)`

b. Unter *Action* definieren Sie, wie die URL umgeschrieben wird und an welchen DNS-Namen oder welche IP-Adresse die Anfrage weitergeleitet wird. Tauschen Sie bei folgender Vorlage `<REWRITE TARGET>` mit dem gewünschten Weiterleitungsziel und `<PORT>` mit dem konfigurierten Port.
`(R:1)://<REWRITE TARGET>:<PORT>/ws/client/websocket{R:2}`

c. Aktivieren Sie *Stop processing of subsequent rules.*

7. Öffnen Sie die zweite Regel mit einem Doppel-Klick und editieren Sie *Match URL und Action*



a. Unter *Match URL* muss ein Regulärer Ausdruck hinterlegt werden, der alle vom ersten Ausdruck nicht erfassten Anfragen trotzdem weiterleitet. Eine Anpassung der Vorlage ist nicht notwendig.
`(.*)`

b. Unter *Action* definieren Sie, wie die URL umgeschrieben wird und an welchen DNS-Namen oder welche IP-Adresse die Anfrage weitergeleitet wird. Tauschen Sie bei folgender Vorlage `<REWRITE TARGET>` mit dem gewünschten Weiterleitungsziel und `<PORT>` mit dem konfigurierten Port.
`http://<REWRITE TARGET>:<PORT>/ {R:1}`

5.1.2. nginx

Installation nginx

Installieren Sie nginx über die Paketverwaltung Ihrer Linux Distribution, z.B. auf Ubuntu:

```
$ sudo apt-get update
$ sudo apt-get install nginx
```

Konfiguration nginx

1. Legen Sie unter `/etc/nginx/sites-Available` eine neue Konfigurationsdatei mit Namen *reverseproxy* an und kopieren Sie die unten beschriebene Beispielkonfiguration in die Datei.
2. Es wird empfohlen, ein vertrauenswürdiges SSL-Zertifikat zu verwenden. Ergänzen Sie die SSL-Konfiguration gemäß http://nginx.org/en/docs/http/configuring_https_servers.html.
3. Tauschen Sie in dem Beispiel `<DNS NAME>` mit Ihrem DNS Eintrag, `<REWRITE TARGET>` mit dem gewünschten Weiterleitungsziel und `<PORT>` mit dem konfigurierten Port aus.
4. Aktivieren Sie die Konfiguration, indem Sie unter `/etc/nginx/sites-enabled` einen symbolischen Link auf die Konfigurationsdatei erzeugen:
   `$ cd /etc/nginx/sites-enabled`
   `$ sudo ln -s /etc/nginx/sites-Available/reverseproxy reverseproxy`
5. Starten Sie den nginx Dienst neu.
   `sudo systemctl restart nginx.service` oder `sudo service nginx restart`

Beispielkonfiguration nginx

```
server {
    listen  80;
    server_name <DNS NAME>;
    rewrite ^ https://$server_name$request_uri? permanent;
}
server {
       listen 443 ssl;
       server_name <DNS NAME>;
       ssl on;
       ssl_certificate /etc/ssl/certs/fullchain.pem;
       ssl_certificate_key /etc/ssl/certs/privkey.pem;
       index index.html index.htm;
       proxy_read_timeout 3600s;

       # https://raymii.org/s/tutorials/Strong_SSL_Security_On_nginx.html
       add_header Strict-Transport-Security max-age=63072000;
       ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
       ssl_ciphers 'EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH';
       ssl_prefer_server_ciphers on;
       ssl_session_cache shared:SSL:10m;
       # DHE generated with
       # cd /etc/ssl/certs && openssl dhparam -out dhparam.pem 4096
       ssl_dhparam /etc/ssl/certs/dhparam.pem;

       location / {
              proxy_set_header X-Real-IP $remote_addr;
              proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
              proxy_set_header Host $http_host;
              proxy_set_header X-NginX-Proxy true;
              proxy_pass http://<REDIRECT TARGET>:<PORT>;
              proxy_redirect off;
       }
       location /ws/client/websocket {
              proxy_pass http://<REDIRECT TARGET>:<PORT>;
              proxy_http_version 1.1;
              proxy_set_header Upgrade $http_upgrade;
              proxy_set_header Connection "upgrade";
       }
}
```

5.2. Informationen zu STUN/TURN

Im Folgenden wird kurz beschrieben, was ein STUN-/TURN-Dienst macht und welche Probleme er bei Audio/Video bzw. Softphone Kommunikation zwischen zwei Clients beseitigt. Anschließend werden noch die Hauptanwendungsfälle aufgezeichnet.

