

STARFACE - Microsoft Teams Integration mit Patton SBC

Thorsten Abbenzeller (STARFACE Trainer – Geschäftsführer netzwerkkontor GmbH & Co.KG)

Fabian Wolf (Geschäftsführer Fluxpunkt GmbH)

Boyan Radovic (Patton Technical Presales / MS-Teams Integration)

Version 1.15/2021.01.07/at

Vorwort:

Das folgende Dokument soll eine Unterstützung für die STARFACE Microsoft Teams Integration darstellen. Es wurde von Techniker für Techniker verfasst und setzt gute Kenntnisse in Netzwerktechnik, sowie gute Office 365 Kenntnisse voraus. Da sowohl MS-Teams, STARFACE als auch Patton stets neue Features herausbringen, kann sich auch die eine oder andere Herangehensweise ändern.

Dieses Dokument hat weder den Anspruch der Vollständigkeit, noch ist es der einzige Weg Teams mit STARFACE zu verheiraten. Es ist ein Weg unter vielen möglichen.

Wir empfehlen dringend, jeweils die aktuellen Patche von Microsoft, STARFACE und Patton installiert zu haben.

Wir wünschen Euch allen viel Spass und Erfolg bei Euren Projekten.

Boyan, Fabian, Thorsten

Grundvoraussetzung

Voraussetzungen für die Umsetzung:

- Kenntnisse in Office 365 Administration (am besten mit Powershell)
- Lizenzen für O365 Telefoniesystem
- Kenntnisse in Patton OS bzw. Administration von Patton SBCs
- Lizenzen von Patton
- STARFACE PBX aktuelle Version / SF-6.7.3 oder höher (Am sinnvollsten SF PBX mit Updatevertrag)
- STARFACE / Fluxpunkt Modul Teams Integration
- Notwendige Lizenzen (UCC / Modullizenzen)
- Zertifikat für den SBC

Notwendige Tools:

- Einen Editor, z.B: Notepad ++
- MS-Powershell mit Teams Modulen (O365 Module)
- SSH Programm – z.B. Putty

Wozu die Teams Integration?

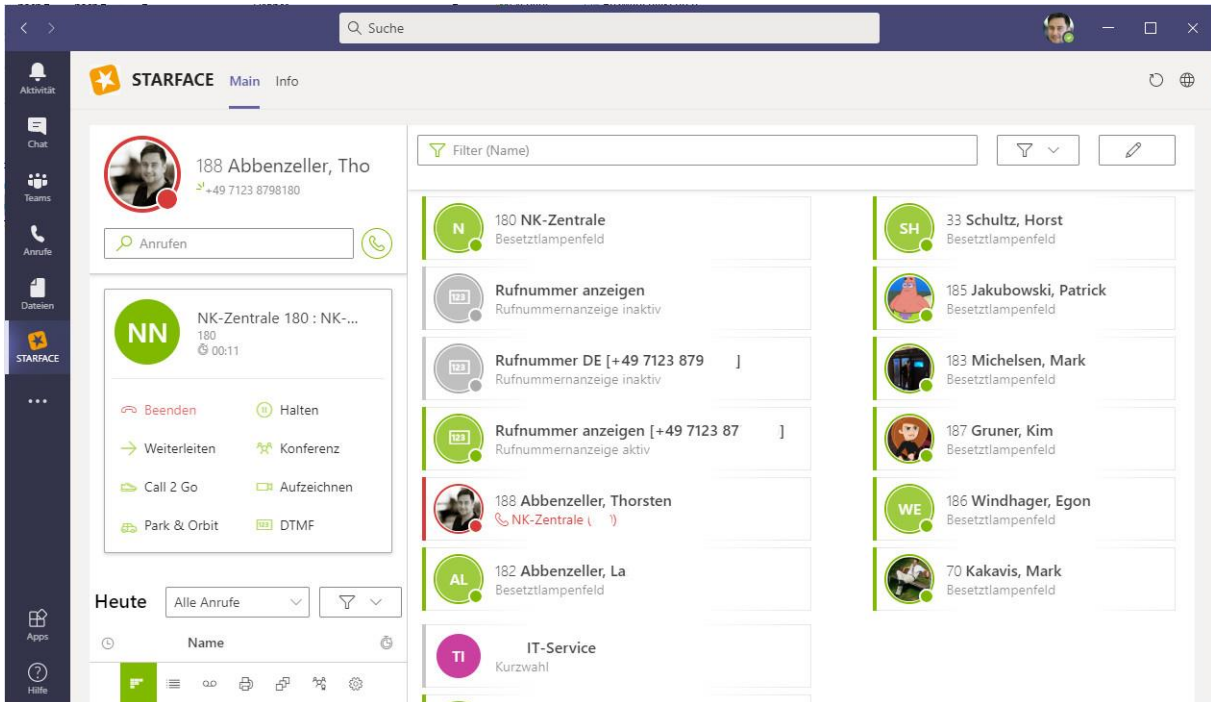
Office 365 ist in aller Munde. Wer hätte vor der Covid-19 Pandemie gedacht, dass sich das Thema Cloud Unified Communication so rasant entwickelt. Im Jahr 2020 wird Microsoft mit dem Produkt MS-Teams die 100 Millionen User Marke knacken. Die Marschroute auf der Microsoft Ignite im Herbst 2020 und vor allem die Keynote zu MS Exchange zeigen, dass Microsoft Office 365 klar im Focus hat. Es sieht so aus, als würde Microsoft die Kunden in die O365 Welt drängen.

MS-Teams ist bereits bei der kleinsten Lizenzierung inkludiert. Es macht durchaus Sinn Teams in der Unternehmenskollaboration einzusetzen, Vorteile durch z.B. Single Sign on mit Azure Active Directory.

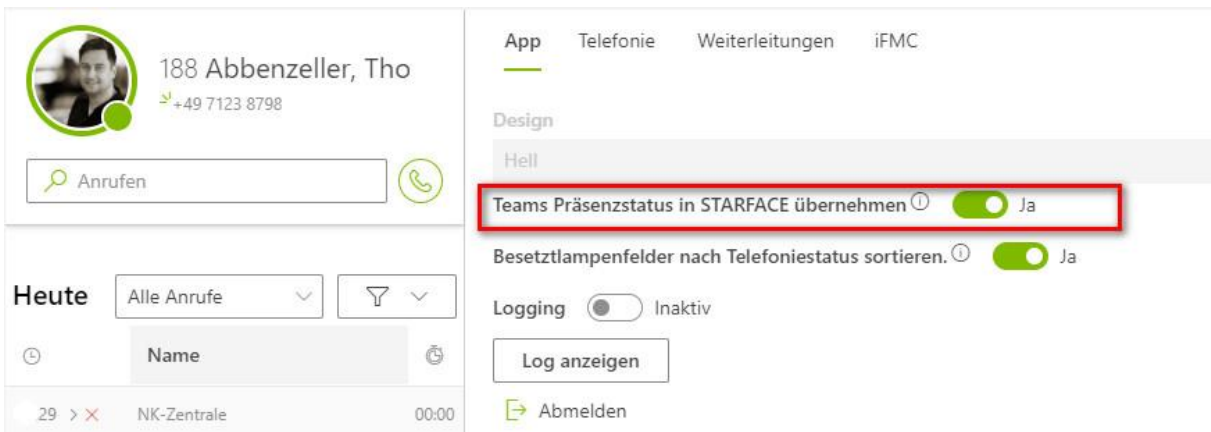
Mit dem O365 Telefonie System wird Teams zur TK-Anlage. Jedoch mit eingeschränkten Features und teilweise doch recht umständlich zu konfigurieren. Da wäre es doch schön, die Vorteile der STARFACE PBX zu nutzen und dann mit Teams zu kombinieren. Das ist mit dem STARFACE/FLUXPUNKT Modul MS-Teams Integration nun möglich.

Folgende Vorteile:

- ⇒ Kombination aus beiden Welten, klassische TK-Funktionalitäten gemeinsam mit den UCC-Features von MS Teams nutzbar.
- ⇒ Der MS Teams Client wird „der“ Client für den täglichen Gebrauch und steuert die Nebenstelle der STARFACE
- ⇒ Anrufmanagement erfolgt über den Teams Client
- ⇒ Status-Abgleich zwischen MS Teams und STARFACE – keine Festnetzanrufe während einer Präsentation



(Abb.1 – Besetztlampenfelder aus der STARFACE in Teams anzeigen)



(Abb.2 – Unter Einstellungen Teams Präsenz in STARFACE übernehmen)

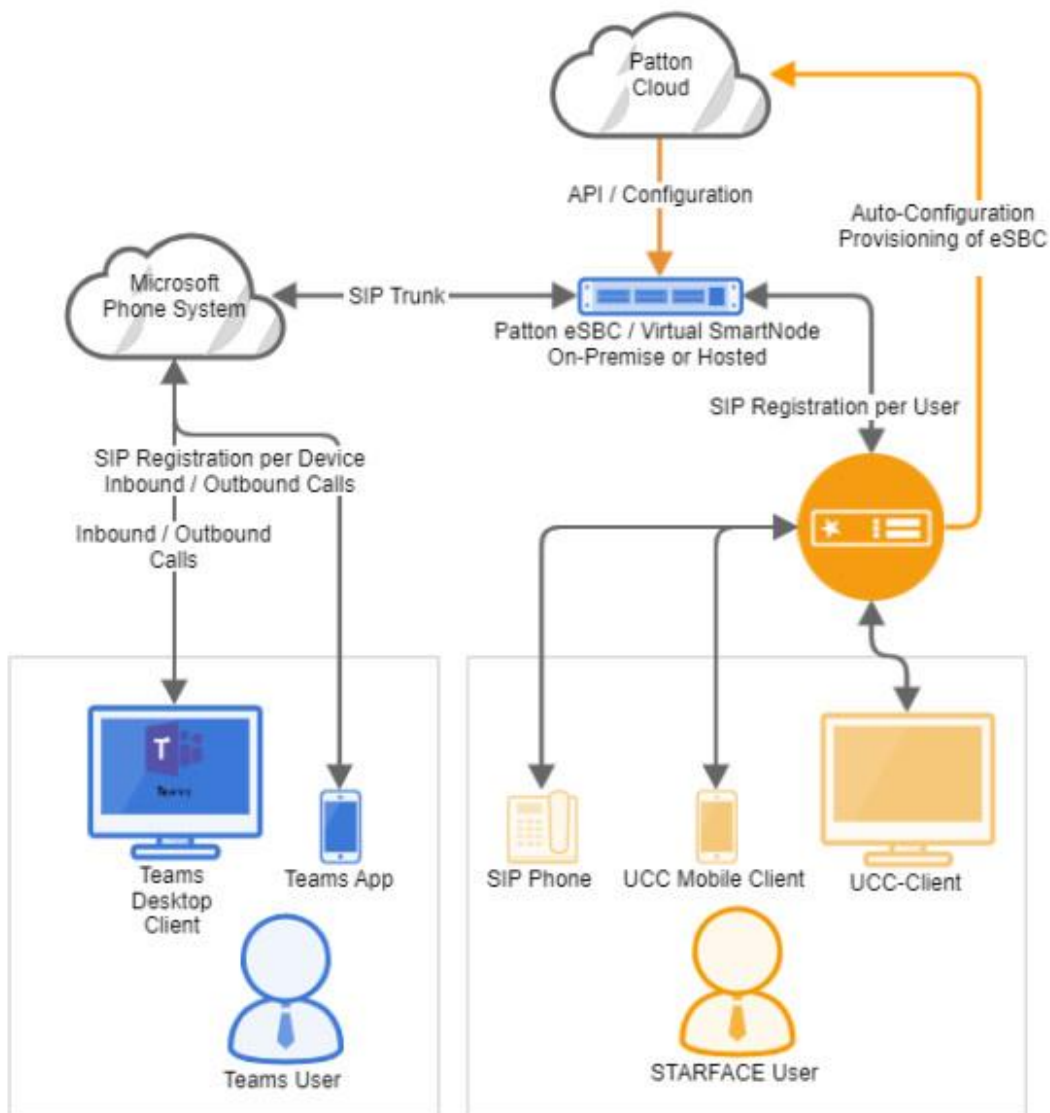
Aufbau der Umgebung:

Da STARFACE als Asterisk basiertes TK – System *eine* Welt darstellt und Microsoft Office 365 *eine andere* Welt darstellt, müssen diese beiden Welten über eine gemeinsame Schnittstelle verheiratet werden. Dies ist in unserem Fall der Patton SBC. Auf die verschiedenen Modelle (Größe / Virtuell oder Hardware) gehen wir im Anhang ein. Wir benutzen für unser Szenario einen Hardware Patton SN5501/8P.



An der Stelle ist es unbedingt wichtig die aktuelle Firmware installiert zu haben. Die Mindestanforderung ist: **3.18.1** oder höher.

Der Patton ist die Brücke zwischen Office 365 und der STARFACE. Im unten gezeigten Bild können wir die zentrale Funktion des Pattons erkennen.



(Abb3 – Der Patton verbindet Office365 Phone System (Teams) mit STARFACE)

Patton vorbereiten

Zuerst kontrollieren wir ob alles für die Integration vorhanden ist:

- **Lizenzen:** Nötige Lizenzen für den Patton beziehen
- **Firmware:** Minimale SW-Version: Trinity 3.18.1 (Freigabe Oktober 2020) – Update erforderlich.
- **Zertifikat:** Das TLS-Zertifikat und den privaten Schlüssel generieren.
Allgemeine Auskünfte vom Kapitel “37 - Public Key Infrastructure (PKI)” vom Patton Trinity CLI Guide als Grundlage verwenden.

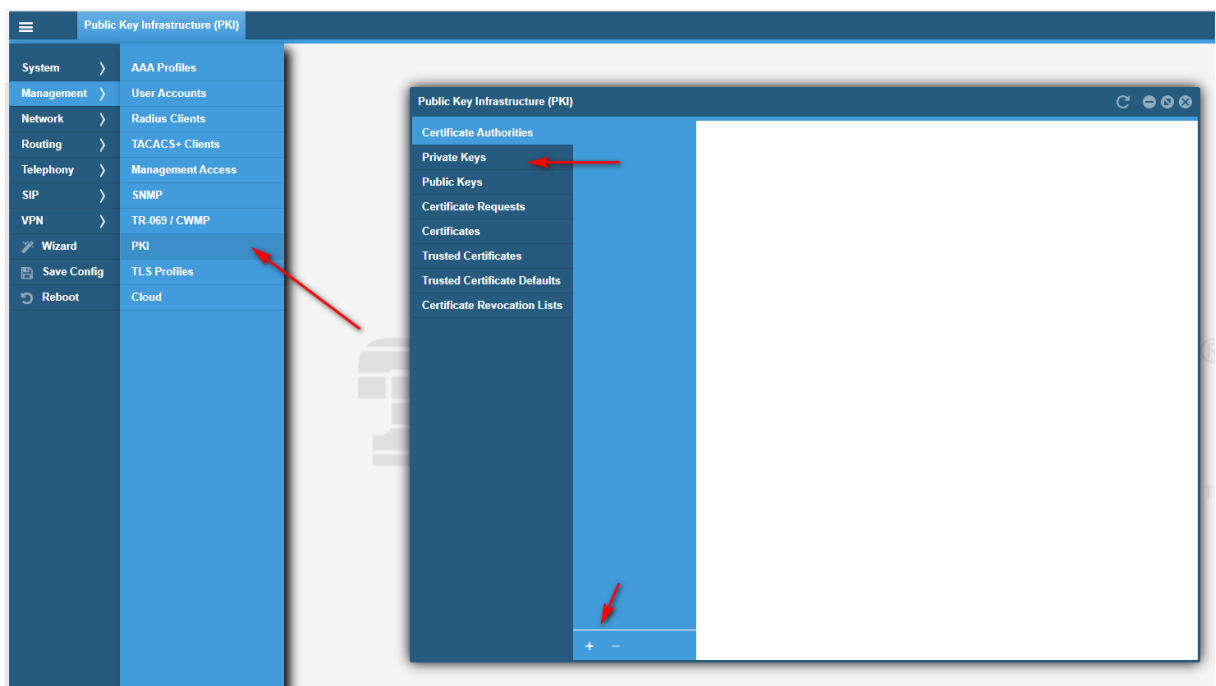
Wenn beide Dateien bereit sind, müssen sie auf den SmartNode hochgeladen werden.
In unserem Laborsystem-Beispiel sind es folgende zwei Dateien:

- TLS-Zertifikat **SBC.MEINEFIRMENDOMAIN.crt**
- Privater Schlüssel **MEINEFIRMENOMAIN.key**
- **Public IPv4:** Es muss eine öffentliche IP-Adresse auf dem SBC konfiguriert werden (in nachfolgender Konfigurationsanleitung generisch als AAA.BBB.CCC.DDD gekennzeichnet), zu welcher der FQDN-Name auflöst, in unserem Beispiel sbc.meinefirmendomain.org
 - D.h. dies muss im öffentlichen DNS auflösbar sein. Ich empfehle den DNS A oder AAAA record frühzeitig zu setzen, damit dieser auch für die spätere Konfiguration in der O365 Adminconsole bereits auffindbar (auflösbar) ist.

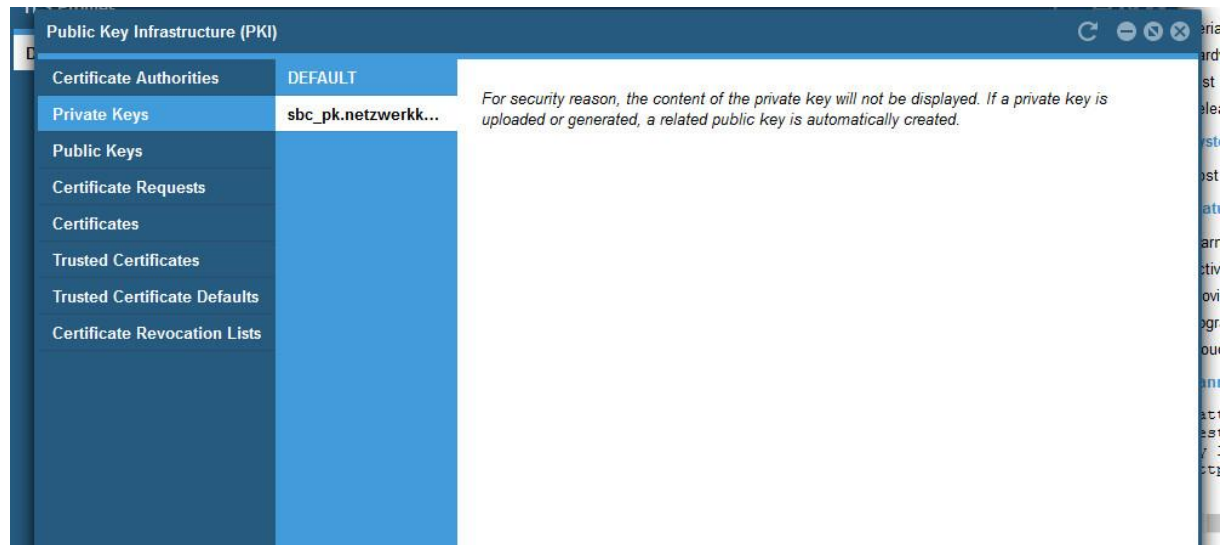
Nachdem wir Firmware und Lizenzen organisiert haben, starten wir mit dem Zertifikat. Dazu müssen wir zuerst einen Private Key, sowie ein CSR generieren.

Den Menüpunkt dazu finden wir unter Management PKI:

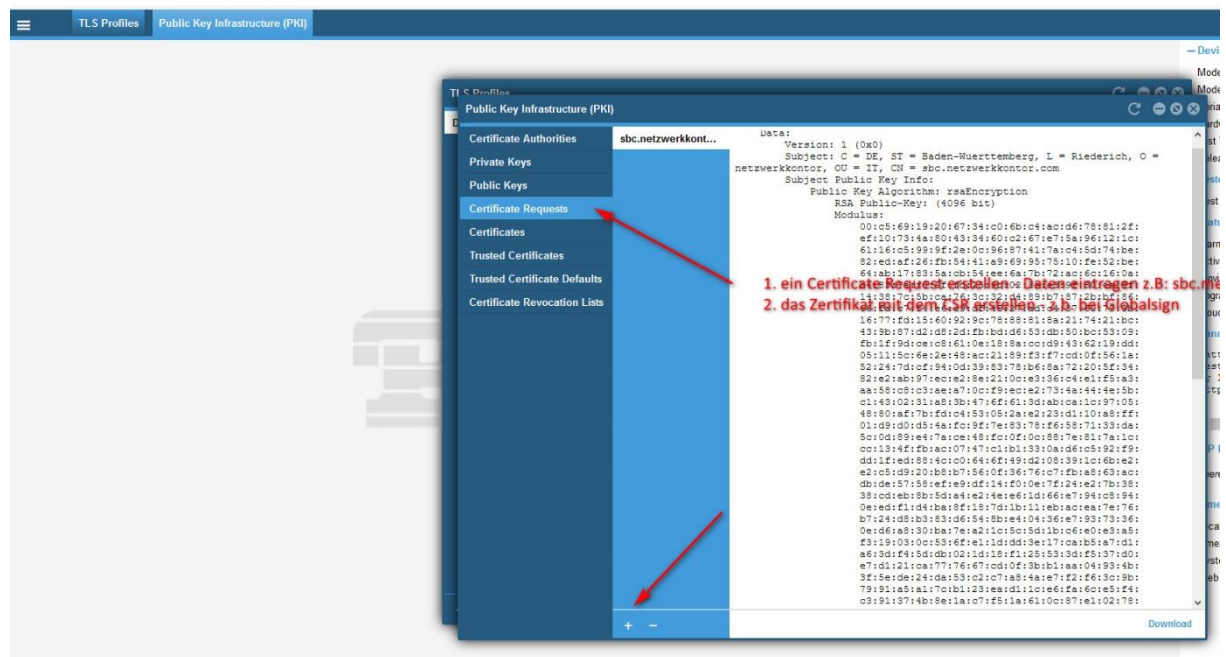
Dort legen wir einen Private Key an und danach erstellen wir den CSR, damit wir das Zertifikat beim CertProvider beantragen können.



