estos
enables easy communication

Veröffentlichung UCServer Webservice

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
D-82319 Starnberg
info@estos.de
www.estos.de

Stand 27.01.2015

Dokumentenhistorie

Version	Datum	Autor	Änderungen
1	29.06.2017	DW	Initial
2	19.09.2017	DW	Anpassung nginx

Inhalt

1. Einleitung

Zusammen mit dem UCServer wird immer ein WebService installiert, der dauerhaft mit dem UCServer verbunden ist. Die Veröffentlichung des UCServer Webservice ermöglicht Ihnen die Nutzung von ProCall Mobile, ProCall (Desktop) und der Web Anwendungen nicht nur im lokalen Netzwerk, sondern auch über das Internet oder aus dem Home-Office. Die Nutzung dieser Applikationen über das Internet erfordert den Zugang zu diesem UCServer aus dem Internet, sowie STUN- und TURN-Server zur Nutzung von Audio- und Video-Chat. Bei der Veröffentlichung unterscheiden wir grundsätzlich drei verschiedene Szenarien.

1. Die Veröffentlichung ohne DMZ
2. Die Veröffentlichung mit DMZ
3. Die Veröffentlichung mit Hilfe unserer ergänzenden Online-Dienste (UCConnect)

Die ergänzenden Online-Dienste sind nicht Gegenstand dieses Dokuments.

2. Voraussetzungen

Die folgenden Voraussetzungen müssen zur Veröffentlichung des UCServer Webservice erfüllt sein/werden:

- *Öffentliche IP Adresse*
  Ihr Internetzugang muss über eine öffentliche IP Adresse verfügen.
- *DNS Eintrag*
  Die öffentliche IP Adresse muss über einen DNS Eintrag auflösbar sein. Fügen Sie einen DNS A Record zu Ihrer Domain hinzu (z.b. ucws.domain.com), verwenden Sie Ihre öffentliche IP Adresse.
- *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 Sie mit einem selbst signierten Zertifikat ('Self Signed Certificate') arbeiten, ist die Verbindung verschlüsselt, aber nicht abhörsicher. Damit ist keine Nutzung von Browser Applikationen möglich.

Vorsicht

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

3. Veröffentlichung durchführen

3.1. Überblick

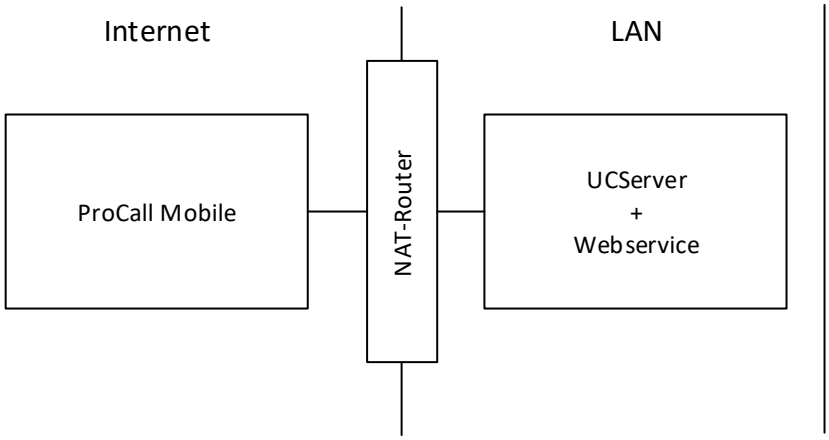
Grundsätzlich gibt es drei verschiedene technische Optionen, die wir bei der Veröffentlichung des UCServer Webservice betrachten.

1. Der UCServer hat eine öffentliche IP Adresse, d.h. er ist direkt mit dem Internet verbunden
2. Der UCServer hat keine öffentliche IP Adresse, d.h. er befindet sich hinter einem NAT-Device und es wird ein „Port Forwarding“ verwendet
3. Der UCServer hat keine öffentliche IP Adresse, d.h. er befindet sich hinter einem NAT-Device und es wird ein „http Reverse-Proxy“ verwendet

Je nach Aufbau Ihrer IT-Infrastruktur (mit/ohne DMZ) empfehlen wir eine unterschiedliche Vorgehensweise.

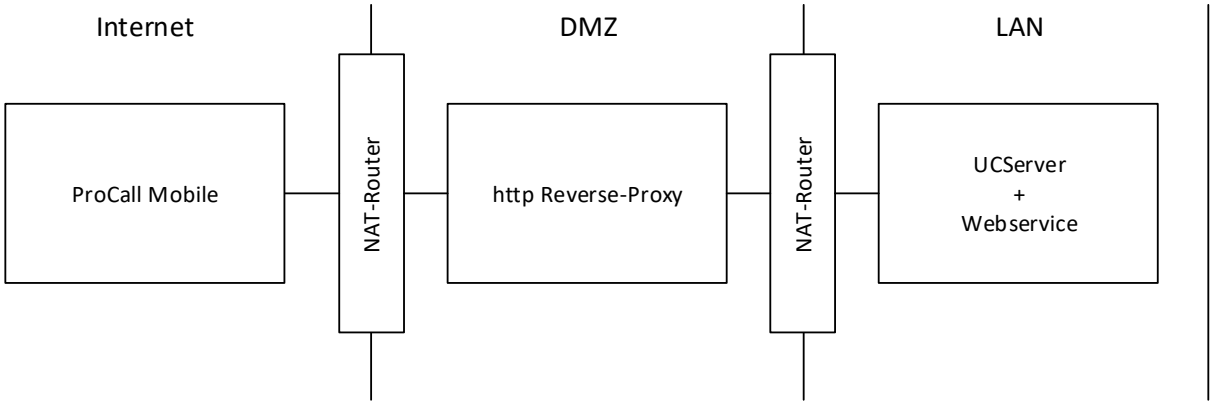
DMZ	Standort UCServer	Vorgehen
Nein	LAN	Port Forwarding
Ja	DMZ	
Ja	LAN	http Reverse-Proxy

Port Forwarding



Konfigurieren Sie den NAT-Router mit einem Port Forwarding, die Verschlüsselung (TLS) der Kommunikation erfolgt durch den UCServer Webservice. Diese Einstellungen finden Sie in der UCServer Verwaltung im Menü unter Extras >> Netzwerkschnittstellen.

http Reverse-Proxy



Unter einen http Reverse-Proxy versteht man einen Server, der http(s) Anfragen entgegennimmt und an einen Server im privaten Netz weiterleitet. Dieser http Reverse-Proxy benötigt das SSL Zertifikat, die Kommunikation wird zum UCServer weitergeleitet über http (auf die Netzwerkschnittstelle des 'WebService http) oder https (auf die Netzwerkschnittstelle des „WebService https“).