Diese Beschreibung soll dazu dienen, ein grundlegendes Verständnis für die Thematik zu vermitteln und geht nicht auf genauere Details ein.

5.2.1. Beteiligte Komponenten und Begriffe

NAT - Network Address Translation (RFC 2663)

NAT beschreibt die Umsetzung des "internen" IPv4-Adressraums eines LAN zu "externen" IPv4-Adressen (und Ports) im Internet. Das trägt zur Sicherheit des internen Netzes bei, da von außen kein direkter, ungewünschter Zugriff auf interne Adressen erfolgen kann.

Ein NAT Device ist z.B. ein Router, der ein LAN mit dem Internet verbindet.

Symmetric NAT

Zusätzlich zum normalen NAT merken sich diese Router nicht nur die interne Client Adresse, sondern auch die von ihm angesprochene Zieladresse und lässt Daten nur von dieser in das interne Netz gelangen. Ein anderes Ziel kann also keine Daten an den internen Client senden, selbst wenn die IP-Adressen (und Ports) bekannt wären. Audio/Video Kommunikation ist in diesem Fall nur in Verbindung mit einem TURN-Server möglich.

NAT Traversal

"NAT Traversal" bezeichnet Techniken zum Aufbau und Halten von Verbindungen über NAT-Umsetzungsstellen hinweg. Zu diesen Techniken gehören STUN und TURN.

STUN - Session Traversal Utilities for NAT (RFC5389)

Dieses Protokoll ermöglicht es einem Client in einem LAN, seine eigene, öffentliche IPv4-Adresse zu ermitteln.

Der rufende Client im LAN kann auf diese Weise dem angerufenen Client außerhalb des LAN mitteilen, welche IPv4-Adresse (und Portnummer) verwendet werden kann, um eine direkte Kommunikation mit ihm zu ermöglichen ("Peer-to-Peer" Verbindung).

TURN - Traversal Using Relays around NAT (RFC5766)

Ein Server im Internet, der das TURN-Protokoll implementiert, ermöglicht es zwei Clients, Daten ohne eine direkte Verbindung auszutauschen ("Relay Server"). Dies wird notwendig, wenn es keine Möglichkeit gibt, eine direkte Client-zu-Client-Verbindung aufzubauen.

ICE - Interactive Connectivity Establishment (RFC5245)

Zwei Clients können die mit Hilfe von STUN und TURN ermittelten Verbindungsinformationen (und andere Daten) mit Hilfe des ICE Protokolls austauschen. Die Übermittlung der Informationen muss

dabei über einen eigenen Dienst erfolgen, einen sog. "Signaling Server". Dieser Dienst muss von beiden Clients erreichbar sein.

Das Zusammenstellen einer ICE Informationen, sog. ICE Kandidaten, erfolgt durch beide Clients. Dazu sammeln beide die verschiedenen Kandidaten (mögliche Protokolle und dazugehörende IP-Adressen mit Ports) aus ihrem LAN heraus ein. Die beiden Clients tauschen diese Kandidaten anschließend über die Signaling Server aus und versuchen daraufhin den jeweils anderen mit Hilfe des passendsten Kandidaten zu erreichen.

Signaling Server

Signaling Server dienen zum indirekten Austausch von Daten zwischen zwei Clients. Dies kann ein Dienst sein, der von beiden Clients erreichbar ist (z. B. UCServer in einem Netzwerk) oder auch mehrere Dienste, die mittels Federation miteinander verbunden sind (z. B. zwei UCServer zweier Firmen, die eine XMPP Federation eingegangen sind).

