

# UCServer Webservice Release Best Practice

### Legal Information/Imprint

The information contained in this document reflects the state of knowledge at the time the document was created. Errors and subsequent alterations are reserved.

estos GmbH rejects any liability for damage caused by the direct or indirect use of this document.

All brand and product names quoted are the trademark or property of their respective owner.

Our current Terms and Conditions of Business can be found on our website at http://www.estos.de/agb.

Copyright estos GmbH. All rights reserved.

estos GmbH Petersbrunner Str. 3a D-82319 Starnberg <u>info@estos.de</u> <u>www.estos.de</u>

27.01.2015

# Document history

Version	Date	Author	Amendments
1	29.06.2017	DW	Initial
2	19.09.2017	DW	nginx adjusted

# Contents

1.	Int	rodu	ction	4
2	Ro	auire	aments	5
۷.	NC	quire.	inchio,	J
3.	Re	lease		6
	3.1.	Ove	erview	6
	3.2.	Cor	nfigure UCServer	7
	3.2	.1.	Port forwarding	7
	3.2	.2.	http reverse proxy	8
	3.3.	Inst	all and configure http reverse proxy	8
	3.3	.1.	Microsoft Internet Information Services (IIS)	9
	3.3	.2.	nginx1	8

# 1. Introduction

Together with the UCServer, a web service is always installed, which is permanently connected to the UCServer. The release of UCServer Webservice allows you to use ProCall Mobile, ProCall (desktop) and other web applications, not only in the local network, but also over the internet or from home. The use of these applications over the internet requires access to this UCS server from the internet, as well as STUN and TURN servers for the use of audio and video chat. At release, we differentiate between three different scenarios.

- 1. Release without DMZ
- 2. Release with DMZ
- 3. Release with the help of our supplementary online services (UCConnect)

The supplementary online services are not covered by this document.

# 2. Requirements

The following requirements must be met to launch the UCServer Webservice:

• Public IP address

Your Internet access must have a public IP address

• DNS entry

The public IP address must be resolvable via a DNS entry. Add a DNS A Record to your domain (such as ucws.domain.com), use your public IP address

• SSL certificate

The certificate should be issued by a public certification authority (CA), which is considered trustworthy by current browsers and operating systems. If you are working with a self-signed certificate, the connection is encrypted, but not secure against tapping. This makes it impossible to use browser applications

Caution

A trustworthy certificate is mandatory for the use of browser applications.

# 3. Release

# 3.1. Overview

Basically, there are three different technical options that have to be considered when launching the UCServer Webservice.

- 1. The UCServer has a public IP address, i.e. it is directly connected to the Internet
- 2. The UCServer has no public IP address, i.e. it is located behind a NAT device and "port forwarding" is used
- 3. The UCServer has no public IP address, i.e. it is behind a NAT device and will use an "http reverse proxy"

Depending on the structure of your IT infrastructure (with/without DMZ), we recommend a different approach.

DMZ	Location UCServer	Method		
No	LAN	Port Forwarding		
Yes	DMZ	Tortrorwarding		
Yes	LAN	http Reverse-Proxy		

Port Forwarding



Configure the NAT router with port forwarding, the encryption (TLS) of the communication is done by UCServer Webservice. These settings can be found in the UCServer administration in the menu under Tools >> Network interfaces.

## http Reverse-Proxy



An http reverse proxy is a server that accepts http(s) inquiries and forwards them to a server in the private network. This http reverse proxy requires the SSL certificate. The communication is forwarded to the UCServer via http (on the network interface of the Web-Service http) or https (on the network interface of the "WebService https").

You can use as a server, for example, nginx (proxy\_pass), Apache (mod\_proxy, ProxyPass), or Microsoft<sup>®</sup> IIS (Application Request Routing).

Note
The http reverse proxy must also allow WebSocket connections (RFC 6455) in addition to
http GET and POST.