Als Server können Sie z.B. nginx (proxy_pass), Apache (mod_proxy, ProxyPass) oder Microsoft® IIS (Application Request Routing) verwenden.

Hinweis

Der http Reverse-Proxy muss zusätzlich zu http GET und POST auch Websocket Verbindungen (RFC 6455) ermöglichen.

3.2. UCServer konfigurieren

Je nach Szenario müssen unterschiedliche Konfigurationen am UCServer vorgenommen.

3.2.1. Port Forwarding

IP Ports festlegen

In der UCServer Verwaltung können Sie im Menü unter Extras >> Netzwerkschnittstellen die Netzwerkeinstellungen des UCServers einsehen und ändern. In der Standardeinstellung beantwortet der UCServer Anfragen über http auf Port 7224 und https auf Port 7225. Im Normalfall muss diese Einstellung nicht geändert werden.

SSL Zertifikat hinterlegen

Im Falle eines Port Forwadings werden alle Anfragen aus dem Internet direkt vom UCServer Webservice entgegengenommen, damit ist er auch für die Verschlüsselung der Verbindung verantwortlich. Wir empfehlen dringend den Einsatz von https mit einem vertrauenswürdigen SSL Zertifikat. 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 nicht möglich.

In der UCServer Verwaltung können Sie im Menü unter Extras >> Netzwerkschnittstellen >> WebService https ein Zertifikat im PFX Format hinterlegen.

Port Forwarding einrichten

Konfigurieren Sie an Ihrem NAT Router ein Port Forwarding, dazu leiten Sie wenn möglich Port 443 TCP von Ihrer öffentliche IP auf den https-Port des UCServer Webservice (Standard: 7225) weiter.

3.2.2. http Reverse-Proxy

IP Ports festlegen

In der UCServer Verwaltung können Sie im Menü unter Extras >> Netzwerkschnittstellen die Netzwerkeinstellungen des UCServers einsehen und ändern. In der Standardeinstellung beantwortet der UCServer Anfragen über http auf Port 7224 und https auf Port 7225. Im Normalfall muss diese Einstellung nicht geändert werden.

SSL Zertifikat hinterlegen

Im Falle eines eines http Reverse-Proxy werden alle Anfragen aus dem Internet zuerst vom Proxy entgegengenommen und danach an den UCServer Webservice weitergeleitet, damit ist der Proxy auch für die Verschlüsselung der Verbindung verantwortlich. Wir empfehlen dringend den Einsatz von https mit einem vertrauenswürdigen SSL Zertifikat. 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 nicht möglich.

Je nach Anforderung können Sie die Anfragen innerhalb Ihres LAN über unverschlüsseltes http oder mit TLS Verschlüsslung weiterleiten. Sollten Sie auch innerhalb Ihres LAN eine verschlüsselte Verbindung bevorzugen, können Sie in der UCServer Verwaltung im Menü unter Extras >> Netzwerkschnittstellen >> WebService https ein Zertifikat im PFX Format hinterlegen.

3.3. http Reverse-Proxy installieren und konfigurieren

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

Im Rahmen dieses Dokumentes wird konkret auf die Einrichtung von drei verschiedenen Proxy-Servern eingegangen. Je nach Fähigkeiten und Präferenzen können sowohl Microsoft Windows als auch Linux als Betriebssystem gewählt werden.

Microsoft Windows kompatibel

- Microsoft Internet Information Services (IIS)

- Apache HTTP Server

Linux kompatibel

- nginx
- Apache HTTP Server

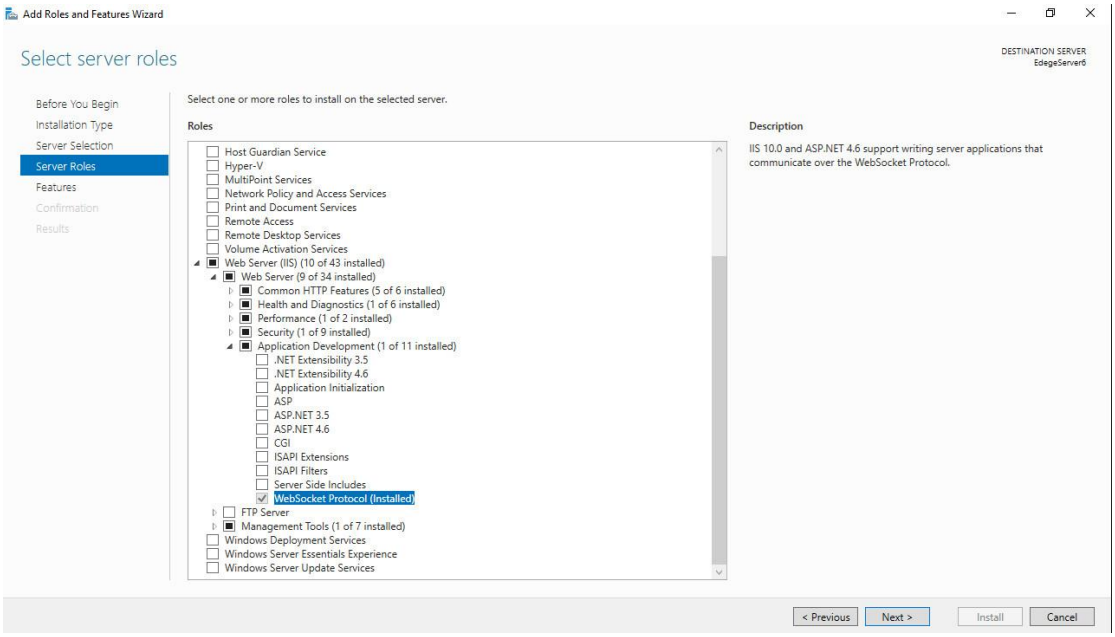
3.3.1. Microsoft Internet Information Services (IIS)

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.



