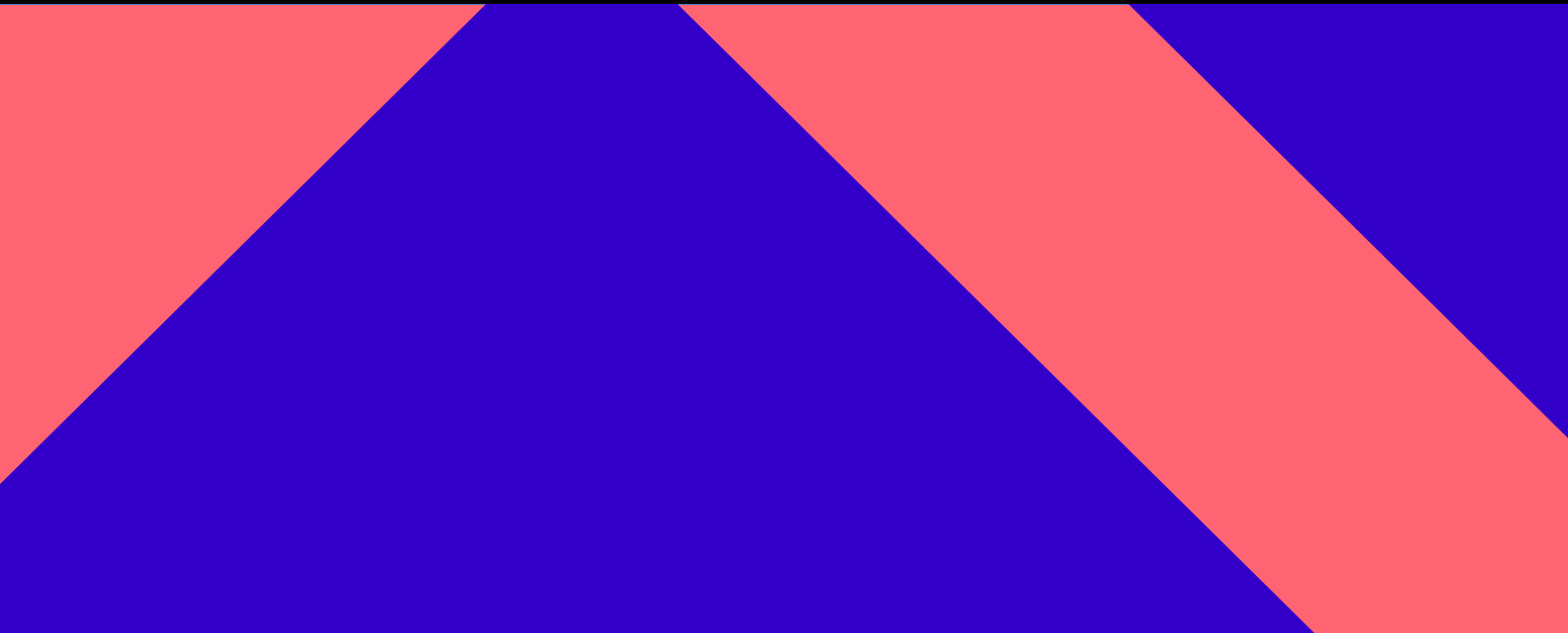


Technical Manual

SIP Trunk Flexx

Step into the cloud without updating your infrastructure



Content

Introduction	4
Geo redundancy	4
SIP Trunk Flexx credentials.....	5
Standard.....	5
Firewall settings	5
CLIP no screening	5
Phone number formats	6
Phone number transmission (incoming NFON to customer)	6
Phone number transmission (outgoing customer to NFON) – CLIP	6
Phone number suppression / calling line identification restriction.....	7
Service configuration	7
General	7
Configuration portal	7
Trunk sets.....	9
Number routing	9
Create PBX endpoint.....	10
PBX endpoint.....	10
PBX configuration	13
Certified vendors.....	13
Support	14
Additional functions	14
Function overview.....	14
High availability	16
Primary / backup	16
Round Robin (load balancing).....	16
Forking	17
Configuration of high availability	19
Call forwarding with and without redirect (302)	20
Backup service	20
Standard backup (N:1) / phone number based.....	20
DDI backup (N:N) / prefix-based number	21
Individual backup (N:M) / individual backup number	22
No backup	22
Backup service configuration	22
Inbound/outbound blacklist	23
eFax Service	25
Mail to fax.....	25
Fax-to-email	25
Sender Policy Framework.....	26
Fax service configuration.....	26
Mail-to-Fax Sending Procedure	27
Conference service.....	27
Conference service configuration.....	28
DTMF (according to RFC 2833)	29
Multi number management.....	29
International number management	30
Emergency call.....	30
Outgoing call barring.....	30
Fraud control.....	33

Authentication static mode	35
User agent checking	36
User agent check – NULL	37
User agent check – reject mismatched user agent	37
SIP password change	38
Protocol features, TLS/ SRTP	39
Customer portal	40
My contract	41
Administration	42
Microsoft Teams enablement – direct routing.....	43
Provisioning overview	44
Before getting started	44
Adding the SBC FQDN as an additional domain	44
Adding a new domain to Microsoft Office 365	44
Sharing the verification code with NFON.....	45
Completing the verification process.....	45
Activating the additional domain on Microsoft Office 365	45
Configuration for NFON standard integration	46
Microsoft Teams tenant configuration	46
NFON PBX endpoint configuration	46
Microsoft Teams enablement – Operator Connect	47
Customer on-bording via Operator Connect	47
Genesys cloud enablement	49
Provisioning overview	49
Configuration of Genesys PBX endpoint	49
Examples	51
Register PBX → NFON	52
Invite incoming call	53
INVITE NFON → PBX with CLIP (E.164 number format)	53
INVITE NFON → PBX with CLIP (national number format).....	54
INVITE NFON → PBX with CLIR.....	55
Invite outgoing call	56
INVITE PBX → NFON with CLIP (E.164 number format)	56
INVITE PBX → NFON with CLIP (national number format).....	57
INVITE PBX → NFON with CLIR.....	58
Emergency call.....	59
INVITE PBX → NFON emergency service number	59
Call forwarding with redirect (302)	60
302 MOVED TEMPORARILY PBX → NFON	60
DTMF	60
DTMF via FRC 2833	61
Terminology	62
Abbreviations.....	63

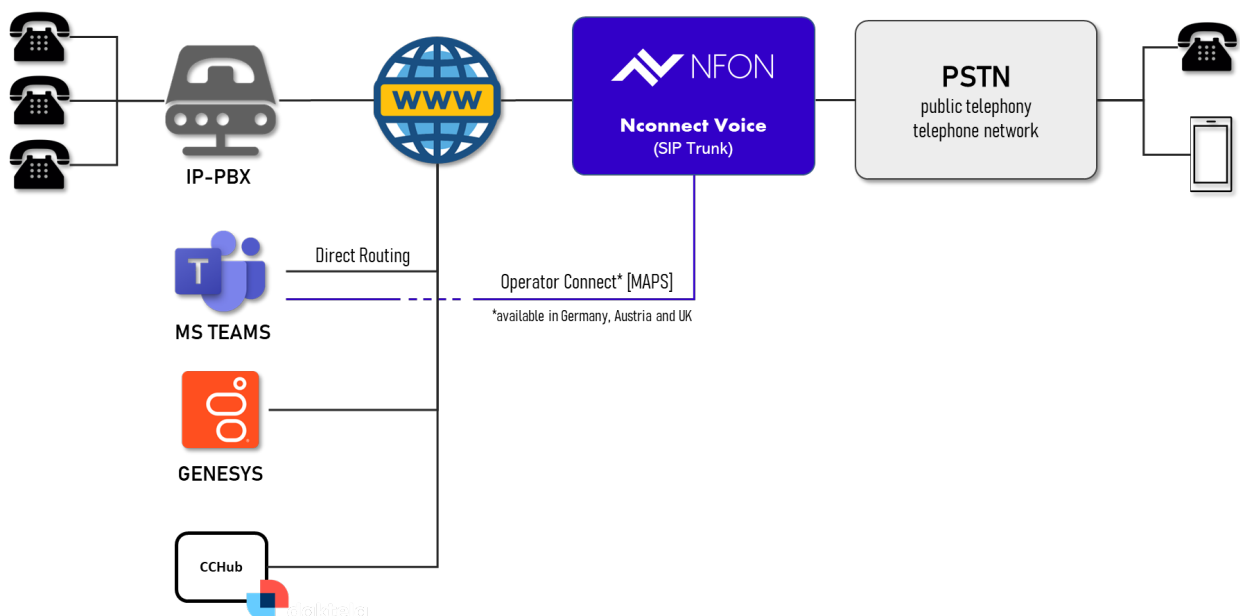
Introduction

This document will assist you in configuring your SIP Trunk Flexx. However, since the SIP protocol often leaves room for interpretation, the document can only serve as a guide and not be considered as binding for the PBX configuration. We recommend testing and documenting all important call scenarios beforehand.

If your telephone system is on the list of certified telephone systems, the vendor generally provides you with a template directly in the PBX setup menu or in their knowledgebase. You then can get the correct settings for SIP trunk by selecting them directly in the setup menu of the telephone system. Please make sure that your system is on the software version mentioned on the list.

If certification has already been completed by a partner or by the NFON Group, a comprehensive and easy-to-use configuration guideline will be available. For details, see chapter "Certified vendors" as well.

In the rare case that a PBX is not on the list of certified vendors, a manual configuration of the PBX endpoint and template will have to be done via the SIP Trunk Flexx configuration portal (see chapter Create PBX endpoint). If the PBX is not IP-capable, a media gateway will be required. In this case, the Beronet media gateway is recommended as it is certified. For all well-known vendors, a template can be activated in the configuration portal that ensures that the NFON server uses the SIP message formats and procedures appropriate for the PBX (see chapter Create PBX endpoint).



Geo redundancy

NFON operates multiple geo-redundant data centers which are built to completely take over from each other if necessary. All sites are interconnected through multiple high-capacity broadband connections to perform all failover scenarios at an instant. All sites have multiple high-capacity internet connections and high-performance pairings with the public internet. SIP trunks are handled on a geo-redundant, high-performance cluster of multiple call routers. Failover scenarios are implemented via data center and across data centers to provide maximum reliability. To accomplish this for each individual setup,

the customer's IP PBX shall only use a Fully Qualified Domain Name (FQDN) instead of individual IP addresses.

SIP Trunk Flexx credentials

SIP users are authenticated via the username / password credentials that will be sent to them after creation of the PBX endpoint. The user name for the PBX endpoint is automatically transferred from the portal and cannot be changed. The password will be sent via SMS to the technical contact named in the order.

The mobile number of the technical contact person can be changed by the partner or by the NFON Support if necessary.

The SMS simply says:

PBX endpoint: <pbx endpoint name>

K number: <K number> (ex. KCHND)

your password: *****



Please treat the SIP credentials confidentially. Stolen SIP credentials can be used for all types of frauds!

Alternatively, IP authentication (static mode) is supported, see chapter "Authentication static mode"

Standard

The technical implementation of NFON SIP Trunk Flexx is based on the SIP connect technical recommendation.

Firewall settings

For basic connectivity, firewall, router, switch and customer network settings, please check the "Leaflet Plug & Play": <https://www.nfon.com/en/systemspecifictopics/leaflet-plug-play/b-firewall-configurations>

Protocol	Target port	Purposes	Targets
UDP	123	NTP	All networks
UDP	53	DNS	Customer DNS server
UDP	all ports	SIP, RTP, T-38, FMC, etc.	109.68.96.0/21
TCP	all ports	SIP/TLS, SIP, FMC	109.68.96.0/21

CLIP no screening

CLIP no screening enables the transmission of an external call number that is not connected to the SIP

trunk. If this feature is enabled, the intended phone number can be communicated to the called party as a phone number using the phone number formats described above. If this feature is deactivated, only numbers that are connected to the SIP trunk can be transmitted. In addition, for legal reasons, a valid number from the SIP trunk must be specified in the PAI header, but this number is not displayed to the called party. All number ranges can be used by the customer and accepted by the system, with the exception of premium rate numbers and emergency numbers. Calls using these will be corrected regarding the originating number. Please note that there are country-specific regulations for the use of CLIP no screening. For further information on call number transfer, please refer to the chapter Call number transfer (outgoing customer to DTS) - CLIP. This feature is ordered together with the SIP trunk (free option).

Phone number formats

Phone number transmission (incoming NFON to customer)

Incoming phone numbers from NFON to the customer are either in the international format with a leading "+" or national format. The required format is defined within the configuration portal. For details, see chapter "Installation".

For example, see: Chapter "Examples: Invite incoming call"

Phone number transmission (outgoing customer to NFON) – CLIP

In general, NFON accepts the transmission of phone numbers in all fields (FROM, TO, P-Asserted Identity, P-Preferred Identity) in the following formats:

Country Code	SIP format
+49	<sip:+49894531234@siptrunk.cloud-cfg.com>
0049	<sip:0049894531234@siptrunk.cloud-cfg.com>
national	<sip:0894531234@siptrunk.cloud-cfg.com>

The following headers for presenting the Caller Number are accepted:

1. P-Preferred-Identity (PPI)
 2. FROM
 3. P-Asserted-Identity (PAI)
- If the "CLIP no screening" feature is not enabled, (see chapter CLIP no screening) all headers are checked and validated if the entries are correct. Otherwise they will be overwritten with a valid customer number.
 - If no PAI header is sent, it will be checked if the FROM or P-Preferred-Identity is a valid customer number, and this will be used for the PAI (PAI is set before sending the INVITE to the carrier). If the number is not valid, a random "valid" number from the assigned number block will be set.

In addition to the formats described above, NFON does allow the following local number formats as caller ID. Please be aware that this is accepted only if the SIP trunk is used for one national prefix only. In case several national prefixes are used, the number format needs to be international E.164.

SIP format	
Telephone number without local area code (LAC)	<sip:4531234@siptrunk.cloud-cfg.com>
Telephone number with local area code (LAC 089)	<sip:0894531234@siptrunk.cloud-cfg.com>

As the FROM / PAI is checked for each call, there are restrictions that do not allow the use of certain numbers, e.g. emergency or service numbers. When call attempts are made with restricted numbers in the FROM / PAI, towards the PSTN the PAI is overwritten with the customer's valid numbers.

Phone number suppression / calling line identification restriction

The caller ID can be suppressed (anonymous calling) for an outgoing call via two methods:

- customer can set "anonymous" in the FROM display name
- or set a Privacy: id header

In both cases the call will be signaled to the carrier as anonymous call. For example, see chapter Examples.

Service configuration

General

After ordering SIP Trunk Flexx, the customer will receive an order confirmation. NFON will also confirm their directory number block(s) – in this example no porting of an existing number from a different service supplier is assumed, but a new number block is allocated to the customer. In addition, the customer will receive access to the customer portal.

Configuration portal

The setup of the SIP Trunk Flexx as well as enabling and adaptation of additional features is done by the customer or partner from the configuration portal.

This can be accessed via the access portal: <https://siptrunk.nfon.com> with your username and password. (as alternative, in case it does not work, please use: <https://start.cloudya.com>)

As part of the order, the technical contact person named in the order form will receive an email that has the link to setup their password:

Welcome to Nconnect Voice

Dear John Doe,

we are pleased to welcome you to Nconnect Voice (SIP Trunk) as a user of NFON AG. Your personal account (jdoe) has just been created. To use the service, you just need to set your personal password at the following URL:
<https://siptrunk.nfon.com>

Set your password now

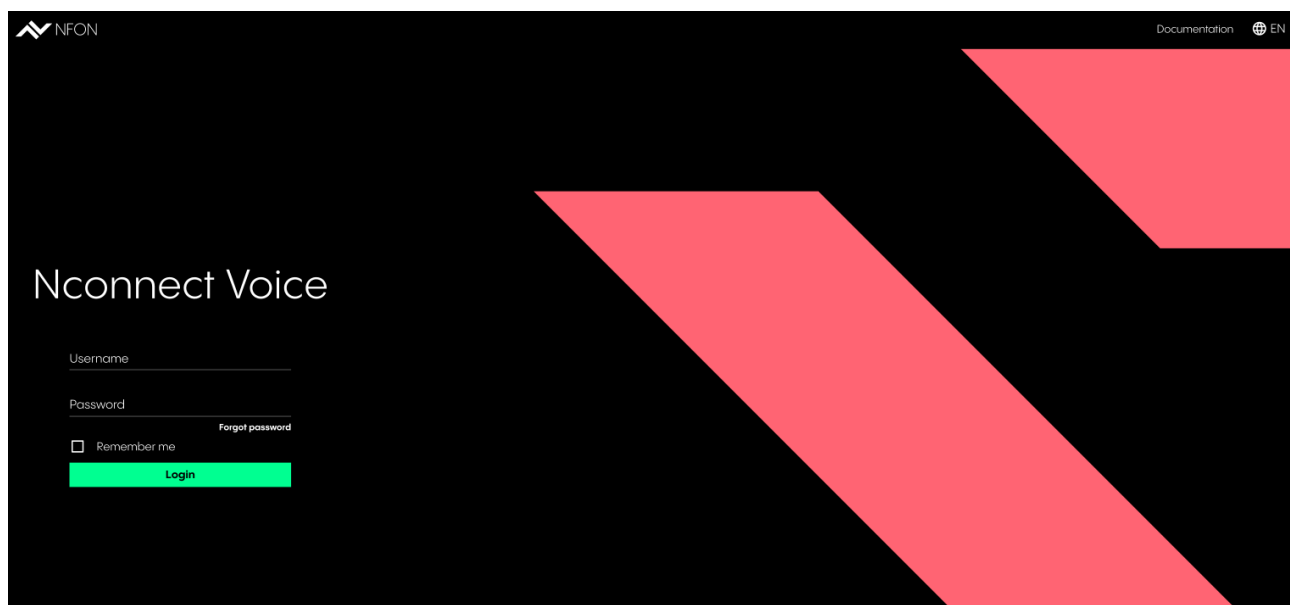
With your personal credentials, you can login at <https://siptrunk.nfon.com> from anywhere at any time.

This is an automatically generated email. Please do not reply directly.

If you have received this email by mistake, please ignore it or contact our support hotline on +44 (3300) 586366.

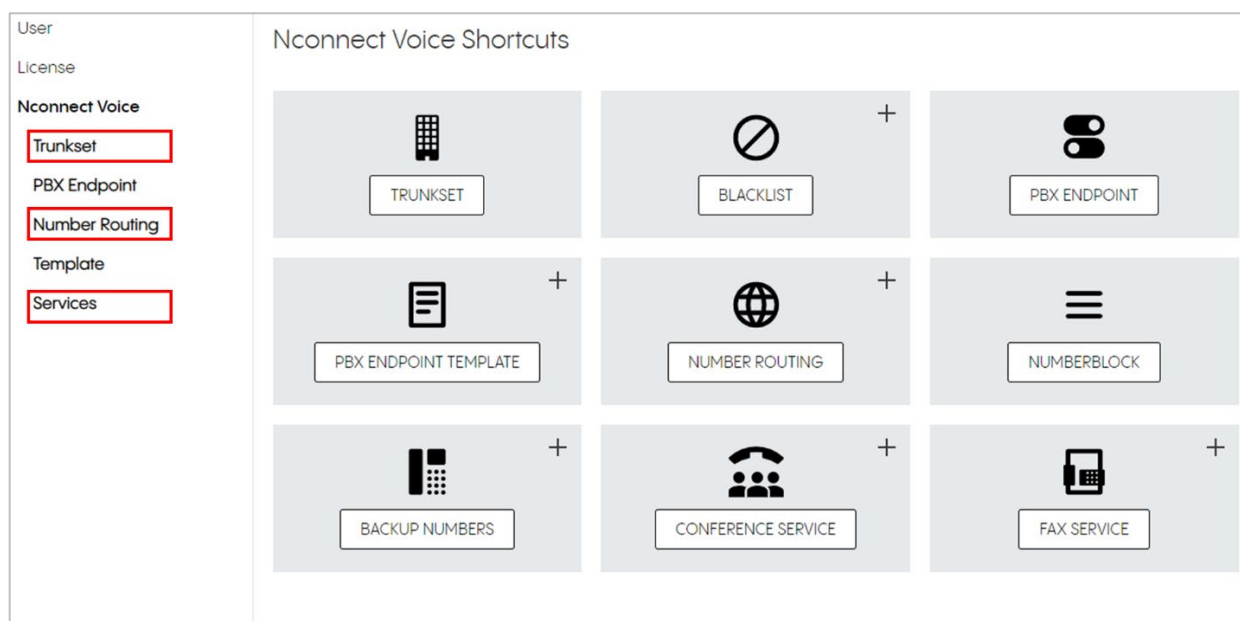
Any questions?
 You can find a quick start guide to our service and its features at
https://www.nfon.com/media/Service/Documentation/Manuals/Nconnect_Voice_2.0/Nconnect_Voice_2.0_Manual_GB.pdf.