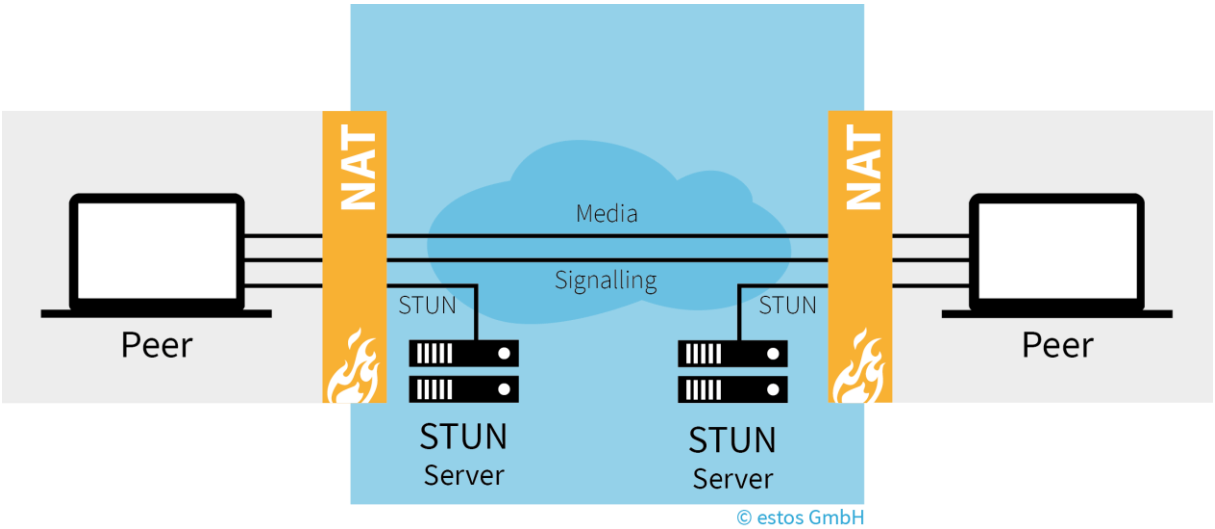


Abbildung0- 1: Erfolgreiche Kommunikation unter Zuhilfenahme eines STUN-Servers.

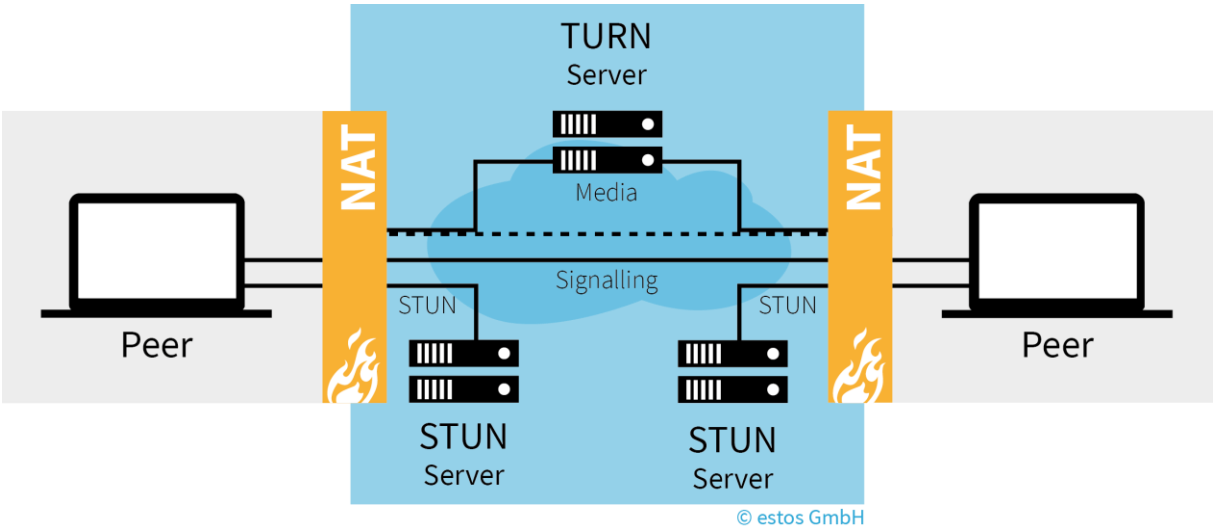


Abbildung0- 2: Erfolgreiche Kommunikation unter Zuhilfenahme eines STUN-/TURN Servers

5.2.2. Anwendungsfälle

Im Folgenden werden die Hauptanwendungsfälle der STUN/TURN-Dienste etwas ausführlicher gezeigt.

