FIRMWARE 5.1

ANLEITUNG

No. 2021-09

Ausgabe 0.6

Ferrari electronic

I. Versionshistorie

Ausgabe	Datum	Autor	Änderungen
0.1	01.04.2019	Johann Deutinger	Erstausgabe, Firmware Version 4.2-385-2069
0.2	15.05.2019	Johann Deutinger	Firmware Version 4.2-1.2137
0.3	12.08.2919	Johann Deutinger	RC1 ab Version 4.2-1.2308 und erste 5.0/64 Bit
0.4	18.02.2020	Chris Helbing	Nur Firmware 5.0, Vorbereitung auf die Veröffentlichung
0.5	22.02.2021	Waldemar Sennert, Rolf Fiedler, Bert Mittelstedt	Anpassung auf Firmware 5.1
0.6	29.09.2021	Waldemar Sennert	Anpassung für Firmware-Release 5.1-90

Tabelle 1: Versionshistorie

Inhaltsverzeichnis

1. Einleitung

Die Konfiguration eines OfficeMaster Gate als Bindeglied zwischen ISDN und SIP ist relativ einfach und verständlich. Zunehmend kommen jedoch reine SIP-Verbindungen ins Spiel und es entstehen komplexe Szenarien mit mehreren unterschiedlichen SIP-Gegenstellen. Die Konfiguration solcher Lösungen wird immer komplizierter und stößt gelegentlich auch an Grenzen. OfficeMaster Gate Firmware Version 5 adressiert diese Probleme, ohne dass erfahrene Anwender alles komplett neu lernen müssen.

Ziel ist es, folgende Anforderungen zu erfüllen:

- Es soll möglichst alles abgebildet werden, was bisher möglich ist (Ausnahme: Fax via OMCUMS-Komponente wird nicht mehr in allen Betriebsarten unterstützt → OfficeMaster DirectSIP Fax als Nachfolge)
- Parallele Nutzung mehrerer SIP-Trunks mit Registrierung
- Vereinfachung des Regelwerks: Eine einzelne Regel führt von der Quelle direkt zum Ziel – es werden nicht mehr korrespondierende Eingangs- und Ausgangsregeln benötigt!
- Flexible Definition von SIP-Endpoints/-Nodes (Interne/externe SIP-Trunks mit/ohne Registrierung, registrierte Endgeräte, fremde SIP-Ziele/Geräte)
- Jeder dieser Endpoints wird mit Eigenschaften konfiguriert – unabhängig vom Regelwerk, und dient als Quelle bzw. Ziel von Regeln
- Das Hinzufügen eines Endpoints wird durch einen Wizard unterstützt; für bekannte Gegenstellen erfolgen so sinnvolle Voreinstellungen
- Die Firmware basiert auf einem 64 Bit Betriebssystem und ist damit zukunftssicher für kommende Hardwaregenerationen
- Mehrfachziele unterstützen wahlweise Load-Balancing- oder Failover-Modus

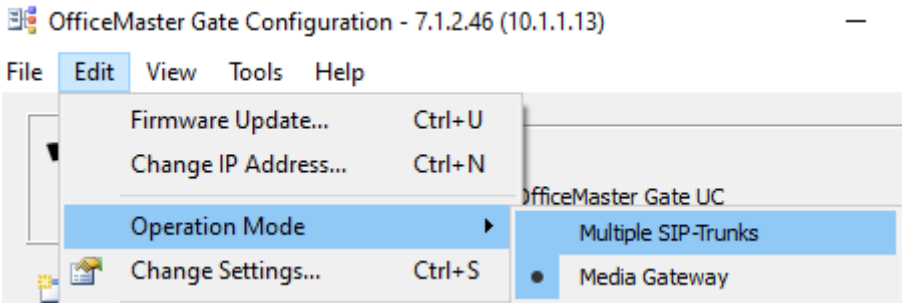
1.1. Einschränkungen in der aktuellen Version

Alle wesentlichen Features für den Betrieb als Session Border Controller sind bereits implementiert. Trotzdem sind im Vergleich zur 4.X-Firmware einige Funktionen im Webinterface (z.B. Testanruf) und den PowerShell Cmdlets nicht mehr vollständig implementiert. Updates hierzu kommen noch.

Hinweis:
Alle Menüs und Dialoge des Konfigurationstools werden in diesem Dokument in der empfohlenen Einstellung „Englisch“ dargestellt (umschaltbar über Hilfe-Menü).

1.2. Entscheidung für eine Betriebsart

Die Firmware 5 beherrscht drei Betriebsarten. Die Konfiguration dieser Betriebsarten ist untereinander nicht kompatibel. Ein Wechsel führt zu deshalb zu einer Neukonfiguration. Das Umschalten erfolgt mit dem Menüpunkt **`Edit → Operation Mode.`**



In der folgenden Tabelle sind die Unterschiede zwischen den unterschiedlichen Versionen und Betriebsarten.

Feature	Release 4.0	Release 4.1	Release 5.1 Media-Gateway-Modus	Release 5.1 Multitrunk-Modus
Messaging Server Mode	✓	✓	✓	✗
Gateway Mode	✓	✓	✓	✗
Multitrunk-Mode	✗	✗	✗	✓
ISDN Schnittstellen	✓	✓	✓	✓
Fax Job-Control/omcums	✓	✓	✓	✗
Fax fipMediaServer	✗	✗	✗	✓
Skype for Business	✓	✓	✓	✓
Microsoft Teams	✗	✗	✗	✓
SIP2Lync	✓	✓	✗	✗
Linux OS EOL	32 Bit / 30.11.20	32 Bit / 30.11.20	64 Bit / 31.5.29	64 Bit / 31.5.29

1.2.1. Betriebsart Media-Gateway

Der klassische Media-Gateway-Modus (sowie der obsolete Messaging-Server-Modus) ermöglicht den Betrieb des Gateways mit gewohnter Konfigurationsoberfläche und Funktionsumfang. In diesem Modus können auch Sicherungen aus einem Gateway mit Firmware 4 wiederhergestellt werden. Für eine Beschreibung dieser Betriebsart wird hier auf das Handbuch der Firmware 4 unter https:/www.ferrari-electronic.de/goto/fw4manual verwiesen. Dem speziellen Fall der Migration von Firmware 4 auf 5 widmet sich das Kapitel 6.

1.2.2. Betriebsart Mehrere SIP-Trunks

Der neue Multi-Trunk-Modus ist die Standardbetriebsart der Firmware 5 in dem alle neuen Funktionen zur

Verfügung stehen. Die Konfiguration wird in den folgenden Kapiteln beschrieben.

1.3. Lizenzierung

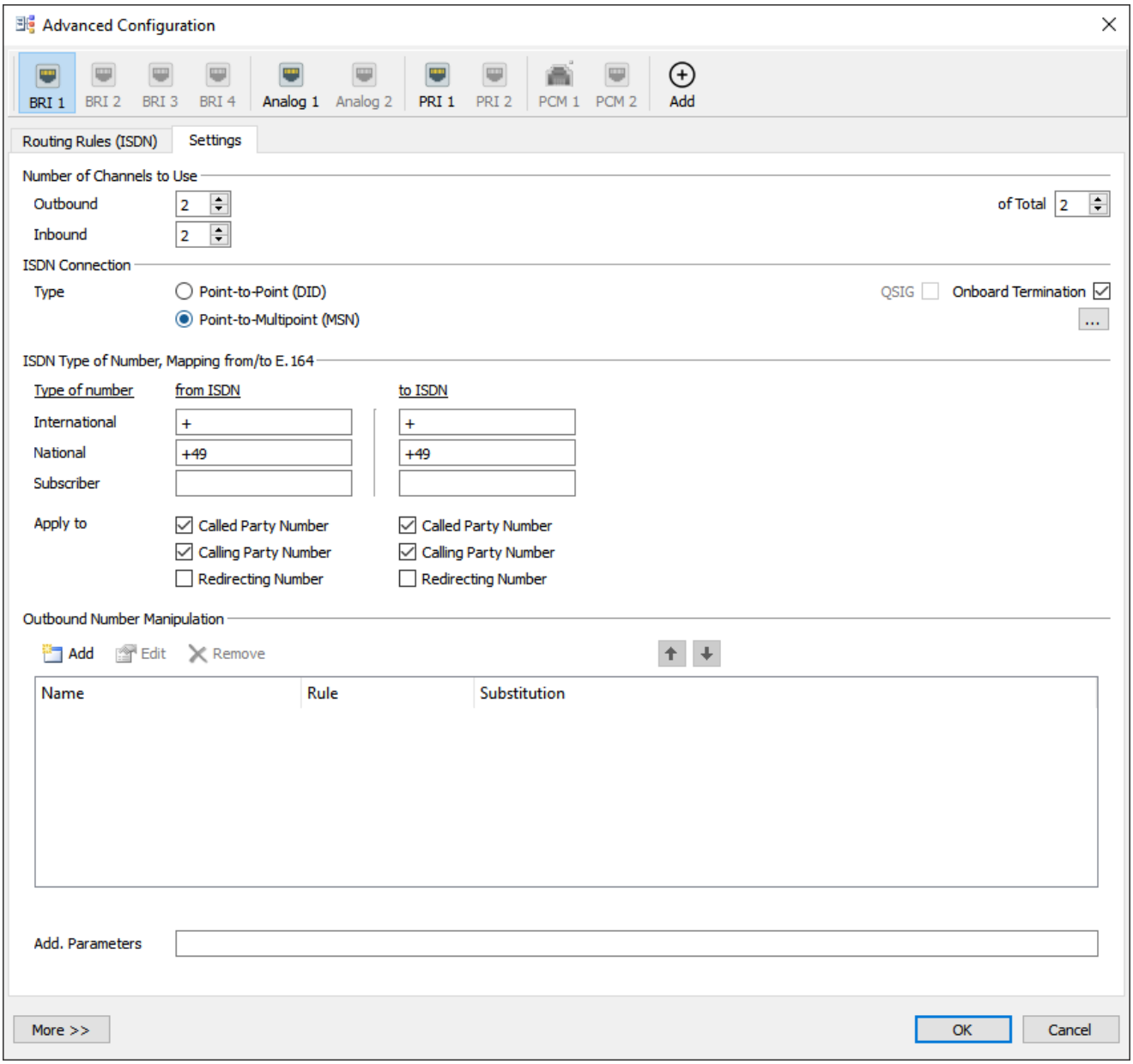
Die Lizenzierung der 5er-Version erfolgt über eine Basis-Lizenz, optionale Erweiterungslizenzen für ISDN/Analog-Trunks sowie durch zusätzliche SIP-Lizenzen (identisch zu den existierenden Lizenzen für 4.1), die im Unterschied zur bisherigen Nutzung als „Concurrent-Calls“ (gleichzeitige Rufe) verwendet werden. Es können also beliebig viele SIP-Trunks mit beliebig vielen Kanälen (Grenzen werden noch definiert) konfiguriert werden. Die Anzahl insgesamt möglicher paralleler Gespräche richtet sich lediglich nach der Anzahl lizenzierter SIP-Kanäle.

2. Trunk-Konfiguration

Alle Trunk-Typen (außer ISDN-Anschlüsse) werden mithilfe eines Assistenten („Wizard“) angelegt und vorkonfiguriert. Weitere Einstellungen bzw. Änderungen können anschließend jederzeit vorgenommen werden.

2.1. ISDN Trunks

Vorhandene ISDN- und Analog-Schnittstellen erscheinen – abhängig von Hardware und Lizenzen – automatisch in der Konfiguration. Ein Großteil der Einstellungen wird in der Registerkarte „Settings“ wie in älteren Firmware-Versionen vorgenommen. Zusätzlich gibt es die Möglichkeit, Regeln zur Nummernmanipulation für ausgehende Anrufe hinzuzufügen („Outbound Number Manipulation“) – siehe Abschnitt 2.6



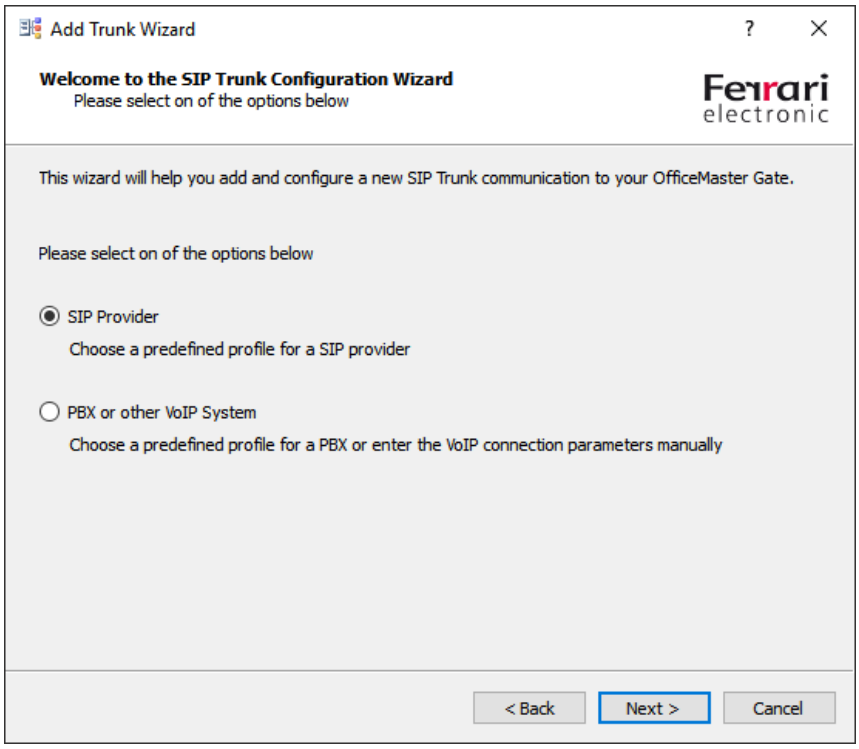
Die Konfiguration eingehender Rufe ist für alle Trunks identisch – sie wird unter 2.5 beschrieben.