Nachdem wir den Private Key angelegt haben, erstellen wir den CSR: - Der Private Key ist nach Erstellung NICHT im Browser sichtbar.



Nun erstellen wir den CSR



HINWEIS:

Microsoft besteht auf „ordentliche Zertifikate eines Certificate Providers“ - eine Liste der zugelassenen Provider finden wir im Microsoft Technet / MSDN. Self Signed Zertifikate oder Let's Encrypt Zertifikate sind von Microsoft nicht zugelassen und daher nicht möglich. Also schlucken wir hier die Kröte und kaufen ein Zertifikat (in unserem Szenario bei Globalsign).

Wichtig ist, dass wir nach Ausstellung des Zertifikates dann auch das root / intermediate Zertifikat dem Patton bereitstellen.

Public Key Infrastructure (PKI)

Certificate Authorities: CA

Private Keys: DEFAULT

Public Keys: sbc.netzwerkkont...

Certificate Requests

Certificates

Trusted Certificates

Trusted Certificate Defaults

Certificate Revocation Lists

Certificate:

Data:

Version: 3 (0x2)

Serial Number:
77:bd:0e:07:42:d5:d9:e9:d0:49:d7:74:d0:2a:6f:9a

Signature Algorithm: sha256WithRSAEncryption

Issuer: OU = GlobalSign Root CA - R3, O = GlobalSign, CN = GlobalSign

Validity

Not Before: Jul 28 00:00:00 2020 GMT

Not After : Mar 18 00:00:00 2029 GMT

Subject: C = BE, O = GlobalSign nv-sa, CN = GlobalSign GCC R3 DV TLS CA

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public-Key: (2048 bit)

Modulus:
00:ac:67:94:95:7f:75:ef:8e:a7:0c:af:09:70:09:

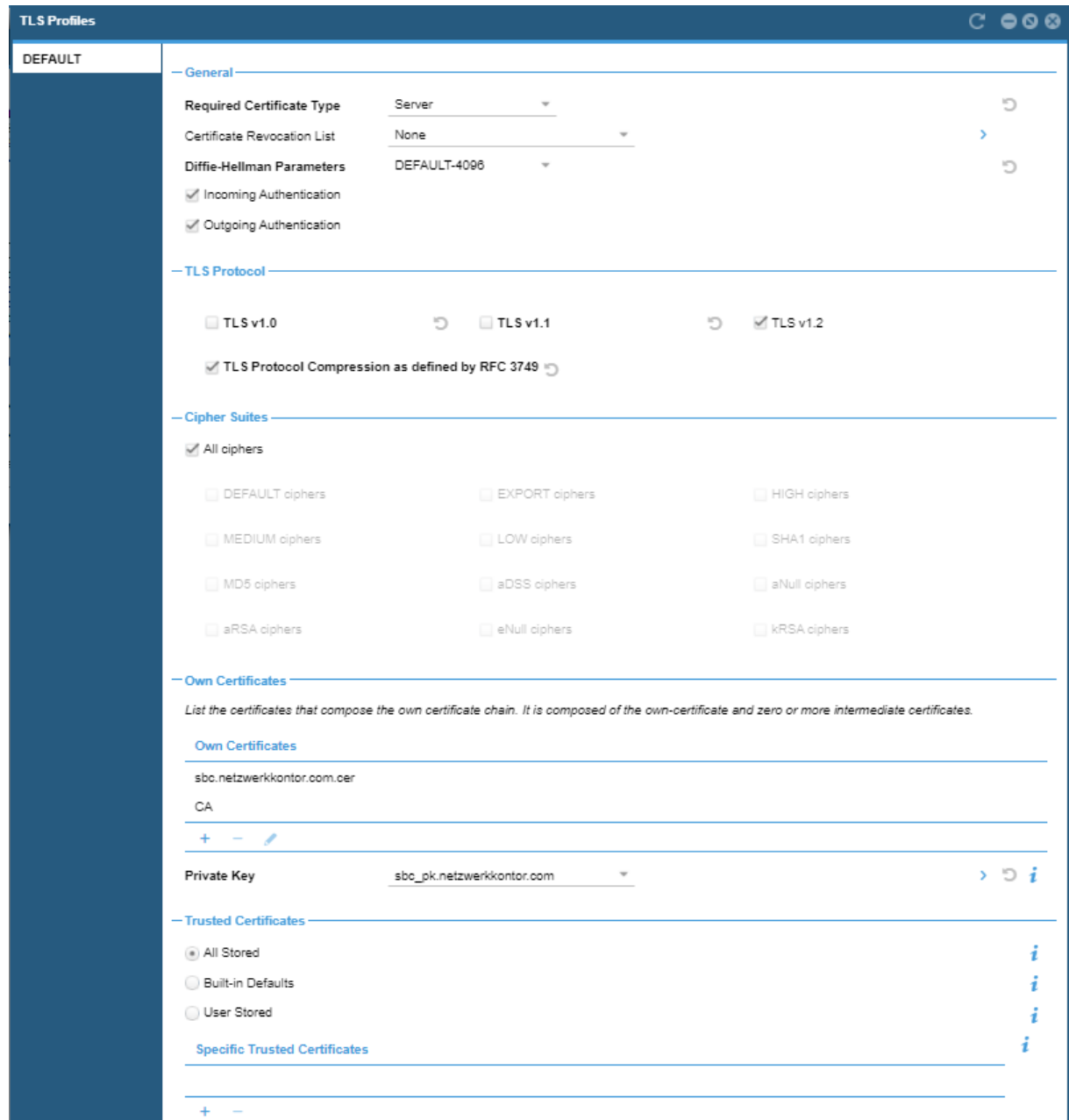
2020

Root Certificate (CA)

Ausgestelltes Zertifikat nach dem Import

Dies ist ein elementarer Schritt, ohne den wir nicht weitermachen können.

Danach weisen wir das Zertifikat in den TLS Profiles zu:



Natürlich können wir das auch mit z.B. Putty in der Shell konfigurieren

CLI: Eingabe auf der Kommandozeile per SSH/Telnet

```

10F2439#import pki:certificate/MYCERTIFICATE
2Paste the contents of the file (enter an empty line when done):
3-----BEGIN CERTIFICATE-----
4MIIGZjCCBU6gAwIBAgIQDfw+rcYnGBfoqe36UQFQPzANBgkqhkiG9w0BAQsFADBH
5QswCQYDVQQGEDJVUzEWMBQGA1UEChMNR2VvVHJ1c3QgSW5JLjEgMB4GN1UEVxMX
6UmF aWRTU0wgU0hBMjU2IENBIC0gRzlwHhcNMTYxMjU2MDAwMDAwWWhcNMjU2MDAw
7.....
8bD8l3HKHS/7u2lOzu/Ja0C5u6CSXdmPeq9Zof77vempXQHx0Bwl+b5bzOAza28p5
9KBbWfi+fdh6kz2ydXUXWGbGZuBykeu1F+M65FchP7/b7ElpKgtFJJyS3EvYH1iY
101wuJqHHBIOB+3Q==

```

```

11-----END CERTIFICATE-----
12
130F2439#import pki:private-key/myprivate.key
14Paste the contents of the file (enter an empty line when done):
15-----BEGIN RSA PRIVATE KEY-----
16/iqCw7vgv+SuzqcCIBtmZ0iH1XAC8fs5RfoM5yeAfv/kOpjGMNg+3hB0f8MVAHcA
17.....
18AiEA+DtGLCgvVangxlyhXbWRbxGGEY4wmNCi7x5ib7yYGBACIQCRQImIL2SHRIED
19-----END RSA PRIVATE KEY-----
20
210F2439#import pki:certificate/CA
22Paste the contents of the file (enter an empty line when done):
23-----BEGIN CERTIFICATE-----
24MChjKSAyMDA4IEdlb1RydXNOIEluYy4gLSBGb3IgYXV0aG9yaXplZCB1c2Ugb25s
25.....
26a2qiiMbpwFd9svlxDJhIMuwlWs7GmOkhlz8seSkD9faUK1Mx85NoV+HXTzrRYaFg
27-----END CERTIFICATE-----

```

Erklärung:

- Zeile 1: Import des eigenen X.509 Zertifikats. Der Name MYCERTIFICATE kann frei gewählt werden und wird im Folgenden für die Referenzierung dieses Zertifikats verwendet. Das Zertifikat selbst (beginnend mit -----BEGIN CERTIFICATE----- wird per Copy&Paste eingefügt. Das Zertifikat endet auf -----END CERTIFICATE----- und muß durch eine Leerzeile abgeschlossen werden.
- Zeile 13: Import des privaten Schlüssels, der zum öffentlichen Schlüssel des X.509-Zertifikats gehört.
- Zeile 21: Import einer Intermediate CA, um die "Chain-of-Trust" von einer vertrauenswürdigen Root-CA bis hin zum eigenen Zertifikat zu bilden.

TLS Profile: Parameter für die verschlüsselte Kommunikation mit Microsoft Phone System

```

1profile tls pf_tls_default
2 no protocol tls-v1.0
3 no protocol tls-v1.1
4 compression
5 authentication incoming
6 authentication outgoing
7 private-key pki:private-key/MEINEFIRMENOMAIN.key
8 own-certificate 1 pki:certificate/ SBC.MEINEFIRMENDOMAIN.crt
9 own-certificate 2 pki:certificate/CA
10 diffie-hellman-parameters pki:diffie-hellman-parameters/DEFAULT-4096
11 require certificate-type server

```

Erklärung

- Zeile 2-3: Durch Deaktivierung der Protokolle TLS 1.0/1.1 wird TLS 1.2 erzwungen.
- Zeile 7: Verweis auf den privaten Schlüssel
- Zeile 8: Verweis auf das eigene X.509 Zertifikat, mit dem sich der SBC ausweist.
- Zeile 9: Verweis auf das/die zuvor importierte(n) Intermediate CA(s).