# 3.2. Configure UCServer

Depending on the scenario, different configurations must be made at the UCServer.

# 3.2.1. Port forwarding

## **IP ports**

In UCServer administration, you can view and change the network settings of the UCServers in the menu under Tools >> Network interfaces. In the default settings, the UCS server answers requests via http on port 7224 and https on port 7225. Normally, this setting doesn't need to be changed.

## SSL certificate

In the case of port forwarding, all requests from the internet are received directly from UCServer Webservice, so it is also responsible for the encryption of the connection. We strongly recommend using https with a trustworthy SSL certificate. If necessary, request an SSL certificate for your DNS name from a public certification authority. If you are working with a self-signed certificate, the connection is encrypted, but not secure against tapping and the use of browser applications is not possible.

In the UCServer administration, you can store a certificate in PFX format under Tools >> Network interfaces >> WebService https.

### Set-up port forwarding

Configure port forwarding on your NAT router by forwarding port 443 TCP from your public IP to the https port of the UCServer Webservice (default: 7225).

# 3.2.2. http reverse proxy

#### **IP ports**

In UCServer administration, you can view and change the network settings of the UCServers in the menu under Tools >> Network interfaces. In the default settings, the UCS server answers requests via http on port 7224 and https on port 7225. Normally, this setting doesn't need to be changed.

#### SSL certificate

In the case of http reverse proxy, all requests from the internet are first accepted by the proxy and then forwarded to UCServer Webservice, so the proxy is also responsible for the encryption of the connection. We strongly recommend using https with a trustworthy SSL certificate. If necessary, request an SSL certificate for your DNS name from a public certification authority. If you are working with a self-signed certificate, the connection is encrypted, but not secure against tapping and the use of browser applications is not possible.

Depending on requirements, you can forward the requests within your LAN via unencrypted http or TLS encryption. If you prefer an encrypted connection within your LAN as well, you can define a certificate in PFX format in the UCServer administration under Tools >> Network interfaces >> WebService https.

## 3.3. Install and configure http reverse proxy

Theoretically, all standard http reverse proxy servers can be used that allow http GET and POST and WebSocket connections (RFC 6455).

Within the framework of this document, the implementation of three different proxy servers will be specifically covered. Depending on their abilities and preferences, both Microsoft Windows and Linux can be selected as the operating system.

Microsoft Windows compatible

- Microsoft Internet Information Services (IIS)
- Apache HTTP Server

#### Linux compatible

- nginx
- Apache HTTP Server

# 3.3.1. Microsoft Internet Information Services (IIS)

Requirements

- Microsoft Internet Information Services (IIS) from Version 10
- WebSocket Protocol Feature for IIS
- Application Request Routing (ARR) from Version 3 (<u>https://www.iis.net/down-loads/microsoft/application-request-routing</u>)
- URL Rewrite Module for IIS from Version 2 (<u>https://www.iis.net/downloads/mi-crosoft/url-rewrite</u>)

## Installation and preparation of Microsoft Internet Information Services (IIS)

- 1. Install Microsoft Internet Information Services (IIS) on the desired server. Download the installation package or add the role via the server administration
- 2. Add the WebSocket protocol feature

🚵 Add Roles and Features Wizard			– 0 ×
Select server roles			DESTINATION SERVER EdegeServerő
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Select one or more roles to install on the selected server.  Role  Paper-V Pap	~	Description IIS 10.0 and ASP.NET 4.6 support writing server applications that communicate over the WebSocket Protocol.
			< Previous Next > Install Cancel

- 3. Install the Application Request Routing (ARR) package
- 4. Install the URL Rewrite module

## Configuration of Microsoft Internet Information Services (IIS)

In order to establish the proxy function, all components involved must be set up in the next step and configured according to your infrastructure.

