

# Dokumentation: Teams Integration for STARFACE

## Übersicht Installation & Konfiguration

1

**Vorbereitende Maßnahmen** - Technische Voraussetzungen

2

**Microsoft Phone System / Teams** – Konfiguration

3

**Die Verbindung zwischen STARFACE und Teams** – Konfiguration Patton Session Border Controller (SBC)

4

**STARFACE** – Teams Modul/App-Integration und SIP-Interkonnektivität

- [1. STARFACE Konfiguration](#)
- [2. Microsoft Phone System Konfiguration](#)
- [3. Patton SBC Konfiguration](#)
- [4. STARFACE Modul und Teams App](#)

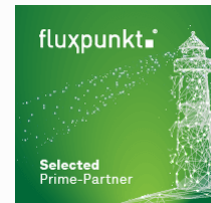
## Inhalt

- [Inhalt](#)
- [Vorwort](#)
- [Technische Voraussetzungen & Vorbereitende Maßnahmen](#)
- [Telefone \(SIP-Accounts\)](#)

## Vorwort

STARFACE-seitig muss je Teams-Benutzer ein SIP-Account (Telefonie-Endgerät) angelegt werden. Dieses Telefonie-Endgerät muß wiederum dem jeweiligen STARFACE-Benutzer zugewiesen werden.

Der SBC registriert sich an diesen SIP-Accounts und kann so die Kommunikation zwischen dem STARFACE-User und dessen Teams-Umgebung herstellen. Teams wird so zum "Endgerät" einer STARFACE, kann parallel zu bestehenden Endgeräten mitklingeln und nach Extern telefonieren.



Für die Umsetzung der Teams Integrationen empfehlen wir Ihnen, ausgewählte **Integrationspartner** auszuwählen, die über das entsprechende Know-How im Bereich Teams, STARFACE und Patton verfügen.

Von Fluxpunkt wurde die folgenden "Leuchtturmpartner" ausgewählt, um andere STARFACE-Partner und Endkunden bei der Integration zu unterstützen:

- [EDV-BV GmbH](#)
- [GDS GmbH](#)
- [Kronshage IT](#)
- [Luithle & Luithle GmbH](#)
- [Netzwerkkontor GmbH & Co. KG](#)
- [SMEA IT Services GmbH](#)
- [STARFACE GmbH](#)
- [swissnet telecommunication ag](#)

Alphabetische Reihenfolge ohne Wertung

## 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

## Telefone (SIP-Accounts)

Im Bereich der STARFACE-Administration muß als vorbereitende Maßnahme je Teams-Benutzer ein SIP-Endgerät angelegt werden. Als Gerätetyp kann "Standard SIP" ausgewählt werden.

Wir empfehlen, den Gerätenamen entsprechend der Benutzeremailadresse zu erzeugen: beispielsweise würde aus [max.mustermann@musterfirma.de](mailto:max.mustermann@musterfirma.de) der Geräte Name "max.mustermann" (der Benutzer, innerhalb der Domäne Musterfirma.de). Dieser Empfehlung liegt die Idee zugrunde, dass ein SIP-Konto, dessen Name dem Namensbestandteil der Emailadresse entspricht, so leicht einem Teams-User in der Microsoft-Umgebung zugeordnet werden kann.

Konfiguration						
Systemstatus	Liste der eingerichteten Telefone					
Benutzer	Einstellungen Konfigurierte Endgeräte ID-Anzeige Sicherheit IP-Beschränkungen					
Gruppen	<input type="text"/> Suchen           Zeilen: 10           << < Seite 1/2 > >>					
Telefone						
Module						
Voicemail						
Konferenz						
	Gerätetyp	Gerätename	IP	Zugeordnete Benutzer	Aktiv	
	✓ Microsoft Teams	user.01	10.108.2.250	Stephan, Wilhelm	✓	
	✓ Microsoft Teams	user.02	10.108.2.250	Wagner, Robert	✓	
	✓ Microsoft Teams	user.03	10.108.2.250	Wolf, Fabian	✓	

Bitte notieren Sie sich die Gerätenamen und SIP-Kennwörter, sowie deren Zuordnung zu einem STARFACE-/Teams-Benutzer (siehe Beispieltabelle). Diese Daten werden für die Einrichtung des SBC in einem späteren Konfigurationsschritt benötigt. Ihnen sollte nun beispielhaft die folgende Liste vorliegen:

Benutzer	Emailadresse	Telefonnummer intern	Telefonnummer extern	SIP-Konto Geräte Name	SIP-Konto Kennwort
Max Mustermann	max.mustermann@musterfirma.de	10	0049 12 12345-10	max.mustermann	kebp:-odInJpXGR
Marianne Musterfrau	marianne.musterfrau@musterfirma.de	20	0049 12 12345-20	marianne.musterfrau	LYi\$&enlubZ&JfeM

Nachdem die SIP-Geräte angelegt wurden, müssen diese dem zugehörigen STARFACE-Benutzer zugeordnet werden. Eine Anleitung finden Sie in der [STARFACE Knowledge Base](#).