Nachdem wir nun das Zertifikat angelegt haben, können wir mit der eigentlichen Konfiguration des Patton beginnen.

PATTON: Access-Lists vorbereiten zum Schutz des Patton und des eigenen Netzes

Da über das WEB INTERFACE viele Details zu klicken und zu beachten sind, empfehle ich die Nutzung eines SSH Clients z.B: Putty. Zusammen mit einem Editor lassen sich die Kommandos einfach vorbereiten und dann schnell einspielen.

Die Befehle sind ähnlich dem CISCO IOS – wer also schon einmal einen CISCO Router konfiguriert hat, wird sich schnell zurechtfinden.

Grundsätzlich gilt: Der SBC ist mit dem Internet verbunden.

D.h. es ist obligatorisch, dass wir als Techniker auch dafür verantwortlich sind, dass der Patton nur von den IPs erreichbar ist, die auch genutzt werden. Auf dem Patton können Access Lists angelegt werden. Nach der Konfiguration ist immer zu prüfen, ob die Accesslists / Firewallregeln auch funktionieren. Es ist dringend ein Test empfohlen.

Hier ein **Beispiel**, das wir mit CLI per SSH konfigurieren:

```
profile acl ACL_LAN_IN_DENY
permit 1 src-ip 172.30.1.1
permit 2 src-ip 10.72.X.X/24
```

⇒ Hier legen wir die Lan Ips fest, die den Patton erreichen dürfen (z.B: STARFACE / INTRANET)

```
profile acl ACL_WAN_IN_DENY
permit 1 src-ip 52.114.148.0
permit 2 src-ip 52.114.132.46
permit 3 src-ip 52.114.75.24
permit 4 src-ip 52.114.76.76
permit 5 src-ip 52.114.7.24
permit 6 src-ip 52.114.14.70
permit 7 src-ip 52.114.16.74
permit 8 src-ip 52.114.20.29
permit 9 src-ip MEIN EIGENES NETZWERTK
```

⇒ Hier legen wir die WAN Ips fest, die den Patton erreichen dürfen (z.B: hier Microsoft und mein eigenes Firmennetz)

```
profile acl ACL_WAN_PROTOCOLS
permit 1 protocol udp dest-port 53,123,5060,5061
permit 2 protocol tcp dest-port 53,443,5060,5061
permit 3 protocol icmp
```

⇒ Hier legen wir fest, welche Protokolle akzeptiert werden

⇒ Nun weisen wir die ACLs den Interfaces zu.

context ip ROUTER

interface WAN

```
ipaddress WAN 213.23.93.180/25
use profile acl in 1 ACL_WAN_IN_DENY
use profile acl in 2 STATEFUL_ACL
use profile acl out 1 ACL_WAN_PROTOCOLS
use profile acl out 2 STATEFUL_ACL
use profile napt NAPT_WAN WAN
```

interface LAN

```
ipaddress LAN 10.1.10.180/16
use profile acl in 1 ACL_LAN_IN_DENY
```

PATTON: Erstellen der VOIP Profile auf dem Patton

Nun erstellen wir VoIP Profile, damit der Patton sowohl mit Microsoft als auch mit der STARFACE reden kann. Das Profil bestimmt die Parameter wie sich unterhalten wird. Also auf welcher Basis der Patton mit Teams / SBC und STARFACE die Kommunikation abläuft.

Am einfachsten funktioniert das mit dem CLI unter Putty:

1. VoIP Profile für die Kommunikation mit Microsoft Phone System / Teams

```

1 profile voip pf_voip_microsoft
2 codec 1 g711alaw64k rx-length 20 tx-length 20 silence-suppression voice-update-frames
3 srtp key-lifetime 31
4 media-processing forced
5 srtp transmission forced
6 rtp rtcp-multiplexing

```

Erklärung:

- Zeile 2: Es wird der Audio-Codec G.711alaw gegenüber dem Microsoft SBC angeboten. Weitere Codecs werden nicht konfiguriert, damit keine Codec-Transkodierung notwendig wird (hierfür werden Hardware DSPs in Patton SmartNodes benötigt, die in begrenzter Anzahl in physikalischen Geräten vorhanden sind; virtualisierte SmartNodes werden Software DSPs mit Transkodierung zu einem späteren Zeitpunkt unterstützen; vgl. Patton Roadmap). Microsoft verlangt von Teams-zertifizierten Geräten die Erzeugung von Komfortauschen, weshalb Stille im Audiodatenstrom erkannt und durch Rauschen ersetzt werden soll ("silence-suppression").
- Zeile 3: Zur Verbesserung der Sicherheit wird nach 2³¹ Paketen der für die Verschlüsselung verwendete SRTP-Schlüssel ausgetauscht.
- Zeile 4: Erzwingt die Verwendung von DSP Ressourcen, die für die Verschlüsselung benötigt werden.
- Zeile 5: SRTP-Verschlüsselung ist zwingend zwischen Microsoft und SBC.
- Zeile 6: RTP und RTCP Multiplexing nach RFC5761 (Verwendung derselben Portnummern; Anforderung von Microsoft).

2. VoIP Profile für die Kommunikation mit STARFACE

```

1 profile voip pf_voip_starface
2 codec 1 g711alaw64k rx-length 20 tx-length 20 silence-suppression voice-update-frames
3 media-processing forced
4 rtp rtcp-multiplexing

```

Erklärung

- Zeile 2: Es wird der Audio-Codec G.711alaw gegenüber der STARFACE angeboten. Weitere Codecs werden nicht konfiguriert, damit keine Codec-Transkodierung notwendig wird.

Damit nun zwischen den Welten gesprochen werden kann, müssen wir „mapping“ Tabellen anlegen. Der Grund ist der, dass O365 Rufnummern in einem bestimmten Format erwartet und die STARFACE in einem anderen Format. Der Patton spielt den Dolmetscher zwischen beiden und übersetzt in beide Richtungen.

Übersetzung von Teams-Telefonnummern in STARFACE Account-Namen

```

1 mapping-table calling-uri to calling-e164 mt_teams2starface-a-e164
2 map sip:(.%) to \1
3 map tel:(.%) to \1
4
5 mapping-table calling-e164 to calling-uri mt_teams2starface-a-uri
6 map \+497123222 to sip:user.01@10.108.2.100
7 map \+497123223 to sip:user.02@10.108.2.100
8 map \+497123224 to sip:user.03@10.108.2.100
9
10 mapping-table called-e164 to called-e164 mt_teams2starface-b-internalCalls
11 map (00)?49(...?)$ to \2

```

Erklärung:

- Zeile 1-3: Das Mapping *calling-uri to calling-e164 mt_teams2starface-a-e164* entnimmt der SIP-URI die Anrufer Rufnummer und setzt diese als Anrufer Rufnummer im Feld *calling-e164*.
- Zeile 5: Das Mapping *calling-e164 to calling-uri mt_teams2starface-a-uri* konvertiert eine konkrete anrufende Telefonnummer zu einer anrufenden SIP-URI.
- Zeile 6-8: Konkrete Telefonnummern werden eine SIP-URI (des jeweiligen STARFACE SIP-Accounts) übersetzt, so dass der Anruf von der STARFACE dem richtigen Endgeräteaccount zugeordnet werden kann. Die IP-Adresse der SIP-URI muss der IP-Adresse der STARFACE entsprechen, da die STARFACE eingehende Anrufe von Teams ansonsten nicht dem richtigen Endgeräte-SIP-Account zuordnen kann.
- Zeile 10-12: Das Mapping *called-e164 to called-e164 mt_teams2starface-b-internalCalls* wandelt von Teams signalisierte zwei- oder dreistellige Zielrufnummern (die von Teams um die Landesvorwahl ergänzt wurden in zwei- oder dreistellige Zielrufnummern ohne Landesvorwahl um. Dadurch lassen sich interne Teilnehmer der STARFACE mit zwei- oder dreistelligen internen Rufnummern erreichen.

3. Übersetzung von STARFACE SIP-Account-Namen in Teams-Telefonnummern

```

1 mapping-table called-uri to called-e164 mt_starface2teams-b-e164
2 map sip:(.+)+@(.+) to +4971234567890
3 map sip:user.01@.+ to +497123222
4 map sip:user.02@.+ to +497123223
5 map sip:user.03@.+ to +497123224

```

Erklärung:

- Zeile 1: Das Mapping *called-uri to called-e164* konvertiert eine konkrete angerufene SIP-URI zu einer angerufenen Telefonnummer.
- Zeile 2: Beispiel für ein Fallback-Mapping eines beliebigen SIP-Accounts zu einer bestimmten Rufnummer (z.B. für einen Abwurfplatz).
- Zeile 3-5: Konkrete SIP-Accounts werden anhand des Account-Namens in eine Telefonnummer übersetzt, so dass der Anruf dem richtigen Teams-User zugeordnet werden kann.

Nun haben wir die Grundlage für die Telefonie gelegt und die Richtungen gemappt. Damit das ganze erweiterbar ist, und für den Patton ausführbar wird, werden die einzelnen Mapping-Tables gegliedert und durch eine sogenannte Complex-Function für eine jeweiligen Anrufrichtungen zusammengefasst. Die Complex Funktionen werden der Reihe nach ausgeführt und passen die jeweiligen SIP Parameter an. Auch das konfigurieren wir am einfachsten mit dem CLI unter z.B: Putty:

4. Sammlung der Anpassungen für die jeweilige Gesprächsrichtung

```

1 complex-function cf_teams2starface
2 execute 1 mt_teams2starface-a-e164
3 execute 2 mt_teams2starface-a-uri
4 execute 3 mt_teams2starface-b-internalCalls
5
6 complex-function cf_starface2teams
7 execute 1 mt_starface2teams-b-e164

```

Erklärung: Complex-Functions sind Ansammlungen von Mapping-Funktionen, die der angegebenen Reihe nach ausgeführt werden und Anpassungen der SIP-Parameter vornehmen.