#### Configure SSL Certificate

It is recommended to use a trustworthy SSL certificate. Set up a server certificate for IIS, as suggested by Microsoft: <u>https://technet.microsoft.com/en-us/cc731977</u>

UCServer Webservice Release

le View Hele						
need the second s	2000					Actions
	WIN-8GHEE76	VGT3 Home				Actions
Start Page	<b>₽</b> ⊁		10			Manage Server
WIN-8GHEE76VGT3 (EDEGESERVER6\Adr	Filter:	🌾 Go 🕞 😽 Show All 🛛 Grou	p by: Area 🔹 🐨	•		Start
Application Pools	lis	-	analas e esta per		^	Stop
V Sites				1 🔯 🕌		View Application Pools
> 🕘 livechat	Application Authentic Cor	mpression Default Dir	ectory Error Pages Hand	ler HTTP HTTP	Logging	View Sites
> 🕘 ReverseProxy	Request R	Document Bro	owsing Mappi	ngs Redirect Respon.		Get New Web Platform
>	p 📩		7 🛃 🛃			
	MIME Types Modules (	Output Request S	erver URL Rewrite Work	er		a ricp
	c	Caching Filtering Cer	tificates Proces	ises		
	Management				*	
		*				
	Configurat Feature S	Shared				
	Editor Delegation Cor	nfigurat				
, , , , , , , , , , , , , , , , , , ,	Features View	ew				
iy >	E Features View 🕰 Content Vie	ew				
y >>	Features View 🖧 Content Vie	ew				
ly htemet Information Services (IIS) Manager	E Features View 🦓 Content Vie	ew				- 0
by hternet Information Services (IIS) Manager € . WIN-8GHEF76VGT3 .	E Features View Content Vie	€W				- 0
by Internet Information Services (IIS) Manager → 4 WIN-8GHEE76VGT3 →	Features View Content Vie	ew				
dy nternet Information Services (IIS) Manager → @ → WIN-8GHEE76VGT3 → e View Help	Eatures View 🕰 Content Vie	ew				- <b>6</b> 2
ty nternet Information Services (IIS) Manager ♀ ♀	Features View Content Vie	ew				- 0 ::
by nternet Information Services (IIS) Manager Q > WIN-8GHEE76VGT3 > e View Help mettions D & &	E Features View Content Vie	ew ates				Actions
ay nternet Information Services (IIS) Manager	Features View Content Vie	ew ates	eb server can use with websites	configured for SSL.		Actions
ay nternet Information Services (IIS) Manager WIN-8GHEE76VGT3 > View Help Interiors Start Page Start Page WIN-8GHEE76VGT3 (EDEGESERVER6).Adr	E Features View Content Vie	ew ates nanage certificates that the W	eb server can use with websites	configured for SSL.		Actions Import Create Certificate Request Complete Certificate Request.
y nternet Information Services (IIS) Manager	Features View Content Vie Server Certifica Use this feature to request and n Filter:	ew ates manage certificates that the W ☞ Go → ₩ Show All   Grou	eb server can use with websites o p by: No Grouping •	configured for SSL.		Actions Import Create Certificate Request Complete Certificate Request Complete Certificate Request
dy Internet Information Services (IIS) Manager	Features View Content Vie	ew ates manage certificates that the W ♥ Go - Go - Go Show All Grou Issued To	eb server can use with websites p by: No Grouping • Issued By	configured for SSL. Expiration Date	Certificate Hash	Actions Import Create Certificate Request Complete Certificate Request Correcte Domain Certificate. Create Domain Certificate.
dy Internet Information Services (II5) Manager e View Help metcions Start Page WIN-8GHEZF6VGT3 (EDEGESERVER6).Adr Application Pools Sites Default Web Site ) Default Web Site ) Default Web Site ) Default Web Site	Features View Content Vie Server Certifica Use this feature to request and n Filter:	ew ates manage certificates that the W © Go - Con Show All Grou Issued To *.ucsoftware.de	eb server can use with websites p by: No Grouping • Issued By ucsoftware-DC-CA	configured for SSL. Expiration Date 01.03.2019 12:55:06	Certificate Hash 3F6E30B020127C4D1	Actions Import Create Certificate Request Complete Certificate Request Create Self-Signed Certificate. Create Self-Signed Certificate. Enable Automatic Rehind e
dy Internet Information Services (II5) Manager	E Features View Content Vie	ew ates manage certificates that the W @ Go ~ Go Show All Grou Issued To *.ucsoftware.de	eb server can use with websites r p by: No Grouping • Issued By ucsoftware-DC-CA	configured for SSL. Expiration Date 0.1.03.2019 12:55:06	Certificate Hash 3F6E30B020127C4D1	Actions Import Create Certificate Request Complete Certificate Request Create Self-Signed Certificate Create Self-Signed Certificate Enable Automatic Rebind o Renewed Certificate
y Internet Information Services (IIS) Manager	Features View Content View Server Certifica Use this feature to request and n Filter:	ew ates manage certificates that the W @ Go ~ En Show All Grou Issued To *.ucsoftware.de	eb server can use with websites p by: No Grouping • Issued By ucsoftware-DC-CA	configured for SSL. Expiration Date 01.03.2019 12:55:06	Certificate Hash 3F6E30B020127C4D1	Actions Import Create Certificate Request Create Certificate Request Create Domain Certificate Create Self-Signed Certificate Enable Automatic Rebind on Renewed Certificate @ Help
by nternet Information Services (IIS) Manager	Features View Content View Server Certifica Use this feature to request and n Filter:	ew ates manage certificates that the W Go - Co Show All Grou Issued To *.ucsoftware.de	eb server can use with websites of by: No Grouping • Issued By ucsoftware-DC-CA	configured for SSL. Expiration Date 01.03.2019 12:55:06	Certificate Hash 3F6E30B020127C4D1	Actions Import Create Certificate Request Complete Certificate Request. Create Self-Signed Certificate Enable Automatic Rebind o Renewed Certificate

