General Guidelines for SIP Trunking Installations

1) ***How do I setup my SIP trunk for inbound/outbound calling?***

We authenticate IP-PBX SIP Trunking traffic by:

IP Authentication (IP address) ***or***
Digest Authentication (service account and PIN)

After you decide which switch platform to use, you will need to establish a SIP trunk with our proxy server (ippbx.net2phone.com port 5060) and input your IP address into our portal or register your switch with us.

IP Authentication *(IP Address)*
The IP Authentication method should be used when you have a static IP-PBX IP Address. IP Authentication provides enhanced security since your SIP trunk can only be used from the IP Address you provide.

On open source applications (such as Asterisk), you can setup your SIP trunk with IP Authentication as follows:

Outgoing Settings:

```
[out-1]
type=peer
port=5060
nat=auto
insecure=invite
ignoresdpversion=yes
host=ippbx.net2phone.com
dtmfmode=rfc2833
context=from-trunk
canreinvite=no
allow=ulaw
allow=g729
```

Incoming Settings:

```
[in-1]
disallow=all
type=peer
port=5060
nat=auto
insecure=invite
host=169.132.136.9
dtmfmode=rfc2833
context=from-trunk
canreinvite=no
allow=ulaw
allow=g729
```

```
[in-2]
disallow=all
type=peer
port=5060
nat=auto
insecure=invite
host=66.33.167.74
dtmfmode=rfc2833
context=from-trunk
canreinvite=no
allow=ulaw
allow=g729
```

If you are using a web-based Asterisk PBX (like FreePBX), IP Authentication setup is slightly different:

In "Outgoing Settings", name the section "out-1"
Then, in "Peer Detail", enter the following:

type=peer
port=5060
nat=auto
insecure=invite
ignoresdpversion=yes
host=ippbx.net2phone.com
dtmfmode=rfc2833
context=from-trunk
canreinvite=no
allow=ulaw
allow=g729

In "Incoming Settings", name the section "in-1" in "User Context"
Then, in "User Detail, enter the following:

disallow=all
type=peer
port=5060
nat=auto
insecure=invite
host=169.132.136.9
dtmfmode=rfc2833
context=from-trunk
canreinvite=no
allow=ulaw
allow=g729

After this has been completed, you will have to create a separate trunk. For the second trunk, name the outgoing "out-2" and again enter the following information:

type=peer
port=5060
nat=auto
insecure=invite
ignoresdpversion=yes
host=ippbx.net2phone.com
dtmfmode=rfc2833
context=from-trunk
canreinvite=no
allow=ulaw
allow=g729

Then, for the second trunk, name the incoming "in-2" and again enter the following information:

disallow=all
type=peer
port=5060
nat=auto
insecure=invite
host=66.33.167.74
dtmfmode=rfc2833
context=from-trunk
canreinvite=no
allow=ulaw
allow=g729

No registration string is required for IP Authentication.

Please make sure to configure your router/firewall to allow traffic from:

66.33.167.74:5060
169.132.136.9:5060
169.132.196.11:5060
66.33.146.52:5060

In addition, please allow all RTP traffic from any IP Address ports 10000-30000 UDP.

Digest Authentication *(Account & PIN)*
On open source applications (such as Asterisk), you can setup your SIP trunk for digest authentication as follows:

Peer Detail
username= <account>
type=peer
secret= <pin>
progressinband=never
port=5060
nat=auto
insecure=very
ignoresdpversion=yes
host=ippbx.net2phone.com
dtmfmode=rfc2833
context=from-trunk
canreinvite=no
allow=g729&g711&g723

User Detail
username=<account>
user=<>
type=user
port=5060
context=from-pstn
canreinvite=no
allow=g729&g711&g723
Register String
acct:pin@ippbx.net2phone.com/siptrunking

There are several GUI interfaces for Asterisk that simplify the installation process. These interfaces allow administrators to view, edit and change most configurations via a Web interface. Unless you are an advanced Asterisk user, we highly recommend downloading one of the following GUI interfaces:

Elastix
http://www.elastix.org/

PBX in a Flash
http://pbxinaflash.net/

AsteriskNOW
http://www.asterisk.org/asterisknow/

On other types of switch platforms, we recommend that you configure your switch as per your vendor guidelines (see Appendix). Please note that we do not provide direct technical support for end user SIP Trunking switch platforms. If your switch is not working as expected, you may need to contact the device manufacturer for technical support.

2) ***Which CODECs do you support?***

We support G711, G729 as well as G723. Generally speaking, we recommend that our customers offer G711 as well as G729 in their initial SIP INVITE to us.

3) ***How do I setup my dialing plan for outbound calling?***

You can choose a dialing plan when provisioning the account through our Partner Resource Center Web site.

If you choose the "Universal" dial plan in the Partner Resource Center, you can then dial in the following formats:
Country Code+ Phone Number
011+Country Code+ Phone Number
00+ Country Code + Phone Number.