Für die Konfiguration von Microsoft Phone System und der Anbindung von Kunden-SBCs ist die Microsoft Dokumentation zu Direct Routing einschlägig: <https://docs.microsoft.com/de-de/microsoftteams/direct-routing-landing-page>

## Inhalt

- Inhalt
- Vorwort
- Technische Voraussetzungen & Vorbereitende Maßnahmen
- Lizenzierung
- TLS Profile
- VoIP Profile
- Mapping Tabellen
- Routing Tabellen
- Interfaces und SIP-Gateways
- IP-Router und physikalische Netzwerkport-Konfiguration

## Vorwort

Das vorliegende Dokument richtet sich an Integrationspartner, die einen Patton SmartNode für die Anbindung der STARFACE an Microsoft Teams einsetzen und für den Kunden betreiben oder bereitstellen möchten.

Beispielhaft werden folgende Annahmen getroffen:

1. STARFACE IP-Adresse: 10.108.2.100
2. STARFACE FQDN: starface.meinefirma.de

### 3. Benutzerdaten:

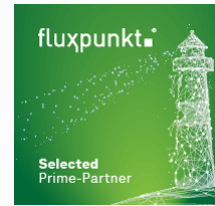
	Rufnummer Extern	Rufnummer Intern	Telefon Benutzername	Telefon Kennwort
Benutzer 1	+497123222	222	user.01	meingeheimessippasswort01
Benutzer 2	+497123223	223	user.02	meingeheimessippasswort02
Benutzer 3	+497123224	224	user.03	meingeheimessippasswort03

4. SBC Externes Interface FQDN/Protokoll/Port: 123.123.123.sbc.meinefirma.de/TLS/5062 (eth01)

5. SBC Internes Interface FQDN/Protokoll/Port: 192.168.1.1/UDP+TCP/5060 (eth00)

Die konkrete Konfiguration des Patton SmartNode SBC ist stark projektabhängig. Die vorliegende Dokumentation dient daher nur als Sammlung relevanter Konfigurationsbestandteile, die von einem Integrationspartner auf die konkrete Kundenumgebung angepasst werden müssen. Fluxpunkt erbringt **keine** Unterstützungsleistungen gegenüber Endkunden oder STARFACE-Partnern, die nicht ausgewählter Integrationspartner sind.

Basis der vorliegenden Konfigurationsbestandteile ist die von Patton mit Microsoft durchgeführte Zertifizierung von SBCs für Microsoft Teams mit Firmware Trinity 3.18.1 (Stand November 2020).




Für die Umsetzung der Teams Integration empfehlen wir Ihnen, ausgewählte **Integrationspartner** auszuwählen, die über das entsprechende Know-How im Bereich Teams, STARFACE und Patton verfügen.

Von Fluxpunkt wurde die folgenden "Leuchtturmpartner" ausgewählt, um andere STARFACE-Partner und Endkunden bei der Integration zu unterstützen:

- EDV-BV GmbH
- GDS GmbH
- Kronshage IT
- Luthle & Luthle GmbH
- Netzwerkkontor GmbH & Co. KG
- SMEA IT Services GmbH
- STARFACE GmbH
- swissnet telecommunication ag

Alphabetische Reihenfolge ohne Wertung

 [Weitere Informationen und Handbücher von Patton](#)

## Technische Voraussetzungen & Vorbereitende Maßnahmen

Für die Umsetzung der Anbindung einer STARFACE an Microsoft Teams mit Hilfe eines Patton SmartNodes sind folgende Voraussetzungen bzw. Anforderungen zu erfüllen:

- Patton SmartNode SBC (oder IAD oder Gateway) mit **Trinity-Firmware 3.18.1 oder neuer**; bevorzugt **SN5500, SN5600 oder Virtual SmartNode mit Teams-Lizenzen**.
- **Öffentliche IP-Adresse** für den SBC (DNAT-/Portforwarding-Szenarien werden nicht unterstützt).



In Patton **Trinity Firmwareversion 3.19 und höher** (ab Februar 2021) werden DNAT-/Portforwarding-Szenarien unterstützt! Der SBC benötigt damit keine eigene öffentliche IP-Adresse mehr, sondern kann über Portforwardings erreichbar gemacht werden.

- **FQDN** bzw. vollqualifizierter Domänenname **für den SBC** (z.B. sbc01.meinefirma.de) mit Verweis **im DNS** auf dessen öffentliche IP-Adresse.
- **X.509 Zertifikat für den SBC** von einer **öffentlichen, vertrauenswürdigen Stammzertifizierungsstelle** sowie Zugriff auf den zugehörigen privaten Schlüssel. Das Zertifikat muß auf den FQDN des SBC ausgestellt sein.
- Der Patton SmartNode SBC muß eine **korrekte Datums-/Uhrzeitkonfiguration** besitzen und sich bestenfalls per **NTP** mit einer präzisen Zeitquelle synchronisieren.
- **Folgende Informationen** werden zusätzlich für die Konfiguration benötigt:
  - STARFACE IP-Adresse
  - Liste aller STARFACE-Benutzer, die die Teams-Anbindung verwenden sollen, inklusive ihrer Telefonnummern (intern/extern) und den SIP-Kontodaten (Benutzername und Kennwort).

Selbstverständlich müssen der SBC und die anzubindende STARFACE per SIP und RTP unbeschränkt miteinander kommunizieren können.

## Lizenzierung

Die Patton SmartNode SBC müssen über Lizenzen mit der gewünschten Anzahl SIP-Sessions (gleichzeitige Gespräche) sowie SRTP-Channels (Anzahl verschlüsselter Kanäle) ausgerüstet werden. Da die Kommunikation mit Microsoft zwingend Verschlüsselung voraussetzt, müssen für die zu erwartende Anzahl gleichzeitiger Gespräche sowohl SIP-Sessions, wie auch SRTP-Channels in gleichem Maße lizenziert werden.