Username is the email address. With those credentials you can log in to the portal:



When you open the portal for the first time, please check that the following items from your order are available:


- Trunk set
- Phone number
- Value added services



The Trunk sets and number blocks are available already as ordered. The administration for all the functions described below can be done from here.

From the "User" menu, it is possible to edit the user via the "Edit Pen" or delete them via the "Basket".

User License Nconnect Voice	User +				
	↑ Username	↑ Name	Extension	↑ App	↑ Admin
	test@nfon.com	TestUser	-	✓	

User Test User User data Permissions License Nconnect Voice	User data		 Restore password Cancel Save
	First name	Last name	
	Test	Test	
	Username	Language	
	test@nfon.com	English	

The invitation is sent out directly when creating a new user.

Trunk sets

When ordering the trunk set, the number of channels for this trunk set is defined. One or more PBXs (Premium) can be connected as endpoints with a trunk set.

Number routing

Number routing is used to determine the destinations, e.g. trunk sets, to which calls coming in from the PSTN are to be routed based on the destination number. The assignment is based on the longest-matching prefix. The available number blocks are visible from the sub- menu "Number block" of the "Number routing" menu:

User License Nconnect Voice Trunkset PBX Endpoint Number Routing Numberblock Backup numbers Template Services	Number Routing +			
	Name	Numberblock	Type	Number of prefixes
	Conf01	+49 (6131) 4 28(0-9)	Service	1

Numbers from the blocks are assigned to the trunk set with the menu "Number routing".

Here a number routing is added and edited.

User
License
Nconnect Voice
Trunkset
PBX Endpoint
Number Routing
Numberblock
Backup numbers
Template
Services

Number Routing
Name
Conf01

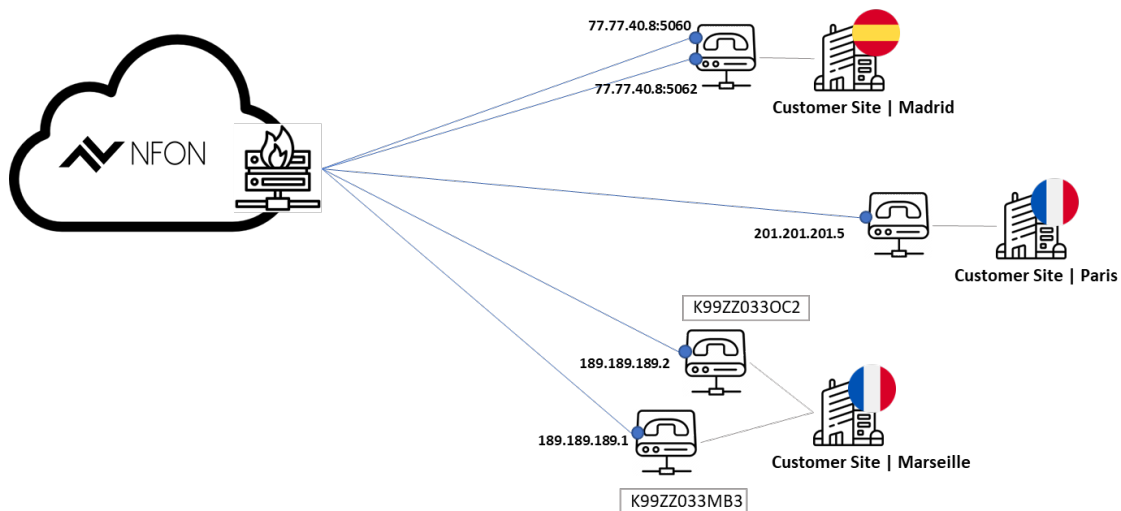
Create number routing
Name
test
Available Trunksets/services
SIP Trunk
Number block
+49 6131 [redacted] 28 (0-9)
Select all available entries
Remove all selected entries
☐ +49 6131 [redacted] 280
☐ +49 6131 [redacted] 280123
☒ +49 6131 [redacted] 280124
☐ +49 6131 [redacted] 281
☐ +49 6131 [redacted] 282
Selected entries: 1/14
Cancel Create

Type
Number of prefixes
service
1

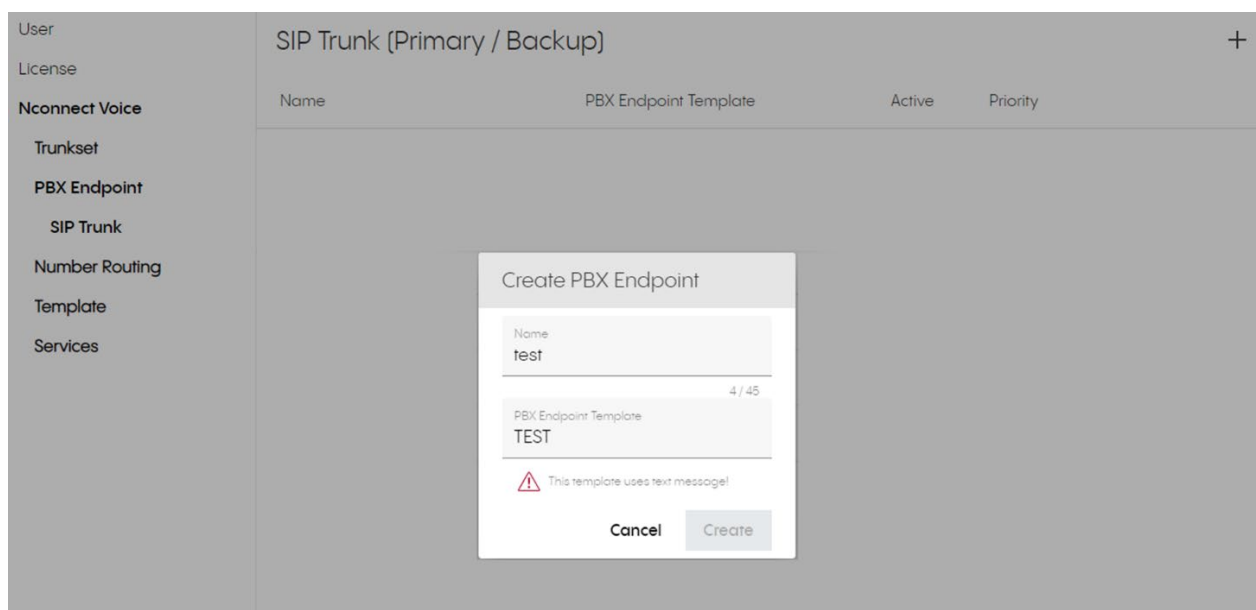
Create PBX endpoint

PBX endpoint

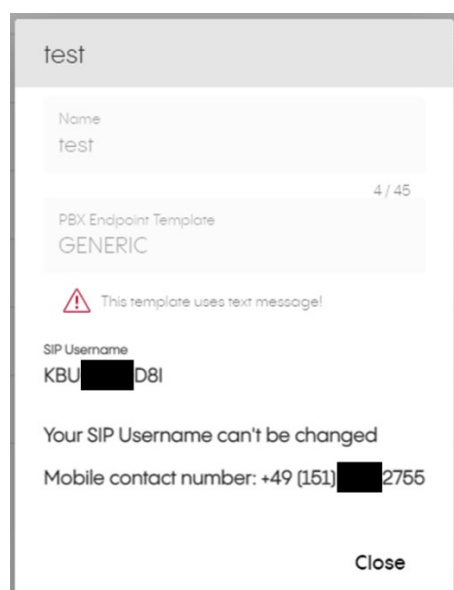
- The PBX endpoint specifies the endpoint on the customer side to which a trunk is connected as part of a trunk set.
- Has no relation to phone numbers on its own



The first step is to create the customer PBX as a SIP endpoint in the configuration portal via the "PBX Endpoint" menu. By clicking the "+" button, select the relevant PBX template and the new endpoint will be created:



The screenshot shows the 'SIP Trunk (Primary / Backup)' configuration page. On the left is a sidebar menu with options: User, License, Nconnect Voice, Trunkset, PBX Endpoint, SIP Trunk, Number Routing, Template, and Services. The main area has a table with columns: Name, PBX Endpoint Template, Active, and Priority. A '+' button is in the top right corner. A modal titled 'Create PBX Endpoint' is open in the center. The modal contains a 'Name' field with the value 'test' (4 / 45 characters), a 'PBX Endpoint Template' dropdown with 'TEST' selected, a warning icon and text 'This template uses text message!', and 'Cancel' and 'Create' buttons.



The screenshot shows the details for the 'test' PBX endpoint. It includes the 'Name' field with 'test' (4 / 45 characters), the 'PBX Endpoint Template' dropdown with 'GENERIC' selected, a warning icon and text 'This template uses text message!', the 'SIP Username' field with 'KBU[REDACTED]D8I', a message 'Your SIP Username can't be changed', the 'Mobile contact number' field with '+49 (151)[REDACTED]2755', and a 'Close' button at the bottom right.

The password for the PBX endpoint is sent via SMS to the provided mobile number of the technical contact partner. For all well-known vendors there is a template available for the PBX (PBX endpoint), so that the messages to the PBX use the right format. In case there is no template available for the PBX vendor, customer / partner has the possibility to create their own template. Go to "PBX Endpoint Template".

User	PBX Endpoint Template		+
License			
Nconnect Voice	Name	Type ↓	
Trunkset	MySuperSuperTemplate	Custom	
PBX Endpoint	Microsoft TEAMS Operator Connect	Global	
Number Routing	GENESYS	Global	
Template	GENERIC NATIONAL	Global	
PBX Endpoint Template	Daktela CC	Global	
Services	Microsoft TEAMS	Global	
	Avaya	Global	
	Alcatel	Global	
	NEC	Global	
	Swyx	Global	
	Elmeg	Global	

Add a new template using the "+" button:

Create PBX Endpoint template

Name
New PBX

Number format
National

Authentication:
☒ Register
☐ IP Address

Clip Style
From Name Clip

Inbound Ruri Format
E164

Cancel Create

With the template the incoming number format (international, national, local), authentication method, CLIP style and inbound URI format (E.164 number vs K- number).

Meaning of CLIP style:

- "From ID Clip": The PBX submits the CLIP number (additional calling party number) within the FROM and the calling party number (verified access number) within the PAI.
- "From Name Clip": Used when the PBX does not send the PAI. In this case both numbers are submitted within the FROM Header, the CLIP number within the DISPLAY-Name part and the calling party number within the SIP-URI of the FROM header.

Once the PBX endpoint is created, the final step is to activate it by clicking the "active" toggle in the "PBX Endpoint" menu.

PBX configuration

After PBX endpoint is set up, the connection to the NFON service has to be configured on the customer PBX. Example configuration values would be:

- **Username:** K1234 (Displayed after the creation of the endpoint)
- **Password:** test1234 (sent via SMS)
- **SIP Registrar:** siptrunk.cloud-cfg.com
- **SIP Proxy:** siptrunk.cloud-cfg.com
- **SIP Port:** 5060 (UDP), 5061 (TLS)
- **Protocol:** IPv4 UDP/TCP/TLS

Certification of the SIP trunk with multiple providers is in progress. Once it is complete, you can obtain the correct settings for the SIP trunk by selecting the appropriate template directly from the PBX endpoint settings menu. There are a number of certifications for the SIP trunk SIP-TK system connection. In principle, these also apply to the SIP trunk, since we use the same interfaces. The SIP registrar and SIP proxy are different (see above), but all other settings are the same. Additionally, the different SIP user identifier (Kxxxxxx instead of phone number) has to be considered.

Certified vendors

Vendor	Template
3CX	n
AGFEO	n
Alcatel-Lucent	n
Askozia	n
Asterisk	n
Auerswald	n
Avaya	n
AVM	n
Bintec Elmeg	n
Clarity	n
DATUS	n
Elmeg	n
GFI	n
Innovaphone	n
Mitel	n
Lancom	n
NEC	n
Panasonic	n
PASCOM	n
Sangoma	n
Starface	n
Swyx	n
Tevitel	n
Tiptel	n
Unify / Atos	n
Wildix	n

Support

The customer or partner is responsible for the setup of the PBX on customer's premises. Since each PBX requires specific knowledge for the various versions and systems, NFON Support cannot provide any advice on how to apply settings or troubleshoot any PBX issues. The customer or partner has to contact the party that is contracted to support the PBX, basically the PBX vendor. Additionally, NFON Support cannot assist with customer network issues that may hinder the implementation of SIP Trunk Flexx nor put any failovers in place if the SIP Trunk Flexx connection fails. Furthermore, NFON Support cannot make sure that there is a backup in place for fallback in case there are problems with the adaptations.

However, there is a chargeable service that is available where we offer technical consulting for projects that can assist with the above issues. Support cannot and will not give binding suggestions for the setup of the PBX. For any PBX setup or configuration, the customer will have to contact the party that is responsible for supporting the PBX. For the SIP Trunk Flexx product itself, NFON Support is able to provide assistance where necessary. This includes call control and voice traffic (SIP & RTP) between the customer PBX and NFON server as well as incoming and outgoing traffic to the PSTN. This is implemented according to the SIP connect 2.0 technical recommendation. If there are any issues with the SIP Trunk Flexx or features, our Support will be available to assist and troubleshoot via the usual channels.

Additional functions

Function overview

The following table provides an overview of supported SIP Trunk Flexx features:

Feature set	Feature Name	Short Feature Description
Basic	Call Handling Features	
	CLIP	Shows own phone number for outgoing calls
	CLIP no screening	Different phone number displayed for outgoing calls
	CLIR	Suppression of the caller number
	Call forwarding using "302 redirect"	Call forwarding triggered by the PBX using "302 redirect" SIP message
	Backup Service	Call forwarding in case trunk not reachable
	Call barring Incoming	Block incoming calls from specific numbers
	Supported Voice- Codecs	Audio codecs G.711 a-law / u-law
	Conferencing Service	Conferencing service allows everyone to dial into the audio-conference-call via a specific conference number belonging to the customer's number block.
	DTMF	Transport of tones according to RFC2833
	Security Features	
	Call barring	Pre-defined call barrier list Individual configuration per trunk-set
	Fraud detection	Fraud detection, automatic system-controlled detection
	Authentication in static mode	Peering
	User Agent Check	User Agent Check, automatic check for outbound call

	Protocol Features	
	TLS 1.2/ SRTP	Allows the encryption of the calls
	Portals	
	Administration Portal	https://siptrunk.nfon.com Note: in case it doesn't work please use https://start.cloudya.com
	Commercial Portal	https://my.nfon.com
Feature set	Feature Name	Short Feature Description
Premium	Basic Feature Set +	
	High Availability	PBX Connect options: Primary/Backup Round Robin,Forking
OPTIONS		
Microsoft Teams Integration		Direct Routing
Genesys Cloud Enablement		Enablement of Genesys Cloud Contact Center termination
FAX Service [Not available yet]		The customer can receive and send faxes without using a fax machine. The e-mail-to-fax procedure allows the sender to send faxes via e-mail. Fax-to-email allows faxes to be received in the SIP trunk at an extension and sent to an email client. Fax transmission with T.38 codec with fallback to G.711 is supported.

High availability

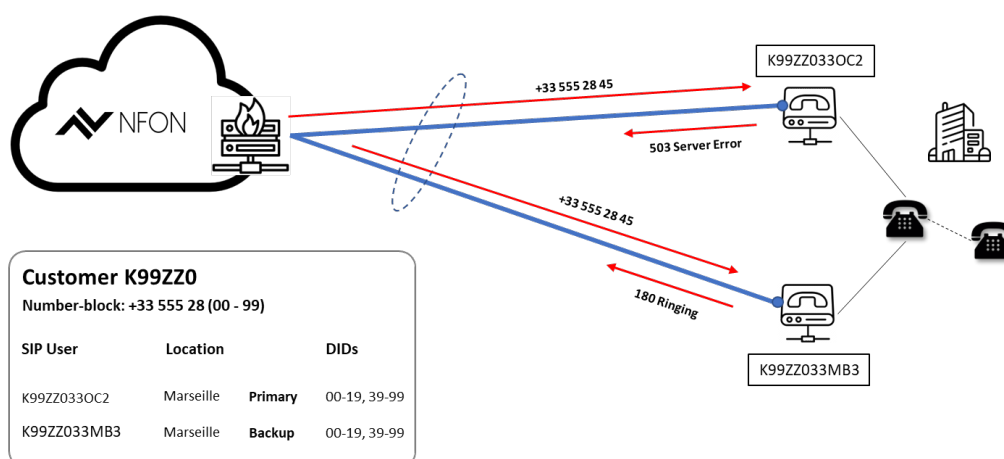
High-availability options are available and can be selected by the user:

- Primary / backup
- Round Robin
- Forking

Primary / backup

If the primary PBX becomes unavailable, calls are delivered to the secondary PBX.

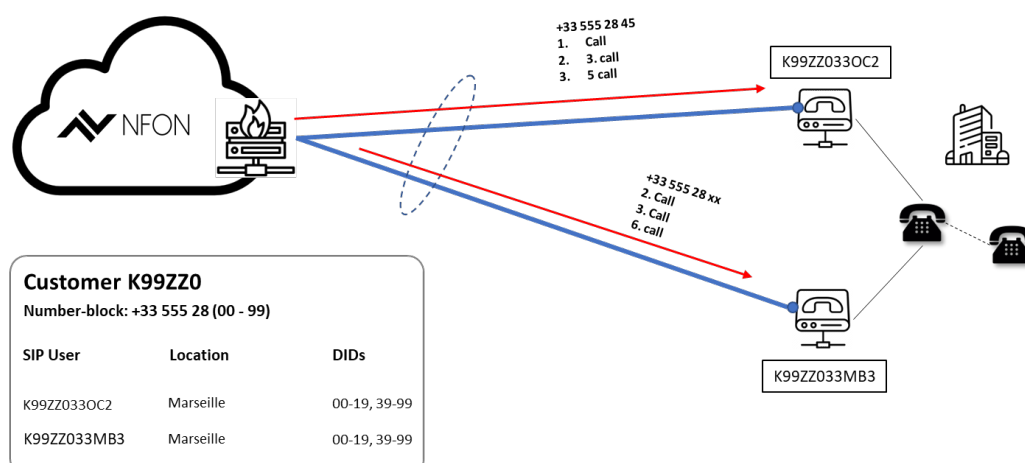
- Hot-standby redundancy
- If the primary PBX endpoint is not ready (not-registered or faulty) the call is routed to the backup instance
- All PBX endpoints of the related trunk set have to share the same extensions.



Round Robin (load balancing)

Every inbound call is sent to the next PBX in a repeating order, e.g. if there are two PBXs (A and B) the first incoming call would be sent to PBX A, the second incoming call to PBX B.

- The PBX endpoints related to a trunk set which is configured to Round Robin have to share the same extensions.
- With every call the next PBX endpoint of the trunk set is selected.

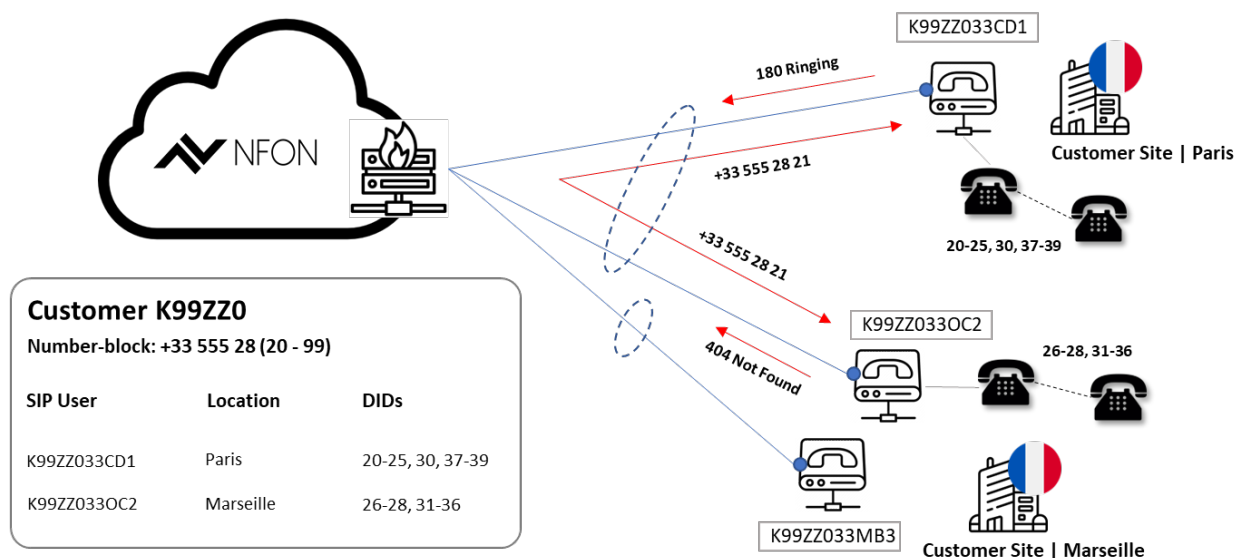


Forking

To improve availability, the customer can link multiple PBX systems to the same trunk set. A call from any facility will be answered. A call from the PSTN is delivered to each facility.