2.2. SIP Trunks

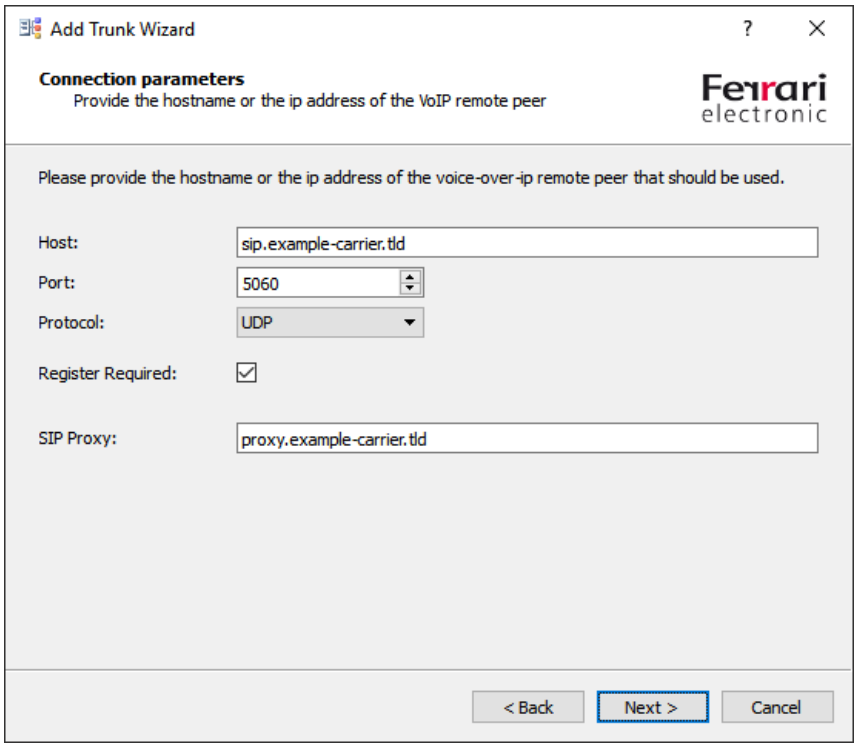
Über den Add-Button 

wird der Wizard zum Hinzufügen eines Trunks gestartet.

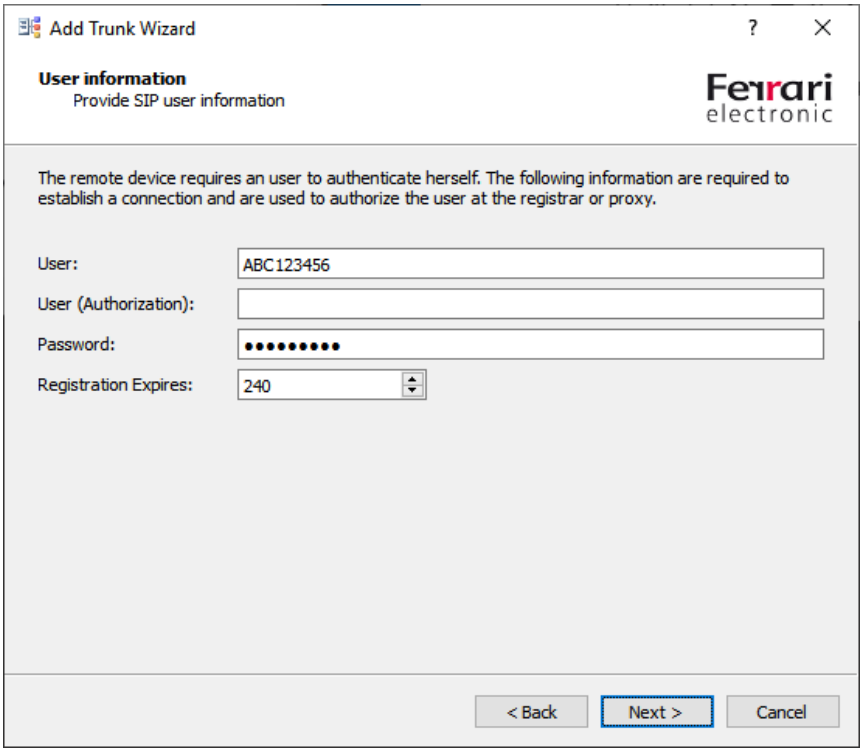
Unter den drei angebotenen Typen wird „SIP Trunk“ gewählt und auf „Next >“ geklickt. Anschließend ist auszuwählen, ob eine SIP-Verbindung zu einem Provider/Carrier oder zu einer IP-PBX bzw. einem UC-System erstellt werden soll:



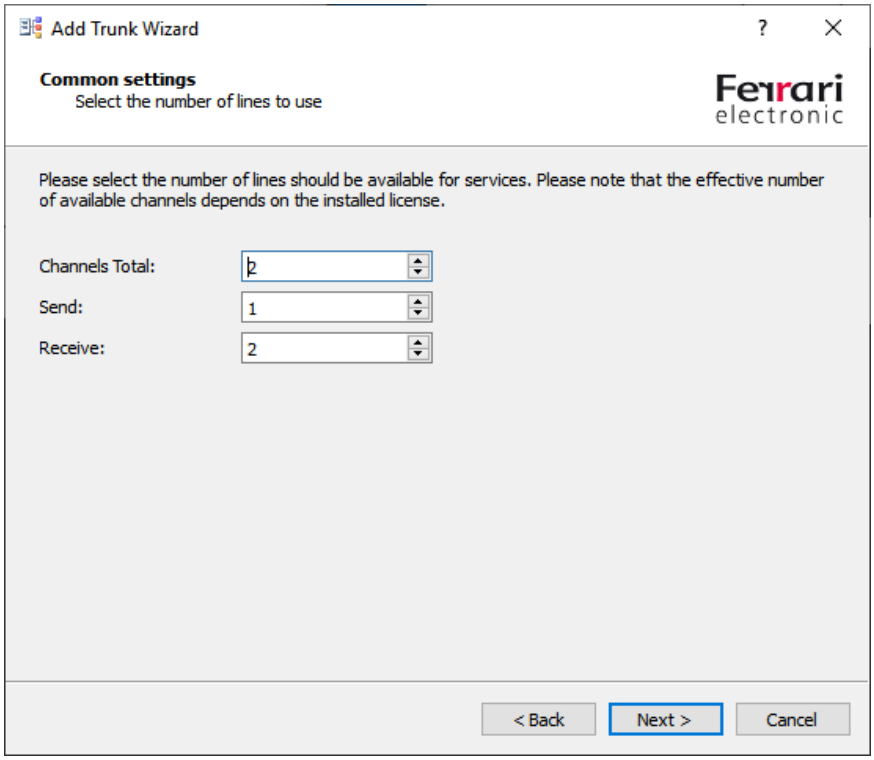
Hier kann eines der vorgegebenen Profile gewählt werden. Falls keine passende Vorlage vorhanden ist, wird das „<Generic Profile>“ verwendet. Unter Host ist im nächsten Schritt das Ziel bzw. die SIP-Domäne anzugeben. Zielport, Protokoll sowie die Angabe, ob eine Registrierung erforderlich ist und ggfs. eine abweichende Proxy-Adresse vervollständigen die Verbindungseinstellungen. Alle Angaben können später jederzeit noch geändert werden.



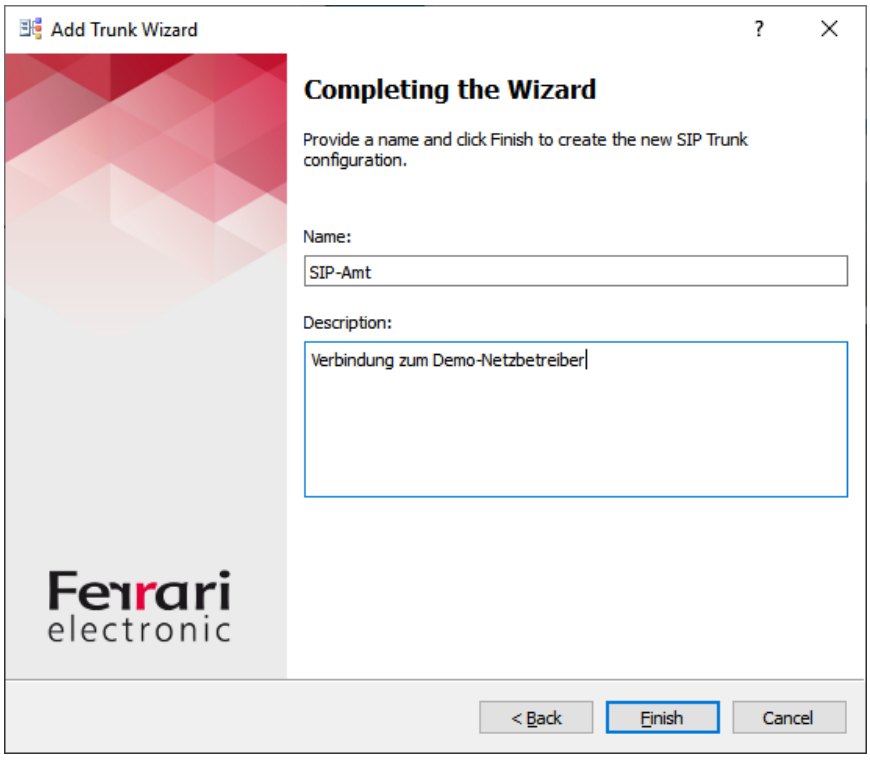
Falls „Register Required“ ausgewählt wurde, erfolgt im nächsten Schritt die Eingabe der Anmeldedaten.



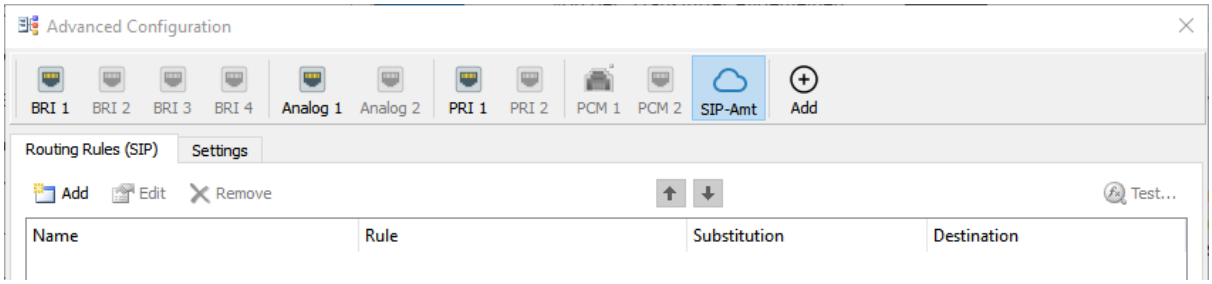
„User (Authorization)“ ist nur anzugeben, wenn er sich vom „User“ unterscheidet. Diese Angaben erhalten Sie von Ihrem Netzbetreiber. Die Gültigkeitsdauer der Registrierung ist ggfs. ebenfalls vom Anbieter vorgegeben. Beim Betrieb aus dem internen Netzwerk über NAT unter Verwendung des UDP-Protokolls darf die Zeitdauer nicht zu lange sein, da sonst der eingehende Weg für ankommende Rufe in der Firewall nicht offenbleibt („UDP hole punching“). Im nächsten Schritt wird die Anzahl paralleler Gespräche konfiguriert.



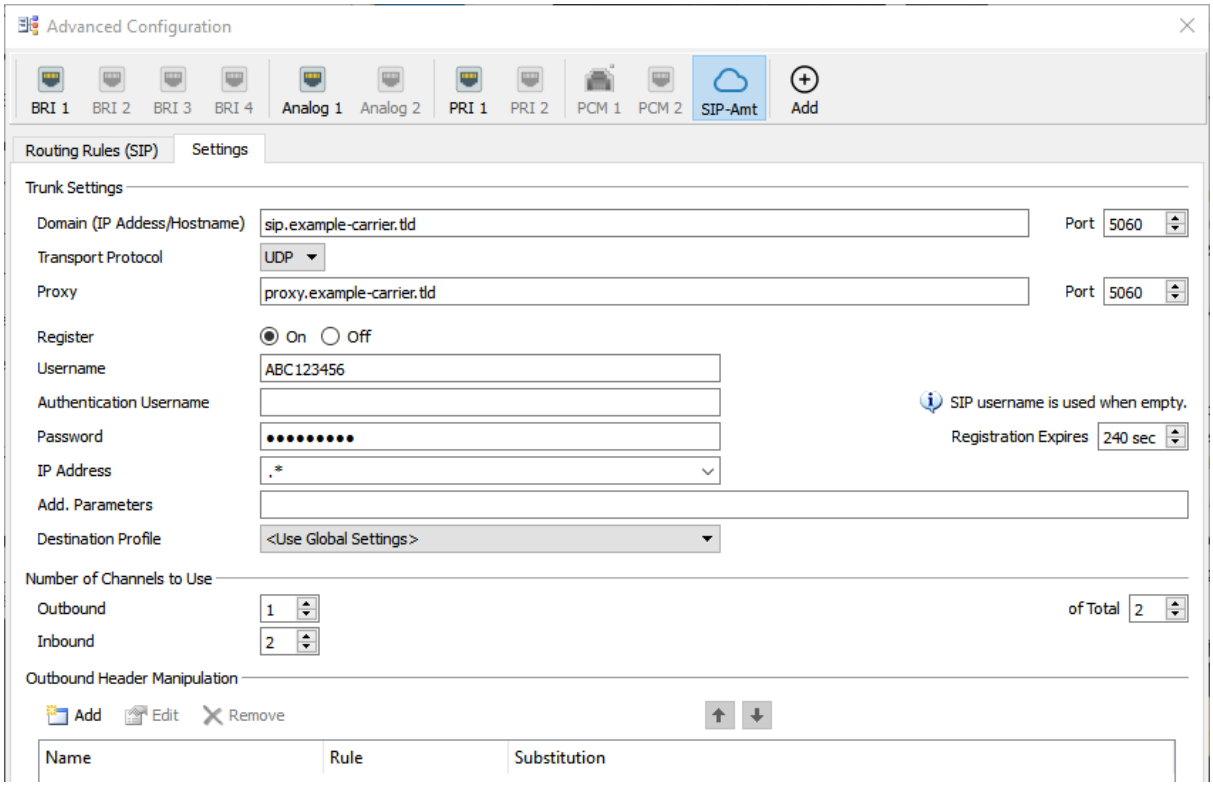
Zuletzt werden Kurzname für den Trunk sowie optional eine ausführlichere Beschreibung konfiguriert.