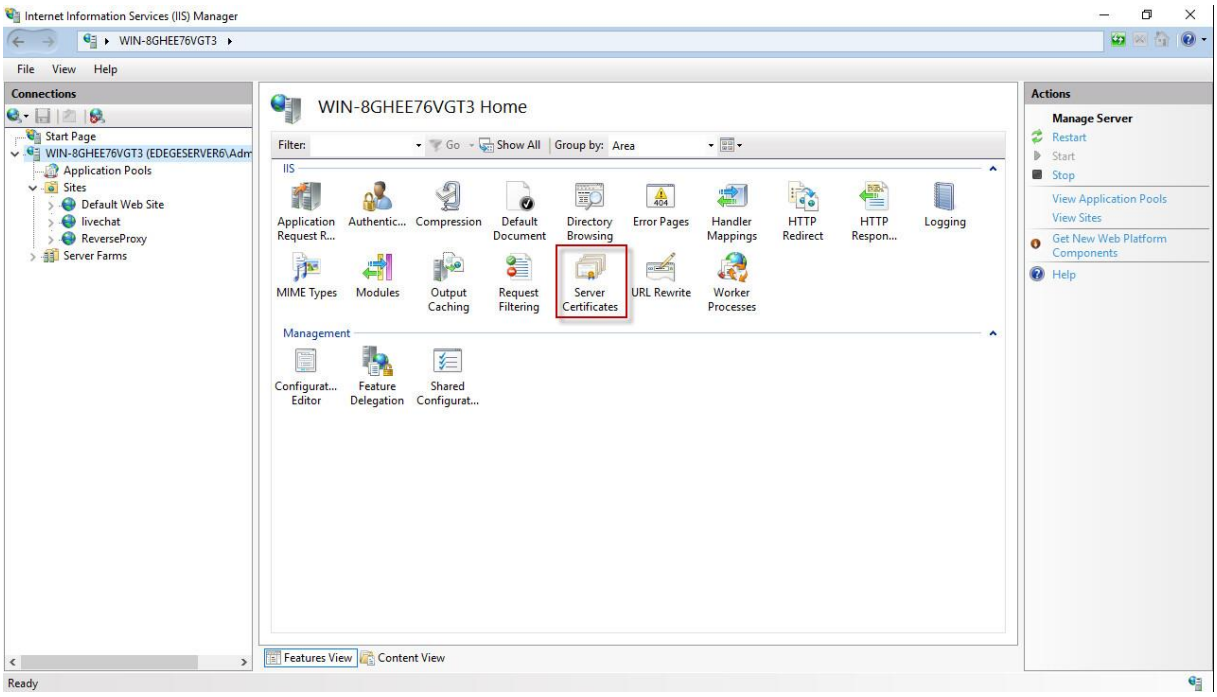
3. Installieren Sie das Application Request Routing (ARR) Paket.
4. Installieren Sie das URL Rewrite Modul.

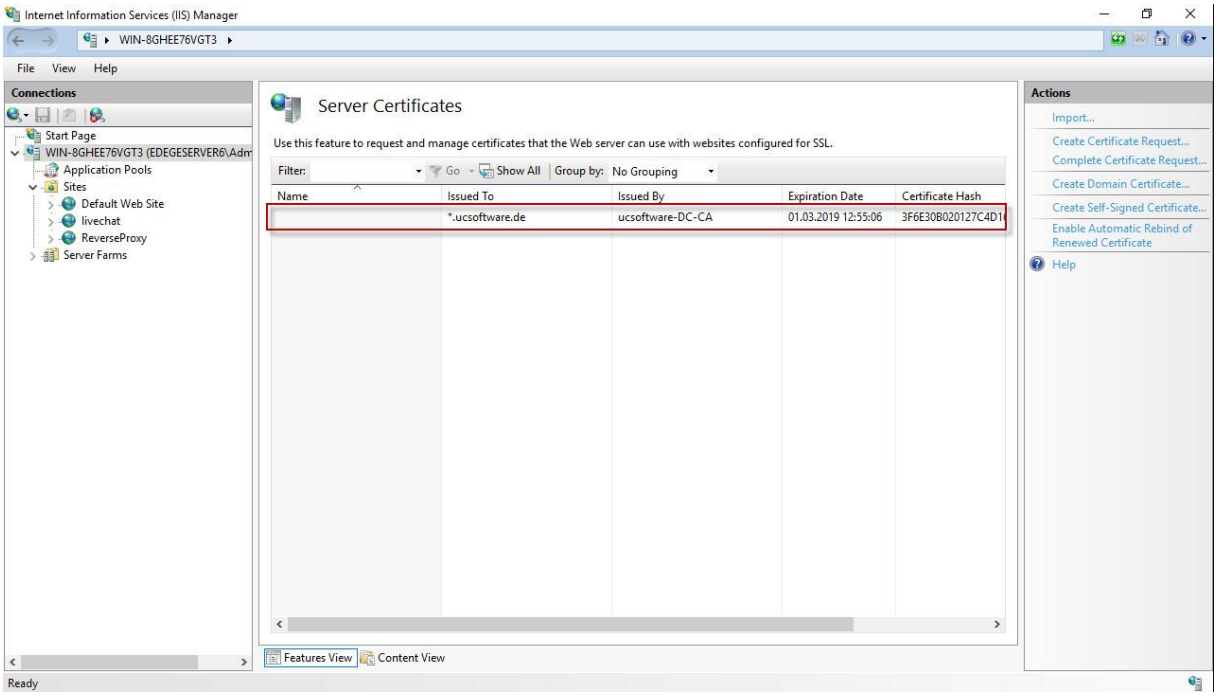
Konfiguration Microsoft Internet Information Services (IIS)

Um die Proxy-Funktion herzustellen müssen im nächsten Schritt alle beteiligten Komponenten eingerichtet und entsprechend Ihrer Infrastruktur konfiguriert werden.