Die Modelle der Serie [SmartNode SN5500](#) lassen sich so auf bis zu 200 gleichzeitige Gespräche aufrüsten.  
 Das Modell [SmartNode SN5600](#) ist für bis zu 1.000 parallele Gespräche ausgelegt.  
 Der [virtualisierte SmartNode](#) kennt keine Beschränkungen – diese sind von der Leistungsfähigkeit der virtuellen Hardware abhängig.

Die von Patton ausgestellte Lizenzdatei sieht hierbei wie folgt aus und kann direkt per Copy&Paste auf der Kommandozeile des Geräts eingegeben werden:

#### CLI: Eingabe auf der Kommandozeile per SSH/Telnet

```
# SIP Sessions [sip-sessions], license serial number: 44879, system serial number: 00aabb0f2439
# Additional SIP Sessions: 20 [extra-sessions=20]
install license YdDBmT/IKgN3CZyBjNDJ6S1m+0yyXlneLhjVeNnWyl3SC

# SRTP Channels [srtp-channels], license serial number: 44880, system serial number: 00aabbcc2439
# Additional SRTP Channels: 20 [extra-channels=20]
install license Gure82bMZFNNe229ee+rEWaV2eVfOe2PJfIFzt60uKwEe
```

Ob die Lizenzen erfolgreich eingespielt wurden, kann anschließend über die Eingabe von *show system licenses* überprüft werden:

```
0F2439(cfg)#show system licenses

Local Licenses
=====

The following licenses are available on the local device:
Serial Number: 00A0BA0F2439

-----
License Name      Source:      Available:      Usage:
                  Blt-In +    Inst. + Leased =    Total    =    Alloc +    Free
-----
sip-sessions      4          20          57          81
srtp-channels     8          20          28          28
voice-channels    4          4           4           4
-----
iprouter          Y
sip-registrar     Y
sip-tls-srtp      Y
transcoding       Y
-----
```

## TLS Profile

Für die Kommunikation mit Microsoft über Direct Routing ist Verschlüsselung obligatorisch. Zunächst muss der SBC mit einem X.509-Zertifikat und dem zugehörigen Private Key ausgestattet werden, um sich gegenüber Microsoft auszuweisen. Die folgenden Zeilen sind auf der Kommandozeile des Geräts einzugeben, um das Zertifikat, den Private Key und die Zertifikate der Intermediate CAs zu importieren (jeweils im [PEM-Format](#)):



Nach Eingabe des jeweiligen Import-Befehls (Zeilen 1, 13 und 21) werden die Zertifikate im PEM-Format per Copy&Paste eingefügt und mit einer Leerzeile abgeschlossen.

Die Darstellung der Zertifikate und des Private-Keys auf der linken Seite sind Beispiele und dienen der Veranschaulichung.

#### CLI: Eingabe auf der Kommandozeile per SSH/Telnet

```
0F2439#import pki:certificate/MYCERTIFICATE
Paste the contents of the file (enter an empty line when done):
-----BEGIN CERTIFICATE-----
MIIGZjCCBU6gAwIBAgIQDfw+rcYnGBfoqe36UQFPzANBgkqhkiG9w0BAQsFADBH
QswCQQYDVQQGEDJVUzEWMBQGA1UEChMNR2VvVHJlc3QgSW5jLjEgMB4GN1UEVxMX
UmF aWRTU0wgU0hBMjU2IENBIC0gRzIwHhcNMTYxMjI1MDAwMDAwWhcNMjAwMTA1
.....
bD8l3HKHS/7u2lOzu/Ja0C5u6CSXdmPeq9Zof77vempXQHx0BwI+b5bzOAza28p5
KBbWfi+fdh6kJz2ydXUXWGbGZuBykeulF+M65FchP7/b7EIpKgtFJJyS3EvYHliY
lwuJqHHBIOB+3Q==
-----END CERTIFICATE-----

0F2439#import pki:private-key/myprivate.key
Paste the contents of the file (enter an empty line when done):
-----BEGIN RSA PRIVATE KEY-----
/iqCw7vgv+SuzqcCIBtmZ0IH1XAC8fs5RfoM5yeAfv/kOpjGMNg+3hB0f8MVAHcA
.....
AiEA+DtGLCgvVangxIyhXbWRbxGGEY4wmNCi7x5ib7yYGBACIQCRQlmlL2SHRlED
-----END RSA PRIVATE KEY-----

0F2439#import pki:certificate/CA
Paste the contents of the file (enter an empty line when done):
-----BEGIN CERTIFICATE-----
MChjKSAYMDA4IEdlblRydXN0IEluYy4gLSBGb3IgYXV0aG9yaXplZCB1c2Ugb25s
.....
a2qiimBpwFd9svIxDJhlMuwIWs7GmOkhlz8seSkD9faUKlMx85NoV+HXTzrRYaFg
-----END CERTIFICATE-----
```

- 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.

Die Parameter für die verschlüsselte Kommunikation werden in einem TLS Profile konfiguriert.

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

```
profile tls pf_tls_default
no protocol tls-v1.0
no protocol tls-v1.1
compression
authentication incoming
authentication outgoing
private-key pki:private-key/myprivate.key
own-certificate 1 pki:certificate/MYCERTIFICATE
own-certificate 2 pki:certificate/CA
diffie-hellman-parameters pki:diffie-hellman-parameters/DEFAULT-4096
require certificate-type server
```

- 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).