Der Trunk erscheint nun zusätzlich zu den bisherigen.



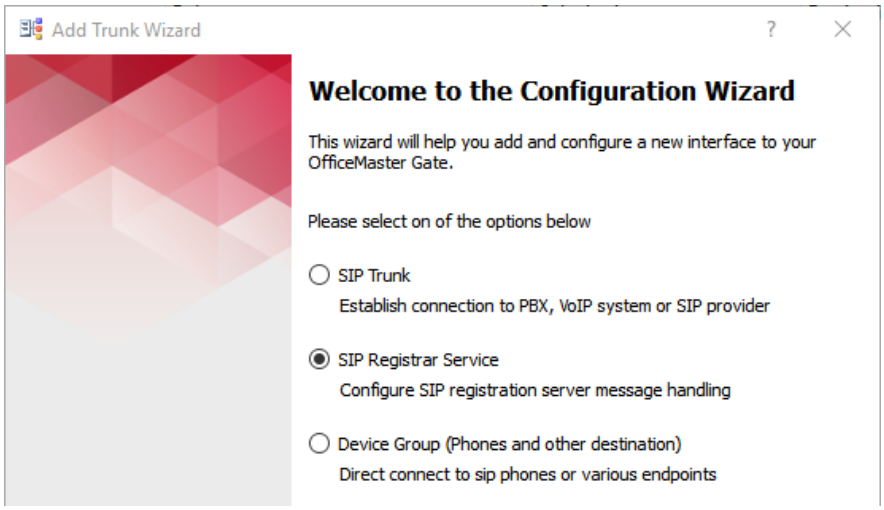
In der Registerkarte „Settings“ können nun alle Einstellungen überprüft bzw. korrigiert oder ergänzt werden.



Zusatzeinstellungen („Additional Parameters“, „Destination Profile“) werden in Abschnitt 5 behandelt. Wichtig ist das Feld „IP Address“: Falls ein eingehendes INVITE nicht anderweitig durch das Feld „Domain“ diesem Trunk zugeordnet werden kann, sollte hier die Absender-IP-Adresse der Gegenstelle angegeben werden, die diesem Trunk zugeordnet ist (Achtung: Syntax als Regulärer Ausdruck!). Mehr dazu im Abschnitt 4.1.

2.3. SIP Registrar Service

Ein spezieller Trunk, der nur einmal angelegt werden kann, ist der „SIP Registrar Service“. Er beinhaltet die Einstellungen für die Registrierung von Geräten und das Regelwerk, das für registrierte Geräte angewendet wird.

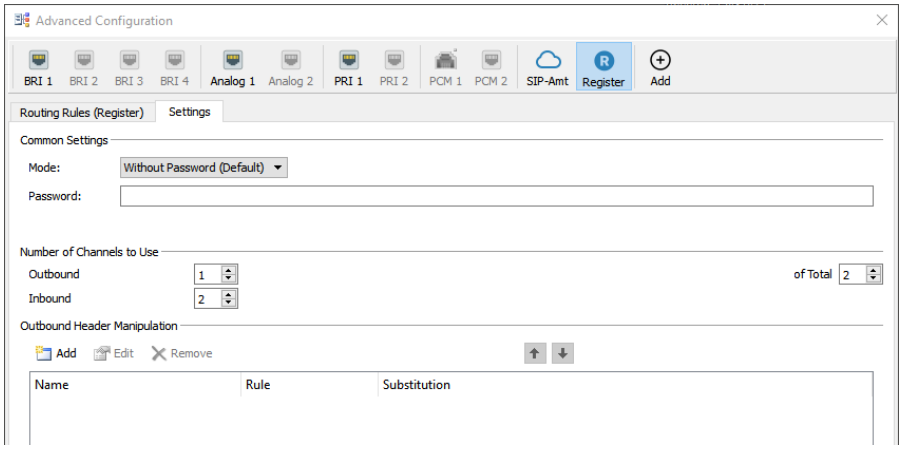


Im nächsten Schritt wird ausgewählt, wie sich SIP-Geräte registrieren können:

- Without Password (Default) – Anmeldung ohne Passwort erlaubt
- Global Password – Anmeldung mit globalem Passwort möglich
- Disabled – Anmeldung nicht erlaubt

Diese Einstellung kann jederzeit geändert werden. Zuletzt wird Name und Beschreibung des Trunks festgelegt.

In der Registerkarte „Settings“ können die Einstellungen nachträglich geändert werden:

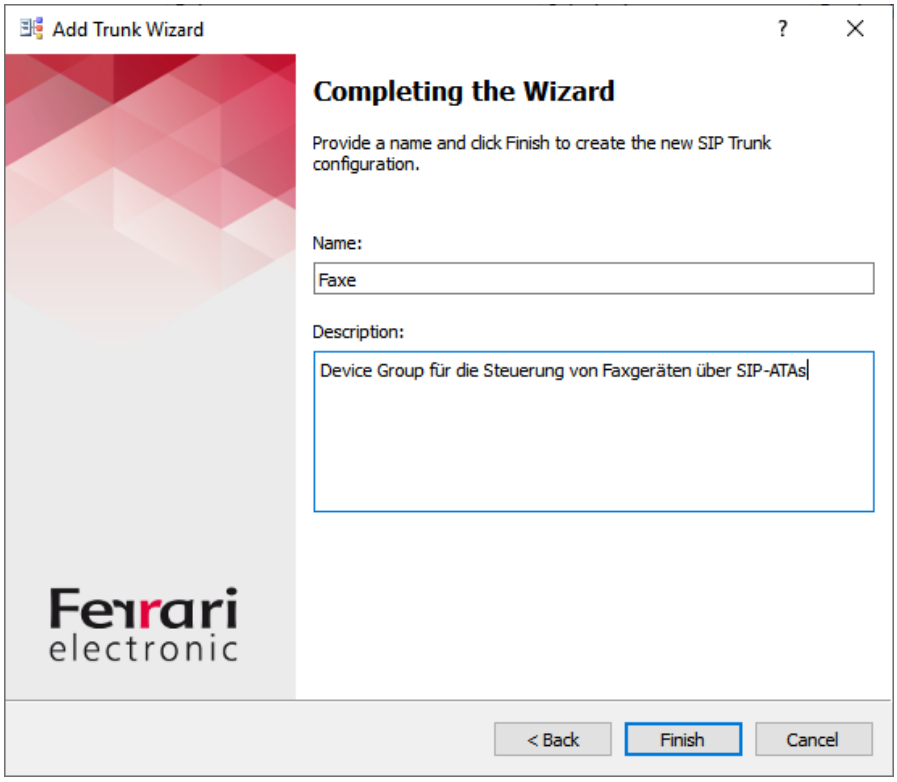


2.4. Device Groups

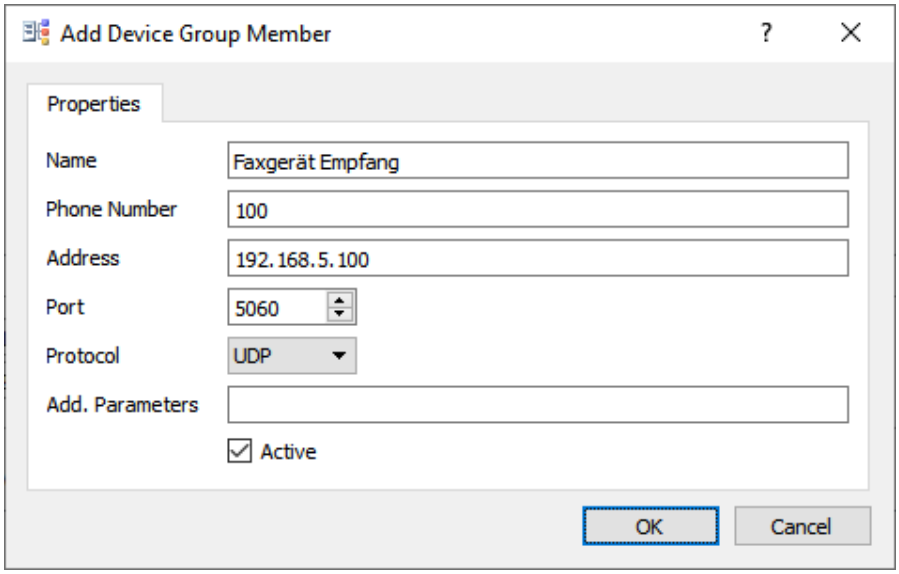
Neben registrierten SIP-Geräten ist es auch möglich, Geräte ohne Registrierung zu nutzen. Analoge Telefone und Faxgeräte, die an SIP-ATAs angeschlossen sind, können wahlweise mit oder ohne Registrierung verwendet werden – dasselbe gilt für SIP-Apparate. Ohne Registrierung können derartige Geräte z.B. nach Standort oder nach Verwendung (Telefone, Faxgeräte, etc.) gruppiert werden, um für jede Gruppe getrennte Einstellungen und Regelwerke zu nutzen.

Erstellt werden solche Gruppen als Trunks wie gewohnt über den Wizard:

Für die Device-Group wird ein Kurzname und eine ausführliche Beschreibung festgelegt:



In „Settings“ werden Mitglieder dieser Gruppe hinzugefügt („Add“):



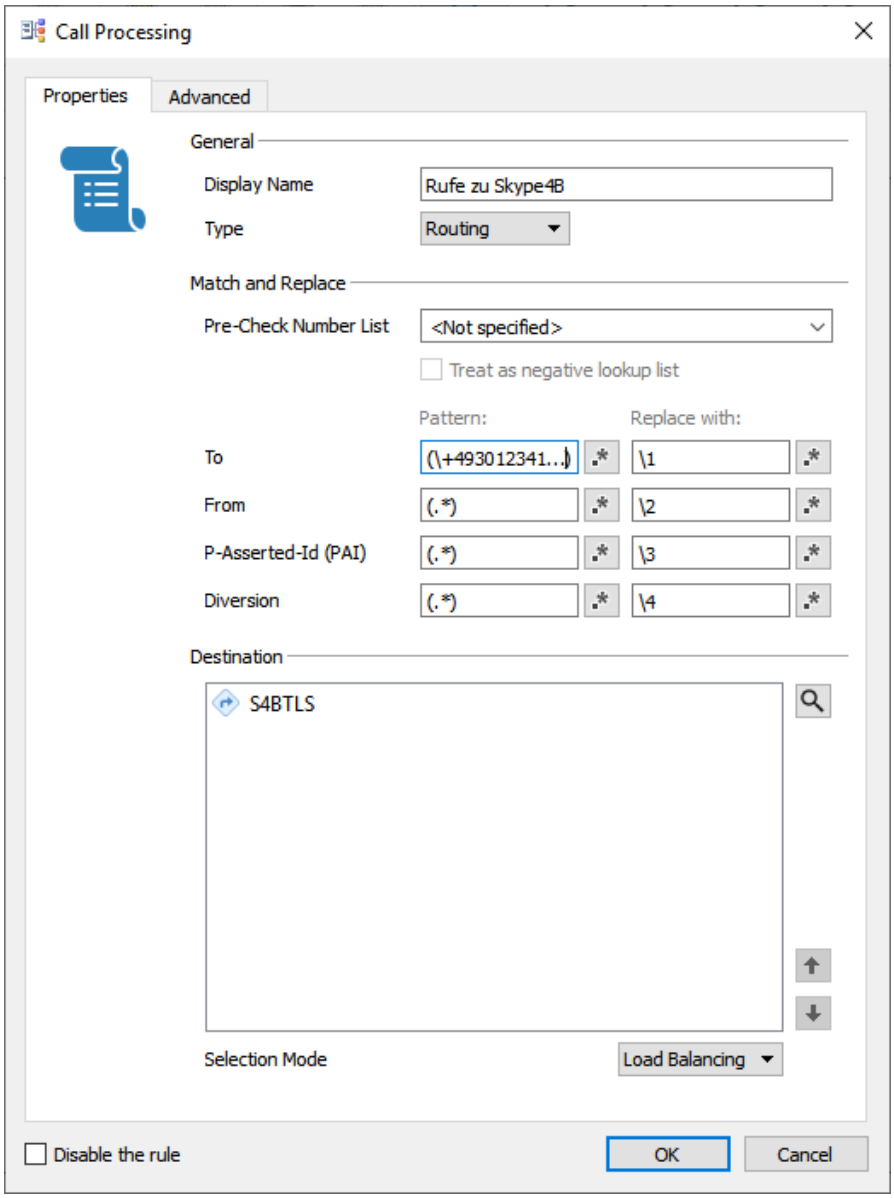
Durch mehrfaches Hinzufügen entsteht eine Liste von Gruppen-Mitgliedern, für die gemeinsame Einstellungen („OutBound Header Manipulation“) und Wahlregeln gelten.