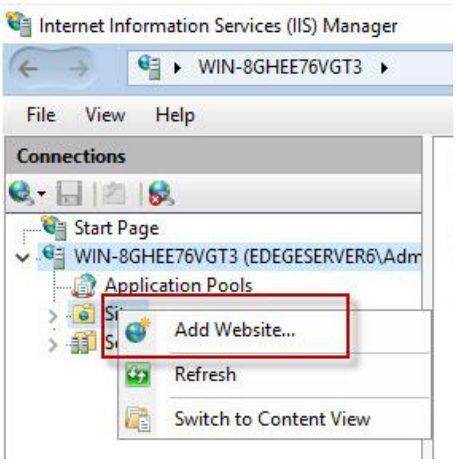
SSL Zertifikat Konfigurieren

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

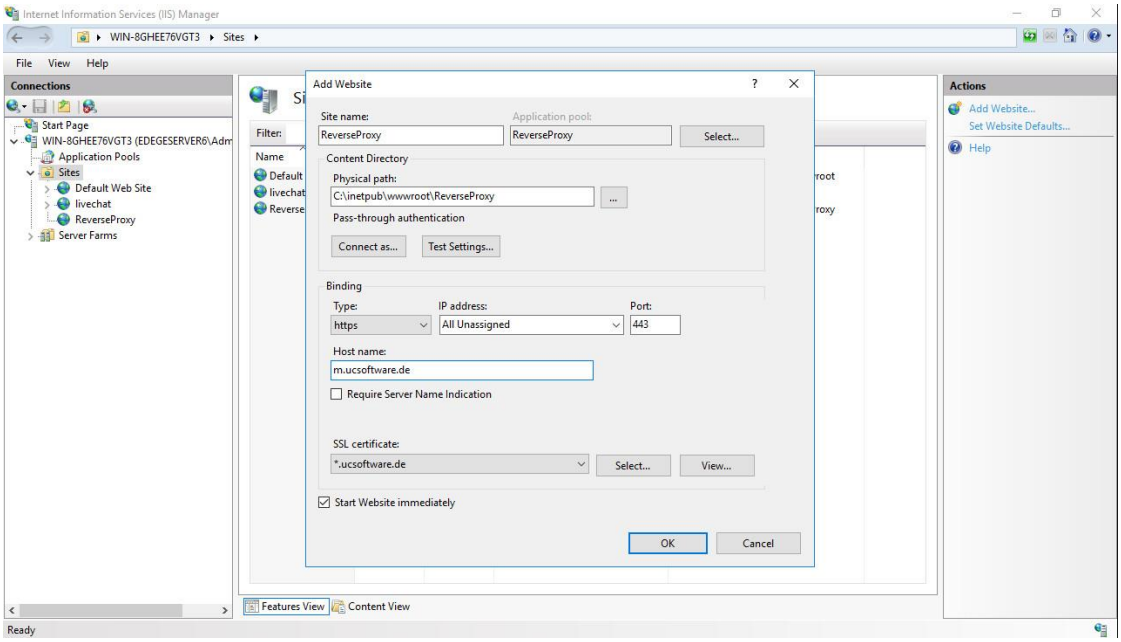




1. Fügen Sie eine neue Webseite hinzu



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



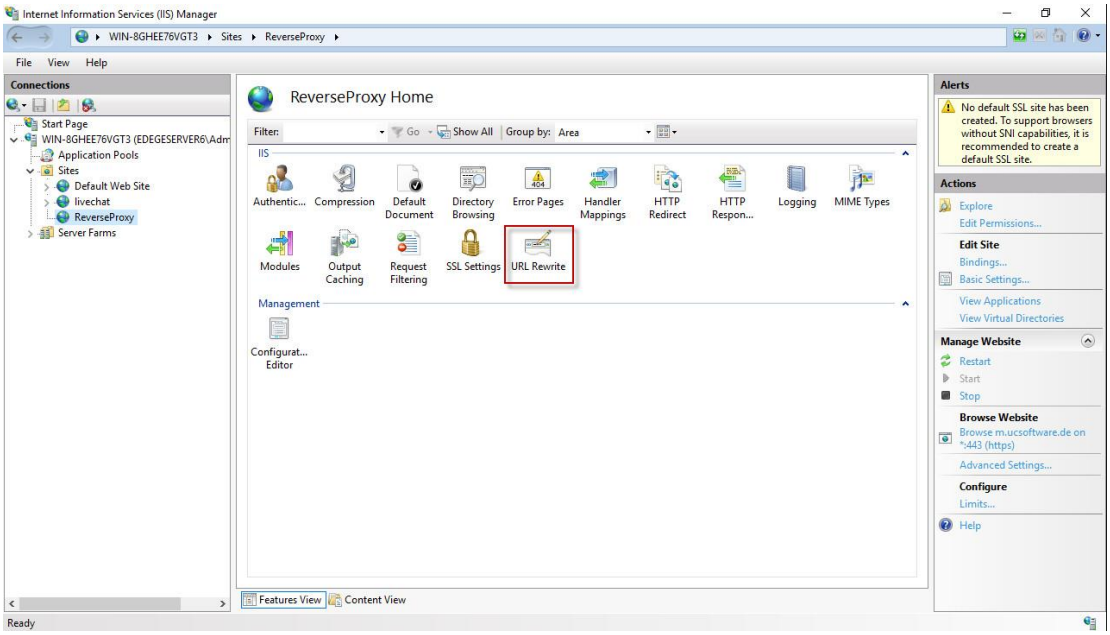
   a. Die Pfad Angabe ist nicht sonderlich relevant, da keine Webseite ausgeliefert wird. Der IIS wird dennoch trotzdem eine web.config Datei anlegen. Wir empfehlen den Pfad: C:\inetpub\wwwroot\ReverseProxy

   b. Verwenden sie https als Binding Type

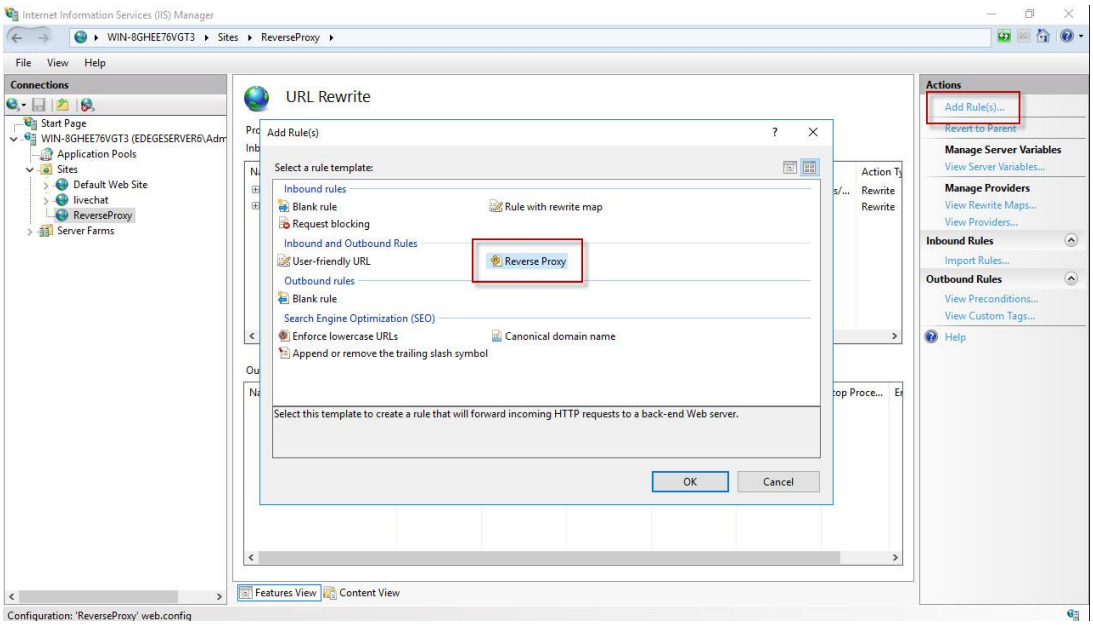
   c. Hinterlegen Sie den Host Name, der Ihrem DNS-Eintrag und Zertifikat entspricht.