## VoIP Profile

Das VoIP-Profil bestimmt die Parameter, mit denen die Audiokommunikation zwischen SBC und Teams respektive SBC und STARFACE abläuft.

### VoIP Profile für die Kommunikation mit Microsoft Phone System / Teams

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

- 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 physikalische 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  $2^{31}$  Paketen der für die Verschlüsselung verwendete SRTP-Schlüssel ausgetauscht. Diese Konfigurationsoption steht ausschließlich auf physikalischen SBCs zur Verfügung und wird auf virtualisierten SmartNodes eine Fehlermeldung erzeugen, die jedoch ignoriert werden kann.
- Zeile 4: Erzwingt die Verwendung von DSP Ressourcen, die für die Verschlüsselung benötigt werden. Diese Konfigurationsoption steht ausschließlich auf physikalischen SBCs zur Verfügung und wird auf virtualisierten SmartNodes eine Fehlermeldung erzeugen, die jedoch ignoriert werden kann.
- Zeile 5: SRTP-Verschlüsselung ist zwingend zwischen Microsoft und SBC.
- Zeile 6: RTP und RTCP Multiplexing nach RFC5761 (Verwendung der selben Portnummern; Anforderung von Microsoft).

### VoIP Profile für die Kommunikation mit STARFACE

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

- Zeile 2: Es wird der Audio-Codec G.711alaw gegenüber der STARFACE angeboten. Weitere Codecs werden nicht konfiguriert, damit keine Codec-Transkodierung notwendig wird.
- Zeile 3: Erzwingt die Verwendung von DSP Ressourcen, die für die Verschlüsselung benötigt werden. Diese Konfigurationsoption steht ausschließlich auf physikalischen SBCs zur Verfügung und wird auf virtualisierten SmartNodes eine Fehlermeldung erzeugen, die jedoch ignoriert werden kann.

## Mapping Tabellen



Die folgenden Abschnitte müssen im **context cs SWITCH** der Patton-Konfiguration eingetragen werden

Der SBC muß zwischen STARFACE und Microsoft Phone System die angerufene Rufnummer bzw. deren URI-Repräsentation in die jeweils erwarteten Formate bzw. Ziele übersetzen. Eine Rufnummer auf Teams-Seite muß in einen SIP-Account-Namen auf STARFACE-Seite konvertiert werden und umgekehrt:



Die jeweiligen Werte für die SIP-Account-Namen und Telefonnummern müssen auf den konkreten Anwendungsfall angepasst werden.  
Die IP-Adresse der calling-uri muß der IP-Adresse der STARFACE entsprechen!

### Übersetzung von Teams-Telefonnummern in STARFACE Account-Namen

```
mapping-table calling-uri to calling-e164 mt_teams2starface-a-e164
map sip:(.*) to \1
map tel:(.*) to \1

mapping-table calling-e164 to calling-uri mt_teams2starface-a-uri
map \+497123222 to sip:user.01@10.108.2.100
map \+497123223 to sip:user.02@10.108.2.100
map \+497123224 to sip:user.03@10.108.2.100

mapping-table called-e164 to called-e164 mt_teams2starface-b-internalCalls
map (00)?49(...)?$ to \2
```

- Zeile 1-3: Das Mapping *calling-uri to calling-e164 mt\_teams2starface-a-e164* entnimmt der SIP-URI die Anrufernummer und setzt diese als Anrufernummer 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 einer 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.

### Übersetzung von STARFACE SIP-Account-Namen in Teams-Telefonnummern

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

- 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.

Zur einfacheren Erweiterbarkeit werden alle notwendigen Anpassungen in die oben angegebenen einzelne Mapping-Tables gegliedert und durch eine Complex-Function für eine konkrete Anrufrichtung zusammengefasst:

### Sammlung der Anpassungen für die jeweilige Gesprächsrichtung

```
complex-function cf_teams2starface
execute 1 mt_teams2starface-a-e164
execute 2 mt_teams2starface-a-uri
execute 3 mt_teams2starface-b-internalCalls

complex-function cf_starface2teams
execute 1 mt_starface2teams-b-e164
```

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

## Routing Tabellen

Routingtabellen definieren, zwischen welchen Schnittstellen (Interfaces) Anrufvermittlung stattfindet. Die Vermittlung von Anrufen kann von verschiedenen Parametern abhängig gemacht werden und es können Regelwerke (Complex-Functions oder Mappingtabellen) auf den vermittelten Anruf angewendet werden.

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

```
routing-table called-el64 rt_from_teams
  route default dest-interface if_sip_starface cf_teams2starface

routing-table called-el64 rt_from_starface
  route default dest-service hg_microsoft-teams cf_starface2teams
```

- 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.