Distributed extension

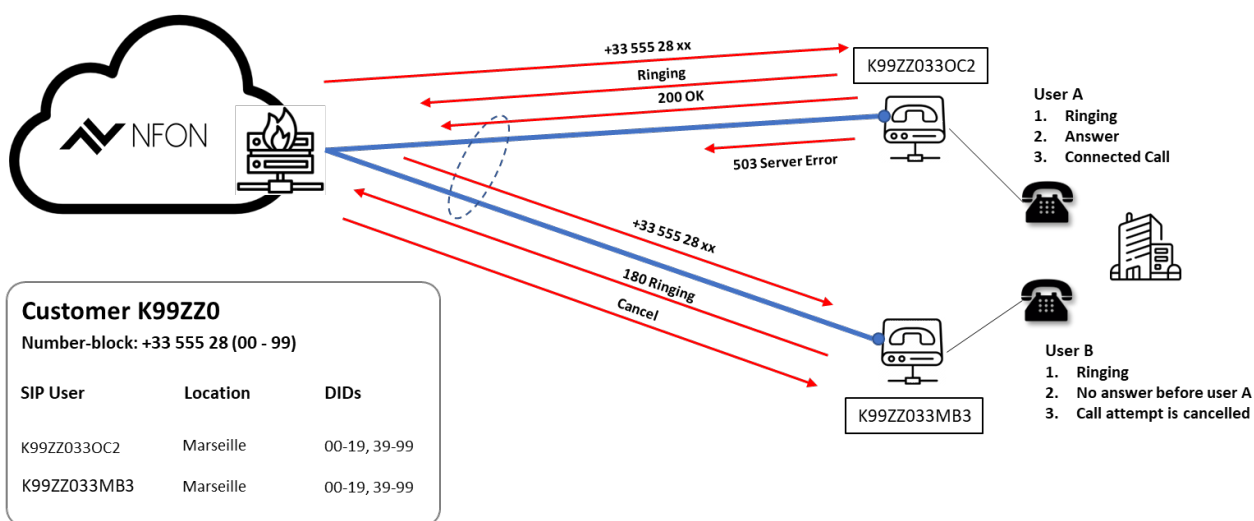
Failover is achieved, but the PBX that manages the extension accepts the call and delivers it to.



Simultaneous / multiple located extension

A call from the PSTN to the PBXs is forked into multiple INVITES. The PBX answering the call first gets this call, while the other call legs are cancelled. i.e inbound calls are delivered simultaneously to primary and secondary destinations, then connected to whichever destination responds first. Early media (i.e. ring back tone) is not supported. 180 provisional SIP response is requested so that progress tone can be passed correctly to the calling party.

- The PBX endpoints related to a trunk set share the same extensions.
- With every call both PBX Endpoints of the trunk set are addressed.
- Ringing is applied to both extensions.
- The extension that answers the call first will receive the call.
- For the other extensions the call is cancelled.

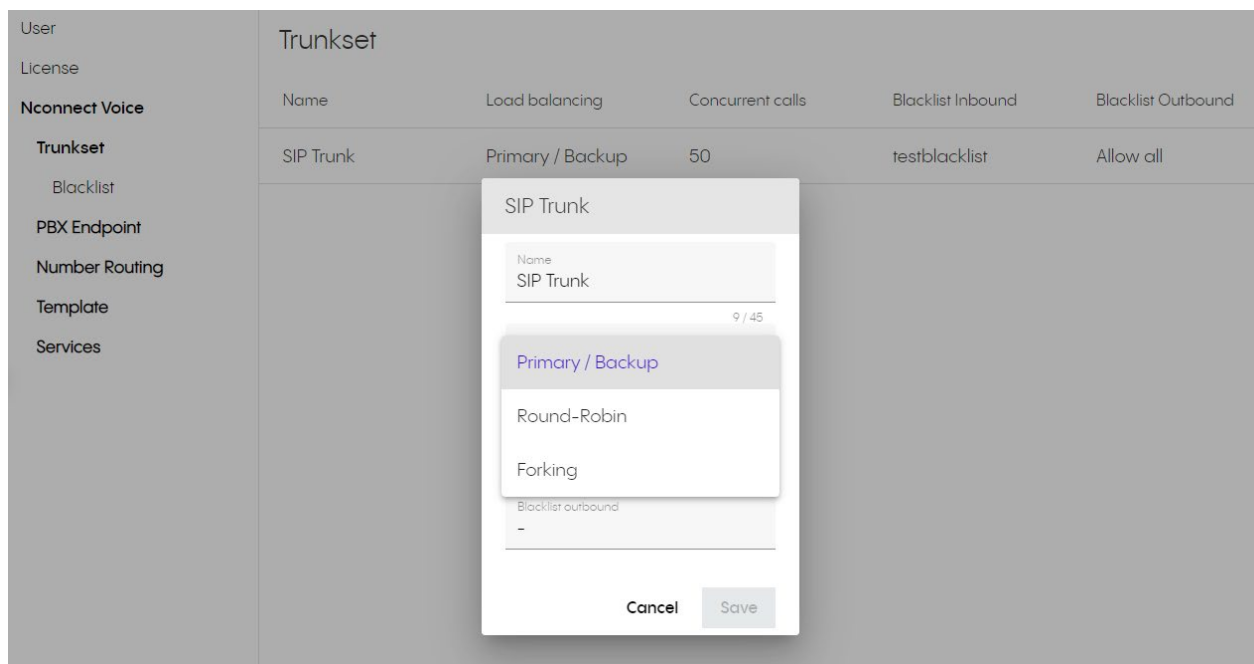


The administration of the high-availability feature is configured in the configuration portal from the trunk set menu:

User	Trunkset				
License					
Nconnect Voice					
Trunkset	Name	Load balancing	Concurrent calls	Blacklist Inbound	Blacklist Outbound
Blacklist	SIP Trunk	Primary / Backup	50	testblacklist	Allow all
PBX Endpoint					
Number Routing					
Template					
Services					

Configuration of high availability

The high availability option is selected on the trunk set:



The screenshot shows the 'Nconnect Voice' configuration page. The 'Trunkset' section is active, displaying a table with columns: Name, Load balancing, Concurrent calls, Blacklist Inbound, and Blacklist Outbound. A modal dialog titled 'SIP Trunk' is open, showing the 'Primary / Backup' option selected. The dialog also includes fields for 'Name' (SIP Trunk), 'Round-Robin', 'Forking', and 'Blacklist outbound'.

The order of the PBX for the "Primary / Backup" option is done by the priority of the respective PBX endpoint.

User	Test (Primary / Backup) +			
License				
Nconnect Voice				
Trunkset				
PBX Endpoint				
Location I				
Test				
Number Routing				
Template				
	Name	PBX Endpoint Template	Active	Priority
	Dieburg II	reg_number	<input checked="" type="checkbox"/>	↑ ↓
	Dieburg I	reg_number	<input checked="" type="checkbox"/>	↑ ↓

The option "Round-Robin" allows to activate or deactivate the endpoints which are addressed in the round-robin. The "Forking" option covers the cases "Distributed extension" and " Simultaneous / Multiple located extension" as described above.

User	Test (Forking) +		
License			
Nconnect Voice	Name	PBX Endpoint Template	Active
Trunkset	Dieburg II	reg_number	<input checked="" type="checkbox"/>
PBX Endpoint	Dieburg I	reg_number	<input checked="" type="checkbox"/>
Location I			
Test			
Number Routing			
Template			

Call forwarding with and without redirect (302)

The customer's PBX may send a 302 to forward the call to an external target. To reduce traffic on the customer's internet connection, the call is removed from the customer's line and forwarded by NFON internally. A forwarded call consumes 2 channels on the SIP Trunk Flexx nevertheless.

Security mechanisms such as fraud control are still in place to detect and handle fraudulent calls. To prevent fraud, we will not forward emergency, premium or direct enquiry services. Handling of the procedure depends on the specific PBX at the customer's site.

Alternatively, the PBX can also forward the call without 302. In this case, the PBX system can set up an outgoing call with INVITE without additional information or it can transmit additional forwarding information (e.g., DDI of the forwarding partner) in a forwarding header. It must be noted that the firewall on the PBX side must be opened outbound via RTP already with INVITE.

Backup service

If the customer's PBX-Endpoint is not reachable (detection based on a failed INVITE, OPTIONS are not used) the call is forwarded to a different number reachable via PSTN. Several options are possible:

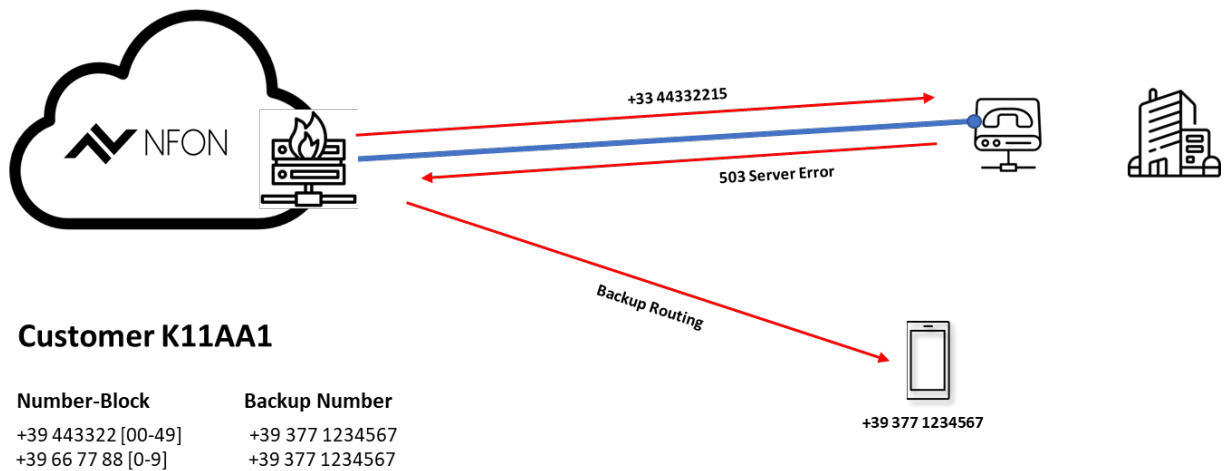
Standard backup (N:1) / phone number based

This is only for smaller customers that can have e.g. one mobile number to forward all failed calls to. Calls are diverted to an alternate phone number. Calls cannot be diverted to emergency, premium service or directory enquiry services.



In case the user has assigned a backup number to a number block and they divide the block afterwards, the new number blocks will not take over the backup number.

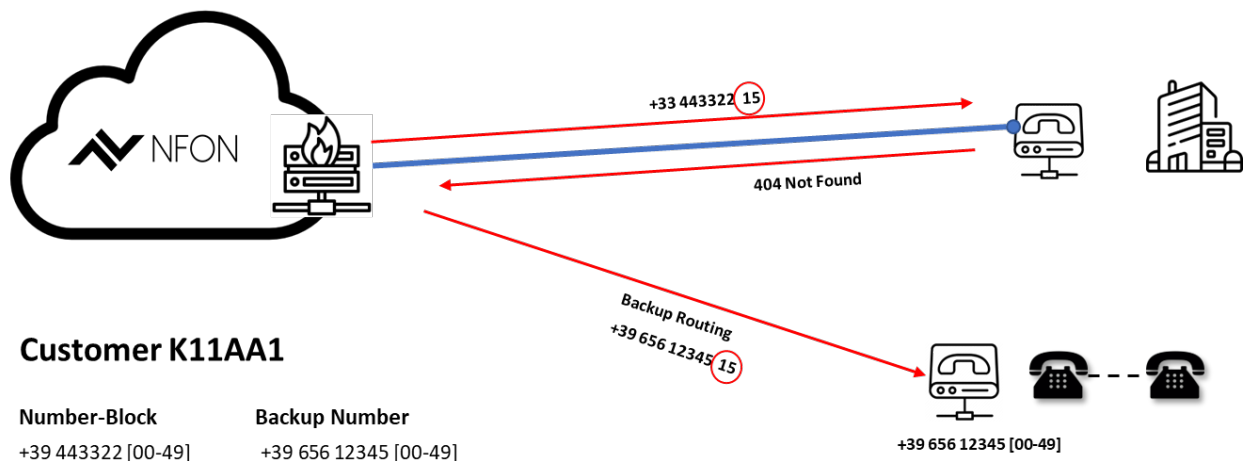
- The customer has one backup number for their number block.
- The call is routed to this backup number if routing fails.



DDI backup (N:N) / prefix-based number

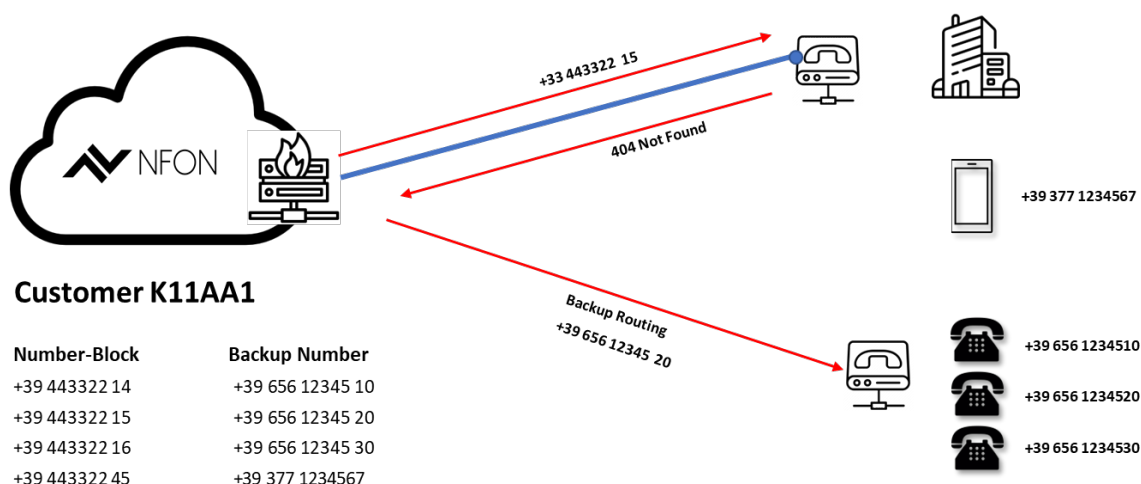
Bigger customers need a more precise solution instead of one central backup number. In a prefix-based configuration, the target prefix is replaced, while the extension is kept, so when the call is sent to the PSTN, the new prefix is used and the extension is kept the same.

- The customer has a backup number with the same number block.
- If the call to the destination number fails, a call to the backup number with the same extension is automatically initiated.
- Example: soft migration



Individual backup (N:M) / individual backup number

Each individual extension may be assigned to individual backup numbers.



It is possible to perform a DDI backup and a single backup for the same number block. In this case, the best/longest number match applies.

No backup

There are customers who do not want a backup, i.e. in case of failure the calls should not be forwarded to a backup number, e.g. private cell phones should not be included as backup and other options do not exist.

Backup service configuration

The user can choose and administrate the options in the configuration portal, menu "Number Routing"

User	Number Routing +			
License				
Nconnect Voice				
Trunkset				
PBX Endpoint				
Number Routing				
Numberblock				
Backup numbers				
Template				
Services				
	Name	Numberblock	Type	Number of prefixes
	Conf01	+49 (6131) [REDACTED] 828(0-9)	Service	1
	GP Fax	+49 (6131) [REDACTED] 828(0-9)	Service	1
	test	+49 (6131) [REDACTED] 828(0-9)	Trunkset	2

Create a backup entry for incoming calls using the "+" button.

Create Backup number

Name

Backup Number

Number block

+49 4937510

Extension

Phone number

Prefix based number

Backup number

+4917512345678

Cancel

Create

Inbound/outbound blacklist

The user may add CLI numbers for malicious calls to be blocked. Currently, only the exact numbers added to the blacklist are blocked. In addition, it is possible to block anonymous calls. To enable this, you have to click the related tick box in the menu.

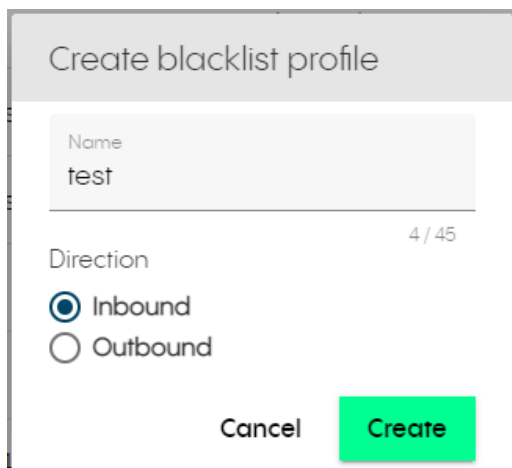
Administration of the blacklist is done under the "Trunk set" menu in the configuration portal:

User	Trunkset				
License					
Nconnect Voice					
Trunkset	Name	Load balancing	Concurrent calls	Blacklist Inbound	Blacklist Outbound
Blacklist	SIP Trunk	Primary / Backup	50	testblacklist	Allow all
PBX Endpoint					
Number Routing					
Template					
Services					

Then select "Blacklist".

User	Blacklist				+
License					
Nconnect Voice					
Trunkset					
Blacklist	Name	Direction	Entries	Type ↑	
PBX Endpoint	testblacklist	Inbound	1	Custom	
Number Routing	Test	Outbound	1	Custom	
Template	SYNC ME	Inbound	-	Custom	
Services	Default Schweden - Class 4	Outbound	438	Custom	
	Default Schweden - Class 2	Outbound	578	Custom	

Create an incoming blacklist from the "+" button.



Create blacklist profile

Name
test

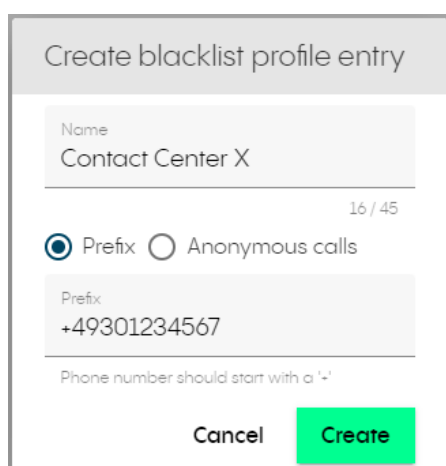
4 / 45

Direction

☒ Inbound
☐ Outbound

Cancel Create

Here you can enter the name of the blacklist profile and the number to be blocked for incoming calls:



Create blacklist profile entry

Name
Contact Center X

16 / 45

☒ Prefix ☐ Anonymous calls

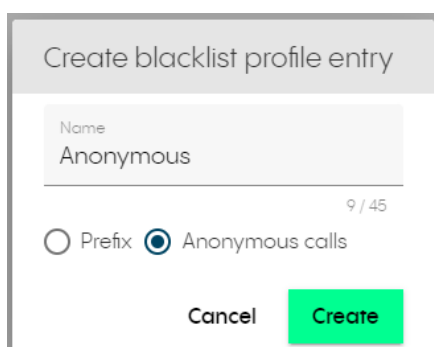
Prefix
+49301234567

Phone number should start with a '+'

Cancel Create

The number format has to start with "+".
Further entries can be added using the "+" button.