Direkte Kommunikation ist möglich (kein STUN/TURN-Dienst notwendig)

Damit Client A die Medienströme von Client B empfangen kann, muss Client A zunächst Client B seine Kontaktdaten (IP-Adresse und Port) mitteilen. Dies geschieht in der Regel über einen Signaling-Server, zu dem beide Clients eine Verbindung haben. Solange sich beide Clients im gleichen LAN befinden ist dies problemlos möglich. Abb. 1 verdeutlicht dies. In Schritt 1 sendet Client A seine IP-Adresse und Port über den Signaling Server an Client B. Daraufhin kann Client B in Schritt 2 damit beginnen einen Medienstrom an Client A zu senden.

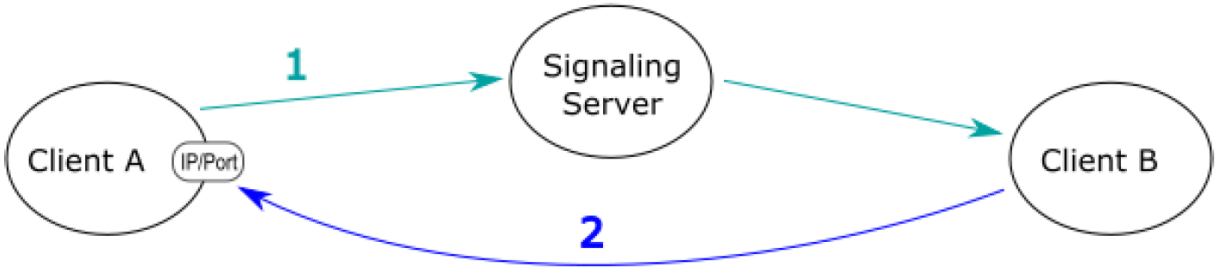


Abbildung 3: Client A ist direkt erreichbar. Client B kann den Medienstrom direkt an Client A senden.

Ein Client befindet sich hinter einem NAT-Router

Befinden sich Client A und Client B in verschiedenen LANs, die durch einen NAT-Router getrennt sind, wird das obige Szenario fehlschlagen. Da Client A nicht weiß, dass er gegenüber Client B mit der öffentlichen IP-Adresse und Port des NAT-Routers erscheint, würde Client A in Schritt 1 seine lokale IP-Adresse und Port an Client B signalisieren. Da diese Adresse aber für Client B nicht erreichbar ist, schlägt das senden des Medienstroms (Schritt 2) fehl (siehe Abb. 2).

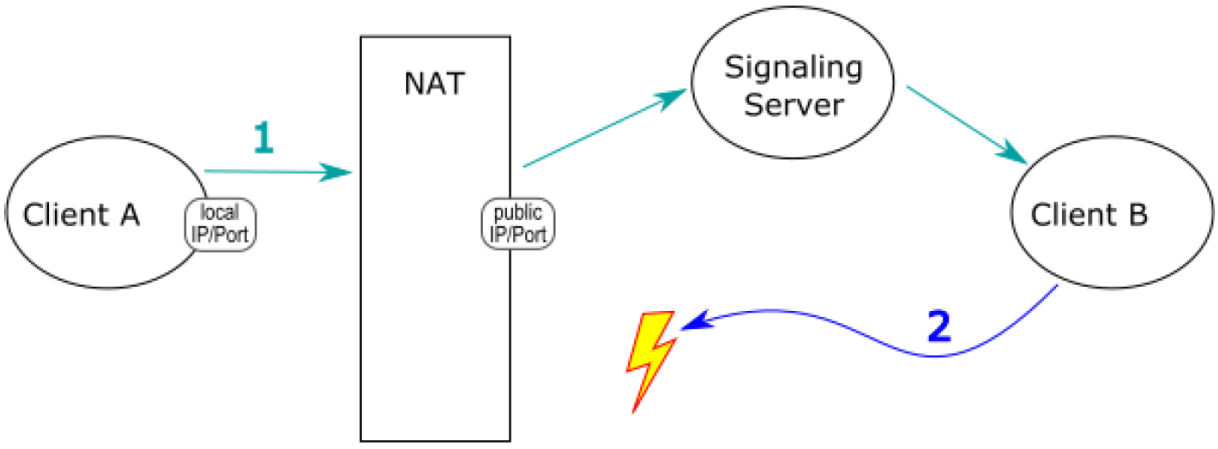


Abbildung 4: Erfolgloser Verbindungsaufbau über einen NAT-Router hinweg.