5. Routing Tabellen

Routingtabellen für die Weiterleitung von Anrufen zwischen STARFACE und Microsoft Phone System / Teams

```
1 routing-table called-e164 rt_from_teams
2 route default dest-interface if_sip_starface cf_teams2starface
3
4 routing-table called-e164 rt_from_starface
5 route default dest-service hg_microsoft-teams cf_starface2teams
```

Erklärung:

- Zeile 1-2: Die Routingtabelle *rt_from_teams* sendet alle Anrufe von Teams zum Interface *if_sip_starface* (dieses wird im folgenden Abschnitt beschrieben) und wendet die Complex-Function *cf_teams2starface* mit den darin enthaltenen Mappings an.
- Zeile 4-5: Die Routingtabelle *rt_from_starface* sendet alle Anrufe der STARFACE zur Hunting-Group *hg_microsoft-teams* (die der Reihe nach drei verschiedene georedundante Microsoft-Peers anspricht) und wendet die Complex-Function *cf_starface2teams* mit den darin enthaltenen Mappings an.

6. Interfaces und SIP-Gateways

Schnittstelle zu Microsoft Phone System / Teams

```
1 interface sip if_sip_microsoft-directrouting-primary
2   bind context sip-gateway gw_sip_wan_5062
3   route call dest-table rt_from_teams
4   remote sip.pstnhub.microsoft.com 5061
5   local sbc.meinefirma.de 5062
6   hold-method direction-attribute inactive
7   no call-transfer accept
8   privacy
9   use profile voip pf_voip_microsoft
10  srtp renegotiate-on-connect
11  penalty-box sip-option-trigger interval 60 timeout 60 force tls
12  session-timer 3600
13  trust remote
14  trust 52.114.0.0/16
15
16 interface sip if_sip_microsoft-directrouting-secondary
17   bind context sip-gateway gw_sip_wan_5062
18   route call dest-table rt_from_teams
19   remote sip2.pstnhub.microsoft.com 5061
20   local sbc.meinefirma.de 5062
21   hold-method direction-attribute inactive
22   no call-transfer accept
23   privacy
24   use profile voip pf_voip_microsoft
25   srtp renegotiate-on-connect
26   penalty-box sip-option-trigger interval 60 timeout 60 force tls
27   session-timer 3600
28   trust remote
29   trust 52.114.0.0/16
30
31 interface sip if_sip_microsoft-directrouting-tertiary
32   bind context sip-gateway gw_sip_wan_5062
33   route call dest-table rt_from_teams
34   remote sip3.pstnhub.microsoft.com 5061
35   local sbc.meinefirma.de 5062
36   hold-method direction-attribute inactive
37   no call-transfer accept
38   privacy
39   use profile voip pf_voip_microsoft
40   srtp renegotiate-on-connect
41   penalty-box sip-option-trigger interval 60 timeout 60 force tls
42   session-timer 3600
43   trust remote
```

```
44 trust 52.114.0.0/16
45
46 service hunt-group hg_microsoft-directrouting
47 timeout 3
48 drop-cause normal-unspecified
49 drop-cause no-circuit-channel-available
50 drop-cause network-out-of-order
51 drop-cause temporary-failure
52 drop-cause switching-equipment-congestion
53 drop-cause access-info-discarded
54 drop-cause circuit-channel-not-available
55 drop-cause resources-unavailable
56 route call 1 dest-interface if_sip_microsoft-directrouting-primary
57 route call 2 dest-interface if_sip_microsoft-directrouting-secondary
58 route call 3 dest-interface if_sip_microsoft-directrouting-tertiary
59
60 location-service ls_microsoft
61 domain 1 microsoft.com
62 domain 2 sip-du-a-eu.pstnhub.microsoft.com
63 domain 3 sip-du-a-us.pstnhub.microsoft.com
64 domain 4 sip-du-a-as.pstnhub.microsoft.com
65 domain 5 pstnhub.microsoft.com
66 domain 6 sip.pstnhub.microsoft.com
67 domain 7 sip2.pstnhub.microsoft.com
68 domain 8 sip3.pstnhub.microsoft.com
69
70 identity-group DEFAULT
71 user phone
72
73 authentication inbound
74 authenticate none
75
76 registration outbound
77 register none
78
79 call outbound
80 transport-protocol force tls
81
82 call inbound
83
84
85
86
87
```

Erklärung:

- Zeile 1: Primärer Microsoft Phone System/Direct Routing Peer.
- Zeile 2: Das Interface wird an das Gateway *gw_sip_wan_5062* gebunden.
- Zeile 3: Anrufe von Microsoft Phone System werden an die Routingtabelle *rt_from_teams* übergeben und dort in Richtung STARFACE geroutet.
- Zeile 4: FQDN und Portnummer des Microsoft Peers
- Zeile 5: Lokale Identität und Portnummer des SBCs
- Zeile 9: Im SIP-Contact-Header für ausgehende Anrufe den FQDN des SBCs setzen.
- Zeile 10: Zuvor konfiguriertes VoIP-Profil verwenden
- Zeile 12: In Intervallen von 60 Sekunden ein SIP-Options-Paket an Microsoft senden (zwingend)
- Zeile 17, 33: Sekundärer und Tertiärer Microsoft Phone System/Direct Routing Peer. Identische Konfiguration wie beim primären Peer; lediglich abweichende Remote-Adresse.
- Zeile 49: Hunting Group, die der Reihe nach die einzelnen Microsoft Peers anspricht (Hochverfügbarkeit); Timeout von 3 Sekunden, falls ein Peer nicht antwortet
- Zeile 63: Location Service, der Pakete von Microsoft von den angegebenen Domänen akzeptiert, "user=phone" der SIP-URI hinzufügt und als Transportprotokoll TLS erzwingt.

Schnittstelle zur STARFACE

```
1 interface sip if_sip_starface
2   bind context sip-gateway gw_sip_lan_5060
3   route call dest-table rt_from_starface
4   remote starface.meinefirma.de
5   hold-method direction-attribute sendonly
6   early-disconnect
7   no call-transfer accept
8   no call-transfer emit
9   address-complete-indication accept set
10  address-translation incoming-call calling-e164 from-header
11  address-translation incoming-call calling-uri from-header
12  address-translation incoming-call calling-name from-header
13  use profile voip pf_voip_starface
14  trust remote
15
16 authentication-service as_starface-sipaccounts
17   username user.01 password meingeheimessippasswort01
18   username user.02 password meingeheimessippasswort02
19   username user.03 password meingeheimessippasswort03
20
21 location-service ls_starface
22
23 identity-group teams
24
25 authentication outbound
26   authenticate 1 authentication-service as_starface-sipaccounts
27
28 authentication inbound
29   authenticate none
30
31 registration outbound
32   registrar starface.meinefirma.de
33   lifetime 180
34   register auto
35
36 call outbound
37   use profile voip pf_voip_starface
38
39 call inbound
40   use profile voip pf_voip_starface
41
42 identity user.01 inherits teams
43 identity user.02 inherits teams
44 identity user.03 inherits teams
```

SIP-GATEWAYS einrichten:

```
1 context sip-gateway GW_STARFACE_PBX
2   bind location-service ls_starface
3
4   interface GW_STARFACE_PBX
5     transport-protocol udp+tcp 5060
6     no transport-protocol tls
7     bind ipaddress ROUTER LAN LAN
8
9 context sip-gateway GW_STARFACE_PBX
10  no answer-untrusted-hosts
11  no shutdown
12
13 context sip-gateway GW_TEAMS
14  use profile tls pf_tls_default
15  bind location-service ls_microsoft
16
17  interface IF_GW_TEAMS
18    no transport-protocol udp+tcp
19    transport-protocol tls 5061
20    bind ipaddress ROUTER WAN WAN
21    spoofed contact-header manual sbc.MEINEFIRMENDOMAIN.org port 5061
22    spoofed via-header manual sbc.MEINEFIRMENDOMAIN.org port 5061
23
24 context sip-gateway GW_TEAMS
25  no answer-untrusted-hosts
26  connection-reuse
27  no shutdown
```

Patton: IP-Router und physikalische Netzwerkport-Konfiguration

IP Router Konfiguration:

```
1 context ip ROUTER
2
3 interface WAN
4  ipaddress WAN 213.123.123.123/25
5  use profile acl in 1 ACL_WAN_IN_DENY
6  use profile acl in 2 STATEFUL_ACL
7  use profile acl out 1 ACL_WAN_PROTOCOLS
8  use profile acl out 2 STATEFUL_ACL
9  use profile napt NATP_WAN WAN
10 tcp adjust-mss rx mtu
11 tcp adjust-mss tx mtu
12
13 interface LAN
14  ipaddress LAN 10.1.10.180/16
15  use profile acl in1 ACL_LAN_IN_DENY
17  tcp adjust-mss rx mtu
18  tcp adjust-mss tx mtu
```

Erklärung

- Zeile 3 und 13 wir weisen den Interfaces des Patton die WAN und LAN Adressen zu

Physikalische Portkonfiguration

```
1 port ethernet 0 0
2  bind interface ROUTER WAN
3  no shutdown
4
5 port ethernet 0 1
6  bind interface ROUTER LAN
7  no shutdown
```

Erklärung

- Wir weisen die unter context IP Router erstellten IPs den Physikalischen Adressen zu.

Microsoft: MS-TEAMS Vorbereiten

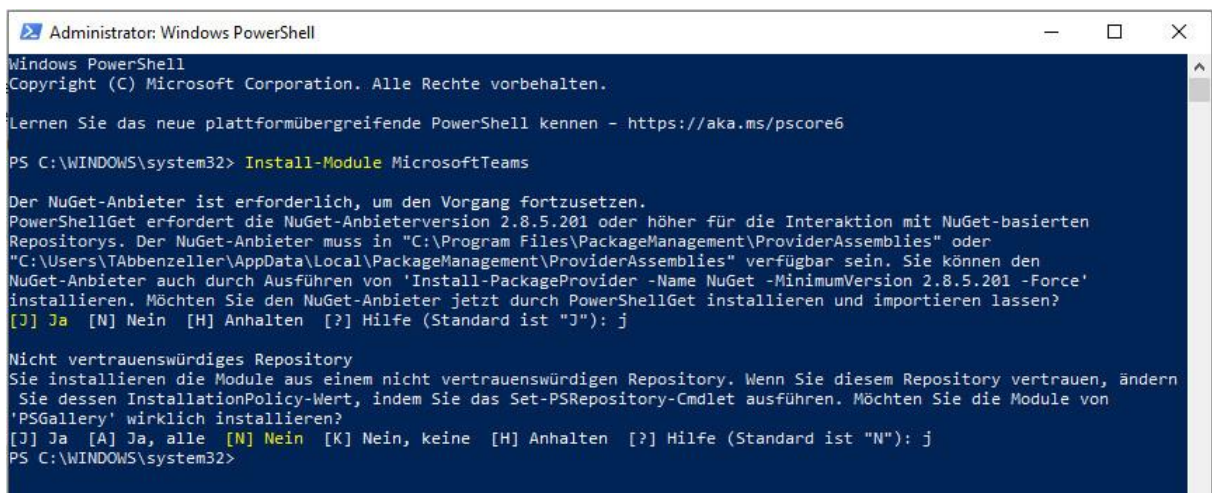
- Voraussetzung: Zugangsdaten als O365 Administrator
- MS-Phone Lizenzen