   d. Wählen Sie das vorher hinterlegte Zertifikat aus

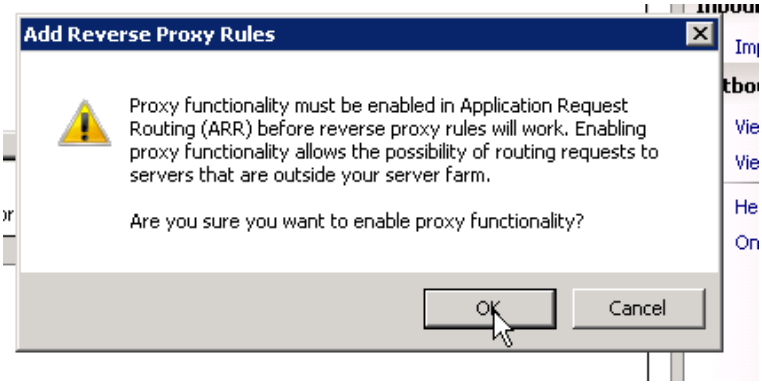
1. Doppel-Klicken Sie auf die neu angelegte Webseite und öffnen Sie URL Rewrite



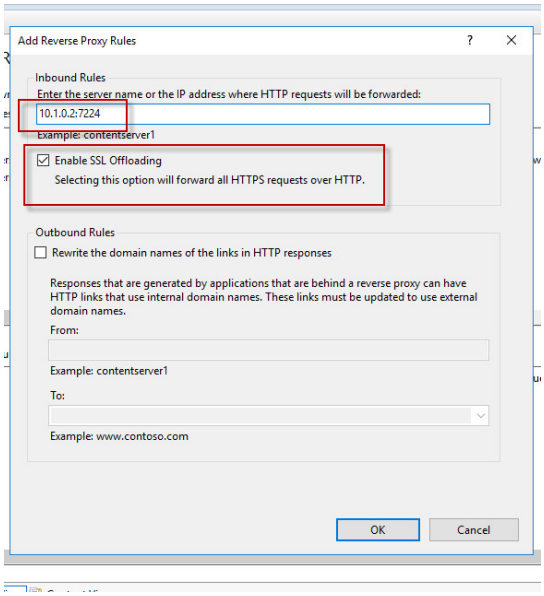
2. Klicken Sie Add Rule(s)… und wählen Sie Reverse Proxy



3. Wenn Sie folgende Warnung erhalten bestätigen Sie mit Ok



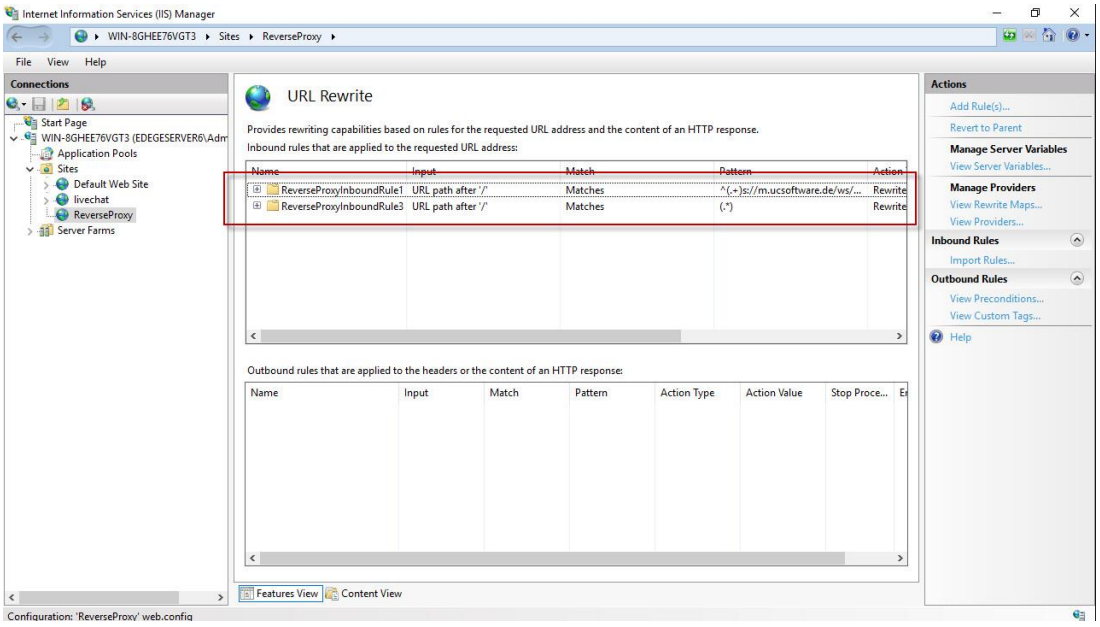
4. Machen Sie im nächsten Dialog Angaben wohin die Anfragen umgeleitet werden sollen.



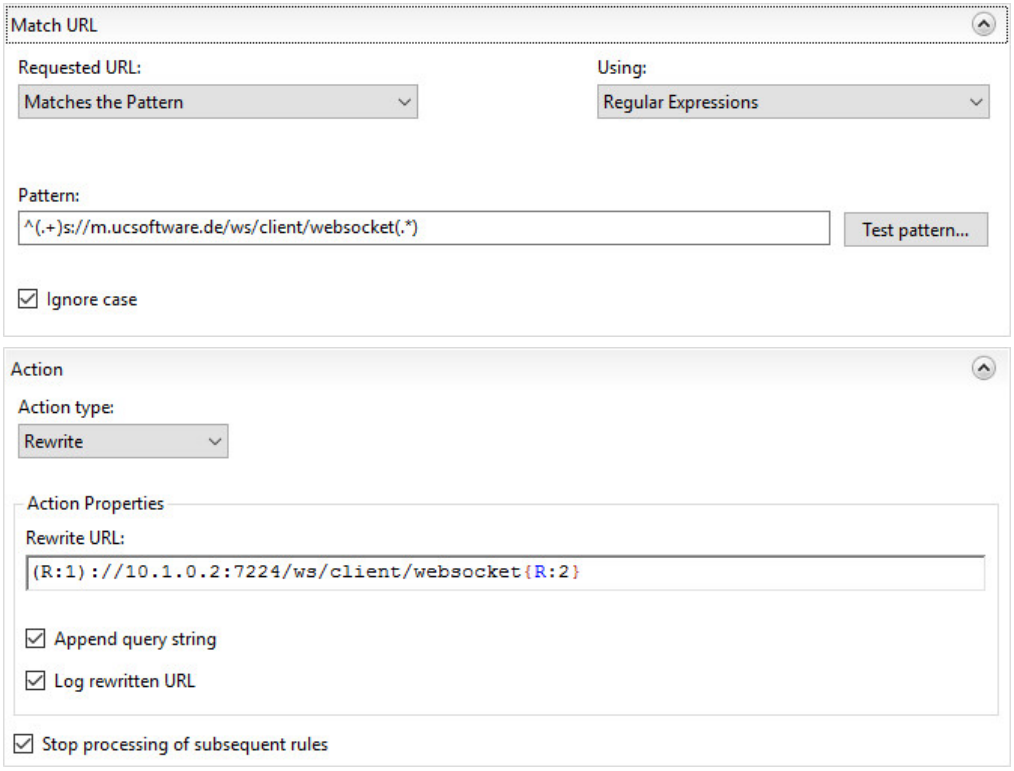
   a. Tragen Sie Inbound Roules den DNS-Namen oder die IP-Adresse ein, auf die die Anfragen umgeleitet werden sollen (z.B. UCServer, Firewall). Ergänzen Sie außerdem den gewünschten Port.