Dieser Trunk-Typ kann mehrfach angelegt und mit Mitgliedern versehen werden.

2.5. Routing-Regeln

Jeder Trunk hat sein eigenes Regelwerk für die Behandlung von eingehenden Rufen. In einer Regel wird direkt zu einem oder mehreren Zielen verwiesen – mehr wird nicht benötigt, um einen Ruf zu behandeln.

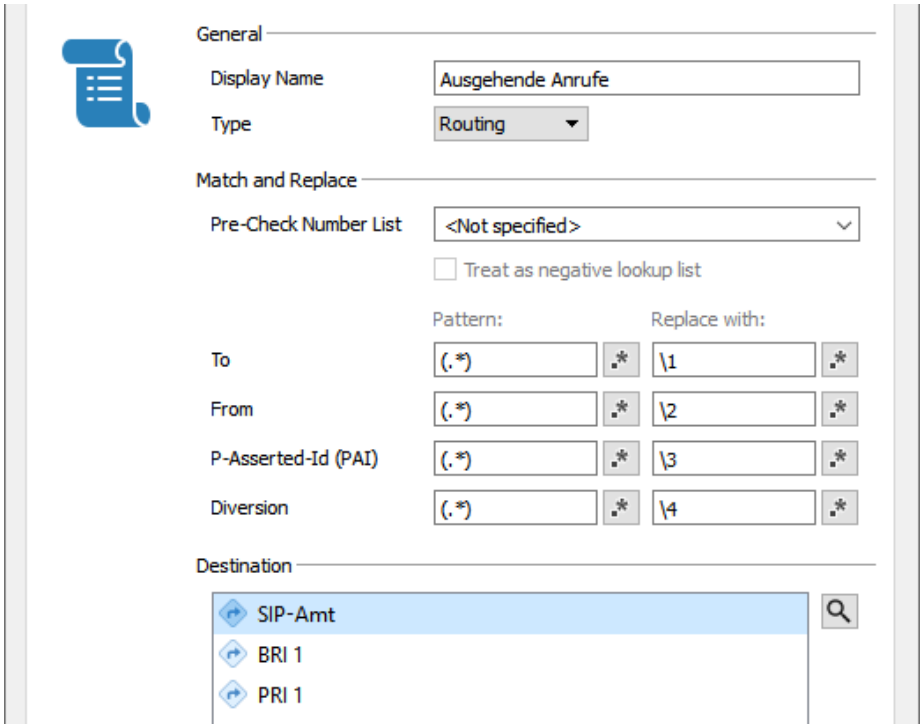
Beispiel für eine Regel vom SIP-Trunk zu Skype for Business – 4-stellige Durchwahlen beginnend mit 1:



Wie in älteren Firmware-Versionen kann zusätzlich eine Nummernliste (von OfficeMaster Directory Service) als zusätzliche Bedingung angegeben werden. In diesem Beispiel wird ein bestimmter Nummernbereich durch einen „Regulären Ausdruck“ ausgewählt – dem Pluszeichen am Anfang muss deshalb ein \ vorangestellt werden, damit der Vergleich mit + als normalem Zeichen stattfindet.

Hinweis:
Wenn mehrere Ziele ausgewählt wurden, kann im „Selection Mode“ zwischen „Load Balancing“ und „Failover“ gewählt werden – diese Möglichkeit gab es in bisherigen Firmware-Varianten nicht!

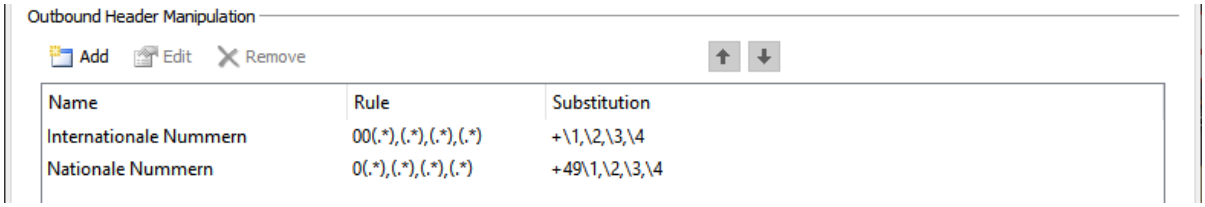
Beispiel für ein Mehrfachziel mit „Failover“ –die Priorität wird durch die Reihenfolge der Ziele festgelegt:



2.6. Korrektur-Regeln für ausgehende Rufe

Jeder Trunk kann von unterschiedlichen anderen Trunks als Ziel angesprochen werden. Dabei kann es vorkommen, dass je nach Quelle verschiedene Rufnummernformate verwendet werden. Manche SIP-Trunks nutzen E.164, während andere nach abweichenden Schemata arbeiten (z.B. 004930… bzw. 030…). Um mit gemischten Quellen arbeiten zu können, werden am ausgehenden Trunk Korrektur-Regeln („Outbound Header Manipulation“) verwendet.

Beispiel zur Umwandlung in E.164 für Skype for Business:



Wenn ausgehende SIP-Trunks kein E.164-Format unterstützen, empfiehlt sich folgende Strategie: In allen eingehenden Regeln wird immer nach E.164 umgewandelt (dazu sind ggfs. mehrere Regeln erforderlich). Ausgehend wird daraus das Format erzeugt, das der jeweilige SIP-Trunk erwartet – unter anderem auch die optionale Angabe des Absenders als „P-Asserted-Identity“ (PAI) Header.

3. Beispiel-Konfigurationen

Hier werden ein paar typische Beispiele im Umfeld von OfficeMaster dokumentiert.

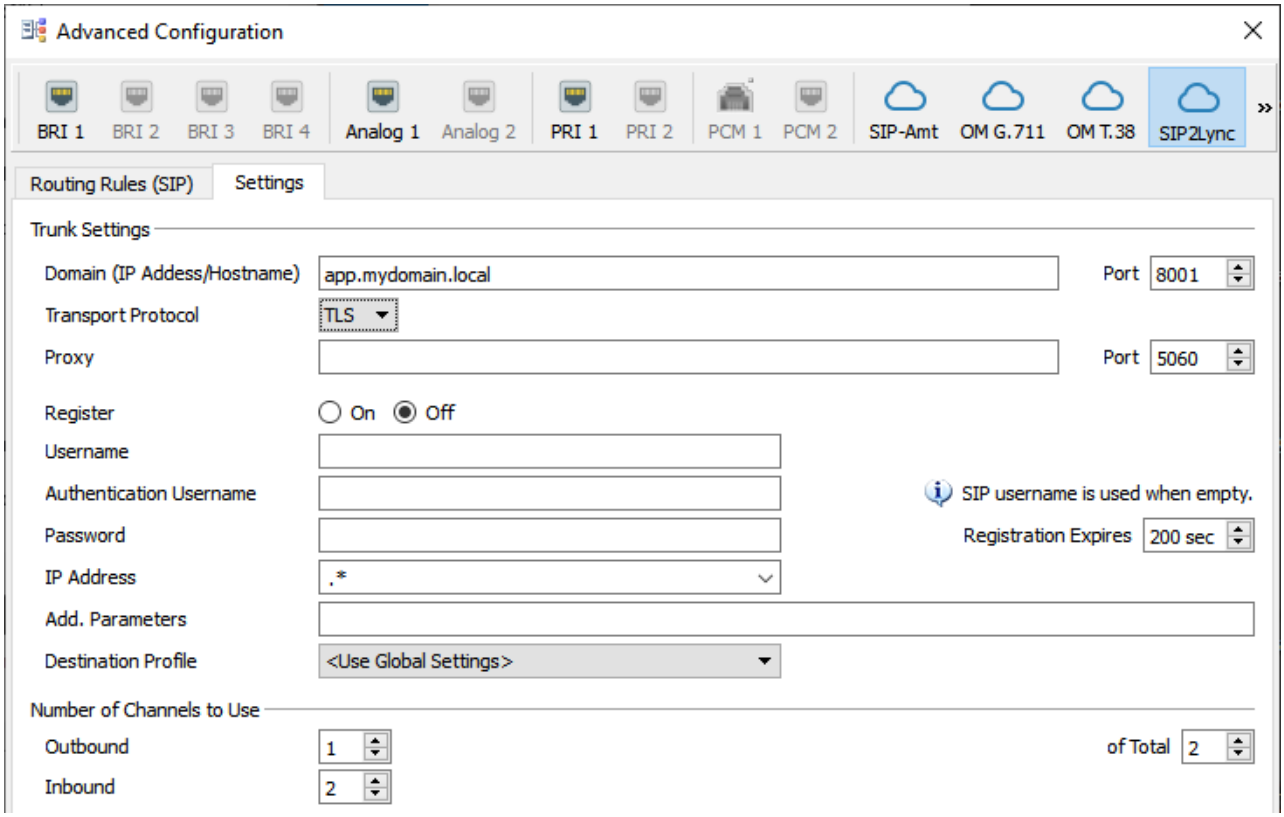
3.1. Fax mit OfficeMaster DirectSIP und anderen FoIP-Gegenstellen

Wie bereits in Abschnitt 1 erwähnt, wird die „alte“ Ansteuerung mit der OMCUMS-Komponente im Multi-Trunk-Modus nicht mehr unterstützt. Stattdessen verhält sich die neue Firmware als Fax-Proxy, das heißt, jegliche Signalisierung bezüglich T.38 bzw. G.711 wird zur anderen Seite durchgereicht. Das Faxverhalten (T.38 Re-Invite senden / akzeptieren / ablehnen) wird also durch die beteiligten Gegenstellen gesteuert. Wenn sich beide Seiten auf T.38 einigen, werden T.38-UDPTL-Pakete transparent durchgereicht, ansonsten wird über G.711-Pass-Through gefaxt.

3.2. Verwendung mit SIP2Lync

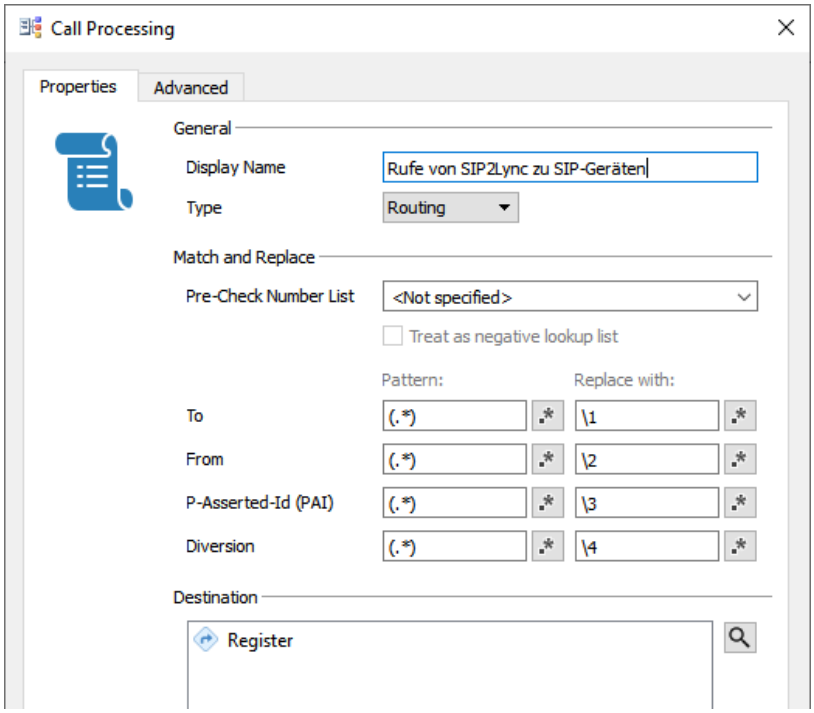
Der SIP2Lync-Server wird zunächst als eigener Trunk eingerichtet.

Beispiel:

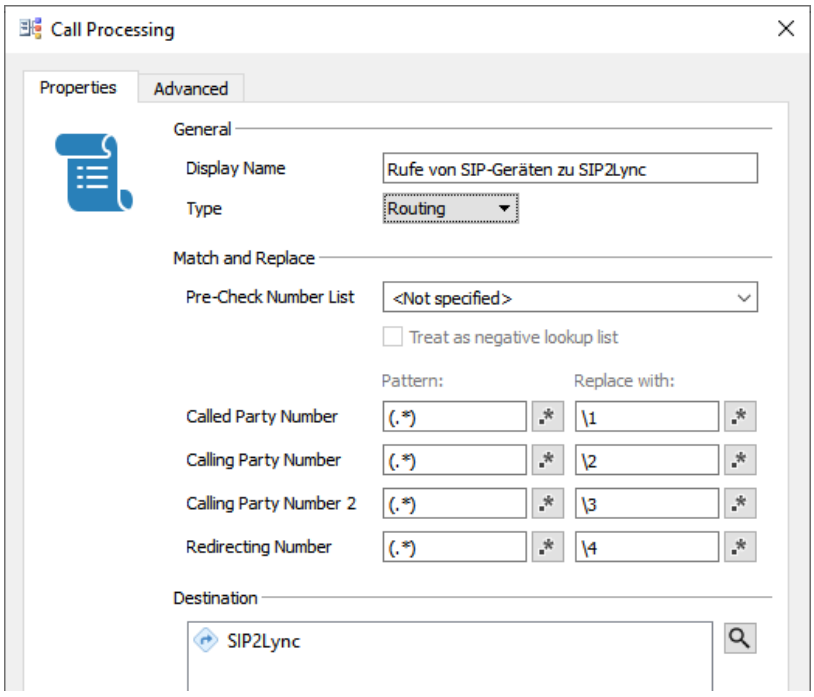


Des Weiteren wird ein „Register“ Trunk für die SIP-Geräte verwendet. Nun muss lediglich zwischen beiden Trunks jeweils eine Regel hinzugefügt werden.