Das Nichterreichbarkeitsproblem kann mit Hilfe eines STUN-Servers gelöst werden wie in Abb. 3 dargestellt. Mit Hilfe des STUN-Servers kann Client A in Schritt 1 seine öffentliche IP-Adresse und Port ermitteln. Diese kann er dann in Schritt 2 an Client B übermitteln woraufhin dieser seinen

Medienstrom an die öffentlich erreichbare Adresse des NAT-Routers senden kann. Der NAT-Router leitet den Medienstrom dann an Client A weiter.

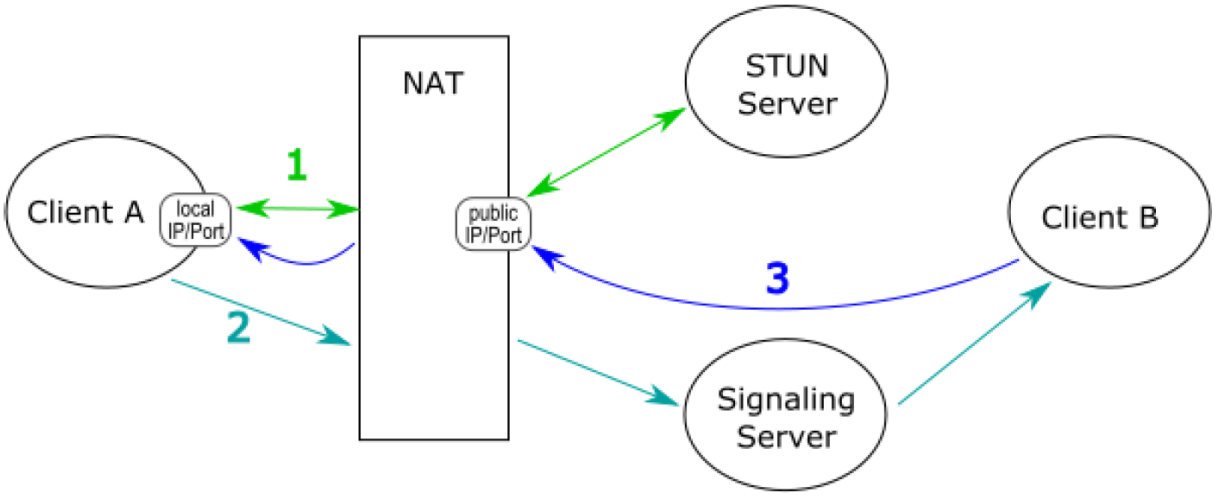


Abbildung 5: Erfolgreiche Kommunikation unter Zuhilfenahme eines STUN-Servers.

Mindestens ein Client kann von außen gar nicht erreicht werden (Symmetric NAT-Router)

Die vorherige Lösung funktioniert allerdings nicht für alle NAT Ausprägungen. Es gibt eine Klasse von NATs, die sog. "Symmetric NAT", die nicht nur einen öffentlichen Port für einen LAN Client A öffnen, sondern für auch jede einzelne Verbindung nach außen. Das hat zur Folge, dass Client A zwar nach wie vor seine öffentliche IP-Adresse/Port vom STUN-Server abfragen kann, diese wären dann aber für Verbindungen mit Client B nicht gültig.