   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

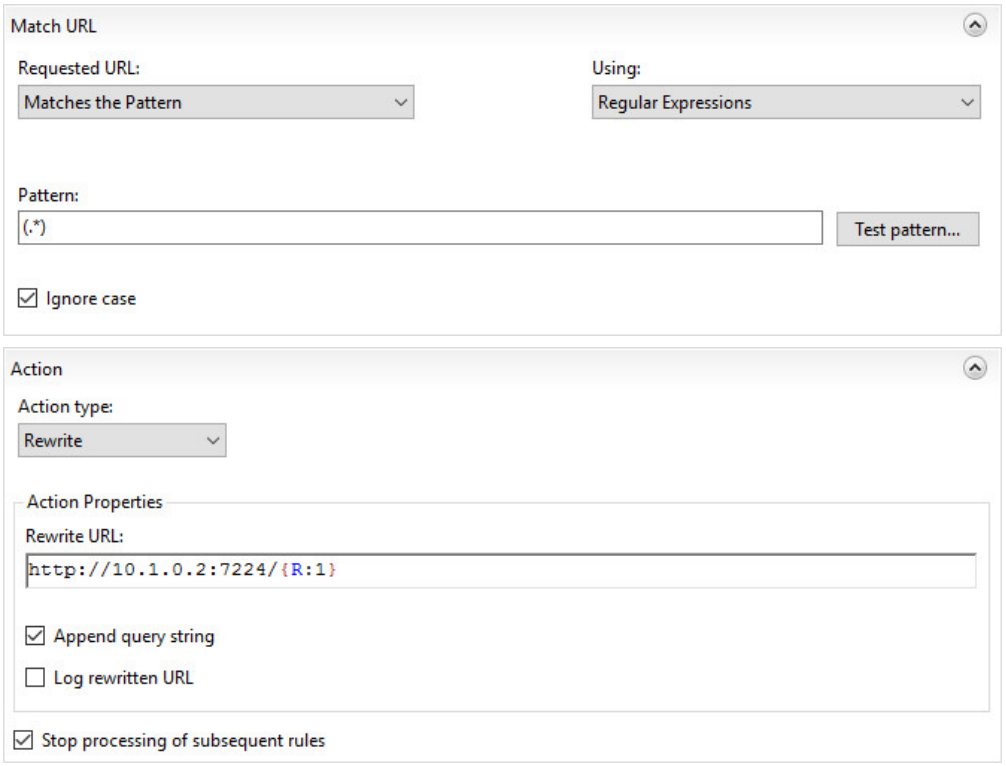


a. Unter Match URL muss ein Regulärer Ausdruck hinterlegt werden, um den Upgrade der http(s) auf eine ws(s) Verbindung abzubilden. Tauschen Sie bei folgender Vorlage <DNS NAME> mit Ihrem DNS Eintrag aus.
^(.+)s://<DNS NAME>/ws/client/websocket(.*)

b. Unter Action definieren Sie wie die URL umgeschrieben wird und an welchen DNS-Namen oder 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