Set up a reverse proxy website

< Ready <

Features View 💦 Content View

6-

1. Add a new website



2. Fill in the required fields (see example below)

inections	0	Add Website		? X		Actions
Start Page     Start Page	Filter: Name Default	Site name: Application pool: ReverseProxy ReverseProxy Content Directory Physical path: Channet in the D	Select		root	Add Website Set Website Defaults     Help
> ⊕ fivechat	Reverse	I connect as  Pass-through authentication Connect as  Fest Settings  Binding Type: IP address: Intrps IIP address: Intrps III Unassigned III Unassigned III Unassigned IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	ort: 43 ct View OK C	ncel	rowy	

- a. The path specification is not particularly relevant since no website is delivered. IIS will still create a web.config file. We recommend the path:
   C:\inetpub\wwwroot\ReverseProxy
- b. Use https as a binding type
- c. Set the host name that corresponds to your DNS entry and certificate
- d. Select the certificate you have previously stored

# Configure the URL rewrite module

1. Double-click the newly created website and open URL Rewrite

Ele View Male		
File View Help Connections View Jack Page View Start P	ReverseProxy Home         Filter          •          •          •	Alerts         ▲ No default SSL site has been created. To support browser without SNL capabilities, in the commended to create a default SSL site.         Actions         ▲ Explore         ■ Bindings         ■ Start         ■ Start         ■ Stop:         Browser Website         ■ Browser Website         ■ Browser Strings         Configure         Limits         ● Help