Anonymous calls are blocked by choosing "Anonymous calls" in the blacklist profile entry:



Create blacklist profile entry

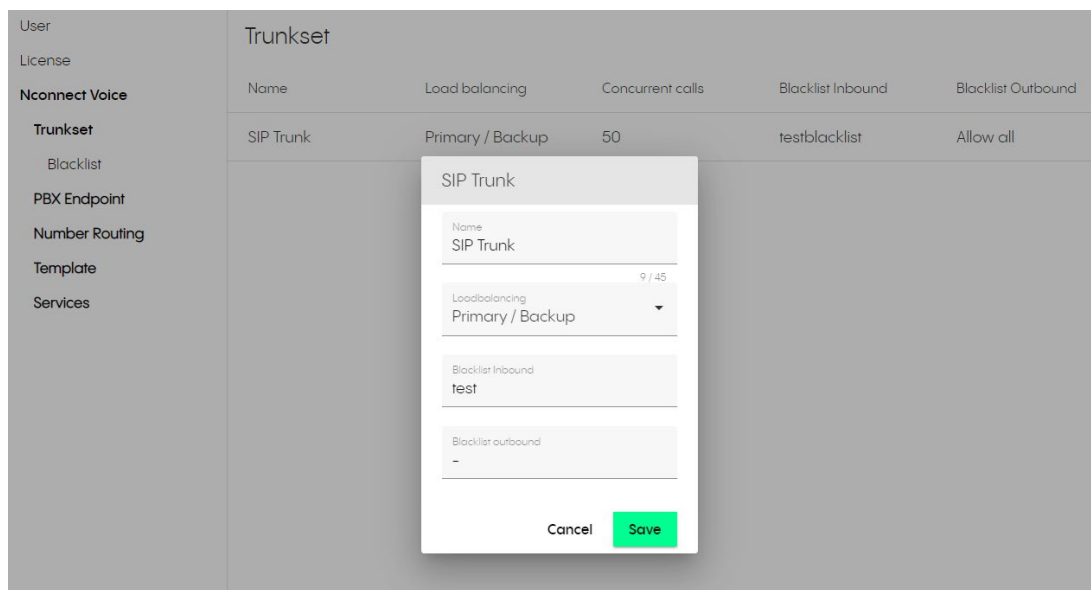
Name
Anonymous

9 / 45

☐ Prefix ☒ Anonymous calls

Cancel Create

By editing the trunk set in the "Trunk set" menu, the blacklist profile can be assigned:



Name	Load balancing	Concurrent calls	Blacklist Inbound	Blacklist Outbound
SIP Trunk	Primary / Backup	50	testblacklist	Allow all

eFax Service

Fax service allows you to send a fax through your email by attaching the document you want to fax to an email message. Then, the e-fax provider's online processor sends the message and attachment to any indicated recipient's fax machine.

Mail to fax

- Email and all attached files (PDF) that can be rendered are converted into a fax.
- The administrator defines which email address to send through which fax number.
- The definition of a sender address is uniquely assigned to only one fax service.
- For each fax service, there is only one outgoing fax number.
- Up to 10 email addresses authorized to send/receive faxes through the fax service can be defined.
- The administrator can define the fax header text and fax header number, which are written in the recipient's fax header.
- With email-to-fax, an email can be sent with file attachments in TIFF or PDF format.
- A qualified transmission report is generated for transmitted faxes:
 - B-number and T.30 recipient number
 - Number of transmitted pages
 - Result (confirmation or error)
 - Notify user when an outbound fax job succeeded
 - Notify user when an outbound fax job failed (with error)
- The domain owned by the Fax Server to be used for sending a fax is: faxgate.cloud-cfg.com
- The mail to format is: <E.164 call number>@faxgate.cloud-cfg.com
- Only the content of the PDF attachment is sent as a fax
- Each sending mail-to-fax mailbox must be unique system-wide

Fax-to-email

- Incoming numbers are assigned to this fax service by number routing.

- The administrator defines the email addresses to which incoming faxes are sent.
- Incoming faxes are converted to PDF and sent to the email addresses specified in the fax service.
- Up to 10 email addresses authorized to send/receive faxes through the fax service can be defined.
- Unlike the email-to-fax scenario, recipient email addresses can be used multiple times
- The fax recipient receives the content from the sender as a mail attachment.
- Unlimited number of pages

T.38 relay standard and G711a audio codec are supported.

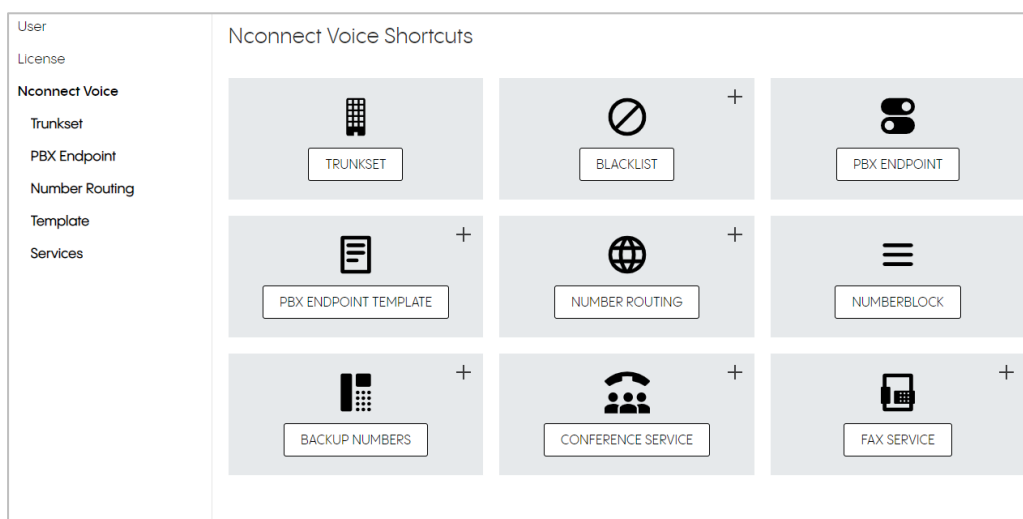
Sender Policy Framework

For security reasons SPF must be specified on the customer DNS to allow inbound mail2fax functionality.

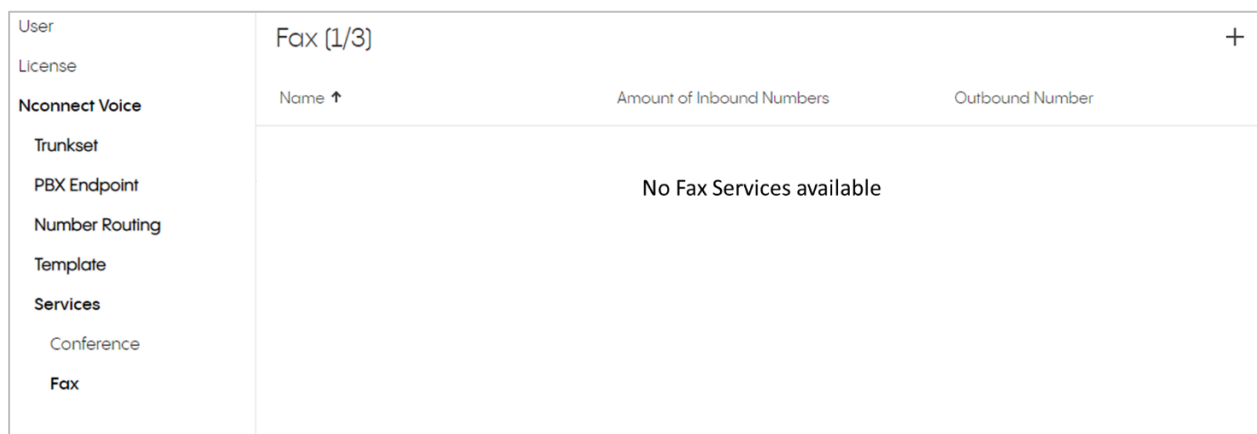
Fax service configuration

Since fax service is included in the basic package but is optional, it has to be specifically requested in the order form.

- Open the SIP Trunk Flexx configuration portal.

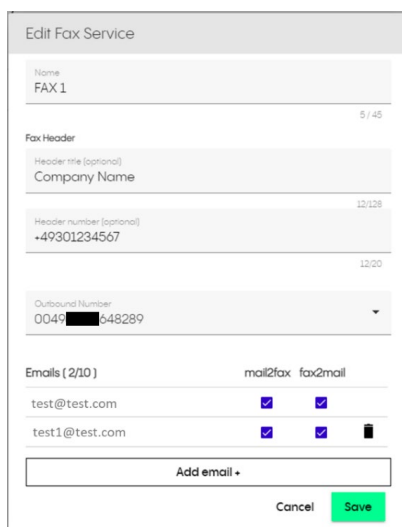


- Click on fax (under Services menu) or the shortcut button.



- Click on the “+” icon to add a new fax service.

- For each fax service:
 - Enter the name of the fax service.
 - Enter the title and the number for your fax header.
 - Specify the outbound number (number routing has to be set first – please see Number routing section).
 - Enter email address associated to mail-to-fax and fax-to-mail scenarios (a maximum of 10 email addresses can be added to the service).
- Click on Save.
- Repeat the steps previously described for each fax service.



Mail-to-Fax Sending Procedure

The procedure for sending a fax using your mail client is as follows:

1. Create a new e-mail message
2. Set the B-number as “To” field



Please note that:

- Phone number must be in international format
- The e-mail format must be text only (no html)
- The use of an attachment is mandatory

Conference service

Conference service makes it easier than ever to conduct conferences for crowds of all sizes.

- The administrator can create/edit multiple conferences for each SIP trunk.
- A maximum number of 5 conference rooms can be created (without reordering).
- Audio conferences/Conference rooms can handle up to 50 participants overall.
- Administrator can create/edit both admin and user pin for each conference room.


Conference service configuration

Since conference service is included in the basic package but is optional, it has to be specifically requested in the order form.


- Open the SIP Trunk Flexx configuration portal.

User
License
Nconnect Voice
Trunkset
PBX Endpoint
Number Routing
Template
Services


Nconnect Voice Shortcuts




TRUNKSET




BLACKLIST




PBX ENDPOINT




PBX ENDPOINT TEMPLATE




NUMBER ROUTING




NUMBERBLOCK



BACKUP NUMBERS



CONFERENCE SERVICE



FAX SERVICE

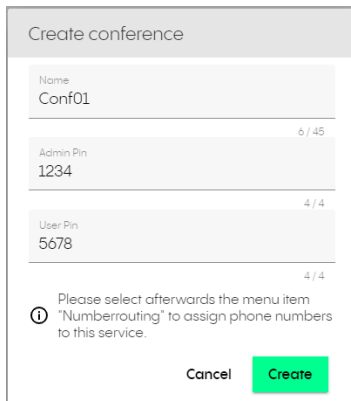
- Click on Conference (under Service menu) or the shortcut button.

User
License
Nconnect Voice
Trunkset
PBX Endpoint
Number Routing
Template
Services
Conference
Fax

Conference

Name	Admin Pin	User Pin	Amount of Inbound Numbers
No Conference Service available			

- Click on the "+" icon to add a new conference service.



Create conference

Name
Conf01

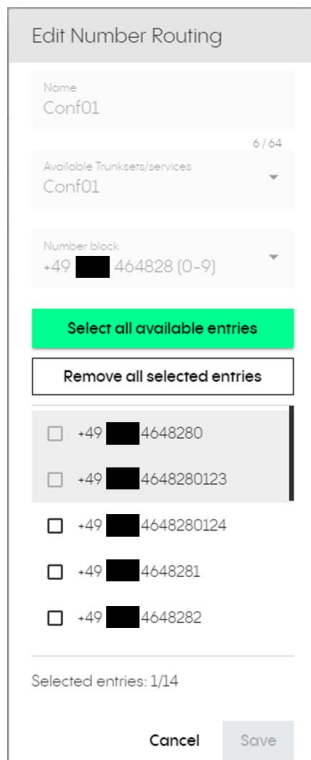
Admin Pin
1234

User Pin
5678

Please select afterwards the menu item "Numberrouting" to assign phone numbers to this service.

Cancel Create

- Create/edit a name for each conference room.
- Enter a four-digit Admin PIN and a four-digit User PIN for the conference room (mandatory).
- Assign one or more than one number to the conference room into the Number Routing menu.



Edit Number Routing

Name
Conf01

Available Trunksets/services
Conf01

Number block
+49 464828 (0-9)

Select all available entries

Remove all selected entries

☐ +49 4648280

☐ +49 4648280123

☐ +49 4648280124

☐ +49 4648281

☐ +49 4648282

Selected entries: 1/14

Cancel Save

- Click on Save.
- Repeat the steps previously described for each conference service.

DTMF [according to RFC 2833]

DTMF tones are transported as marked events within the RTP stream.

Multi number management

The customer can add one or several numbers or number blocks to the SIP Trunk. Size and content of the blocks is specific per country depending on the country regulation. Any called number from those number blocks is then routed to the PBX according to the fixed number routing (see chapter Number routing). The number of concurrent calls is calculated from the number of calls over all assigned numbers, i.e. the number is per SIP Trunk, not per number block.

International number management

Number blocks can be provided from all countries that are available via the NFON carrier interconnects. Outgoing calls are always terminated via a carrier in the country of the number block of the calling party.

Accounting is done according to the rate table valid for that country.

Emergency call

The customer can dial any emergency service number that is provided in the country of the used SIP Trunk. The Location is assigned to the number blocks. If the customer dials an emergency number, the country is selected via the site location assigned by the customer and the call is routed over the carrier interconnect of that country. The customer is responsible for recording the complete and correct location. In addition, the customer is responsible for signaling the correct calling party number so that it is possible to determine the correct location and enable callback.

If the emergency call is made from a different location than the address entered (nomadic use), DTS cannot ensure that the emergency call is routed to the nearest emergency service location. Basically, the call is routed to the emergency location assigned to the entered address in combination with the used calling party number. To avoid such problems, it is possible to order a DN at the location of the usage and assign the correct address to this DN in the order. By using CLIP no screening (see chapter CLIP no screening) the location can be hidden for all non- emergency calls.

Outgoing call barring

As fraud is typically related to specific countries (e.g. Africa or Middle East) various generic call barring security classes are used to protect SIP trunk.


The customer can switch between the "security classes":

- **Class 2:** International destinations critical for fraud and national premium services (common European destinations accessible)
- **Class 4** is less restrictive
- **Class 6** has even fewer restrictions that only blocks destinations very critical for fraud
- **Class 99** (allow all): No destinations blocked (this option is not visible in the blacklist and is only a selectable option when assigning a blacklist profile to a trunk set)

Per default, critical international destinations and national premium services are blocked. Details about the blocked destinations per security class are visible from the configuration portal. These classes are the same for all countries, except the national specific premium services. They are the pre-defined barring classes.

In addition to the default security classes, customers can define their own custom class and assign the custom class to the required trunk set. It is not possible to have a default class and an individual barring class in parallel. Within their custom barring class, the customer is able to define specific destinations and individual numbers that requires blocking. Customers can block destinations in their PBX. However, these are on top, i.e. it is not possible to open a destination from the PBX that is blocked in the assigned barring class and vice versa. Call barring administration is done in the configuration portal. There is no specific authentication required for call barring administration.

Administration of outgoing call barring is done from the trunk set:

User	Trunkset				
License					
Nconnect Voice	Name	Load balancing	Concurrent calls	Blacklist Inbound	Blacklist Outbound
Trunkset	SIP Trunk	Primary / Backup	50	test	Allow all 
Blacklist					
PBX Endpoint					
Number Routing					
Template					
Services					

Click on the edit pencil of the trunk set that requires the barring class. The default blocking classes are always available:

SIP Trunk

User

License

Nconnect Voice

Trunkset

Blacklist

PBX Endpoint

Number Routing

Template

Services

Blacklist

To see the content of a blocking class (blacklist), go to the "Blacklist" menu:

Choose the content button on the right-hand side of the related blacklist:

User	Class 4 (Outbound, Global)	
License		
Nconnect Voice	Name	Prefix
Trunkset	Afghanistan-Mobile AWCC	+9370
Blacklist	Afghanistan-Mobile Etisalat	+9378
custom	Afghanistan-Mobile MTN	+9376
PBX Endpoint	Afghanistan-Mobile Others	+937
Number Routing	Afghanistan-Mobile Roshan	+9372
Template	Albania-AMC Fixed	+35568
Services	Albania-Tirana	+355422
	Albania	+355
	Albania-Mobile Others	+35566
	Albania-Mobile-Eagle	+35567
	Albania-Mobile Vodafone	+35569

To configure an individual blacklist, choose the "+" button in the blacklist menu:

Create blacklist profile

Name

test

4 / 45

Direction

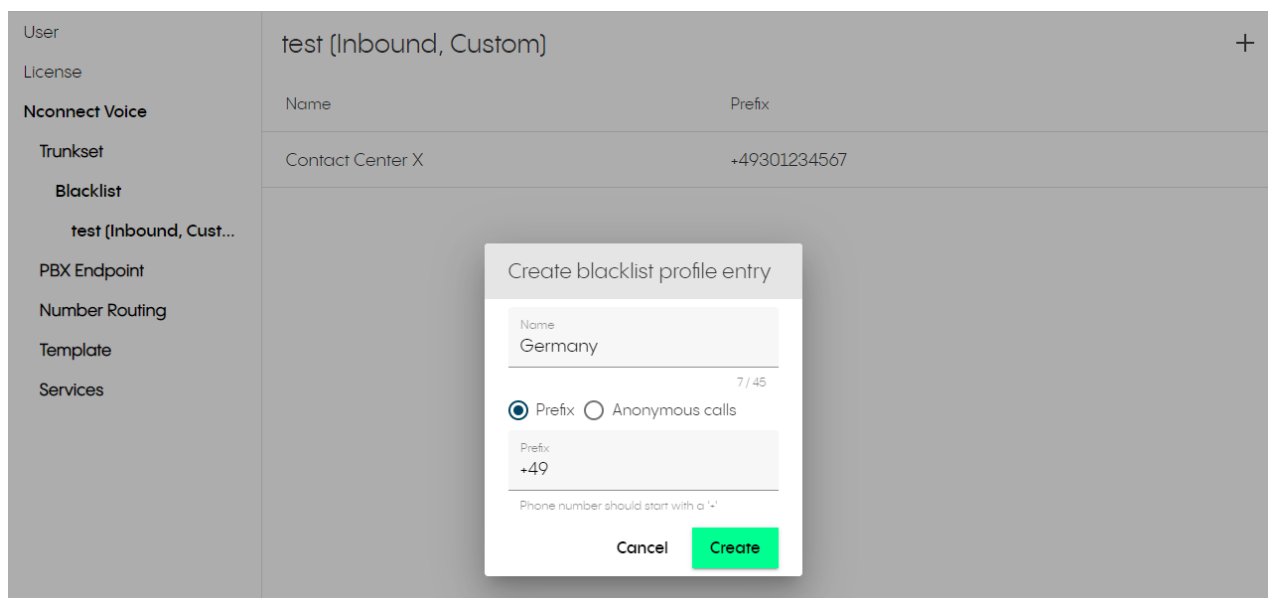
☒ Inbound
 ☐ Outbound

Cancel

Create

After creating the barring class, click on the "+" button to add the number prefix or whole number that is to be blocked.

Please note that the number prefix or whole number has to start with a "+".



The screenshot shows the NFON interface with a sidebar on the left containing menu items: User, License, Nconnect Voice, Trunkset, Blacklist, test (Inbound, Cust..., PBX Endpoint, Number Routing, Template, and Services. The main area displays the 'test (Inbound, Custom)' profile. A modal titled 'Create blacklist profile entry' is open, showing a form with the following fields: Name (Germany), Prefix (+49), and a radio button selection for 'Prefix' (selected) and 'Anonymous calls'. A note at the bottom of the modal states 'Phone number should start with a '+''. The modal has 'Cancel' and 'Create' buttons.

Fraud control

Fraud detection is based on a cost limit for the sum of all speech channels. If this limit is exceeded within one hour, the SIP trunk is blocked for national/international/service calls. The limit is valid for the sum of speech channels within one country.

The limits are:

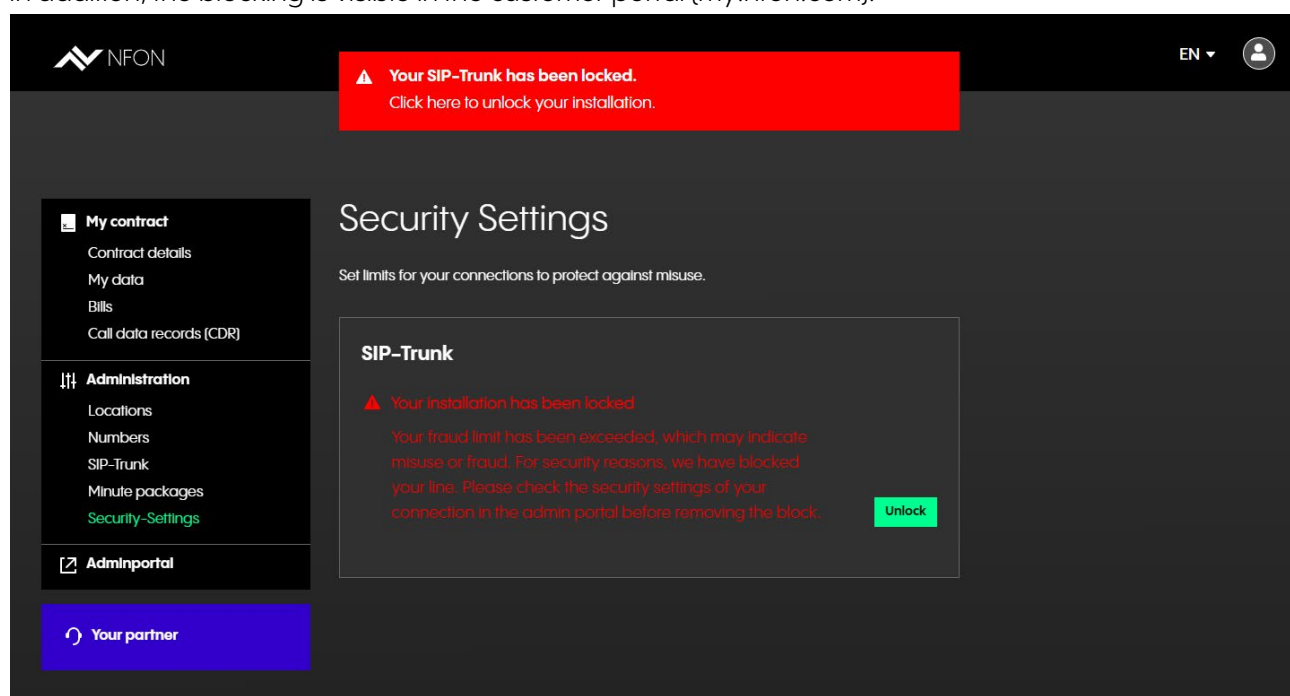
Channels	Number of channels	Threshold
SIP Trunk Flexx per channel	Two channels	25 €
	Three channels	
	Four channels	
	Five channels	30 €
	Six channels	
	Seven channels	35€
	Eight channels	
	Nine channels	40€
Bundles	10 channels	40€
	20 channels	45€

50 channels

60€

The limit is checked for every call. It is not checked per channel, but the sum over all channels is checked. That means if the customer has 10 channels / concurrent calls) and their airtime costs exceeds 40€ within one hour, our fraud prevention will trigger. On the other hand, if the airtime costs for one channel is 39€ within one hour and the other channels do not have any costs, the fraud prevention will not trigger.