US dialing plans are setup in the North American Numbering Plan (NANP) format of 1 + area code + 7 digit number (for US calls) and 011 + country code + number (for non-US calls). The 1 prefix should be used on all US calls. The 011 prefix should be used on all non-US calls. For more information on the NANP, please visit http://www.nanpa.com/index.html

If you choose to setup a non-US dialing plan, you will first have to configure your service account on our Partner Resource Center Web site with the specific dialing plan of your choice. Then you would dial exactly the same way you typically dial from within the country, with local calls being dialed in the way you normally dial local calls in country.

4) ***Which format should I use when setting up Caller ID in my switch?***

We recommend using the PAID (P-Asserted-Identity) option for CLI as per RFC 3325. Our platform also supports RPID (Remote-Party-ID). For more information, please visit http://www.ietf.org/rfc/rfc3325.txt

5) ***What ports should I open in my router/firewall?***

Please allow traffic from:

66.33.167.74:5060 UDP
169.132.136.9:5060 UDP
169.132.196.11:5060 UDP
66.33.146.52:5060 UDP

In addition, please allow all RTP traffic from any IP Address ports 10000-30000 UDP.

6) ***In what format should I configure the phone number for inbound routes?***

In order to receive inbound calls, you will have to build an inbound route on your switch and map it to a valid extension or ring group. Please make sure that you have configured the inbound route properly on your switch. Also, please make sure that you are allowing the inbound SIP traffic to pass to your switch from our proxy server (ippbx.net2phone.com).

We will send all inbound calls in the North American Numbering Plan (NANP) format of 1 + area code + 7 digit number (US calls) and 011 + country code + number (non US calls). This is how virtual phone numbers (DIDs) will display in the Partner Resource Center. You should input the DID in your inbound route in the exact format displayed in the panel.

7) ***Do you offer location based proxies so I can register with a proxy closer to my location?***

We currently offer four proxies for registration that will send both SIP and media packets from that location. However, registering with the default ippbx.net2phone.com proxy will also route media traffic depending on your location.

The proxy information and additional IP addresses necessary to clear your firewall are as follows:

Location: USA
Proxy: ippbx.net2phone.com
IP Address: 169.132.196.11
IP Address: 66.33.146.52

Location: Hong Kong
Proxy: siphk.net2phone.com
IP Address: 111.235.152.132

Location: United Kingdom
Proxy: sipuk.net2phone.com
IP Address: 213.166.103.5

Location: Brazil
Proxy: sipbr.net2phone.com
IP Address: 177.53.194.8
IP Address: 177.53.194.2

8) ***Which DTMF settings should I set on my switch?***

We recommend that you enable RFC 2833 payload type 101 for DTMF. Please note that DTMF is supported over our Platinum routes (prefix 99901) only.

9) ***How can I capture a SIP trace on my switch?***

When setting up a new SIP trunk with a provider or troubleshooting call failures, it's important to be able to capture a signaling trace of an outbound call. This is also important when troubleshooting SIP registration issues with a new provider.

In Asterisk, you can activate SIP debugging via the Asterisk CLI using the SIP set debug commands:

SIP set debug peer on
Turns on SIP debugging globally showing all SIP traffic to and from the Asterisk gateway

SIP set debug IP xxx.xxx.xxx.xxx
Allows you to debug only to and from a particular IP address

SIP set debug off
Turns off all SIP debugging

If you don't want to enable debugging on your switch, you can use a network protocol analyzer such as Wireshark to capture the SIP and media traffic on your calls. To learn more about Wireshark, please visit http://www.wireshark.org/. This site includes step-by-step videos on how to setup Wireshark on your network.

10) ***Which protocol do you support for fax transmissions?***

Generally speaking, we support T.38 protocol as well as G711 pass-through for fax transmissions. The majority of our carriers prefer T.38 protocol.

Appendix

Support links to various switch vendor platforms:

Asterisk - Support Forum
http://forums.asterisk.org/

3CX - Support Forum
http://www.3cx.com/forums/

Avaya - Support Forum
http://support.avaya.com/css/appmanager/public/support

Elastix - Support Forum
http://www.elastix.org/index.php/en/component/kunena/

Trixbox - Support Forum
http://fonality.com/trixbox/forum

Grandstream - Support Forum
http://forums.grandstream.com/forums/

Cisco - Support Forums
http://www.cisco.com/cisco/web/support/index.html

FreePBX - Support Forum
http://www.freepbx.org/forums

Talkswitch - Support Forum
http://www.talkswitch.com/us/en/support/

AudioCodes - Support
http://www.audiocodes.com/support

Voipswitch - Support
http://www.voipswitch.com/

IPsmarx - Support
http://www.ipsmarx.com/Support.html

Huawei - Support
http://support.huawei.com/support/

Sonus Networks - Support
http://sonusnetworks.force.com/PortalLoginPage

PortaOne - Support
http://portaone.com/support/portacare/