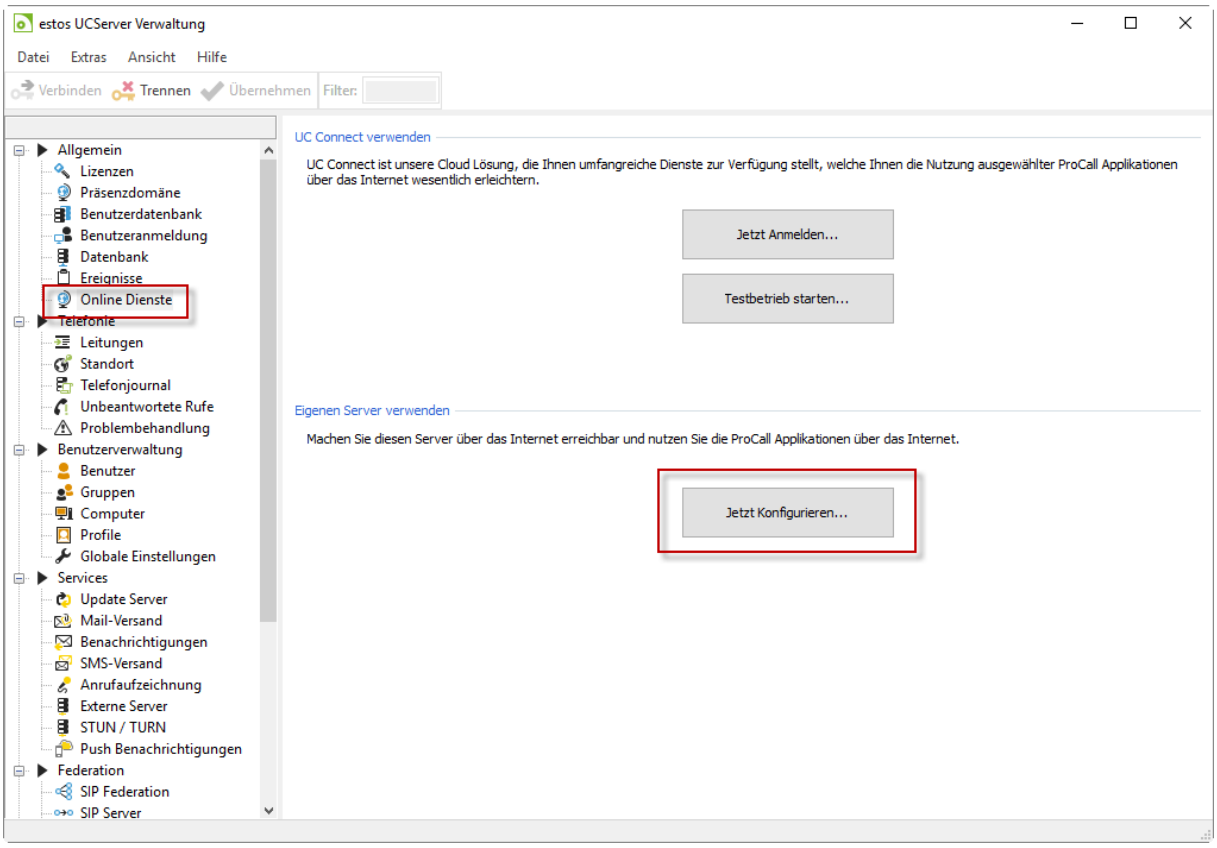


   a. Unter Match URL muss ein Reguläre Ausdruck hinterlegt werden, der alle vom ersten Ausdruck nicht erfassten Anfragen trotzdem weiterleitet. Eine Anpassung der Vorlage ist nicht notwendig.
   (.*)

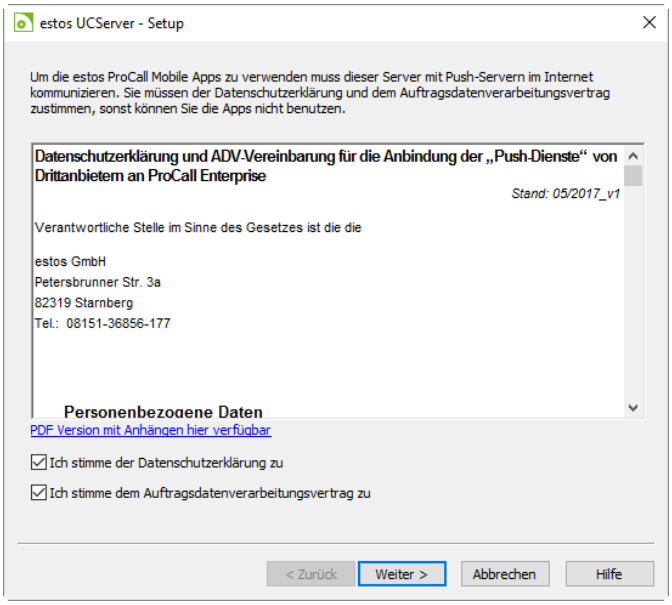
   b. Unter Action definieren Sie wie die URL umgeschrieben wird und an welchen DNS-Namen oder IP-Adresse die Anfrage weitergeleitet wird. Tauschen Sie bei folgender Vorlage <REWRITE TARGET> mit dem gewünschten Weiterleitungsziel und <PORT> mit dem konfigurierten Port.
   http://<REWRITE TARGET>:<PORT>/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

Konfiguration abschließen und prüfen

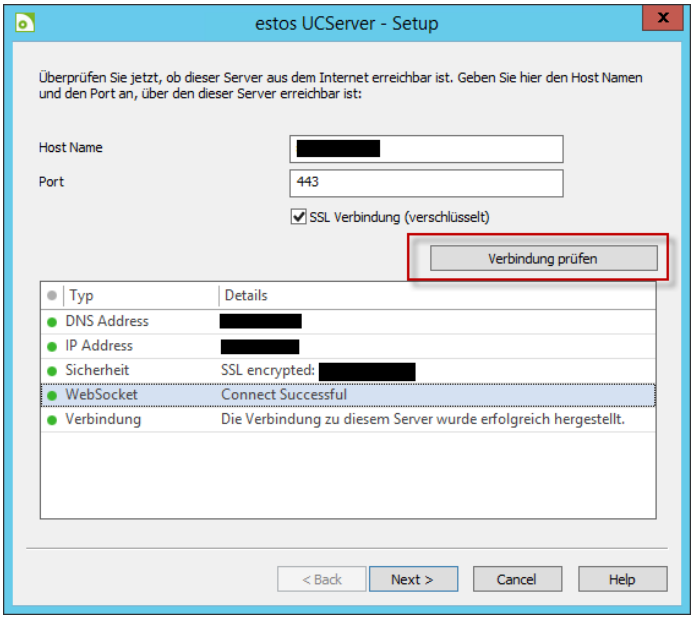
Zum Abschluss der Konfiguration rufen Sie bitte die UCServer Verwaltung auf und navigieren zu dem Punkt Online Dienste unter Eigenen Server verwenden klicken Sie auf Jetzt Konfigurieren…



Bitte akzeptieren Sie im nachfolgenden Dialog die Datenschutzerklärung und die ADV-Vereinbarung für die Nutzung der Push-Dienste für ProCall Mobile.



Anschließen können Sie über die integrierte Diagnose Funktion überprüfen ob der UCServer Webservice erfolgreich veröffentlicht wurde.



Geben Sie dazu unter Host Name den von ihnen gewählten DNS Namen ein und aktivieren Sie SSL Verbindung. Anschließen wird eine Diagnose durchgeführt, sollten Sie ein zum obigen Screenshot vergleichbares Bild erhalten wurde die Veröffentlichung erfolgreich durchgeführt.