So as a reminder, if the limit is reached, extended services (i.e. international calls and service calls) will be blocked. Stable calls will not be released; the limit is checked only after each call. Therefore, it may happen that the limit is crossed but the blocking applies at a later point in time, e.g. if a long call is established to an distant destination, the limit may be reached during the call. The blocking will apply only after the call, when costs are already above the limit. When the block is triggered, an email notification is sent to customer informing them of the suspected fraud. In addition, the blocking is visible in the customer portal (my.nfon.com).

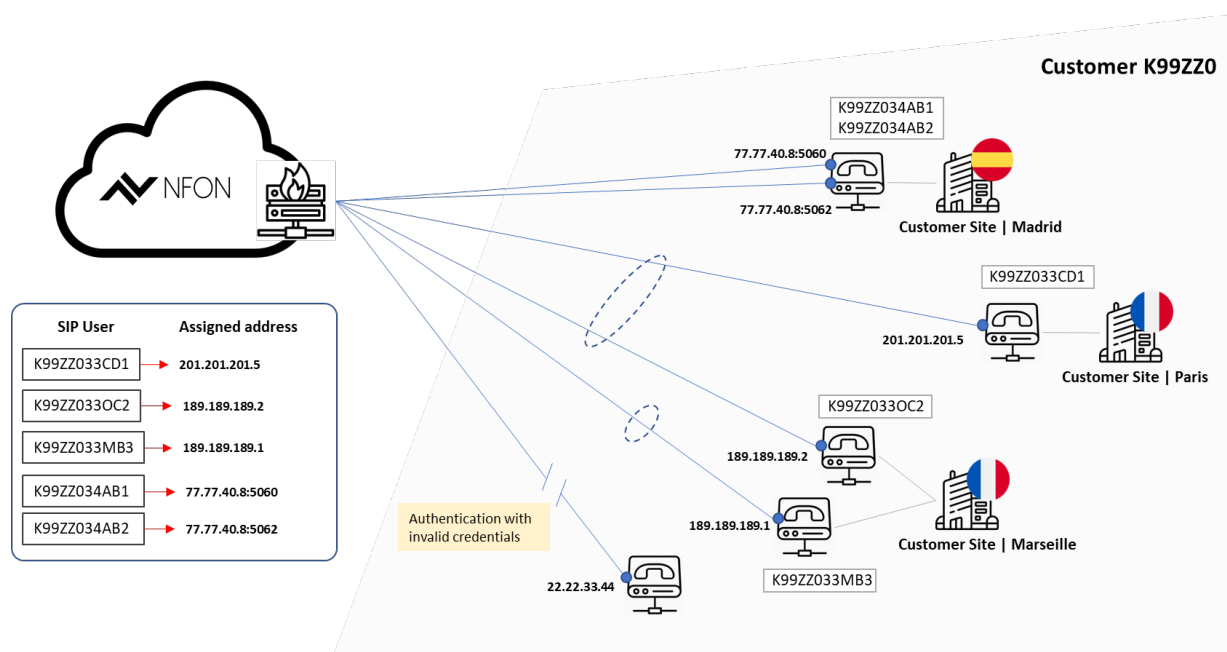


Customer can unblock the SIP trunk in the SIP Trunk Flexx customer portal. There is no check whether the cause of the fraud has been solved by the customer, i.e. NFON cannot make sure that the reason for the high costs is solved. So it might happen that within the next hour the limit is crossed again, the high costs will rise again and the access will be blocked again. After unblocking the SIP trunk, the limit counter is reset to zero but if the limit is exceeded again in an hour, access will be blocked again.

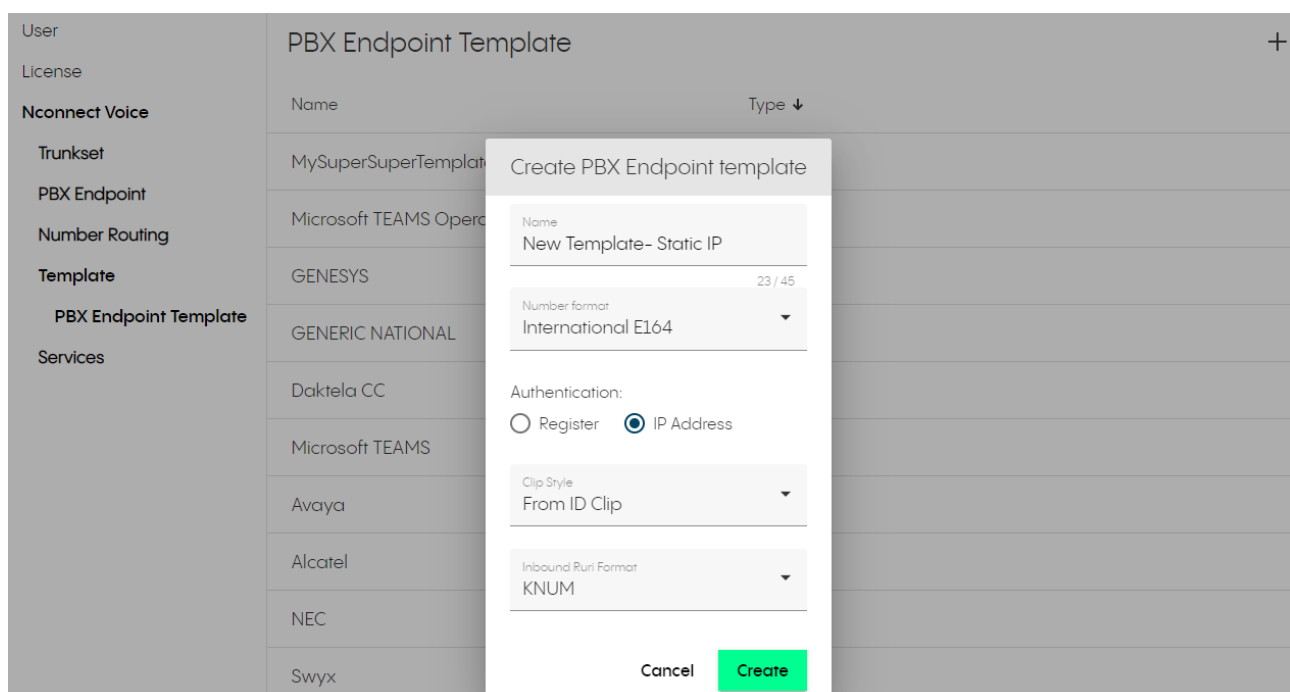
Authentication static mode

With this authentication mode, traffic is only sent to and from the customer's public (static) IP address. For some firewalls, the static mode that it uses does not support "two-way communication". In this case, the "REGISTER" method will have to be configured.

- The PBX authenticates to receive and send calls to/from a dedicated PBX endpoint.
- The PBX can authenticate with a well-known static IP address.



The configuration for IP authentication and handling of the IP address for authentication in static mode is done in the configuration portal. When creating a PBX endpoint template, set the authentication to IP address:



User

License

Nconnect Voice

Trunkset

PBX Endpoint

Number Routing

Template

PBX Endpoint Template

Services

PBX Endpoint Template

Name

Type ↓

MySuperSuperTemplate

Microsoft TEAMS Oper

GENESYS

GENERIC NATIONAL

Daktela CC

Microsoft TEAMS

Avaya

Alcatel

NEC

Swyx

Create PBX Endpoint template

Name

New Template- Static IP

Number format

International E164

Authentication:

☐ Register ☒ IP Address

Clip Style

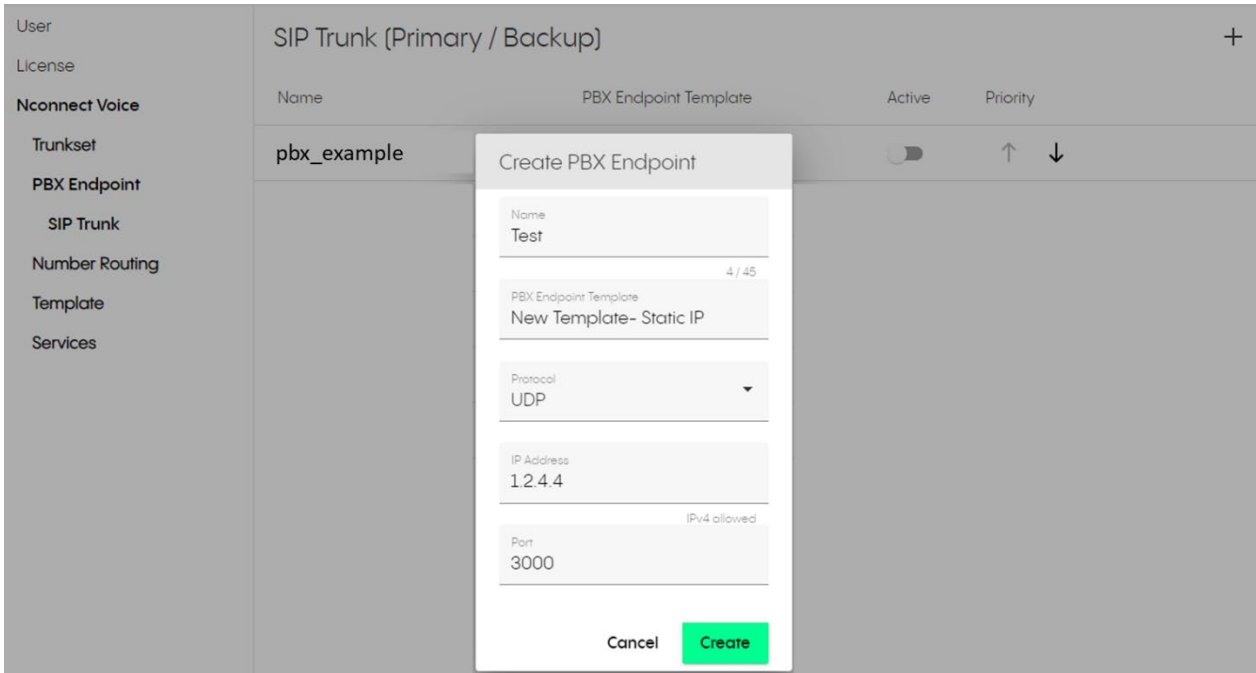
From ID Clip

Inbound Ruri Format

KNUM

Cancel Create

When creating a PBX endpoint, assign that template. You can then add the IP address that will be used for authentication. Please note that the IP address needs to be a public IP address.



The screenshot shows the 'SIP Trunk (Primary / Backup)' configuration page. A modal dialog titled 'Create PBX Endpoint' is open, allowing the user to create a new endpoint. The dialog contains the following fields:

- Name:** Test
- PBX Endpoint Template:** New Template- Static IP
- Protocol:** UDP (selected from a dropdown menu)
- IP Address:** 1.2.4.4
- Port:** 3000

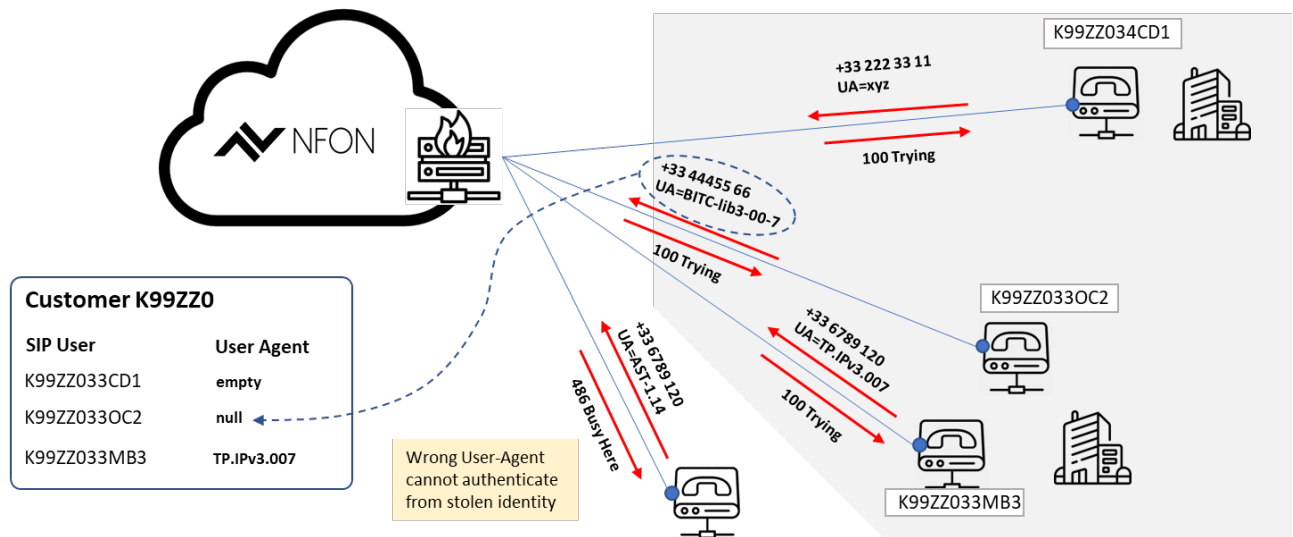
At the bottom of the dialog are 'Cancel' and 'Create' buttons. The background shows a table with columns: Name, PBX Endpoint Template, Active, and Priority. The first row has the name 'pbx_example'.

User agent checking

The "User Agent" parameter (header of SIP INVITE) is checked by a prefix to allow only those calls from the customer PBX that have a correct value. The first REGISTER after a SIP password change resets the prefix. This is to avoid abuse of leaked credentials.

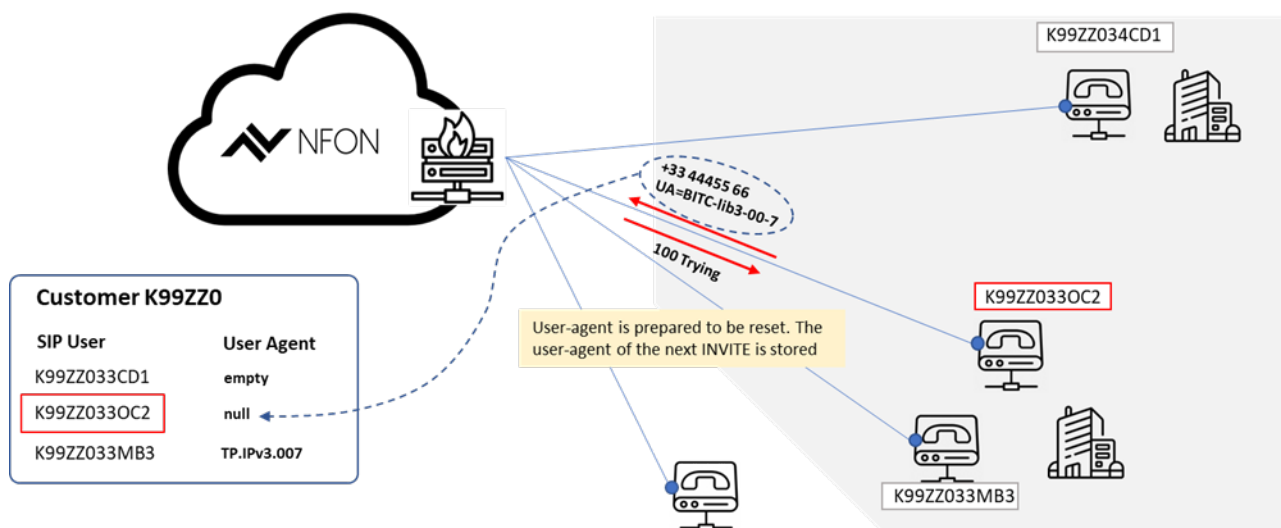
Only the first five characters of the user agent information are checked:

- If the check is enabled, it will only allow user agents (header field of the INVITE) that are assigned to the PBX endpoint.
- User agent configuration set to „null“ reconfigures with next INVITE
- Only INVITE messages are verified.
- Non-matching user agents get a „Busy“ response.



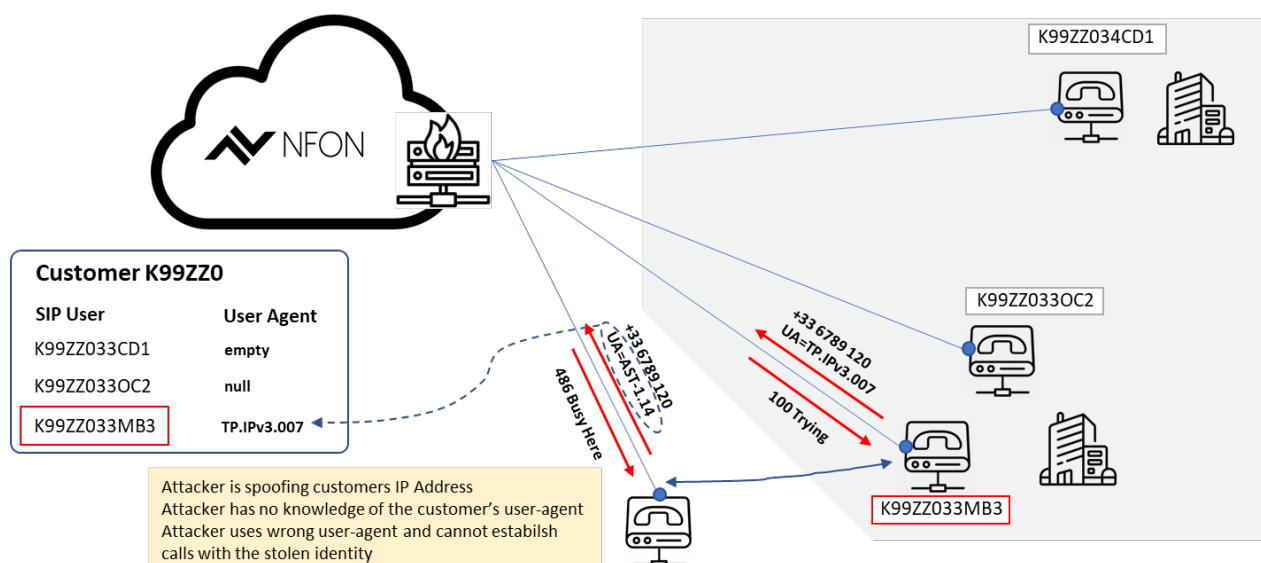
User agent check – NULL

- The customer can only reset the user agent (e.g. in order to connect a new PBX type).
- User agent's value set to "null" reconfigures with next INVITE.
- The user agent of the next INVITE (received from that SIP user) is stored as new user agent.