## Interfaces und SIP-Gateways

### Schnittstelle zu Microsoft Phone System / Teams

```
interface sip if_sip_microsoft-directrouting-primary
  bind context sip-gateway gw_sip_wan_5062
  route call dest-table rt_from_teams
  remote sip.pstnhub.microsoft.com 5061
  local sbc.meinefirma.de 5062
  hold-method direction-attribute inactive
  no call-transfer accept
  privacy
  address-translation outgoing-call contact-header user-part fix sbc.meinefirma.de
  use profile voip pf_voip_microsoft
  srtp renegotiate-on-connect
  penalty-box sip-option-trigger interval 60 timeout 60 force tls
  session-timer 3600
  trust remote
  trust 52.114.0.0/16

interface sip if_sip_microsoft-directrouting-secondary
  bind context sip-gateway gw_sip_wan_5062
  route call dest-table rt_from_teams
  remote sip2.pstnhub.microsoft.com 5061
  local sbc.meinefirma.de 5062
  hold-method direction-attribute inactive
  no call-transfer accept
  privacy
  address-translation outgoing-call contact-header user-part fix sbc.meinefirma.de
  use profile voip pf_voip_microsoft
  srtp renegotiate-on-connect
  penalty-box sip-option-trigger interval 60 timeout 60 force tls
  session-timer 3600
  trust remote
  trust 52.114.0.0/16

interface sip if_sip_microsoft-directrouting-tertiary
  bind context sip-gateway gw_sip_wan_5062
  route call dest-table rt_from_teams
  remote sip3.pstnhub.microsoft.com 5061
  local sbc.meinefirma.de 5062
  hold-method direction-attribute inactive
```



```

no call-transfer accept
privacy
address-translation outgoing-call contact-header user-part fix sbc.meinefirma.de
use profile voip pf_voip_microsoft
srtp renegotiate-on-connect
penalty-box sip-option-trigger interval 60 timeout 60 force tls
session-timer 3600
trust remote
trust 52.114.0.0/16

service hunt-group hg_microsoft-directrouting
    timeout 3
    drop-cause normal-unspecified
    drop-cause no-circuit-channel-available
    drop-cause network-out-of-order
    drop-cause temporary-failure
    drop-cause switching-equipment-congestion
    drop-cause access-info-discarded
    drop-cause circuit-channel-not-available
    drop-cause resources-unavailable
    route call 1 dest-interface if_sip_microsoft-directrouting-primary
    route call 2 dest-interface if_sip_microsoft-directrouting-secondary
    route call 3 dest-interface if_sip_microsoft-directrouting-tertiary

location-service ls_microsoft
    domain 1 microsoft.com
    domain 2 sip-du-a-eu.pstnhub.microsoft.com
    domain 3 sip-du-a-us.pstnhub.microsoft.com
    domain 4 sip-du-a-as.pstnhub.microsoft.com
    domain 5 pstnhub.microsoft.com
    domain 6 sip.pstnhub.microsoft.com
    domain 7 sip2.pstnhub.microsoft.com
    domain 8 sip3.pstnhub.microsoft.com

identity-group DEFAULT
    user phone

    authentication inbound
        authenticate none

    registration outbound
        register none

    call outbound
        transport-protocol force tls

    call inbound

```

- 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

```
interface sip if_sip_starface
  bind context sip-gateway gw_sip_lan_5060
  route call dest-table rt_from_starface
  remote starface.meinefirma.de
  hold-method direction-attribute sendonly
  early-disconnect
  no call-transfer accept
  no call-transfer emit
  address-complete-indication accept set
  address-translation incoming-call calling-el64 from-header
  address-translation incoming-call calling-uri from-header
  address-translation incoming-call calling-name from-header
  use profile voip pf_voip_starface
  trust remote

authentication-service as_starface-sipaccounts
  username user.01 password meingeheimessippasswort01
  username user.02 password meingeheimessippasswort02
  username user.03 password meingeheimessippasswort03

location-service ls_starface
  domain 1 starface.meinefirma.de

identity-group teams

  authentication outbound
    authenticate 1 authentication-service as_starface-sipaccounts

  authentication inbound
    authenticate none

  registration outbound
    registrar starface.meinefirma.de
    lifetime 180
    register auto

  call outbound

  call inbound

    identity user.01 inherits teams
    identity user.02 inherits teams
    identity user.03 inherits teams
```

## SIP-Gateways

```
context sip-gateway gw_sip_lan_5060
  bind location-service ls_starface

  interface if_gw_sip_lan_5060
    transport-protocol udp+tcp 5060
    no transport-protocol tls
    bind ipaddress ROUTER if_eth00 if_eth00

context sip-gateway gw_sip_lan_5060
  no answer-untrusted-hosts
  no shutdown

context sip-gateway gw_sip_wan_5062
  use profile tls pf_tls_default
  bind location-service ls_microsoft

  interface if_gw_sip_wan_5062
    no transport-protocol udp+tcp
    transport-protocol tls 5062
    bind ipaddress ROUTER if_eth01 if_eth01
    spoofed contact-header manual sbc01.fluxpunkt.de port 5062
    spoofed via-header manual sbc01.fluxpunkt.de port 5062

context sip-gateway gw_sip_wan_5062
  no answer-untrusted-hosts
  connection-reuse
  no shutdown
```

## IP-Router und physikalische Netzwerkport-Konfiguration

### IP Router Konfiguration

```
context ip ROUTER

  interface if_eth00
    ipaddress if_eth00 192.168.1.1/24
    tcp adjust-mss rx mtu
    tcp adjust-mss tx mtu

  interface if_eth01
    ipaddress if_eth01 123.123.123.123/28
    tcp adjust-mss rx mtu
    tcp adjust-mss tx mtu
```

### Physikalische Portkonfiguration

```
port ethernet 0 0
  bind interface ROUTER if_eth00
  no shutdown

port ethernet 0 1
  bind interface ROUTER if_eth01
  no shutdown
```

## Inhalt

- [Inhalt](#)

- [Vorwort](#)
- [Sicherheit](#)
- [Technische Voraussetzungen & Vorbereitende Maßnahmen](#)
- [Installation des STARFACE Moduls](#)
  - [Lizenzierung](#)
  - [Konfiguration](#)
- [Inbetriebnahme der STARFACE Teams App](#)
  - [Teams App herunterladen und organisationsweit verteilen](#)
  - [Verbindung zu Ihrer STARFACE](#)
  - [Anmeldung an Ihrer STARFACE](#)

## Vorwort

Auf der STARFACE muss das Modul für die Teams Integration installiert werden. In Teams muss die Teams App installiert werden. Anschließend können sich Benutzer der Teams App mit Ihrer STARFACE verbinden.