Zuerst Installieren wir uns die Microsoft Powershell Umgebung. Dazu öffnen wir die Powershell als Administrator:

Dann geben wir folgenden Befehl ein:

```
1 Install-Module MicrosoftTeams
2
3 Exit
```

Dann öffnen wir erneut die Powershell als Administrator



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

Lernen Sie das neue plattformübergreifende PowerShell kennen - https://aka.ms/pscore6

PS C:\WINDOWS\system32> Install-Module MicrosoftTeams

Der NuGet-Anbieter ist erforderlich, um den Vorgang fortzusetzen.
PowerShellGet erfordert die NuGet-Anbieterversion 2.8.5.201 oder höher für die Interaktion mit NuGet-basierten
Repositorys. Der NuGet-Anbieter muss in "C:\Program Files\PackageManagement\ProviderAssemblies" oder
"C:\Users\TAbbenzeller\AppData\Local\PackageManagement\ProviderAssemblies" verfügbar sein. Sie können den
NuGet-Anbieter auch durch Ausführen von 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'
installieren. Möchten Sie den NuGet-Anbieter jetzt durch PowerShellGet installieren und importieren lassen?
[J] Ja [N] Nein [H] Anhalten [?] Hilfe (Standard ist "J"): j

Nicht vertrauenswürdige Repository
Sie installieren die Module aus einem nicht vertrauenswürdigen Repository. Wenn Sie diesem Repository vertrauen, ändern
Sie dessen InstallationPolicy-Wert, indem Sie das Set-PSRepository-Cmdlet ausführen. Möchten Sie die Module von
'PSGallery' wirklich installieren?
[J] Ja [A] Ja, alle [N] Nein [K] Nein, keine [H] Anhalten [?] Hilfe (Standard ist "N"): j
PS C:\WINDOWS\system32>
```

Danach müssen wir den Skype Online Connection installieren.

Ich empfehle dies in einem Notepad vorzubereiten und dann mit Copy Paste hinzuzufügen

```
Import-Module SkypeOnlineConnector
```

```
$userCredential = Get-Credential -Credential MEINACCOUNT@Domain.onmicrosoft.com
```

```
$sfbSession = New-CsOnlineSession -Credential $userCredential -OverrideAdminDomain "mydomain.onmicrosoft.com"
```

```
Import-PSSession $sfbSession
```

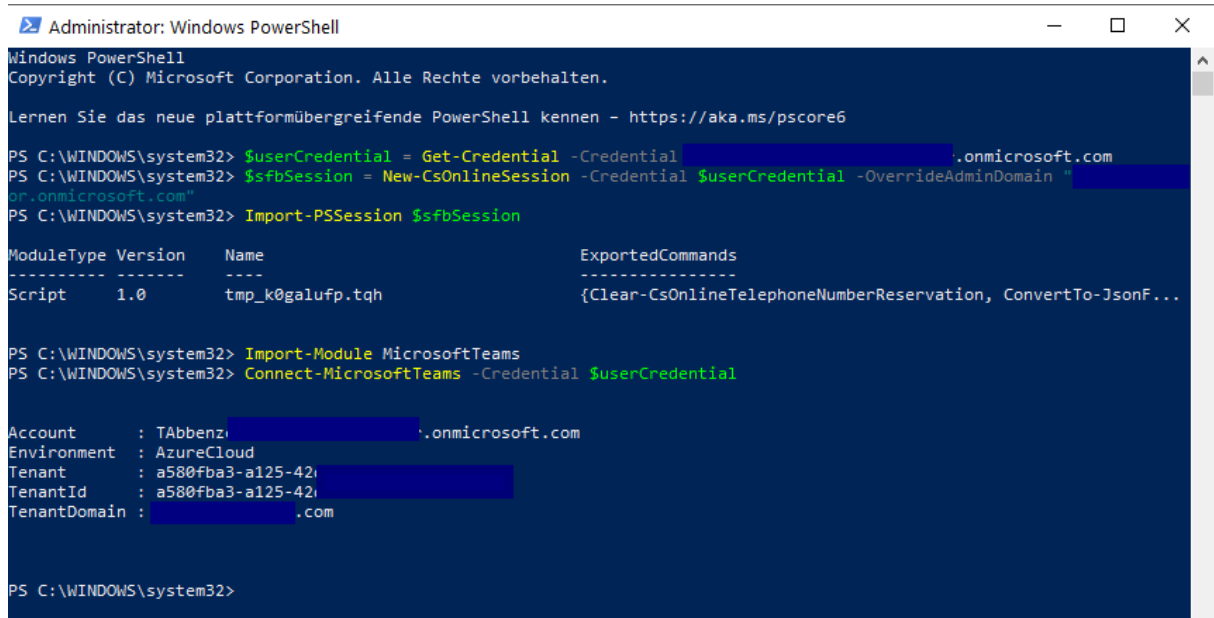
```
Enable-CsOnlineSessionForReconnection
```

```
Import-Module MicrosoftTeams
```

```
Connect-MicrosoftTeams -Credential $userCredential
```

Je nach Powershellversion genügt auch folgendes:

```
$userCredential = Get-Credential -Credential MEINACCOUNT@DOnmain.onmicrosoft.com
$sfbSession = New-CsOnlineSession -Credential $userCredential -OverrideAdminDomain
"MEINEDOMAIN.onmicrosoft.com"
Import-PSSession $sfbSession
Import-Module MicrosoftTeams
Connect-MicrosoftTeams -Credential $userCredential
```



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

Lernen Sie das neue plattformübergreifende PowerShell kennen - https://aka.ms/pscore6

PS C:\WINDOWS\system32> $userCredential = Get-Credential -Credential [REDACTED].onmicrosoft.com
PS C:\WINDOWS\system32> $sfbSession = New-CsOnlineSession -Credential $userCredential -OverrideAdminDomain "[REDACTED].onmicrosoft.com"
PS C:\WINDOWS\system32> Import-PSSession $sfbSession

ModuleType Version Name ExportedCommands
-----
Script 1.0 tmp_k0galuFp.tqh {Clear-CsOnlineTelephoneNumberReservation, ConvertTo-JsonF...

PS C:\WINDOWS\system32> Import-Module MicrosoftTeams
PS C:\WINDOWS\system32> Connect-MicrosoftTeams -Credential $userCredential

Account : Tabbenzi [REDACTED].onmicrosoft.com
Environment : AzureCloud
Tenant : a580fba3-a125-42[REDACTED]
TenantId : a580fba3-a125-42[REDACTED]
TenantDomain : [REDACTED].com

PS C:\WINDOWS\system32>
```

Dann können wir loslegen.

 Microsoft: SBC anlegen

Wir loggen wie eben gezeigt in der Powershell und Parallel im Browser im O365 Portal ein und legen den SBC an.

Dazu gehen wir in Office365 auf die TEAMS Administration und legen den SBC an.

- Wichtig ist, dass wir vorher den DNS-Namen rechtzeitig auf dem DNS angelegt haben, so dass er auflösbar ist.
1. Wir wechseln in der Navigationsleiste zu VOIP -> Direct Routing und klicken SBCs
 2. Wir fügen einen neuen SBC hinzu
 3. Wir geben den Full Qualified Domain Name (FQDN) für unseren SBC an, also z.B: SBC.MEINEDOMAIN.ORG – ACHTUNG: dies muss wie bereits angesprochen im DNS auffindbar sein und WICHTIG: das Zertifikat muss bereits auf dem Patton SBC angelegt sein.

Direct Routing

Mit Direct Routing können Sie sich mit einem unterstützten Session Border Controller (SBC) mit dem Microsoft-Telefonsystem verbinden, um die Funktion für Sprachanrufe zu aktivieren. Sie können Informationen über Ihre SBCs, Ihre VoIP-Routen und Ihre PSTN-Verwendungseinträge hinzufügen, bearbeiten und anzeigen. Weitere Informationen

Direct Routing - Übersicht

Gesamt SBCs: 0 | VoIP-Routen: 1 | SBCs mit PSTN-Verträgen: 0

1. Wechseln Sie in der linken Navigationsleiste zu VoIP > Direct Routing, und klicken Sie dann auf die Registerkarte SBCS.

2. Klicken Sie auf Hinzufügen.

3. Geben Sie einen FQDN für den SBC ein.

4. Stellen Sie sicher, dass der Domänenname-Teil des FQDN einer Domäne entspricht, die in Ihrem Mandanten registriert ist, und konfigurieren Sie die folgenden Einstellungen für den SBC basierend auf den Anforderungen Ihrer Organisation. Details zu den

Konfigurieren Sie die folgenden Einstellungen für den SBC basierend auf den Anforderungen Ihrer Organisation. Details zu den

SBC	Netzwerkeffizienz	Durchschnittliche Anrufdauer	TLS-Verbindungsstatus	Status der SIP OPTIONS	Kapazität für gleichzeitige Anrufe	Aktiviert
+	Hinzufügen	Bearbeiten	Löschen	Elemente		
✓	SBC					
✓	sbcs.netzwerkkontor.com	0% (0)	0 Sek. (0)	Aktiv	Aktiv	Innerhalb der Grenzen

Wir haben nachgesehen, aber es sind noch keine Daten verfügbar.

Wenn der SBC dann angelegt ist, erscheint er nach ein paar Minuten als aktiv.

SBCs | VoIP-Routen

+ Hinzufügen | Bearbeiten | Löschen | Elemente

✓	SBC	Netzwerkeffizienz	Durchschnittliche Anrufdauer	TLS-Verbindungsstatus	Status der SIP OPTIONS	Kapazität für gleichzeitige Anrufe	Aktiviert
✓	sbcs.netzwerkkontor.com	0% (0)	0 Sek. (0)	Aktiv	Aktiv	Innerhalb der Grenzen	Ein

sbc.netzerkkontor.com

DE

Status
Inaktiv

SIP signaling port
5061

SIP Options status
Aktiv

Network effectiveness (Calls)
0% (0)

TLS connectivity status
Aktiv

Average call duration (Calls)
0 Sek. (0)

Concurrent calls capacity
0 % (0/8)

Das der SBC ein Ausrufezeichen hat stört uns nicht. Wir haben ja auch noch nicht darüber telefoniert. Wichtig ist aber, dass er **AKTIV** angezeigt wird. Sofern ein anderer Port als 5061 auf dem Patton festgelegt wurde, ist dieser auch hier entsprechend zu konfigurieren.