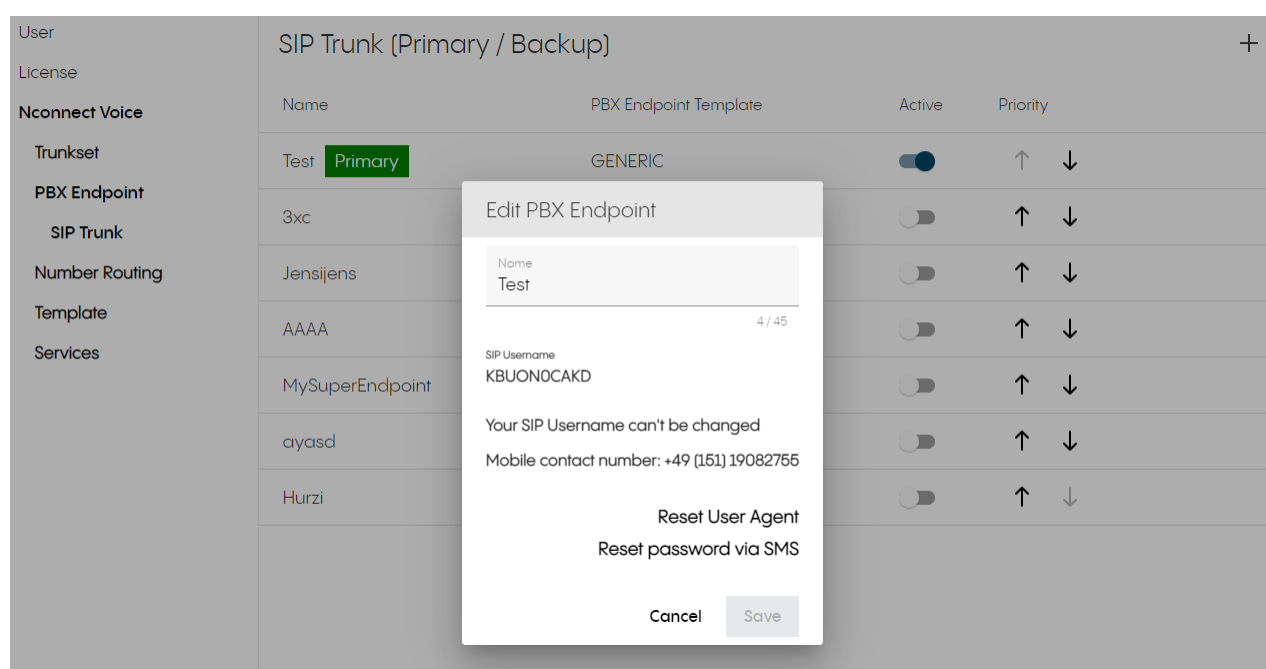


User agent check – reject mismatched user agent

Non-matching user agents get a "Busy" response.



User agent reset is done in the configuration portal in the PBX endpoint administration.



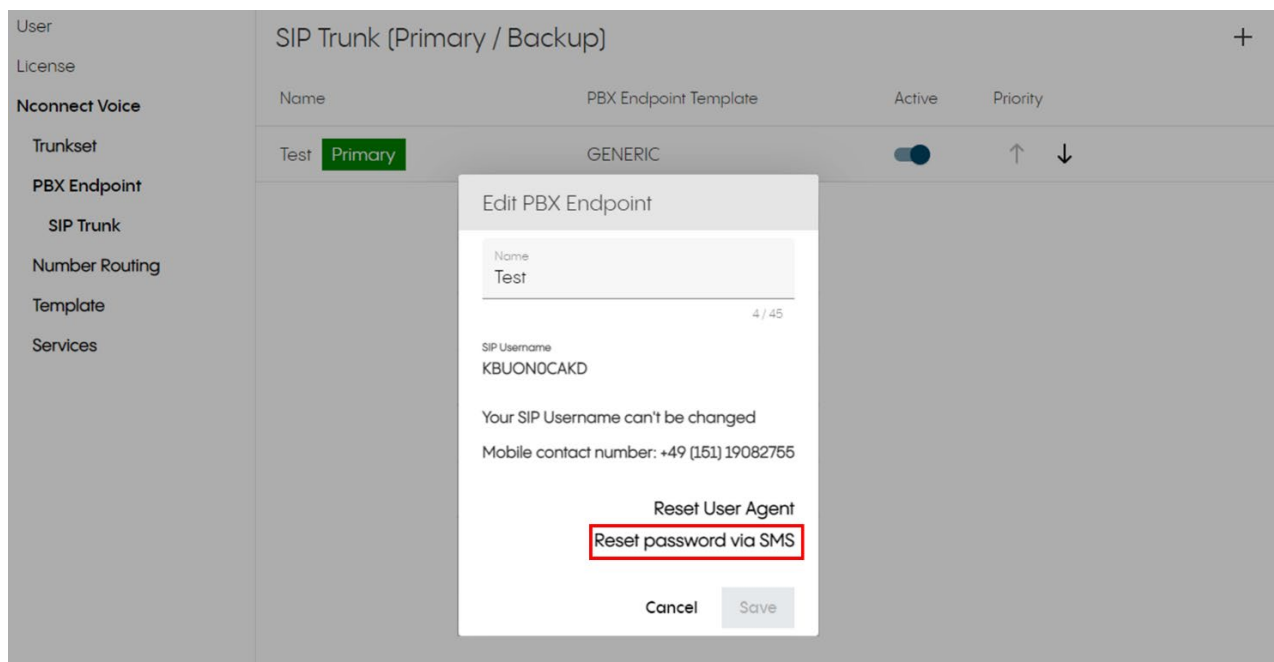
Register PBX → NFON or Invite outgoing call

SIP password change

The administrator may regenerate (not specify) a new SIP password which is sent via SMS to the mobile number that has been defined with the order.

This resets the user agent prefix filter.

A password reset is done from the "Edit PBX Endpoint" menu in the configuration portal:



Protocol features, TLS/ SRTP

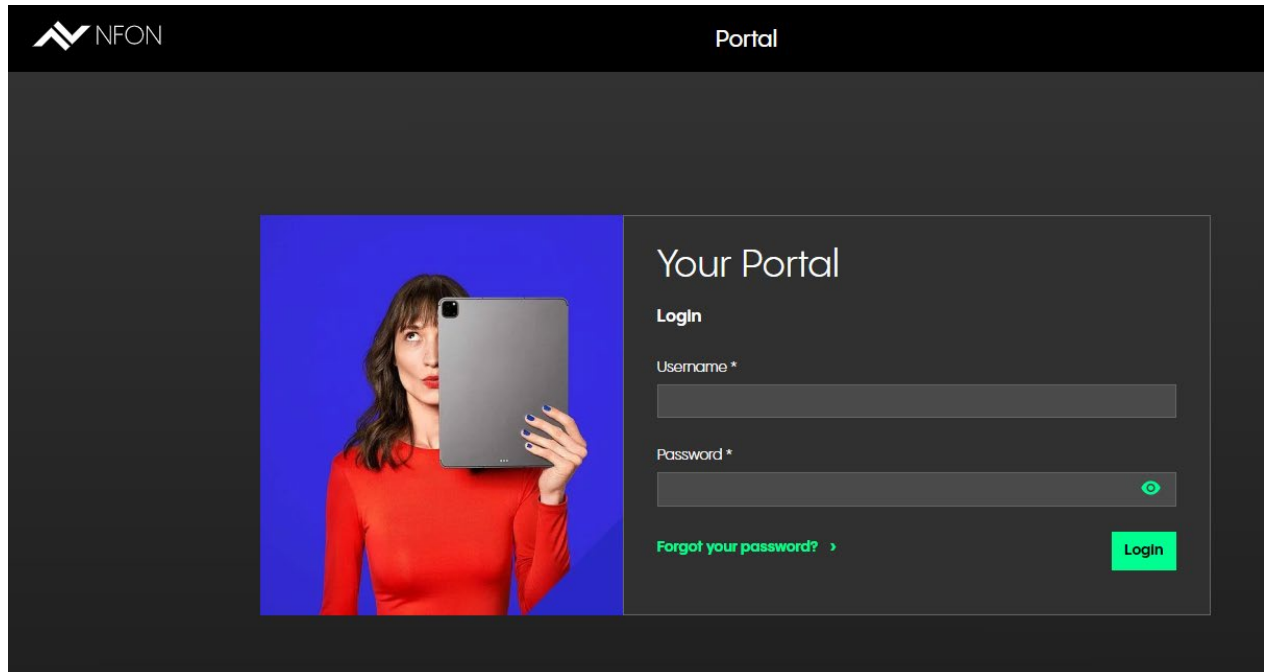
Supported protocols:

Protocol	Note
IPv4	-
UDP	Port 5060
TCP	Port 5061
TLS	(Transport Layer Security) TLS1.2 for encrypting call signaling and SRTP (Secure Real Time Protocol) for encrypting media streams. TLS1.2 is downward compatible with TLS1.1 so that there is no additional effort for customers still using TLS1.1. (we do not allow TLS with unsecure RTP.)

Customer portal

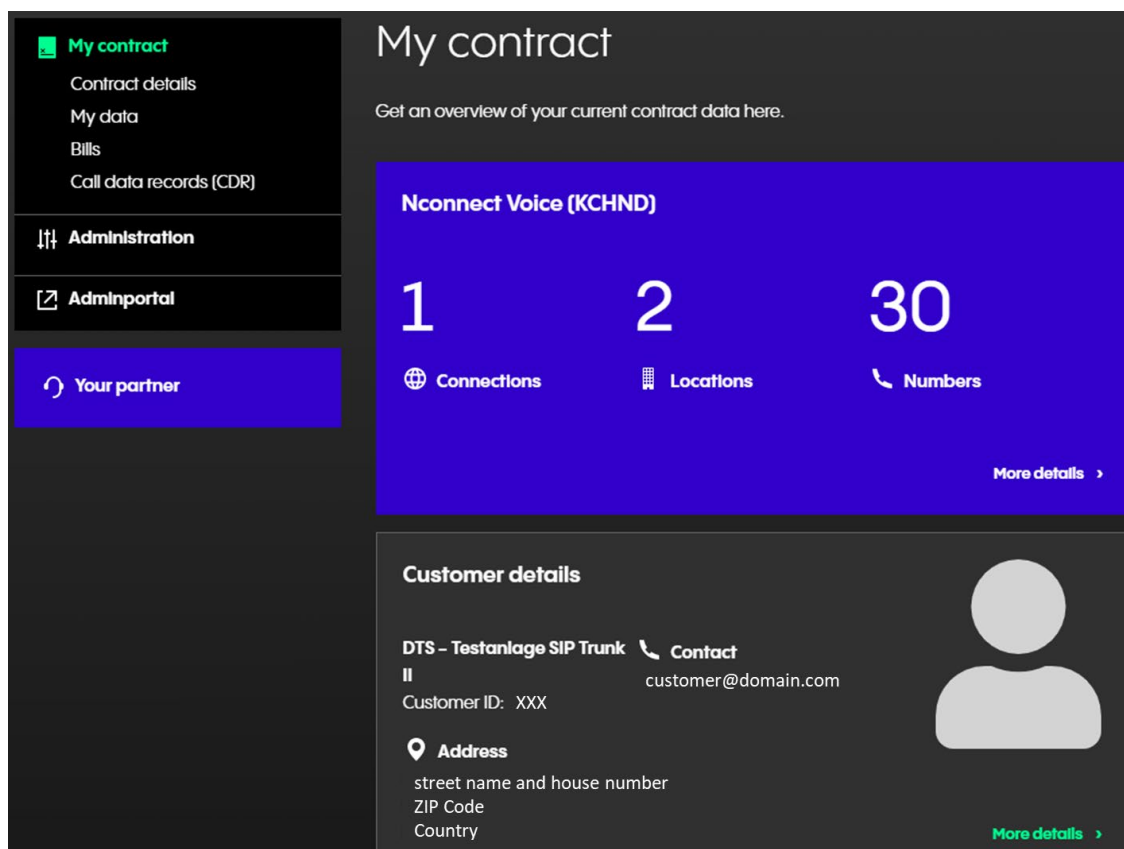
Access to the customer portal is via the username and password. When the order is completed, an email is sent to the customer with their customer number and a link to setup their password.

Access to the portal is at my.nfon.com:



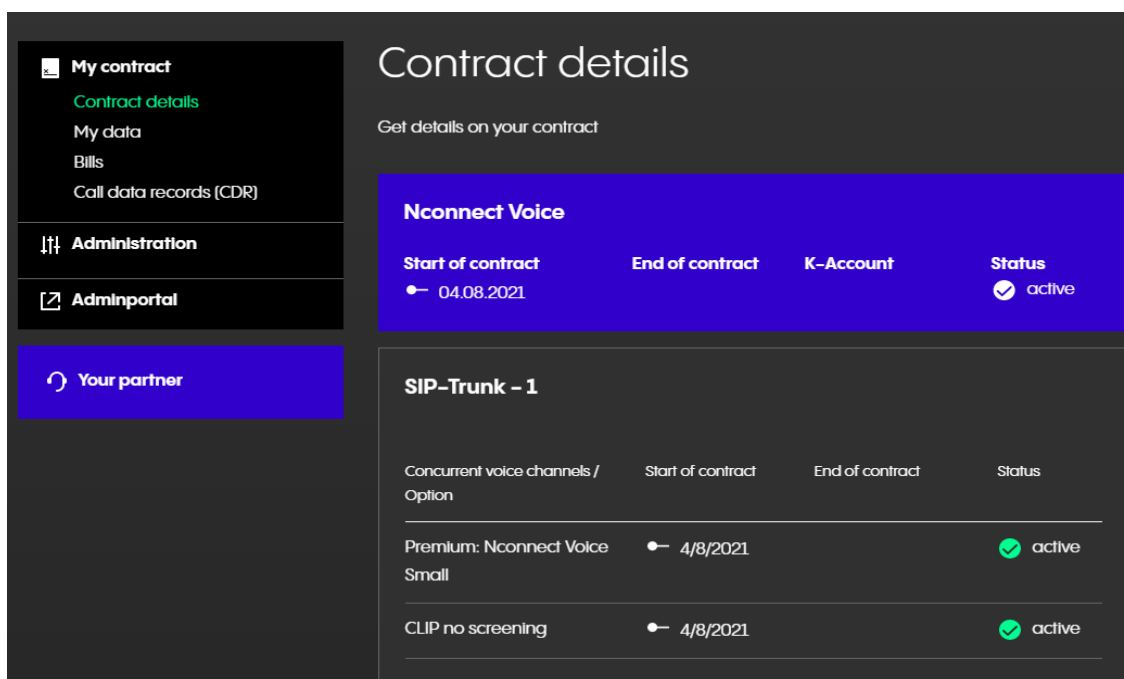
My contract

The landing page shows the customer's contract:



The screenshot shows the 'My contract' landing page. On the left is a sidebar with navigation links: 'My contract' (selected), 'Contract details', 'My data', 'Bills', 'Call data records (CDR)', 'Administration', 'Adminportal', and 'Your partner'. The main content area is titled 'My contract' and includes a sub-header 'Get an overview of your current contract data here.' Below this is a blue card for 'Nconnect Voice (KCHND)' displaying three key metrics: '1' for Connections, '2' for Locations, and '30' for Numbers. A 'More details' link is present. Below the metrics is a 'Customer details' section with a profile icon and fields for 'DTS - Testanlage SIP Trunk II', 'Contact' (customer@domain.com), 'Customer ID: XXX', and 'Address' (street name and house number, ZIP Code, Country). Another 'More details' link is at the bottom right.

Within the contract details page, details pertaining to the contract can be checked e.g. minute packages, number blocks.



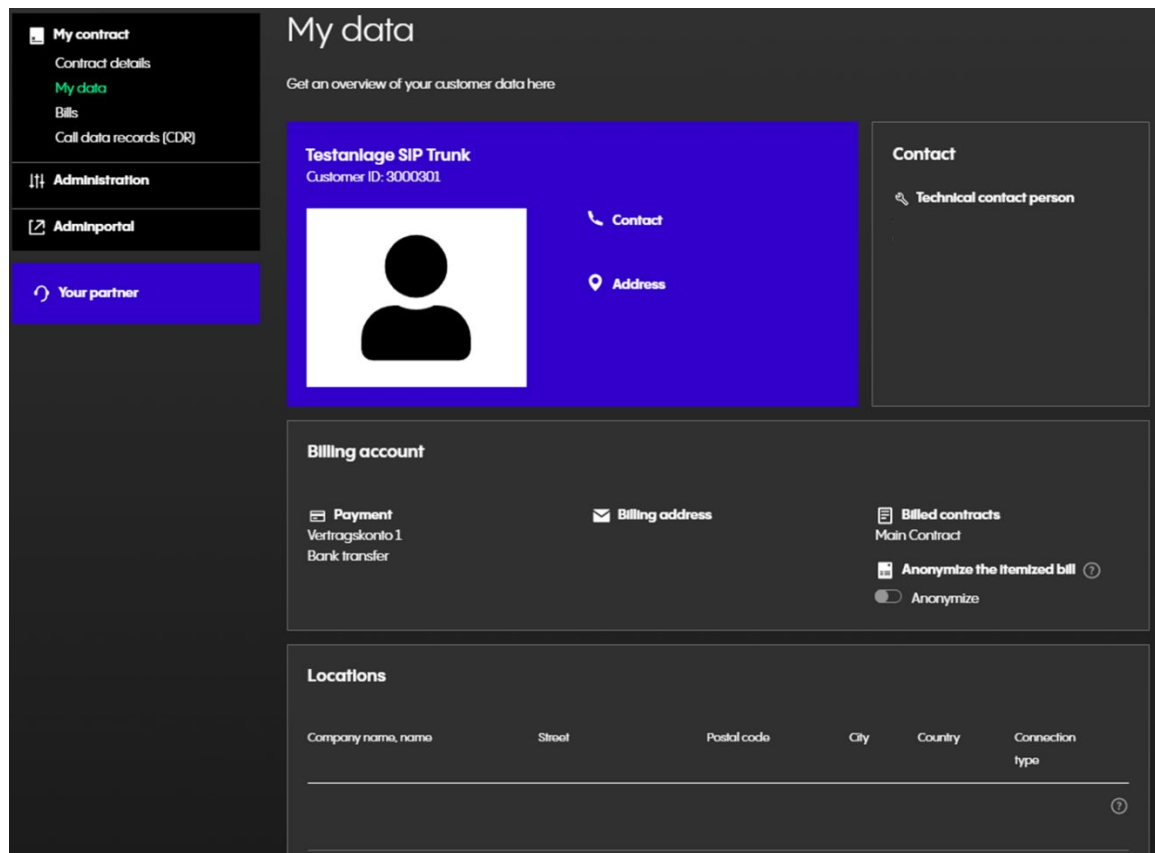
The screenshot shows the 'Contract details' page. The sidebar is identical to the previous page. The main content area is titled 'Contract details' and includes a sub-header 'Get details on your contract'. Below this is a blue card for 'Nconnect Voice' with a table showing contract details:

Start of contract	End of contract	K-Account	Status
04.08.2021			active

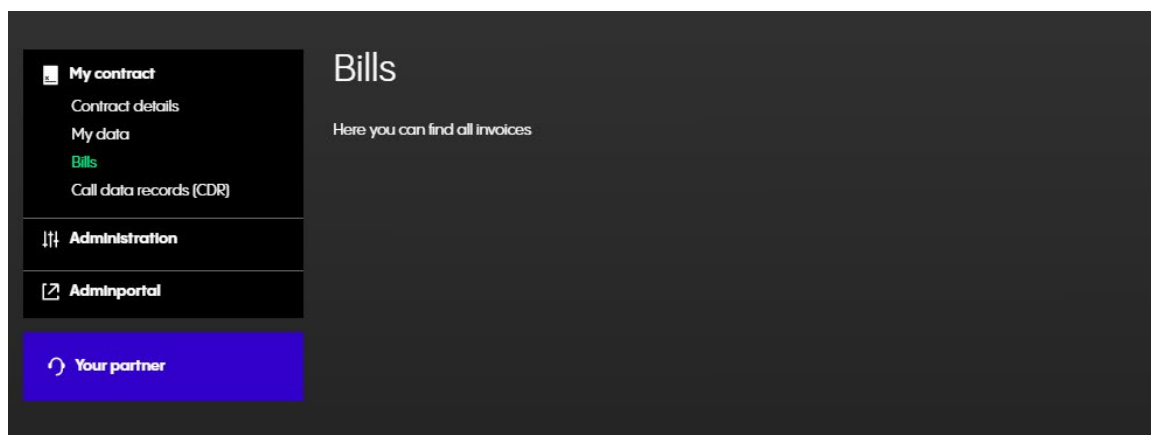
Below this is a section for 'SIP-Trunk - 1' with a table showing voice channel options:

Concurrent voice channels / Option	Start of contract	End of contract	Status
Premium: Nconnect Voice Small	4/8/2021		active
CLIP no screening	4/8/2021		active

"My data" shows the data stored about the customer



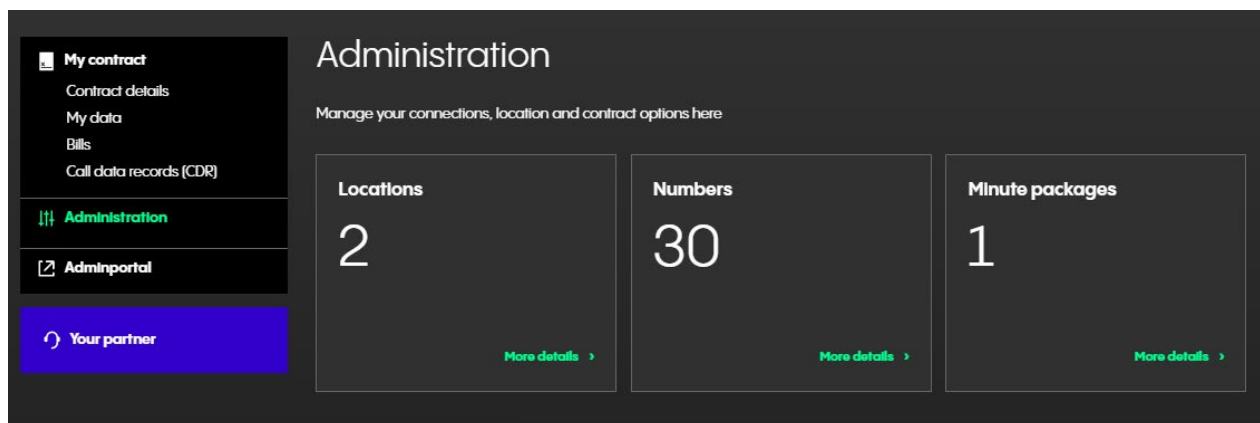
Using "Bills", the user can check and/or download their bills in .CSV or .PDF format:



Administration

This menu allows the user to do the following:

- check their locations
- check their numbers
- manage their minute packages




Microsoft Teams enablement – direct routing

SIP Trunk Flexx can be connected to MS Teams tenant to allow PSTN calling from/to a Microsoft Teams tenant (direct routing calls). This additional function has to be ordered explicitly in the order form.