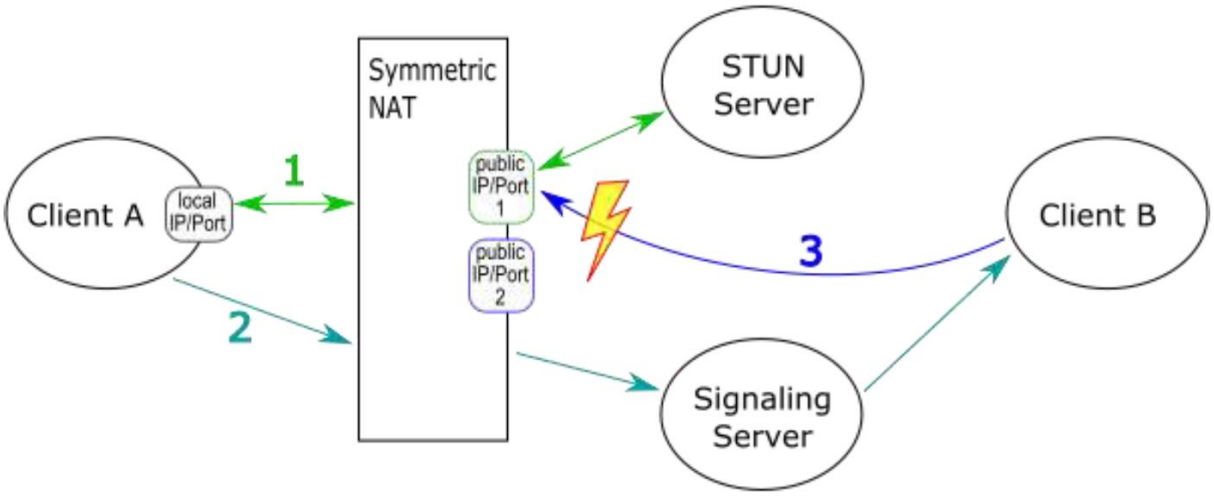


Abbildung 6: Erfolgloser Kommunikationsversuch über ein "Symmetric NAT".

Da der korrekte öffentliche Port über den STUN-Server nicht ermittelt werden kann, schlägt das Senden eines Medienstroms von Client B fehl.

Um dieses Problem mit dem "Symmetric NAT" zu lösen, benötigt man einen TURN-Server (siehe Abb. 5). Sobald Client A feststellt, dass direkte und STUN Verbindungen nicht möglich sind (Schritt 1), kann er Client B über den Signaling-Server mitteilen, dass er eine Verbindung zu einen

gemeinsam bekannten TURN-Server (Schritt 2) aufbauen soll. In Schritt 3 haben beide Clients eine Verbindung zum TURN-Server und können darüber nun Daten austauschen.

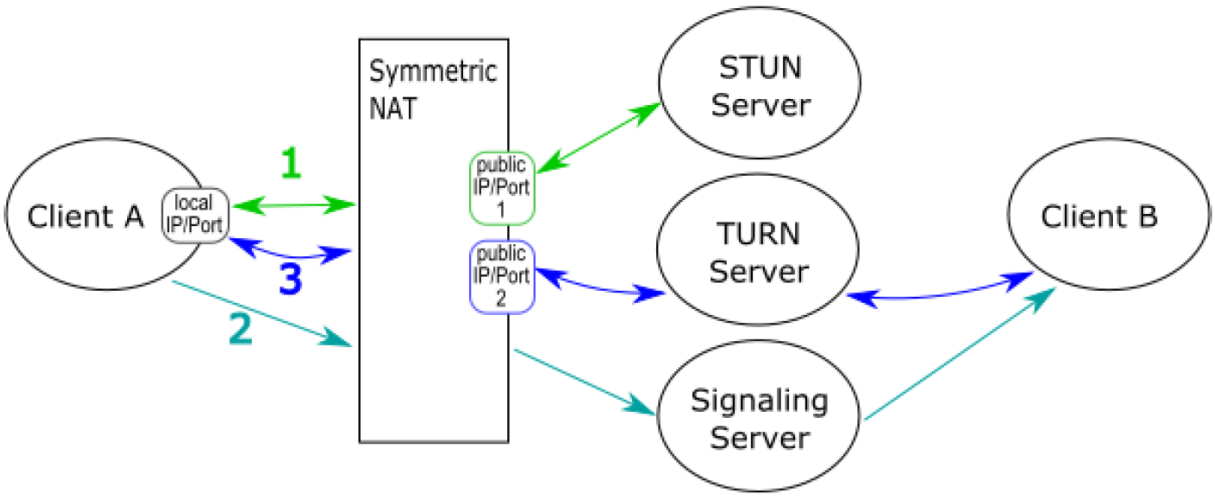


Abbildung 7: Erfolgreicher Kommunikationsversuch über ein "Symmetric NAT" durch Nutzung eines TURN-Servers.

Da die Nutzdaten bei dieser Lösung direkt über den TURN-Server fließen, hat ein TURN-Server insbesondere bei mehreren parallelen Verbindungen sehr hohe Anforderungen an die Bandbreite zu erfüllen. Deshalb wird diese Lösung nur dann gewählt, wenn es keine andere Möglichkeit für eine Datenübertragung gibt.