Auch das können wir natürlich einfach mit einem Powershell cmdlet erledigen – hier im Beispiel legen wir gleich 2 SBCs an:

```
New-CsOnlinePSTNGateway -Fqdn sbc1.MEINEDOMAIN.org -SipSignallingPort 5061 -ForwardCallHistory $True -MaxConcurrentSessions 200 -Enabled $True
```

```
New-CsOnlinePSTNGateway -Fqdn sbc2.MEINEDOMAIN.org -SipSignallingPort 5061 -ForwardCallHistory $True -MaxConcurrentSessions 200 -Enabled $True
```

```
Set-CsOnlinePstnUsage -Identity Global -usage @{Add="PSTN_Usage_1"}
```

```
Set-CsOnlinePstnUsage -Identity Global -usage @{Add="PSTN_Usage_2"}
```

ACHTUNG – Nachdem das konfiguriert wurde, den obligatorischen IT-Kaffee trinken. Es kann bis zu 15 Minuten dauern bis das bei Microsoft repliziert wurde und damit aktiv ist. Es kann durchaus vorkommen, dass man eine Powershell Fehlermeldung erhält, wenn der vorherige Schritt noch nicht repliziert wurde.

Dann weisen wir o365 die SBC Leitung PSTN zu:

Das passiert in der SBC Directroutingseite unter VoIP Routen:

	Hinzufügen	Bearbeiten	Nach oben	Nach unten	Löschen	Elemente	Suche
<input checked="" type="checkbox"/>	Priorität	VoIP-Route	Beschreibung	Gewähltes Nummernmuster	PSTN-Verwendung	Registrierte SBCs	
1		Route_SBC1		.*	PSTN_Usage_1	sbc.netzerkkontor.com	
2		LocalRoute		^\{+1[0-9]{10}\}\$		sbc.netzerkkontor.com	

Oder einfacher wieder mit der Powershell:

```
Set-CsOnlinePstnUsage -Identity Global -usage @{Add="PSTN_Usage_1"}
```

```
Set-CsOnlinePstnUsage -Identity Global -usage @{Add="PSTN_Usage_2"}
```

```
New-CsOnlineVoiceRoute -Identity "Route_SBC1" -NumberPattern ".*" -OnlinePstnGatewayList sbc1.MEINEDOMAIN.org -Priority 1 -OnlinePstnUsages "PSTN_Usage_1"
```


Dann brauchen wir eine VoIP Routing Richtlinie

The screenshot shows the 'VoIP-Routingrichtlinien' (VoIP Routing Policies) page in the Microsoft Teams admin center. The left sidebar contains navigation options like Dashboard, Teams, Geräte, Standorte, Benutzer, Besprechungen, Nachrichtenrichtlinien, Teams-Apps, and VoIP. The main content area is titled 'VoIP-Routingrichtlinien' and includes a descriptive paragraph: 'Die VoIP-Routingrichtlinie wird unten über PSTN-Verwendungseinträge mit einer VoIP-Route verknüpft. Sie können vorhandene PSTN-Verwendungseinträge hinzufügen, die Reihenfolge ändern, in der die Verwendungen verarbeitet werden, und die VoIP-Routingrichtlinie Benutzern zuweisen. Weitere Informationen'. Below this are two summary cards: 'VoIP-Routingrichtlinien-Zusammenfassung' showing 1 Standardrichtlinie and 1 Benutzerdefinierte Richtlinie, and 'Benutzerstatistiken' showing 3 Benutzerdefinierte Richtlinien and 3 Standardrichtlinien. At the bottom, there is a table with columns for Name, Beschreibung, and PSTN-Verwendungseinträge. The table contains two entries: 'Global (organisationsweiter Sta)' and 'Routing_Policy_1' linked to 'PSTN_Usage_1'. Action buttons like 'Hinzufügen', 'Bearbeiten', 'Duplizieren', 'Löschen', and 'Benutzer verwalten' are visible above the table.

Oder wieder simpel mit der Powershell

[New-CsOnlineVoiceRoutingPolicy "Routing_Policy_1" -OnlinePstnUsages "PSTN_Usage_1"](#)

ACHTUNG – Nachdem das konfiguriert wurde, den obligatorischen IT-Kaffee trinken. Es kann bis zu 15 Minuten dauern bis das bei Microsoft repliziert wurde and damit aktiv ist. Es kann durchaus vorkommen das man eine Powershell Fehlermeldung erhält, wenn der vorherige Schritt noch nicht repliziert wurde.

O365 User zuweisen

Sobald die vorherigen Schritte konfiguriert sind, können wir Benutzer Rufnummern zuweisen. Dies muss logischerweise mit den Rufnummern der STARFAE und des Pattons übereinstimmen.

Das geht am besten mit der Powershell. Ich habe keine guten Erfahrungen mit dem Browser an dieser Stelle gemacht, daher nur der Powershellcommand.

WICHTIS IST: der Benutzer benötigt vorher die Phonesystemlizenz zugewiesen.

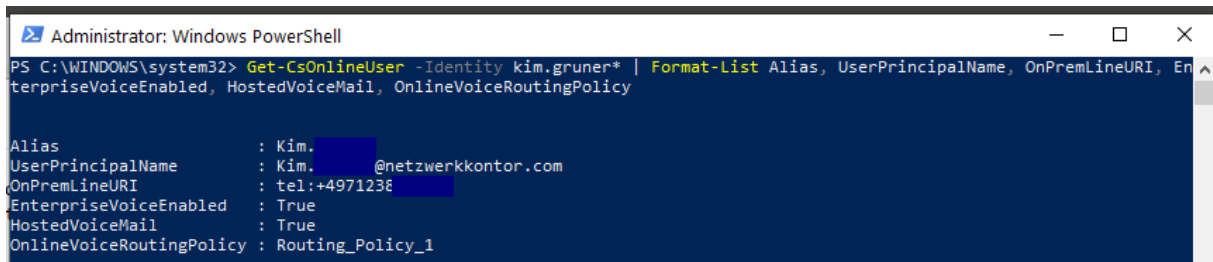
```
Set-CsUser -Identity "Mein.Benutzer@MEINEOMAIN.org" -OnPremLineURI tel: +497123123456 -EnterpriseVoiceEnabled $true -HostedVoiceMail $true
```

```
Grant-CsOnlineVoiceRoutingPolicy -Identity " Mein.Benutzer@MEINEOMAIN.org " -PolicyName "Routing_Policy_1"
```

Wie kann ich feststellen, ob das funktioniert hat?

Cmdlet output examples of `Get-CsOnlineUser` / configuration status with assigned routing policy:

Bsp: `Get-CsOnlineUser -Identity MeinBenutzer* | Format-List Alias, UserPrincipalName, OnPremLineURI, EnterpriseVoiceEnabled, HostedVoiceMail, OnlineVoiceRoutingPolicy`



```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Get-CsOnlineUser -Identity kim.gruner* | Format-List Alias, UserPrincipalName, OnPremLineURI, EnterpriseVoiceEnabled, HostedVoiceMail, OnlineVoiceRoutingPolicy

Alias                : Kim.
UserPrincipalName    : Kim. @netzwerkkontor.com
OnPremLineURI        : tel:+4971238
EnterpriseVoiceEnabled : True
HostedVoiceMail       : True
OnlineVoiceRoutingPolicy : Routing_Policy_1
```

Dies ist für jeden einzelnen Benutzer durchzuführen.

STARFACE Konfiguration

Damit nun die STARFACE mit dem Patton und somit mit Teams spricht, müssen SIP Accounts (Telefone) angelegt werden. Diese müssen den Benutzern zugewiesen werden.

Der SBC registriert dann diese Telefone und dadurch ist die Kommunikation möglich. Teams ist also ein Telefon auf der STARFACE und klingelt parallel zu den anderen Geräten, bzw. wird dadurch ein Teams Call zum PSTN (Providernetz) möglich.

Technische Voraussetzungen & Vorbereitende Maßnahmen

Für die Umsetzung der Anbindung einer STARFACE an Microsoft Teams sind folgende Voraussetzungen bzw. Anforderungen zu erfüllen:

- STARFACE **Version 6.7.3.11 oder neuer**
- STARFACE **Lizenz** "MS Teams Integration" sowie "UCC-Client Premium" für jeden Teams-Benutzer
- Unbeschränkte **Erreichbarkeit externer HTTPS-Dienste** (TCP/443; kein HTTPS-Proxy!):
 - login.microsoftonline.com
 - service-cloud-connector.fluxpunkt.de
 - omni-client.fluxpunkt.de

Systemstatus		Liste der eingerichteten Telefone				
Benutzer	Einstellungen	Konfigurierte Endgeräte	ID-Anzeige	Sicherheit	IP-Beschränkungen	
Gruppen	teamspatton01		Suchen	Zeilen: 10	Seite 1/1	
Telefone	Gerätetyp	Gerätename	IP	Zugeordnete Benut...	Aktiv	
Module	✓ Standard Sip	TeamsPatton01	10.1.10.180	Abbenzeller, Thor...	✓	 

STARFACE MODUL INSTALLIEREN UND KONFIGURIEREN

[Teams Integration für STARFACE - Fluxpunkt Knowledge Base - Fluxpunkt GmbH](#)

Technische Voraussetzungen & Vorbereitende Maßnahmen

Für die Installation des STARFACE Moduls sind folgende Voraussetzungen bzw. Anforderungen zu erfüllen:

- STARFACE **Version 6.7.3.11 oder neuer**
- STARFACE **Lizenz** "MS Teams Integration" sowie "UCC-Client Premium" für jeden Teams-Benutzer
- Unbeschränkte **Erreichbarkeit externer HTTPS-Dienste** (TCP/443; kein HTTPS-Proxy!):
 - login.microsoftonline.com
 - service-cloud-connector.fluxpunkt.de
 - omni-client.fluxpunkt.de

1. Lizenzierung

Es gibt zwei Möglichkeiten, STARFACE Benutzer für die Teams App zu lizenzieren.

Mit **User-Assigned-Licenses** von STARFACE kann einzelnen Benutzern das Recht für die Teams Integration zugewiesen werden. Die Installation der Lizenzen erfolgt über den üblichen Weg, STARFACE-eigene Lizenzen in die Anlage einzutragen (STARFACE Weboberfläche → Admin → Server → Lizenzen).