It should be noted that the MS Teams tenant does not support high-availability features, i.e. it is not possible to connect two MS Teams tenants in parallel to achieve high availability. PSTN connectivity high availability is guaranteed by the NFON and Microsoft architecture.

In the case where a PBX is connected to SIP Trunk Flexx, the telephone functions supported by MS Teams can be used:



Call Queues	Auto Attendant	Call Parking	Call Transfer	Bild Transfer	Announce D-Transfer
✓	✓	✓	✓	✓	✓
Hold	Block calls with no Caller ID	Voicemail	eFax	Caller ID Policies	Central Phonebook
✓	✓	✓	✓	✓	✓
Skills	Time Control Service	Source Based Call-Forwarding	Phone No-Block (0-999 etc)	Fall-Back-To GSM Call (only with Cloudya clients)	
✗	✓	✗	✓	✗	

On top of that, security functions like blacklists incoming and outgoing, fraud detection, portals and backup are available.

Provisioning overview

Hereafter, you can find the provisioning process for the NFON integration with Microsoft Teams, which will allow you to connect the NFON multi-tenants Session Border Controller (SBC) to your Microsoft 365 tenant.

1. Order is accepted by NFON.
2. NFON sends the setup instructions to the customer technical contact, including the Session Border Controller (SBC) Fully Qualified Domain Name (FQDN)
3. The customer Microsoft 365 admin adds the SBC FQDN as an **additional DNS domain** into their Microsoft tenant.
4. The customer Microsoft 365 admin sends the verification code provided by the Microsoft admin portal to NFON (TXT record).
5. NFON notifies the customer Microsoft 365 admin when they can proceed with the verification of the additional DNS domain.
6. The customer Microsoft 365 admin completes the verification process on the Microsoft admin portal.
7. The customer Microsoft 365 admin informs NFON when the verification of the additional DNS domain has been completed, so that NFON can activate the SBC.
8. The customer Microsoft 365 admin activates the additional DNS domain in the Microsoft admin portal.
9. The NFON multi-tenants is connected and direct routing can now be configured.

Before getting started

- **Wait until NFON provides the SBC FQDN to your technical contact!**
- Ensure that you have appropriate rights and permissions for the Microsoft Office 365 tenant to which the SBC is being added.
- Adding the SBC requires an additional domain to the Microsoft Office 365 tenant.
- You can only add new domains if you sign into the **Microsoft 365 Admin Center** as a **global administrator**.

Adding the SBC FQDN as an additional domain

These are the steps to follow (in the right order) to complete the provisioning tasks:

1. Add the NFON SBC as an additional domain into your Microsoft Office 365 tenant.
2. Share the verification code with NFON (TXT record).
3. Complete the verification process.
4. Activate the additional domain on Microsoft Office 365.

Adding a new domain to Microsoft Office 365

- Log into the [Microsoft Admin Centre](#) as a global administrator.
- In the Microsoft 365 Admin Center, go to **Settings > Domains**.
- Click on Add domain.
- In the **Domain name** box, enter the SBC FQDN that NFON has provided to you (example FQDN: KBUY9-01.customers.teams-pbx.cloud).
- Click on "Next".
- As the SBC FQDN has never been registered as a domain in the Microsoft 365 tenant, in this next step you will have to verify the domain. Select **Add a TXT record**.

- Click on "Next" and note the TXT record value provided to verify the domain name.
- Once you have made a note of the TXT record name and value, you can click on "Close".

Sharing the verification code with NFON

Email the TXT record and the details shown below to the email address that has been provided to the technical contact when NFON confirmed the SBC FQDN details:

Example:

To: <email address provided by NFON>

Subject: KBUY9-01 - MS Teams Direct Routing Activation

- Teams SBC : KBUY9-01.customers

- TXT Verification: MS=1234567

Completing the verification process

- Log in to the [Microsoft Admin Centre](#) as a global administrator.
- Go back to **Settings > Domains**.
- The SBC FQDN domain will appear with a status of incomplete setup.
- Click on the domain name.
- Click on "Start setup".
- On the verify domain screen, click on "Verify".
- If you get an error message stating that there's a missing record:
 - Check the details of the TXT value you have provided to NFON.
 - Wait for a few minutes and try again (DNS record replication can take up to 60 minutes to fully propagate).
- On the "Choose your online services" page, clear all options and click on "Next".
- Click on "Finish" on the Update DNS settings page.
- Now that you have completed the SBC FQDN setup by adding it as a domain, **you have to inform NFON**.
- To do this, reply to the email you have received to inform you that the domain is ready to be verified.
- **Wait for NFON to confirm that the SBC has been activated.**

Activating the additional domain on Microsoft Office 365

- Log into the [Microsoft Admin Centre](#) as a global administrator.
- Go to **Users > Active Users**.
- In the active users page, click on Add a user.
- Set up the basics as follows:
 - **First name:** Kxxxx SBC (example: **KBUY9 SBC**)
 - **Last name:** Activation (example: Activation)
 - **Display name:** Kxxxx SBC Activation (example: **KBUY9 SBC Activation**)
 - **Username / Domain:** sbcactivation / kxxxx-01.customers.teams-pbx.cloud (example: **sbcactivation / kbuy9-01.customers.teams-**)
 - **Password settings:** Auto Generate

- **License required:** Assign licence(s) to this user that includes Phone System (See the licensing options article for more information about the right licences combination)
- Click on "Next".
- Assign a licence to this user, which includes the Phone System app.
 - To do this, expand the Apps section and scroll down to check that Phone System is enabled.
- From the previous step, click on "Next".
- Click on "Next" again.
- Click on "Finish adding".

Configuration for NFON standard integration

Microsoft Teams tenant configuration

Before starting the call routing configuration on the Microsoft phone system (i.e. direct routing), you should:

1. have added the additional domain that is required for the connection into the NFON multi-tenant Session Border Controller (SBC); The following provisioning process will allow you to connect the NFON multi-tenants Session Border Controller (SBC) to your Microsoft 365 tenant.
2. be familiar with PowerShell and have installed the PowerShell module for Microsoft Teams (for more information about PowerShell, please visit the [Microsoft Documentation website](#)). Installation instructions for this module are available in the documentation article on the Microsoft website: [Install Microsoft Teams PowerShell Module](#).

NFON PBX endpoint configuration

Before starting to configure direct routing in your MS Teams tenant, you should ensure that NFON has activated the SBC. To do so, log in to the SIP Trunk Flexx configuration portal.

<div>User</div> <div>Nconnect Voice</div> <div>Trunkset</div> <div>PBX Endpoint</div> <div>Microsoft Teams</div>	MICROSOFT TEAMS			
	Name	PBX Endpoint Template	Active	Priority
	Teams Endpoint	Primary	Microsoft TEAMS	<div> <div></div> <div></div> </div>

- Click on "**PBX Endpoint**".
- Click on the "+" icon to add a new PBX endpoint.
- Select the "**Microsoft Teams**" (Auth: MS Teams) template.
- Once you have selected the template the SBC address should be listed in the "MS Teams domain" dropdown box.

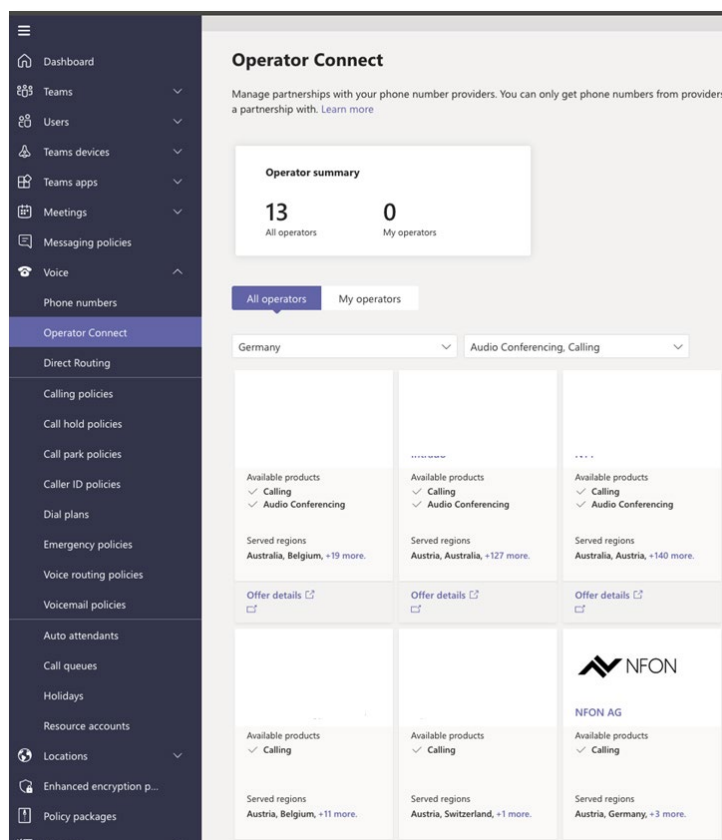
Microsoft Teams enablement – Operator Connect

Operator Connect is the plug-and-play alternative to direct routing proposed by Microsoft. It allows the customer to connect Microsoft Teams to the PSTN network via NFON's SIP trunk Flexx with almost zero administrative effort. On the SIP Trunk Flexx side there are not any changes; Microsoft Teams is basically a PBX like Avaya or Cisco, we just add it as a supported PBX configuration.

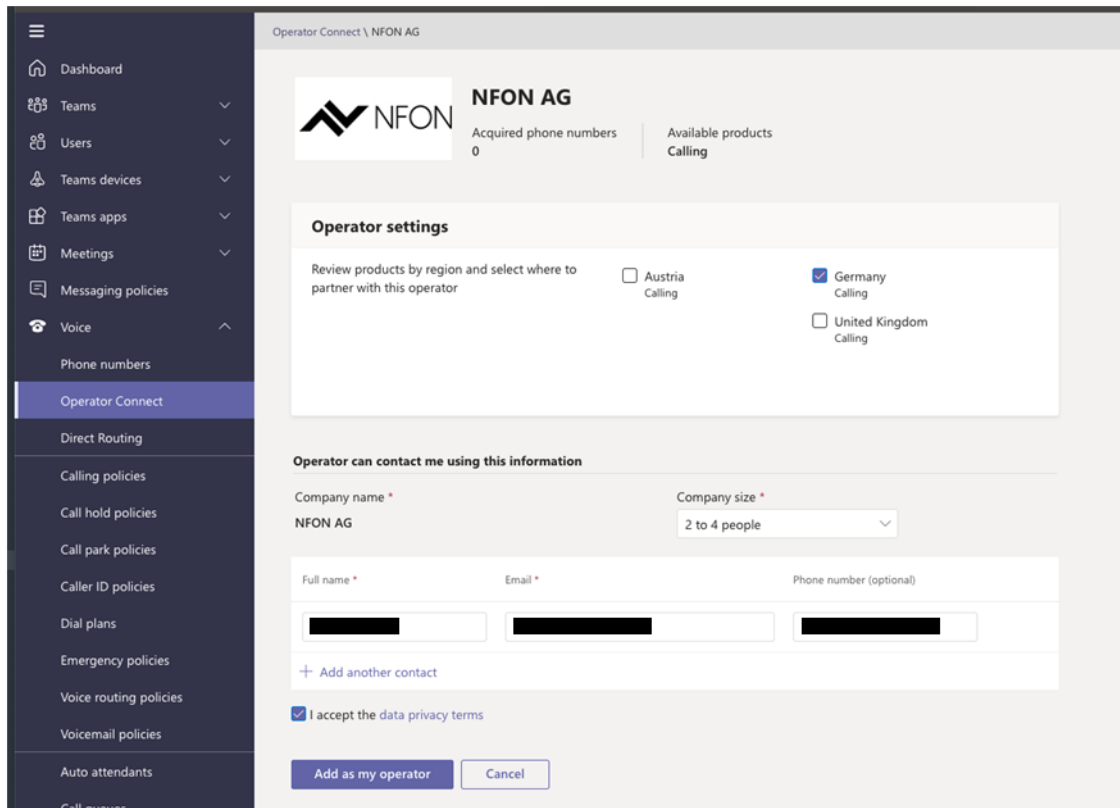
NFON is now listed as an operator in the Teams Admin Center and the [Microsoft Cloud Partners directory](#).

Customer on-boarding via Operator Connect

1. The customer uses the Teams Admin Center and selects NFON as SIP trunk operator:
<https://admin.teams.microsoft.com/operators/c5715995-a037-4b75-b95f-7d97d942df9e/add>



- From there, a request can be sent to NFON that includes the country, company size, and contact information:



Operator Connect \ NFON AG

NFON AG

Acquired phone numbers: 0

Available products: Calling

Operator settings

Review products by region and select where to partner with this operator

☐ Austria Calling

☒ Germany Calling

☐ United Kingdom Calling

Operator can contact me using this information

Company name *: NFON AG

Company size *: 2 to 4 people

Full name *: [Redacted]

Email *: [Redacted]

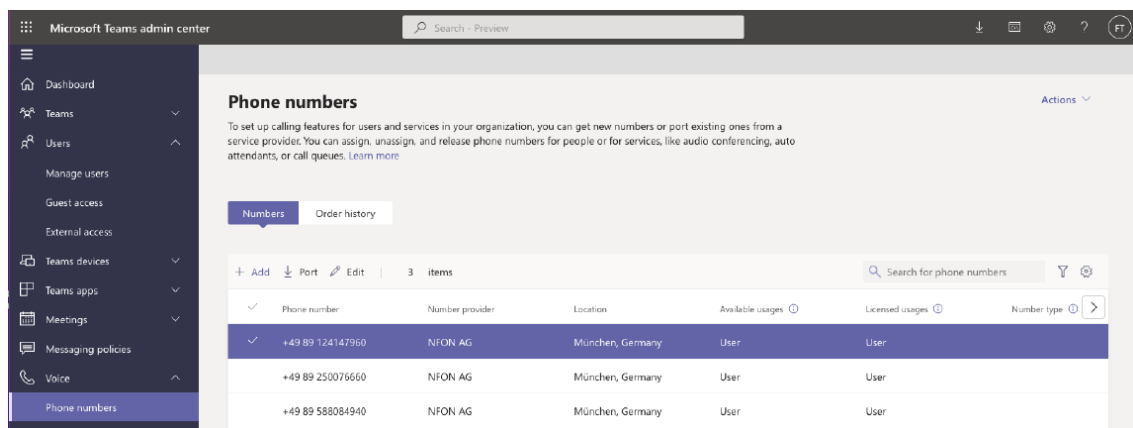
Phone number (optional): [Redacted]

[+ Add another contact](#)

☒ I accept the data privacy terms

[Add as my operator](#) [Cancel](#)

- After clicking on "Add as my Operator", the request is sent to Microsoft and available for NFON to be processed.
- The customer is contacted by NFON to receive all the information needed to configure a SIP Trunk sized in line with business needs.
- After a contract is signed, the SIP trunk Flexx is activated.
- Phone numbers are uploaded automatically to the Microsoft Teams tenant and become visible in the Teams Admin Center.



Microsoft Teams admin center

Search - Preview

Phone numbers

To set up calling features for users and services in your organization, you can get new numbers or port existing ones from a service provider. You can assign, unassign, and release phone numbers for people or for services, like audio conferencing, auto attendants, or call queues. [Learn more](#)

Numbers Order history

[+ Add](#) [↓ Port](#) [✎ Edit](#) | 3 items

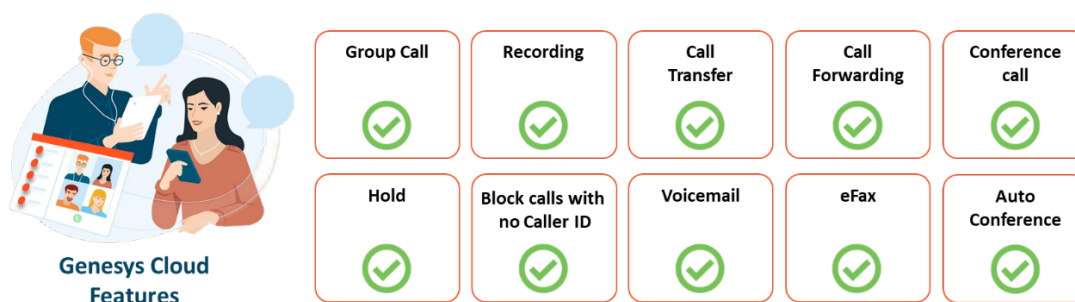
Search for phone numbers

✓	Phone number	Number provider	Location	Available usages ⓘ	Licensed usages ⓘ	Number type ⓘ
✓	+49 89 124147960	NFON AG	München, Germany	User	User	
	+49 89 250076660	NFON AG	München, Germany	User	User	
	+49 89 588084940	NFON AG	München, Germany	User	User	

- Phone numbers can now be assigned to the Teams users and used without any need of using the SIP Trunk Flexx configuration portal.

Genesys cloud enablement

SIP Trunk Flexx can be connected to Genesys cloud tenant to allow PSTN calling from/to a Genesys Cloud tenant. High availability of Genesys Cloud tenant is guaranteed by Genesys. PSTN connectivity high availability is guaranteed by the NFON. In the case where a PBX is connected to SIP trunk, the telephony features that are supported by Genesys cloud can be used:



Provisioning overview

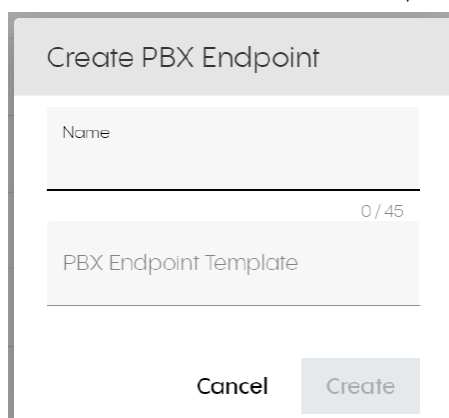
Hereafter you can find the provisioning process which will allow you to connect SIP trunk Flexx to your Genesys cloud tenant:

- The customer has to book the Genesys cloud service from Genesys or a solution partner.
- The customer receives the domain from Genesys (mandatory)
Example domain: bodedt.byoc.mypurecloud.de
- Customer has to book a SIP Trunk Flexx from NFON to enable a SIP trunk with Genesys (this additional function has to be ordered explicitly in the order form).

Configuration of Genesys PBX endpoint

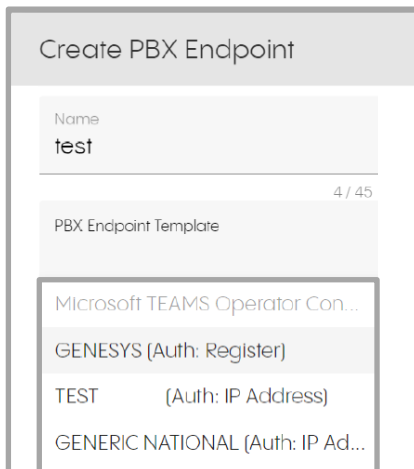
Log in to the SIP Trunk Flexx configuration portal and do the following:

- Click on **"PBX endpoint"**.
- Click on the **"+"** icon to create/add a new PBX endpoint.