2. Click Add Rule(s) ... and select Reverse Proxy

rile view neip			
<ul> <li>Yev Prep</li> <li>Connections</li> <li>Start Page</li> <li>With effect?/vCT3 (EDEGESERVER6/Adm</li> <li>With effect?/vCT3 (EDEGESERVER6/Adm</li> <li>With effect?/vCT3 (EDEGESERVER6/Adm</li> <li>O Default Web Site</li> <li>O Default Web Site</li> <li>O Default Web Site</li> <li>O EnverseProxy</li> <li>Server Farms</li> </ul>	VILL Rewrite VILL Rewrite VILL Rewrite VILL Remplate VILL	op Proce E	Actions Add Rule(s) Revert to Parent Manage Server Variable Manage Providers View Rewrite Maps View Rewrite Maps View Providers Inbound Rules Import Rules Outbound Rules View Preconditions View Custom Tags We Preconditions View Custom Tags

3. If you receive the following warning, confirm with OK

Add Reverse Proxy Rules	Imj
Proxy functionality must be enabled in App Routing (ARR) before reverse proxy rules proxy functionality allows the possibility of servers that are outside your server farm. Are you sure you want to enable proxy fu	olication Request will work. Enabling routing requests to nctionality?
	Cancel

4. In the next dialog box, enter the information as to where the requests are to be forwarded

la Reverse Proxy Rules	?	×
Inbound Rules		
Enter the server name or the IP address where HTTP requests will be forwarded:		
10.1.0.2:7224		
Example: contentserver1		
Enable SSL Offloading		
Selecting this option will forward all HTTPS requests over HTTP.		
Outbound Rules		
Rewrite the domain names of the links in HTTP responses		
Responses that are generated by applications that are behind a reverse proxy can	have	
HTTP links that use internal domain names. These links must be updated to use e	xternal	
domain names.		
domain names. From:		
domain names. From: Example: contentsever1		
domain names. From: Example: contentserver1		
domain names. From: Example: contentserver1 To:		
domain names. From: Example: contentserver1 To:	~	
domain names. From: Example: contentserver1 To: Example: www.contoso.com	~	
domain names. From: Example: contentserver1 To: Example: www.contoso.com	~	
domain names. From: Example: contentserver1 To: Example: www.contoso.com	~	
domain names. From: Example: contentserver1 To: Example: www.contoso.com	~	
domain names. From: Example: contentserver1 To: Example: www.contoso.com	×	

- a. Enter in Inbound Rules the DNS name or the IP address to which the requests are to be forwarded (for example, UCServer, Firewall). Also add the desired port
- b. If you enable SSL offloading, the requests are forwarded unencrypted. It is assumed that the option was activated
- 5. In this way, add two identical rules

e View Help									
nections								Actions	
	URL Rewrite	Add Rule(s)							
	Provides rewriting capabilities base	ed on rules for the	requested URL a	ddress and the cont	tent of an HTTP n	esponse.		Revert to Parent	
	Inbound rules that are applied to t	he requested URL	address:					Manage Server Varial	bles
	Name	Innut		Match		Dattern	Action	View Server Variables	
	ReverseProxvInboundRule	1 URL path after	7	Matches		^(.+)s://m.ucsoftware.de/	ws/ Rewrite	Manage Providers	
	🗉 🧮 ReverseProxyInboundRule	3 URL path after	7	Matches		(.*)	Rewrite	View Rewrite Maps	
			~					View Providers	
								Inbound Rules	
								Import Rules	
								Outbound Rules	
								View Preconditions	
								View Custom Tags	_
	¢						>	🕑 Help	
	Outbound rules that are applied to	the headers or th	e content of an H	HTTP response:					
	Name	Input	Match	Pattern	Action Type	Action Value St	top Proce Er		

6. Open the top rule with a double-click and edit Match URL and Action

Using:
Regular Expressions
Test pattern
at (D.2)

- a. Under Match URL, a regular expression must be placed to map the upgrade of http(s) to a ws(s) connection. In the following template, replace <DNS NAME> with your DNS entry ^(.+)s://<DNS NAME>/ws/client/websocket(.\*)
- b. Under Action, define how the URL is to be copied and to which DNS name or IP address the request is forwarded. In the following template, replace <RE-WRITE TARGET> with the desired forwarding destination and <PORT> with the configured port (R:1)://<REWRITE TARGET>:<PORT>/ws/client/websocket{R:2}
- c. Select Stop processing of subsequent rules