Im SIP2Lync Trunk:



Im „Register“ Trunk:



Wie bisher muss noch die globale SIP2Lync Einstellung konfiguriert werden – mehr ist nicht erforderlich.

4. Troubleshooting

In diesem Abschnitt gibt es Hilfestellungen zur Diagnose, wenn mal etwas nicht so klappt wie beabsichtigt. Wesentliche Basis sind dabei Syslog-Dateien – das Logging sollte deshalb stets aktiviert sein! Für die Analyse von Logdateien wird der mitinstallierte „Syslog-Analyzer“ (syslogwin.exe) verwendet. Es empfiehlt sich, in diesem Tool die Einstellung Edit → „Treat all as Regular Expression“ zu aktivierten – dann werden Suchbegriffe immer als Reguläre Ausdrücke interpretiert (alternativ kann ein Suchstring mit einem Pluszeichen beginnen, dann wird der Rest ebenfalls als Regulärer Ausdruck verarbeitet). In den folgenden Beispielen wird davon ausgegangen, dass die hier beschriebene Einstellung aktiv ist.

4.1. Zuordnung eingehender SIP-Calls

Wenn Rufe nicht so verarbeitet werden wie erwartet, liegt es oft daran, dass das eingehende INVITE nicht dem korrekten Trunk zugeordnet und deshalb das falsche Regelwerk verwendet wird. Für die Zuordnung werden IP-Adressen sowie Domain-Namen aus SIP Headern mit den Trunkkonfigurationen verglichen. Zusätzlich muss in einem Trunk, der auf diese Weise gefunden wurde, mindestens eine Regel vorhanden sein, deren Bedingungen erfüllt sind. Dadurch ist es möglich, auch mehrere Trunks mit denselben Domains zu verwenden, die unterschiedliche Rufnummernbereiche abdecken. Diese Rufnummernkreise müssen in den Rufregeln entsprechend selektiert werden. Sollte eine Zuordnung nicht möglich sein, kann zusätzlich die Absenderadresse bzw. ein Adressbereich im Feld „IP Address“ als Regulärer Ausdruck vorgegeben werden (Default „.*“, also beliebige Adressen). Beispiel: **`10\.10\..*`** für Adressen im Bereich 10.10.0.0/16

Um die Zuordnung zu Trunks im Syslog zu überprüfen, muss zunächst das eingehende INVITE gefunden werden. Die Eingabe von „Rx: INV“ reicht aus, um alle eingehenden Rufe aufzulisten. Durch Anklicken des zu untersuchenden Anrufs wird das INVITE im oberen Fenster angezeigt. Die Verarbeitung der konfigurierten Trunks (von links nach rechts) und deren Regeln ist unmittelbar vor dem INVITE zu sehen und kann dort durch Zurückscrollen gefunden werden.

Beispiel: Anruf über Telekom SIP-Trunk, der zweimal existiert für verschiedene Rufnummern (gekürzt)

Die ersten zwei Trunks sind nicht aktiv:

```
ROUTE: check  D-Channel 1
ROUTE: check  D-Channel 2
```

Trunk 3 ist aktiv, verwendet jedoch nicht die Telekom-Domäne:

```
ROUTE: check  D-Channel 3
ROUTE: check  D-Channel 3 is active
ROUTE: trunk based destination route: 4d trunk fromHost test if "sip-trunk.telekom.de" is contained
in "10.6.1.33" (10.6.1.33)
```

Trunk 4 ist aktiv und für Telekom konfiguriert, es gibt aber keine passende Regel zur Rufnummer

```
ROUTE: check  D-Channel 4
ROUTE: check  D-Channel 4 is active
ROUTE: trunk based destination route: 4d trunk fromHost test if "sip-trunk.telekom.de" is contained
in "sip-trunk.telekom.de" (sip-trunk.telekom.de)
ROUTE: trunk based destination route: 4e trunk fromHost found sip-trunk.telekom.de
ROUTE: RouteIsdnInitiated("+49301234567,+491729876543,,") startAfter='nil' ConfigId=4
ROUTE: test 1 To Skype4B Hans "+49301234567,+491729876543,,","^(.*2),(.*),(.*),(.*)"
ROUTE: test 2 DirectSIP T.38 pass-through "+49301234567,+491729876543,,","^(.*3),(.*),(.*),(.*)"
```

Trunk 5 ist aktiv und für Telekom konfiguriert, es gibt auch eine passende Regel

```
ROUTE: check  D-Channel 5
ROUTE: check  D-Channel 5 is active
ROUTE: trunk based destination route: 4d trunk fromHost test if "sip-trunk.telekom.de" is contained
in "sip-trunk.telekom.de" (sip-trunk.telekom.de)
ROUTE: trunk based destination route: 4e trunk fromHost found sip-trunk.telekom.de
ROUTE: RouteIsdnInitiated("+49301234567,+491729876543,,") startAfter='nil' ConfigId=5
ROUTE: test 1 To Skype4B Hans "+49301234567,+491729876543,,","^(.*7),(.*),(.*),(.*)"
ROUTE: found 1 To Skype4B Hans "+4930455946","+491729876543","","",""
          string_replacedCallingPartyNumber2=\3
          string_replacedCalledPartyNumber=+4930455946
          string_Destination=trunk
          string_RegularExpressionForIpAddressMatch=.*
          string_replacedRedirectedPartyNumber=\4
          bool_InvertNumberList=false
          string_RegularExpression=^(.*1),(.*),(.*),(.*)
          string_disabled=no
          struct_DestinationList
             1
                string_Id=2004.a
          string_NumberList=
          string_replacedCallingPartyNumber1=\2
          string_Description=To Skype4B Hans
          ushort_DestinationSelectionMode=0
          string_AdditionalParameters=
          string_action=stop
          struct_DestinationId
             1
                destination=7
ROUTE: check  D-Channel 6
…
```

Am Ende wird die Liste der gefundenen Ziel-Trunks angegeben:

```
ROUTE: D-Channel list is ,7,
```

4.2. Syslog Anruf-Analyse

Zur Auswertung einzelner SIP-Calls müssen diese zunächst im Syslog gefunden werden. Als Suchbegriff kann eine beteiligte Rufnummer dienen, möglich sind auch Suchbegriffe wie „Tx: INVITE“ für abgehende Rufe oder „Rx: INVITE“ für ankommende Rufe. In beiden Fällen ist es hilfreich, den Anrufzeitpunkt mit auszuwerten. Durch Rechtsklick innerhalb einer SIP-Nachricht erscheint ein Kontextmenü. Die Auswahl „Filter Call SIP Commands“ erzeugt automatisch einen passenden Suchbegriff, um die gesamte Konversation dieses Anrufs herauszufiltern. Per Klick auf einzelne Zeilen wird im oberen Fenster an die entsprechende Stelle im Syslog positioniert.

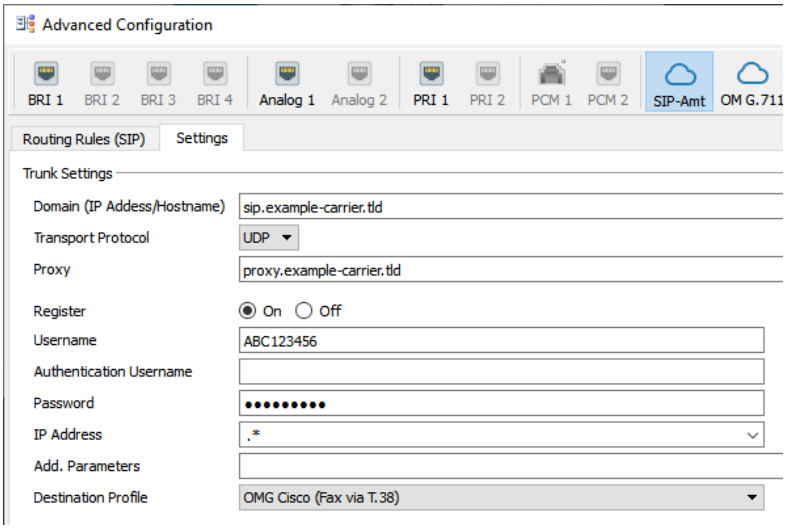
5. Spezial-Einstellungen

In bestimmten Situationen ist es erforderlich, ein vom Standard abweichendes besonderes Verhalten einzustellen, um z.B. bestimmte optionale SIP-Header zu verwenden, andere Abläufe (z.B. Fax mit oder ohne T.38 zu nutzen) und so weiter. Hierfür gibt es zwei verschiedene Möglichkeiten: Parameter-Profile und Zusatz-Parameter.

5.1. Parameter-Profile

Diese existieren bereits in früheren Firmwarevarianten und dienen dazu, mehrere Parameter zu gruppieren. Ein solcher Parametersatz kann über seinen Namen direkt im Konfigurationsprogramm ausgewählt werden.

Beispiel (Destination Profile in Trunk Settings):



Die Liste der wählbaren Parameter-Profile kann bei Bedarf erweitert werden. Wie das geht und welche Parameter verwendbar sind, beschreibt eine separate Dokumentation für Spezialisten („OfficeMaster Gate Previously Undocumented Parameters“).

5.2. Zusatz-Parameter

An verschiedenen Stellen im Konfigurationstool befindet sich das Feld „Add. Parameters“ (Addtional Parameters = Zusatz-Parameter). Hier können einzelne Einstellungen gezielt vorgenommen werden, auch mehrere solcher Werte sind kombinierbar. Bedeutung der Parameter und Syntax sind ebenfalls in dem in Anschnitt 5.1 erwähnten Dokument beschrieben.

5.3. Parameter pro Trunk / pro Regel

Parameter können an verschiedenen Stellen konfiguriert werden:

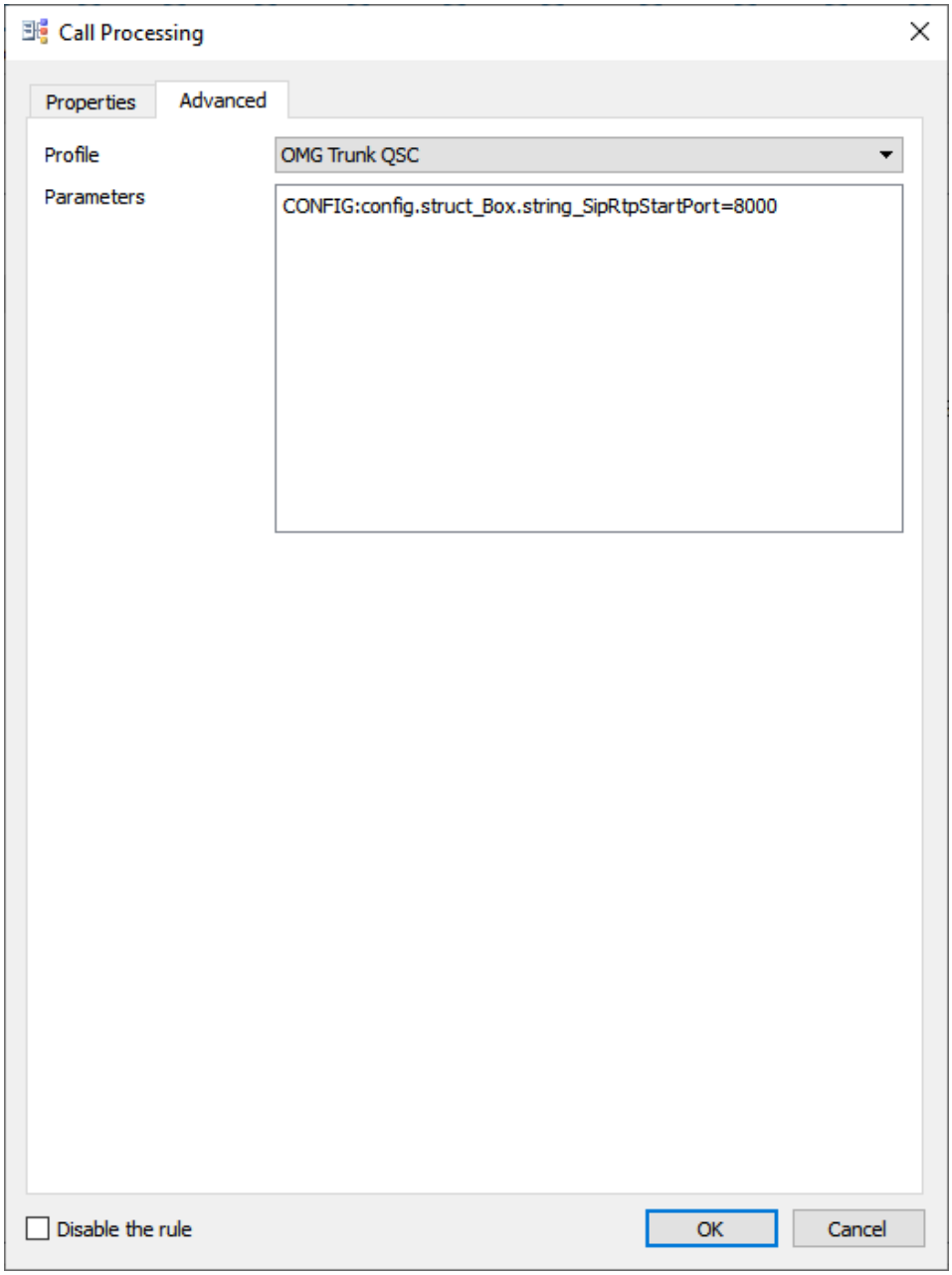
- In den Trunk-Settings
- In einer einzelnen Regel

5.3.1. Parameter in Trunk-Settings

Parameter-Profile und Zusatz-Parameter mit dem Präfix „CONFIG:“ gelten für den jeweiligen Trunk sowohl für eingehende als auch für ausgehende Rufe. Sollten Zusatz-Parameter nur für eingehende oder nur für ausgehende Rufe gelten, muss statt „CONFIG:“ das Präfix „IN:“ bzw. „OUT:“ verwendet werden.