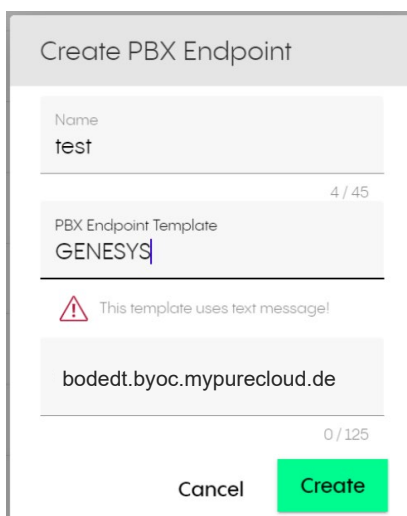


The screenshot shows a form titled "Create PBX Endpoint". It contains two input fields: "Name" and "PBX Endpoint Template". The "Name" field has a character count "0 / 45" next to it. At the bottom of the form, there are two buttons: "Cancel" and "Create".

- Select a PBX endpoint name and the **"Genesys"** PBX endpoint template.



- Fill in the domain previously received from Genesys (example: *bodedt.byoc.mypurecloud.de*).
- Click on **"Create"**.



- Click on **"Send Text message"** in order to send your credentials.

test

Name

test

4 / 45

PBX Endpoint Template

GENESYS

⚠

This template uses text message!

bodedt.byoc.mypurecloud.de

10 / 125

Cancel

Send text message

Examples

The purpose of the following examples is to provide a reference for the SIP header contents in the SIP messaging between the customer's PBX and the NFON platform.

By manually configuring the SIP headers from the customer's PBX to match the format provided, SIP trunk should work properly.



Attention: IP addresses within these examples are artificial.

For the live traffic, please use the FQDN of the NFON Registrar.

Reference setup

Setting	Value	Note
Registrar Public IP	siptrunk.cloud-cfg.com	
PBX Public IP	101.222.10.33	Arbitrary public or private IP address of the PBX
Username	Kwxyz12345	Provided at: siptrunk.cloud-cfg.com
DDIs	+49 322 222 8516 (0-9)	

Register PBX → NFON

The initial REGISTER send from the PBX to the NFON platform

```
From: <sip:Kwxyz12345@ siptrunk.cloud-cfg.com >;tag=a5065835-ff58-45a8-a15b-195c93c60153
To: sip:Kwxyz12345@ siptrunk.cloud-cfg.com
Call-ID: a96da278-493d-4d35-b7d1-90444d9d9369
CSeq: 4048 REGISTER
Contact:
sip:Kwxyz12345@101.222.10.33:5060
Expires: 3600
Allow: OPTIONS, REGISTER, SUBSCRIBE, NOTIFY, PUBLISH, INVITE, ACK, BYE, CANCEL,
UPDATE,PRACK, MESSAGE, REFER
Max-Forwards: 70
User-Agent: Asterisk PBX 16.11.1
Authorization: Digest username="Kwxyz12345", realm=" siptrunk.cloud-cfg.com ",
nonce="<encrypted data>", uri="sip:siptrunk.cloud-cfg.com:5060",
response="<encrypted data>"
Content-Length: 0
```

Register message with DDI number instead of K- number within FROM, TO and CONTACT header is accepted as well – using the format +49322xxx or 49322xxx

Invite incoming call

INVITE NFON → PBX with CLIP (E.164 number format)

Incoming call to DDI +49322222851601 from
:+4921096000INBOUND-INVITE, CLIP, E.164 numbers
INVITE sip: +49322222851601@101.222.10.33:5060 SIP/2.0
Record-Route:
sip:102.222.10.33;r2=on;lr;ftag=6+9160e5a6+6bf72685 Record-
Route: sip:103.222.10.33;r2=on;lr;ftag=6+9160e5a6+6bf72685
Via: SIP/2.0/UDP
102.222.10.33:5060;branch=z9hG4bK9cd7.f04663d6.0Via:
SIP/2.0/UDP
103.222.10.33:5160;rport=5160;received=103.222.10.33;branch=z9hG4bK+466cb2808baa04ed5dd8
76fd3e62a18c1+sip+6+a64e0a07
From: "the callers name"
<sip:+4921096000@td>;tag=6+9160e5a6+6bf72685To:
sip:+49322222851601@nfon.net
CSeq:28809 INVITE
Expires: 180
Content-Length: 242
Supported: timer,replaces,norefersub,100rel
Contact:
sip:5e5745f26e971c407da0cce44de4d533@10.111.222.44:5160;transport=udp
Content-Type: application/sdp
Call-ID: 252df563e4606ec155758467025751e7
Allow: OPTIONS, REGISTER, SUBSCRIBE, NOTIFY, PUBLISH, INVITE, ACK, BYE, CANCEL,
UPDATE,PRACK, MESSAGE, REFER, INFO
Session-Expires: 1800
Min-SE: 90
Max-Forwards: 65
Accept: application/sdp,
application/dtmf-relayv=0
o=- 118897834547758 118897834547758 IN IP4 10.111.222.44
s=-
c=IN IP4 10.111.222.44
t=0 0
m=audio 32950
RTP/AVP 8 101
a=sendrecv
a=rtpmap: 8 PCMA/8000
a=rtpmap: 101 telephone-event/8000
a=fmtp: 101 0-16
a=maxptime: 150
a=ptime: 20

INVITE NFON → PBX with CLIP (national number format)

Incoming call to DDI +49322222851601 from
:+49210960000INBOUND-INVITE, CLIP, national
numbers
INVITE sip: 0322222851601@101.222.10.33:5060 SIP/2.0
Record-Route:
sip:102.222.10.33;r2=on;lr;ftag=6+9160e5a6+6bf72685 Record-
Route: sip:103.222.10.33;r2=on;lr;ftag=6+9160e5a6+6bf72685
Via: SIP/2.0/UDP
102.222.10.33:5060;branch=z9hG4bK9cd7.f04663d6.0Via:
SIP/2.0/UDP
103.222.10.33:5160;rport=5160;received=103.222.10.33;branch=z9hG4bK+466cb2808baa04ed5dd8
76fd3e62a18c1+sip+6+a64e0a07
From: "the callers name"
<sip:0210960000@td>;tag=6+9160e5a6+6bf72685To:
sip:0322222851601@nfon.net
CSeq:28809 INVITE
Expires: 180
Content-Length: 242
Supported: timer,replaces,norefersub,100rel
Contact:
sip:5e5745f26e971c407da0cce44de4d533@10.111.222.44:5160;transport=udp
Content-Type: application/sdp
Call-ID: 252df563e4606ec155758467025751e7
Allow: OPTIONS, REGISTER, SUBSCRIBE, NOTIFY, PUBLISH, INVITE, ACK, BYE, CANCEL,
UPDATE,PRACK, MESSAGE, REFER, INFO
Session-Expires: 1800
Min-SE: 90
Max-Forwards: 65
Accept: application/sdp,
application/dtmf-relayv=0
o=- 118897834547758 118897834547758 IN IP4 10.111.222.44
s=-
c=IN IP4 10.111.222.44
t=0 0
m=audio 32950
RTP/AVP 8 101
a=sendrecv
a=rtpmap: 8 PCMA/8000
a=rtpmap: 101 telephone-event/8000
a=fmtp: 101 0-16
a=maxptime: 150
a=ptime: 20

INVITE NFON → PBX with CLIR

Incoming call to DDI +,34932222851601 from "anonymous" (unknown calling party) INBOUND-INVITE, CLIR, national numbers
INVITE sip: 0322222851601@101.222.10.33:5060 SIP/2.0
Record-Route:
sip:102.222.10.33;r2=on;lr;ftag=1+d5ba10ee+d7a3c469 Record-Route: sip:103.222.10.33;r2=on;lr;ftag=1+d5ba10ee+d7a3c469
Via: SIP/2.0/UDP
102.222.10.33:5060;branch=z9hG4bK10eb.4c661622.0Via:
SIP/2.0/UDP
103.222.10.33:5160;rport=5160;received=103.222.10.33;branch=z9hG4bK+3d89a857a2daab8a40af0224bf0b3aec1+sip+1+a64e0a88
From:
<sip:anonymous@td>;tag=1+d5ba10ee+d7a3c46
9To: sip:0322222851601@nfon.net
CSeq: 22377 INVITE
Expires: 180
Content-Length: 238
Supported: timer,replaces,norefersub,100rel
Contact:
sip:5e5745f26e971c407da0cce44de4d533@10.111.222.44:5160;transport=udp
Content-Type: application/sdp
Call-ID: ca1eabe3b78eaf01622d30882e637987
Allow: OPTIONS, REGISTER, SUBSCRIBE, NOTIFY, PUBLISH, INVITE, ACK, BYE, CANCEL, UPDATE,PRACK, MESSAGE, REFER, INFO
Session-Expires: 1800
Min-SE: 90
Max-Forwards: 65
Accept: application/sdp,
application/dtmf-relayv=0
o=- 9298861535403 9298861535403 IN IP4 10.111.222.44
s=-
c=IN IP4 10.111.222.44
t=0 0
m=audio 33394
RTP/AVP 8 101
a=sendrecv
a=rtpmap: 8 PCMA/8000
a=rtpmap: 101 telephone-event/8000
a=fmtp: 101 0-16
a=maxptime: 150
a=ptime: 20

Invite outgoing call

INVITE PBX → NFON with CLIP (E.164 number format)

Outgoing call from DDI 0322222851601 to
021096001OUTBOUND-INVITE, CLIP, E.164
numbers
INVITE sip:+4921096001@101.222.10.33 SIP/2.0
Via: SIP/2.0/UDP 102.222.10.33:5060;rport;branch=z9hG4bKPj6aee2878-23e7-
4197-a12f-767694ed85ec
From: <sip:+49322222851601@nfon.com>;tag=a08fb153-44ee-4c57-aac9-
130114691a0dTo: sip:+4921096001@101.222.10.33
Contact: sip:asterisk@102.222.10.33:5060
Call-ID: 486c2aeb-8e33-4de5-bc9f-
6f87a17da320CSeq: 10775 INVITE
Allow: OPTIONS, REGISTER, SUBSCRIBE, NOTIFY, PUBLISH, INVITE, ACK, BYE, CANCEL,
UPDATE,PRACK, MESSAGE, REFER
Supported: 100rel, timer, replaces,
norefersubSession-Expires: 1800
Min-SE: 90
P-Asserted-Identity:
sip:+49322222851601@nfon.com;user=phoneMax-
Forwards: 70
User-Agent: Asterisk PBX 16.11.1
Authorization: Digest username="<user-name>", realm="nfon.com", nonce="<encrypted
data>",uri="sip:021096001@101.222.10.33", response="<encrypted data>"
Content-Type:
application/sdp
Content-Length: 243
v=0
o=- 2081109992 2081109992 IN IP4 102.222.10.33
s=Asterisk
c=IN IP4 102.222.10.33
t=0 0
m=audio 19054 RTP/AVP 8 101
a=rtpmap: 8 PCMA/8000
a=rtpmap: 101 telephone-event/8000
a=fmtp: 101 0-16
a=ptime: 20
a=maxpti
me: 150
a=sendrec
v

INVITE PBX → NFON with CLIP (national number format)

Outgoing call from DDI 0322222851601 to
021096001OUTBOUND-INVITE, CLIP, national
numbers
INVITE sip: 021096001@101.222.10.33 SIP/2.0
Via: SIP/2.0/UDP 102.222.10.33:5060;rport;branch=z9hG4bKPj7ab88620-3f47-
4e05-a273-6fabe3f53ed8
From: <sip:0322222851601@nfon.com>;tag=a2f713d5-3174-41d1-9b46-
81d90084036dTo: <sip:021096001@101.222.10.33>
Contact: <sip:asterisk@102.222.10.33:5060>
Call-ID: 3534c70b-1f20-47e0-81bb-
b3f2072bbd00CSeq: 5965 INVITE
Allow: OPTIONS, REGISTER, SUBSCRIBE, NOTIFY, PUBLISH, INVITE, ACK, BYE, CANCEL,
UPDATE,PRACK, MESSAGE, REFER
Supported: 100rel, timer, replaces,
norefersubSession-Expires: 1800
Min-SE: 90
P-Asserted-Identity:
<sip:0322222851601@nfon.com;user=phone>Max-
Forwards: 70
User-Agent: Asterisk PBX 16.11.1
Authorization: Digest username="<user-name>", realm="nfon.com", nonce="<encrypted
data>",uri="sip:021096001@101.222.10.33", response="<encrypted data>"
Content-Type:
application/sdp
Content-Length: 242
v=0
o=- 1423454714 1423454714 IN IP4 102.222.10.33
s=Asterisk
c=IN IP4 102.222.10.33
t=0 0
m=audio 9706
RTP/AVP 8 101
a=rtpmap:8
PCMA/8000
a=rtpmap: 101 telephone-event/8000
a=fmtp: 101 0-16
a=ptime: 20
a=maxpti
me: 150
a=sendrec
v

INVITE PBX → NFON with CLIR

Outgoing call from DDI 0322222851601 to 021096001 with calling party number suppressed "anonymous"

OUTBOUND-INVITE, CLIR, national numbers

```
INVITE sip: 021096001@101.222.10.33 SIP/2.0
Via: SIP/2.0/UDP 102.222.10.33:5060;rport;branch=z9hG4bKPjb95874f3-227c-4382-9852-06fb17bb0fdf
From: "anonymous" <sip:anonymous@anonymous.invalid>;tag=3710ecde-8b95-4646-a4e2-e8ecf1edf3ed
To: sip:021096001@101.222.10.33
Contact: sip:asterisk@102.222.10.33:5060
Call-ID: 0ef52492-f85d-4288-8fb6-84dc9364d7e6CSeq: 20155 INVITE
Allow: OPTIONS, REGISTER, SUBSCRIBE, NOTIFY, PUBLISH, INVITE, ACK, BYE, CANCEL, UPDATE, PRACK, MESSAGE, REFER
Supported: 100rel, timer, replaces, norefersub
Session-Expires: 1800
Min-SE: 90
P-Asserted-Identity: sip:0322222851601@nfon.com;user=phone
Max-Forwards: 70
User-Agent: Asterisk PBX 16.11.1
Authorization: Digest username="<user-name>", realm="anonymous.invalid",
nonce="<encrypteddata>", uri="sip:021096001@101.222.10.33", response="<encrypted data>"
Content-Type:
application/sdpContent-
Length: 241
v=0
o=- 311382222 311382222 IN IP4 102.222.10.33
s=Asterisk
c=IN IP4 102.222.10.33
t=0 0
m=audio 14776 RTP/AVP 8 101
a=rtpmap: 8 PCMA/8000
a=rtpmap: 101 telephone-event/8000
a=fmtp: 101 0-16
a=ptime: 20
a=maxptime: 150
a=sendrecv
```

Alternatively, privacy header can be used (privacy id)

Emergency call

INVITE PBX → NFON emergency service number

Outgoing call from DDI +493222228516 to 112
OUTBOUND-INVITE, Emergency
INVITE sip: 112@101.222.10.33 SIP/2.0
Via: SIP/2.0/UDP 102.222.10.33:5060;rport;branch=z9hG4bKPjcbf9b900-4e88-4319-8052-2f6181f7b321
From: "+493222228516" <sip:+4932222285160@nfon.com>;tag=2f8e248e-ecef-4722-ab79-950b9b9cdfa8
To: sip:112@101.222.10.33
Contact: sip:asterisk@102.222.10.33:5060
Call-ID: e9e09267-3545-4fbf-b5b7-89d59e1b43c3CSeq: 30547 INVITE
Allow: OPTIONS, REGISTER, SUBSCRIBE, NOTIFY, PUBLISH, INVITE, ACK, BYE, CANCEL, UPDATE, PRACK, MESSAGE, REFER
Supported: 100rel, timer, replaces, norefersubSession-Expires: 1800
Min-SE: 90
P-Asserted-Identity:
sip:+49322222851601@nfon.com;user=phoneMax-Forwards: 70
User-Agent: Asterisk PBX 16.11.1
Authorization: Digest username="<user-name>", realm="nfon.com", nonce="<encrypted data>", uri="sip:021096001@101.222.10.33", response="<encrypted data>"
Content-Type:
application/sdpContent-Length: 242
v=0
o=- 2033286139 2033286139 IN IP4 102.222.10.33
s=Asterisk
c=IN IP4 102.222.10.33
t=0 0
m=audio 8314 RTP/AVP 8 101
a=rtpmap: 8 PCMA/8000

a=rtpmap: 101 telephone-event/8000
a=fmtp: 101 0-16
a=ptime: 20
a=maxptime:
150a=sendrecv

Call forwarding with redirect (302)

302 MOVED TEMPORARILY PBX → NFON

Incoming call forwarded to
+4921096001302 Redirect for an
incoming call
SIP/2.0 302 Moved
TemporarilyVia:
SIP/2.0/UDP
101.222.10.33:5060;rport=5060;received=101.222.10.33;branch=z9hG4bK10dd.6048
211.0 Via: SIP/2.0/UDP 102.222.10.33:5160;rport=5160;
received=102.222.10.33;branch=z9hG4bK+f0a158dfe92819ce2074a53190a12581+sip+6+a64
e0b07 Record-Route: sip:101.222.10.33:5060;lr;r2=on;ftag=6+5d6972fc+144a91b2
Record-Route:
sip:103.222.10.33;lr;r2=on;ftag=6+5d6972fc+144a91b2Call-ID:
1940fe68e00e2de7021a4ae7451fe93c
From: "test-carrier" <sip:+4921096000@td>;tag=6+5d6972fc+144a91b2
To: <sip:+4932222851601@nfon.net>;tag=156d6b6f-3b25-42e8-b893-
47ffe2304164CSeq: 6350 INVITE
Server: Asterisk PBX 16.11.1
Contact: sip:+4921096001@101.222.10.33
Reason:
Q.850;cause=0
Content-Length:
0

DTMF

DTMF via FRC 2833

Negotiated codec number in SDP for telephone-event: 101

Start DTMF tone (first packet) -

digit '6'Raw Binary Packet:

0000 80 e5 57 a2 22 82 73 38 3c 07 33 8f 06 0a 00 a0 ..W.".s8<.3.....

Decoded:

Real-Time Transport Protocol

10 = Version: RFC 1889 Version (2)

..0 = Padding: False

...0 = Extension: False

.... 0000 = Contributing source identifiers

count: 01 = Marker: True

Payload type: telephone-event (101)

Sequence number: 22434

[Extended sequence number:

87970]Timestamp: 578974520

Synchronization Source identifier: 0x3c07338f

(1007104911)RFC 2833 RTP Event

Event ID: DTMF Six

6 (6) 0 = End of

Event: False

.0 = Reserved: False

..00 1010 = Volume: 10

Event Duration: 160

End DTMF tone (first 'end'

packet)Raw Binary Packet:

0000 80 65 57 a9 22 82 73 38 3c 07 33 8f 06 8a 05 00 .eW.".s8<.3.....

Decoded:

Real-Time Transport Protocol

10 = Version: RFC 1889 Version (2)

..0 = Padding: False

...0 = Extension: False

.... 0000 = Contributing source identifiers

count: 00 = Marker: False

Payload type: telephone-event (101)

Sequence number: 22441

[Extended sequence number:

87977]Timestamp: 578974520

Synchronization Source identifier: 0x3c07338f (1007104911)

RFC 2833 RTP Event

Event ID: DTMF Six
6 {6}1 = End of
Event: True
.0. = Reserved: False
..00 1010 = Volume: 10
Event Duration: 1280

Terminology

Term	Description
Customer	<ul style="list-style-type: none"> ▪ Person or organization that orders, uses and pays for NFON services. ▪ A customers can have different sites in one or more countries.
Customer site	<ul style="list-style-type: none"> ▪ The customer site is the location where the customer is resident. It has a defined postal address. ▪ The customer site is important for emergency calls.
SIP user	<ul style="list-style-type: none"> ▪ The SIP user identifies the connected entity (usually a PBX) at a PBX endpoint located at the customer ▪ A SIP user authenticates either by a fixed IP address or with user/password credentials. ▪ SIP users also exist for IP authenticated connections.
Trunk set	<ul style="list-style-type: none"> ▪ It is the entity number blocks are assigned to. A trunk set can have multiple number blocks assigned. ▪ It combines 1 to N trunks, that share the same number block. ▪ A PBX endpoint can belong to only one single trunk set. ▪ The simplest trunk set has a single PBX endpoint and a single number block assigned.
Number block	<ul style="list-style-type: none"> ▪ A number block is a consecutive range of numbers. ▪ It is assigned to a single trunk set (while a trunk set can have multiple number blocks). ▪ Sub-ranges of a number block can be assigned to a different trunk set. ▪ The smallest sub-range is a single number.

Abbreviations

CLIR	Calling Line Identification Restriction
COLP	Connected Line Presentation
COLR	Connected Line Presentation Restriction
DDI / DID	Direct Dialing Inward / Direct Inward Dialing
DN	Directory Number
FQDN	Fully Qualified Domain Name
LAC	Local Area Code
MS	Microsoft
PAI	P-Asserted Identity
PBX	Private Branch Exchange
PSTN	Public switched Telephone Network (Fixed Net)
RTP	Real Time Protocol
SRTP	Secure Real Time Protocol
TLS	Transport Layer Security