7. Open the second rule with a double-click and edit Match URL and Action

Match URL		٢
Requested URL:	Using:	
Matches the Pattern $\vee$	Regular Expressions	~
Pattern:		
(.*)		Test pattern
☑ Ignore case		
Action		٢
Action type: Rewrite ~		
Action Properties		
Rewrite URL:		
http://10.1.0.2:7224/{R:1}		
Append query string		
Log rewritten URL		
Stop processing of subsequent rules		

- a. Under Match URL, a regular expression must be stored, which still redirects all requests not recorded by the first expression. An amendment of the template is not necessary

   (.\*)
- b. Under Action, you define how the URL is to be copied and to which DNS name or IP address the request is forwarded. In the following template, replace <REWRITE TARGET> with the desired forwarding destination and <PORT> with the configured port http://<REWRITE TARGET>:<PORT>/ {R:1}

#### Complete and check the configuration

To complete the configuration, please select UCServer Administration and navigate to the Online Services section under Use your own server, click Configure Now...



Please accept the privacy and the contract data processing policy for the use of push services for ProCall Mobile in the following dialog box.

estos UCServer - Setup	×
Um die estos ProCall Mobile Apps zu verwenden muss dieser Server mit Push-Servern im Internet kommunizieren. Sie müssen der Datenschutzerklärung und dem Auftragsdatenverarbeitungsvertrag zustimmen, sonst können Sie die Apps nicht benutzen.	
Datenschutzerklärung und ADV-Vereinbarung für die Anbindung der "Push-Dienste" von Drittanbietern an ProCall Enterprise Stand: 05/2017_v1	^
Verantwortliche Stelle im Sinne des Gesetzes ist die die	
estos GmbH Petersbrunner Str. 3a 82319 Starnberg Tel.: 08151-36856-177	
Personenbezogene Daten	~
PDF Version mit Anhängen hier verfügbar	
🗹 Ich stimme der Datenschutzerklärung zu	
🗹 Ich stimme dem Auftragsdatenverarbeitungsvertrag zu	
< Zurück Weiter > Abbrechen Hilfe	

You can use the integrated diagnostics function to check whether UCServer Webservice was successfully launched.

•	estos UCServer - Setup
Überprüfen Sie jetzt, ob dies und den Port an, über den di	er Server aus dem Internet erreichbar ist. Geben Sie hier den Host Namen eser Server erreichbar ist:
Host Name	
Port	443
	SSL Verbindung (verschlüsselt)
	Verbindung prüfen
• Тур	Details
DNS Address	
IP Address	
Sicherheit	SSL encrypted:
WebSocket	Connect Successful
Verbindung	Die Verbindung zu diesem Server wurde erfolgreich hergestellt.
	< Back Next > Cancel Help

Enter your DNS name under Hostname and enable the SSL connection. A diagnosis will be carried out. The launch was successfully carried out if you receive a similar image to the screenshot above.

# 3.3.2. nginx

#### nginx installation

Install nginx over the package management of your Linux distribution, e.g. on Ubuntu:

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

#### nginx configuration

- 1. In /etc/nginx/sites-available create a new configuration file named *reverseproxy* and copy our Fehler! Verweisquelle konnte nicht gefunden werden. in this file
- 2. It is recommended to use a trustworthy SSL certificate. Complete the SSL configuration as shown <u>http://nginx.org/en/docs/http/configuring\_https\_servers.html</u>
- 3. In the example, replace <DNS NAME> with your DNS entry, <REWRITE TARGET> with the desired forwarding destination, and <PORT> with the configured port
- 4. Activate the configuration /etc/nginx/sites-enabled by creating a symbolic link to the configuration file under:

```
$ cd /etc/nginx/sites-enabled
$ sudo ln -s /etc/nginx/sites-available/reverseproxy
```