3.3.2. nginx

Installation nginx

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

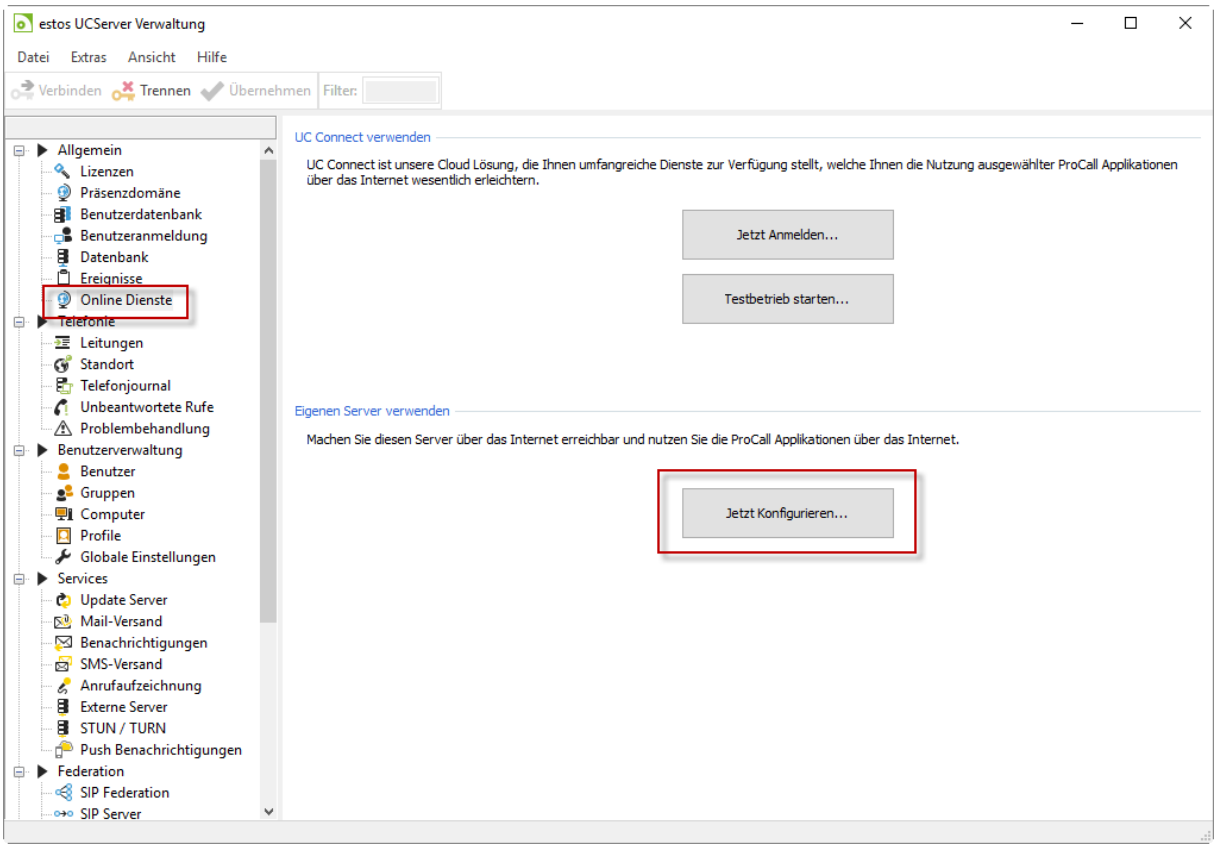
```
$ sudo apt-get update
$ sudo apt-get install nginx
```

Konfiguration nginx

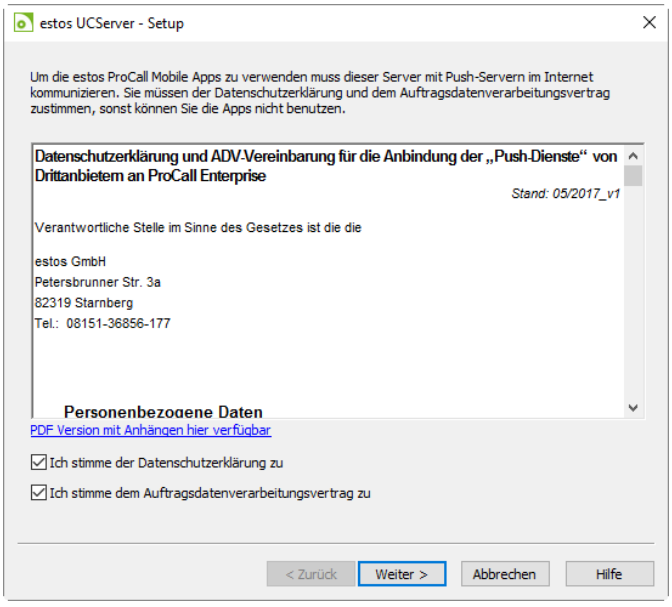
1. Legen Sie unter `/etc/nginx/sites-available` eine neue Konfigurationsdatei mit Namen *reverseproxy* an und kopieren Sie unser nginx Beispielkonfiguration in die Datei.
2. Es wird empfohlen ein vertrauenswürdiges SSL-Zertifikat zu verwenden. Ergänzen Sie die SSL-Konfiguration gemäß http://nginx.org/en/docs/http/configuring_https_servers.html.
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`

Konfiguration abschließen und prüfen

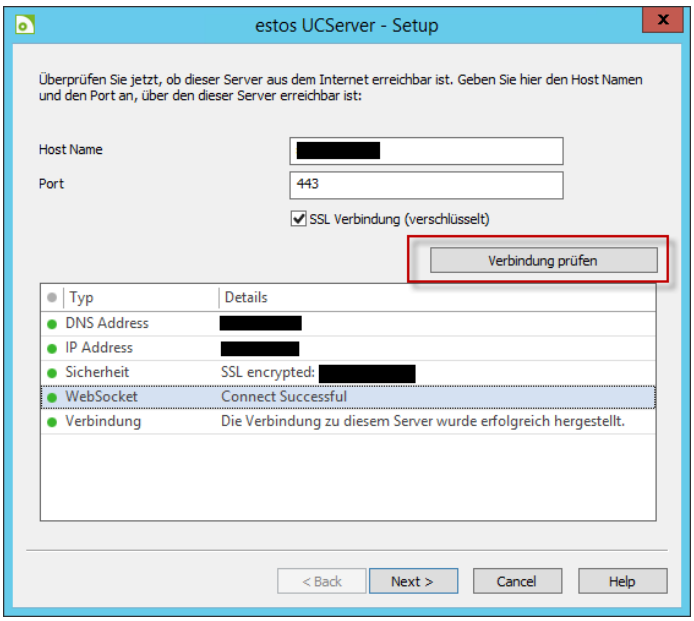
Zum Abschluss der Konfiguration rufen Sie bitte die UCServer Verwaltung auf und navigieren zu dem Punkt Online Dienste unter Eigenen Server verwenden klicken Sie auf Jetzt Konfigurieren…



Bitte akzeptieren Sie im nachfolgenden Dialog die Datenschutzerklärung und die ADV-Vereinbarung für die Nutzung der Push-Dienste für ProCall Mobile.



Anschließen können Sie über die integrierte Diagnose Funktion überprüfen ob der UCServer Webservice erfolgreich veröffentlicht wurde.



Geben Sie dazu unter Host Name den von ihnen gewählten DNS Namen ein und aktivieren Sie SSL Verbindung. Anschließen wird eine Diagnose durchgeführt, sollten Sie ein zum obigen Screenshot vergleichbares Bild erhalten wurde die Veröffentlichung erfolgreich durchgeführt.

nginx Beispielkonfiguration

```
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";
       }
}
```