## Sicherheit

Bei der Architektur der STARFACE Teams Integration haben wir großen Wert auf Sicherheit gelegt: So ist es möglich, die STARFACE von "außen" unerreichbar, hinter einer Firewall zu betreiben. Es sind **keine Port-Forwardings** oder von Extern erreichbare Dienste innerhalb Ihrer Infrastruktur notwendig. Für die Kommunikation mit Teams, baut das auf der STARFACE laufende Modul, **ausgehend einen verschlüsselten Tunnel** (Websocket-Verbindung; TCP/443) zu einem zentralen und hochskalierbaren Cloud-Connector-Dienst auf.

Jede STARFACE-Installation wird über den Hostnamen bzw. *Name der Anlage* im Cloud-Connector-Dienst registriert. Der Cloud-Connector verbindet anfragende Teams-Clients, nach Übermittlung eines korrekten Schlüssels, mit der für sie zuständigen (und durch den Anlagenamen definierten) STARFACE-Installation über den bestehenden Tunnel. Der Schlüssel verhindert, dass unberechtigte Anfragen ungefiltert an die STARFACE-Installation weitergereicht werden und z.B. Anmeldeversuche (Brute-Force) stattfinden können. Während die UCI-Schnittstelle der STARFACE für den STARFACE Mobile- oder UCC-Client freigegeben werden muß, **schirmt der Cloud-Connector-Dienst der Teams-Integration diese vor externen Zugriffen ab.**

Aus Sicherheitsgründen wird der Schlüssel zufällig vom Modul erzeugt und kann nicht vom Benutzer eingegeben werden. **Bitte behandeln Sie den Schlüssel vertraulich** und geben diesen nur an Benutzer weiter, die berechtigterweise eine Verbindung zu Ihrer STARFACE aufbauen können sollen. Wenn Zweifel an der Vertraulichkeit des Schlüssels bestehen, kann dieser neu generiert und erneut verteilt werden.

Client-Anfragen, die einen korrekten Anlagenschlüssel übermitteln, können sich im nächsten Schritt für eine UCI-Verbindung authentifizieren. Dies ist vergleichbar mit der Anmeldung eines UCC-Clients an der STARFACE. **Der Cloud-Connector-Dienst speichert selbst keine Zugangsdaten** sondern leitet berechnete Anfragen lediglich an die STARFACE weiter. Benutzerauthentifizierung, Berechtigungssteuerung und Umsetzung der Sicherheitskonzepte steuert weiterhin die STARFACE.

## 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](https://login.microsoftonline.com)
  - [service-cloud-connector.fluxpunkt.de](https://service-cloud-connector.fluxpunkt.de)
  - [omni-client.fluxpunkt.de](https://omni-client.fluxpunkt.de)

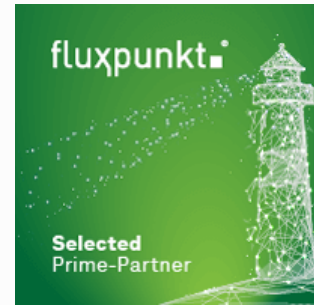
## Installation des STARFACE Moduls

Laden Sie eine kompatible Modulversion aus unserem Wiki unter [Teams Integration for STARFACE](#) herunter. Befolgen Sie die [Anleitung zur Installation von STARFACE Modulen](#).

### Maximal eine Modulkonfiguration

Achten Sie darauf, dass nicht mehr als eine Modulkonfiguration auf Ihrer STARFACE existiert. Ein Betrieb mit mehreren Modulkonfigurationen ist nicht unterstützt.

## Lizenzierung



**Integrationspartner**  
auszuwählen, die über das entsprechende Know-How im Bereich Teams, STARFACE und Patton verfügen.

Von Fluxpunkt wurde die folgenden "Leuchtturmpartner" ausgewählt, um andere STARFACE-Partner und Endkunden bei der Integration zu unterstützen:

- [EDV-BV GmbH](#)
- [GDS GmbH](#)
- [Kronshage IT](#)
- [Luithe & Luithe GmbH](#)
- [Netzwerkkontor GmbH & Co. KG](#)
- [SMEA IT Services GmbH](#)
- [STARFACE GmbH](#)
- [swissnet telecommunication ag](#)

Alphabetische Reihenfolge ohne Wertung

Für

Es gibt zwei Möglichkeiten der Lizenzierung: STARFACE User-Assigned-Licenses und Fluxpunkt Floating-Licenses, die unterschiedliche Anwendungsfälle abdecken:

## 1. STARFACE User-Assigned-License (UAL)

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:

Konfiguration

Systemstatus

Benutzer

Gruppen

Telefone

Module

Voicemail

Konferenz

Adressbuch

Rufnummern

Leitungen

Routing

Server

Auswertung

Anlagenverbund

Sicherheit

Erweiterte Einstellungen

Serverkonfiguration

Status

Zeit/Datum

Netzwerk

Mail-Server

Webserver

Backup

Log-Datei

Lizenzen

Lizenzinformationen

Lizenzierte Benutzer: 26

Noch verfügbar: 0

Lizenzierte Light Benutzer: 0

Noch verfügbar: 0

Lizenzierte UCC Premium Benutzer: 4

Noch verfügbar: 1

Update-Option

Benutzer: 29

Lizenzschlüssel: \*

Firma: \*

Straße: \*

PLZ / Ort: \*

Bundesland: \*

Land: \*

Germany

Telefon: \*

Fax: \*

E-Mail: \*

Modullizenzen

Lizenzschlüssel: \*

Pflichtfeld

Registrieren

Abbrechen

Lizenz hinzufügen

Anzeige aktualisieren

Speichern

Übernehmen

Abbrechen

Schließen

Konfiguration

Systemstatus

Benutzer

Gruppen

Telefone

Module

Voicemail

Konferenz

Adressbuch

Rufnummern

Leitungen

Routing

Server

Auswertung

Anlagenverbund

Sicherheit

Erweiterte Einstellungen

Benutzer: Kachelmann, Kerstin

Daten

Umleitung

Telefone

Rufnummern

iFMC

Tasten

Gruppen

Berechtigungen

Skills

Berechtigungen festlegen

Bereich

Definition

Aktiv

Remote Connect

Konferenzen

Fax

Tasten

iFMC

E-Mail-Benachrichtigungen

Telefon-Login

UCI

UCC Premium-Funktionen

Integration mit Microsoft Teams

Windows Terminalserver

STARFACE NEON Video-Meeting

Providerseitige Dienstmerkmale

Speichern

Übernehmen

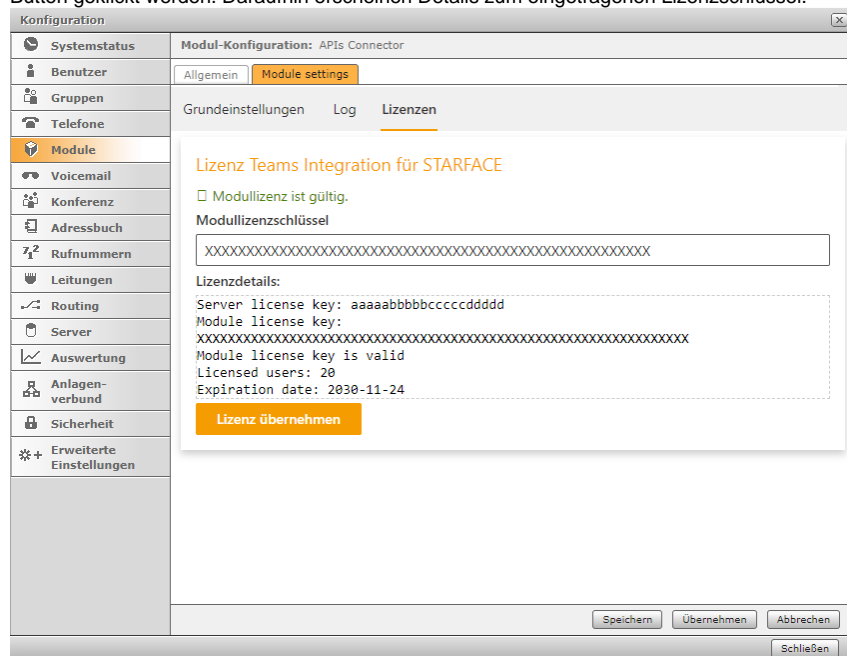
Abbrechen

Schließen

Das Benutzerrecht *Integration mit Microsoft Teams* ist als "Unterrecht" der *UCC Premium-Funktionen* realisiert. Es ist also notwendig, für den Benutzer *UCC Premium-Funktionen* bereitzustellen, bevor das Teams-Recht gewährt werden kann. Die STARFACE Teams-Lizenz enthält nicht bereits die UCC Premium-Lizenz.

## 2. Fluxpunkt Floating-License (FL)

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 orangefarbene Speichern-Button geklickt werden. Daraufhin erscheinen Details zum eingetragenen Lizenzschlüssel.



### Konfiguration

Im Tab Grundeinstellungen muss ein STARFACE Name und ein Schlüssel vergeben werden. Der Schlüssel kann (aus Sicherheitsgründen) nicht von Hand eingetragen werden, sondern wird vom System erzeugt. Gehen Sie wie folgt vor:

1

Tragen Sie den eindeutigen Hostnamen Ihrer STARFACE-Installation ein.

2

Klicken Sie auf den Button *Neuen Schlüssel eintragen*, um einen neuen Anlagenschlüssel zu generieren.

3

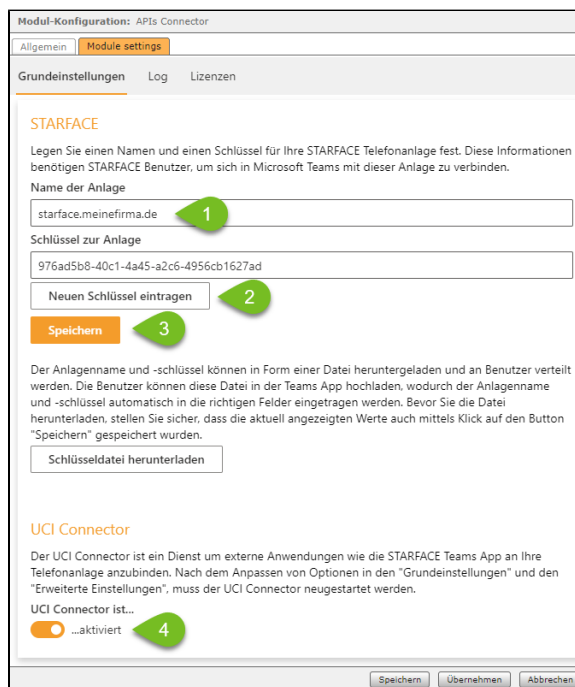
Klicken Sie auf *Speichern*, um den Namen und den Schlüssel der Anlage zu übernehmen.

Im Anschluss ist es möglich, eine Schlüsseldatei mit diesen Einstellungen herunterzuladen und an Mitarbeiter zu verteilen.

4

(Re-)Aktivieren Sie die UCI-Verbindung.

Der UCI-Connector erlaubt es Teams-Benutzern, sich mit der UCI-Schnittstelle der STARFACE zu verbinden. In diesem Moment wird eine Anmeldung mit STARFACE-Zugangsdaten in der STARFACE Teams App möglich.



Den STARFACE Hostnamen und Schlüssel müssen Benutzer später in der Teams App eintragen, um sich mit Ihrer STARFACE-Installation zu verbinden. Sie können die Daten entweder über Kommunikationswege wie Teams-Chat oder E-Mail weitergeben oder Sie laden die vom Modul generierte Schlüsseldatei herunter und verteilen diese an Ihre Benutzer. Die Schlüsseldatei lässt sich per Drag&Drop in das Anmeldefenster der STARFACE Teams App ziehen und übergibt damit die notwendigen Konfigurationsdaten an die Client App.

## Inbetriebnahme der STARFACE Teams App

Die Inbetriebnahme der STARFACE Teams App ist ein dreistufiger Vorgang, wobei die *organisationsweite Bereitstellung* einmalig von einem Administrator durchzuführen ist. Alternativ kann eine benutzerspezifische Bereitstellung auch über das Importieren der App durch einen normalen Benutzer erfolgen.

1

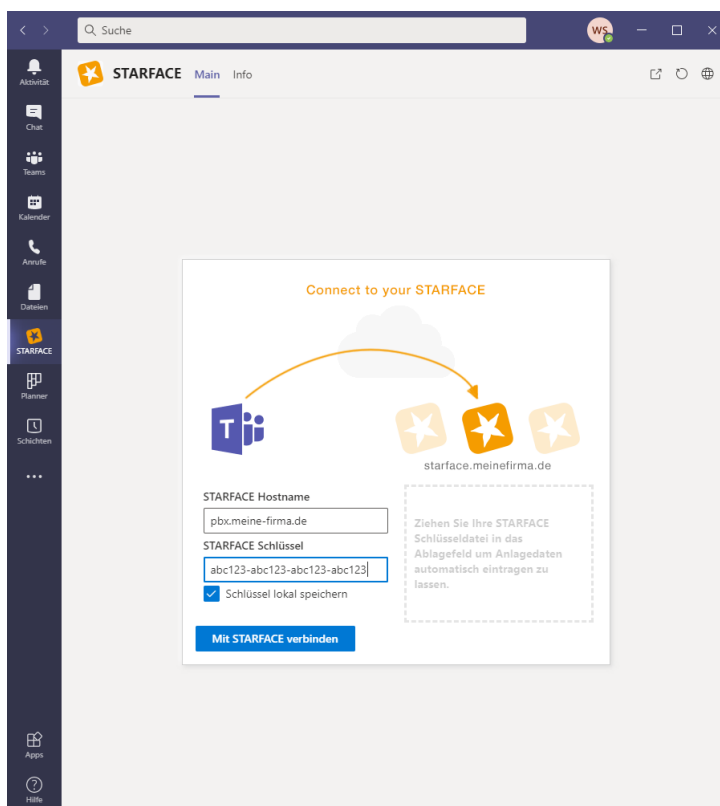
### Teams App herunterladen und organisationsweit verteilen

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.

2

### 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.



3

### Anmeldung an Ihrer STARFACE

Melden Sie sich nun mit Ihren STARFACE Zugangsdaten an

The screenshot shows the STARFACE login screen within a Microsoft Teams application. The interface includes a dark blue sidebar on the left with icons for 'Aktuelle', 'Chat', 'Teams', 'Kalendar', 'Anrufe', 'Dateien', 'STARFACE', 'Planner', 'Scheint', and 'Apps'. The main content area has a header with the 'STARFACE' logo and 'Main Info' tabs. A central white box titled 'Login to your STARFACE' features a diagram showing a connection between a Microsoft Teams icon and a STARFACE icon. Below the diagram, the text 'STARFACE Anmeldung' is followed by instructions: 'Geben Sie Ihre STARFACE Zugangsdaten ein. Teams wird sich anschließend mit dieser Anlage verbinden.' The login form contains two input fields: 'STARFACE Benutzername' with the value '0011' and 'STARFACE Passwort' with masked characters. A checkbox labeled 'Passwort lokal speichern' is checked. At the bottom, there is a green 'Anmelden' button and a link 'Andere STARFACE wählen'.

Suche

WS

STARFACE Main Info

Login to your STARFACE

STARFACE Anmeldung

Geben Sie Ihre STARFACE Zugangsdaten ein. Teams wird sich anschließend mit dieser Anlage verbinden.

STARFACE Benutzername

0011

STARFACE Passwort

Passwort lokal speichern

Anmelden Andere STARFACE wählen