5.3.2. Parameter in einer Regel

Parameter-Profile und/oder Zusatz-Parameter werden auf der Registerkarte „Advanced“ angegeben:



Die Einstellungen pro Regel gelten jeweils für die eingehende, nicht aber für die weitergehende Verbindung!

6. Migrationsleitfaden OfficeMaster Gate Firmware 4.x auf 5.1

6.1. Einleitung

Beim Update eines OfficeMaster Gate sind eine Reihe von Punkten zu beachten. Dieses Dokument enthält die für diesen Updateprozess nötigen Informationen.

6.2. Unterstützte Geräte

Die Firmware 5.1. nutzt ein aktuelles 64 Bit Betriebssystem. Damit können leider nicht alle OfficeMaster Gate Geräte aktualisiert werden, da es relativ alte Geräte gibt, die nur einen 32 Bit Prozessor enthalten. Im Folgenden sind die Gateways gelistet, für welche die Firmware 5.1 Hardware-Unterstützung bietet:

- OfficeMaster Gate Advanced R2 (OMGA)
- OfficeMaster Gate 19“ mit UEFI-Unterstützung und Lieferdatum ab 1.1.2016 (Fujitsu PRIMERGY RX1330 und Fujitsu PRIMERGY RX100 S8 und neuer)
- OfficeMaster Gate Virtual Edition (OMGV) auf aktuellen Virtualisierungsumgebungen

Bei älteren/anderen Gateways kann kein Update durchgeführt werden. In diesem Fall kann die Firmware 5.1 nur über eine Neuanschaffung eingesetzt werden.

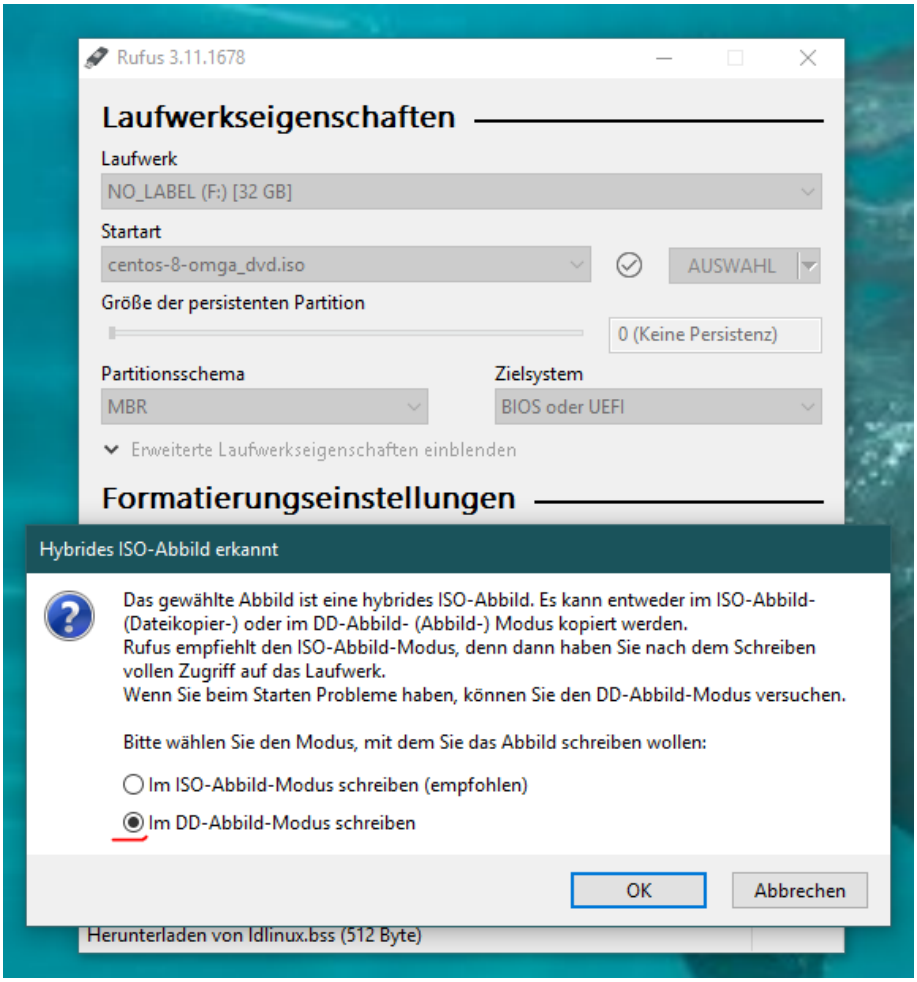
6.3. Update-Szenarien

Verschiedene Update-Szenarien werden unterstützt. Falls ein altes (silbernes) OfficeMaster Gate durch ein OfficeMaster Gate Advanced R2 ersetzt werden soll, kann der Abschnitt „Installation der Firmware 5.1“ übersprungen werden.
Für ein Inplace-Update eines vorhandenen Gateways kann diese Anleitung benutzt werden. Der Abschnitt „Austausch der Hardware“ kann dann weggelassen werden und die Bezeichnungen „altes Gateway“ und „neues Gateway“ beziehen sich auf die gleiche Hardware.
Ein weiteres Szenario ist ein Update eines vorhandenen OfficeMaster Gate Advanced R2 von Firmware 4 auf 5 mit dem Ziel, die Einstellungen eines anderen, älteren Gateways zu übernehmen. Hierbei müssen die Konfigurationen beider Gateways gesichert werden und zuerst die Konfiguration des OfficeMaster Gate Advanced wiederhergestellt werden. Dieser Schritt ist wichtig, um die Basislizenz und etwaige Erweiterungslizenzen das OfficeMaster Gate Advanced über das Firmware-Upgrade zu erhalten. Falls die Basislizenzen verloren gehen, können diese nur durch Kontakt mit dem Support-Team der Ferrari electronic AG wiederhergestellt werden.

6.4. Vorbereitungen

Die Firmware 5.1 benötigt zur Konfiguration eine aktuelle OfficeMaster Gate Konfiguration (>=7.1.3-12). Diese kann unter ferrari-electronic.de/downloads.html (Filter „Unified Communications“ und „Software“) heruntergeladen und danach installiert werden.

Einen Boot-fähigen USB-Stick mit dem Installations-Image der Firmware 5.1 erstellen. Dazu kann unter Windows z.B. das Programm Rufus verwendet werden. Zuerst muss das Installations-Image von https://download.ferrari-electronic.de/Firmware5/ heruntergeladen werden. Danach ist mit Rufus mit der Option DD-Abbild-Modus der USB-Stick zu beschreiben. Siehe Abbildung.



6.5. Backup der Konfiguration des alten Gateways

Konfiguration der bisherigen Firmware 4 vollständig sichern. Dazu die OfficeMaster Gate Konfiguration öffnen, eine Verbindung zum zu sichernden Gateway herstellen und den Menüpunkt „Datei -> Sicherung… -> Alle relevanten Daten (als ZIP Datei)…“ auswählen.

Falls auf dem zu aktualisierenden Gateway auch ein OfficeMaster Call Recording installiert ist und übernommen werden soll, die Verzeichnisse

/etc/EyeSDN-USB4

/data/eyesdn

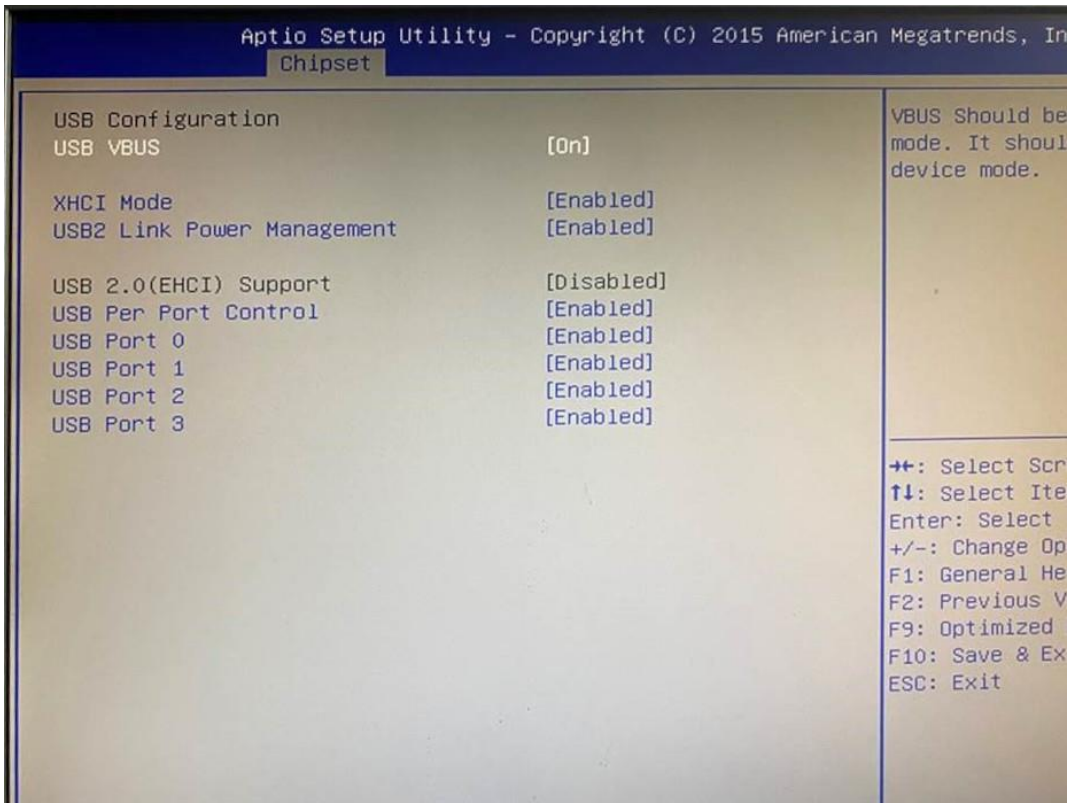
/var/spool/EyeSDN-USB4

inkl. aller Unterverzeichnisse und Dateien per WinSCP oder ähnlichen sichern.

Falls im OfficeMaster Gate ssh-Keys hinterlegt wurden, sind diese (falls nötig) manuell zu sichern und nach dem Update wieder manuell einzuspielen.

6.6. Installation der Firmware 5.1

1. Vor der Installation ist das Gateway auszuschalten (das Backup der Konfiguration sollte bereits erfolgt sein).
2. Der Update-Prozess benötigt eine USB-Tastatur und einen Bildschirm. Diese sind anzuschließen.
3. Das Gateway nun wieder einschalten. Im Fall eines OMGA sind für den Update-Prozess **beide Netzteile gleichzeitig** zu verwenden.
4. Nach dem Einschalten das BIOS-Setup aufrufen (je nach System Entf-Taste oder F11 drücken).
5. Sicherstellen dass EFI-Boot aktiviert ist. Bei einem OMGA muss außerdem sichergestellt werden, dass die Einstellungen unter „Chipset -> Southbridge -> USB Configuration“ identisch zur Abbildung gesetzt sind. **Falls die USB-Einstellungen nicht korrekt sind, wird der USB Stick oder das EFI-Boot-Image nicht erkannt bzw. das Abschalten verhindert.**
   Bitte auch überprüfen, ob unter „Advanced -> Watchdog“ der POST- und Runtime-Watchdog deaktiviert ist. **Falls der Watchdog aktiv ist, kann die Installation nicht fertiggestellt werden, da das Gateway vorher durchstartet.**



6. Recovery USB-Stick in das zu aktualisierende Gateway einstecken.
7. Gerät neu starten und den Abschluss der Installation abwarten. Das Gateway sollte sich nach Abschluss der Installation abschalten. Ist dies nach ca. 40 Min. noch nicht erfolgt, aber die Meldung „Starting Shutdown“ auf der Konsole zu erkennen, kann das Gerät manuell abgeschaltet werden.
8. In jedem Fall vor dem Neustart den USB-Stick abziehen!!!
9. OMGA neu starten lassen und den Login-Prompt abwarten, aber nicht Einloggen, denn es erfolgt automatisch ein weiterer Reboot nach ca. 30 Sek.
10. Ist der Neustart des OMGA abgeschlossen, erscheint das „omgmenu“ auf der Konsole.
11. An der Konsole (ggf. anmelden, Benutzer root, Passwort omc) und das OMGMENU mit den Tasten <m> und <b> beenden.

12. Das Kommando „ip a“ eingeben und die per DHCP vergebene IP-Adresse des OMGA notieren.
13. Damit ist die Installation der neuen Firmware abgeschlossen und diese kann nun konfiguriert werden.