Bei **Floating-Licenses** von Fluxpunkt wird die Anzahl der Nutzer, die gleichzeitig die Teams App verwenden können, lizenziert. Wenn sich ein Benutzer abmeldet, kann sich stattdessen ein anderer Benutzer über die Teams App mit der STARFACE verbinden.

Ein Lizenzschlüssel von Fluxpunkt muss im Tab Lizenzen der Modulkonfiguration in das entsprechende Feld eingetragen und anschließend der orangefarbenen Speichern-Button geklickt werden. Daraufhin erscheinen Details zum eingetragenen Lizenzschlüssel.

Konfiguration

Systemstatus

Benutzer

Gruppen

Telefone

Module

Voicemail

Konferenz

Adressbuch

Rufnummern

Leitungen

Routing

Server

Auswertung

Anlagenverbund

Sicherheit

Erweiterte Einstellungen

Modul-Konfiguration: APIs Connector

Allgemein **Module settings**

Grundeinstellungen Log **Lizenzen**

Lizenz Teams Integration für STARFACE

Modullizenz ist gültig.

Modullizenzschlüssel

XX

Lizenzdetails:

Server license key: aaaaabbbbccccddddd

Module license key:
XX

Module license key is valid

Licensed users: 20

Expiration date: 2030-11-24

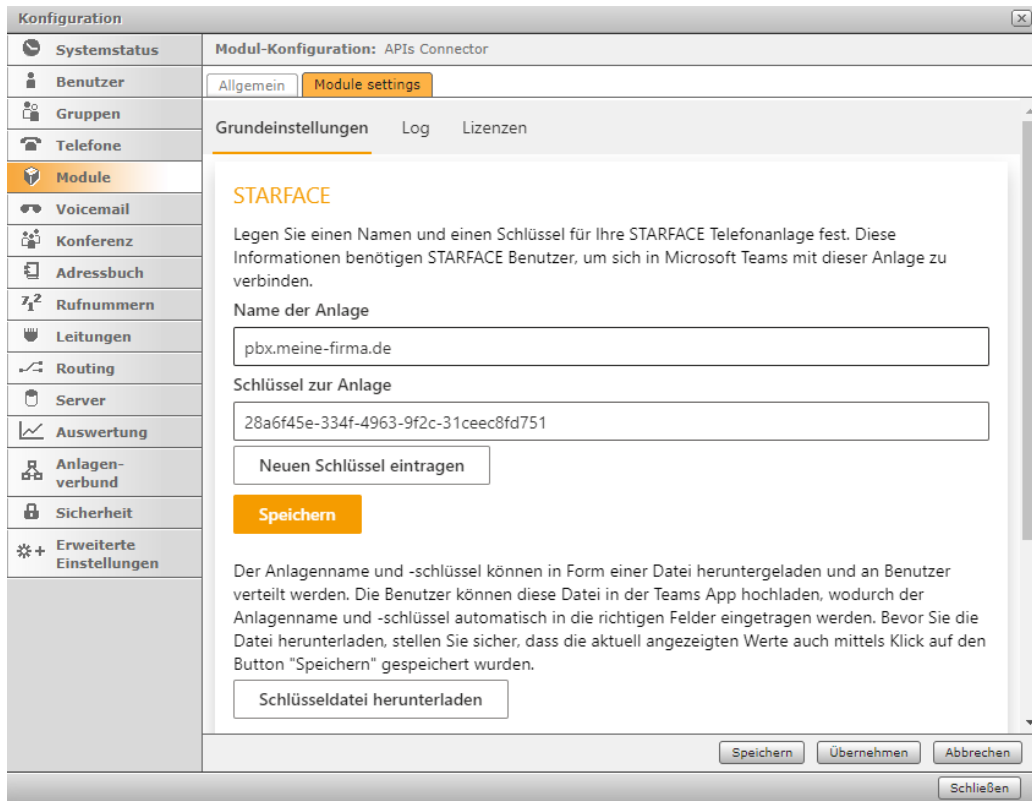
Lizenz übernehmen

Speichern Übernehmen Abbrechen

Schließen

2. Grundeinstellungen

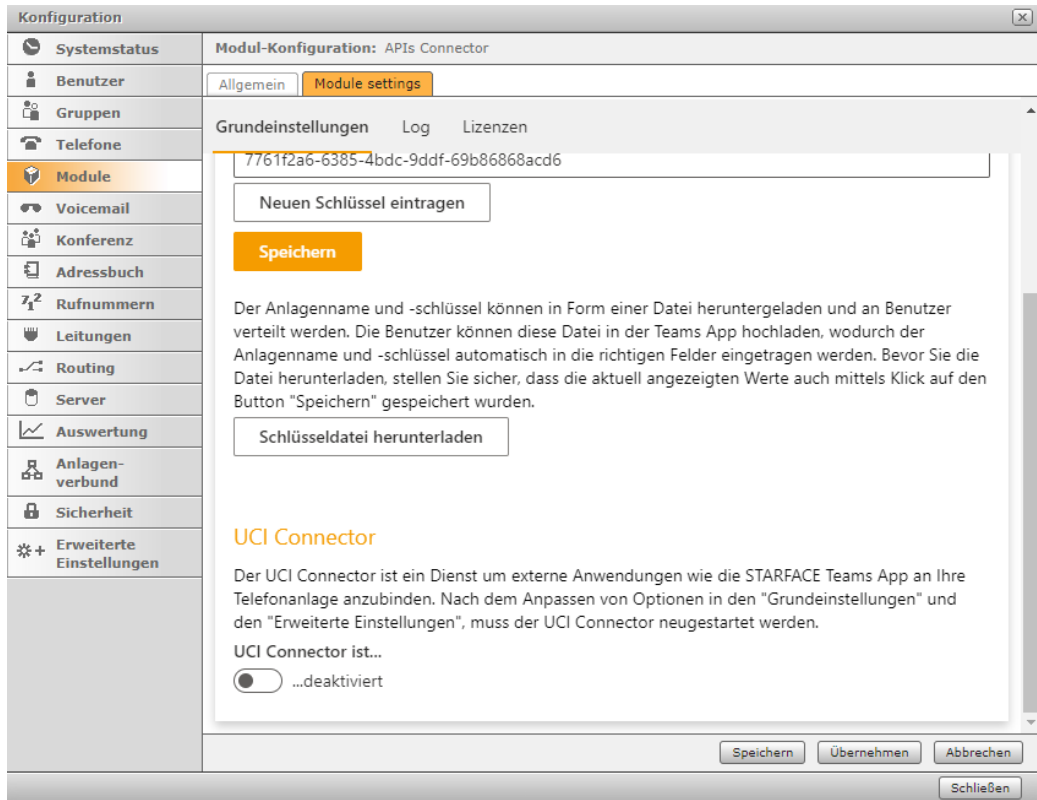
Im Tab Grundeinstellungen muss nun ein STARFACE Name und ein Schlüssel vergeben werden. Der Schlüssel kann nicht von Hand eingetragen werden, sondern muss vom System erzeugt werden. Klicken Sie dazu den Generieren-Button unter dem Eingabefeld.



Den STARFACE Name und Schlüssel müssen Benutzer später in der Teams App eintragen, um sich mit Ihrer STARFACE verbinden zu können. Sie können die Daten entweder über Kommunikationswege wie Teams-Chat oder E-Mail weitergeben oder Sie laden im Modul die sogenannte Schlüsseldatei herunter und senden diese an Ihre Benutzer. Diese kann in Teams verwendet werden, um STARFACE Name und Schlüssel automatisch zu übernehmen.

3. UCI Connector starten

Damit sich Teams Benutzer mit Ihrer STARFACE verbinden können, muss der UCI Connector gestartet werden. Klicken Sie dazu auf den Toggle im unteren Bereich des Tabs Grundeinstellungen. Nun erreichen Teams Benutzer Ihre Anlage über den zuletzt gespeicherten STARFACE Name und Schlüssel, und können sich anschließend mit ihren STARFACE Zugangsdaten anmelden.



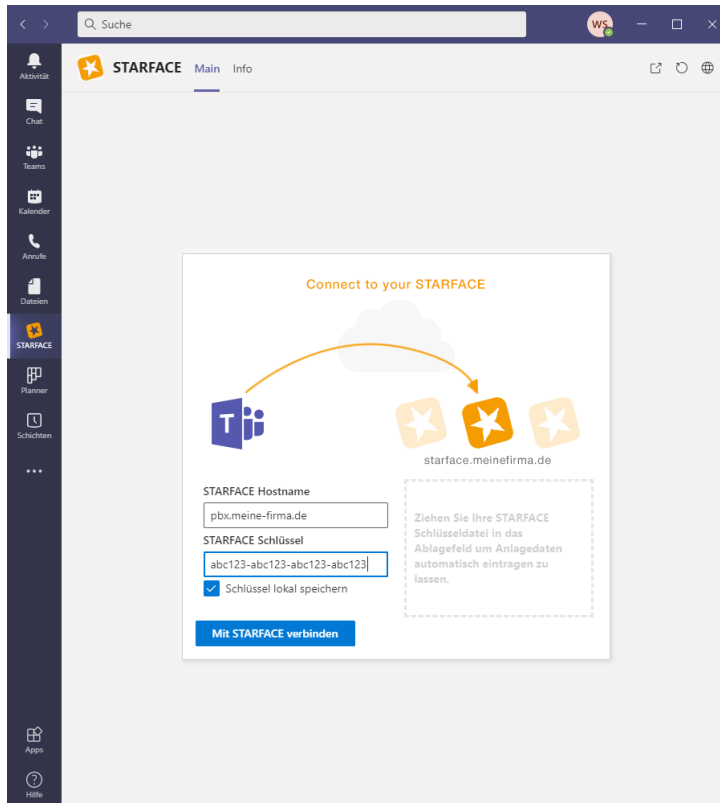
Installation Teams App

Laden Sie eine Teams App Version aus unserem Wiki herunter ([Teams Integration for STARFACE](#)), die kompatibel mit der eingesetzten STARFACE Modulversion ist. Eine Anleitung zur Installation der App-Datei in Teams finden Sie unter <https://docs.microsoft.com/de-de/microsoftteams/platform/concepts/deploy-and-publish/apps-upload>.

Eine Verteilung der Teams App über den Teams App "Store" ist in Planung.

1. Verbindung zu Ihrer STARFACE

Wählen Sie Ihre STARFACE, indem Sie den STARFACE Namen und Schlüssel aus Ihrer Modulkonfiguration eintragen oder die heruntergeladene Schlüsseldatei in das hellgraue Drag-and-Drop Feld ziehen.



2. Anmeldung an Ihrer STARFACE

Melden Sie sich nun mit Ihren STARFACE Zugangsdaten an