5. Restart the nginx service

sudo systemctl restart nginx.service **Of** sudo service nginx restart

## Complete and check the configuration

To complete the configuration, please select UCServer Administration and navigate to the Online Services section under Use your own server, click Configure Now...

estos UCServer Verwaltung		_		×
Vakiadan X Tanana (200				
Verbinden 😋 Irennen 🖤 Obe	menmen Filter:			
	UC Connect verwenden			
<ul> <li>Allgemein         <ul> <li>Allgemein</li> <li>Lizenzen</li> <li>Präsenzdomäne</li> <li>Benutzerdatenbank</li> <li>Benutzeranmeldung</li> <li>Datenbank</li> <li>Ereignisse</li> <li>Online Dienste</li> </ul> </li> <li>Telefonje</li> <li>Telefonjournal</li> <li>Unbeantwortete Rufe</li> <li>Arobemutzervwaltung</li> <li>Benutzervwaltung</li> <li>Benutzerverwaltung</li> <li>Benutzerverwaltung</li> <li>Gruppen</li> <li>Computer</li> <li>Profile</li> <li>✓ Globale Einstellungen</li> <li>SSNS-Versand</li> <li>SUN-Versand</li> <li>STUN / TURN</li> <li>Push Benachrichtigungen</li> <li>SIP Federation</li> <li>SIP Federation</li> </ul>	UC Connect ist unsere Cloud Lösung, die Ihnen umfangreiche Dienste zur Verfügung stellt, welche Ihnen die Nutzung ausgewählter über das Internet wesentlich erleichtern. Jetzt Anmelden Testbetrieb starten Egenen Server verwenden Machen Sie diesen Server über das Internet erreichbar und nutzen Sie die ProCall Applikationen über das Internet. Jetzt Konfigurieren	ProCall A	pplikation	en

Please accept the privacy and the contract data processing policy for the use of push services for ProCall Mobile in the following dialog box.

• stos UCServer - Setup	×
Um die estos ProCall Mobile Apps zu verwenden muss dieser Server mit Push-Servern im Internet kommunizieren. Sie müssen der Datenschutzerklärung und dem Auftragsdatenverarbeitungsvertra zustimmen, sonst können Sie die Apps nicht benutzen.	9
Datenschutzerklärung und ADV-Vereinbarung für die Anbindung der "Push-Dienste" vo Drittanbietern an ProCall Enterprise Stand: 05/2017_	n ∧ _v1
Verantwortliche Stelle im Sinne des Gesetzes ist die die	
estos GmbH	
Petersbrunner Str. 3a	
82319 Starnberg	
Tel.: 08151-36856-177	
Personenbezogene Daten	~
PDF Version mit Annangen hier verfugbar	
☑ Ich stimme der Datenschutzerklärung zu	
☑ Ich stimme dem Auftragsdatenverarbeitungsvertrag zu	
< Zurück Weiter > Abbrechen H	ilfe

You can use the integrated diagnostics function to check whether the UCServer web service was successfully launched.

•	estos UCServer - Setup
Überprüfen Sie jetzt, ob dies und den Port an, über den di	er Server aus dem Internet erreichbar ist. Geben Sie hier den Host Namen eser Server erreichbar ist:
Host Name	
Port	443
	SSL Verbindung (verschlüsselt)
	Verbindung prüfen
• Тур	Details
DNS Address	
IP Address	
Sicherheit	SSL encrypted:
WebSocket	Connect Successful
Verbindung	Die Verbindung zu diesem Server wurde erfolgreich hergestellt.
	< Back Next > Cancel Help

Enter your DNS name under Hostname and enable the SSL connection. A diagnosis will be carried out. The launch was successfully carried out if you receive a similar image to the screenshot above.

#### nginx sample configuration

```
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";
      }
```