6.7. Austausch der Hardware (bei Wechsel der Gateway-Hardware)

Nach dem Sichern der Konfiguration des alten Gateways kann dieses vom Netz und allen Kabeln getrennt werden. Falls das alte Gateway nicht vom Ethernet getrennt wird, kann es bei Übernahme der alten Einstellungen in das neue Gateway zu einem IP-Adresskonflikt kommen (falls statische IP-Adresse genutzt wurde). Also entweder die Adresse des alten Gateways nach sichern der Konfiguration ändern oder das Netzwerkkabel herausziehen.
Die Kabel bitte an die neue Austauschhardware anschließen und das neue Gateway mit der Stromversorgung verbinden. Es sollte dann automatisch starten und nach kurzer Zeit mit der OfficeMaster Gate Konfiguration auffindbar sein.

6.8. Einspielen der alten Konfiguration in ein neues Gateway

1. Das OfficeMaster Gate Konfigurationsprogramm öffnen mit der notierten IP-Adresse verbinden.
2. Über den Menüpunkt „Datei -> Wiederherstellen…“ das beim Backup der alten Konfiguration erstellte ZIP-Archiv öffnen und wiederherstellen.
3. Nach dem automatisch erfolgten Reboot erneut mit dem OMGA verbinden. Dabei ist zu beachten, dass sich durch das Einspielen der alten Konfiguration die IP-Adresse auf die des alten Gateways ändern kann.
4. Sofern ein selbst gewählter Hostname verwendet wurde, diesen wieder über das OfficeMaster Gate Konfigurationsprogramm einstellen (Achtung: Bei Verwendung von TLS muss dieser den Zertifikaten entsprechen, andernfalls müssen neue Zertifikate erstellt werden).
5. Handelt es sich um ein neues OMGA, dass ein bisheriges classic OMG ersetzt, können nun optionale NEUE (nicht die bisherigen eines classic OMG) Erweiterungslizenzen eingespielt werden.

6.9. Wiederherstellen der Call Recording Funktion (optional)

1. Mittels WinSCP die unter Punkt 2 / Backup gesicherten Verzeichnisse an ursprünglicher Stelle wiederherstellen.
2. Mittels WinSCP die Datei db.lock sowie die Dateien warm* im Verzeichnis /var/spool/EyeSDN-USB4/recordings löschen.
3. Mittels WinSCP die Datei /etc/EyeSDN-USB4/registry.xml nach /data/eyesdn/registry.xml kopieren.
4. Das unter Call Recording | Ferrari electronic AG (ferrari-electronic.de) erhältliche aktuelle Call-Recording Package als manuelles Firmware-Update mit dem OfficeMaster Gate Konfigurationsprogramm installieren.
5. Das OMGA neu starten.
6. Die Call-Recording Software auf dem Windows PCs aktualisieren (Sammeldienst und Client-Programme).
7. Die ggf. notwendige Update-Lizenz für das Call-Recording über den Mitschnittfinder installieren und aktivieren.

6.10. Funktionstest

1. Die Fax- und SMS-Funktion kann über die OfficeMaster Suite getestet werden.
2. Die Telefoniefunktion sollte über Testanrufe aus der Skype for Business-Umgebung getestet werden.
3. Bei vorhandenem Call Recording sollten (je nach Regelwerk) die Testanrufe zu Mitschnitten führen.

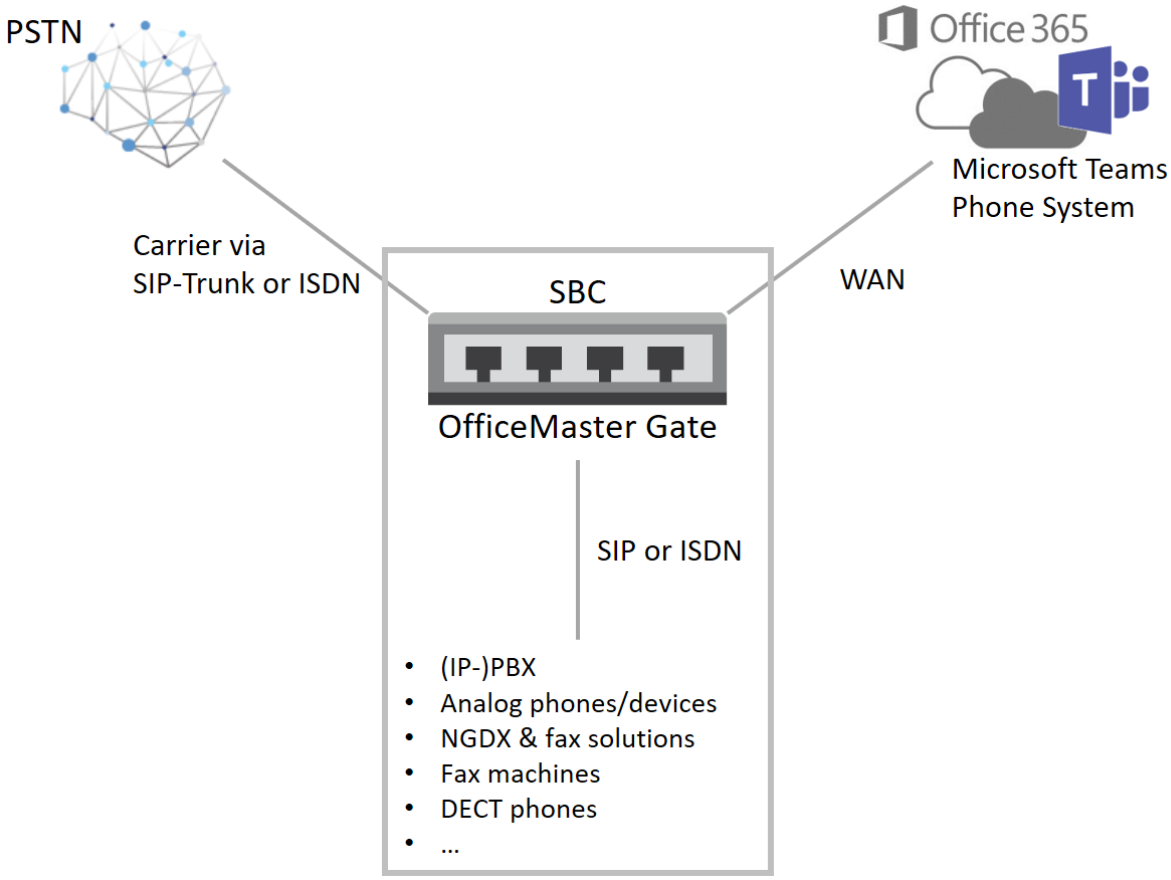
7. Einrichtung mit Microsoft Teams Direct Routing

7.1. Einführung

Microsoft Phone System Direct Routing ist eine elegante Lösung zur Unterstützung der Cloud-basierten Telefonie mit Microsoft Teams zusammen mit der PSTN-Konnektivität vor Ort. Somit können Kunden nicht nur ihre bestehenden SIP- oder ISDN-Trunks nutzen, sondern auch alle Arten von lokalen Kommunikationsinfrastrukturen integrieren, einschließlich:

- Analoge Geräte
- Notfalltelefone in Aufzügen
- Faxgeräte und Faxserver
- Bestehende PBX-Systeme
- Contact-Center-Lösungen
- DECT-Telefone
- …

Im Vergleich zu früheren Angeboten ist das Direct Routing viel einfacher - es benötigt nur einen SBC, um eine Verbindung zwischen der Infrastruktur von Microsoft Teams in Office 365 und lokalen Geräten und Leitungen herzustellen.



7.1.1. Anforderungen im Amt 365

Wichtige Informationen zur Planung des Direct Routing finden Sie hier:
https://docs.microsoft.com/en-us/MicrosoftTeams/direct-routing-plan

Die Konfiguration ist hier ausführlich dokumentiert:
https://docs.microsoft.com/en-us/MicrosoftTeams/direct-routing-configure

Im Allgemeinen sind die Anforderungen:

- Büro 365 Tenant mit ordnungsgemäßer Lizenzierung
  - Lizenz für Telefonanlage erforderlich (in E5 enthalten, optional für E3), Skype für Business Online (Plan 2)
- User registrar
  - Der Benutzer muss im Office 365 angelegt sein
- Domains
  - Eine der im Office 365 registrierten Domains bildet die Basis für das SBC FQDN. Beispiel: *teamssbc.contoso.com*. Hinweis: onmicrosoft.com ist keine gültige Domain für diesen Zweck! Die Domäne kann sich von den den Benutzern zugewiesenen SIP-Domänen unterscheiden.

7.1.2. Anforderungen an die lokale SBC-Konfiguration

Voraussetzungen für den Einsatz und die Konfiguration von SBC sind:

- Session Border Controller (SBC) - wie in diesem Papier dokumentiert
- An den SBV angeschlossene Telefonleitungen - entweder direkt oder über eine vorhandene Telefonanlage
- Öffentliche IP-Adresse und FQDN mit DNS-Eintrag für den SBC
- Öffentliches vertrauenswürdiges Zertifikat für den SBV aus der Liste der unterstützten Behörden (Wildcard-Zertifikate werden unterstützt)
- Anschlusspunkte für direktes Routing (geografisch abgebildet):
    - sip.pstnhub.microsoft.com (höchste Priorität)
    - sip2.pstnhub.microsoft.com (sekundärer FQDN)
    - sip3.pstnhub.microsoft.com (tertiärer FQDN)
- Firewall-IP-Adressen und Ports für Direct Routing-Medien (SIP-Proxy und Medien)
- Medientransportprofil (RTP/SAVP)
- Firewall-IP-Adressen und -Ports für Microsoft-Team-Medien

7.2. Konfigurieren Sie Office 365 Tenant für Microsoft Teams Direct Routing

Die erforderlichen Schritte sind hier ausführlich dokumentiert: https://docs.microsoft.com/en-us/MicrosoftTeams/direct-routing-configure

7.2.1. Verbindung mit Skype für Unternehmen online über PowerShell herstellen

Nachdem die Verbindung erfolgreich hergestellt wurde, kann die Liste der Befehle zur Verwaltung des SBC durch Ausführen des Befehls "*gcm *onlinePSTNGateway*" in der PowerShell-Sitzung gefunden werden.

7.2.2. Koppeln Sie den SBV mit dem Mieter

Mit dem PowerShell-Cmdlet "*New-CsOnlinePSTNGateway*" wird der SBC mit dem Mieter verknüpft.

7.2.3. Validieren Sie die Paarung

Verwenden Sie "*Get-CsOnlinePSTNGateway"*, um zu sehen, ob der SBC in der Liste der gekoppelten SBCs vorhanden ist.
Aktivieren Sie SIP-OPTIONEN in den OfficeMaster VoIP-Parametern (Intervall auf 60 Sekunden einstellen) und prüfen Sie die vom Syslog-Dienst geschriebenen Protokolle, wenn die OPTIONEN erfolgreich gesendet und bestätigt wurden. In diesem Fall sollten auch eingehende OPTIONS-Anforderungen gesehen werden.

7.2.4. Benutzer für den Direct Routing Service aktivieren

Die notwendigen Schritte sind:

- Benutzer in Office 365 anlegen und die Lizenz zuweisen
- Stellen Sie sicher, dass der Nutzer in Skype für Unternehmen Online heimisch ist.
- Konfigurieren Sie die Telefonnummer und aktivieren Sie die Sprach- und Voicemailfunktion des Unternehmens
- Konfigurieren Sie die Sprachweiterleitung

7.2.5. Anruf für Microsoft-Teams aktivieren

Wenn die Registerkarte "Anrufe" in Microsoft Teams nicht angezeigt wird, stellen Sie sicher, dass "*Private Anrufe zulassen*" in den Microsoft-Team-Einstellungen und -Diensten des Mieters auf "*Ein"* gesetzt ist.

7.3. OfficeMaster Gate SBC-Konfiguration

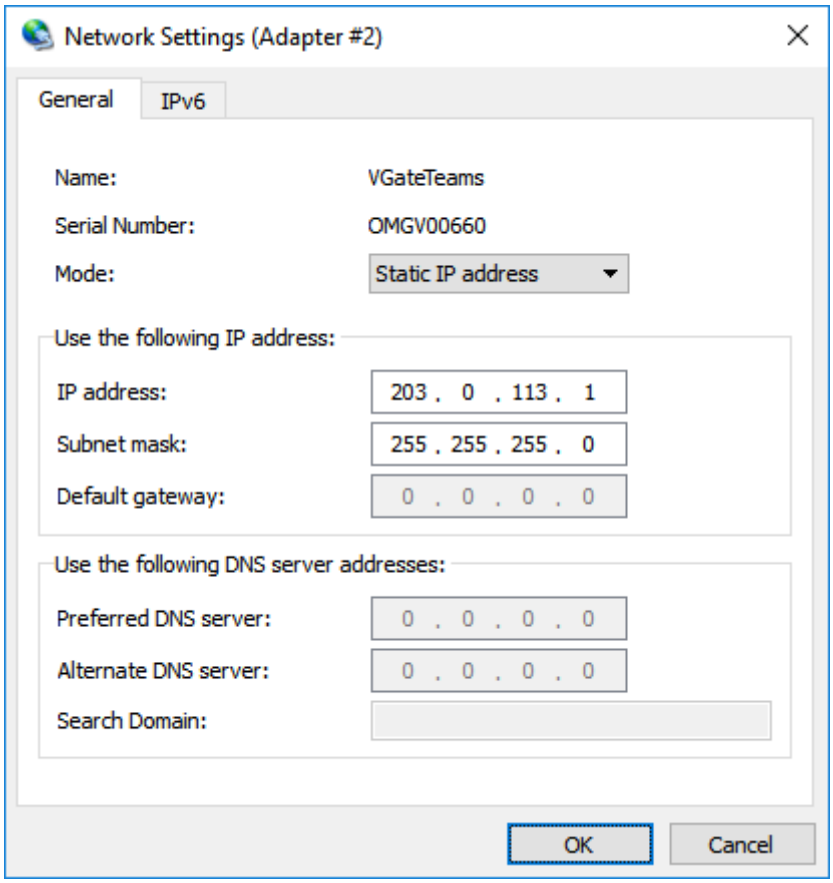
7.3.1. Voraussetzungen für OfficeMaster Gate

Es können alle Hardware- und virtuellen Versionen von OfficeMaster Gate, die mit der Firmware 5 und höher kompatibel sind, verwendet werden. Es werden Firmware-Versionen ab 5.0 und höher unterstützt (einschließlich Media Bypass!).
Zusätzlich werden SIP-Line-Lizenzen benötigt. Zur Konfiguration wird das OfficeMaster Gate Konfigurationstool 6.26.1474 oder neuer benötigt!

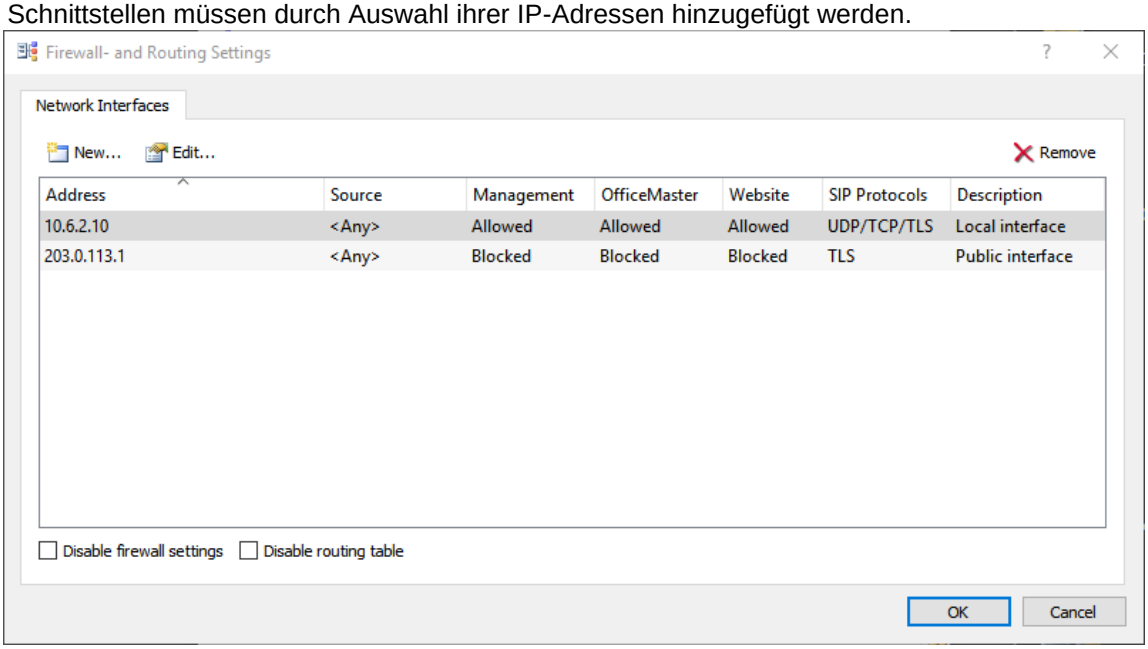
7.3.2. Netzwerk- und Firewall-Konfiguration

Die erste Schnittstelle sollte eine lokale IP-Adresse aus dem internen Netzwerk erhalten. Außerdem sollten das DNS und das Standard-Gateway auf interne Ressourcen verweisen.
Für die Verbindung mit Microsoft Teams SBC muss die zweite Schnittstelle ("*Adapter #2*...") mit einer öffentlichen IP-Adresse konfiguriert werden.

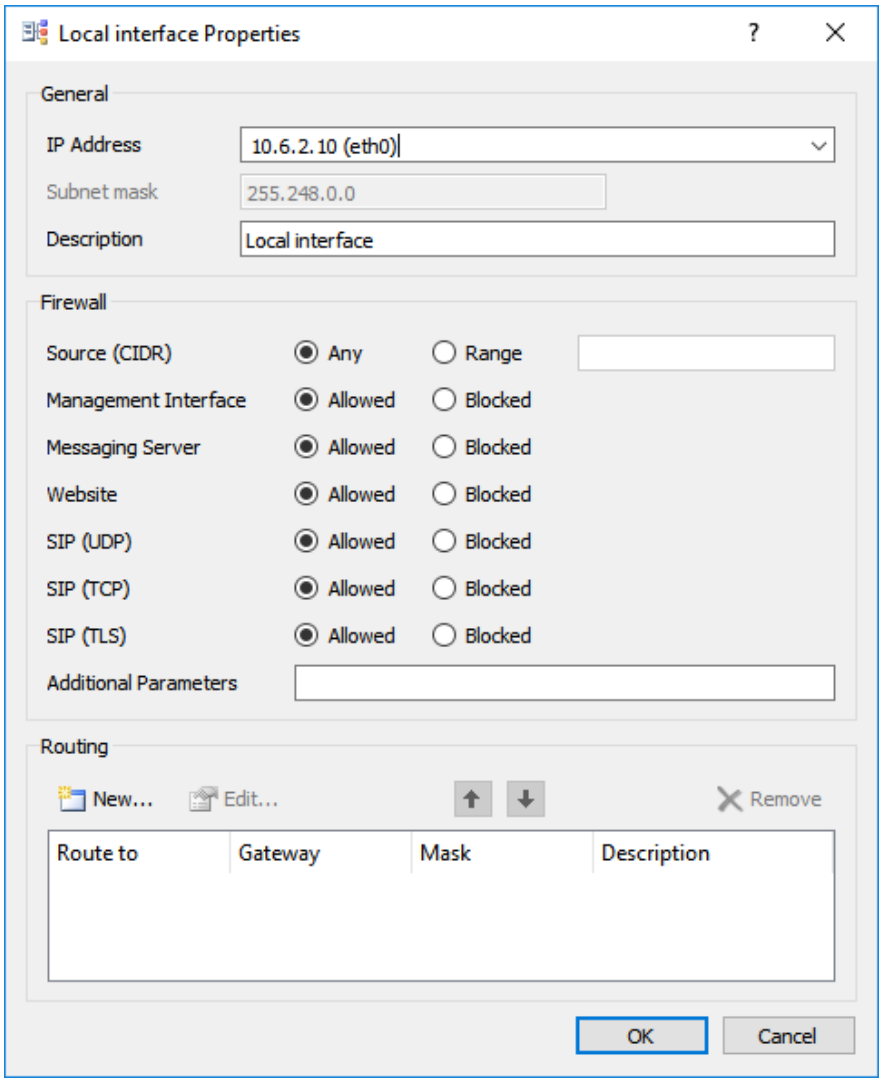
Beispiel:



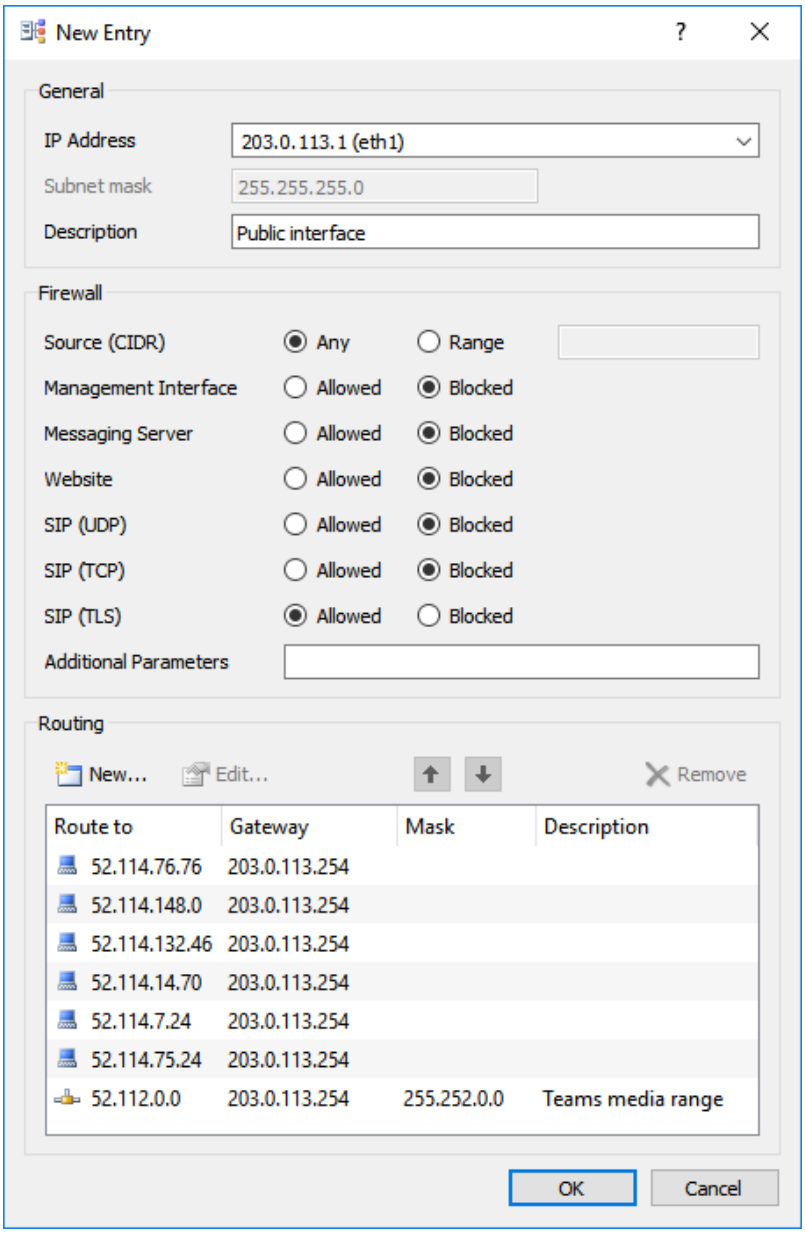
Jetzt müssen statische Routen auf die öffentlichen IP-Adressen für externen SIP- und Medienverkehr zeigen. Bevor diese Routen konfiguriert werden können, muss die Firewall sowohl für interne als auch für externe Schnittstellen aktiviert werden. Dies geschieht durch Auswahl von "*Bearbeiten - Firewall/Routing... - Neu---*". Beide Schnittstellen müssen durch Auswahl ihrer IP-Adressen hinzugefügt werden.



In der Regel müssen interne Dienste nicht blockiert werden:



Externe Dienste erfordern mehr Einschränkungen - lassen Sie einfach eingehende SIP (TLS)-Verbindungen zu. Der gesamte andere Verkehr wird durch diese Einstellung blockiert. Um SIP- und Medienkommunikation zu ermöglichen, müssen alle bekannten Ziele separat definiert werden, um über die externe Schnittstelle geroutet zu werden. Daher würde der gesamte andere (nicht erlaubte) Verkehr nicht über die externe Schnittstelle laufen.



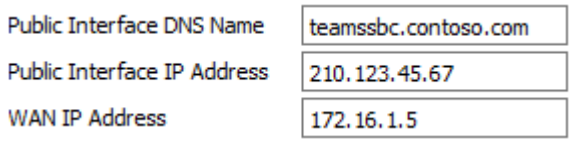
Diese IP-Adressen für SIP und das Subnetz für den Medienverkehr finden Sie in der Online-Dokumentation zu Microsoft Direct Routing.

7.3.3. SBC-Zertifikat installieren

Um das Zertifikat für den öffentlichen SBC-FQDN zu installieren, benötigen Sie sowohl das Zertifikat als auch den privaten Schlüssel in der Syntax von base64/PEM. Unter Windows können diese Daten bei Bedarf aus dem Zertifikatsviewer konvertiert werden. Das Zertifikat kann über das Konfigurationstool OfficeMaster Gate installiert werden. Um den privaten Schlüssel zu importieren, muss die pem-Datei nach "*/data*" als "*key.pem*" kopiert werden.

7.3.4. Globale Konfigurationseinstellungen

Die meisten Einstellungen in "*Edit/VoIP-Parameter*" können auf ihren Standardwerten belassen werden. Die Optionen sollten auf 60 Sekunden eingestellt werden. Sowohl der SBC-FQDN als auch die IP-Adressen müssen mit der neuesten **Version der OfficeMaster Gate-Konfiguration** konfiguriert werden:



Public Interface DNS Name: Das ist der FQDN des SBCs, wie er bei Teams hinterlegt ist.
Public Interface IP Address: Die öffentliche IP zu der FQDN auflöst
WAN IP Address: Die IP des Netzwerk-Ports über den der Netzwerkverkehr zu Teams erfolgt. Sollte der Port die Public IP haben, sind beide IPs identisch. Bei einem Setup mit NAT ist es entweder die DMZ-IP oder die IP des einzigen genutzten Ports.

7.3.5. Konfigurieren Sie die Routing-Regeln

Eine Beispielkonfiguration wird in *"teams-sample.ofg"* (Downloadcenter auf der Website der Ferrari electronic AG oder auf der Landingpage zur Firmware 5.0) zur Verfügung gestellt. Diese Datei kann mit dem OfficeMaster Gate Config-Tool geöffnet werden. Mindestens vier Stammobjekte müssen hinzugefügt werden:

- 1 Trunk zum SIP-Provider oder zur lokalen IPBX
- 3 Stämme zu Microsoft-Teams (sip, sip2 und sip3)

Anrufe von SIP-Trunk oder PBX sollten im Failover-Modus in der in der Beispielkonfiguration gezeigten Reihenfolge an diese Ziele geroutet werden: